

Risk Analysis of GPS-Dependent Communications Critical Infrastructure Utilized by the US
Electric Power Grid

A Thesis

Presented to
the faculty of the School of Engineering and Applied Science
University of Virginia

in partial fulfillment
of the requirements for the degree

Master of Science

by

Joshua M. Bogdanor

May

2014

APPROVAL SHEET

The thesis
is submitted in partial fulfillment of the requirements
for the degree of
Master of Science


AUTHOR

The thesis has been read and approved by the examining committee:

Dr. Yacov Y. Haimen

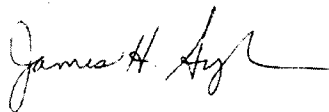
Advisor

Dr. Barry M. Horowitz

Dr. Garry M. Jacyna

Dr. James H. Lambert

Accepted for the School of Engineering and Applied Science:



Dean, School of Engineering and Applied Science

May
2014

Abstract

The nation's Critical Infrastructure (CI) forms a complex System of Systems (S-o-S) comprised of 16 sectors defined by the United States Department of Homeland Security (DHS). This S-o-S is characterized by myriad interconnections and interdependent subsystems. Of these 16 sectors, the communications sector and electricity subsector provide basic functionality to one another, as well as to the remaining 14 sectors of CI. As the nation moves forward with Department of Energy's (DOE) Smart Grid initiative, the dependence of these sectors upon GPS timing is rapidly increasing. Under this initiative, the electricity subsector becomes dependent upon GPS timing through the proposed use of Phasor Measurement Units (PMUs) for determining control actions on the grid, as well as by the already existing dependence on GPS timing through communications CI utilized by the electricity subsector for the transmission of PMU and Supervisory Control and Data Acquisition (SCADA) data. While there is extensive literature addressing GPS timing dependency of PMUs in the electricity subsector, this thesis provides a systematic risk analysis of the threats to the electricity subsector through the use of GPS timing dependent communications CI. This thesis provides a methodological approach for first assessing the risks to the US electric power grid through the use of GPS-dependent communications CI to carry both PMU and SCADA data, and then determining risk management options for mitigating the risk to electricity subsector through the use of GPS-dependent communications CI. The thesis builds upon fault and event tree analysis, and addresses scenario development for events with unknown likelihoods.

Acknowledgments:

I would like to thank a few of the many people who have made putting together this thesis possible. First and foremost I would like to acknowledge my advisor, Yacov Haimes. Professor Haimes, has helped me with much more than just my thesis research, and has served as not just an advisor, but also as a mentor. I did not expect in coming to the University of Virginia to have my way of thinking about and approaching problems so radically impacted over the two year course of the MS program. A large reason for these changes has been the overwhelmingly positive influence of working with Professor Haimes, and gaining from his keen insights in fields ranging from risk analysis to modeling, to general philosophy. It has been an absolute pleasure to work with Yacov, and I can proudly say that I stand on the shoulders of this giant.

Thank you goes to Erika Evans, the manager of the Center for Risk Management of Engineering Systems, for all that she has done to help this research and me personally over my time at Virginia. Erika has been amazing to work with, and was an essential component to the completion of this thesis as well as my degree in general here at UVA.

I also want to thank the team from MITRE for their help with completing this thesis. The team of Garry Jacyna, Mike Tierney, and Mike Cohen provided invaluable support from day one of this thesis. The team at MITRE helped guide me into a tractable and meaningful path for addressing GPS timing concerns within critical infrastructure, and helped to steer the course over the life of this project. I am thankful that the team would make sure to clear time in their schedules to meet with me when I came up to MITRE, and a special thanks goes to Dr. Jacyna for making time to meet and discuss this thesis research on multiple occasions at the University of Virginia.

The capstone team of Nick Maupin, Kenneth Chen, Cedric Heckel-Jones, and Sam Ruben also provided valuable support over the course of this research. In helping to advise their capstone project, it provided me with a weekly sounding board to bounce ideas off of. Their questions in our weekly sessions forced me to pay extra close attention to the technical aspects of this project so that I would be able to provide answers. It was of great benefit to work with these young men, and have the opportunity to see how they dealt with similar challenges related to the technical aspects of this thesis, and have the chance to work together on overcoming them.

Linden Mercer of the Naval Research Laboratory deserves a special thank you for providing a tutorial on the timing requirements of communications systems, and the use of GPS disciplined oscillators. When Linden heard about my research from my father, he took an immediate interest in

helping in whatever way he could. At the crux of this thesis is the relationship between GPS timing and communications system networks, without Linden's help, I do not think that I would have been able to properly quantify these relationships.

I would like to thank my parents, Jim and Lyric Bogdanor, for their encouragement to go back to school and pursue this degree. Without their continual and unconditional support, I would most likely not have pursued this degree, and would have missed out on this invaluable educational experience. My brother, Mike Bogdanor, also deserves acknowledgement and thanks for his support throughout this process. I would like to thank Mike for not only his support and encouragement, but also for his willingness to take late night calls to talk about whatever was on my mind, whether it was discussing challenges in my research, or answering questions about computer programming; thank you Mike.

Last but not least, I would like to say a special thank you to my wonderful fiancée, Charlene. Whether it was sending me articles related to my project, driving 3 hours to bring me a notebook I had lost, or just listening to me work through problems out loud, without her, none of this would have been possible. Thank you Charlene, I love you.

To the many others who helped along the way, thank you.

Table of Contents

1. Problem Definition and Motivation	6
2. Review of the Literature	11
3. Technical Understanding of the CI System of Systems	13
3.1 GPS Timing	13
3.1.a GPS Disciplined Oscillators	15
3.1.b Applications of GPS Timing	15
3.1.c Risks to GPS Timing	16
3.2 Electricity Subsector	18
3.2.a The Electricity Subsector and the evolving base	19
3.2.b Dependencies upon GPS Timing	21
3.3 Communications Sector	22
3.3.a GPS Timing within the Communications	23
3.4 PMU/SCADA Systems	24
3.4.a Phasor Measurement Systems (PMUs)	24
3.4.b Supervisory Control and Data Acquisition (SCADA) Systems	25
3.5 Other 14 Sectors of Critical Infrastructure	26
4. Methodological Approach Outline	27
4.1 Modeling Interconnections of CI S-o-S	28
4.2 Shared States	31
4.2.a Identifying Essential States	31
4.2.b Shared State Variables	42
4.2.c Characterizing Interdependencies through Shared States	43
4.3 Fault Tree Analysis	44
4.3.a Electricity Subsector Failure Fault Tree	46
4.4 Event Tree Analysis	48
4.4.a Communications Failure Event Tree	48
4.5 Shared Decisions Revisited	52
4.6 Risk Filtering, Ranking, and Management	55

5. Discrete Event Simulation Model and Results	60
5.1 Discrete Event Simulation Model Outline	61
5.2 Discrete Event Simulation Model Implementation	62
5.3 Discrete Event Simulation Model Results	69
6. Conclusions	70
6.1 Key Challenges	71
6.1 Summary of Contributions	72
6.2 Recommendations for Future Research	73
7. References	75
 Appendix A. RFRM Characteristics	 78
Appendix B. Discrete Event Simulation SIMAN Code	79

1. Problem Definition and Motivation

The nation's critical infrastructure (CI) forms a complex Systems of Systems (S-o-S) comprised of 16 sectors defined by the Department of Homeland Security (DHS), characterized by myriad interconnections and interdependencies. Due to the high degree of complexity and interconnectedness amongst these CI systems, oftentimes there is a requirement for synchronization with sub-microsecond accuracy. The electricity subsector (part of the energy sector of CI) and the communications sector of CI have such requirements to provide basic functionality, power and communications, not only within their own sector, but across all other sectors of CI.

Providing accurate time-of-day and frequency measurements across long distances is a complicated process that has benefited greatly through the use of the Department of Defense (DoD) owned and operated Navstar Global Positioning System (GPS) to do just this. The United States Naval Observatory (USNO), from whom GPS derives its system time, admonishes GPS as "the most competent system for time transfer." While this may be the case, GPS timing is not without risks, and the reliance upon GPS timing within the electricity subsector and communications sector of CI introduces vulnerabilities within these sectors, and across the CI S-o-S as a whole, to GPS anomalies both naturally occurring and intentional.

The vulnerabilities introduced through reliance upon GPS timing for synchronization of systems within the electricity subsector and communications sector are exacerbated by the advent of Smart Grid initiatives. The Smart Grid initiative from the Department of Energy (DoE) encompasses many potential changes within the electricity sub-sector; one of the largest changes is that of pursuing autonomous control across the grid. While the driving force behind this change from human-in-the-loop to

automated control promises improved efficiency and reliability associated with electric power; the change brings new requirements for timing along with a new set of risks and vulnerabilities.

The introduction of phasor measurement units (PMUs) within the electric power grid has given many researchers hope of achieving autonomous control through leveraging extremely accurate synchrophasor measurements provided by PMUs. These synchrophasor measurements capture voltage and current phase and magnitude measures along with a GPS derived timestamp. PMU systems sample at a rate on the order of 60 times a second at a given node, and compare measurements amongst measurement stations across wide areas to determine the state of the grid. At current time, these measurements are used primarily for grid forensics following anomalous events; however under full Smart Grid implementation these measurements would be used to issue automatic controls to the grid. If the timestamps associated with measurements from a given node became compromised, at best, the data would be unusable; while at worst, if these systems were to issue improper control actions based on erroneous measurements there could potentially be cascading blackouts.

In addition to the increased dependency upon GPS timing within the electricity subsector through the use of PMUs, there is also an increased dependency through the communications methods employed by the electricity subsector. As the amount of data that will need to be transferred to and from PMUs is greatly increased from previous Supervisory Control and Data Acquisition (SCADA) requirements due to the increased measurement rate, from one measurement every few seconds to 60 every second, and the increased resolution of each measurement, electricity utilities will need to rely more and more upon carriers within the communications sector of CI to meet this need. Many of the networks utilized by communications carriers require frequency derived from GPS to synchronize transmissions and ensure the transfer of data between nodes. If the GPS derived frequency differs past acceptable thresholds between nodes, messages cannot be recovered, and the information acquired

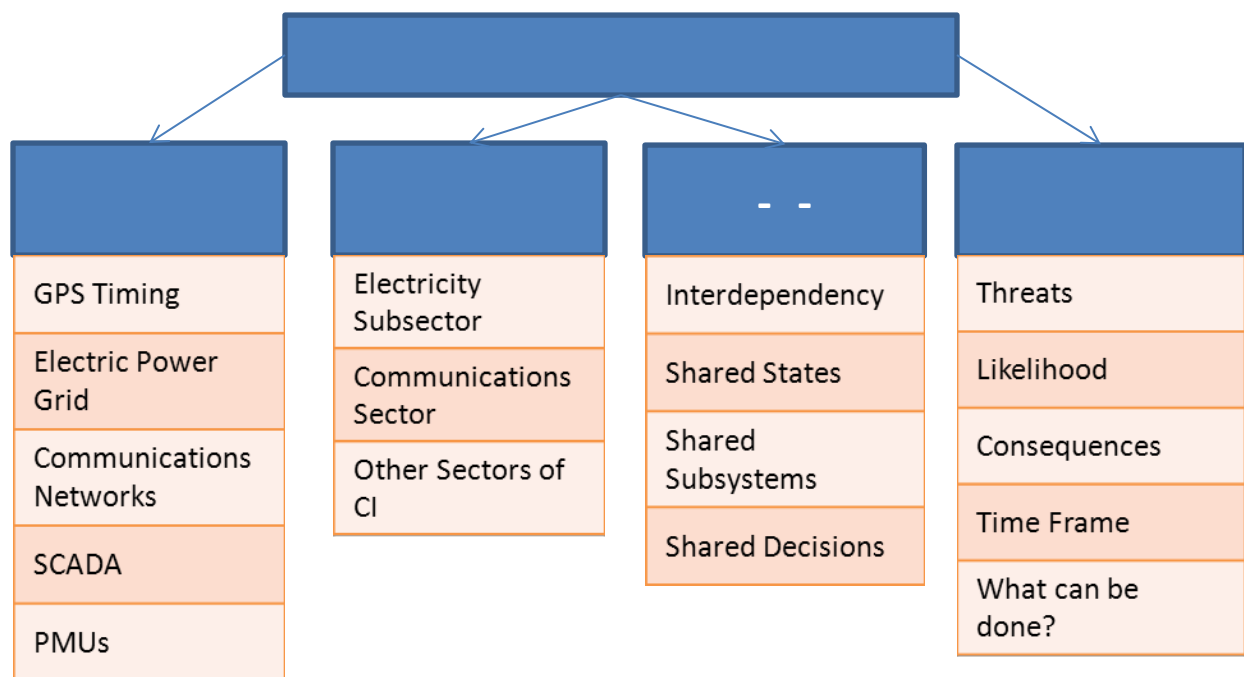
from affected PMUs could be lost. If the loss of these communications coincided with a change in the state of the grid necessitating prompt action, the consequences could be catastrophic.

There exists a complex S-o-S composed of GPS Timing, the electricity subsector, the communications sector, and SCADA/PMUs. While the electricity subsector provides the vast majority of their own communications, in determining the designation of a specific system to a sector of CI, the main determining factor is that of ownership. Note that S-o-S can be characterized not only by shared states and subsystems, but also by shared decisions. The vulnerabilities of the electric power grid to GPS timing disturbances originate not only from the introduction of PMUs and automated control, but also from the impact of shared decisions with the communications sector. Decisions made by the communications sector with consequences shared across the board.

This research explores the level of interconnectedness and interdependency amongst GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems in order to address the risks facing the electricity subsector from a GPS timing based attack. In doing so, this research establishes a methodological approach for analyzing complex and interconnected S-o-S through exploitation of shared states, subsystems, and decisions. The research builds upon fault- and event-tree analyses to develop scenarios for which subsequent risks to the S-o-S can be assessed and subsequently managed.

Modeling complex S-o-S requires an iterative approach encapsulating multiple perspectives and representative models. More specifically, to model the S-o-S, which is comprised of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems, the degree of coupling among these four sectors must be assessed, and the associated risks resulting from these interdependencies must be addressed (see Figure 1).

Furthermore, to model the above S-o-S it is important to first gain a degree of understanding of the technical aspects of each of the included systems. Models should be as simple as possible, yet as complex as required. While the modeling efforts in this thesis do not duplicate every technical aspect within the S-o-S, such as the algorithms within the disciplined oscillators of GPS timing systems; this research is cognizant of the complex technical nature of each component within the S-o-S. Through exploring each subsystem from its technical perspective, initial models for each subsystem have been developed in terms of essential state variables.



(Figure 1) Multiple perspectives to modeling the vulnerability of the electricity subsector to GPS timing based attacks.

While the technical perspective to approaching this problem considers the problem “one piece at a time,” the complimentary big picture view encompassing the impacts of vulnerabilities to GPS timing disturbances on the sector-wide scale is equally important. Due to the level of interconnectivity amongst systems within the electricity subsector, it is essential to explore the propagation of the resulting consequences throughout the entire system from events impacting GPS timing. The same

approach can be applied to the communications sector, as well as to the other 14 sectors of CI. This high-level view builds upon the insights gained from modeling the S-o-S subsystems from a technical perspective.

In developing understanding of the interconnections and interdependencies amongst the components forming this S-o-S, we explore these linkages through shared states, subsystems, and decisions. From the technical perspective, and the development of technical models based upon state variables and physical components to each system, this research identifies shared state variables as well as shared subsystems amongst the systems from our S-o-S to gain better understanding into the degree of interconnection amongst these systems. In addition, from exploring the CI impacts, the research identifies shared decisions between the electricity subsector and communications sector. The shared decisions have important implications to the risks facing the electricity subsector especially, from decisions they share with the communications sector.

The final perspective with which this thesis addresses is that of the risks facing the S-o-S through GPS timing disturbances. This perspective builds upon the technical understanding of the S-o-S, as well as the impacts on CIs, and interdependencies through shared states, subsystems, and decisions. It is imperative to understand how the systems comprising the S-o-S in question are connected so that the associated risks may be properly assessed. In risk assessment, there are four basic questions to address, the first three from Kaplan and Garrick in 1981, and the fourth was added by Haimes in 1991: (1) what can go wrong? (2) what are the consequences? (3) what is the likelihood? and (4) what is the time frame?

Combining these four perspectives together, this thesis employs Fault Tree Analysis to gain further insight into the interconnectedness of these systems through the exploitation of shared state variables and subsystems. Due to the sensitive nature of CI research, the development in fault trees is

not necessarily for determining the numerical reliability of these systems; rather, to gain a better understanding of the interdependencies and interconnections between these systems. From here, the research builds upon the combined fault tree analysis with event-tree analysis to develop scenarios that capture the essence of “what can go wrong?” from a GPS timing attack to the consequences felt within the electricity subsector. The use of event-tree analysis to augment the fault tree analysis is a solution to the lack of numerical likelihoods from open literature. As this research considers the likelihoods associated with events such as GPS spoofing attacks against US CI, no information exists on these occurrences within the open literature. However, by building scenarios to capture the essence of these events, we are still able to determine the impact of risk management solutions upon the likelihoods of consequences, without needing to determine the actual underlying likelihoods of these events occurring. We set forth a framework for modeling the complex S-o-S comprised of GPS timing, the electricity subsector, communications sector, and SCADA/PMU systems, from a systems-based perspective, so that agencies with access to the appropriate likelihoods related to the scenarios described in the research, can determine the associated likelihoods with given consequences.

2. Review of the Literature

With the advent of Smart Grid initiatives calling for continuous real-time monitoring of the electric power grid, the criticality of GPS dependent precision timing is increasing. The shift to the use of *phasor measurement units* (PMUs) which utilize clocks synchronized by GPS from *supervisory control and data acquisition* (SCADA) systems which do not take synchronous measurements coupled with the possibility of using GPS dependent communication architectures has introduced new vulnerabilities to the electric power grid.

While a large portion of the literature (Carta et al. 2009, Das et al. 2012, Zhong et al. 2005, etc.) on PMU Systems treats the accuracy, availability, and integrity of GPS Timing as a given, Sheppard et al.

(2012) have shown that PMUs are vulnerable to GPS spoofing attacks. Their research has shown that it is possible in only a few microseconds for a GPS based attack to push an electric power system past the maximum allowed phase error. Further, they have shown that in a preexisting system in Mexico at the current time a GPS spoofing attack could trip a generator.

This research built upon the work of Humphreys (2009) in which he demonstrates the simplicity of the system necessary to carry out such a spoofing attack. Humphreys goes on to suggest possible countermeasures, which aid in the development of risk management alternatives in this thesis research. The work of Jiang et al. (2013) also calls for the need of developing countermeasures to the GPS Spoofing threat to phasor measurement units, as they also demonstrated the feasibility of a GPS spoofing attack disrupting the electric power grid.

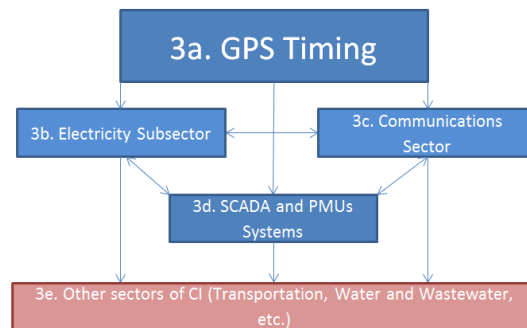
Due to the large amount of data generated by PMUs many options for communicating data between PMUs and Phasor Data Concentrators (PDCs) are being considered. In their survey of Smart Grid possibilities, Fang et al., in 2012, cite the potential structure for a Smart Grid system outlined in the frequency network (FNET) project of Zhang et al. (2010). The survey goes on to list five wireless and two wired communications infrastructure possibilities to facilitate the data transfer under this structure. The five wireless communication possibilities: (1) wireless mesh network (WMN), (2) cellular communications, (3) cognitive radio, (4) IEEE 802.15, and (5) satellite communications. The two potential wired communication methods: (1) fiber-optic communications and (2) power line communications.

While the survey from Fang et al. does not explore the dependence of these communication forms on GPS timing, they do mention the need for time synchronization in certain cellular communication protocols (i.e. CDMA), as well as in certain cognitive radio infrastructures (i.e. WirelessHart). As the investigation of the dependence upon GPS timing for communication forms was beyond the scope of

this survey, it is necessary in this research to identify any communication option in which GPS timing introduces added vulnerability to the electric power grid.

3. Technical Understanding of the CI System of Systems

The S-o-S for which we conduct this risk analysis is comprised of four major systems: GPS Timing, the Electricity Subsector, the Communications Sector, and PMU/SCADA systems (see Figure 3).



(Figure 3) Hierarchical S-o-S Model

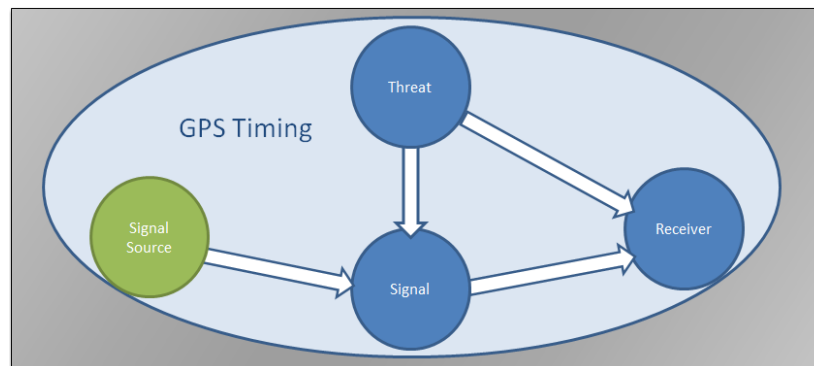
3.1 GPS Timing

GPS Timing is provided by the NavStar Global Positioning System, which is a Global Navigation Satellite System (GNSS) owned and operated by the United States Department of Defense (DoD), and a S-o-S in its own right. GPS is comprised of a constellation of 31 satellites in 6 geocentric elliptical orbits operating at 60 degrees inclination. In addition to the satellites themselves, there are five ground control stations spread across the globe as well as several ground augmentation systems that provide differential GPS (DGPS) functionality to users. DGPS accounts for atmospheric anomalies in calculating position, velocity, and timing (PVT) for users and improves the overall accuracy of measurements provided by GPS.

