Taxonomy of Information Security Threats in Wide Area Measurement Systems

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

by

Nagarjuna Nuthalapati

Major Professor: Jia Song, Ph.D.

Committee Members: Jim Alves-Foss, Ph.D.; Brian Johnson, Ph.D.

Department Administrator: John C. Crepeau, Ph.D.

December 2017

Authorization to Submit Thesis

This thesis of Nagarjuna Nuthalapati, submitted for the degree of Master of Science with a major in Computer Science and titled "Taxonomy of Information Security Threats in Wide Area Measurement Systems," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____Date_____
Jia Song, Ph.D.

Committee Members: _____Date_____
Jim Alves-Foss, Ph.D.

_____Date_____
Brian Johnson, Ph.D.

Department Administrator: _____Date_____
John C. Crepeau, Ph.D.

Abstract

This thesis is part of a National Science Foundation (NSF) project focused on securing power grids against data injection attacks. Power grids are undergoing their largest technological transformation since their invention. Wide Area Measurement Systems (WAMS) adopt several advanced components and the Phasor Measurement Unit (PMU) is considered the most important one in them. In a power grid, PMUs are used to obtain measurements of the system and report them to the control center with a time-stamp for real-time monitoring and analysis. PMUs in North America utilize GPS (Global Positioning System) to get a precise to allow operators a wide area snapshot of a power grids and therefore enhance the reliability of the system. However, PMUs may be susceptible to cyber-attacks as well. This thesis surveys the vulnerabilities that can affect the operation of power grids through PMUs and develops a fault tree of studied vulnerabilities.

In addition, this thesis evaluates threats associated with WAMS that can affect the proper functioning of WAMS. A taxonomy of threats in WAMS is developed using both an impact-oriented and a threat-oriented approach, considering both benign and malicious faults. The taxonomy of WAMS threats is based on an abstract WAMS model with PMUs as sensor units and PDCs (Phasor Data Concentrators) and Super PDCs as correlation units. A qualitative assessment scale is used to describe associated impact for the threat sources.

Acknowledgements

I would like to thank my major professor Dr. Jia Song for all the knowledge she has imparted, for her support, and her patient guidance in helping to make this thesis a reality.

I would like to thank my committee member and instructor Dr. James Alves-Foss for his constant support, encouragement and valuable advice that he shared through my study at the University of Idaho.

I would like to thank my committee member Dr. Brian Johnson for helping with this thesis and taking time out of his busy schedule to review and provide their valuable suggestions.

I would like to thank Dr. Sara Eftekharnejad for providing an opportunity to be a part of this project and supporting this thesis. I would like to thank Sagnik Basumallik and Nathen Davis for their input at various stages of my research.

I would like to thank all the faculty and staff members of Department of Computer Science for their help and support during my study in the department.

I wish to acknowledge the National Science Foundation (NSF), for supporting me during the course of this research through grant number 1600058.

Finally, I would like to thank my family and friends for being supportive, and for being part of the joyful life I had in Moscow, Idaho.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

Background and Overview

A power grid is an interconnected network that transmits electrical power from generators to consumers. These grids are generally vast in size and constant system response actions is required to ensure proper operation. Unlike traditional power grids, a modern grid uses advanced technology to enable faster two-way communication between power generators and consumers with more bandwidth. Due to a rise in the use of intermittent energy sources like the solar and wind, traditional grids are more fully utilizing this two-way communication model to keep the system stable and fulfill the needs of the consumers. The two-way communication model helps a power system operator in filling the gap between supplies like traditional power generators and intermittent sources, and various power demanding loads. A sample power grid model is illustrated in Figure 1.1:

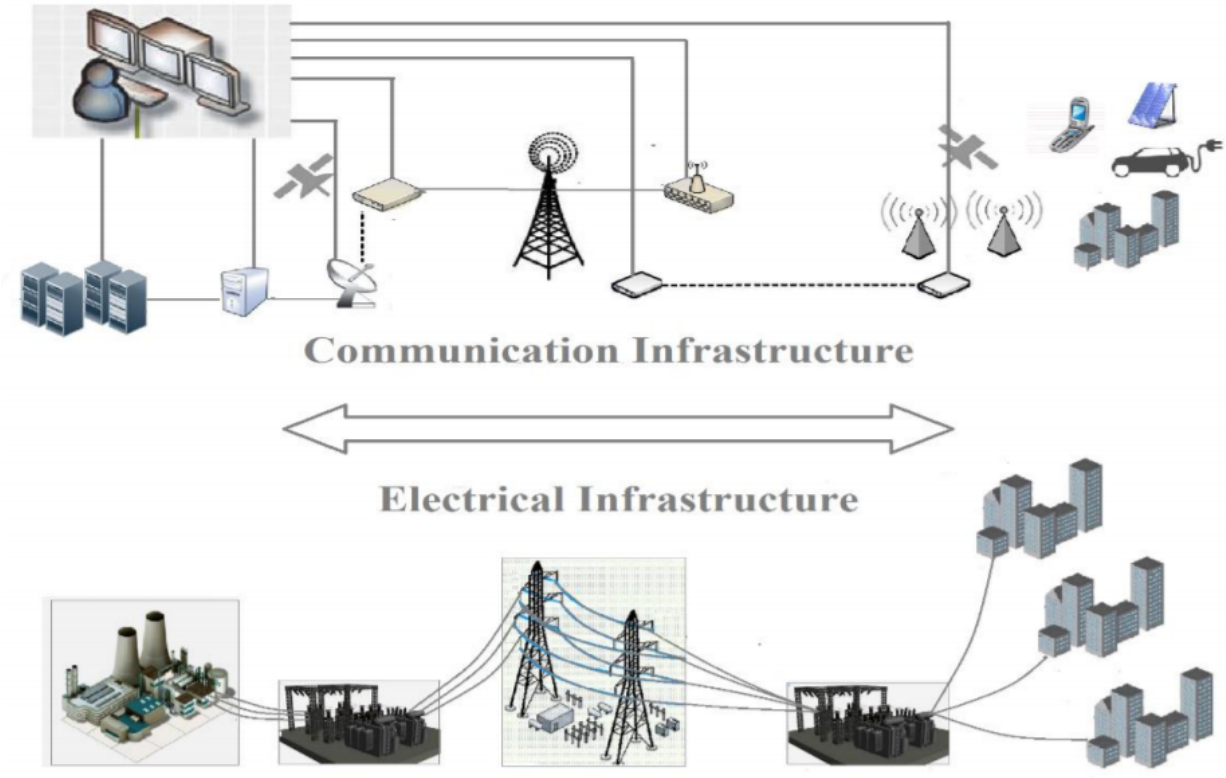

Figure 1.1: Generic power Grid model
[1]

Modern power grids are also adopting various advanced measurement utilities to help in preserving the health of the grid. Phasor Measurement Units (PMUs), an advanced measurement utility used in the power grids, can accurately communicate the magnitude and phase angle of voltage and current of electrical waves by time stamping the readings using signals provided by a Global Positioning System (GPS) receiver. With a primary objective of real-time monitoring and control, grids owners adopt several additional components to support PMUs including aggregators and communication devices.

1.1 WAMS and SCADA

A Supervisory Control and Data Acquisition (SCADA) system is responsible for taking a high amount of measurements at a large number of locations in the grid. The measurements are taken continuously and used for operation and control of the power grids. SCADA systems primarily measures aspects such as voltage magnitude, active, reactive, or injection flows which have been utilized in the power system for a long time [2]. A Wide Area Measurement Systems (WAMS) monitors health of the power grid using new data acquisition technologies like PMUs. However, a SCADA system has some drawbacks when compared to Wide Area Measurement Systems (WAMS). Some of them include: not being fully time synchronized, low transmission rate, and uncoordinated acquisitions. Typically a SCADA system uses steady-state voltage and power flow measurements, through which operators can mathematically observe a nonlinear system which describes energy flow in each transmission line. However, steady-state power flow cannot observe dynamic characteristics of the system response. The data transmission is polled on a frequency ranging from 0.1 to 0.25 Hz in SCADA systems due to limited communication when first built, resulting in slow data updates. Due to SCADA's low polling rate, contingency analysis to perform power system security analysis is done at much longer intervals than what is potentially available using WAMS [1].

WAMS can provide a continuous time-dependent snapshot of the whole grid. Due to its

synchronization, potentially no state estimation is required when using WAMS and phasors of the voltages can be examined dynamically. Due to its requirement of high resolution synchronized readings, the communication infrastructure required in a WAMS is different from the infrastructure for a traditional SCADA system. The data polling rate required in WAMS is also much higher when compared to a traditional SCADA [3]. In a WAMS, a PMU is considered as the main technology and is of the highest importance [1]. While PMUs work at lower level in the hierarchy in a WAMS, additional tools are required such as Phasor Data Concentrators (PDCs) and super PDCs which work at a higher level in the hierarchy. As many organizations in the power industry believe PMUs to be a developing technology, they implement a hybrid SCADA system integrated with a WAMS system, where WAMS acts as a backup for decision making. Though PMU is a promising technology, the cost outweigh the benefits based on current consensus since the full SCADA build-out already exists. An integrated WAMS and SCADA is shown in Figure 1.2:

1.1.1 Phasor Measurement Units and State Estimation

State estimation is used in system monitoring to estimate the power grid operating state through the analysis of meter measurement data and power system models [5]. It correlates meter measurements and estimates the unknown state variables, usually voltage phase angles to observe the power grid and to perform contingency analysis to improve reliability.

As state estimation determines both current and voltage phasors, the problems associated with nonlinearity regarding measurement and state variables can be resolved in a simple and quick way. Based on the output from state estimation, operators at control centers perform contingency analysis. State estimation is crucial because its result will lead to actions related to potential operation problems in the grid. For example, if lines are tripped due to faults, the results from the state estimation are used by the operator to maintain reliable operation by changing the set points of generators.

In addition, state estimation routines are equipped with bad data detection algorithms

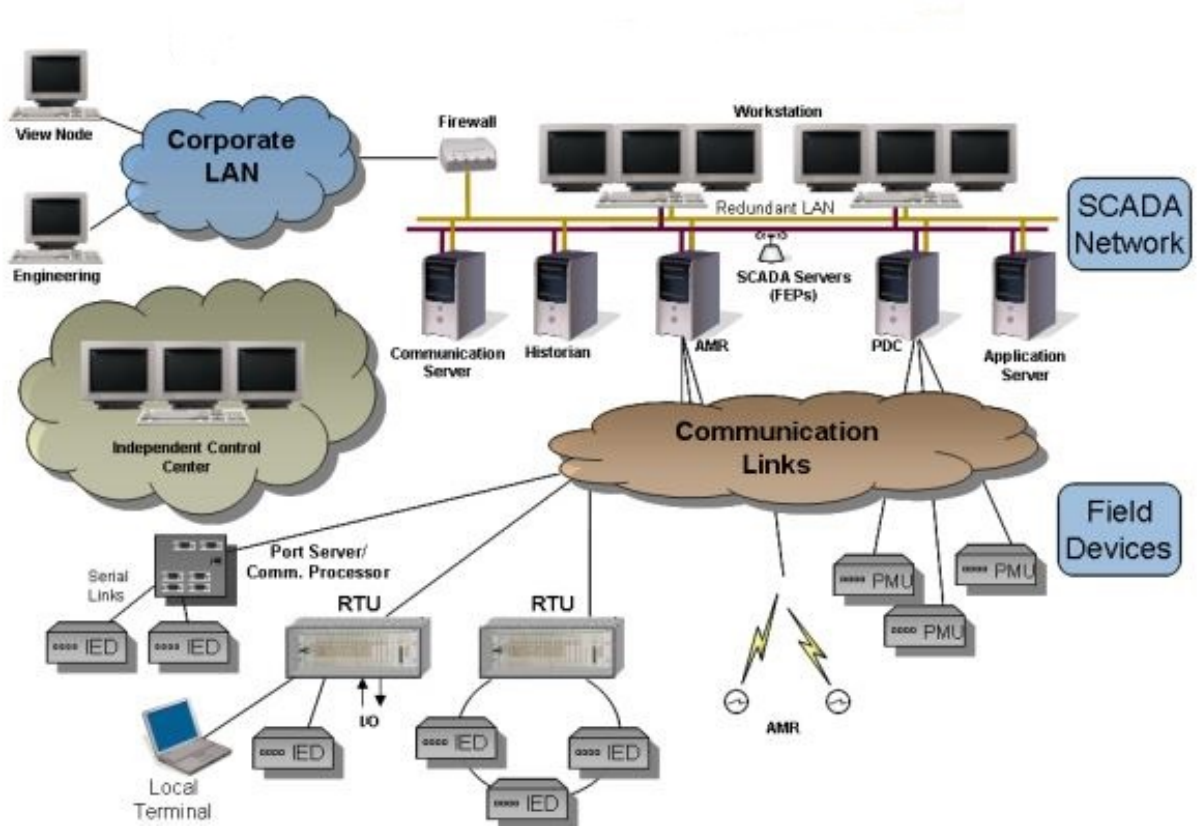

Figure 1.2: Integrated system consisting WAMS and SCADA [4]

that helps state estimation by identifying corrupted values from faulty meters. Genuine meter values help state estimation to produce a close estimate of unknown power grid state variables. However, when the measurements that are fed to the state estimation are not close to their actual value, the deviation in the state estimation result in less effective operation and could impact reliability. Hence, power grid adopts bad data detection algorithms to reduce weighting for faulty measurements. Most Bad data detection algorithms calculate a measurement residual of the readings and checks whether the residual value lies with in the allowed threshold. If the calculated measurement residual is not in the threshold, then respective reading is considered faulty and given reduced weight. However, if a faulty measurement's residual lies in the threshold boundary then it is considered a legitimate measurement. As a result, attackers who possess sensitive information about power grid including variable values used to calculate measurement residual and the allowed threshold

