Vaasan yliopisto
UNIVERSITY OF VAASA

Jari-Pekka Kankaanpää

GNSS Related Threats to Power Grid Applications

School of Technology and Innovations
Master's thesis in Economics and
Business Administration
Information Systems

Vaasa 2021

UNIVERSITY OF VAASA
School of Technology and Innovations
Author: Jari-Pekka Kankaanpää
Title of the Thesis: GNSS Related Threats to Power Grid Applications
Degree: Master of Science in Economics and Business Administration
Programme: Master's Programme in Information Systems
Supervisor: Heidi Kuusniemi
Year: 2021 **Pages:** 110

ABSTRACT:

As power grid environments are moving towards the smart grid vision of the future, the traditional schemes for power grid protection and control are making way for new applications. The advancements in this field have made the requirements for power grid's time synchronization accuracy and precision considerably more demanding. So far, the signals provided by Global Navigation Satellite Systems have generally addressed the need for highly accurate and stable reference time in power grid applications. These signals however are highly susceptible to tampering as they are being transmitted. Since electrical power transmission and distribution are critical functions for any modern society, the risks and impacts affiliated with satellite-based time synchronization in power grids ought to be examined.

This thesis aims to address the matter. The objective is to examine how Global Navigation Satellite Systems are utilized in the power grids, how different attacks would potentially be carried out by employing interference and disturbance to GNSS signals and receivers and how the potential threats can be mitigated. A major part of the research is done through literature review, and the core concepts and different implementations of Global Navigation Satellite Systems are firstly introduced. The literature review also involves the introduction of different power grid components and subsystems, that utilize Global Positioning System for time synchronization. Threat modeling techniques traditionally practiced in software development are applied to power grid components and subsystems to gain insight about the possible threats and their impacts. The threats recognized through this process are evaluated and potential techniques for mitigating the most notable threats are presented.

KEYWORDS: Power grids, Smart grids, Global Navigation Satellite Systems, Global Positioning System, Time Synchronization, Cyber security, Threat modeling

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Jari-Pekka Kankaanpää
Tutkielman nimi: GNSS Related Threats to Power Grid Applications
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietojärjestelmätiede
Työn ohjaaja: Heidi Kuusniemi
Valmistumisvuosi: 2021 **Sivumäärä:** 110

TIIVISTELMÄ:

Sähköverkot ovat siirtymässä kohti tulevaisuuden älykkäitä sähköverkkoja ja perinteiset sähköverkon suojaus- ja ohjausmenetelmät tekevät tilaa uusille sovelluksille. Alan kehitys on tehnyt aikasynkronoinnin tarkkuusvaatimuksista huomattavasti aikaisempaa vaativampia. Tarkka aikareferenssi sähköverkoissa on tähän saakka saavutettu satelliittinavigointijärjestelmien tarjoamien signaalien avulla. Nämä signaalit ovat kuitenkin erittäin alttiita erilaisille hyökkäyksille. Sähkönjakelujärjestelmät ovat kriittinen osa nykyaikaista yhteiskuntaa ja riskejä sekä seuraamuksia, jotka liittyvät satelliittipohjaisten aikasynkronointimenetelmien hyödyntämiseen sähköverkoissa, tulisi tarkastella.

Tämä tutkielma pyrkii vastaamaan tähän tarpeeseen. Päämääränä on selvittää, miten satelliittinavigointijärjestelmiä hyödynnetään sähköverkoissa, kuinka erilaisia hyökkäyksiä voidaan toteuttaa satelliittisignaaleja häiritsemällä ja satelliittisignaalivastaanottimia harhauttamalla ja kuinka näiden muodostamia uhkia voidaan lieventää. Valtaosa tästä tutkimuksesta on toteutettu kirjallisuuskatselmoinnin pohjalta. Työ kattaa satelliittinavigointijärjestelmien perusteet ja esittelee erilaisia tapoja, kuinka satelliittisignaaleja hyödynnetään sähköverkoissa erityisesti aikasynkronoinnin näkökulmasta. Työssä hyödynnettiin perinteisesti ohjelmistokehityksessä käytettyjä uhkamallinnusmenetelmiä mahdollisten uhkien ja seurausten analysointiin. Lopputuloksena esitellään riskiarviot uhkamallinnuksen pohjalta tunnistetuista uhkista, sekä esitellään erilaisia menettelytapoja uhkien lieventämiseksi.