As GPS itself is a system of systems in its own right, for the purpose of this research, we use a simplified model of GPS Timing comprised of four main sub-systems: signal source, signal, receiver, and

threat (see Figure 3.1). The signal source is comprised of the satellites themselves, as well as the control stations and ground/space augmentation systems, which help to provide users with DGPS functionality. Due to the sensitive nature of these specific components to the security of the nation, as these systems also help to control the weapon systems of the US, they are treated as exogenous variables in this thesis.

Since the event of a threat to the actual sources of the GPS signal are beyond the scope of this thesis and research, the threat modeled here on is considered only to the point of impacting the signal received or the receiver of the GPS signal.



(Figure 3.1) GPS Timing Sub-model

The signal in this model is typically classified by three main characteristics: availability, accuracy and integrity. The state of signal availability within this research is a measure of the likelihood that GPS timing services are accessible by a given receiver. In general, GPS availability across the continental US, approaches availability levels of 100 percent of the time available (Hsiao and Massimini, 2006). Events such as intentional GPS jamming aim to alter this state of signal availability, and remove the option of GPS timing functionality to affected receivers. GPS timing provides timing information to users accurate to within 100 billionths of a second of UTC time. The accuracy of these signals in addition to their

integrity comes into play in the event of spoofing attacks, in which false signals are produced in an effort to “trick” receivers into believing that the time is different than what it actually is.

3.1.a GPS Disciplined Oscillators

The use of GPS Disciplined Oscillators (GPSDO) has become common practice for many precise timing and frequency applications due to the cost benefits when compared with more expensive atomic clocks that provide similar levels of accuracy. GPSDO systems utilize the precise timing information provided by GPS in order to steer much less accurate oscillators to a nominal frequency. These systems work by averaging the GPS signal characteristics with those of the internal oscillator, providing long term stability. While higher quality quartz and rubidium oscillators offer excellent short term stability, over time these oscillators can be influenced by natural bias and drift from nominal frequencies. The addition of disciplining through GPS timing information provides the best of both worlds, providing both short and long term stability to these systems. One major concern with the utilization of GPSDO systems lies within the inherent vulnerability to GPS spoofing attacks. There exists a risk that a GPSDO system can be steered away from the nominal frequency during a GPS spoofing attack. While GPSDO systems can be equipped with spoofing detection measures most commonly based upon discriminating signals based upon relative or absolute signal strength or on the implied rate at which these oscillators drift, attacks have been designed to circumvent these risk management strategies (Wesson 2013). GPSDO implementation provides a less expensive timing alternative to atomic clocks; however, the introduction of these technologies into timing applications associated with CI inserts new vulnerabilities to spoofing attacks into the entire system.

3.1.b Applications of GPS Timing

GPS timing is used to provide accurate and precise timing to many CI applications including utilization in both the electricity subsector and communications sector of CI. Within the electricity

subsector, GPS timing serve as the primary source for acquiring time stamps of PMU measurements. With Smart Grid initiatives predicting automatic control within the electricity subsector based upon PMU measurements by 2030, GPS timing plays a critical role in the development of Smart Grid architectures. Within the communications sector, GPS timing is used in virtually every type of communications network, ranging from the public switch telephone network (PSTN), to cellular communications, as well as internet communications. Synchronous Optical Networking (SONET) also leverages the accuracy of GPS timing for network synchronization. SONET systems are used across the nation, and serve the electricity subsector, establishing another dependency of the electricity subsector upon GPS Timing.

3.1.c Vulnerabilities of GPS Timing

GPS timing systems are vulnerable to threats both naturally occurring and intentional. The primary focus of this research is that of intentional threats. Intentional attacks against GPS timing systems come in two varieties, GPS jamming attacks, and GPS spoofing attacks. GPS jamming attacks attempt to stop receivers from acquiring GPS signals, thus preventing GPS timing systems from being able to use GPS timing functionality. While most applications of GPS timing have internal oscillators that have some holdover capability, the ability for GPS timing systems to maintain timing/frequency within an acceptable range depends largely upon the quality of oscillator, the duration of the outage, and the specific application for which these systems are used. For communications sector applications, the PSTN and internet there exists a requirement of timing resolution accurate to within 62.5 μ s to insure that frames of information do not slip, resulting in the loss of information. PMUs implemented within 60 Hz electric subsector applications require an accuracy of 26 μ s according to IEEE standard C37.118.2-2011. When devices no longer have the timing provided by GPS, the quality of the backup clock system comes into play. Clocks are classified into a hierarchy known as Stratum, with Stratum 1 clocks describing clocks of the highest accuracy followed by, Stratum 2, Stratum 3E, and finally Stratum 3. Stratum 1

clocks have a time offset per day of less than one microsecond, while Stratum 3 clocks have a frequency on the order of tens of milliseconds per day (THE PRESIDENTS NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, 2008). This discrepancy equates to holdover times for which communications applications can still function based upon relying on these back up clocks ranging from 72 days for Stratum 1 clocks to as little as three minutes for Stratum 3 clocks, and for PMU utilization from one month for Stratum 1 to just over one minute for Stratum 3 clocks. If GPS timing were to be lost for extended periods of time, even the best backup clocks could become useless for these precision applications.

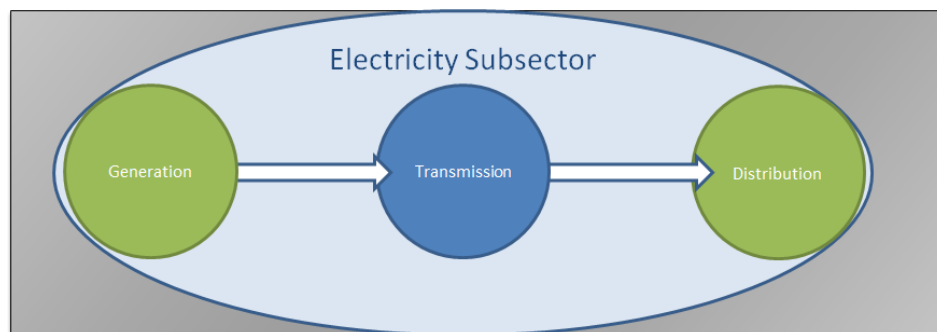
Two highly publicized and well-documented cases of GPS jamming, the San Diego Harbor Naval jamming event of 2007, and the Newark Airport event of 2013, highlight the reality of the threat of GPS jamming attacks to CI systems. In the latter event, a civilian using a personal jamming device unintentionally jammed GPS signals at Newark Airport, disrupting air traffic control towers. In the San Diego event, an intentional disruption of radio signals for a Naval training exercise had unintended consequences when the jamming also disrupted GPS signals. While the exercise lasted for only a few hours, the event impacted transportation, financial, and communications CI. Following the event, it took three days to discover the source of the disruption. This event highlights an ideal situation for detectability, given that it was not intentionally hidden and originated from a stationary source; this implications for the ability to discover an intentional attack that may be moving and actively trying not to be discovered imply that there exists the potential for GPS jamming events of much greater duration.

The threat of GPS spoofing attacks is of greater concern due to their ability to bypass detection schemes. The Radionavigation Laboratory at the University of Texas has conducted numerous experiments in which they have demonstrated the reality of the threat of GPS spoofing to numerous CI systems (Humphreys 2009). By designing attacks that bypass detection schemes, GPS spoofing can wreak true havoc on a system by deceiving the system into believing things are not as they seem. If a

GPSDO believes that it needs to adjust its frequency when it is on the proper frequency, it can be pulled away from UTC and not realize it until the application for which the GPSDO supports also fails. At this point in time, as demonstrated by the difficulty in diagnosing the San Diego Harbor incident, it may not even be possible to readily attribute the failure to a GPS spoofing attack. Even in the event of detection, if GPS timing devices were sent into “holdover” modes, these clocks would still be constrained by the same frequency instabilities as those experiencing a GPS jamming attack.

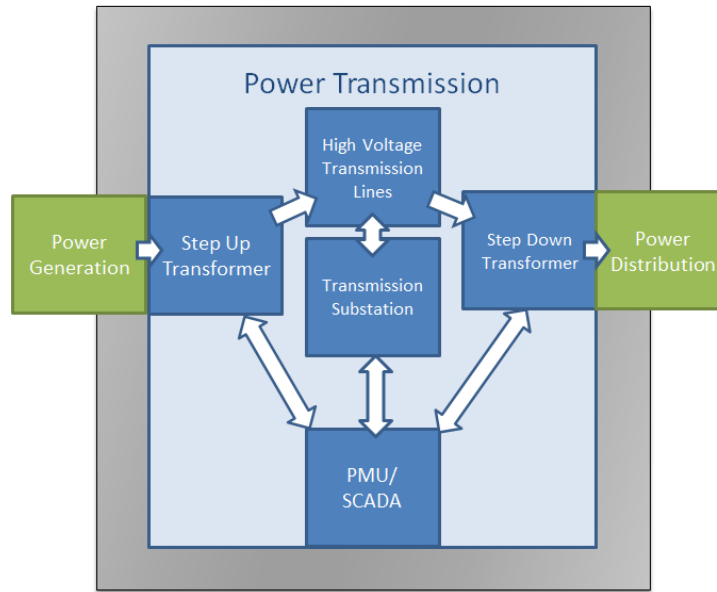
3.2 Electricity Subsector

The Electricity Subsector CI represents a complex S-o-S comprised of many people, organizations both public and private, billions of dollars of physical infrastructure spread across the nation, and is subject to numerous local and national policies and initiatives. For the purpose of understanding the risks to the electricity subsector through its dependence on GPS timing, we take a generalized look at the electricity subsector (Figure 3.2-1).



(Figure 3.2-1) Electricity Subsector Sub-model

The life cycle for electricity in the power grid can be described by three main phases: generation, transmission, and distribution. In the transmission phase of the life cycle, PMU/SCADA systems are used to measure and monitor the state of power flow across the grid. The PMU measurements require accurate timestamps provided by GPS timing. For this thesis, the electricity subsector transmission component is investigated using the model depicted in Figure 3.2-2.



(Figure 3.2-2) Power Transmission Sub-model

In order for electricity to be transmitted across long distances, the voltage is stepped up at transformers to ultra-high voltage so that the current can be kept low to minimize power losses. Electric power then crosses large areas of land on high voltage transmission lines, which are connected at transmission substations, before eventually being stepped back down to be distributed to consumers. These transformers and substations represent nodes on the electric power grid, which must be kept to within given levels of phase in terms of both current and voltage synchrophasors. This is why PMUs are used at select nodes to measure the state of the grid and inform operators of control decisions to be performed on the grid.

3.2.a The Electricity Subsector and the Evolving Base

Timeframe plays an important role when addressing what are the risks facing the electricity subsector from dependency upon GPS timing. At current time, control actions are performed by human-in-the-loop systems relying on data from SCADA systems to measure and monitor the state of the electric grid. According the North American Synchrophasor Initiative (NASPI), by the end of 2014,

virtually the entire transmission system of the United States will be able to be monitored by a network of 1100 PMUs (U.S. Department of Energy, 2012). While the current use of PMUs within the grid is to monitor the state of the electric power grid, providing support and information to human operators, Smart Grid initiatives call for PMUs to provide automated control within the grid.

The shift from SCADA based control schemes to PMU automated/semi-autonomous control schemes represents a dramatic shift in the portfolio of risks from the current electric grid to that of the 2030 grid, the predicted date of full Smart Grid conversion. SCADA systems take measurements on the order of once every four to six seconds, while PMUs measure at a rate on the order of 50 measurements per second. This dramatic increase in the amount of data compounded by an increased amount of data within each PMU measurement compared to those of SCADA raises the demand for data transmission capacity within the electricity subsector. It remains to be seen if the electricity subsector is capable of keeping up with the demand for this increased data transmission capability, however it is not unlikely that electricity utilities will increase their utilization of networks falling under the classification of communications CI. This shift towards greater reliance upon communications CI within the electricity subsector exposes the electricity subsector to risks also facing the communications sector. This raises the question of “what is an acceptable level of risk, and for whom?” Due to the reliance of the electricity subsector upon the communications sector in this scenario for providing data transmission to PMU systems, it is imperative that the decisions made by the communications sector regarding choices of network components and topology take into account the risk tolerance of the electricity subsector for communications outages.

Current decisions regarding electric grid control actions are constrained by the response time of human operators, while in future Smart Grid implementations, certain control actions are predicted to be made and delivered to substations for implementation in as little as 3 ms (Wang et al., 2011). In the

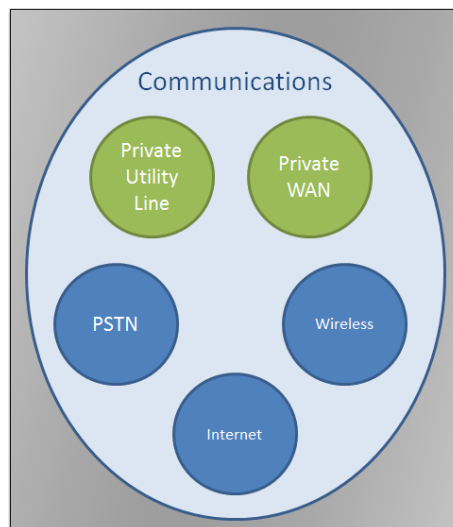
scenario of future Smart Grid implementation, near immediate actions increase the vulnerability of the system to the execution of unnecessary control actions. If a PMU system begins issuing improper control decisions, due to the immediacy of these actions, by the time a problem is realized, it may be too late to reverse the consequences. This change in system architecture, requirements, and subsequent risks represents an evolving base within the electricity subsector moving from the current state to the Smart Grid. As the Smart Grid moves forward, it is important to keep future considerations at the forefront, and consider the impact of current decisions on future options.

3.2.b Dependencies upon GPS Timing

Keeping in mind the importance of timeframe, the dependency of the electricity subsector is anticipated to increase dramatically over the next twenty years due to Smart Grid implementation. Currently, the electricity subsector relies upon GPS timing for the synchronization of communications networks both owned privately by the utilities themselves and for those from communications CI carriers. While the demand for synchronous networks increases over time due to Smart Grid considerations, the dependence of the electricity subsector on GPS timing to provide communications network synchronization is expected to increase. In addition, with PMUs taking an increasingly important role in the control of the electric power grid, the electricity subsector will have greater dependence upon GPS timing in order to measure, monitor, and control the grid through the reliance upon PMUs. GPS timing plays a critical role in the future of the Smart Grid, and the inherent vulnerabilities within GPS timing systems to both jamming and spoofing attacks must be addressed within the context of how the consequences following these attacks permeate throughout the entire electricity subsector.

3.3 Communications Sector

The communication networks serving the electricity subsector are formed by the conglomeration of five main sources: private utility lines, private wide-area networks (WAN), the public switch telephone network (PSTN), wireless communications, and the internet (see Figure 3.3).

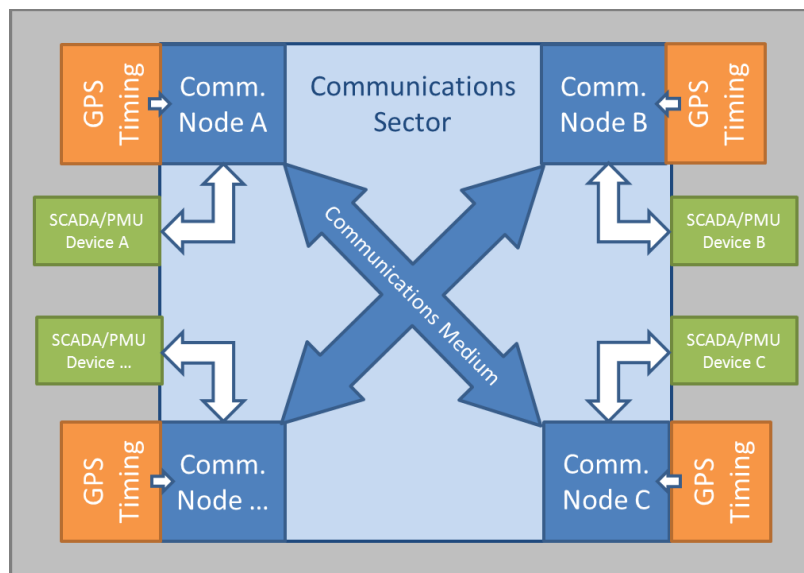


(Figure 3.3) Communications Utilized by Electric Utilities

As the electric utilities rely upon the infrastructure provided by public for-profit communications companies to provide a portion of their communications, as is the case with the last three systems: PSTN, wireless, and internet; it is essential for the utility companies to understand the risk posed to the power grid from reliance on these communications sources. This research focuses upon those communication methods depicted in Figure 3.3 in blue, those owned and operated by communications CI carriers. This subset of communications utilized by the electricity subsector is of particular importance due to the implications upon risks to the electricity subsector through shared decisions with the communications sector.

3.3.a GPS Timing within the Communications Sector

Within the communications sector, for the purposes of the thesis, only networks dependent upon GPS timing, servicing the electricity subsector, are considered. Within PSTN, internet, and wireless networks, GPS timing serves as the primary means for network synchronization. Due to the vast array of assorted networks servicing the electricity subsector, a generic representation of the communications sector as utilized by the electricity subsector is depicted in Figure 3.3a. The communications sector is comprised of network of nodes, with each node relying upon GPS timing in some form or fashion. This dependency may stem from the use of a GPSDO or from a network of GPS dependent master clocks steering the local timing and frequency applications. These nodes are connected through some medium, for instance telephone lines, fiber optic cable, or through air for wireless communications. Each of these nodes represents a contact point to the network SCADA/PMU devices. These SCADA/PMU devices could be measurement devices, controllers, or control centers, regardless of the specific type of device, they must be connected to some network through a given communication node in order to function within the grid.



(Figure 3.3a) GPS-Dependent Communications CI as Utilized by the Electricity Subsector

These communications rely upon GPS timing to provide accurate frequency measures to allow networks to maintain basic send/receive functionality across all nodes. In the case of SONET, information is sent across fiber-optic cables between nodes. In order for data to be read at its destination, it is important for the information to be read at a pre-specified rate, this is where GPS timing comes in. GPS timing provides this accuracy frequency reference so that the data received can be interpreted. SONET transmits data at a frequency of 8000 Hz, equating to 8000 frames every second, or one frame every 125 μ s. In the event that every node were exactly calibrated to UTC, if one of said nodes drifted 125 μ s away from the standard time, frames would slip in the delivery of data amongst nodes with the affected node, and information would be lost. If this assumption that all other nodes are exactly on time is removed, then as long as all nodes are within 62.5 μ s of UTC, communications are unaffected by GPS timing discrepancies. This timing accuracy requirement is the same for both PSTN and internet networks.

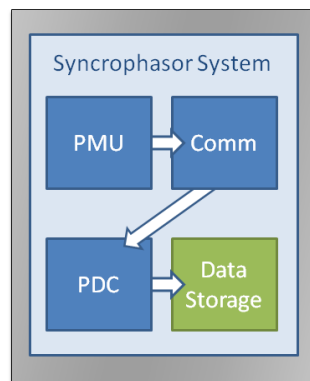
3.4 PMU/SCADA Systems

The control actions issued across the electric power grid are made based upon measurements primarily collected from SCADA systems. As the electric power grid evolves and transitions towards more autonomous and semi-automated control, the use of PMUs for both collecting data and implementing control is growing. In order to issue control actions to address faults in the power grid, decisions must be made on the scale of milliseconds, for which the PMU depends on GPS timing for this degree of accuracy.

3.4.a Phasor Measurement Systems (PMUs)

PMUs are used to measure synchrophasors, which are measurements of magnitude and phase angle of voltage and current accompanied by a timestamp accurate to microseconds. The PMU is a piece of a larger synchrophasor system. The synchrophasor system includes the following components:

PMU, communications, phasor data concentrator (PDC), and data storage (see Figure 3.4a). The PMU takes on the order of 60 measurements per second, with a high degree of accuracy. Due to the volume of data which PMUs collect, fiber optic lines are used primarily to transmit data from PMUs to a centrally located PDC. The dependence upon GPS timing for accurate timestamps impacts the synchrophasor system at both the PMU and communications components. If GPS timing were to fail within the PMU itself, measurement data could be unusable or worse. In the event of a GPS spoofing attack, measurement data from affected PMUs may indicate the need for unnecessary action to be taken. If these control actions are implemented, there exists a potential for the power grid to be pushed from an acceptable state to an unacceptable one without operators even noticing this has happened until it is too late.



(Figure 3.4a) Synchrophasor System Sub-model

3.4.b Supervisory Control and Data Acquisition (SCADA) Systems

While SCADA systems do not require time-synchronous measurements, and thus do not have direct dependence upon GPS-timing, they still play an important role in state-estimation for the electric power grid. As of the current time, SCADA systems greatly outnumber their PMU counterparts, and serve as the primary mechanism for control the state of the electric power grid. These systems take measurements of the power grid and communicate the information with control centers, who in turn communicate back to SCADA control devices appropriate actions to take. This dependence upon

communications networks within SCADA systems introduces the system to the same vulnerabilities facing those communications networks through reliance upon GPS timing for accurate time/frequency measurements. If communications were lost stemming from a failure within GPS timing, then SCADA measurements and control actions would be lost. This in turn could potentially adversely impact the electricity subsector depending upon the current state of the power grid, and the duration of the outage. If the power grid were to experience a sudden change during this communication outage requiring immediate action be taken, if communication of this change were not available to control centers, then operators may not even know that prompt action is necessary. Even in the event that operators were able to recognize the problem, if these operators are not able to communicate with control devices, then negative consequences such as power outages or equipment damage may be unavoidable at that point.

3.5 Other 14 Sectors of Critical Infrastructure

While the other 14 sectors of CI are beyond the scope of this thesis, the potential for cascading effects throughout these sectors initiated by GPS failure is acknowledged. As electric power and communications serve as essential inputs to all of the other sectors, it follows that a failure in either sector initiated from a GPS timing failure would likely impact the other sectors adversely. In addition SCADA units have represented a significant dependence upon GPS timing through the communications networks supporting the transfer of their data. As SCADA systems in general govern CI systems of all forms, ranging from those in the electricity subsector, to water and wastewater management sector, transportation sector, agriculture sector, etc., the potential for cascading effects throughout the entire CI S-o-S is very real following a GPS timing attack.

4. Methodological Approach Outline

The methodology developed through this thesis research is based upon the centrality of state variables to understanding and subsequently modeling the behavior of complex systems of systems. While for some S-o-S, relationships amongst comprising systems may be described based upon simple input-out relationships, complex S-o-S are characterized by systems sharing at minimum one shared state variable, subsystem, or decision variable with other systems within the S-o-S. It is with this in mind that the interconnections amongst GPS timing, the electricity subsector, the communications, and SCADA/PMU systems are developed.