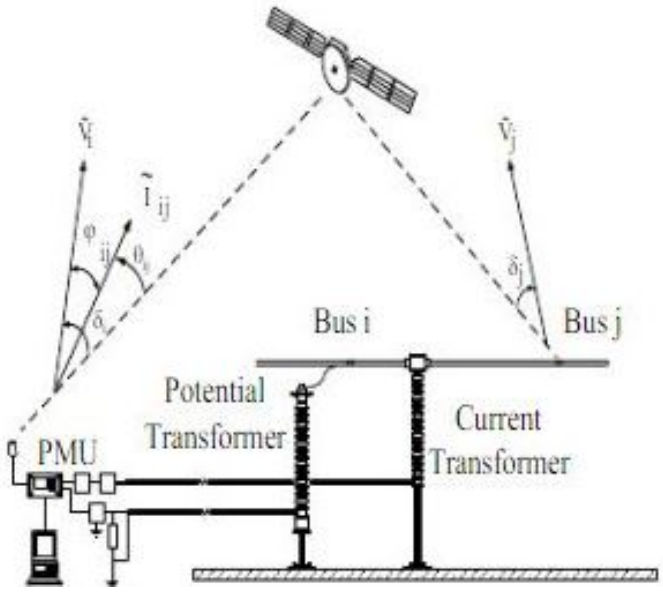

Figure 1.3: PMU diagram
[3]

can inject values that can bypass the bad data detection algorithm.

PMUs and state estimation processes use different approaches for determining phasors of voltage required for evaluating the power system. It is believed that integrating WAMS to traditional power grids by adding PMUs will improve accuracy and precision in determining the state of power grids [2]. As both state estimation and PMUs determine accurate phase angles, one system can act as a backup to the other. However, the phasor angle differences provided by the PMUs are potentially updated every cycle and the ones provided by state estimation are updated over tens of cycles. With the help of clock signals received by GPS receivers, the synchronization provided by the PMUs offer better time precision than a traditional SCADA system with state estimation.

1.1.2 Phasor Data Concentrator and Super PDC

Information gathered from PMUs is taken as a time-stamped input stream for correlation and interpretation by a PDC. Generally, PDCs act at a higher level in a hierarchy than PMUs to collect data from multiple PMUs and often take the information from the fellow PDCs

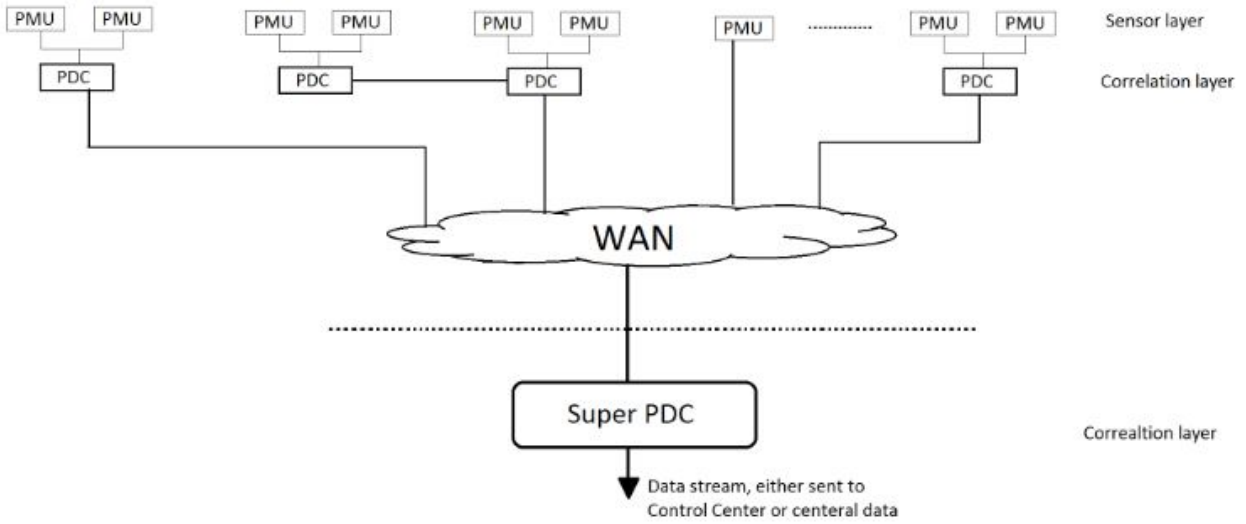

Figure 1.4: A sample hierarchy of a WAMS

which are present in the same hierarchy. PDCs are also responsible for the evaluation of quality and accuracy of the received values. In WAMS, streams from PDCs are either sent to a higher level of the hierarchy or to the control center for power system analysis.

A super PDC has similar functionality to a regular PDC. The Super PDC performs operations at a higher level in the hierarchy than regular PDCs. They are responsible for collecting the data from remote PDCs and PMUs prior to data visualization. Super PDCs are connected to a central database so that correlated data can be stored and accessed easily. As a result, a super PDC does not require a significant amount of storage space to collect data and can be polled at sampling rates of 30, 60 or 120 samples per second.

1.2 Phasor Measurement Units

Advanced and intelligent units like PMUs enable performance of many precise operations. In this research, PMUs and other WAMS entities are studied from a security point of view, exploring the vulnerabilities and exploits associated with using them. In this section, a brief introduction to PMUs and their importance is discussed, along with communication protocols used in WAMS and their respective security aspects.

1.2.1 Importance of PMU in Power Grids

A WAMS based on PMUs can potentially help a power grid by: [1]:

- Monitoring the system in a delay-sensitive high data rate manner, which leads to a rapid response of the system in irregular and anomalous situations.
- More accurate state estimation allowing real-time stability monitoring, improving post-disturbance assessment ability.
- Dynamic system monitoring of the power grid to reduce congestion.
- Increased reliability and robustness in distorted situations.
- Restoration of the power system following a blackout.
- Real-time overload and voltage stability monitoring.

To enable all the above actions, measurements from PMUs are weighted based on location, assigning more importance to data from some PMUs. A weighted implementation for PMUs can potentially enhance the reliability, as operators can give importance to weighted PMUs and deviations from a light weighted PMU can be discarded. However, performing weighted implementation requires dealing with several challenges related to correlation in final PDCs, the correctness of metering devices, different accuracies of available PMUs, manufacturer's class of errors [6]. Normalization of PMU measurements helps improve security aspects related to packet injection attacks, so it is mostly recommended even though it leads to additional computational complexity [6].

1.2.2 Motivation for PMUs

Imbalance of power consumption compared to generation and transmission capacity causes frequency instability in the grid. One of the primary motivations for installing initial PMU was overcoming voltage instability in the power grid [1].

Power grids in North America have great level of complexity, includes over 200,000 miles of power lines and are controlled by approximately 500 entities to maintain stability [1]. Cooperating entities coordinate with each other to maintain the desired ratio between the power supply and load. Goodney et al. [7] indicated that the current system lacks real-time exchange of information regarding power grid status among these entities. Several attempts have been made in the past to fill the gap by providing real-time measurement, and Wells et al. [8] studied measurements from a set of PMUs that were installed in 2004 for data during a blackout that occurred June 15, 2005. It was found out that frequency and phase angle difference between Little Rock, AK and Houston, TX indicated the cascading of the instability in the power grid and shpwed the onset of blackout. Phase difference was steady until 27 minutes before the blackout where a change in angle difference occurred that kept on increasing from 35 degrees to 120 degrees between the two buses. By going through publicly available graphs, authors determined that a reclose failure on one of the lines caused an instant increase in impedance, leading to the increase of phase differences between the two cities/buses. Major blackouts cause huge economic losses and also waste human hours. For example, a blackout that occurred in the northeastern United States and southern Canada in 2003 caused a loss in the billions of dollars and considered one of the worst blackout [7].

Hence, investigations towards a possibility of using PMU technology in North American power grid has been made several times by United States Department of Energy (DOE) following blackouts. This investigation following 2003 blackout led to the information of the North America Synchrophasor Initiative (NASPI), and in its collaboration with North America Electric Reliability Corporation (NERC). NASPI has been operating for over a decade with a primary aim to provide complete coverage of the transmission grid [7].

As noted earlier, the PMU is the core unit for the functionality of WAMS and is responsible for basic measurements essential for monitoring the health of the power grid. Ideally, PMUs are placed in the power grid based on the observability of the grid, and each of these PMUs are fed with a time synchronization from GPS receivers. Synchronization in all the

measured PMUs values is done based on the time stamp that PMU attaches to a reading. This accurate time-stamped and synchronized signal is correlated up the hierarchies through PDCs as shown in Figure 1.4, and the stream is sent to a control center or a data server for further contingency analysis. As a result, it is important to maintain a high Quality of Service (QoS) by the PMU as any sufficient delay in information can lead to problems in correlation. Khan et al. [9] stated that broad utilization of the PMUs are currently restricted by the lack of proper communication infrastructure in power grids, but not by the QoS a PMU can potentially offer. Due to rise in intermittent sources like solar and wind energy along with decommission of coal plants, accurate wide area snapshots of the power grid are recommended for maintaining the reliability of the grid. The Smart Grid Investment Grant (SGIG) program recommended using PMUs for residential and commercial demand units which operate at lower voltage [8].

The concept of PMU as an intelligent electronic device (IED), was first developed by Phadke and Thorp in 1988 at the Virginia Tech Power System Research Laboratory [3]. The first PMU was developed with an aim to continuously measure analog voltage in the substation with a sampling rate of 20, 30, or 60 samples per second. Along with voltage, current and frequency of the voltage are added with a time stamp provided by a GPS receiver. These time-stamped measurements were later called synchrophasors, thus obtaining the name synchrophasors technology [10].

The Digital Signal Processors (DSP) in PMUs process the 50/60 Hz AC signal after analog to digital conversation at configured sampling rates. Along with DSP unit, PMUs also receivers an input unit for GPS receiver to achieve synchronized sampling rate of 1 millisecond accuracy. A block diagram of a PMU is illustrated in Figure 1.5.

1.3 Synchrophasor Network

In a simple synchrophasor network, one PMU and one PDC communicate with each other, where the PMU takes the readings and the PDC correlates them. In a practical system, a

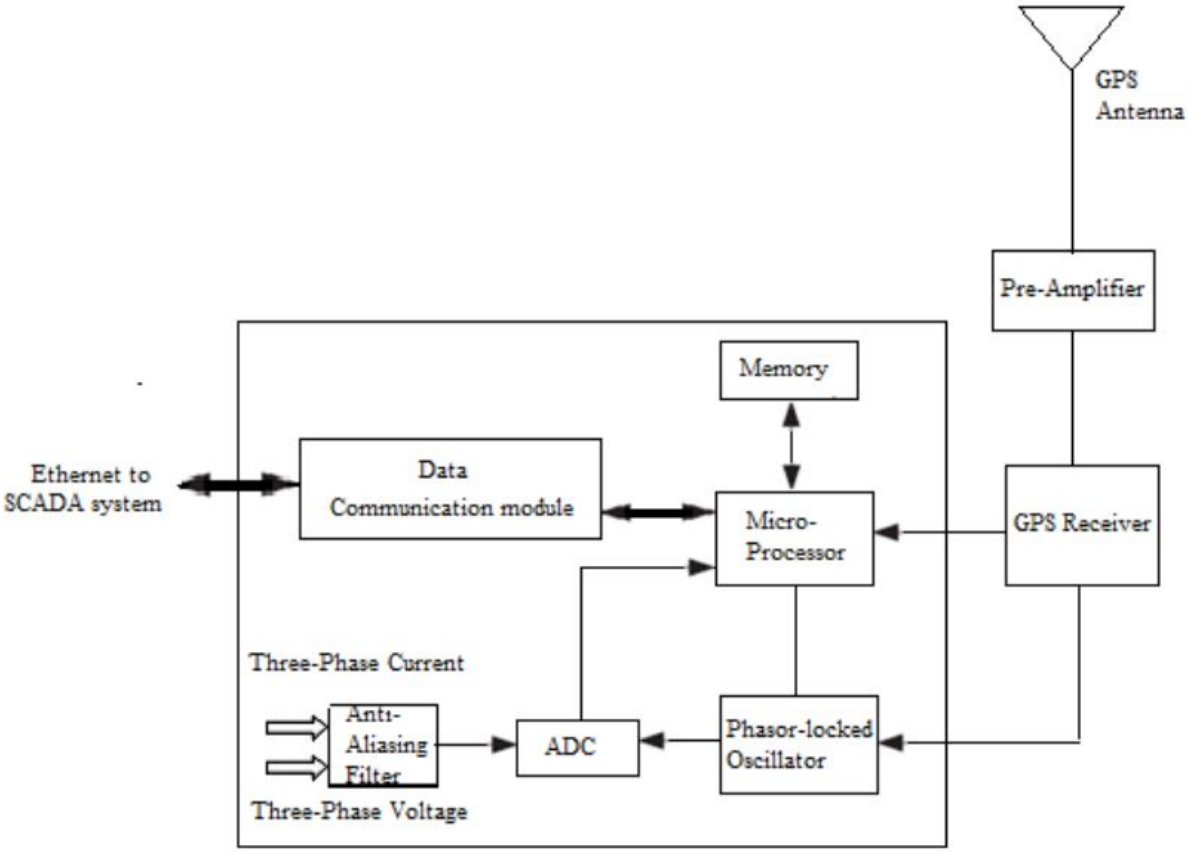

Figure 1.5: A sample block diagram of PMU
[11]