AVAINSANAT: Sähköverkot, älyverkot, satelliittipaikannusjärjestelmät, GPS, aikasynkronointi, kyberturva, uhkamallinnus

Contents

1 Introduction 9

2 Literature review and research objectives 11

3 Theoretical framework 17

3.1 Threat modeling 17

3.1.1 Threat modeling process 18

3.1.2 Attack Surface Analysis 20

3.1.3 Attack trees 21

3.1.4 STRIDE 23

3.2 Data gathering 25

3.3 Risk assessment 25

3.4 Research process 26

4 Global navigation satellite systems 27

4.1 Functional segments 27

4.2 GNSS Signals 31

4.3 Timing receivers 32

4.4 Navigation satellite systems 34

4.4.1 Global positioning system 35

4.4.2 GLONASS 37

4.4.3 Galileo 38

4.4.4 BeiDou 40

5 Power grid protection and control 42

5.1 IEC 61850 Standard 45

5.2 GNSS in power grids 46

5.2.1 Phasor measurement unit 46

5.2.2 Phasor data concentrator 48

5.2.3 Precision Time Protocol 50

5.2.4 Sampled Values (IEC 61850-9-2) 53

5.2.5 Merging Unit 54

5.2.6 Traveling wave fault location 55
5.2.7 Protection and Control Relays 56
6 Known threats and disruptions 58
6.1 Natural phenomenon 58
6.1.1 Ionospheric scintillation 58
6.1.2 Geomagnetic storms 59
6.1.3 Signal blockage 60
6.1.4 Multipath 61
6.2 Unintentional threats 62
6.2.1 RF interference 63
6.2.2 Unintentional Signal Jamming 63
6.3 Intentional threats 64
6.3.1 Intentional Signal Jamming 64
6.3.2 Spoofing attacks 65
6.3.3 Time synchronization spoofing attacks 66
6.3.4 Data Layer attacks 67
6.3.5 Receiver software attacks 69
6.4 Possible consequences 69
7 Threat analysis 73
7.1 Synchrophasor-based generation-shedding 73
7.1.1 DFD and STRIDE 74
7.1.2 Potential attacks 76
7.2 Line current differential protection 79
7.2.1 DFD and STRIDE 80
7.2.2 Potential attacks 82
7.3 Traveling wave fault location system 84
7.3.1 DFD and STRIDE 86
7.3.2 Potential attacks 88
8 Mitigating GNSS based threats 92
8.1 Mitigation techniques 93

9 Discussion and conclusions 97

References 100

Appendices 109

Appendix 1. Risk evaluation for identified threats 109

Figures

Figure 1. A modern DFD model (Shostack, 2014, p. 46). 19

Figure 2: Attack Tree for ATM machine (Mantel, & Probst, 2019, p. 186). 22

Figure 3. GNSS architecture modelled after GPS (Swamy, 2017, p. 1157). 28

Figure 4. Equatorial and inclined orbits (Groves, 2013, p. 301). 29

Figure 5. 1-PPS pulse generation (Jianfeng et. al., 2016, p. 1). 33

Figure 6. IEC 61850 based substation (Bayliss, & Hardy, 2011, p. 358). 43

Figure 7. WAMPAC Architecture (Terzija et. al., 2011, p. 82). 44

Figure 8. Representation of generic PMU (Parashar et al, 2012, p. 15-9). 47

Figure 9. PDC network (IEEE, 2013, p. 6). 49

Figure 10. PTP network topology (Watt et. al., 2015, p .2). 51

Figure 11. End-to-end and peer-to-peer delays (Watt et. al., 2015, p. 2). 52

Figure 12. Fault location in transmission line (Schweitzer et. al., 2016, p. 115). 56