Upon gaining some insight to the nature of these interconnections amongst the systems forming this CI S-o-S, it is possible to identify the shared states between these systems which define the conglomeration as a complex S-o-S. Keeping in mind that models are designed to address specific questions, and should be as simple as possible and as complex as required; the modeling efforts in this model all address the question of, “what is the risk to the electricity subsector if something were to happen to GPS timing?” From this preliminary list of shared state variables amongst the component systems the list is pared down to the essential state variables which are shared across the S-o-S and can be linked to addressing the question at hand.

Once the essential shared states have been identified, and the interrelationships amongst components of the CI S-o-S are characterized, the research uses the previous findings to construct fault trees for analyzing the reliability of the electricity subsector within the context of failures originating from GPS timing discrepancies. The fault tree analysis furthers the understanding of technical and physical interconnections within the CI S-o-S, and gives insight into paths of failure from a GPS timing failure to an electricity subsector failure. It is important to note that the fault tree analysis performed here is not carried out for purposes of developing numerical reliabilities associated with the electricity

subsector, but rather to support and augment the understanding of the shared state variables, subsystems, and decision variables within the CI S-o-S.

Building upon the results from the fault tree analysis, event trees are next developed. The event trees add new depth to the overall modeling efforts by incorporating an aspect of timeframe within the analysis, due to their sequential nature. It is at the level of the event tree analysis where the shared decisions between the electricity subsector and communications sector are most readily recognized. Through following the paths of the event tree analysis, it is clear to see where decisions made by the communications sector impact the likelihood of failure within the electricity subsector following an error from GPS timing.

4.1 Modeling Interconnections and Interdependencies of CI S-o-S

In order to model the behavior of S-o-S it is imperative to understand how components forming the S-o-S interact with one another first. To model the interconnections and interdependencies amongst the systems of GPS timing, the electricity subsector, the communications sector, and SCADA/PMUs we build upon the technical basis and simple models developed for each system independently in Section 3 of this thesis. Starting with GPS timing comprised of signal source, signal, threat, and receiver; the receiver is a shared subsystem within PMUs as well as several of PSTN, internet, and wireless communications networks.

Thus GPS timing is connected to PMUs through the shared system of the GPS receiver, as well as to communications networks, similarly, through the same shared subsystem of GPS receiver. It is through this interconnection that threats impacting the signal entering the receiver in the GPS timing system can propagate effects into the communications sector or PMU systems. From the communications sector, we see that there are many interconnections shared with the electricity subsector. For instance, the electricity subsector plays a vital role in providing primary power for the vast majority of the nation's

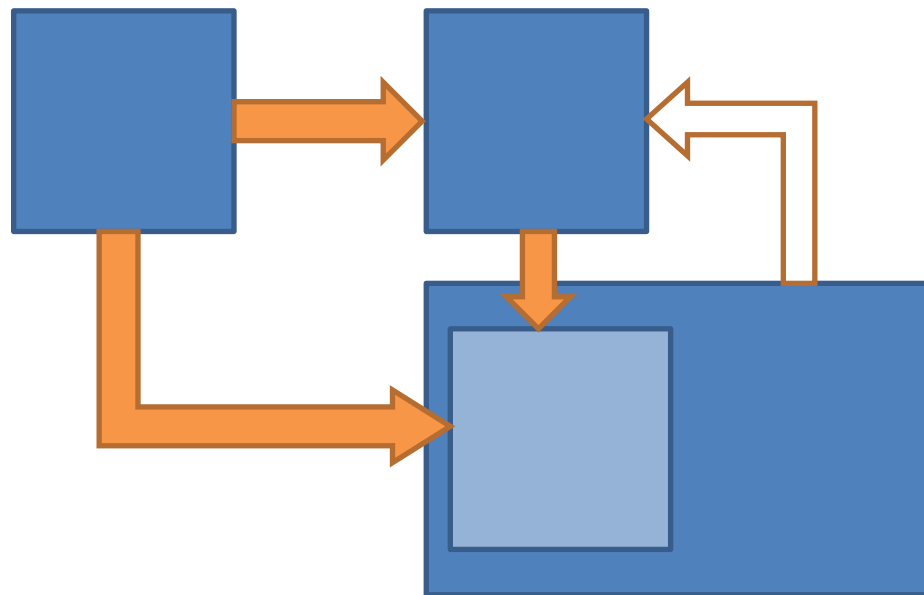
communications CI. The communications sector provides important communication services for the electricity subsector, ranging from cell phones and wireless data connections for technicians in the field, to voice connections for customers to call in outages. However, the communications sector infrastructure for which this research is focused upon is that in direct support of transmitting SCADA/PMU measurements, data, and controls.

As Smart Grid implementation increases in prevalence, it is expected based upon communications with electricity utility providers that the extent of this interconnection between communications CI and the electricity subsector will increase, and electric utilities will rely less upon private communications infrastructure, and more on communications carriers to provide their data networks. The role of communications CI networks in transmitting data for all types of SCADA systems across the nation is essential to providing basic functionality within many sectors whether it be for the energy sector, transportation water, water and wastewater management sector, etc. The subset of all SCADA devices that are for use within the electricity subsector is the focus of this research, and remain the focus of all modeling efforts presented in this thesis.

These SCADA devices measure and control the state of the electric power grid, and serve as a subsystem to the electricity subsector in that respect. Many forms of communications exist to serve data transmissions for SCADA systems such as privately owned microwave transmission networks, fiber optic networks such as SONET, and PSTN networks. Those networks that are owned and operated by communications CI carriers and rely upon GPS timing for synchronization remain the focus of this thesis, and have important implications on risks of power loss and blackout facing the electricity subsector through their shared decisions with communications CI carriers, which is developed in section 4.5.

PMUs share similar interdependencies and interconnections to both the electricity subsector and communications sector in future scenarios. At the current time, PMUs are used for monitoring the

state of the electric grid. In the future, Smart Grid initiatives plan to utilize PMUs to perform real-time autonomous/semi-automated control. It is under these future scenarios where PMUs and SCADA perform quite similar roles within the grid albeit with different sets of associated risks. PMUs have the added interconnection with GPS timing due to their reliance upon GPS timing to generate accurate timestamps for the measurement of synchrophasors within the grid. In order to focus upon addressing the risk of failure within the electricity subsector following a failure within GPS timing, the previous model for interconnections between GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems (see Figure 1) has been modified to the figure below.



(FIGURE 4.1-2) Interconnections and Interdependencies amongst GPS timing, electricity CI, communications CI, and SCADA/PMUs

In Figure 4.1-2, GPS timing has a one way relationship with communications CI as well as with PMUs (The text for PMUs is highlighted in orange to indicate that the direct dependency upon GPS timing within SCADA/PMUs corresponds with PMUs; SCADA in this model does not directly rely upon GPS timing for synchronization.) Due to the communications of interest within this thesis being solely

those networks used to provide support to SCADA/PMU systems, communications CI is shown to connect to electricity CI through serving as an input to SCADA/PMUs by providing the communications necessary for these systems to function within the electricity subsector. SCADA/PMUs are modeled as a subsystem of the electricity subsector to improve the understanding of SCADA/PMUs functionality in the context of this research. The final interconnection in this model is that of the electricity subsector back into the communications sector. This thesis research is aware of the reliance of communications CI upon the electric power provided by the electricity subsector, and the potential for cascading effects to propagate through this feedback loop following the event of a GPS timing attack, yet acknowledges that developing these events is beyond the scope of this research (The reason for the connection from electricity CI to communications CI being left white.)

4.2 Shared States, Subsystems, and Decisions

Interconnections and Interdependencies amongst systems can be attributed to the existence of shared: state variables, subsystems, or decision variables between said systems. To illustrate the synonymy of interconnections between systems and the existence of shared states we take a look at the state space representation of a simple example. Let there be two systems, system 1, \mathbf{S}_1 , and system 2, \mathbf{S}_2 . The essence of each of these systems can be completely captured through each system's two unique state variables $\mathbf{S}_1 = [x_1 \ x_2]^T$, $\mathbf{S}_2 = [x_3 \ x_4]^T$. The dynamical equation representing this simple system of systems is given as

$$\begin{bmatrix} \dot{\mathbf{S}}_1 \\ \dot{\mathbf{S}}_2 \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \end{bmatrix} \quad (4.1a)$$

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \quad (4.1b)$$

Here the matrix, \mathbf{A} , represents the relationships amongst the values of current states and their impact on the values of future states of each system. If the two systems were not interconnected and completely independent of one another, then this \mathbf{A} matrix would be decomposable into four quadrants (As depicted in equation 4.2a) with, \mathbf{A}_{11} , representing the upper left quadrant, and, \mathbf{A}_{22} , representing the lower right quadrant such that:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \left[\begin{array}{cc|cc} \mathbf{A}_{11} & \mathbf{A}_{12} & & \\ \mathbf{A}_{21} & \mathbf{A}_{22} & & \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \quad (4.2a)$$

$$\text{and } \begin{cases} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \mathbf{A}_{11} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \\ \begin{bmatrix} \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \mathbf{A}_{22} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} \end{cases} \quad (4.2b)$$

$$\Rightarrow \mathbf{A}_{12} = \mathbf{A}_{21} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (4.2c)$$

Intuitively, since there exists no interconnection between these two systems, it follows that the off diagonal matrices of \mathbf{A}_{12} and \mathbf{A}_{21} would necessarily have all entries equivalent to zero, as the current value of a state variable from system 1 would have no impact the future value for a state variable from system 2, otherwise an interconnection would necessarily exist, forming a contradiction. However, if there were no assumptions made upon the relationship between system 1 and system 2, and we were to consider a matrix, \mathbf{A}^* , of the following form:

$$\mathbf{A}^* = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \quad (4.3)$$

The decomposition of the dynamical equation in equation 4.2b no longer holds. Since, \mathbf{A}_{12}^* , is no longer comprised of all zero entries, there exists a relationship between the future value of the state

variable, x_1 , and the current value of state variable, x_3 . In order to represent all of the system dynamics impacting system 1 over time, the simplest form of said dynamical equation would be:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad (4.4)$$

Yet in this example, system 2 could still be represented by the second equation of equations 4.2b above. We say that the full behavior of system 1 cannot be described without taking into account the value of state variable, x_3 . Since the inclusion of the state variable, x_3 , is essential to describing the behavior of both system 1 and system 2, we say that x_3 is a shared state variable between system 1 and system 2. In this example of a S-o-S following the dynamical form of $\dot{\mathbf{S}} = \mathbf{A}^* \mathbf{S}$, the notion of interconnections between systems within the S-o-S is shown to be synonymous with the existence of shared states (This same argument would apply for the existence of shared subsystems between these systems).

For a S-o-S that is represented by the dynamical equation of form $\dot{\mathbf{S}} = \mathbf{A} \mathbf{S} + \mathbf{B} u(t)$, where, $u(t)$, represents the value associated with a decision to be made at a given time impacting the S-o-S, and, \mathbf{B} , represents the impact of said decision on the future values of each state variable, consider a S-o-S comprised of two systems each with two state variables, as before, $\mathbf{S}_1 = [x_1 \ x_2]^T$, $\mathbf{S}_2 = [x_3 \ x_4]^T$, in which there are no shared state variables:

$$\begin{bmatrix} \dot{\mathbf{S}}_1 \\ \dot{\mathbf{S}}_2 \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \end{bmatrix} + \mathbf{B} u(t) \quad (4.5a)$$

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \left[\begin{array}{cc|cc} \mathbf{A}_{11} & \mathbf{0} & & \\ \mathbf{0} & \mathbf{A}_{22} & & \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \mathbf{B} u(t) \quad (4.5b)$$

Despite there being no shared state variables amongst these two systems, there may still exist

interconnections between system 1 and system 2. Let $\mathbf{B} = [b_1 \ b_2 \ b_3 \ b_4]^T$, where b_1 , b_2 , b_3 , and b_4 represent the impact of current decision, $u(t)$, on the future value of the state variables, x_1 , x_2 , x_3 , and x_4 , respectively. If either both values of b_1 and b_2 , or both values of b_3 and b_4 are equivalent to zero, then system 1 and system 2 are independent of one another, and there exist no shared state variables, nor shared decisions between them. For example, if b_1 and b_2 were both equivalent to zero, then both systems could be represented by the use of two independent state space equations with no interconnections or interdependencies:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \left[\begin{array}{c|c} \mathbf{A}_{11} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{A}_{22} \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ b_3 \\ b_4 \end{bmatrix} u(t) \quad (4.6a)$$

$$\Rightarrow \begin{cases} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \mathbf{A}_{11} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ \begin{bmatrix} \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \mathbf{A}_{22} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} b_3 \\ b_4 \end{bmatrix} u(t) \end{cases} \quad (4.6b)$$

However, if at least one entry in the set of b_1 and b_2 , and the set of b_3 and b_4 contain a nonzero value, then the equations from 4.6b become:

$$\begin{cases} \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \mathbf{A}_{11} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} u(t) \\ \begin{bmatrix} \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \mathbf{A}_{22} \begin{bmatrix} x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} b_3 \\ b_4 \end{bmatrix} u(t) \end{cases} \quad (4.7)$$

System 1 and system 2 share no state variable interdependencies; however, the behavior of both systems in the future is dictated by the values corresponding to the shared decision, $u(t)$. System 1 and system 2 are interconnected through this shared decision, as decisions made to impact one of these two systems, necessarily impact the other system as well. It is based upon this synonymy of shared state variables, subsystems, and decisions with interconnected systems that the thesis seeks to uncover such

shared components amongst GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems to gain further insight into the dynamic behavior of this CI S-o-S.

4.2.a Identifying Essential States

From the previous section, the importance of the identification shared state variables to improving the understanding of interconnections amongst systems within S-o-S empowers the development of state space models of component systems to provide key insights to the behavior of S-o-S. When considering the systems of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems, it is imperative to pare down any list of state variables representing any of these systems into a list of essential state variables in order that any tractable form of analysis may be performed. Considering the system of GPS Timing for example; there is a state of physical location as a function defined as the ephemeris for each of 31 satellites in the Navstar GPS constellation. Keeping in mind once again that models are designed to address specific questions; and, should be as simple as possible, but as complex as required, this state associated with each of 31 satellites in the constellation is not essential to addressing the risk of failure within the electricity subsector resulting from a GPS timing attack. The additional insight that this additional information could bring to a model would be small compared to the impact of knowing the characteristics of a specific signal received by an affected GPS timing receiver, and would only contribute value within the most complex of models.

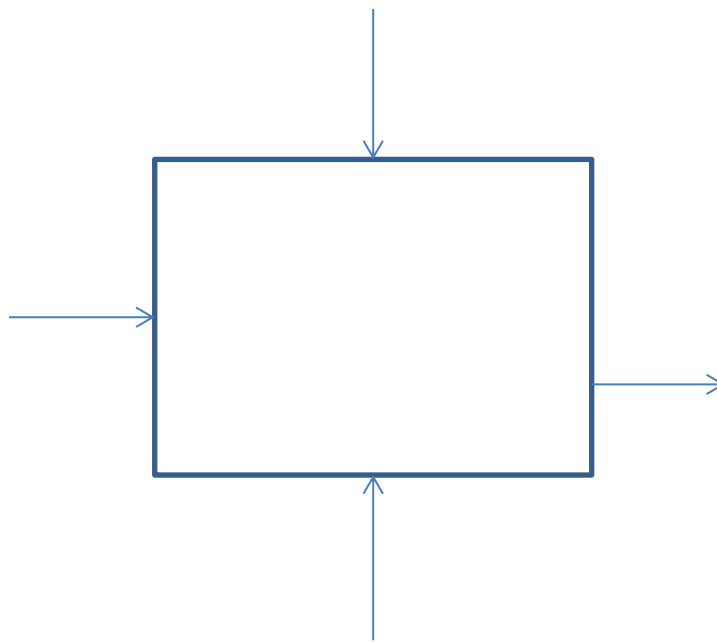
The discovery of state variables within a given system is not only important for characterizing interconnections and interdependencies amongst different systems, but also at the essence of describing the behavior of a system. State variables, combined with the impact of input variables, random variables, and decision variables correspond to generate the output of a given system. Furthermore, all decisions made regarding a system are made in order to change or maintain the state

of the system (Haimes, 2009). State variables serve as the most basic of building blocks on which models of systems can be built.

In considering the system of GPS timing, there are myriad state variables which impact the output of a GPS time-of-day/frequency measurement. The input to the GPS timing system is a GPS signal, generated from a combination of the constellation of 31 satellites in geocentric orbit combined with augmentations provided by both GBAS and SBAS. This signal can be characterized by the state variables of signal accuracy, signal availability, and signal integrity. It is important to note that the signal accuracy, availability and integrity states within the GPS timing model do not necessarily share the same values with the signal accuracy, availability and integrity states of the GPS signal serving as an input, as the state of the GPS timing state variables are also impacted by random and decision variables. While GPS signals boast high levels of accuracy, availability, and integrity across the United States when originating from the DoD owned and operated Navstar constellation, the characteristics of a signal used by a GPS timing receiver may not meet such standards. For instance, in the event of a signal jamming attack, while GPS signals may be available, the state of signal availability for the signal within the GPS timing model is unavailable for that particular receiver.

Random variables such as signal jamming or spoofing attacks, solar or other space weather events, atmospheric anomalies, etc., impact the signal accuracy, availability, and integrity of the actual signal received, which may or may not differ from the GPS signal sent. It is important to also note the distinction between accuracy and integrity under this same light. A lack of signal accuracy and a lack of signal integrity do not necessarily go hand in hand. Brief random events may impact genuine signals originating from GPS satellites. While the signal received may not be accurate, it is still a genuine signal and can be trusted to the extent that it is most likely correct, and while the corresponding time-of-day or frequency measurement should not be used, it is not necessary to check for a new signal to acquire,

deeming the genuine signal as not trustworthy. Additionally, an accurate signal does not necessarily equate to a signal with high integrity. Sophisticated spoofing attacks convince receivers to trust their signal bypassing checks for integrity that are based upon the accuracy of the incoming signal. These attacks gradually decrease the accuracy of the signal overtime much akin to the classic boiling frog example. Decisions impacting this signal at the level of the GPS Timing system have to do with corrections made to account for anomalies either predicted or documented impacting the interpretation of a GPS signal received, and may be sent through the signal from control stations on the ground.



(Figure 4.2-1) State Variable Model for GPS Timing System

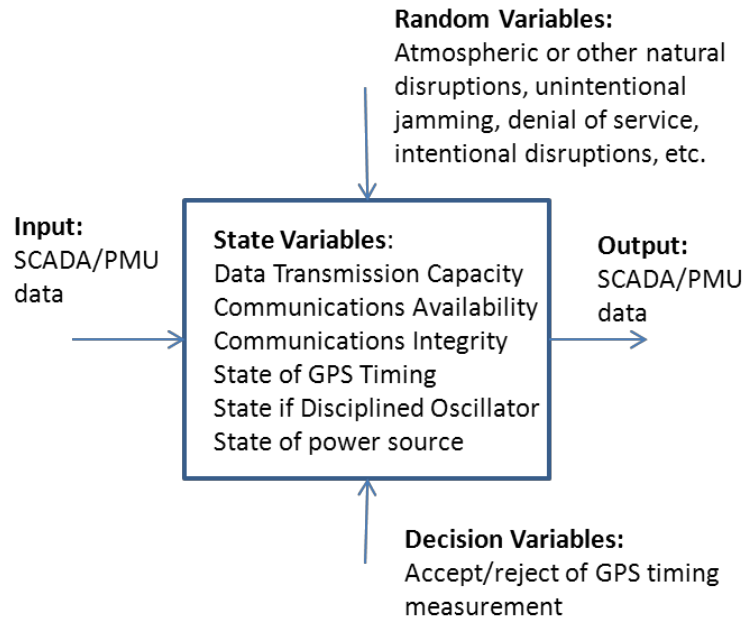
Taking a similar approach to the communications CI from Figure 4.1-2, the input and output of the communications sector are both SCADA/PMU data. This data transmitted across communications CI networks accounts for both measurements taken by SCADA or PMU devices as well as control actions issued from control centers to these devices. In either instance, there are essential state variables associated with the communications sector CI servicing the electricity subsector SCADA/PMU systems

which dictate the successful delivery of this information. Regardless of the specifications of the communications network serving these systems, there are essential states of: data transmission capacity, communications availability, and communications integrity. The first, data transmission capacity, is a major concern moving forward with Smart Grid initiatives. As the amount of data transmitted by PMUs greatly exceeds that of current SCADA systems, it is essential for communications networks to be able to keep up with this demand. If portions of a network were to become unavailable due to timing discrepancies initiated by a GPS timing attack, this change in the state of data transmission capacity could severely impact the data output from these communication networks. If measurement data was delayed in arriving at control centers, improper control actions might be implemented within the grid. If time sensitive control data were delayed in arriving to the proper systems, impacts such as blackouts might be realized more rapidly. The state variable of communications availability has two distinct states similar to the availability of GPS signals, either it is available, or it is not. The state of communications availability may be described by a likelihood that at any given time the communications network is available (as is also the most common case with GPS signals). Communications Integrity is a measure of the trustworthiness of communications at a given point in time. For the purposes of this research, accounting for the integrity associated with communications CI networks is beyond the scope of the thesis; however it is acknowledged that vulnerabilities related to this state within the communications of SCADA/PMU data represent a real and significant threat to the state of the electricity subsector.

In considering those portions of communications CI that exhibit vulnerabilities within the electricity subsector to GPS timing attacks, it is imperative to consider the state of GPS timing responsible for providing either accurate time-of-day or frequency measurements to those communications CI nodes supporting the electricity subsector. The state of GPS timing here is characterized by the same characteristics as that in the GPS timing model previously depicted (Figure 4.2-1). These three states

impact the disciplined oscillator subsystem within these communication nodes. As communication protocols dependent upon GPS timing use GPS to calibrate frequency for message encoding/decoding, the signal accuracy is imperative, as if it passes certain threshold values (i.e. timing error on the order of 125 μ s for SONET/internet/PSTN connections at 10 MHz nominal frequency) then frames may slip, and communications at this point are lost, as messages are not able to be deciphered on the receiving end. Signal availability impacts the GPS disciplined oscillator system in that if GPS timing is not available, the oscillator enters holdover mode. Depending upon the quality of oscillator, once the system enters holdover mode, the device may maintain frequency accuracy for as long as a few days for costly rubidium oscillators, to as little as a few hours for inexpensive quartz oscillators. Under certain risk management schemes, the signal integrity may also be used to determine whether the GPSDO should enter holdover mode. Acceptance/rejection of GPS timing measurements represents a critical decision impacting the successful transfer of SCADA/PMU data based upon limitations of the oscillator in holdover mode combined with the likelihood of a successful spoofing attack, an attack which is undetected and drives the disciplined oscillator past its threshold value for successful transmission.