PDC communicates with multiple PMUs located in nearby substations and aggregate data into a single stream based on the time stamps. To evaluate the correctness of data, PDCs check a Cyclic Redundancy Code (CRC) that is appended by PMUs and stores them in an internal memory. After evaluating the correctness of data, PDC correlates the measurement from different PMUs based on the UTC time stamp [3]. The data stream from PDCs is directed to upper levels of the hierarchy, and/or the output is processed by using software such as a Real Time Dynamics Monitoring System (RTDMS) [12]. A RTDMS allows operators to visualize data and show values of voltage, frequency, current, MW, and MVAR of the data stream measurements directly as their personal computers. Higher hierarchal level devices like super PDCs are responsible for collecting information from other PDCs and provide an interconnected wide area snapshot of the grid. Figure 1.6 illustrates the architecture and

communication model in a WAMS.

1.3.1 PDC and Super PDC substations

A PDC will most likely be located in a substation and communicates with PMUs with a shared Ethernet. After correlating the data, PDCs apply pre-configured control decisions to the data and stream the data to the higher nodes. In a power grid with a large number of PMUs, communication associated with the PDC may become a bottleneck if the communication system is not designed effectively [1].

A super PDC also called a central PDC, analyzes and stores information that it receives from the lower layers. Substations that house super PDCs may also be responsible for assessing operational patterns for their respective region of power grid. Accessing super PDCs requires higher levels of authentication when compared to units in the lower layers. Some super PDCs are also configured such that they can initiate time critical commands associated with controllers and other IEDs.

1.4 Communication Infrastructure in WAMS

In general, WAMS uses several means of communication-based on connection requirements. Some of them are described below [4].

Virtual Private Networks (VPNs):

A Virtual Private Network (VPN) allows secure communication between nodes in an unsecured public environment. Secure Socket Layer (SSL) and Internet Protocol Security (IPsec) are the two most used security protocol suites used in VPNs, and they are responsible for the key establishment, encryption of data and authentication while transmitting WAMS data. Since a VPN operates at layer 3 of the OSI model to secure data it encrypts addresses and network data, attackrs in WAMS could be able to inject incorrect data and gain access to unauthorized network data before it is encrypted [1].

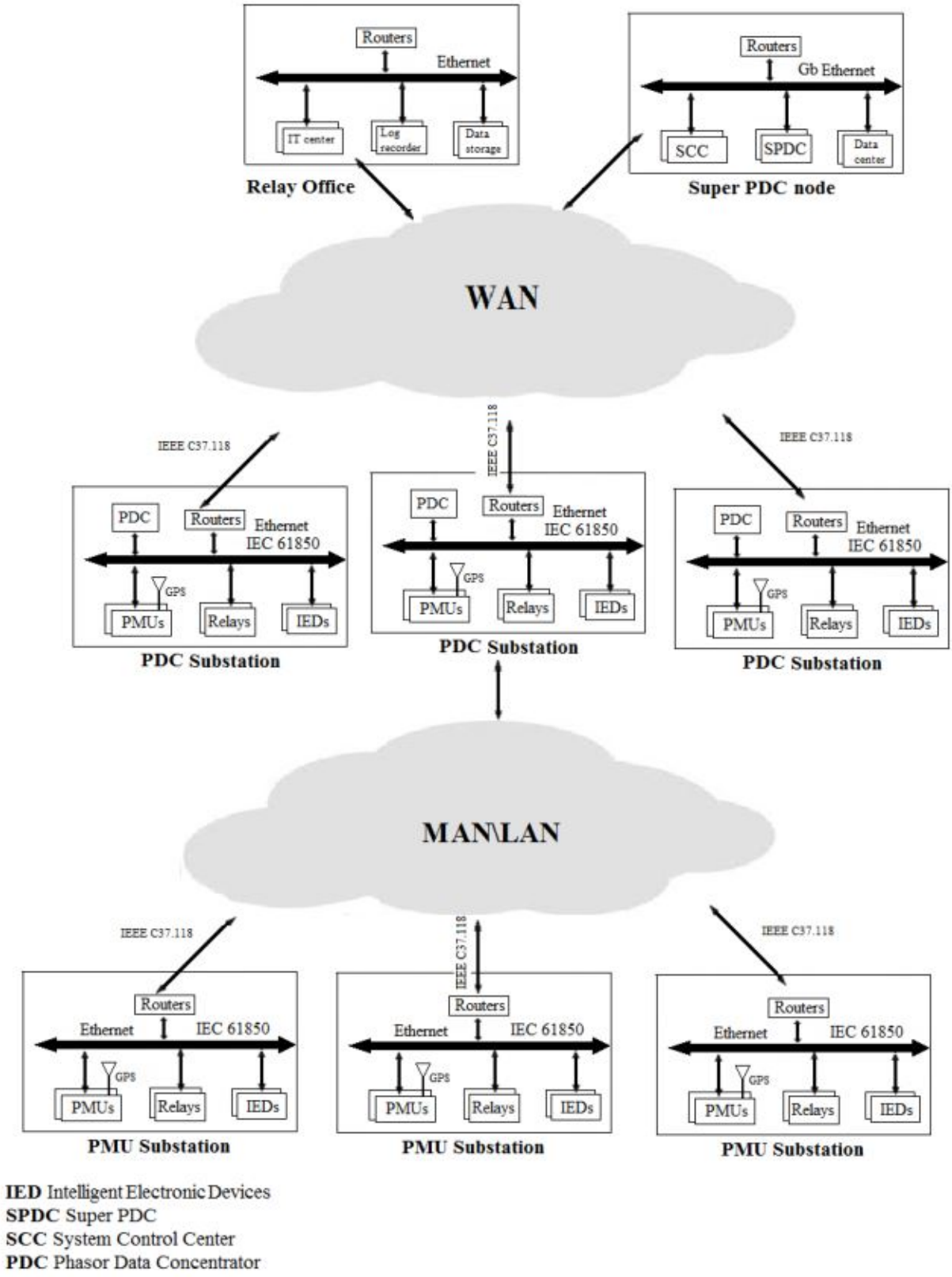

Figure 1.6: A sample hierarchy model in WAMS
[3]

Analog/Digital Microwave:

In rare case, WAMS uses an analog microwave connection to maintain communication between PMU and PDC. However, analog microwave connection is not preferred in communication between PDCs and Super PDCs due to low bandwidth relative to the volume of traffic. Similar to wireless communication attacks, analog microwave connection is susceptible to attacks like traffic analysis, jamming, and signal monitoring and recording.

Serial Communication:

Similar to SCADA networks [4], older substations of WAMS can use serial communication in most of the connections in a substation. Using a modem, it can transmit data at high speeds with at least 30 frames per second. However, these modems are susceptible to several attacks associated with command sequences that can reveal crucial information.

The communication mode depends on which layers the communication nodes are using. Communication systems in a substation can be divided into 3 types based on their primary functionality, for communication within the substation or with other substation:

Wide-Area Fiber Optic Networks:

Communication in top layers of synchrophasor networks like PDCs to other PDCs, and PDCs to Super PDCs require high bandwidth. To handle this, WAMS uses fiber-optic networks to support the transmission of required volumes of data.

High-Performance Regional Networks:

Generally, network utilities that are used for connecting distributed PMUs to one PDCs are designed exclusively for power systems. Operators at a PDC substation can take decisions to obtain local grid stability based on the readings from that are transmitted from the local grid PMUs to the PDC.

Intra-Substation Local Area Networks (LANS):

For communication within the substation, IEC 61850 [13] is begining used, which have an implementation constraint to have a response time under 4 millisecond. As a result, using large transmission bandwidth Ethernet is started to become more common in substations

with PMUS to guarantee the 4 millisecond response time.

1.5 IEEE C37.118 Standard

There are several protocols that support communication between PMUs and correlation units. IEEE C37.118-2005 [14] is a synchrophasor protocol that is designed specifically to allow communication between two synchrophasor network units. It is the successor of IEEE 1344-1995 [1] which was approved in 1995. IEEE C37.118 improves upon the drawbacks of IEEE 1344 such as response time, phasor measuring process and accuracy of the measurements, and by also adding information about software, hardware, and a security specification of the protocol. Each measurement is attached with a time stamp of number of seconds from Unix epoch (January 1st, 1970) for synchronization. A revision of the standard in 2006 [14] added features like combining phasor measurements from several PMUs, which made it compatible with other substation communication standards, and a sample modification to the fraction of second as used in other substation protocols like IEC 61850. Later in 2011, IEEE C37.118 was divided into 2 parts because of the classification of PMUs to measurement and protection categories:

- IEEE C37.118-1, which deals with phasor estimation
- IEEE C37.118-2, a communication protocol

However, IEEE C37.118 doesn't include security features supporting confidentiality, integrity or availability. As a result, it is vulnerable to several cyber-attacks where one can inject or disrupt the data communication in PMUs or correlation units.

The primary aim of the IEEE C37.118 protocol is to define a frame format for transmitting data to and from the PMUs. The frame format in IEEE 37.118 can be one of 4 types based on requirement: Configuration frame, Command frame, Data frame, and Header frame. Generally, the configuration frame, the command frame and the data frame messages are in binary, and header packets are in ASCII. Out of all of the frame formats in IEEE C37.118,

Table 1.1: Frame format of Data Block in IEEE C37.118

Field	**Size (Bytes)**	**Comments**
SYNC	2	Synchronization byte
FRAME SIZE	2	Number of bytes in frame
ID CODE	2	PMU ID
SOC	4	Second of Century time stamp
FRACSEC	4	Time fraction and quality flag
STAT	2	Bitmapped Flag
PHASORS	4 * 4 (signed integer)	No. of Phasors
FREQ	2 (signed integer)	Frequency
DFREQ	2 (signed integer)	Rate of change of frequency
ANALOG	2 * 4 (32-bit,Floating point)	Analog Data
DIGITAL	1 * 2	1 Digital data (16 bit field)
CHK	2	Cyclic Redundancy Checks

the data frame is the most commonly transmitted frame as it consists of measured values from a PMU [15]. The phasor vector, frequency, rate of change of frequency, signed three phase voltage, current, real and active power, individual phase RMS values, and detection of unbalanced conditions are some of the values including the data message. A machine-readable message and configuration are responsible for calibration [1]. The Header packet is 16 bytes of ASCII characters, and it is the only human readable packet among those in IEEE C37.118. In general, the frequency of transmission of the header and command messages are comparatively low. The payload format (Data format) of the packets is stated in Table 1.1 [9].

The available reporting frequencies of IEEE C37.118 are 10 Hz and 25 Hz for the 50 Hz based power system and 10, 12, 15, 20, 30 Hz for the 60 Hz based power system [4]. The Delay in the communication is set to the inverse of the reporting frequency so that the current measurement is received before the next one is ready for transmission.

1.6 IEC 61850 and IEC 62351

The IEC 61850 set of communication [16] standards were introduced by IEC Technical Committee 57 (TC 57). To obtain a response time of under 4 milliseconds, it uses a TCP/IP

Table 1.2: Sublayers of IEC 61850

Protocol Version	**Primary Intra-Substation Usage**
IEC 61850-10	Conformance testing
IEC 61850-8-x and IEC 61850-9-x	Specific communication service mapping
IEC 61850-7-4	Compatible logic node classes and data classes
IEC 61850-7-3	Common data classes
IEC 61850-7-2	Abstract communication service interface
IEC 61850-7-1	Principles and models
IEC 61850-6	Communication language configuration of IEDs in substation
IEC 61850-5	Communication requirements of function and devices

model or Ethernet sharing methods. It maps the data model into a group of protocols such as the Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Event (GOOSE), and Sampled Measured Values (SMV) Table 1.2 lists the sublayers of IEC 61850 [17]. IEC 61850 utilizes UDP, a non-reliable protocol for time synchronization and TCP/IP for MMS communication.