Figure 13. Outdoor multipath and shadowing (Kaplan & Hagerty, 2017, p. 600). 62

Figure 14. Chicoasén-Angostura system overview (Schweitzer et. al., 2010, p. 1-2). 74

Figure 15. Chicoasén-Angostura generation-shedding scheme data flow diagram 75

Figure 16. Attack tree for tripping the Angostura generators 77

Figure 17. Attack tree for an attack aimed at the Angostura generators 78

Figure 18. Line current differential protection overview (Liu et. al., 2011, p. 521). 79

Figure 19. Line current differential protection dataflow diagram 80

Figure 20. Attack tree for filling event logs 82

Figure 21. Attack tree for triggering the current line differential protection 83

Figure 22. Wide-area traveling wave location system (Chen et. al., 2013, p. 1208) 84

Figure 23. TWFL network topology (Chen et. al., 2013, p. 1214). 85

Figure 24. Wide-area TWFL system dataflow diagram 86

Figure 25. Attack tree for invalidating a substation record in TWFL system 89
Figure 26. Attack tree for switching the initial detection substation 90

Tables

Table 1. Elements of DFD (Shostack, 2014, p. 45). 19
Table 2. STRIDE mnemonics (Shostack, 2014, p. 62-63). 24
Table 3: STRIDE-per-element (Shostack, 2014, p. 78). 24
Table 4. Risk matrix 26
Table 5. Threats by diagram element and threat type 26
Table 6. Comparison between different GNSS constellations 34
Table 7. Present and Future Generations of GPS satellites (Groves, 2013, p. 172) 35
Table 8. STRIDE-per-element analysis for generation shedding scheme 75
Table 9. Threats affecting the generation shedding scheme 76
Table 10. STRIDE-per-element for line current differential protection 81
Table 11. Threats affecting Line current differential protection 81
Table 12. STRIDE-per-element analysis for TWFL system 87
Table 13. Threats affecting TWFL 88
Table 14. Root causes and mitigations of GNSS based threats 92

Abbreviations

AOA	Angle of Arrival
CB	Circuit Breaker
CT	Current Transformer
DFD	Data Flow Diagram
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IED	Intelligent Electronic Device
PMCU	Phasor Measurement and Control Unit
PMU	Phasor Measurement Unit
PVT	Position, Velocity and Time
RFI	Radio Frequency Interference
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
UTC	Coordinated Universal Time
TSSA	Time Synchronization Spoofing Attack
VT	Voltage Transformer
WAMPAC	Wide-Area Monitoring, Protection and Control
WAMS	Wide-Area Measurement System

1 Introduction

Modern power grid infrastructure has been rapidly moving towards the smart grids of the future. Remote control, operation and monitoring have become commonplace and the state-of-the-art monitoring and protection schemes often require constant communication between different devices in the power grid. This development has exposed the power grids to the world at large in ever increasing pace. The industry is facing new challenges that it has not been accustomed to as new power grid applications have become more demanding. This has made cyber-security one of the main concerns among the parties dealing in electrical power distribution and distribution solutions.

Many of the modern devices and applications in power grids require precise time between themselves. These days the utilization of time synchronization devices is common in the energy management systems, precise time is a critical requirement for various power system applications and this requirement will be even more prevalent in the smart grids of the future. The accuracy of timing is crucial for power grid analysis and diagnosis. Merging data from different sources, accurate estimates of grid state, the safety of decentralized control and effective responses to fluctuations all rely on precise time stamps (Moussa et. al., 2016, p. 1952).

It has been noted that time synchronized recordings of dynamic events in power grid provide invaluable data for the purposes of system performance analysis, understanding the system behavior and the recognition of control actions during large-scale disturbances (Terzija et. al., 2011, p. 83). The North American blackout in August 2003 effectively proved that accurate timing and unified time source for data alignment are necessary for ensuring the grid stability. The most preferred candidates for achieving the demanded precision are Global Navigation Satellite System (GNSS) based signals and Precision Time Protocol (PTP). The downside to this is, that these time synchronization methods are susceptible to various attacks that affect their services (Moussa et. al., 2016, p. 1952). The fact that GNSS based synchronization methods rely on outside signal sources makes them vulnerable to threats originating from outside the power grid. The

nature of GNSS expose the systems to various threats ranging from natural phenomenon to unintentional interference and to intentional attacks.