The states depicted in Figure 4.2-2 are impacted by random occurrences both natural and intentional. Atmospheric or other natural disruptions related to weather can impact the success of SCADA/PMU data transmissions; as can unintentional jamming, which disables GPS updates within the GPSDO subsystems. Intentional attacks that go undetected can push disciplined oscillators past their acceptable thresholds and disable communications. Even attacks that are detected can wreak havoc upon communications depending on their duration. Detected GPS attacks are likely to disable disciplining algorithms leaving oscillators to be governed by their natural drift, if left without proper disciplining for long enough these oscillators may still drift past the range of tolerable frequency for communications to be maintained.



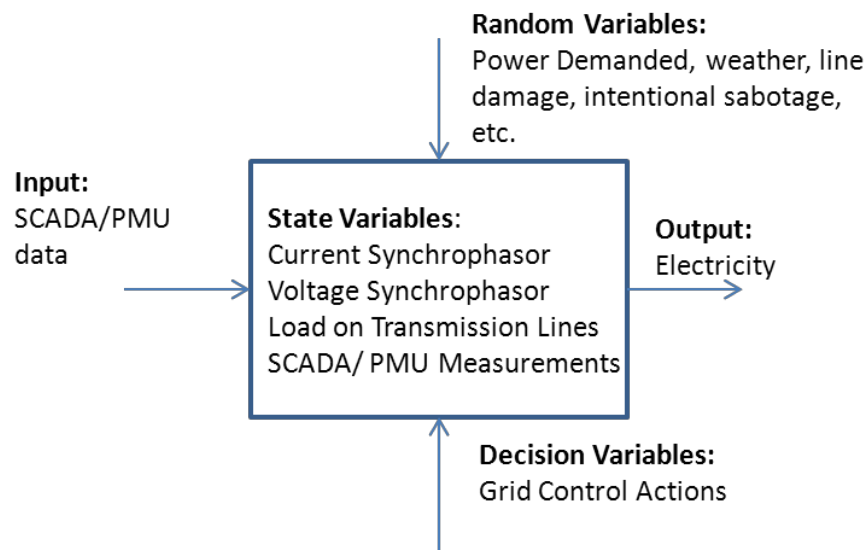
(Figure 4.2-2) State Variable Model for GPS Timing-Dependent Communications CI utilized by the Electricity Subsector

These SCADA/PMU data containing measurements and control actions serve as an input to the electricity subsector of CI. Based upon these measurements, grid control actions are issued. The successful transmission of electric power can be characterized by the states of the current synchrophasor, voltage synchrophasor, and corresponding measurements compared from node to contiguous node. If the current or voltage phase angle difference between two nodes exceeds a threshold of 10 degrees (Sheppard et al., 2012), then a failure to transmit power between any two given nodes is likely. The measurements of these synchrophasors play an important role in the decision for application of control. If these measurements are not accurate, improper control actions (whether implemented or failed to be implemented) can push the phase angle difference between two nodes past the acceptable range. The load on transmission lines also impacts the propensity for discrepancies in phase angle values to cause blackouts and is impacted significantly by random fluctuations in power

demand (however much of this random behavior is accounted for by significant forecasting efforts.)

The dependence upon communications CI within the electricity subsector is implicit within the state variable of SCADA/PMU Measurements, as well as the decision variable regarding grid control actions.

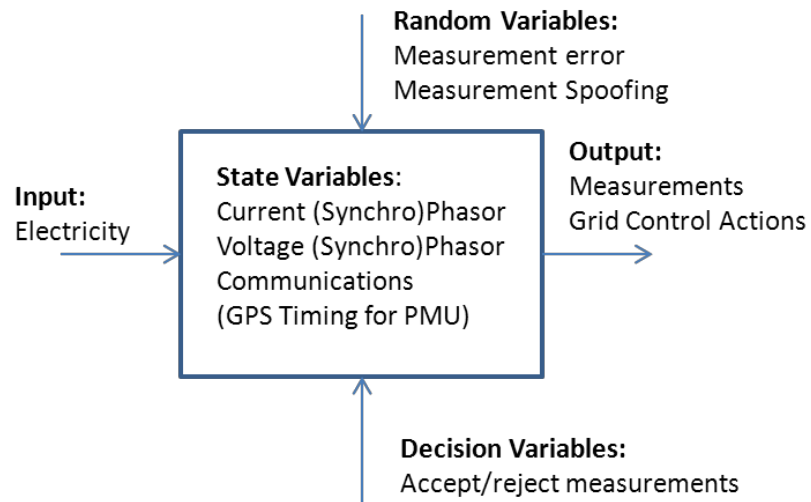
As communications networks serve as a fundamental component of transferring the data from SCADA/PMU systems within the electricity subsector.



(Figure 4.2-3) State Variable Model for the Electricity Subsector

The final state variable model is that of SCADA/PMU systems. These systems take electricity from a given node as an input, and return corresponding measurements along with grid control actions as outputs. The essential states for SCADA and PMU systems both are that of the current phasor (synchrophasor for PMU) and voltage phasor (synchrophasor for PMU) along with the state of communications at a given node. The state of the current and voltage phasors, combined with random measurement error, determine the values associated with the SCADA/PMU measurements. These measurements along with the state of communications are used to then determine grid control actions. In the event of communication failure, these actions may not be delivered to the proper control systems from control centers within the SCADA networks supporting the electricity subsector. PMUs also

depend upon GPS timing to develop these measurements. PMUs have been shown to be vulnerable to GPS spoofing, which can greatly degrade the accuracy and henceforth value of measurements obtained by spoofed PMUs (Sheppard et al., 2012).



(Figure 4.2-3) State Variable Model for SCADA/PMU Systems

4.2.b Shared State Variables

Based upon comparing the sets of essential state variables across each of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems, there exists shared state variables between systems for which interconnections were previously established.

The states of signal accuracy, signal availability, and signal integrity within GPS timing are shared with the communications sector as well as SCADA/PMU systems (depicted in green, see Figure 4.2-4). Data transmission capacity, communications availability, and communications integrity represent shared state variables between the communications sector and SCADA/PMU systems (shown in red). Current and voltage phasors are shared between the electricity subsector and SCADA systems, while their synchrophasors are shared states between the electricity subsector and PMUs (shown in blue). Lastly

load on power lines is a shared state variable between the electricity subsector and communications sector (depicted in gold).

GPS Timing	Communications CI	Electricity CI	SCADA/PMU
1. Signal Accuracy 2. Signal Availability 3. Signal Integrity	1. Data Transmission Capacity 2. Comm. Availability 3. Comm. Integrity 4. GPS Timing 5. State of power source	1. Current Synchrophasor 2. Voltage Synchrophasor 3. Load on Transmission Lines	1. Current Phasor 2. Voltage Phasor 3. State of Comm. PMU 1. Current Synchrophasor 2. Voltage Synchrophasor 3. State of Comm. 4. GPS Timing

(Figure 4.2-4) Compilation of Shared State Variables

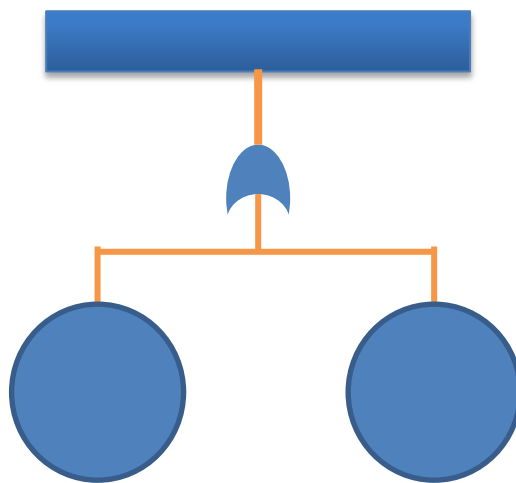
4.2.c Characterizing Interconnections through Shared States

In looking back to Figure 4.1-2, we see that the model shows interconnections between: GPS timing and communications CI, GPS timing and PMUs, communications CI and both SCADA/PMUs, communications CI and the electricity subsector, as well as with the electricity subsector with both SCADA/PMUs. Each of these interconnections can be characterized through shared state variables. The interconnection between GPS timing systems and the communications sector exists through signal accuracy, signal availability and signal integrity. These same three state variables characterize the connection flowing from GPS timing systems to PMUs. The connection from communications CI to SCADA/PMUs is characterized through the shared state variables of data transmission capacity, communications availability, and communications accuracy. Current and voltage phasor/synchrophasor

link the electricity subsector to SCADA/PMU systems. And the load on power lines connects the electricity subsector back in to the communications sector.

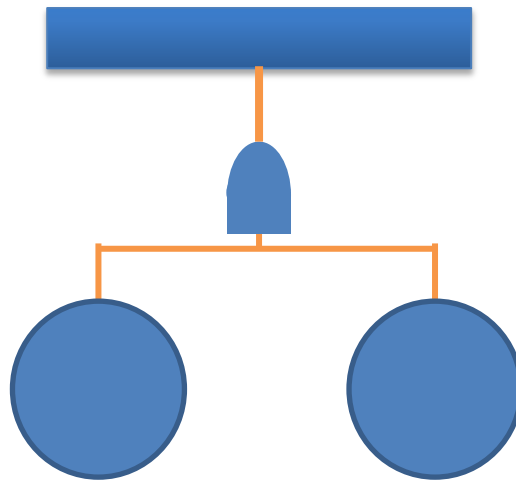
4.3 Fault Tree Analysis

Fault tree analysis represents a core tool used in reliability analysis. The likelihood of a total failure within a given system, or conversely the reliability of said system, is calculated from combining the reliabilities of components within the system based upon a hierarchical structure formed from a combination of series and parallel relationships. In fault tree analysis, systems are rewarded with greater reliabilities for incorporating redundancy within their structure through parallel relationships. If we consider two possible structures for a basic system formed from two components, A and B, where each component has a 50 percent chance to fail. In the first proposed structure, the two components are connected in series. This is equivalent saying that the system fails if component A or component B fails. This notion of an “or”-gate in fault tree analysis is depicted below:



(Figure 4.3-1) Fault Tree for structure one: series connection

In the second proposed structure, the two components are connected in parallel. This means that the system fails only if component A and component B both fail. Nodes that are connected in parallel are joined by an “and”-gate in fault tree analysis.



(Figure 4.3-2) Fault Tree for structure one: parallel connection

In order to compute the likelihood of total system failure within the first structure, the series connection, the likelihood of failure is equivalent to the compliment of the overall reliability of the system. Reliability for a series connection is equivalent to the product of component reliabilities (assuming independence of component failures). Thus for components A and B connected in series, the overall system reliability is equivalent to $0.5 \times 0.5 = 0.25$. Taking the compliment we find that the likelihood of total system failure following this series connection is 0.75. For the second example of a parallel connection, the likelihood of failure for the system is equivalent to the product of component failure likelihoods (once again, assuming independence of component failures). Since $0.5 \times 0.5 = 0.25$, the likelihood of total system failure for this second, parallel connection is 0.25, considerably less than that of the series connection. Despite both systems being formed from the same components, it is quite intuitive that the second system is more reliable because it only fails when both A and B fail, while the first system fails when either A or B fail.

The notion of minimal cut set in fault tree analysis is the equivalent of finding the path of least resistance to total system failure. As systems are only as strong as their weakest links, series dependencies upon components with low reliabilities weaken the overall reliability of the system. Introducing parallel connections amongst components incorporates redundancy within a system, and

improves overall reliability of system. Weaker components may be combined with stronger more reliable components to further improve reliability of a system through introducing diverse redundancy to said system.

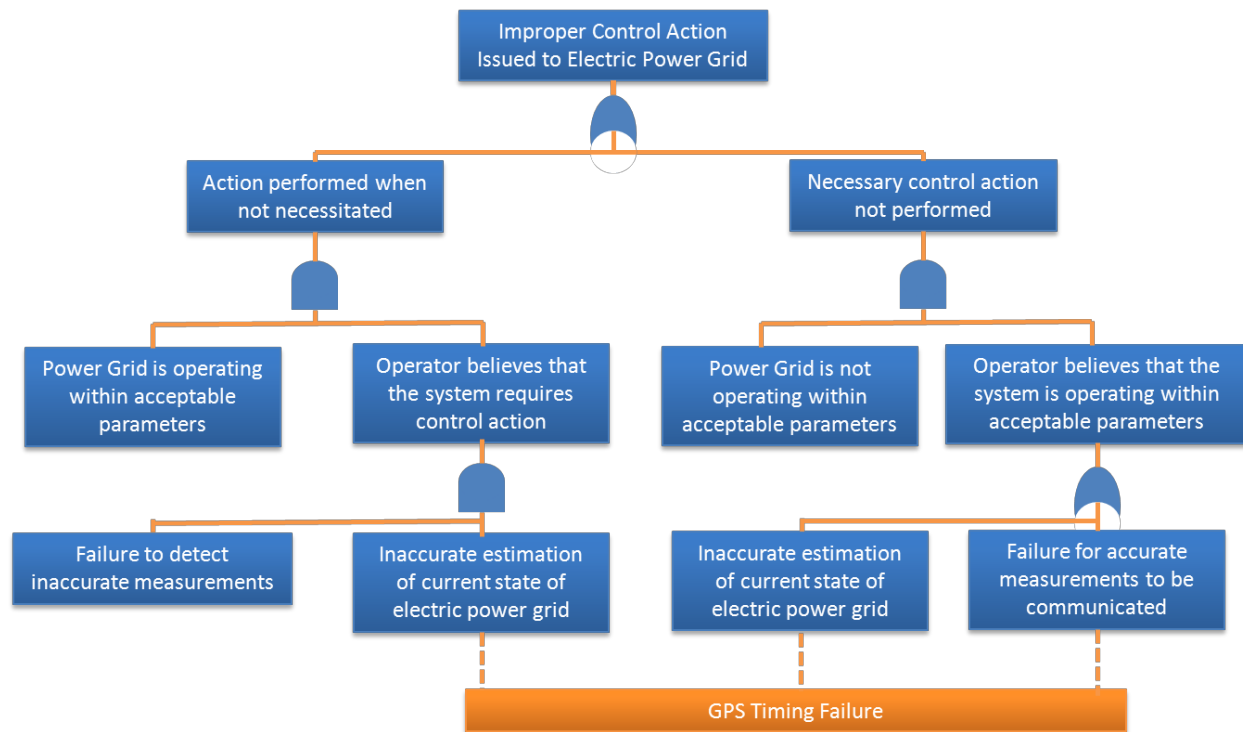
While fault tree analysis provides an elegant analytical methodology for calculating numerical reliabilities for systems, it also provides the opportunity to gain insight into weak links in complex systems. Through developing fault trees for complex system and identifying series connections with components throughout the system, component failures that triggers system failures can still be identified. Finding these weak links provide a starting point for prioritizing the implementation risk management strategies. When there are components whose failure cause a total system failure, these components must be addressed, and either improved or augmented through the introduction of redundancy.

4.3.a PMU Failure Fault Tree

When considering the structure of the CI S-o-S comprised of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems in the future scenario of Smart Grid PMU autonomous control, we find a representative fault tree for failure within the electricity sector in Figure 4.3-3.

Total failure is precipitated by some improper control action being issued to the electric power grid. This can occur either when an action is performed that was not necessary to be performed or, when a necessary control action was not performed. When an unnecessary control action is performed it occurs because the grid is operating within acceptable parameters yet the system controlling system believes that grid requires control to be implemented. This occurs in the event that an inaccurate estimation of the current state of the electric power grid has been made while simultaneously there is a failure to detect these inaccuracies. When considering the risk that GPS timing attacks pose to the

electricity subsector, it is important to realize that this inaccurate estimation can stem from GPS timing failures which introduce error to measurements taken from PMUs.



(Figure 4.3-3) Smart Grid Fault Tree

In the event that a necessary control action is not performed, the power grid must first be operating in a range that requires control to be implemented while the control system believes that the grid is operating in an acceptable range. This occurs either when there is error in the measurements, which could be the result of GPS timing failure or the state of the grid is properly measured yet the communication of this information fails to be received by the control system, once again, a potential GPS timing failure may be to blame. Through tracing back up the tree in Figure 4.3-3, we see a clear path to electricity subsector failure depicted initiated from failure in GPS timing systems.

4.4 Event Tree Analysis

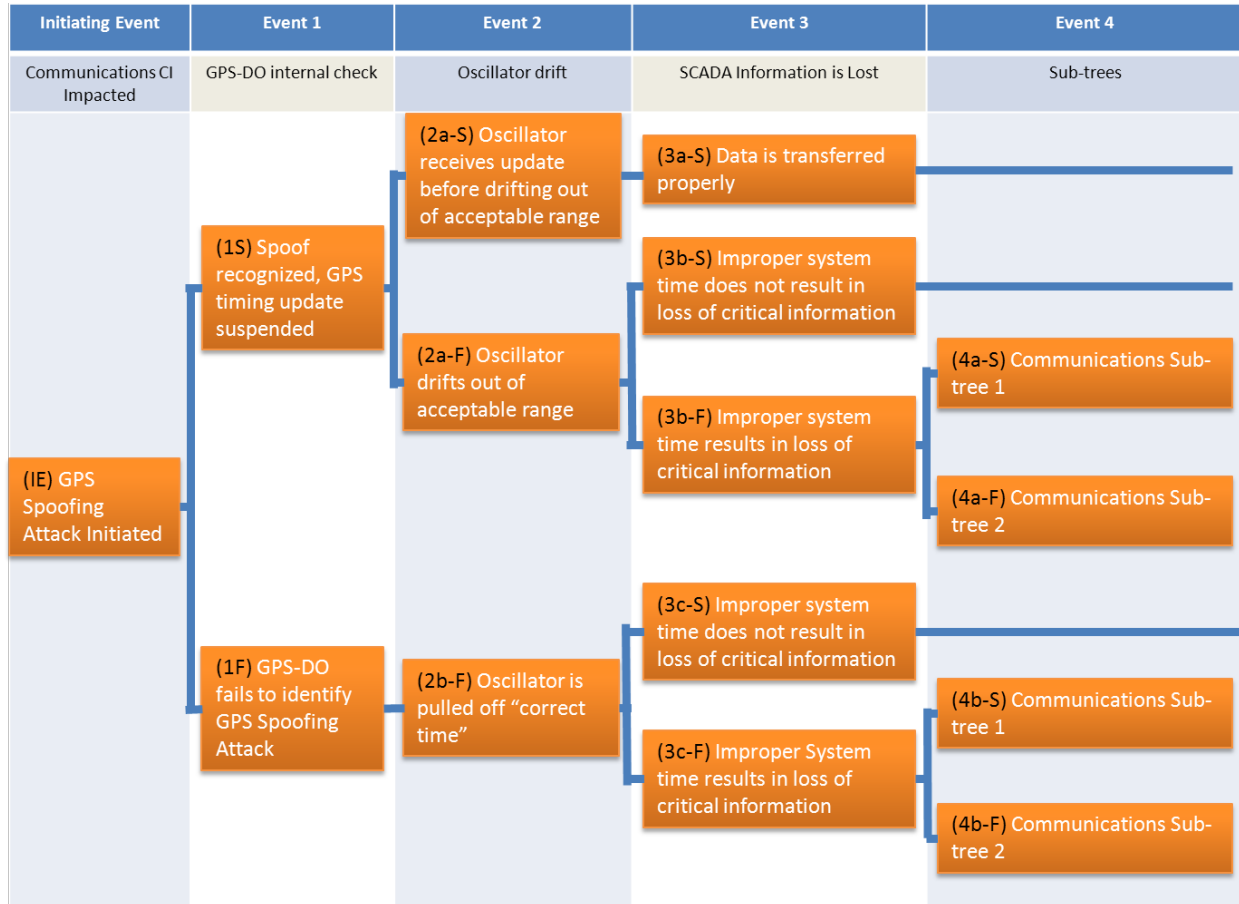
While the fault tree analysis in the previous section exhibits paths to electricity subsector failure initiated from failures within GPS timing systems, the structure of the fault tree does account for the timeframe associated with these failures. Event Tree Analysis may be used to augment these findings, and lend a notion of timeframe of events in the path to total system failure. Event Tree Analysis follows a chronological event from an initiating event, through successes and failures at different stages of time to all possible outcomes. Through a combination of the law of total probability in that the sum of the likelihood of success and failure is one, and the assumption of the independence of the likelihood of failure at any given stage, event tree analysis provides an analytical framework for determining the respective likelihood of all possible outcomes.

4.4.a Communications Failure Event Tree

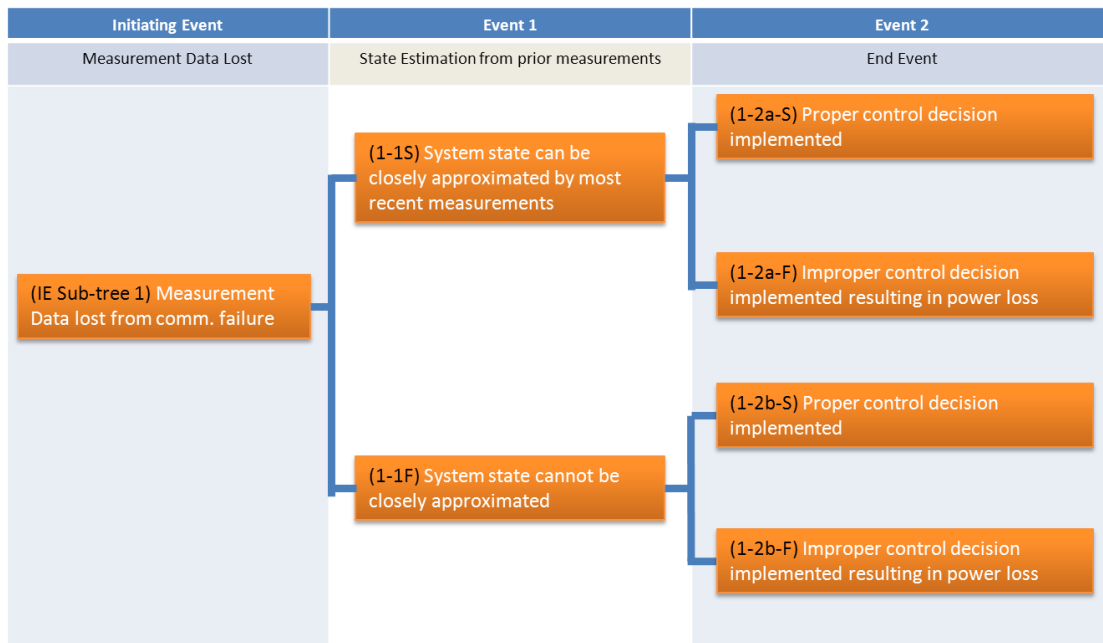
When considering the impact of GPS spoofing attacks versus communications CI dependent upon GPS timing for providing accurate frequency calibration we find an event tree characterized in Figures 4.3-4 through 4.3-6.