The primary aim of developing IEC 62351 was to secure several communication protocols like IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970. In particular to IEC 61850, IEC 62351 has primarily enhanced the security in MMS and GOOSE. For MMS, peer authentication and TLS are enforced, and $\{TLS\_DH\_RSA\_AES\_128\_SHA2\}$ and $\{TLS\_DH\_DSS\_AES\_256\_SHA1\}$ are the minimum suggested cipher suits.

1.7 NERC Guidelines

In 2002, the North American Electric Reliability Corporation (NERC) issued the first version of a guideline to protect the power infrastructure from cyber-attacks. These

guidelines have been evolving since then based on the evolving threats and evolving power grid infrastructure. The NERC guidelines are developed to perform the following [18]:

- Assess sector vulnerabilities,
- Develop a plan to reduce electric system vulnerabilities,
- Propose a system for identifying and averting attacks,
- Develop a plan to alert electricity sector participants and appropriate government agencies that an attack is imminent or in progress, and
- Assist in reconstituting minimum essential electric system capabilities in the aftermath of an attack

The NERC Critical Infrastructure Protection (CIP) guideline covers various aspects of the power grid security ranging from vulnerability and risk assessment to employee screening. Vulnerability and risk assessment should identify all the critical resources in the power grid along with their vulnerabilities. Using the results from the power grid's vulnerability and risk assessment, the power grid operators should consider restricting access to the critical resources to "need to know" individuals [18]. Similarly, the NERC guidelines to threat response capability and emergency management ensures power grid personals are able to respond efficiently to various known and unknown threats to the organization. Guidelines associated with minimizing the interruption to power grid functionality are addressed in continuity and business process standards, and communication standards. Cyber security and physical security guidelines help in mitigating risk from inside and outside threats sources, while guidelines to employee screening helps in combating threats from insiders.

The vulnerability and risk assessment guideline stated by the NERC outlines the risk analytical approach into 4 stages [18]:

- Identification of assets and loss impacts,

- Identification and analysis of vulnerabilities,
- Assessment of risk and the determination of priorities for the protection of critical assets, and
- Identification of countermeasures, their costs, and trade-offs.

1.8 Objectives of This Thesis

This research concentrates on identification and analysis of vulnerabilities by identifying potential vulnerabilities based on various threat sources. Along with it, degree of risk associated with each threat sources is estimated. Threats are identified from a cyber security point of view and threats associated with predisposing conditions such as being in a flood-prone area are addressed but are not discussed in detail. The primary objective of this thesis is to provide an insight regarding various threat sources in a power grid, and to do so the identified threats as classified into group along with their respective impacts levels. For deriving the taxonomy, an abstract WAMS model with PMUs, PDCs, and super PDCs is considered. Impact-oriented approach and Threat-oriented approach are used to identify the threat sources and a qualitative scale is derived to express respective impact levels.

In chapter 2, a review of literature in cyber-attacks that can potentially affect the operation of the power grid is discussed. In chapter 3 various methodologies that are used to carry risk assessment are stated. In chapter 4, methodologies from chapter 3 are adopted to present a taxonomy of information security threats, and summary and future work is addressed in chapter 5.

CHAPTER 2

Review of Literature on Security in WAMS

Preserving confidentiality, integrity, and availability in WAMS through secure real-time data measurement and transmission is very important in electrical power grids. For this reason, several efforts have been made to identify vulnerabilities and to proposing mitigation techniques that have led to the development of several security protocols and measures. Though security measures are available, these protocols/measures require additional computation costs and energy for PMUs and other devices, leading to a trade-off between the implementation of resources and security [19]. Consequently, many implementations choose resources over security because of capital cost, deployment schedules, maintenance, etc. As a result, security factors associated with measured data cannot be guaranteed and remain vulnerable to different security threats. The level of sensor node security has been classified into four groups based on its encryption and authentication: non-security service as level zero; single security service (single encryption or authentication) as level one; double security service (single encryption and authentication) as level two; triple security service (double encryption and authentication) as level three. An example of this categorization is the classification of IEC 62351 as level one because of its exclusive use of digital signatures to authenticate. The digital signatures in IEC 62351 also are used for tamper detection and integrity.

Among the Confidentiality, Integrity, and Availability (CIA) triad, availability is crucial in power grids, as lack of availability affects the functionality of the power grid devices, causing problems in obtaining the real-time data and wide area snapshots leading to potential operational problems. Lack of availability in set of measurement devices can also cause inaccuracy in the continuous monitoring data, eventually leading to a contingency in the grid. As a result, backup power sources were suggested for SCADA system in the past by M. Popa and M. Alba [20]. To prevent single point of failure, redundant storage system for data servers that stores systems files and momentary acquisition files were suggested.

When data is corrupted in the control center, accidentally or intentionally, information from redundant storage systems can be used to recover to normal functioning in short order. The authors concentrate on discussions to improve the functionality of PMU-like devices in a cost-efficient manner. In additional to PMUs, they stress the importance of supporting factors like humidity, temperature, and power quality, etc., and importance of supporting devices such as GPS receivers for their role in synchronization through providing time-stamps to PMU. To enhance security against cyber-threats, suggestions like implementation of VPN tunnel and strong authentication methods were discussed [20].

Morris et al. have studied cyber-threats associated with PMUs and PDCs, includes reconnaissance attacks, packet injection attacks, and Denial of Service (DoS) attacks that could affect the function of WAMS [21]. When these attacks are used effectively, they could lead to loss of visibility of power and control system by forcing the target device to go offline. They have also suggested mitigation techniques like using SSL and IPSEC for transmission of measurement data and control center actions.

2.1 Reconnaissance Attack:

A reconnaissance attack is an information gathering attack on systems or communication services by an intruder. It can be performed by anyone who is connected to the network in several ways like introducing trojans, phishing, spam emails, social network analysis, malicious email/link, or using tools like NMAP [22]. The author in [21] used NMAP to learn about the open ports, MODBUS addresses, MODBUS points, IP addresses of PMUs and PDCs by fingerprinting connected systems and by maintaining a remote environment which includes target's operating system and network stack daemons. Authentication is important while communicating with advanced measurement devices used in a power grid. PMUs and PDCs authenticate with each other periodically to prevent data tampering and to support remote access and control. If there are any un-encrypted data transmissions, WiresharkTM [23] can be used to analyze data packets, searching for crucial information.

Authors in [21] took advantage of un-encrypted transmission between PMUs and PDCs, and gained credentials of respective devices. An attacker can also perform eavesdropping on a communication protocol in an unencrypted channel, and analyze network traffic to gather information about PMU location. However, the authors have also mentioned that using protection tools like SSL and IPSEC between firewall at the substation and control center room can prevent all the cyber-threats that were performed in the simulation.

2.2 Packet Injection Attack:

A Man-in-the-middle (MITM) attack is a type of eavesdropping attack that happens when a malicious agent secretly inserts himself into an unauthorized communication channel. Packet-injection attacks are similar to MITM attacks, where an adversary injects sensor data packets or command/request packets between two communicating nodes with a malicious intent, such as causing inaccurate measurements or disrupting PMU's functionality. An advanced measurement device like a PMU can transmit quasi real-time voltage and current phasors based on how it is configured. It can act as a strict transmission node or a transmission receiver node where it takes commands and requests from a control center to send specific data. When a PMU/PDC/IED is configured to receive commands from a control center, an attacker can inject arbitrary supervisory control actions leading to overwriting the operational code, ladder logic and the register setting of the respective device. These attacks can be done on a set of PMUs by injecting arbitrary values as measurements and leading to an inaccurate state estimation which can sabotage operation in the power grid. When a substation is using IEEE C37.118 to communicate with correlation units, MITM attack vectors like Ettercap can be used to inject packets between PMUs and a PDC with correct frame formats. In addition to IEEE C37.118, some PMUs still provide compatibility with DNP3 and MODBUS communication interfaces for remote monitoring and control without any cryptographic signatures. These communications are highly vulnerable to many communication attacks, especially MITM attacks. Suggestions to mitigate these attacks are

discussed by Morris et al. [21] by including SSL and IPSEC, preserving confidentiality and integrity. IEC 61850 has been used in some substations for communication between PMUs, protection relays, and other IEDs. Due to the single level security mechanisms like included cryptographic signatures, this protocol reduces the chances of being attacked by a packet-injection attacks. However, IEC 61850 still has vulnerabilities which can be exploited [1]. Another way to counter packet injection attacks is to include a trust metric attribute to PMUs and having a modified algorithm based state estimation [24]. Using this method, PDCs which communicate with PMUs assign a dynamic trust metric factor to each PMU based on the legitimateness of their reading. The accuracy of the PMU reading can be obtained based on readings from neighboring PMUs. By following this approach, faults indicated by a lighter weighted PMU can be taken less seriously than results indicated by more heavily weighted one. Such a system would allow operators to calculate distributed state estimation and central state estimation, which increases the reliability of the grid. For initial short periods, the trust factor associated with PMUs would be fluctuating, leading to un-stabilized model. However, the stability of such system would increase as the time goes on by utilizing stored data.

2.3 Denial of Service:

Denial of Service (DoS) attacks involve attempts to cause disruption in the normal functioning of a system. In a typical DoS attack, the attacker will try to choke the communication system by introducing numerous random packets in the system, with the aim to cause a non-responsive hardware and software in control systems. DoS attacks are performed to disrupt functions like remote terminal access and master terminal access [21]. In WAMS, a DoS attack causes loss of visibility by forcing target devices to go offline. When done for longer periods, it breaks the control loop and disables the automated event detection methods. Morris et al. [21] suggested using a MU Dynamic MU-4000 Analyzer [25] which can detect several DoS attacks to which PMUs and PDCs are vulnerable. The MU Dynamic

MU-4000 can also be used to analyze the network for un-authorized nodes and to identify man-in-the-middle attacks. The authors in [21] performed DoS attack in their experiment in a simulated environment by fuzzing a known protocol mutation where numerous network packets are generated with random values in their respective packet field. In real-time, an attacker would try to take advantage of all the possible protocols that a PMU/PDC supports and will fuzz all options to cause disruptions in its functionality prior to being discovered. Effects of this attack depend on the target devices, and the number of protocols they support. Advanced measurement utilities support HTTP, ICMP, TCP, UDP, IP, ARP, MODBUS, DNP3 and IEEE C37.118. As a result, performing a fuzzing protocol mutation attack could cause crashing of individual services, unintended software resetting, crashing applications in the device and creating congestion for request commands. Hence, the author concluded that it is important to check a PMU's performance against fuzzing attacks before implementing it in the field. The experiment conducted by the author, also indicates that the PMUs and PDCs tested either hung or experienced unintentional reset in the presence of high volumes of traffic. A typical mitigation for such high volume traffic attacks would be setting acceptable traffic rates and implementing gatekeeper algorithms. Traffic rates can also be controlled dynamically by the operator whenever a contingency occurs. The authors in [21] have also suggested closing all the ports that do not carry information or have no functionality, and configuring connections between PMUs and PDCs. Accessing the network for injecting large amounts of packets is difficult in the real-time power grid. Power grid operators use their private networks for communication and generally have multiple authentication levels before granting access to the network.

Denial of service attacks can also be tackled by maintaining redundancy [26] for critical measurement devices. However, maintaining redundancies increases network complexity and impact network scalability. Redundancies also need to deal with high-level resource utilization on latencies. The wireless version of DoS attacks are known as PHY attacks [27]. A PHY attack is a malicious attempt to disrupt communication in a wireless medium. As

wireless signals cannot be protected physically from intrusion in larger areas, any person who is in the signal range can perform PHY attacks. While wireless communication is rare in power transmission application, it sees some use the distribution systems. Lee, Gerla, and Oh [27] have classified PHY attacks into categories: injecting, jamming, eavesdropping, and restricting access.

2.4 Data Integrity Attack

Data Integrity attacks use a vulnerability in the power grid to try to stay undetected [28]. In this attack, the attacker changes the measurements from power meters that are compromised in advance. The modified values remain close to those seen in changes in electrical loads and could bypass bad-data detection algorithms in state estimation, so potentially this attack is undetected. This attack can either be done with an intent of self-profit or with a malicious intent to affect the grid. Either way, data integrity attacks will cause errors in estimating the state and in contingency analysis. Giani et al. [28] have also discussed how readings from legitimate PMUs are needed to mitigate the compromised meter readings. In their experiment, the known and secure PMUs were identified first, and their transmission was secured using the North America Synchro-Phasor Initiative Network (NASPInet) [29] architecture for reliability. It was found that to neutralize p compromised PMUs, a power grid would need p+1 secure PMUs at chosen buses.

2.5 Traffic Analysis Attacks

In a traffic analysis attack, which is also known as a traffic correlation attack, the attackers would investigate and evaluate a network looking for features like time, volume, etc. [30]. Similar to reconnaissance attack, a traffic analysis attack is used to gather information that will help to craft a much more malicious attack on the PMUs. By analyzing the traffic between PMUs and PDCs, attackers can find the presence of encryption by studying the time

taken to respond by a node. Similarly, rough information about the number of packets can be realized by dividing time into fixed-size frames between two ends. Due to the importance of synchronization of data in WAMS, delays will be minimized. This property of WAMS helps attackers to have reliable traffic analysis attack. In unencrypted networks, traffic analysis attacks can also lead to gathering information about PMU locations. Authors have suggested mixing up measurements while performing correlation in the higher level of the hierarchy and dropping data from selective PMUs can help to mitigate locating PMU through traffic analysis. Similarly, concatenating PMUs data into random size contiguous measurements will mitigate network traffic correlation analysis. Light weight encryption techniques can also be used to destroy packet content correlations.

2.6 Time Synchronization Attacks

Time synchronization attacks concentrate on disrupting the synchronization of the system by disrupting information for the timestamps. The whole functionality of WAMS depends on synchronization. Accurate timing information helps WAMS with fault detection and event location estimation in the power grid. Any disruption in timing information will lead to problems with synchronization and cause contingencies in the system. The importance of synchronization and impacts of time synchronization attacks in WAMS has been studied by Zhang et al. [6]. PMUs attach each measurement with accurate time stamps for synchronization between the measurements and between devices at the data concentrator. This time stamp is provided by a GPS receiver which lies close to the PMU. Time synchronization attacks in WAMS can be performed by GPS spoofing, GPS blocking and GPS jamming. In GPS spoofing, the attacker forges time signals into PMU communication. Several research articles have simulated GPS spoofing attacks. Goodin [31] and Jafarnia-Jahromi [32] performed practical ones. The attackers just have to move around Time Synchronized Measuring Devices (TSMDs) and disrupt their communication to perform time synchronization attacks. To counter GPS spoofing, use smoothing filters is suggested [6]. While GPS spoof-

ing attacks aim to inject false signals, GPS jamming attacks try to break the connection between TSMDs and PMUs. GPS jamming attacks are not as effective as GPS spoofing, as the time signals provided by the TSMD are primarily used to reduce clock drifts in PMU. However, when done for longer periods, GPS jamming attacks can cause effective errors. If a PMU doesn't receive any signals related to a time stamp, the corrections to PMU's clock drift cannot be done. Hence, for longer periods data cannot be synchronized.

In addition to GPS spoofing and GPS jamming, GPS blocking is also a time synchronization attack that aims to disrupt signals to GPS receiver. While performing a GPS blocking attack, the attacker intends to cause a disturbance in the signals that are to be received by the GPS antenna. Hence, it requires the attacker to be close to the GPS receiver antenna. While GPS spoofing attack concentrates on changing data from GPS receiver, a replay attack [33] aims to insert delays in the communication signal from the satellite. However, at any given point of time, GPS receiver can communicate with a minimum of four satellites. Inserting delay in a satellite signal will be noticed by the GPS receiver, and it will notify the operators about the attacks. When performing replay attacks in real-time, the attacker takes additional measurements to avoid detection. Such attacks with measurements have already been crafted in the past [34]. Most of the typical time synchronization attacks can be mitigated by installing additional TSMD devices in the substation or installing additional PMU ports like a management port [4].

2.7 Side Channel Attacks

Authentication is an important property to preserve in a power grid, as weak authentication mechanisms can lead to undesired injection in PMU measurements. The authentication property is primarily targeted by side channel attacks (SCA). HMAC (hash-based message authentication code) is the most often suggested authentication algorithm used in the power grid layout with PMU measurements [35]. In general, side channel attacks or physical attacks have two phases, 1) an interaction phase where the attacker exploits the physical characteris-

tics of the system, and 2) an exploitation phase, where the obtained values in the interaction phase are correlated to gain secret information. The exploitation phase is based on two methods: a simple side channel attack and a differential side channel attack. In a simple side channel attack, the key related information is gained by tracing the leakages. But in practice, there will be lots of noise interrupting the simple side-channel attacks. Therefore, the attack applies many statistical methods to eliminate the noise and obtain the information, and these type of attacks are called differential side channel attacks (DSCA) [36].

2.7.1 Timing Attacks

In a timing attack, the attacker tracks the execution time taken by the cryptographic device to reveal secret information about the key. The attacker makes the device process a bunch of messages to exploit the corresponding time. For IEC 62351 protocol, HMAC-SHA1 is the suggested algorithm for authentication. The vulnerability of the HMAC-SHA1 algorithm against a timing side-channel attacks has been investigated in the past [1] [37].

An attacker can retrieve some information about the stored key and hamming weight used in the HMAC-SHA1 through timing side channel attacks. As any other SCA, timing attacks also have two phases:

Interaction Phase:

In this phase, the execution time of the algorithm will be exploited. A set of 48 samples, containing 48 different values as input measurements and their respective assumed keys are assumed. Each sample will have a different data length, data hamming weight, key length, and key hamming weight. As IEC 62351 does not include any encryption, the attacker can access each pair of samples and their corresponding times.

Exploitation Phase:

In this phase, statistical methods (DSCA) are applied to obtain the correlation between the information obtained in the above phase and secret information. Two different models of regression, namely negative binomial regression and linear regression, are run in IBM SPSS

statistics [38].

2.7.2 Power Analysis and Electromagnetic Field Analysis Attacks

In a power analysis attack, the attacker tries to obtain the power trace of an implemented algorithm to reveal secret information. Unlike a timing SCA attack, power analysis attack gives a 2-dimensional information about power consumption per time unit. Differential power analysis and correlational power analysis were studied in various reports [39]. Similarly, electromagnetic attacks take advantage of the EM fields around the crypto implementation to access the stored secret data. The general way is to place a core around the device and analyze the EM fields through simple EMA or differential EMA. A broader perspective of EM leakage attacks and methodologies can be studied in various papers [40].

CHAPTER 3

Introduction to Risk Assessment Methodologies

Based upon discussion from the previous chapter, there are several threats that can affect the functionality of the power grid. Lack of proper security mechanisms in WAMS can lead to contingencies in the power grid which could in the worst case potentially result in a blackout or damage to equipment, life, or the economy. As a result, it is important to protect power grid against all vulnerabilities.

3.1 Risk Mitigation Process

The risk mitigation process helps organizations reduce adverse effects by identifying, assessing and prioritizing risk factors to respective organization. As per NIST special publication 800-39 [41], the risk mitigation process includes four important stages: framing risk, assessing risk, responding to risk and monitoring risk.

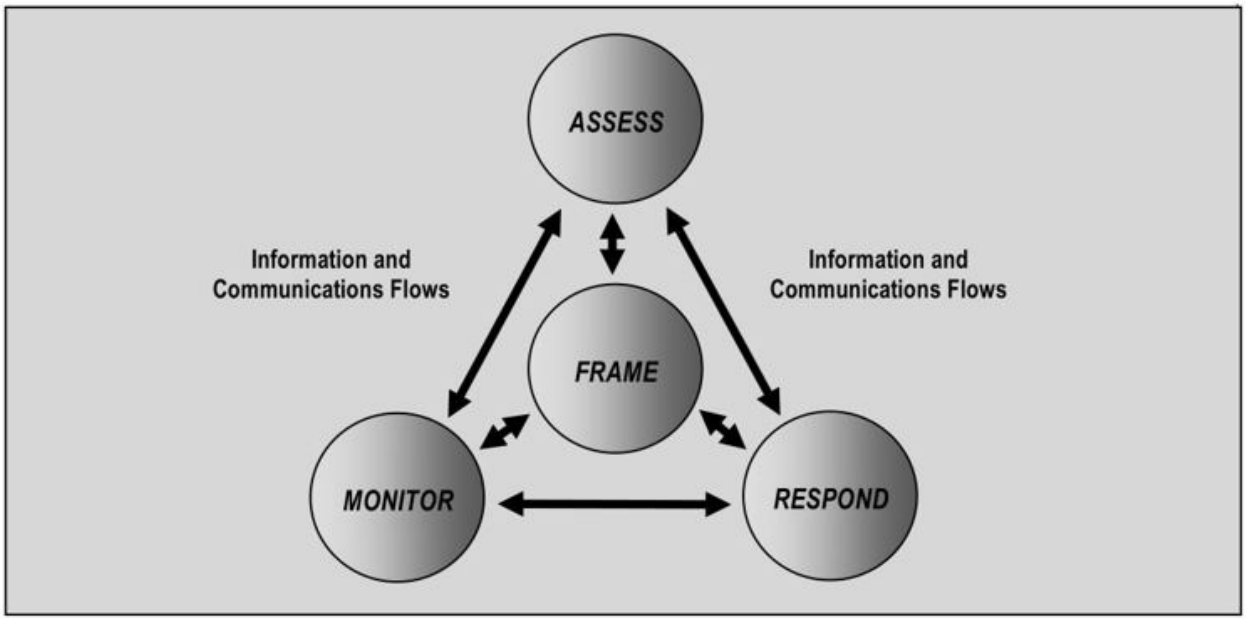

Figure 3.1: Risk Management Process
[41]

Framing risk is the very first component of the risk mitigation process, where organi-

zations frame risk or acknowledge the environment in which risk-based decisions are being made. The risk management strategy deals with information about how to assess, respond, and monitor risks depending on how the risk is framed based on the situation. Risk assessment is the second component of the risk mitigation strategy, where organizations assess risk within the boundaries of organizational risk frame. Risk determination follows risk assessment, typically along with a function of a degree of harm and likelihood of harm occurring. The third component of the risk mitigation process is risk response which deals with how a system or an organization responds to risk once the risk is determined based on the results of risk assessment. This stage of risk management strategy is responsible for developing alternative courses of action for responding to risk, implementing risk responses, evaluating the alternative courses of actions, determining the appropriate course of action consistent with organizational risk tolerance. The fourth and final stage in risk management strategy according to NIST special publication 800-39 [41] is risk monitoring. As per [42], organizations typically carry out following steps while performing risk monitoring:

- Verify if the risk responses are implemented.
- Determine the ongoing effectiveness of risk responses.
- Identify risk-impacting changes to organizational information systems and the environments in which the systems operate.
- Information security requirements are derived from all the potential risk factors that are traceable to organizational missions/business functions federal legislation, directives, regulations, policies, standards, and while making sure that guidelines are satisfied.

3.2 Risk Assessment Process

A risk assessment process is a fundamental component of an organizational risk management system which is used to identify, estimate and prioritize risk to organizational opera-

tions, organizational asserts, individuals, other organizations and the nation resulting from the operation and use of information systems [42]. To put in simple words, risk assessment in an organization should carefully examine what could cause damage to the functions and values of the respective organization by their occurrence and effect so that the organization can take respective actions to mitigate them. The primary purpose of a risk assessment process is to identify:

- Relevant threats to organizations or threats directed through organizations against other organizations.
- Vulnerabilities both internal and external to organizations.
- Impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities.
- Likelihood that damage will occur.

Risk assessment is not a one-time process but should be done periodically, as the threats associated with an organization always change and mature into different states. Most organizations, especially critical systems like power grids conduct the risk assessment on a periodic basis throughout system development and maintenance cycles considering different hierarchies in the system.

A risk assessment methodology typically consists of four important phases: a risk assessment process, an explicit risk model, an assessment approach, and an analysis approach. The risk assessment process starts with identifying the need for risk assessment, and stating how a derived model will help the organization mitigate threats. While performing the second stage, the organization generally defines all the key terms and assessable risk factors that are associated with the organization. A qualitative relation between them is also stated at this stage. In the assessment approach, an organization will define the type of approach and calculate the risk associated with the defined keywords. These assessment approaches

can be quantitative, qualitative or semi-quantitative. Finally, in the analysis approach, risk assessment performer describes how a series or combination of risk factors will affect the approach. Vulnerability oriented, threat-oriented, or asset/impact-oriented are typical analysis approaches that are used by the organization. In practice, organizations perform the risk assessment with multiple risk models, especially when dealing with critical systems of state or nation.

3.3 Risk Model

As discussed earlier, while drawing a risk model the organization will identify and define all the risk factors that are associated with the respective organization. Each risk factor is assessed, and the relationships between these factors are also stated in this stage of assessment. Each risk factor is used as an input to the risk assessment to define their associated impact level. As per NIST special publication 800-30 [42], common risk factors include threat, vulnerability, impact, likelihood and predisposing conditions. Each of these can again be decomposed into their respective threats sources and threat events. Defining an accurate risk model is important for performing analysis, as these risk factors act as inputs for further stages.

3.3.1 Threat

As per the NIST special publication 800-30 guidelines [42], a threat is any circumstance or event with the potential to adversely impact organizational operations and assets as well as individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. While defining threat, an organization can also define threat based upon sets and/or sequences of related actions, activities, and/or circumstances or single events, actions, or circumstances.