In this example, communications CI is first impacted from the initiation of a GPS spoofing attack. (Successes within the system are attributed to outcomes with positive effect on the system and denoted by “S’s”, while failures are linked to outcomes with negative effects, denoted by “F’s” in the above figures.) The first event following this initiating event is that of the corresponding GPS-DO internal check, which is considered a success if the spoof is recognized, and the GPS timing update is suspended, sending the oscillator into holdover mode. This GPS-DO internal check is a failure if the GPS-DO fails to identify that it has been spoofed. Following a success in event one, the second event is that of oscillator drift, if the oscillator maintains a frequency within the acceptable range to allow communications of SCADA/PMU data to be transmitted, then event two is a success. However if the oscillator drifts out of

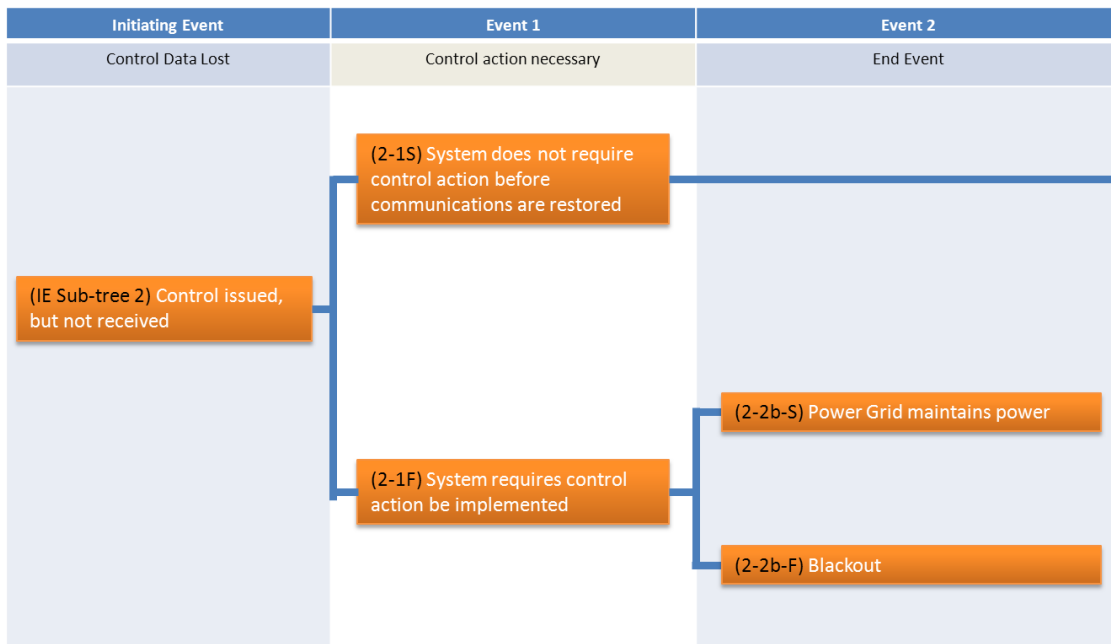
the acceptable frequency range, then a failure has occurred. Following a failure in event two, then the oscillator is pulled away from the acceptable range necessitating a failure be attributed in event two with absolute probability 1.



(Figure 4.3-4) GPS Spoofing Attack vs. Communications CI Event Tree



(Figure 4.3-5) GPS Spoofing Attack vs. Communications CI Sub-tree 1



(Figure 4.3-6) GPS Spoofing Attack vs. Communications CI Sub-tree 2

The third event is the determination of whether SCADA information has been lost. Successes in events one and two indicate that this data is transferred properly, and there exists a success in event three. If the oscillator has drifted from the acceptable range, then either the improper system time/frequency measurement does not result in a loss of critical information, which would represent a success, or this discrepancy does result in the loss of critical information, a failure. If critical information is not lost during the third event following the initiation of the attack, then the system continues business as usual, and the negative effects of the GPS spoofing attack are not realized by the electricity subsector, however, if critical information is lost, it could result in one of two outcomes either SCADA measurement information or control data has been lost (Note: that in reality there is a likelihood if one of these two data forms have been lost then both may have been lost)

When measurement data has been lost we continue to sub-tree one in Figure 3.4-5. The first event following the loss of this measurement data is the state estimation from previous measurements. If the state of the system can be closely approximated by recent measurements, then there is a success at this stage. However if the state of the grid cannot be closely approximated, a failure has occurred. In either event it remains to be seen if proper control will be implemented based upon the most recent estimation for the state of grid. It follows that if the approximation was close, then the likelihood of implementing appropriate control is higher than if the approximation was not close.

If control data has been lost, we then consider sub-tree two in Figure 4.3-6. When control data is lost, either the system does not require some control be implemented before communications are restored, a success, or the system requires some control action be implemented, a failure. Following a success at this previous stage, the end outcome is a success. However following a failure, the power grid may successfully maintain power, or fail, resulting in power loss/blackouts. The likelihood of failure

in this last stage is a result of the severity of the change within the state of the power grid over the time for which communications have been lost.

Many factors contribute to the likelihoods associated with the success or failure of each event within the tree. Of particular interest to DHS should be those factors directly stemming from the existence of shared decisions between the electricity subsector and the communications sector of CI. These shared decisions are further developed in the section 4.5 of the thesis.

4.5 Shared Decisions Revisited

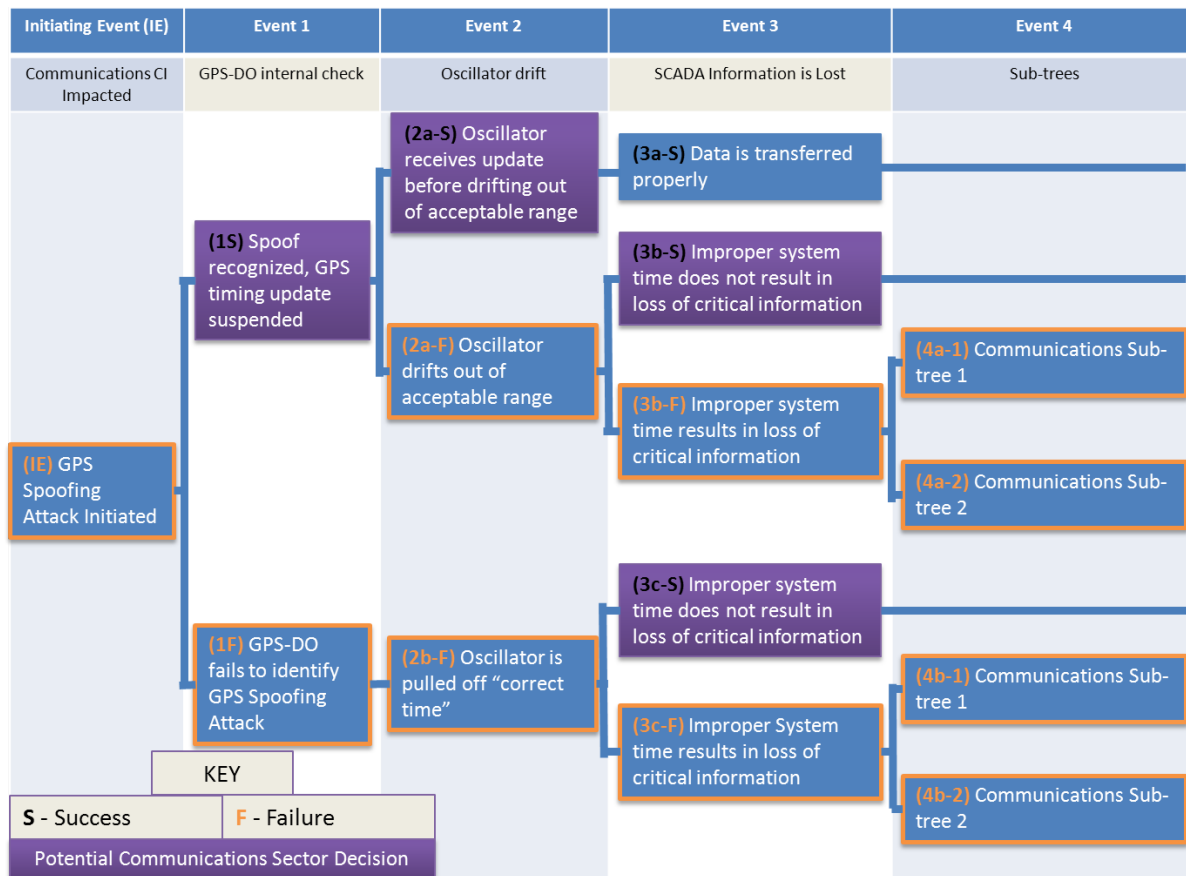
Shared decisions represent a subset of critical interconnections between systems within a S-o-S. The importance of identifying shared decisions is intensified when the parties responsible for each respective system involved in the shared decision are not the same. Issues arise when multiple parties are responsible for making a given decision, and win-win outcomes, where all parties involved are satisfied by the final decision is highly sought after. The matter is further complicated when a decision is shared through the implications, yet one party is making the decision for both. It is important that the party responsible for making said decision considers the impact of their choice not only on their own system, but also on the other systems for which the decision is shared.

The communications sector and electricity subsector have a history of not taking the previously stated perspective into account. When the communications sector removed copper telephone wires to meet the demands of the financial sector for fiber optic networks, the communications sector failed to account for the impact to the electricity subsector. Following 9/11, two substations were destroyed in lower Manhattan, and the electricity subsector was not able to bring a new substation online using their conventional method requiring the removed copper wires. As the implementation of Smart Grid technologies becomes a reality, and the electricity subsector looks to the communications sector to provide more of its communication networks it is essential that the communications sector take into

account the risks facing the electricity subsector stemming from decisions the communications sector makes.

Returning to the event tree in Figure 4.3-4, we highlight events with corresponding likelihoods that are directly impacted from decisions shared between the communications sector and the electricity subsector (see Figure 4.5). We see that the likelihood of a spoof being recognized by a GPS-DO internal check is directly impacted by communications sector decisions. Shared decisions in this context may be somewhat of a misnomer as the decision-making may not be a shared responsibility; however, the impact of the decision is most definitely shared. Considerations upon whether the communications CI has the ability to identify a spoofing attack, and how reliable is the system at identifying which type of attacks, both play part into determining the likelihood of success in this scenario.

In the second event following the initiating event of a GPS spoofing attack, the likelihood that an oscillator receives a timing update before drifting out an acceptable range is determined in part by decisions made by the communications sector. The decision on what type of oscillator is used in these systems, whether it is quartz or rubidium, etc. directly affects this probability. Also, if there is some backup system to update the clock in the event of a GPS failure, the likelihood of success at this juncture could approach unity. When considering the likelihood that improper system time/frequency does not result in the loss of critical information, the overall architecture of the communications network must be taken into account. What forms of diverse redundancy are there? Are there backup networks running in parallel? These are all decisions made by the communications sector that have direct impact upon the electricity subsector.



(Figure 4.5) Shared Decisions between Electricity and Communications CI

Due to the reliance of the electricity subsector upon the communications sector for a portion of their communications networks, the communications sector is able to determine to a certain extent what is an “acceptable” level of risk for the electricity subsector. It is imperative that the communications augment their understanding of the third question of risk management, “what are the impacts of current decisions on future options?” to include the perspective of, “what are the impacts of *our* decisions on *their* future options?” When accounting for essentiality of the provision of electric power to the nation, it is critical that the communications sector account for this perspective.

4.6 Risk Filtering, Ranking, and Management

Risk filtering, ranking, and management, represents a multistage systematic framework for prioritizing risk management options associated with scenarios regarding large-scale systems (Haimes et al., 2002). Typically the process is comprised of eight stages. This research applies the findings from RFRM to form a modified risk filtering method for scenarios in which the likelihoods of occurrence are not well defined or unknown. In this modified RFRM approach, the first two stages are the same as those of the original RFRM: (1) Identification of risk scenarios, (2) Scenario filtering based on scope, temporal domain and level of decision making. The implications of the shared decisions between communications CI and the electricity subsector represent the subset of events for which the filtering has selected. Referring to Figure 4.5, events for which a shared decision between the communications sector and electricity subsector have a shared decision in which the choice made impacts the probability of success are found at: (1S) Spoof recognized, GPS timing update suspended, (2a-S) Oscillator receives update before drifting out of acceptable range, and (3b-S) Improper system time does not result in loss of critical information.

In order to gain insight into the risks associated with specific scenarios for each of these shared decisions, we use the fourth phase of RFRM: multi-criteria filtering (The research has skipped over phase III, bi-criteria filtering, due to the likelihood of negative consequences being unknown for these events.) For the multi-criteria filtering, eight characteristics are used to help understand the severity of the risks faced in a given scenario: (1) un-detectability; (2) uncontrollability; (3) multiple paths to failure; (4) irreversibility; (5) duration of effects; (6) cascading effects; (7) required attack sophistication; and (8) design immaturity. Each scenario is given an associated qualitative risk severity rating of low, medium, or high. (Explanations of the characteristics used within the modified RFRM analysis along with the implications of their ratings can be found in Appendix A)

In the first event following the initiation of a GPS spoofing attack against the GPS receiver associated with a given node within the communications sector, there exist three main scenarios of interest regarding the likelihood of detection of the attack: (1) the GPSDO system does not have an internal detection mechanism; (2) the GPSDO system has spoofing detection based upon absolute signal power monitoring; and (3) the GPSDO system has detection based upon relative timing difference. Of these three main scenarios, scenarios (1) and (2) have further sub-scenarios: (2 a) the spoofing attack falls outside of the range of acceptable signal power; (2 b) the spoofing attacks falls within the range of acceptable signal power; (3 a) the spoofing attack changes the reference timing at a rate fast enough to trigger an alarm; and (3 b) the spoofing attack changes the reference timing at a rate slow enough to bypass the alarm. Applying the multi-criteria evaluation across scenarios (1), (2 a), (2 b), (3 a), and (3 b) could represent in a risk profile facing the electricity subsector similar to that found in Figure 4.6-1.

Criterion	Scenario 1	Scenario 2 a	Scenario 2 b	Scenario 3 a	Scenario 3 b
<i>Un-detectability</i>	High	Low	High	Low	High
<i>Uncontrollability</i>	High	Low	Medium	Low	Medium
<i>Multiple paths to failure</i>	High	Low	Medium	Low	Medium
<i>Irreversibility</i>	Medium	Medium	Medium	Medium	Medium
<i>Duration of Effects</i>	High	Low	High	Low	High
<i>Cascading Effects</i>	High	High	High	High	High
<i>Required Attack sophistication</i>	High (Low sophistication)	Low (High sophistication)	Medium	Low	Medium
<i>Design Immaturity</i>	High	Low	Medium	Low	Medium

(Figure 4.6-1) Multi-Criteria Evaluation of GPSDO Internal Check Scenarios

From the perspective of communications CI carriers, the decision of spoofing detection measure can help to dictate which of the three scenario categories that are observed in the event of any attack.

Regardless of the specifications of the spoofing attack initiated, there is high risk across all categories (irreversibility is at medium due to the ability for systems to recover to previous levels by disabling GPS timing updates), indicating that this first scenario should be avoided at all costs. Scenarios (2 a) and (3 a) as well as scenarios (2 b) and (3 b) have similar rankings under these eight characteristics. Depending on the relative likelihoods between an attack being able to bypass the spoofing detection measures identified by scenarios (2) and (3), communications carriers should opt to utilize the spoofing detection measure which is less likely to be circumvented.

The second shared decision discovered in the event tree analysis, regarding the likelihood of an oscillator drifting past an acceptable frequency range is analyzed under the following scenarios: (1) the system has a backup reference time to GPS, and (2) the system does not have a backup reference time. The second scenario comes with three sub-scenarios: (2 a) the attack lasts for less than one hour, (2 b) the attack lasts for between one and eight hours, and (2 c) the attack lasts for greater than eight hours. Once multi-criteria evaluation is applied to these four scenarios, a representative risk profile for the electricity subsector may look as follows in Figure 4.6-2.

While the decision facing communications of whether or not to employ a backup reference timing system to GPS at a given node faces risks lower in severity independent of the attack duration, the relative decrease in overall risk depends upon which of the likelihood of entering each of the three sub-scenarios associated with not having a backup timing reference. While the majority of associated severities increase as the duration of the attack increases, the risk of an attack being un-detectable decreases as the attack duration increases. An attack that lasts longer has a greater likelihood of being detected, due to the fact that lasting longer gives more opportunities for the attack to be detected. Depending upon the how long the communications sector thinks that an attack will need to last in order to cause an oscillator to drift, coupled with the likelihood of detection in the first event of the event tree

in Figure 4-5, communications carriers should choose to either implement a backup reference or not based on the implied expected impact resulting from their decision in event one along with these likelihoods.

Criterion	Scenario 1	Scenario 2 a	Scenario 2 b	Scenario 2 c
<i>Un-detectability</i>	Low	High	Medium	Low
<i>Uncontrollability</i>	Not Applicable	Not Applicable	Not Applicable	Not Applicable
<i>Multiple paths to failure</i>	Low	Medium	Medium	Medium
<i>Irreversibility</i>	Low	Low	Medium	High
<i>Duration of Effects</i>	Low	Low	Medium	High
<i>Cascading Effects</i>	Low	Medium	Medium	High
<i>Required Attack sophistication</i>	Low (High Sophistication)	Medium	Medium	Low (High Sophistication)
<i>Design Immaturity</i>	Low	Medium	Medium	Medium

(Figure 4.6-1) Multi-Criteria Evaluation of Oscillator Drift Scenarios

For the last shared decision identified within the event tree analysis of section 4.5, once prior failure have led to the event of SCADA information being lost or not there are two possible scenarios that stem from communications sector decisions that can impact this likelihood: (1) A backup communications network has been implemented to serve the SCADA devices which have lost primary communications functionality; and (2) no back communications network is in place. Once the event tree has entered into this stage, the risk profile faced by the electricity subsector under each of these scenarios could look like that of Figure 4.6-3.

Criterion	Scenario 1	Scenario 2
<i>Un-detectability</i>	Low	Medium
<i>Uncontrollability</i>	Low	High
<i>Multiple paths to failure</i>	Low	Medium
<i>Irreversibility</i>	Low	High
<i>Duration of Effects</i>	Low	Unknown
<i>Cascading Effects</i>	Low	High
<i>Required Attack sophistication</i>	Low (High Sophistication)	Medium
<i>Design Immaturity</i>	Low	Medium

(Figure 4.6-3) Multi-Criteria Evaluation for Primary Communications Outage Scenarios

While the severity of consequences facing the electricity subsector dictates far better conditions in the event of a backup communication system being in place, the decision to implement such a network must be made taking into account many additional considerations. One of such considerations is that of the likelihood associated with a GPS attack initiated event reaching this stage of the event tree. Given the results of the previous two decisions, if it is likely that a GPS spoofing attack could reach this stage where oscillators have been pulled away from their nominal values by an unacceptable amount, then the choice of implementing a backup communications network may be deemed necessary, regardless of the cost. However, if it is deemed to be unlikely for an attack to reach this stage in the event tree, then the immense cost associated with implementing this risk management strategy may be deemed excessive, and unnecessary.

In terms of relative cost, these three shared decisions are ordered in the same fashion as their chronological occurrence. The first decision regarding the level of detection associated with GPSDO is on the order of hundreds of dollars. The second decision regarding backup timing systems and choice of

internal oscillator could be as high as hundreds of thousands of dollars for atomic clock reference systems, to as low as tens of thousands for rubidium replacements for quartz oscillators. The third decision is most costly, with implementation of GPS-timing independent backup communications networks costing potentially millions of dollars. By looking at the structure of the event tree in Figure 4.5, we see that increasing the likelihood of success in the first event of the GPSDO internal check by implementing some form of spoofing detection can greatly decrease the likelihood of ever needing a backup communications network, by basically eliminating the bottom half of the tree. This second group of decisions regarding backup timing references and choices of GPSDO materials can all but eliminate the need for backup communications networks, if holdover capabilities of these systems without GPS timing were sufficient to maintain frequency for the duration of all but the most unlikely of attacks. This means that the risk management options facing communications carriers are actionable, in that the most effective measures to preventing failures in the electricity subsector stemming from GPS timing attacks; also happen to be among the least expensive of options.