A threat source is the cause of threats to an organization. Threat sources can be characterized as:

- Benign threat sources, where vulnerabilities are exploited accidentally,
- Malicious asymmetric threats that are targeted to exploit a specific set of vulnerabilities,
- Accidental or intentional human errors,
- Structural failure of organization-controlled resources,
- Threat sources that are beyond organization control, like natural and man-made disasters.

Effects from various threat sources can have similar outcomes. For example, the availability of a PMU measurements can be compromised by a maliciously crafted denial of service attack, accidental/intentional operator command, substation maintenance errors, a hardware failure, floods, or power failure. Complexity and levels of detail associated with the risk model depend on the adopted risk model. With a detailed risk model, threat scenarios can also be analyzed. While a threat scenario can also happen with accidental events, its likelihood is very low when compared to crafted scenarios.

For identifying threats associated with an adversary, an organization should conduct analysis considering tactics, techniques, and procedures (TTPs) employed by the adversaries. By analyzing adversary TTPs, an organization can extract insights into details associated with certain threat sources. Also realizing adversaries and their capabilities give a better understanding of malicious threat events. The set of target events can also be narrowed when the adversary is identified along with intent and targeting aspects of potential attacks. When dealing with critical systems, the risk model should consider threat shifting where adversaries change some characteristics of the attacks to hide from safeguards. Based on the dynamic information, threat shifting can take place in one or more domains:

- Time domain, where attackers postpone or move to an earlier time to carry out the attack,
- Target domain, where attackers change the target such as going for least expected domain,
- Resource domain, adding resources to attacks to add computer power or to bypass protection mechanisms,
- Attack planning, changing attack weapon or attack path.

3.3.2 Vulnerabilities and Predisposing Conditions

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [42]. The organization associated vulnerabilities can be mitigated by implementing security protocols. However, even after implementing security mechanisms, there will still be weaknesses. Vulnerabilities also emerge over time, when the devices used in the organizations are getting older. As a result, it is important for an organization to periodically perform risk assessment and identify the vulnerabilities in the system. Such a periodic risk assessment gives a situational awareness about boundaries of the system. While dealing with a critical asset as per NIST special publication 800-30, risk assessment should consider vulnerabilities not just with information systems but also:

- Organization governance structures such as poor intra-agency communications, misalignment of enterprise architecture to support mission/business activities or lack of effective risk management strategies and adequate risk framing,
- External relationships such as dependencies on particular energy sources, supply chains, information technologies, and telecommunications providers,

- Mission/business processes such as poorly defined processes or processes that are not risk-aware,

- Enterprise/information security architectures such as poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems.

The predisposing condition is a state condition that affects the environment of the operation, mission or business purpose, information systems or enterprise architecture. Once initiated, predisposed conditions affect the likelihood of threat events associated with the organization. For example, a stand-alone network for information systems without any other outside connections, or the location of facilities in flood-prone areas have a predisposing risk with the floods. After they arise, threats associated with the predisposing events cannot be easily mitigated.

3.4 Assessment Approaches

Typically, risks related to the various factors can be presented in three ways: qualitative assessment, quantitative assessment, or semi-quantitative assessment. In a quantitative assessment approach, the organization will apply a set of rules to risk factors and state the risk associated with it in terms of numbers. A scale associated with these numbers is maintained to assess the impact of the risk. This type of assessment approach requires in-depth knowledge to set the rules for quantitative assessment. The result from quantitative assessment may not always be clear and may require additional interpretation and explanation.

Unlike quantitative assessment, qualitative assessment develops and applies a set of rules and principles to risk factors and gives their associated risk with no numerical categories. Though this approach supports a well-defined communication between the risk and the decision maker, the range of values that can be assigned is comparatively small. This sometimes sets back the risk assessment process by limiting its prioritization level to risk factors. However, qualitative assessment has better repeatability and reproducibility if the organization

manages to use detailed annotation of assessed values.

In a semi-quantitative approach, the risk assessment employs multiple rules and methods for risk factors, generates risk associated with various representations like bins, scales, or representative numbers. A semi-quantitative risk assessment that is carried out using bins and scales can be translated into a quantitative assessment easily by developing a comparison scale. However, a major drawback of this method is that relative comparisons within the factors of the same bin are highly insignificant. The organization selects a risk assessment approach based on factors like attitude towards defining uncertainty and risk communication and organization culture.

3.5 Analysis Approach

As per the NIST special publication on risk assessment, there are three types of analysis approaches for risk assessment: threat-oriented, asset/impact-oriented, or vulnerability oriented. The selection of the analysis approach depends on the starting point of the risk assessment, and level of detail the organization is planning for the assessment.

In the threat-oriented approach, the analysis starts from identifying the threats at various levels of the organization. After identifying threats, this approach will concentrate on analyzing threat sources, threat events, and threat scenarios. All the known vulnerabilities in the system are correlated with the threats associated with it, and adversary threats are correlated based on adversary intent. Unlike the threat-oriented approach, the asset/impact-oriented approach starts with identifying impacts on the organization. Based on the impact, organizations will develop threat events that can be associated with the threat sources which can potentially lead to that impact level. Similarly, a vulnerability-oriented approach will start by identifying the predisposing conditions or exploitable deficiencies associated with organization environment or information system. After identifying an approach, an organization will analyze all the possibilities of all threat events that can potentially exploit vulnerabilities. Though the input details are the same for all of the stated analysis ap-

proaches, the order of outcomes and the set of risk assessment activities differ based on the approach.

No matter which approach the organization chooses, each will apply several rigorous analysis methods like graph-based or fault-tree based analysis to state an accurate model, defining many-to-many relationships like [41]:

- Threat sources and threat events. A single threat event can be caused by multiple threat sources and a single threat source can cause multiple threat events,
- Threat events and vulnerabilities. A single threat event can exploit multiple vulnerabilities, and a single vulnerability can be exploited by multiple threat events,
- Threat events and impacts/assets. A single threat event can affect multiple assets or have multiple impacts, and a single asset can be affected by multiple threat events.

These rigorous analysis approaches also help in establishing ways to carry risks based on specific time frame, adversary impacts and potential frequency of the specified adversary impacts. This information can help the organization identifying the area to improve specific security measures and possible ways to recover from these impacts.

CHAPTER 4

Taxonomy of Cyber-Threats in WAMS

In this chapter, a risk assessment model for a generic WAMS is described. The risk assessment model helps in identifying the specific areas where a power grid using WAMS can improve its security aspects. Risk assessment is done on a generic WAMS model using a hybrid model with impact-oriented and vulnerability analysis, and results are described using a qualitative scale.

4.1 Methodology

The primary purpose of developing this taxonomy is to give insight regarding adversarial and non-adversarial vulnerabilities in WAMS. As this thesis is developed with a primary focus on cyber-threats associated with WAMS, factors related to environmental events and predisposed conditions are mentioned but not elaborated. A generic WAMS model with a network of PMUs, PDCs, and Super PDCs is considered while developing this taxonomy. At the current time WAMS works along with SCADA, so vulnerabilities that are common to both and that can affect WAMS through SCADA networks are also considered.

The following model is developed with a high level of abstraction, starting with an impact-oriented analysis over WAMS. Later, adversarial and non-adversarial vulnerabilities associated with a generic WAMS model are discussed. The developed taxonomy model is designed to tolerate incompleteness. For example, Incident reports often provide terse accounts of attacks for reasons of sensitivity. For example, a report may mention how an attack was carried out, but omit its consequences. Alternatively, a report may describe a system vulnerability and how its exploitation may cause damage, but it may not discuss how attackers might conduct the exploit [43].

4.2 Assessment Scale

In this section, a description of the qualitative scales used for presenting the results is explained. The assessment scale used for measuring the impacts associated with the threat source is classified into two categories based on the intention behind the threat source. A fault in a device used in power grid can occur either accidentally or due to being targeted by adversaries with a malicious intent. Either way, the fault can potentially lead to the device's failure or a system failure.

Table 4.1 presents the description of assessment scale regarding non-adversarial threat sources. The qualitative scale used for this table consists attribute values of very low, low, moderate, high and very high. Any software or hardware resource that helps the power grid by preventing an unauthorized event or by alerting an authorized operator when a unauthorized event occurs can be grouped as cyber resources. A power grid's functionality is not affected directly when a failure occurs in cyber resources. However, failure in cyber resource leaves critical resources that are vital for maintaining power grid's proper functionality vulnerable. The impact levels for the non-adversarial class can vary based on the number of effected cyber resources and critical resources when the respective threat event takes place. In a power grid, a non-adversarial threat can arise from various threat sources:

- Accidental error by operators
- Deterioration of software or hardware resources in power grid
- Predisposing conditions and act of nature

Similarly, Table 4.2 and Table 4.3 present the assessment scale associated with adversarial threats. Impact of an event associated with adversaries varies based on the adversary's capability, intent, and targeting. Similar to non-adversarial events, a qualitative scale consisting values ranging from very low to very high is used to present the associated impact levels. The attacker's capability varies based on his level of expertise, resources they possess, and oppor-

Table 4.1: Assessment scale: Non-Adversarial threat sources

Qualitative Scale	Description
Very Low	The effects of the error, accident, or act of nature are minimal. Involving unavailability to few cyber resource and general purpose resources, but not to any critical resources.
Low	The effects of the error, accident, or act of nature are limited. Involving damage or unavailability to some of the cyber resources and general purpose resources, but not to any critical resources
Moderate	The effects of the error, accident, or act of nature are wide-ranging. Involving significant portion of cyber resources and general purpose resources, including some critical resources.
High	The effects of the error, accident, or act of nature are extensive. Involving damage to most of the cyber resources and general purpose resources, including many critical resources.
Very High	The effects of the error, accident, or act of nature are sweeping, involving almost all cyber resources, general purpose resources, and critical resources.

tunities they can create for conducting a successful attack. An attacker with a higher level of capabilities can perform continuous and coordinated attacks. Impacts associated with an attacker also depend on the intent of the attacks. The impact from a threat event caused by an attacker who has an intent of damaging the core functionality and critical resources is a lot higher than attacker with an intent to test the cyber resources of the power grid. The intent of an attacker also depends on how the attacker manages to disguise their attack from the power grid's Intrusion Detection System (IDS). Attackers who are more concerned about being detected will adopt various methods to hide from the IDS and are classified with a higher intent than attackers who are not concerned. Similar to attacker's intent and capability, the impact associated with a non-adversarial threat depends on the attacker targeting

Table 4.2: Assessment Scale: Adversarial threat sources.

Qualitative Value	Characteristics	Description
Very Low	Capability	The adversary possess limited expertise, resources, and opportunities to support a successful attack
	Intent	The adversary seeks to usurp, disrupt, or deface the power grid's cyber resources, and does so without concern about attack detection/disclosure of tradecraft
	Targeting	The adversary may or may not target any specific power grid or substation of power grid
Low	Capability	The adversary has limited resources, expertise, and opportunities to support a successful attack
	Intent	The adversary actively seeks to obtain critical or sensitive information or to disrupt the power grid functionality, and does so without concerning about attack detection/disclosure
	Targeting	The adversary uses publicly available information/ reconnaissance to entities related to power grid and seeks targets of opportunity within that respective entity
Moderate	Capability	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
	Intent	The adversary aims to obtain or modify specific critical or disrupt respective power grid's cyber resources. The adversary is concerned about being detected and can/will take respective action to avoid detection. The adversary is willing to delay/change attack methods to disrupt functionality of the grid
	Targeting	The adversary analyzes publicly available information/reconnaissance/intruded information to target specific entities that are not protected completely

Table 4.3: Assessment Scale: Adversarial threat sources: Extension

Qualitative Value	Characteristics	Description
High	Capability	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks
	Intent	The adversary aims to possess/analyze critical aspects of the power grid, by maintaining a presence in the power grid information systems, infrastructure and/or management. The adversary is very concerned about minimizing their attack to avoid detection
	Targeting	The adversary analyzes information obtained through public information, reconnaissance and/or internal management to target a specific under protected element in a power grid.
Very High	Capability	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks
	Intent	The adversary seeks to undermine, severely damage or destroy a core functionality through affecting confidentiality, integrity and availability of the power grid and maintain a single/multiple presence inside power grid. The adversary is very concerned about detection and can minimize attack with an insight of intrusion detection system methods
	Targeting	The adversary analyzes information obtained through public information/high-grade reconnaissance/internal management/critical function operators to target specific under protected element in the power grid; specifically, with information about system topology and action results

abilities. The impact from the attacker who has detailed knowledge about the system such as vulnerabilities in cyber resources and information related to critical resources is higher that the attacker who knows nothing about the system. An attacker can obtain such crucial

information from multiple sources ranging from publicly available information to working with privileged insiders.

This thesis aims to provide an insight to power grid operators regarding possible areas to evaluate the security requirements in the power grid. Impact values that are associated with the respective threat source are expressed using a range of attributes from the qualitative assessment scale while presenting results from the impact-oriented approach in the next section.

4.3 Impact-Oriented Approach

To describe an Impact-Oriented threat taxonomy, the abstract WAMS model in Figure 1.4 is assumed. The model classifies threat factors based on three categories: structural units, human factors, and environmental factors. Each category is again classified based on the threat source. In this impact-oriented approach, possible threat sources are identified initially with its respective aggregated class. Each aggregation consists of a threat class based on the threat source. A tabular form is used to represent data, with columns: threat source, associated threat events, and their respective impact level.

Table 4.4 presents a taxonomy of threats associated with structural units. Structural units associated with a generic WAMS model can be classified based on the hardware related to information and technology, systems that help to maintain the environment, and software that helps in maintaining WAMS functionality. In a WAMS communication system, any leaf node that transmits measurements can be classified into the sensor class. In a strict synchrophasor network, PMUs would be the only sensor nodes associated with information and technology equipment. However, this thesis also assumes threats associated with SCADA can indirectly affect WAMS functionality, like reconfiguring PMUs based on system configuration changes that are obtained by fault SCADA measurements. The impact associated with threats varies based on several factors like the resources an adversary possesses, the intensity of the attack or the number of units that are compromised. The

Table 4.4: Taxonomy of Threats associated with WAMS Structural Units

Type of Threat Source	Associated Threat Event	Impact
Information Technology Equipment		
Sensor	Benign faults in PMUs	Very Low to Moderate
	Malicious faults in PMUs	Low to High
	Benign faults in IEDs	Very Low to Moderate
	Malicious faults in IEDs	Low to High
Processing	Benign faults in PDCs	Low to Moderate
	Malicious faults in PDCs	Low to Moderate
	Benign faults in Super PDC	Moderate to High
	Malicious faults in Super PDCs	Moderate to High
	Benign faults in control center processing system	High
	Malicious faults in control center processing system	Very High
Communication	Benign faults in communication	Low to High
	Malicious faults in communication	Moderate to Very High
Storage	Benign faults in database/stream server	Low
	Malicious faults in database / stream server	Moderate
Environmental Infrastructure Control		
Temperature and Humidity Controls	Temperature control problems in substations	Low
Power Supply	Power supply failure	Low
Software		
General-Purpose Application	Benign faults	Very Low to Low
	Malicious faults	Low
Multi-Purpose Application	Benign faults	Low
	Malicious faults	Low to Moderate

processing class consists of correlation units like PDCs and Super PDCs. Faults associated with the measurement data processing and analysis in control center is also represented in a processing class. The software used to maintain mission purpose of the power grid, such as software associated with reading, analyzing and processing measurement data are classified as Mission-Purpose Applications, and the non-engineering software that works on a higher tier and helps running the power grid utility are classified as General-Purpose Applications. Similarly, threat events associated with maintaining infrastructure control is classified into Environmental Infrastructure Control.

When a benign fault occurs in a PMU or other IED measurement units, based on the

possible scenario in Table 4.7, its effect can range from going offline to affecting the outcome of the state estimation. When a non-adversarial fault occurs in a single measurement unit, the threat event will be either detected by the control center if the faulty measurement unit's value lies far from the acceptable boundary or will cause a non-effective deviation in the state estimation by sending a close measurement value with a small deviation. In either case the functionality of the power grid is not affected. However, when considered a less likely situation such as multiple non-adversary faults in heavily weighted PMUs, the outcome of the state estimation can change due to the faulty measurements. Hence, the impact level associated with the PMUs and IEDs varies from very low where none of the critical resources are affected to moderate where some of the critical resources like state estimation are affected. Similarly, based on the listed benign faults of PDCs, they can affect multiple PMUs measurement values while concentrating the data. As a result, any non-adversary fault can lead to damage varying from multiple cyber resources and general purpose resources to affecting the functionality of mission-critical resources. As a result, an attacks respective impact level is presented using an interval from low to moderate. Benign faults in super PDCs impact are presented with an interval of moderate to high as super PDCs work on a higher level of hierarchy which streams data directly to control center or storage server. Any non-adversary fault in a super PDC may potentially affect measurements from all the hierarchies beneath it, and cause damage from correlation error to the faulty outcome of state estimation and contingency analysis. Impact level for benign fault in control center processing system represented with high attribute value based on the number of critical resources a control center typically handles in a power grid. Impact levels associated with benign faults in communication and storage are also presented based on the number of resources it can potentially damage.

Similar to benign faults, the impact levels of malicious attacks are presented using an interval of qualitative values based on adversary qualities like capability, intent and targeting. Adversaries can possess different qualitative values for capability, intent, and targeting,

and the highest qualitative level among those is considered for risk associated with them. Malicious faults in measurements units can range from causing damage from non-availability in a device to affecting the outcome of the state estimation. When an attacker coordinates a well-crafted attack on multiple PMUs, they can potentially bypass the bad data detection algorithm and can potentially cause state estimation to omit desired output. As a result, impact level of malicious faults in PMUs and other IEDs ranges from low to high. Similarly, impact levels of malicious faults in PDCs varies from low to moderate and the impact levels of Super PDCs varies from moderate to high based on the adversary qualities and the number of resources they can potentially damage. Out of the malicious attacks listed in Table 4.9, any successful malicious attack on a control center can result in very high level impacts and an attack on storage source will a cause moderate level impact.

Table 4.5 presents a taxonomy of threats associated with human beings. The cause of the threat source can vary from an unintentional accident to crafted malicious cyber-attacks. The third column of Table 4.5 describes impacts associated with the respective threat source. Impact level may vary based on capability, intent, and targeting of respective threat source. Adding an insider to any threat source will increase potential impact associated with respective threat event as internal users can provide insight about the power grid based on their authorization level. An adversary with an insider's feedback can craft attacks that can cause a severe impact on the power grid functionality.

Table 4.6 presents threats sources associated with environmental factors of the power grid. Based on the stated assessment scale for non-adversarial threats, comparative impacts of threats associated with the environment is stated. Potentially every threat can cause an impact ranging from very low to very high. However, impacts levels in Table 4.6 are stated using NERC impact terminology [42]. The purpose of this table is to acknowledge the presence of this threat source, but further analysis is outside the scope of this research.

Table 4.5: Taxonomy of Threats Associated with Human Factors

Type of Threat Source	Associated Threat Event	Impact
Accidental	User in information system level	Very low
	User in mission/business processes	Low
	Semi-privileged user	Low to high
	Administrator	Moderate to very high
Individual(adversarial)	Outsider	Very low to low
	Insider	Low to moderate
	Trusted insider	Moderate to high
	Privileged insider	High to very high
Group	Ad Hoc (without insiders)	Moderate to very high
	Ad Hoc (with insiders)	High to very high
	Established (without insiders)	Moderate to very high
	Established (with insiders)	High to very high
Organization	Competitor	Low to moderate
	Supplier	Low to high
	Partner	Low to high
	Customer	Low
Nation-state	Attacks associated with nation/state	Moderate to very high

Table 4.6: Taxonomy of Threats Associated with Environment

Type of Threat Source	Associated Threat Event	Impact
Natural or man made disasters	Fire	Very low to moderate
	Flood/Tsunami	Moderate to very high
	Windstorm/Tornado	Low to high
	Hurricane	Moderate to high
	Earthquake	Low to high
	Bombing	Low to high
Unusual natural event	Disruption of power line(animals/tress)	Low to moderate

4.4 Threat-oriented Approach

In this section, vulnerabilities within WAMS, which could be exploited by a threat source are explained. Due to the ever-increasing complexity of the power grids, vulnerabilities associated with a threat event tend to be large and can increase the overall complexity of the analysis. As a result, vulnerabilities associated with threat events in this approach are stated in a highly abstract manner. Threats are classified based on the benign or malicious

Table 4.7: Benign Faults in WAMS

Threat Event	**Description**
Hardware Failure in Measurement Units	Hardware failure in devices like PMUs, PDCs, super PDCs and other crucial IEDs, force device to go offline
Passive Hardware Failure (PMUs)	Hardware failure in devices like PMUs and other advanced measurement units, leading to situations like: - Sending most recent value to control center but not current measurements. - Failing to respond to control center requests - Failing to synchronize with high hierarchy devices (PDCs) - Un-corrected clock drifts
Passive Hardware Failure (PDCs and Super PDCs)	Hardware failure in correlation devices like PDCs and Super PDCs, leading to situations like: - Failing to respond to control center requests - Failing to synchronize with higher and lower hierarchy devices (super PDCs and PMUs) - Synchronization error while correlating data - Sending real-time measurements with delay drifts
Hardware/transmission failure in TSMD	A failure in TSMD and/or GPS due to which PMUs don't receive time stamps
Control Center Processing System	Hardware failure in computational systems used at control center
Communication	Degraded communication performance due to hardware failure in switches, modems, routers used in data transmission in WAMS or due to unintended/unexpected disturbances purpose

event. Each category of threats are discussed in their respective tabular form, with threat event and description listed.

To state possible threat events, adversaries, the Tactics, Techniques and Practices (TTP)

Table 4.8: Benign Faults in WAMS: Extension

Threat Event	Description
Storage	Hardware failure in servers/buffer containers that stores streaming data like corrupt storage in disk error or lack of availability due to hardware/power failure
Resource depletion	Degraded processing performance due to resource depletion
Mishandling information	Authorized users releasing information to unprivileged user or outsiders, exposing data varying from system specifications to grid topology
Incorrect privilege settings	Authorized user or administrator accidentally assigns privileges to un-authorized user
General-Purpose Application	Vulnerabilities or bugs in system software, leading to improper functioning.
Mission-Purpose Application	Vulnerabilities or bugs in mission-purpose software, leading to improper functioning.
Temperature control and power failure	Failure in environmental factors that helps is system functioning like temperature control and power failure.

associated with the adversaries must be studied first. By understanding TTPs adopted by an attacker on WAMS, associated threat events can be described at various locations in a synchrophasor network. Based on cyber-attacks discussed in Chapter 2, a fault tree diagram associated with adversarial threats that aim to damage the power grid functionality is shown in Figure 4.1.

With the aim of disrupting the functionality of the grid, attackers can perform dedicated attacks that could disrupt the mission purpose of the WAMS. However, apart from the attacks mentioned in the fault tree, there are numerous threats/threat scenarios that can be used by an attacker to disrupt the functionality of the grid.

Table 4.9, Table 4.10, and Table 4.11 consists various threat events that an attacker can use to take advantage. Based on the adversary TTP, possible areas where an attacker can exploit are aggregated into multiple classes. These aggregated classes consists potential threat event.