5. Discrete Event Simulation Model and Results

Merging all of the previous modeling efforts into a representative example that can be modified to fit different specific architectures for GPS timing systems, electricity CI systems, communications CI systems, and SCADA/PMU systems the research has developed the basic structure for an adaptable discrete event simulation model to serve as a potential application of the findings within this research. While numerical determinations of likelihoods associated with events and consequences have not been included in previous sections, the goal of this simulation is to gain some insight into the “relative likelihoods” associated with negative consequences following a GPS timing attack. These likelihoods of negative consequences vary greatly depending on the architectural topologies of all interconnected networks, as well as based upon the specific components within each implementation. It is because of this fact that discrete event simulation is used to create a representative model, due to the ability to

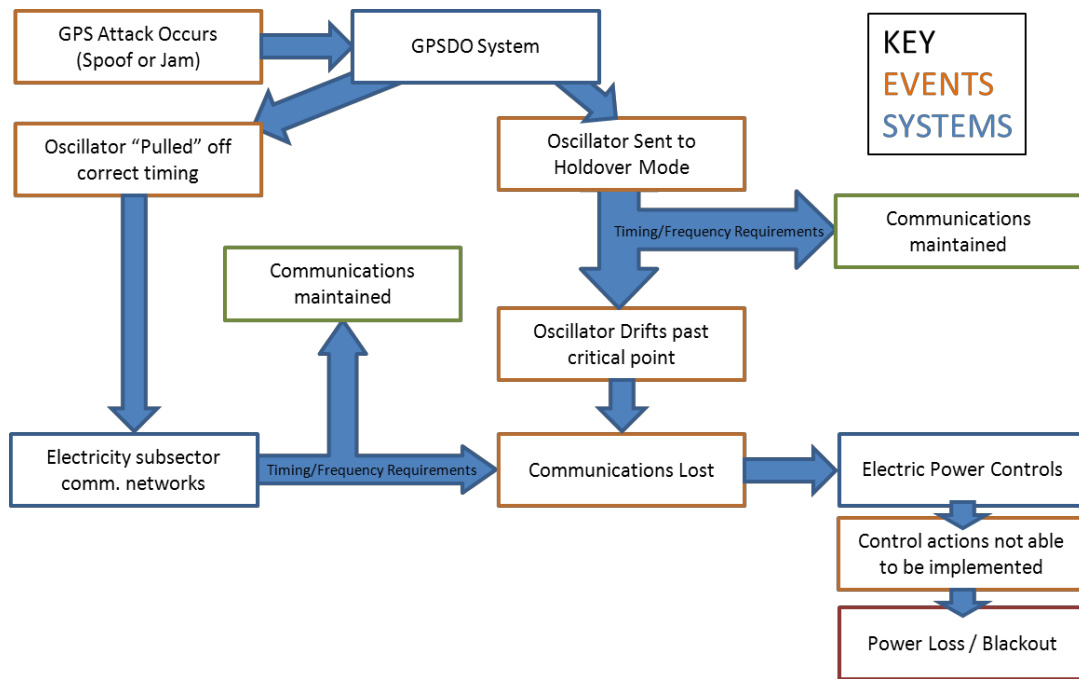
construct an adaptable, modular model, which can be applied to a variety of system configurations (The model is performed within the student version of Arena environment).

5.1 Discrete Event Simulation Model Outline

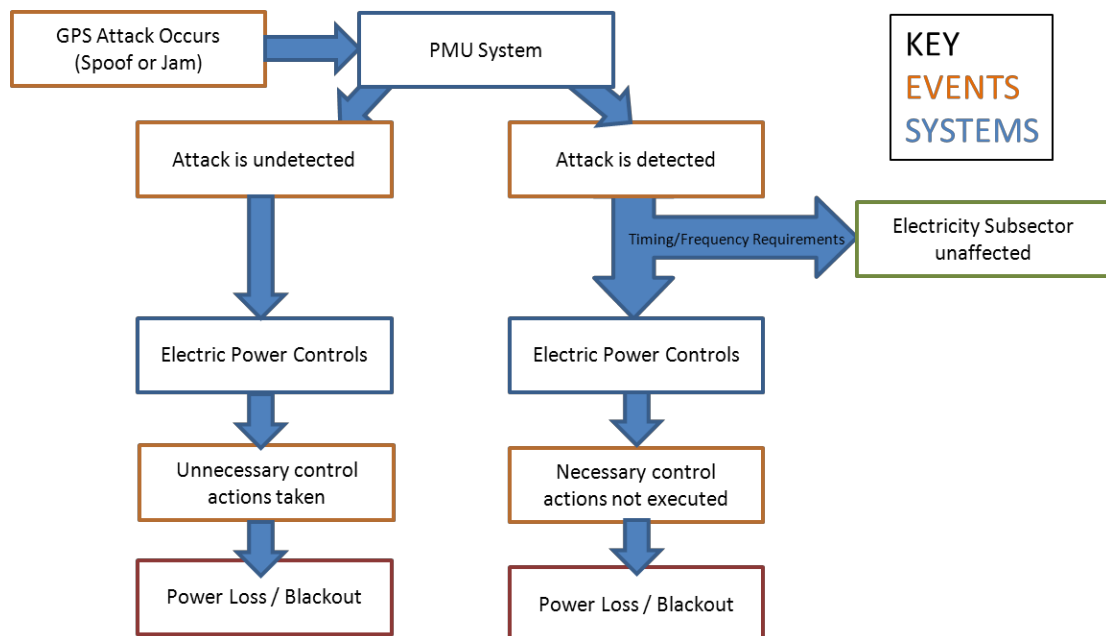
The basic outline for the discrete simulation can be seen in Figures 5.1-1 and 5.1-2. In Figure 5.1-1, the event of A GPS Spoofing attack occurs impacting a node within the communications sector, utilized by the electricity utility. This event impacts the GPSDO system. If the system does not detect the attack, then the oscillator can be “pulled” off the correct timing. This impacts the communications utilized by the electricity subsector; and depending on the timing/frequency requirements of the network, coupled with the duration and intensity of the attack, communications can either be lost or remain intact. If the attack is detected by the GPSDO internal check, then the oscillator is sent to holdover mode. Once in holdover mode, the oscillator is no longer steered by GPS, and left to drift according to the natural bias of the oscillator. Once again, whether or not communications are maintained, depends upon the duration of the attack, combined with the timing/frequency requirements of the communications networks along with the quality of the oscillator when left undisciplined. Once communications have been lost, the electricity subsector is no longer able to issue controls to that particular node until communications are restored. If the phase angle difference between two nodes connected nodes within the electric power grid, then power is lost across the lines connecting those two nodes.

Figure 5.1-2 depicts the event of a GPS Spoofing attack versus a PMU system. In this case, the attack is either detected or undetected at the level of the PMU System. An undetected attack will result influence the electric power control systems, and if left to run its course, cause a failure within the electricity subsector. A detected attack has a chance of not affecting the electricity subsector, depending upon the duration of the attack, along with the timing/frequency standards of the PMU

system itself. If the PMU System is left without GPS timing for too long however, necessary control actions may not be implemented, and the resulting effect could be a blackout.



(Figure 5.1-1) Discrete Event Simulation GPS Attack versus Communications Outline

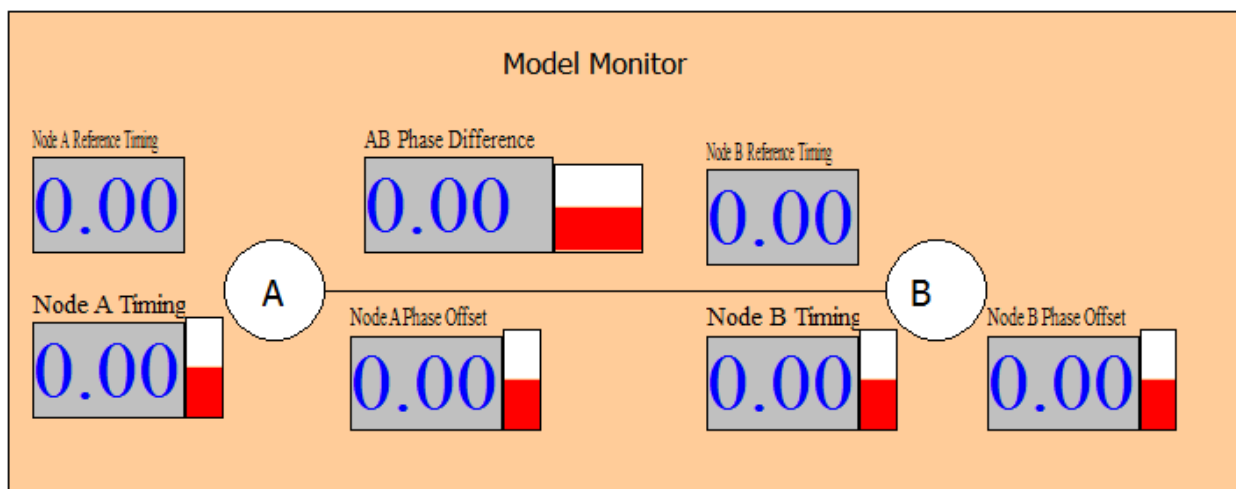


(Figure 5.1-2) Discrete Event Simulation GPS Attack versus Communications Outline

Combining these two models together forms a model outlining the possible paths to failure within the electricity subsector stemming from GPS timing attacks.

5.2 Discrete Event Simulation Model Implementation

The model outlined above is implemented within the Arena environment for a simple two node network to demonstrate the possibility of monitoring the interconnections of the S-o-S comprised of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems in a Smart Grid configuration through simulation. This model can be adapted to simulate networks of more than two nodes, with varying structures and requirements due to the modularity of components within the model (Due to limitations within the student version of arena license, a more complex network could not be demonstrated at the current time). The numerical values and distributions selected for the implementation of this simulation have been selected in an effort to remain consistent with the values found in open literature; however, these values are used purely for demonstrating the possibilities for modeling this S-o-S through simulation. Figure 5.2-1 depicts the monitoring screen allowing the progress of the simulation to be viewed during the execution.



(Figure 5.2-1) Simulation Monitoring Window

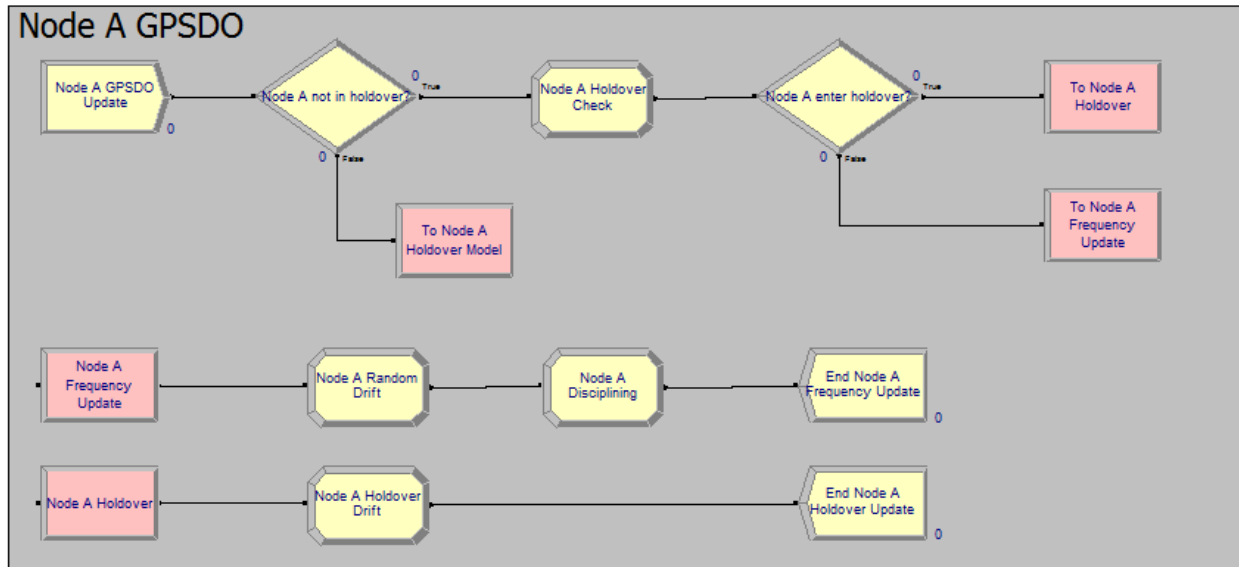
In this simulation monitoring window, the two nodes are depicted along with information about the current state of essential states within the system. The module tracking, “AB Phase Difference,”

displays the phase angle difference between nodes A and B. The simulation runs until such time that the phase angle difference between the two nodes exceeds 10 degrees. For both nodes, the reference time, "Node A/B Reference Timing," represents the time offset from UTC of the reference signal in microseconds. In the event of a spoofing attack, the reference timing moves from zero to the value specified in the attack characteristics. "Node A/B Timing" represents the time offset from UTC of the GPSDO associated with the communications system at that given node, once again in microseconds. Lastly, "Node A/B Phase Offset" represents the offset in degrees from a predetermined angle that serves as the reference for the entire power grid.

Each of the systems identified within the discrete event simulation model outline have their own sub-model within the simulation model. These sub-models are additionally created for both nodes A and B, so that they may be assigned different values, representing differing physical configurations; the simulations run for the purposes of demonstration however have the exact same configurations for nodes A and B. The GPSDO sub-model is shown in Figure 5.2-2. In this sub-model, the simulation is updated once every second. An entity is spawned, which first checks to see if the system is in holdover mode. If the GPSDO is not currently in holdover mode, it checks to see if it should enter holdover mode. This decision is made by comparing the difference between the system time, and the reference time. If these two values differ by greater than ten microseconds, then the system enters holdover mode, otherwise, the system moves to undergo a frequency update.

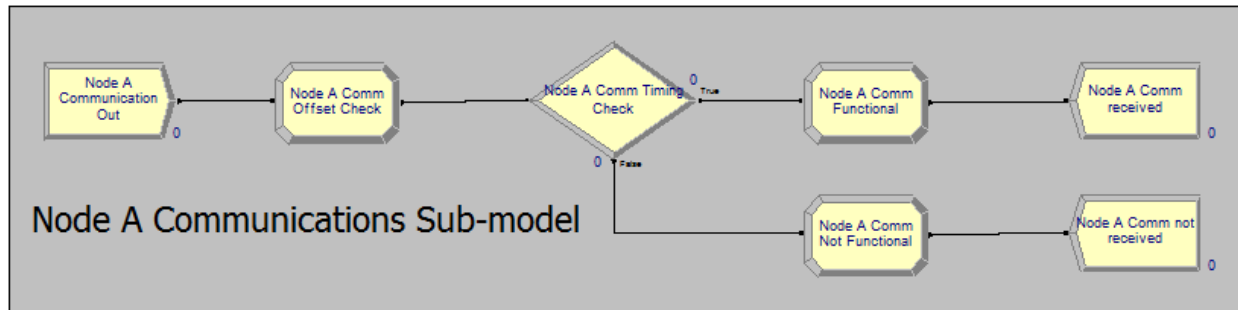
Upon being sent for a frequency update, random drift is assigned to the oscillator based upon an assumption of a quartz oscillator that has holdover duration of one day, with second to second fluctuations that are less than one microsecond in either direction. Once this random drift has been attributed, the oscillator is then disciplined by the reference signal by moving the oscillator, or system time, to the average of the two values. If the system is sent to holdover mode, then the random drift is

attributed and the system is told that it is now in holdover mode until such time that the GPS timing attack has stopped, disabling the disciplining algorithm.



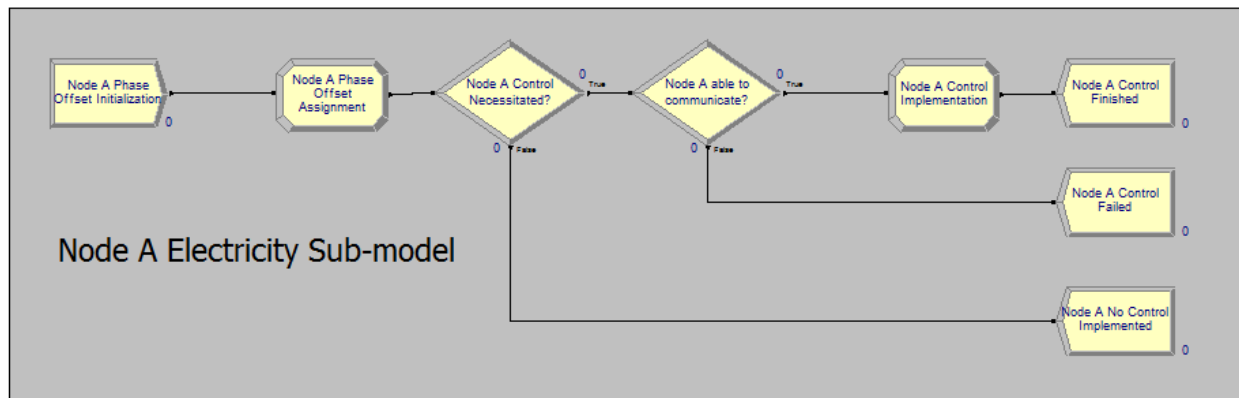
(Figure 5.2-2) Discrete Event Simulation GPSDO Sub-model

The communications system for each node is checked every second for the availability of communications. Once every second, an entity is created that checks to see if the system time is within 125 μ s of UTC, to determine if communications with that given node are intact. The value of 125 μ s is the upper-bound for this decision, in that it assumes the entity communicating with a given node has perfect timing, if this assumption were thrown out, then this threshold could be much lower. As long as the system time value is within 125 μ s of UTC, the node is able to receive communications from control centers, and control actions to adjust the phase angle associated with the node may take place. If communications are not functional, then the node is alerted, and no longer is able to receive these control orders for the electricity subsector component of that node (Figure 5.2-3).



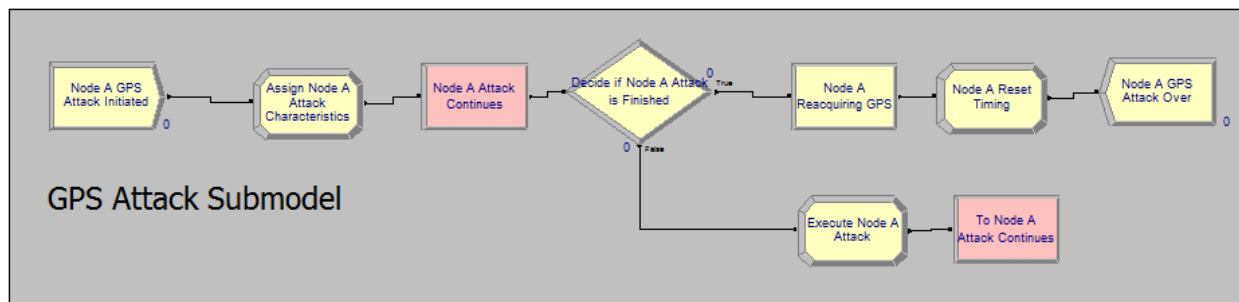
(Figure 5.2-3) Discrete Event Simulation Communications Sub-model

Figure 5.2-4 shows the electricity sub-model for node A. In this model, once again, the state of phase angle at node A is checked every second. Once an entity is spawned, the phase angle offset associated with the node moves in the direction of a predetermined random bias of one one-hundredth of a degree in either the positive or negative direction; in addition, the phasor observes a second by second random bias of one one-hundredth of a degree. The choice for these values is due to an assumption of controls needing to be implemented on the order of once a minute for peak load considerations, and following the IEEE Standard C37.118, which calls for PMU systems to maintain a phase offset of less than 0.573 degrees. Once the phase angle has been adjusted, the system determines whether or not a control action to adjust the phase angle is necessary based upon the IEEE Standard C37.118. If control is not necessary, then the entity is disposed of, and a new one is spawned the next second to repeat the process. If a control action is necessitated, the system next checks to see if communications are available. If communications are not currently available, then the control action fails. If communications are available, then a control action is implemented, moving the phase angle to within one one-hundredth of a degree of the notional zero angle. At this point the bias of the phasor is randomly reassigned to either the positive or negative direction, under an assumption the issuing the control action may or may not have some momentum associated with the change.



(Figure 5.2-4) Discrete Event Simulation Electricity Sub-model

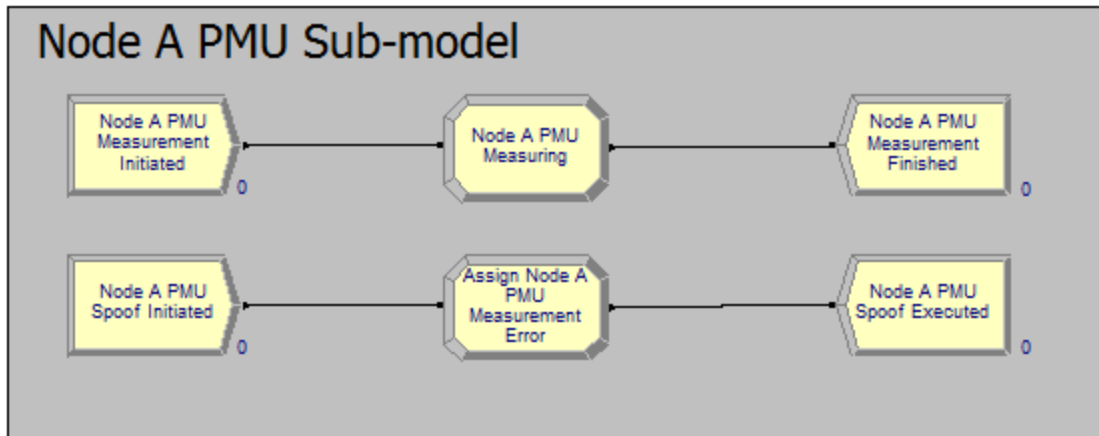
In order to model the event of a GPS spoofing attack against a specified node within a communications network, the model requires the attack to have a pre-specified duration and intensity. Once the attack has started, the model then checks periodically to see if the attack is currently ongoing. If the attack has not stopped, then the reference frequency for the node which the attack is applied is updated, and the duration of the attack is then decreased by one. At this point in time the GPS attack entity travels back to decide if the attack is still ongoing. Once the attack has finished, the system begins to reacquire GPS timing (for the purposes of demonstration this process has been said to take five minutes). Once GPS timing is restored the reference timing and system timing are both restored to UTC (Figure 5.2-5).



(Figure 5.2-5) Discrete Event Simulation GPS Attack Sub-model

PMUs are incorporated within the model at each node (see Figure 5.2-6), and subsequently change the behavior of the electricity sub-model. The electricity sub-model depicted in Figure 5.2-4 is not responding to the actual phase angle offset of a given node, but rather to the measurement of the phase angle offset taken by a PMU located at that specific node. For the purposes of this simulation, these measurements are taken once every second due to the frequency of control checks; while in reality there are on the order of 50 measurements taken every second. The PMU measurement is taken by adding the inherent measurement error of the PMU system to the actual phase angle offset at a given node. In the event of a spoofing attack against a PMU device, measurement error is assigned to the PMU based upon characteristics of the spoofing attack.

The last component of the simulation is that of the second to second check for the difference in phase angle between nodes A and B. In this check if the value of this difference exceeds ten degrees in actual phase angle difference, not difference in PMU measurements, then the simulation is terminated, and the time of blackout is recorded. Due to the structure of model implementer knowing both the characteristics of the spoofing attack along with the system requirements for detecting such attacks, the purpose of this simulation model is not to develop likelihoods of attacks being successful, as this designation is deterministic in this application. Rather, the simulation aims to model the interconnections and interdependencies amongst these systems, and potentially answer questions regarding the timeframe in which these attacks can move from initiation to negative consequences.



(Figure 5.2-6) Discrete Event Simulation PMU Sub-model

5.3 Discrete Event Simulation Model Results

The model was first run in the absence of spoofing attacks against either communications systems or PMU systems. The purpose for these dry runs was to ensure that the system behaved as intended in the absence of these anomalies. After running 10 replications of 10 days simulation time worth of trials, the simulation performed as expected with the GPSDO systems never entering holdover mode, and maintaining accuracy of greater than one microsecond of UTC. In addition control actions were implemented on average once every 59.3 seconds, with the quickest time between control actions being 31 seconds, and the longest 110 seconds.

In an attempt to duplicate an attack as demonstrated by Radionavigation Laboratory from the University of Texas outlined by Sheppard et al., in which a GPS spoofing attack bypasses detection by accelerating the rate of offset, inducing the system to produce failure within the electric power grid through issuing unnecessary control actions in 250 seconds, the discrete event simulation was able to obtain similar results. Following 100 replications of this simulated spoofing attack, failure between nodes A and B following a spoofing attack initiated against node A at time zero was found on average to occur after 258.45 seconds, with a 95% confidence interval of ± 2.96 seconds. The quickest that the

attack was found to succeed within the simulation was 245 seconds, while the longest was 293 seconds.

The attack was simulated by increasing the error of PMU measurements by a value of

$4X(\text{current time})^2/2095850$ following the prescribed acceleration of change of 4 m/s^2 (Sheppard et al., 2012).

The simulation also discovered that in the event of a coordinated spoofing attack, where PMUs at nodes A and B spoofing the measurement error in opposite directions using attacks of the same ramping nature as in the previous simulation took on average 198.7 seconds to induce power grid failure, with a 95% confidence interval of ± 0.5 seconds over 100 runs. The quickest of these runs occurred in 197 seconds, while the longest took 216 seconds. This level of coordinated attack was able to induce failure on average one minute faster than in the event of a single attack.

The model was also able to demonstrate bypassing internal GPSDO checks by increasing system time to values just under the designated threshold. In the instance of these attacks, the time to failure could be found as a direct result of the maximum allowable offset of the reference time from system time before sending the GPSDO into holdover mode. Once in holdover mode in these simulations, failure within the electric power grid came at the time predetermined by the oscillator holdover duration.

6. Conclusions

GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems form a complex S-o-S characterized by interconnections and interdependencies stemming from shared state variables, subsystems, and decisions. The electricity subsector is vulnerable to the threat of a GPS timing attack impacting either, the communications CI networks on which they rely for the transmission of SCADA/PMU data, or the PMU systems themselves, and the measurements which they provide. The likelihoods associated with these negative consequences experienced by the electricity subsector can be

directly impacted based upon decisions made by the communications sector of CI regarding choices of network architecture, and specific systems implemented.

It may not be possible to determine numerical values for the probabilities associated with the electricity subsector experiencing a failure due to a failure within GPS timing. However this thesis has shown that it is not unlikely that a GPS spoofing attack in particular could induce a failure within the electricity subsector. This is especially true in the future, when Smart Grid technologies drastically increase the dependence of the electricity subsector upon GPS timing for providing synchronization of nodes across the grid. This increased dependency stems from both the inception of automated control schemes based upon the use of PMUs and from an increased reliance upon communications sector networks with GPS timing dependencies. In the case of the former, the electricity subsector is able to determine the level of risk with which it is faced by maintaining the ability to decide their risk management options. As for the latter, the decisions made by the communications sector regarding the acceptable level of risk of communications outages caused by GPS timing failures that can potentially impact the electricity subsector depends upon cross-sector coordination in determining appropriate risk management strategies.

Through a foundation of state-based relationships amongst GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems, this thesis introduces a systematic methodological approach that can be applied to modeling other complex CI S-o-S as well. Through using these interconnections and interdependencies to develop fault and event trees, critical shared decisions amongst sectors of CI can be uncovered. Through the subsequent development of scenarios, based upon the event tree analysis performed, the implications of these shared decisions can be explored, and risk management options addressed.

6.1 Key Challenges

Of the numerous challenges associated with this thesis research, the greatest is arguably the lack of open source information regarding intentional GPS disruptions. While there are anecdotal accounts of GPS jamming events within the open literature, there is very little technical specificity associated with these examples, and virtually no account of malevolent GPS spoofing. This is especially true for the specific event of a GPS attack causing or even attempting to cause failure within the electricity subsector. In order to bridge this gap in the research, information from theoretical attacks was used in place of historical data. This made it difficult to determine any sort of numerical likelihood associated with these events taking place. However through developing the relationships amongst the systems of GPS timing, the electricity subsector, the communications sector, and SCADA/PMU systems, it was able to be shown that such an event was not unlikely.

Additionally, the complexity of each system comprising the CI S-o-S of interest within this research presented a key challenge. The electricity subsector is a complex S-o-S in its own right, and understanding the entirety of its workings is well beyond the scope of this thesis. In order to assess the risk with which GPS timing attacks pose to the electricity subsector, it was essential to understand essential state variables that characterize the relationships between the electricity subsector and GPS timing. This thesis required a technical understanding of GPS timing, GPSDO systems, the electricity subsector, communications networks, as well as SCADA and PMU systems in order to model the interconnections and interdependencies amongst these systems.

6.2 Summary of Contributions

First and foremost, this research introduces a systems-based methodological approach to addressing specific vulnerabilities within large scale complex CI S-o-S. Through a foundation rooted in developing relationships amongst systems at the state variable level, the thesis outlines a traceable path from the simplest of building blocks to the behavior of complex S-o-S composed of integrated systems. The research links event tree analysis to the augmentation of fault tree analysis when numerical

reliabilities and probabilities are not easily/possible to be determined. Since the approach is adaptable, it can be implemented to a specific instantiation of CI system to determine the corresponding likelihoods of negative consequences resulting from specific initiating events.

The discrete event simulation model serves as a starting point for modeling the impact of a GPS timing attack against a specific portion of CI. The model is modular and adaptable so that it may be implemented to model actual systems in the real world. It has been shown to produce repeatable results consistent with those found through physical experimentation. While physical experiments on the scale of the electricity subsector as a whole are not feasible due to the essentiality of the subsector maintaining working condition, simulation can serve as means for addressing system-wide concerns, and exhibits the ability to observe cascading effects that would not be producible through physical experimentation.

The research raises awareness into the interdependencies amongst the electricity subsector and communications sector through highlighting critical shared decisions between these sectors with direct implications on the level of risk faced by the electricity subsector to the threat of a GPS timing attack.

6.3 Recommendations for Future Research

The primary recommendation for future research would be to apply the methodology outlined to an existing portion of the electricity subsector. In order to do this, the research would need to be partnered with both the electric utility provider, as well as the communications carriers servicing the region. This effort would require a great deal of coordination, however would serve to further raise awareness of critical interdependencies between these two sectors. In addition to serving to further validate the methodology outlined in this thesis, the concerted effort including parties from both the electricity subsector and communications sector would shed new light onto shared decisions between two sectors of CI that have arguably the largest impact upon the nation's CI S-o-S.

Future research should also consider the feedback loop described yet not developed of the electricity subsector back into the communications sector. In developing further understanding of this interdependency, the potential for cascading effects resulting from a GPS spoofing attack could be explored.

While the discrete event simulation is developed within the thesis to demonstrate the efficacy of the modeling methodology outlined prior, it serves as a starting point for simulating specific instantiations of the electric power grid. Future research can apply the same modular approach to specific electricity subsector grid configurations. Through applying this methodology to specific power grids, decision-makers from the electric utilities could identify key nodes. These key nodes represent physical locations that require the most attention when risk management strategies are developed to combat the threat of GPS timing attacks to the electricity subsector. By addressing these key nodes, the electricity subsector could reduce the risk of cascading failures resulting from a GPS timing attack.

7. References

- 1) Carta, A.; Locci, N.; Muscas, C., "A PMU for the Measurement of Synchronized Harmonic Phasors in Three-Phase Distribution Networks," *Instrumentation and Measurement, IEEE Transactions on* , vol.58, no.10, pp.3723,3730, Oct. 2009.
- 2) Carta, Andrea ; Locci, Nicola ; Muscas, Carlo ; Pinna, Fabio ; Sulis, Sara "GPS and IEEE 1588 synchronization for the measurement of synchrophasors in electric power systems." *Computer Standards & Interfaces* 33.2 (2011): 176-181.
- 3) Coffed, Jeff. "The Threat of GPS Jamming: The Risk to an Information Utility," February, 2014.
[Online]. Available:
http://www.exelisinc.com/solutions/signalsentry/Documents/ThreatOfGPSJamming_February2014.pdf
- 4) Das, K.; Hazra, J.; Seetharam, D.P.; Reddi, R.K.; Sinha, A.K., "Real-time hybrid state estimation incorporating SCADA and PMU measurements," *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on* , vol., no., pp.1,8, 14-17 Oct. 2012
- 5) Garofalo, A.; Di Sarno, C.; Coppolino, L.; D'Antonio, S., "A GPS Spoofing Resilient WAMS for Smart Grid," EWDC 2013, LNCS 7869, pp. 134–147, 2013.
- 6) Haimes, Y. Y. (1991), Total Risk Management. Risk Analysis, 11: 169–171.
- 7) Haimes, Y. Y. (2009). *Risk modeling, assessment, and management*. 3rd ed. Hoboken, NJ: John Wiley & Sons.
- 8) Haimes, Y.Y., Kaplan, S., and Lambert, J.H. (2002) Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling. Risk Analysis, 22(2). Pp 383-397.
- 9) Hsiao, T., Massimini, S.V.. "Availability of GPS and WAAS with Standard and Degraded Constellations." PowerPoint presentation. The MITRE Corporation. June 2006.
- 10) Humphreys, T. et al., "Assessing the spoofing threat," *GPS World*, Jan. 2009.
- 11) IEEE Standard for Synchrophasor Data Transfer for Power Systems," *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)* , vol., no., pp.1,53, Dec. 28 2011
doi: 10.1109/IEEESTD.2011.6111222
- 12) Jacyna, G. "An Open-Ended Discussion on the Power Grid Facilitated Through Modeling Examples."

PowerPoint presentation. University of Virginia, Charlottesville, VA. February 21, 2014.

- 13) Jiang, X.; Zhang, J.; Harding, B.J.; Makela, J.J.; Dominguez-Garcia, A.D., "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," *Power Systems, IEEE Transactions on* , vol.28, no.3, pp.3253,3262, Aug. 2013.
- 14) Kaplan, E. D. and Hegerty, C., *Understanding GPS: Principles and Applications*, 2nd edition, Norwood, MA: Artech House Publishers, 2005.
- 15) Kaplan, S. and Garrick, B. J. (1981), On the Quantitative Definition of Risk. *Risk Analysis*, 1: 11–27.
- 16) Key, E., *Techniques to Counter GPS Spoofing*, MITRE Corp., Feb. 1995, internal memorandum.
- 17) Lombardi, M.A., "Microsecond accuracy at multiple sites: is it possible without GPS?," *Instrumentation & Measurement Magazine, IEEE* , vol.15, no.5, pp.14,21, Oct. 2012
- 18) Lombardi, M. A., "Legal and technical measurement requirements for time and frequency," *NCSLI Measure J. Meas. Sci.*, vol. 1, no. 3, pp. 60-69, Sept. 2006.
- 19) Phadke, A.G. and Thorp, J. , *Synchronized Phasor Measurements and Their Applications*. New York, NY, USA: Springer, 2008.
- 20) Shepard, D., Humphreys, T., and Fansler, A. "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," in *Proc. Int. Conf. Critical Infrastructure Protection*, Washington, DC, USA, 2012.
- 21) Symmetricom, "GPS Threats and Vulnerabilities: Power Industry GPS Timing Requirements", July 2010. *The Future of the Electric Grid*, 2011. [Online]. Available: http://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf
- 22) THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS), February 28, 2008.
- 23) The SmartGrid: An Introduction, 2013. [Online]. Available: <http://energy.gov>.
- 24) Summary of the North American SynchroPhasor Initiative (NASPI) Activity area, June 2012. [Online]. Available: <http://energy.gov/sites/prod/files/North%20American%20Synchrophasor%20Initiative%20%28NASPI%29%20Program%20Factsheet.pdf>.
- 25) Wang, Wenye ; Xu, Yi ; Khanna, Mohit (2011). "A survey on the communication architectures in smart grid." *Computer Networks*, 55 (15), 3604-3629.
- 26) Warner, J., and Johnston, R., *GPS Spoofing Countermeasures*, Dec. 2003, Los Alamos Research Paper LAUR-03-6163.15)

- 27) Wesson, K. "Spoofing & Implications for Telecom." September 18, 2013. [Online]. Available: http://rntfnd.org/wp-content/uploads/GPS-Spoofing-for-Telecom_UTex.pdf.
- 28) Y. Zhang, P. Markham, T. Xia, L. Chen, Y. Ye, Z. Wu, Z. Yuan, L. Wang, J. Bank, J. Burgett, R. W. Conners, and Y. Liu. Wide-area frequency monitoring network (FNET) architecture and applications. *IEEE Trans. Smart Grid*, 1(2):159–167, 2010.
- 29) Zhian Zhong; Chunchun Xu; Billian, B.J.; Li Zhang; Tsai, S.S.; Conners, R.W.; Centeno, V.A.; Phadke, A.G.; Yilu Liu, "Power system frequency monitoring network (FNET) implementation," *Power Systems, IEEE Transactions on*, vol.20, no.4, pp.1914,1921, Nov. 2005

Appendix A. RFRM Characteristics

1. **Un-detectability** – In the given scenario, is it possible to detect that the threat is present, and further, how difficult is it to detect the threat, with high un-detectability representing a threat that is undetectable, medium representing a difficulty in detecting the threat, and a low rating corresponding to being able to easily detect the threat.
2. **Uncontrollability** – Given that the threat has occurred and is recognized, at this point, what can be done to mitigate the resulting impact? A high uncontrollability rating equates to behavior that is uncontrollable, while a low rating represents a system that is easily controllable in this situation.
3. **Multiple Paths to Failure** – Given that the initiating event has occurred in the given scenario, this is the measure of how many ways the system can fail. If there are many ways in which the system can fail following the initiating event, then the risk level here is deemed high. A low rating is given when there is only one path in which the system can fail.
4. **Irreversibility** – After the initiating event has occurred is there any way to get the system back to its previous state. If not, and actions are irreversible, the risk level is high, since if the event were to occur, then there may not be a way to recover from the consequences; low corresponds with cases where the consequences are easily reversible.
5. **Duration of Effects** – How long are the impacts from the given scenario felt in the given system and those systems depending upon the directly affected system? A high risk level is given when the duration of effects is long, while low risk is given when the effects are of short duration.
6. **Cascading Effects** – In the scenario, are systems and persons other than the system in question put at risk from the consequences of the initiating event. For example, in the event of a localized black out, increased strain on the grid in other regions could result in more blackouts in other locations. If there are many potential cascading effects, this poses a high risk, while a low potential for cascading effects corresponds with a low risk for this category.
7. **Required Attack Sophistication** – In order for the scenario to occur, and the initiating event to take place, what level of sophistication is required of the attacker? Attacks of low sophistication or likely, naturally occurring events are deemed as representing high risk due to an increased likelihood of occurrence relative to lower likelihood attacks with high levels of sophistication. This is a measure of both the states of resilience, and vulnerability to specific threats. (Note: This measure does not directly account for differences in the other measures associated with more sophisticated attacks that pose a greater risk in other areas than low level attacks.)
8. **Design Immaturity** – This measure takes into account the risk associated with both new technologies that have not been tested as well as systems that are not as developed as is possible with the current state of technology. High risk is given to systems that do not take all of the available precautions, while low risk is given to systems that incorporate diverse redundancy with tried and tested methods. Increasing the maturity of design subsequently raises the required level of sophistication for an attack to be successfully implemented versus the system.

Appendix B. Discrete Event Simulation SIMAN Code

```

;
;
;   Model statements for module:  BasicProcess.Create 1 (Model Initialization)
;

80$           CREATE,
1,HoursToBaseTime(0.0),Initializer:HoursToBaseTime(EXPO(1)),1:NEXT(81$);

81$           ASSIGN:           Model Initialization.NumberOut=Model
Initialization.NumberOut + 1:NEXT(1$);

;
;
;   Model statements for module:  BasicProcess.Assign 1 (Assign Initial Parameters)
;
1$           ASSIGN:           Node A Time Bias=UNIF(-125,125):
                                Nominal Timing=0:
                                Node A Reference Timing=0:
                                Node A Timing=0:
                                Node A Phase Offset=0:
                                Node A Phase Bias=DISC(0.5,-.01,1.0,.01):
                                Node A PMU Attack Number=1:
                                Node A PMU Measurement=0:
                                Node A Daily Drift=UNIF(-125,125):
                                Node A Drift=Node A Daily Drift/86400:
                                Node B Time Bias=UNIF(-125,125):
                                Node B Reference Timing=0:
                                Node B Timing=0:
                                Node B Phase Offset=0:
                                Node B Phase Bias=DISC(0.5,-.01,1.0,.01):
                                Node B PMU Attack Number=1:
                                Node B PMU Measurement=0:
                                Node B Daily Drift=UNIF(-125,125):
                                Node B Drift=Node B Daily Drift/86400:NEXT(0$);

;
;
;   Model statements for module:  BasicProcess.Dispose 1 (Finish Initialization)
;
0$           ASSIGN:           Finish Initialization.NumberOut=Finish
Initialization.NumberOut + 1;
84$           DISPOSE:         Yes;

;
;
;   Model statements for module:  BasicProcess.Create 2 (Electricity Check)
;

85$           CREATE,           1,SecondstoBaseTime(0.0),Electricity
Checker:SecondstoBaseTime(1):NEXT(86$);

86$           ASSIGN:           Electricity Check.NumberOut=Electricity Check.NumberOut +
1:NEXT(2$);

```

```

;
;
;   Model statements for module:  BasicProcess.Assign 2 (Check for AB Phase
Difference)
;
2$   ASSIGN:      AB Phase Difference=ABS(Node A Phase Offset - Node B
Phase Offset):NEXT(3$);

;
;
;   Model statements for module:  BasicProcess.Dispose 2 (End Electricity Check)
;
3$   ASSIGN:      End Electricity Check.NumberOut=End Electricity
Check.NumberOut + 1;
89$   DISPOSE:    Yes;

;
;
;   Model statements for module:  BasicProcess.Create 3 (Node A GPSDO Update)
;

90$   CREATE,      1,SecondstoBaseTime(0.0),GPS Updater
A:SecondstoBaseTime(1):NEXT(91$);

91$   ASSIGN:      Node A GPSDO Update.NumberOut=Node A GPSDO
Update.NumberOut + 1:NEXT(4$);

;
;
;   Model statements for module:  BasicProcess.Decide 1 (Node A not in holdover?)
;
4$   BRANCH,      1:
                If,Node A HO==0,94$,Yes:
                Else,95$,Yes;
94$   ASSIGN:      Node A not in holdover?.NumberOut True=Node A not in
holdover?.NumberOut True + 1:NEXT(8$);

95$   ASSIGN:      Node A not in holdover?.NumberOut False=Node A not in
holdover?.NumberOut False + 1:NEXT(6$);

;
;
;   Model statements for module:  BasicProcess.Assign 3 (Node A Holdover Check)
;
8$   ASSIGN:      Node A GPS Check=ABS(Node A Reference Timing - Node A
Timing):NEXT(5$);

;
;
;   Model statements for module:  BasicProcess.Decide 2 (Node A enter holdover?)
;
5$   BRANCH,      1:
                If,Node A HO Check>=10,96$,Yes:
                Else,97$,Yes;
96$   ASSIGN:      Node A enter holdover?.NumberOut True=Node A enter
holdover?.NumberOut True + 1:NEXT(7$);

```

```

97$      ASSIGN:      Node A enter holdover?.NumberOut False=Node A enter
holdover?.NumberOut False + 1:NEXT(9$);

;
;
;      Model statements for module:  AdvancedTransfer.Route 2 (To Node A Holdover)
;
7$      ROUTE:      0.000000000000000,Node A Holdover;

;
;
;      Model statements for module:  AdvancedTransfer.Route 3 (To Node A Frequency
Update)
;
9$      ROUTE:      0.000000000000000,Node A Frequency Update;

;
;
;      Model statements for module:  AdvancedTransfer.Route 1 (To Node A Holdover
Model)
;
6$      ROUTE:      0.000000000000000,Node A Holdover;

;
;
;      Model statements for module:  AdvancedTransfer.Station 1 (Node A Frequency
Update)
;

10$      STATION,      Node A Frequency Update;
100$     DELAY:      0.0,,VA:NEXT(11$);

;
;
;      Model statements for module:  BasicProcess.Assign 4 (Node A Random Drift)
;
11$      ASSIGN:      Node A Timing=Node A Timing + Node A Drift + UNIF(-
1,1):NEXT(12$);

;
;
;      Model statements for module:  BasicProcess.Assign 5 (Node A Disciplining)
;
12$      ASSIGN:      Node A Timing=Node A Reference Timing + (Node A Reference
Timing - Node A Timing)/2:NEXT(13$);

;
;
;      Model statements for module:  BasicProcess.Dispose 3 (End Node A Frequency
Update)
;
13$      ASSIGN:      End Node A Frequency Update.NumberOut=End Node A
Frequency Update.NumberOut + 1;
101$     DISPOSE:      Yes;