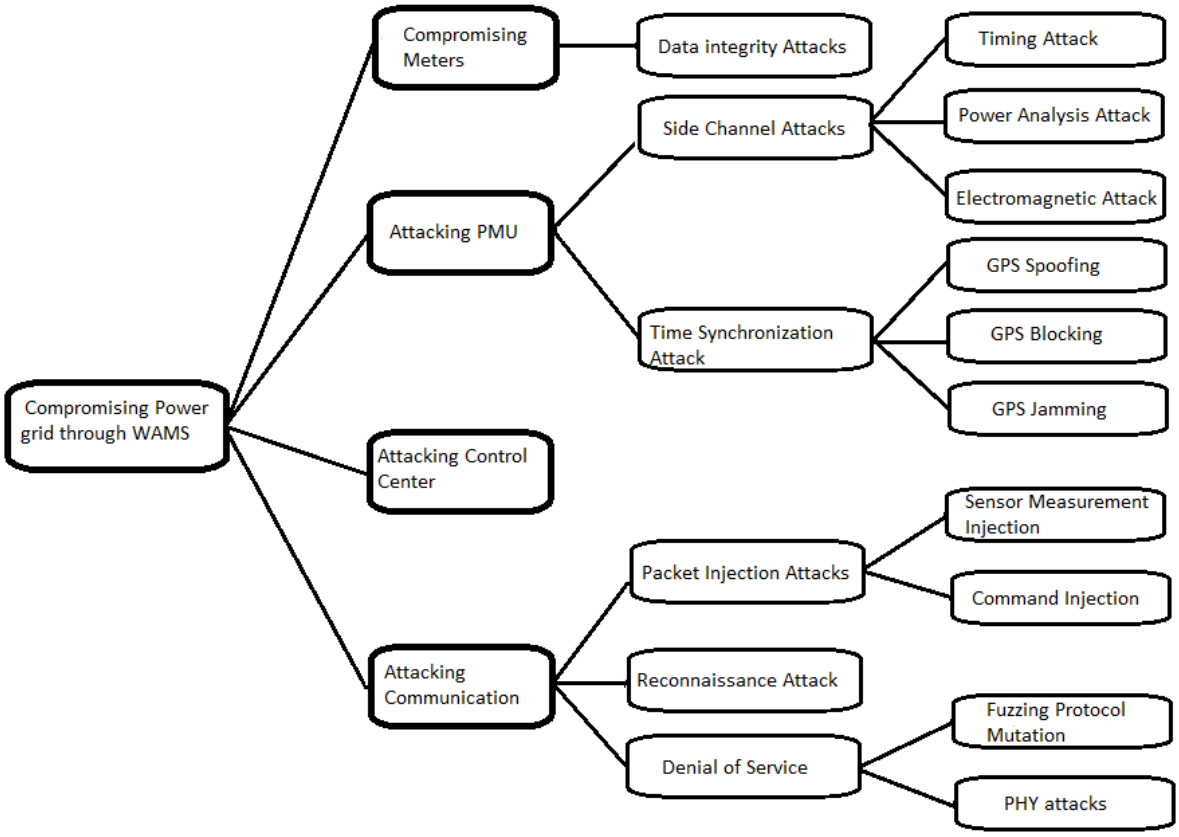

Figure 4.1: Adversary TTP Based Fault-Tree

Table 4.9: Malicious Faults in Power Grid Through WAMS

Threat Event	Descriptions
Reconnaissance and Information Gathering	
Reconnaissance (Network)	Adversaries use various programs to scan organizations perimeters to gain information which will be used to craft a malicious payload or attack.
Reconnaissance (Malware)	Adversaries use malware that is on an authorized user's device and performs reconnaissance attack through it. By doing so, the chance of being detected by the intrusion detection system is much less.
Network sniffing	Adversaries try to sniff the external network like a data channel to communicate, to analyze about the component, resources and protection.
Analyzing open source information	Analyzing PMU and other IEDs manuals to understand the details of the system.
Available and Crafted Attacks Tools	
Phishing attacks	Adversaries perform phishing attacks in high volumes, including on systems admin, operators and high management employees.
Spear phishing attacks	Vulnerabilities or bugs in mission-purpose software, leading to improper function.
Targeted general malware	Delivering malware to an organization's internal information system, like sending through email and tricking a user to click or through USB.
Targeted crafted malwares	Adversaries craft special attacks tools like dedicated malware tool with known details of the system. These attacks can be very effective.
Untargeted crafted malware	Delivering untargeted malware like ransomware. A possibility to do so can be placing the malware in a software download click bait.
Spoof website	Adversaries spoof PMU/service provider website, tricking operators to enter credentials.
Spoof certificates	Adversaries spoof certificates to make their attack tool legitimate. By doing so, they can stay legitimate with broken SSL too.
Specific Mission-Purpose Attacks	
Communication interception attack	In the presence of weak-encryption and outdated protection schemes, an attacker can break an SSL and interpret information between PMUs, PDCs and other nodes.
Denial of service attacks	To affect availability, attackers can perform DoS attacks on the targets like PMUs, PDCs, super PDCs, processing units and other IEDs. To intensify the attack, adversaries could perform distributive denial of service. It can be done by fuzzing attacks or PHY attacks.

Table 4.10: Malicious Faults in Power Grid Through WAMS: Extension

Threat Event	Descriptions
Specific Mission-Purpose Attacks	
Sensor measurement injection	Adversaries inject data into the network, communicate as PMUs and deliver arbitrary data.
Command injection attack	Adversaries inject commands into PMUs and other processing units, communicate as a control center.
Time synchronization attacks	Adversaries disrupt the synchronization in the measurements by disrupting communication with GPS receiver.
Side channel analysis	Perform side channel analysis attack to gain information about authentication details.
Data integrity attacks	Changing the values of a meter to cause operator to trip apparatus in the system.
Exploits	
Known exploits	Attackers use known exploits in the PMUs, PDCs and super PDCs.
Known exploits in organization information systems	Attackers use known exploits in the information systems used by the organization.
Known exploits in personal systems	Attackers use known exploits in the laptops, smart phones and other PDAs.
Attacking unauthorized port and services	Adversaries take advantage of unprotected and unauthorized port, protocols and services in PMUs, and other devices.
Tampered hardware	Adversaries intervene in hardware supply and delivering tamper hardware with preloaded payloads and tools.
Cloud based attacks	If the power grid is using any cloud services, adversaries can perform attacks like cloud scavenging to gather any data related to the grid.
Password cracking	Adversaries try to crack the password, either through brute force or through known information to gain remote access to devices.
Physical/Social Engineering Attacks	
Compromising through physical access	Compromising PMUs, PDCs, super PDCs and other IEDs through physical access.
Drafting	Adversaries bypass physical security access through tailgating into substation or control room.
Social engineering	Conduct social engineering attacks, either as an outsider or an insider to obtain critical information about the system.

Table 4.11: Malicious Faults in Power Grid Through WAMS: Extension

Threat Event	**Description**
Physical/Social Engineering Attacks	
Inserting subverted individual	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to the organization.
Inserting subverted individual in privileged position	Adversary places individuals within organizations into privileged positions who are willing and able to carry out actions to cause harm to the organization, and can leak sensitive information.
Compromising supply chain	Adversaries compromise partners, suppliers and install malicious software on power grid systems.

CHAPTER 5

Summary and Future Work

5.1 Summary

In the last 15 years, cyber security measures in power systems have been questioned as unavailability in the power grid potentially causes great losses to the economy and human hours. In addition, over the past 20 years power grids have adopted advanced measurements tools, paving a path for advanced and reliable power operation and control schemes. As these advanced measurement tools require communication networks that may have paths to the internet, they tend to attract several cyber-attacks, so integrating advanced measurement units like PMUs comes with a risk of increasing vulnerabilities. This thesis is developed with a goal to provide a taxonomy of threats, which can help power organization to make risk management decisions.

At present, WAMS is primarily used as a back-up or supplement for SCADA system. Therefore, the adaptation of PMUs, PDCs, and Super PDCs differ based on a specific WAMS's purpose. As a first step, an abstract model power grid with PMUs as primary sensor units, and PDCs and super PDCs as primary correlation units is assumed. Using this model, an impact-oriented taxonomy is created considering benign and malicious faults. Factors associated with the environment and predisposing conditions are also mentioned in the thesis, but not elaborated as they do not fit into the scope of this thesis. Based on the threat-oriented approach, associated benign and malicious faults are elaborated further covering threat sources.

To ease extensibility, a qualitative-approach scale is used to describe impact associated with threat sources, using the following terms: very low, low, moderate, high, and very high. Impacts associated with the threat sources may vary based on the unintentional faults and intensity of failures for benign faults, and factors like adversarial capability, intent and targeting for malicious faults. Description for adopting qualitative scale values are also

elaborated in chapter 4.

5.2 Future Work

Several aspects of this project could be investigated future. Some of these areas include:

1. Adding Likelihood to Taxonomy

Apart from deriving threat sources, deriving their respective likelihood can improve the current taxonomy. The updated taxonomy can help in making decisions that involve trade-off between security measures and their respective implementation cost while performing risk management. However, an accurate power grid network is needed for deriving a set of rules to calculate the respective likelihood of a threat source.

2. A Complete Taxonomy of Threats in Power Grids

The current taxonomy is based on an abstract WAMS model which only considers PMUs, PDCs, and Super PDCs as mission purpose entities with few SCADA units which will indirectly affect these mission purpose entities. However, in recent years, WAMS is used along with a SCADA and SCADA is not likely to go away. As a result, a complete taxonomy in modern power grids should cover threats associated with WAMS and SCADA.

3. Threats Scenarios and Threat Shifting

The current taxonomy did not include aspects related to threat shifting, where adversaries change the properties of threats to decrease the chance of being detected. Similarly, the current taxonomy did not include threat scenarios where the correlation between different threats and their respective combined effects are studied. Including threat scenarios and threat shifting properties can improve the taxonomy.

4. Integrating Vulnerability-Oriented Approach

The current taxonomy is based on a hybrid model that considers the impact-oriented and threat-oriented approach. Finding a way to integrate vulnerability oriented approach can surely increase the reliability of the taxonomy.

Bibliography

[1] M. Sharifian, "Security analysis of phasor measurement units in smart grid communication infrastructures," Master's thesis, University of Nebraska, Available in DigitalCommons of University of Nebraska, May 2014.

[2] M. Hurtgen and J.-C. Maun, "Applications of pmu measurements in the belgian electrical grid," Published as Technical Report, Tech. Rep., 2012.

[3] Y. Deng, H. Lin, A. G. Phadke, S. Shukla, J. S. Thorp, and L. Mili, "Communication network modeling and simulation for wide area measurement applications," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*. IEEE, 2012, pp. 1–6.

[4] M. Hadley, J. McBride, T. Edgar, L. Neil, and J. Johnson, "Securing wide area measurement systems," *US Department of Energy*, 2007.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[6] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[7] A. Goodney, S. Kumar, A. Ravi, and Y. H. Cho, "Efficient PMU networking with software defined networks," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*. IEEE, 2013, pp. 378–383.

[8] C. Wells, A. Moore, K. Tjader, and W. Isaacs, "Cyber secure synchrophasor platform," in *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*. IEEE, 2011, pp. 1–4.

[9] R. H. Khan and J. Y. Khan, "Wide area PMU communication over a WIMAX network in the smart grid," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on.* IEEE, 2012, pp. 187–192.

[10] N. Report. "Real-Time Application of Synchrophasors for Improving Reliability". [Online]. Available: http://www.nerc.com/docs/oc/rapirtf/RAPIR%20final%20101710.pdf

[11] C. Report. "Phasor Technology ". [Online]. Available: http://www.phasor-rtdms.com/phaserconcepts/phasor_adv_faq.html#Question2

[12] E. P. Group. "RTDMS:Real Time Dynamics Monitoring System". [Online]. Available: http://www.electricpowergroup.com/rtdms.html

[13] R. Mackiewicz, "Overview of IEC 61850 and benefits," in *Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES.* IEEE, 2006, pp. 623–630.

[14] K. E. Martin, "Synchrophasor standards development-IEEE C37. 118 & IEC 61850," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on.* IEEE, 2011, pp. 1–8.

[15] K. Narendra and T. Weekes, "Phasor measurement unit (pmu) communication experience in a utility environment," in *Conference on power systems*, 2008, pp. 19–21.

[16] D. Baigent, M. Adamiak, R. Mackiewicz, and G. M. G. M. SISCO, "IEC 61850 communication networks and systems in substations: An overview for users," *SISCO Systems*, 2004.

[17] J. Horalek and V. Sobeslav, "Datanetworking aspects of power substation automation," *Communication and management in technological innovation and academic globalization*, pp. 147–153, 2010.

[18] D. Watts, "Security and vulnerability in electric power systems," in *35th North American power symposium*, vol. 2, 2003, pp. 559–566.

[19] M. Qiu, H. Su, M. Chen, Z. Ming, and L. T. Yang, "Balance of security strength and energy for a PMU monitoring system in smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.

[20] M. Popa and M. Albu, "Implementation overview of pmu functionalities on a regular computer," in *Smart Measurements for Future Grids (SMFG), 2011 IEEE International Conference on*. IEEE, 2011, pp. 40–44.

[21] T. H. Morris, S. Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–6.

[22] "NMAP Security Scanner". [Online]. Available: http://www.nmap.org

[23] "Wireshark". [Online]. Available: http://www.wireshark.org

[24] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *Control & Automation (MED), 2012 20th Mediterranean Conference on*. IEEE, 2012, pp. 716–721.

[25] "MU Dynamics". [Online]. Available: http://www.mudynamics.com

[26] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 799–821, 2012.

[27] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, 2012.

[28] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[29] P. T. Myrda and K. Koellner, "Naspinet-the internet for synchrophasors," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on.* IEEE, 2010, pp. 1–6.

[30] B. Sikdar and J. H. Chow, "Defending synchrophasor data networks against traffic analysis attacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 819–826, 2011.

[31] E. P. Group. "US spy drone hijacked with GPS spoof hack". [Online]. Available: https://www.theregister.co.uk/2011/12/15/us_spy_drone_gps_spoofing/

[32] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attacks on a vector-based tracking gps receiver," in *Proceedings of the International Technical Meeting of The Institute of Navigation*, 2012.

[33] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[34] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Domı *et al.*, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[35] Smartgrid.gov. "Computer Security Division:2010 Annual Report". [Online]. Available: https://www.smartgrid.gov/files/Smart_Grid_Cyber_Security_200209.pdf

[36] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." *IACR Cryptology ePrint Archive*, vol. 2005, p. 388, 2005.

[37] F. Koeune and F.-X. Standaert, "A tutorial on physical security and side-channel attacks," in *Foundations of security analysis and design III.* Springer, 2005, pp. 78–108.

[38] A. Field, *Discovering statistics using IBM SPSS statistics.* Sage, 2013.

[39] F. Zhang and Z. J. Shi, "Differential and correlation power analysis attacks on hmac-whirlpool," in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on.* IEEE, 2011, pp. 359–365.

[40] D. Agrawal and B. Archambeault, "The em side-channel (s): Attacks and assessment methodologies," *Cryptographic Hardware and Embedded Systems–CHES*, 2002.

[41] S. NIST, "800-39.(2011)," *Managing Information Security Risk–Organization, Mission, and Information System View. National Institute of Standards and Technology. Retrieved from http://csrc. nist. gov/publications/nistpubs/800-39/SP800-39-final. pdf.*

[42] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002.

[43] T. Fleury, H. Khurana, and V. Welch, "Towards a taxonomy of attacks against energy control systems. critical infrastructure protection ii," *The International Federation for Information Processing*, vol. 290, 2009.