```

```

;
;
;   Model statements for module:  AdvancedTransfer.Station 2 (Node A Holdover)
;

14$      STATION,      Node A Holdover;
104$     DELAY:        0.0,,VA:NEXT(15$);

;
;
;   Model statements for module:  BasicProcess.Assign 6 (Node A Holdover Drift)
;
15$      ASSIGN:       Node A HO=1:
                        Node A Timing=Node A Timing + Node A Drift:NEXT(16$);

;
;
;   Model statements for module:  BasicProcess.Dispose 4 (End Node A Holdover
Update)
;
16$      ASSIGN:       End Node A Holdover Update.NumberOut=End Node A Holdover
Update.NumberOut + 1;
105$     DISPOSE:      Yes;

;
;
;   Model statements for module:  BasicProcess.Create 4 (Node A Communication Out)
;

106$     CREATE,       1,SecondstoBaseTime(0.0),Node A
Comm:SecondstoBaseTime(1):NEXT(107$);

107$     ASSIGN:       Node A Communication Out.NumberOut=Node A Communication
Out.NumberOut + 1:NEXT(17$);

;
;
;   Model statements for module:  BasicProcess.Assign 7 (Node A Comm Offset Check)
;
17$      ASSIGN:       Node A Comm Offset=ABS(Node A Timing):NEXT(18$);

;
;
;   Model statements for module:  BasicProcess.Decide 3 (Node A Comm Timing Check)
;
18$      BRANCH,       1:
                        If,Node A Comm Offset<=125,110$,Yes:
                        Else,111$,Yes;
110$     ASSIGN:       Node A Comm Timing Check.NumberOut True=Node A Comm
Timing Check.NumberOut True + 1:NEXT(19$);

111$     ASSIGN:       Node A Comm Timing Check.NumberOut False=Node A Comm
Timing Check.NumberOut False + 1:NEXT(21$);

;
;
;   Model statements for module:  BasicProcess.Assign 8 (Node A Comm Functional)

```

```

;
19$          ASSIGN:          Node A Comm ON=1:NEXT(20$);

;
;
;      Model statements for module:  BasicProcess.Dispose 5 (Node A Comm received)
;
20$          ASSIGN:          Node A Comm received.NumberOut=Node A Comm
received.NumberOut + 1;
112$         DISPOSE:        Yes;

;
;
;      Model statements for module:  BasicProcess.Assign 9 (Node A Comm Not Functional)
;
21$          ASSIGN:          Node A Comm ON=0:NEXT(22$);

;
;
;      Model statements for module:  BasicProcess.Dispose 6 (Node A Comm not received)
;
22$          ASSIGN:          Node A Comm not received.NumberOut=Node A Comm not
received.NumberOut + 1;
113$         DISPOSE:        Yes;

;
;
;      Model statements for module:  BasicProcess.Create 5 (Node A GPS Attack
Initiated)
;
114$         CREATE,          0,SecondstoBaseTime(1.0),GPS Attacker
A:SecondstoBaseTime(1),1:NEXT(115$);

115$         ASSIGN:          Node A GPS Attack Initiated.NumberOut=Node A GPS Attack
Initiated.NumberOut + 1:NEXT(23$);

;
;
;      Model statements for module:  BasicProcess.Assign 10 (Assign Node A Attack
Characteristics)
;
23$          ASSIGN:          Node A Attack Duration=10000:
                             Node A Attack Timing Change=UNIF(.4,.4):
                             Node A Attack Time=1:NEXT(25$);

;
;
;      Model statements for module:  AdvancedTransfer.Station 3 (Node A Attack
Continues)
;
25$          STATION,         Node A Attack Continues;
120$         DELAY:          0.0,,VA:NEXT(24$);

;

```

```

;
;   Model statements for module:  BasicProcess.Decide 4 (Decide if Node A Attack is
Finished)
;
24$           BRANCH,           1:
                               If,Node A Attack Time>Node A Attack Duration,121$,Yes:
                               Else,122$,Yes;
121$           ASSIGN:           Decide if Node A Attack is Finished.NumberOut True=
                               Decide if Node A Attack is Finished.NumberOut True +
1:NEXT(29$);

122$           ASSIGN:           Decide if Node A Attack is Finished.NumberOut False=
                               Decide if Node A Attack is Finished.NumberOut False +
1:NEXT(27$);

;
;
;   Model statements for module:  AdvancedProcess.Delay 1 (Node A Reacquiring GPS)
;
29$           DELAY:             300.0000000000000000,,VA:NEXT(30$);

;
;
;   Model statements for module:  BasicProcess.Assign 12 (Node A Reset Timing)
;
30$           ASSIGN:           Node A Reference Timing=0:
                               Node A Timing=0:NEXT(26$);

;
;
;   Model statements for module:  BasicProcess.Dispose 7 (Node A GPS Attack Over)
;
26$           ASSIGN:           Node A GPS Attack Over.NumberOut=Node A GPS Attack
Over.NumberOut + 1;
123$          DISPOSE:          Yes;

;
;
;   Model statements for module:  BasicProcess.Assign 11 (Execute Node A Attack)
;
27$           ASSIGN:           Node A Reference Timing=Node A Reference Timing + Node A
Attack Timing Change:
                               Node A Attack Time=Node A Attack Time + 1:NEXT(28$);

;
;
;   Model statements for module:  AdvancedTransfer.Route 4 (To Node A Attack
Continues)
;
28$           ROUTE:            1,Node A Attack Continues;

;
;
;   Model statements for module:  BasicProcess.Create 6 (Node A Phase Offset
Initialization)
;

```

```

124$      CREATE,          1,SecondstoBaseTime(0.0),Node A
Electricity:SecondstoBaseTime(1):NEXT(125$);

125$      ASSIGN:         Node A Phase Offset Initialization.NumberOut=Node A Phase
Offset Initialization.NumberOut + 1
                        :NEXT(31$);

;
;
;      Model statements for module:  BasicProcess.Assign 13 (Node A Phase Offset
Assignment)
;
31$      ASSIGN:         Node A Phase Offset=Node A Phase Offset + DISC(0.5,-
.01,1.0,.01)+Node A Phase Bias:NEXT(40$);

;
;
;      Model statements for module:  BasicProcess.Decide 7 (Node A Control
Necessitated?)
;
40$      BRANCH,         1:
                        If,ABS(Node A PMU Measurement)>=0.573,128$,Yes:
                        Else,129$,Yes;
128$      ASSIGN:         Node A Control Necessitated?.NumberOut True=Node A
Control Necessitated?.NumberOut True + 1
                        :NEXT(32$);

129$      ASSIGN:         Node A Control Necessitated?.NumberOut False=Node A
Control Necessitated?.NumberOut False + 1
                        :NEXT(41$);

;
;
;      Model statements for module:  BasicProcess.Decide 6 (Node A able to
communicate?)
;
32$      BRANCH,         1:
                        If,Node A Comm ON==1,130$,Yes:
                        Else,131$,Yes;
130$      ASSIGN:         Node A able to communicate?.NumberOut True=Node A able to
communicate?.NumberOut True + 1:NEXT(33$);

131$      ASSIGN:         Node A able to communicate?.NumberOut False=Node A able
to communicate?.NumberOut False + 1
                        :NEXT(35$);

;
;
;      Model statements for module:  BasicProcess.Assign 14 (Node A Control
Implementation)
;
33$      ASSIGN:         Node A Phase Offset=UNIF(-0.1,0.1)+Node A Measurement
Error:
                        Node A Phase Bias=DISC(0.5,-.01,1.0,.01):NEXT(34$);

;
;
;      Model statements for module:  BasicProcess.Dispose 8 (Node A Control Finished)

```

```

;
34$      ASSIGN:      Node A Control Finished.NumberOut=Node A Control
Finished.NumberOut + 1;
132$     DISPOSE:     Yes;

;
;
;      Model statements for module:  BasicProcess.Dispose 9 (Node A Control Failed)
;
35$      ASSIGN:      Node A Control Failed.NumberOut=Node A Control
Failed.NumberOut + 1;
133$     DISPOSE:     Yes;

;
;
;      Model statements for module:  BasicProcess.Dispose 12 (Node A No Control
Implemented)
;
41$      ASSIGN:      Node A No Control Implemented.NumberOut=Node A No Control
Implemented.NumberOut + 1;
134$     DISPOSE:     Yes;

;
;
;      Model statements for module:  BasicProcess.Create 7 (Node A PMU Measurement
Initiated)
;

135$     CREATE,      1,SecondstoBaseTime(0.0),Node A PMU
Entity:SecondstoBaseTime(1):NEXT(136$);

136$     ASSIGN:      Node A PMU Measurement Initiated.NumberOut=Node A PMU
Measurement Initiated.NumberOut + 1:NEXT(36$);

;
;
;      Model statements for module:  BasicProcess.Assign 15 (Node A PMU Measuring)
;
36$      ASSIGN:      Node A PMU Measurement=Node A Phase Offset + Node A
Measurement Error:NEXT(37$);

;
;
;      Model statements for module:  BasicProcess.Dispose 10 (Node A PMU Measurement
Finished)
;
37$      ASSIGN:      Node A PMU Measurement Finished.NumberOut=Node A PMU
Measurement Finished.NumberOut + 1;
139$     DISPOSE:     Yes;

;
;
;      Model statements for module:  BasicProcess.Create 8 (Node A PMU Spoof Initiated)
;

140$     CREATE,      0,SecondstoBaseTime(0.0),PMU Spoof
Entity:SecondstoBaseTime(1),250:NEXT(141$);

```



```

141$      ASSIGN:      Node A PMU Spoof Initiated.NumberOut=Node A PMU Spoof
Initiated.NumberOut + 1:NEXT(38$);

;
;
;      Model statements for module:  BasicProcess.Assign 16 (Assign Node A PMU
Measurement Error)
;
38$      ASSIGN:      Node A PMU Attack Number=Node A PMU Attack Number + 1:
Node A Measurement Error=
Node A Measurement Error + 4*(Node A PMU Attack
Number)*(Node A PMU Attack Number)/2095850
:NEXT(39$);

;
;
;      Model statements for module:  BasicProcess.Dispose 11 (Node A PMU Spoof
Executed)
;
39$      ASSIGN:      Node A PMU Spoof Executed.NumberOut=Node A PMU Spoof
Executed.NumberOut + 1;
144$      DISPOSE:      Yes;

;
;
;      Model statements for module:  BasicProcess.Create 9 (Node B GPSDO Update)
;

145$      CREATE,      1,SecondstoBaseTime(0.0),GPS Updater
B:SecondstoBaseTime(1):NEXT(146$);

146$      ASSIGN:      Node B GPSDO Update.NumberOut=Node B GPSDO
Update.NumberOut + 1:NEXT(42$);

;
;
;      Model statements for module:  BasicProcess.Decide 8 (Node B not in holdover?)
;
42$      BRANCH,      1:
If,Node A HO==0,149$,Yes:
Else,150$,Yes;
149$      ASSIGN:      Node B not in holdover?.NumberOut True=Node B not in
holdover?.NumberOut True + 1:NEXT(43$);

150$      ASSIGN:      Node B not in holdover?.NumberOut False=Node B not in
holdover?.NumberOut False + 1:NEXT(45$);

;
;
;      Model statements for module:  BasicProcess.Assign 17 (Node B Holdover Check)
;
43$      ASSIGN:      Node B GPS Check=ABS(Node B Reference Timing - Node B
Timing):NEXT(44$);

;
;

```

```

;      Model statements for module:  BasicProcess.Decide 9 (Node B enter holdover?)
;
44$      BRANCH,          1:
                        If,Node B HO Check>=10,151$,Yes:
                        Else,152$,Yes;
151$      ASSIGN:         Node B enter holdover?.NumberOut True=Node B enter
holdover?.NumberOut True + 1:NEXT(46$);

152$      ASSIGN:         Node B enter holdover?.NumberOut False=Node B enter
holdover?.NumberOut False + 1:NEXT(47$);

;
;
;      Model statements for module:  AdvancedTransfer.Route 6 (To Node B Holdover)
;
46$      ROUTE:           0.0000000000000000,Node B Holdover;

;
;
;      Model statements for module:  AdvancedTransfer.Route 7 (To Node B Frequency
Update)
;
47$      ROUTE:           0.0000000000000000,Node B Frequency Update;

;
;
;      Model statements for module:  AdvancedTransfer.Route 5 (To Node B Holdover
Model)
;
45$      ROUTE:           0.0000000000000000,Node B Holdover;

;
;
;      Model statements for module:  AdvancedTransfer.Station 4 (Node B Frequency
Update)
;
48$      STATION,         Node B Frequency Update;
155$     DELAY:           0.0,,VA:NEXT(49$);

;
;
;      Model statements for module:  BasicProcess.Assign 18 (Node B Random Drift)
;
49$      ASSIGN:          Node B Timing=Node B Timing + Node B Drift + UNIF(-
1,1):NEXT(50$);

;
;
;      Model statements for module:  BasicProcess.Assign 19 (Node B Disciplining)
;
50$      ASSIGN:          Node B Timing=Node B Reference Timing + (Node B Reference
Timing - Node B Timing)/2:NEXT(51$);

;
;

```

```

;      Model statements for module:  BasicProcess.Dispose 13 (End Node B Frequency
Update)
;
51$      ASSIGN:      End Node B Frequency Update.NumberOut=End Node B
Frequency Update.NumberOut + 1;
156$      DISPOSE:      Yes;

;
;
;      Model statements for module:  AdvancedTransfer.Station 5 (Node B Holdover)
;

52$      STATION,      Node B Holdover;
159$      DELAY:      0.0,,VA:NEXT(53$);

;
;
;      Model statements for module:  BasicProcess.Assign 20 (Node B Holdover Drift)
;
53$      ASSIGN:      Node B HO=1:
                        Node B Timing=Node B Timing + Node B Drift:NEXT(54$);

;
;
;      Model statements for module:  BasicProcess.Dispose 14 (End Node B Holdover
Update)
;
54$      ASSIGN:      End Node B Holdover Update.NumberOut=End Node B Holdover
Update.NumberOut + 1;
160$      DISPOSE:      Yes;

;
;
;      Model statements for module:  BasicProcess.Create 10 (Node B Communication Out)
;

161$      CREATE,      1,SecondstoBaseTime(0.0),Node B
Comm:SecondstoBaseTime(1):NEXT(162$);

162$      ASSIGN:      Node B Communication Out.NumberOut=Node B Communication
Out.NumberOut + 1:NEXT(55$);

;
;
;      Model statements for module:  BasicProcess.Assign 21 (Node B Comm Offset Check)
;
55$      ASSIGN:      Node B Comm Offset=ABS(Node B Timing):NEXT(56$);

;
;
;      Model statements for module:  BasicProcess.Decide 10 (Node B Comm Timing Check)
;
56$      BRANCH,      1:
                        If,Node B Comm Offset<=125,165$,Yes:
                        Else,166$,Yes;
165$      ASSIGN:      Node B Comm Timing Check.NumberOut True=Node B Comm
Timing Check.NumberOut True + 1:NEXT(57$);

```

```

166$      ASSIGN:      Node B Comm Timing Check.NumberOut False=Node B Comm
Timing Check.NumberOut False + 1:NEXT(59$);

;
;
;      Model statements for module:  BasicProcess.Assign 22 (Node B Comm Functional)
;
57$      ASSIGN:      Node B Comm ON=1:NEXT(58$);

;
;
;      Model statements for module:  BasicProcess.Dispose 15 (Node B Comm received)
;
58$      ASSIGN:      Node B Comm received.NumberOut=Node B Comm
received.NumberOut + 1;
167$      DISPOSE:      Yes;

;
;
;      Model statements for module:  BasicProcess.Assign 23 (Node B Comm Not
Functional)
;
59$      ASSIGN:      Node B Comm ON=0:NEXT(60$);

;
;
;      Model statements for module:  BasicProcess.Dispose 16 (Node B Comm not received)
;
60$      ASSIGN:      Node B Comm not received.NumberOut=Node B Comm not
received.NumberOut + 1;
168$      DISPOSE:      Yes;

;
;
;      Model statements for module:  BasicProcess.Create 11 (Node B Phase Offset
Initilization)
;

169$      CREATE,      1,SecondstoBaseTime(0.0),Node B
Electricity:SecondstoBaseTime(1):NEXT(170$);

170$      ASSIGN:      Node B Phase Offset Initilization.NumberOut=Node B Phase
Offset Initilization.NumberOut + 1
: NEXT(61$);

;
;
;      Model statements for module:  BasicProcess.Assign 24 (Node B Phase Offset
Assignment)
;
61$      ASSIGN:      Node B Phase Offset=Node B Phase Offset + DISC(0.5,-
.01,1.0,.01)+Node B Phase Bias:NEXT(79$);

;
;

```

```

;      Model statements for module:  BasicProcess.Decide 14 (Decide 14)
;
79$      BRANCH,          1:
                        If,ABS(Node B PMU Measurement)>=0.573,173$,Yes:
                        Else,174$,Yes;
173$      ASSIGN:          Decide 14.NumberOut True=Decide 14.NumberOut True +
1:NEXT(62$);

174$      ASSIGN:          Decide 14.NumberOut False=Decide 14.NumberOut False +
1:NEXT(66$);

;
;
;      Model statements for module:  BasicProcess.Decide 11 (Node B able to
communicate?)
;
62$      BRANCH,          1:
                        If,Node B Comm ON==1,175$,Yes:
                        Else,176$,Yes;
175$      ASSIGN:          Node B able to communicate?.NumberOut True=Node B able to
communicate?.NumberOut True + 1:NEXT(63$);

176$      ASSIGN:          Node B able to communicate?.NumberOut False=Node B able
to communicate?.NumberOut False + 1
                        :NEXT(65$);

;
;
;      Model statements for module:  BasicProcess.Assign 25 (Node B Control
Implementation)
;
63$      ASSIGN:          Node B Phase Offset=UNIF(-0.1,0.1)+Node B Measurement
Error:
                        Node B Phase Bias=DISC(0.5,-.01,1.0,.01):NEXT(64$);

;
;
;      Model statements for module:  BasicProcess.Dispose 17 (Node B Control Finished)
;
64$      ASSIGN:          Node B Control Finished.NumberOut=Node B Control
Finished.NumberOut + 1;
177$      DISPOSE:          Yes;

;
;
;      Model statements for module:  BasicProcess.Dispose 18 (Node B Control Failed)
;
65$      ASSIGN:          Node B Control Failed.NumberOut=Node B Control
Failed.NumberOut + 1;
178$      DISPOSE:          Yes;

;
;
;      Model statements for module:  BasicProcess.Dispose 19 (Node B No Control
Implemented)
;
66$      ASSIGN:          Node B No Control Implemented.NumberOut=Node B No Control
Implemented.NumberOut + 1;

```

```

179$      DISPOSE:      Yes;

;
;
;      Model statements for module:  BasicProcess.Create 12 (Node B GPS Attack
Initiated)
;

180$      CREATE,      0,SecondstoBaseTime(0.0),GPS Attacker
B:SecondstoBaseTime(1):NEXT(181$);

181$      ASSIGN:      Node B GPS Attack Initiated.NumberOut=Node B GPS Attack
Initiated.NumberOut + 1:NEXT(67$);

;
;
;      Model statements for module:  BasicProcess.Assign 26 (Assign Node B Attack
Characteristics)
;
67$      ASSIGN:      Node B Attack Duration=10000:
                        Node B Attack Timing Change=UNIF(.4,.4):
                        Node B Attack Time=1:NEXT(68$);

;
;
;      Model statements for module:  AdvancedTransfer.Station 6 (Node B Attack
Continues)
;

68$      STATION,      Node B Attack Continues;
186$      DELAY:      0.0,,VA:NEXT(69$);

;
;
;      Model statements for module:  BasicProcess.Decide 13 (Decide if Node B Attack is
Finished)
;
69$      BRANCH,      1:
                        If,Node B Attack Time>Node B Attack Duration,187$,Yes:
                        Else,188$,Yes;
187$      ASSIGN:      Decide if Node B Attack is Finished.NumberOut True=
                        Decide if Node B Attack is Finished.NumberOut True +
1:NEXT(70$);

188$      ASSIGN:      Decide if Node B Attack is Finished.NumberOut False=
                        Decide if Node B Attack is Finished.NumberOut False +
1:NEXT(73$);

;
;
;      Model statements for module:  AdvancedProcess.Delay 2 (Node B Reacquiring GPS)
;
70$      DELAY:      300.0000000000000000,,VA:NEXT(71$);

;
;
;      Model statements for module:  BasicProcess.Assign 27 (Node B Reset Timing)

```

```

;
71$          ASSIGN:          Node B Reference Timing=0:
                          Node B Timing=0:NEXT(72$);

;
;
;      Model statements for module:  BasicProcess.Dispose 20 (Node B GPS Attack Over)
;
72$          ASSIGN:          Node B GPS Attack Over.NumberOut=Node B GPS Attack
Over.NumberOut + 1;
189$         DISPOSE:         Yes;

;
;
;      Model statements for module:  BasicProcess.Assign 28 (Excute Node B Attack)
;
73$          ASSIGN:          Node B Reference Timing=Node B Reference Timing + Node B
Attack Timing Change:NEXT(74$);

;
;
;      Model statements for module:  AdvancedTransfer.Route 8 (To Node B Attack
Continues)
;
74$          ROUTE:           1,Node B Attack Continues;

;
;
;      Model statements for module:  BasicProcess.Create 13 (Node B PMU Measurement
Initiated)
;
190$         CREATE,          1,SecondstoBaseTime(0.0),Node B PMU
Entity:SecondstoBaseTime(1):NEXT(191$);

191$         ASSIGN:          Node B PMU Measurement Initiated.NumberOut=Node B PMU
Measurement Initiated.NumberOut + 1:NEXT(75$);

;
;
;      Model statements for module:  BasicProcess.Assign 29 (Node B PMU Measuring)
;
75$          ASSIGN:          Node B PMU Measurement=Node B Phase Offset + Node B
Measurement Error:NEXT(76$);

;
;
;      Model statements for module:  BasicProcess.Dispose 21 (Node B PMU Measurement
Finished)
;
76$          ASSIGN:          Node B PMU Measurement Finished.NumberOut=Node B PMU
Measurement Finished.NumberOut + 1;
194$         DISPOSE:         Yes;

;
;

```

```
;      Model statements for module:  BasicProcess.Create 14 (Node B PMU Spoof
Initiated)
;

195$      CREATE,          0,NSEXPO(Schedule 1),PMU Spoof Entity:NSEXPO(Schedule
1),250:NEXT(196$);

196$      ASSIGN:          Node B PMU Spoof Initiated.NumberOut=Node B PMU Spoof
Initiated.NumberOut + 1:NEXT(77$);

;
;
;      Model statements for module:  BasicProcess.Assign 30 (Assign Node B PMU
Measurement Error)
;
77$      ASSIGN:          Node B PMU Attack Number=Node B PMU Attack Number + 1:
                          Node B Measurement Error=
                          Node A Measurement Error + 4*(Node B PMU Attack
Number)*(Node B PMU Attack Number)/2095850
                          :NEXT(78$);

;
;
;      Model statements for module:  BasicProcess.Dispose 22 (Node B PMU Spoof
Executed)
;
78$      ASSIGN:          Node B PMU Spoof Executed.NumberOut=Node B PMU Spoof
Executed.NumberOut + 1;
199$      DISPOSE:        Yes;
```