Power grid stability plays an important role in many of the key functions in societies and this stability relies increasingly more on precise and unified time between different applications and devices. As Huang et. al (2018, p. 69023) state the necessity for cybersecurity and resilient systems has become abundantly clear for the electric industry. For example, on December 23, 2015, the self-control capabilities of the Ukrainian power grids were lost in an attack. The power supply for over 80 000 users was disrupted as seven 110-kV substations and twenty-three 35-kV substations suffered a blackout due to the attack.

This research was conducted on behalf of ABB Distribution Solutions and the primary motivations for this thesis was to gain experience on threat modeling and to investigate different ways how GNSS signals are utilized in power grids. Thus, the objective of this study was to recognize and analyze different kinds of GNSS-based threats, that might jeopardize the integrity of the power grid environments and to come up with ways to mitigate the most probable and harmful threats. This study was performed mainly through literature review and analysis of different use cases. Power grid infrastructure and different applications utilized in these environments are covered to an extent for gaining insight about possible threats and the fundamentals of different GNSSs are covered as well. The analysis and ranking of threats are performed with threat modeling techniques and frameworks traditionally used in software development. The results of this study are the threat modeling artifacts produced from the use cases, generalized list of threats and a collection of ways to mitigate the identified threats. The conclusions of this thesis and further research on the subject are discussed in the last chapter.

2 Literature review and research objectives

Power grids are time-related systems and the measured units are based to sampled waveform, the analysis and real-time control of electric power production relies on power grid's time synchronization (Yao et. al., 2012, p. 81). Without the time synchronized data, it would require a long time and considerable efforts to analyze and assess the root causes for large-scale disturbances (Terzija et. al., 2011, p. 83). Number of incidents have already proved that accurate timing and unified time source are crucial components in power grid monitoring and control. Time synchronization already plays an important role in many of the power grids that are in use at present moment and its importance will only grow in the future, as more advanced devices and applications are introduced to the power grids.

In England and Wales the monitoring, protection and control of the power grid has been realized with dedicated substation-based systems which have fixed architectures, configurations and settings (Terzija et. al., 2011, p. 90). Currently it is usual that digital substations and intelligent dispatch technique are utilized for safe operations and stability in power grids. The normal operation of power systems, early warnings, identification of incidents, failure analysis, dispatching and intelligent power grid operation and management are accomplished through data integration for the use of intelligent dispatch technique. Whether the substation is used for protection devices, monitoring and control devices, electronic transformers or intelligent switch, it cannot be separated from the synchronization information. This makes the time synchronization system an important part of a digital substation architecture. Though in reality the highly accurate time synchronization is more essential for fault analysis, fault location, troubleshooting, adaptive protection and self-recovery control and other functional requirements of the power grid (Yao et. al., 2012, p. 81).

United Kingdom plans to go through significant changes for the aging power grid infrastructure between the years 2020 and 2030. The modernization activities concerning the power systems will become more challenging and this requires the development of new

support and management tools and solutions. United Kingdom's National Grid is expected to specify the requirements for monitoring and control through R&D projects, pilot installations and coordination with other utilities and suppliers. It is planned that some existing monitoring systems at several generator sites will be supported by a small number of phasor measurement units (PMU) at strategic locations which are affected by the new network investments (Terzija et. al., 2011, p. 90). PMUs measure physical quantities based on sampled voltage and current waveforms and they are applied for monitoring, protection and control purposes in power grid environments. Values measured by the PMUs are synchronized to Coordinated Universal Time (UTC) with synchronization signals received from different Global Navigation Satellite Systems. The deployment and operation of PMUs is still an ongoing research and development activity as the industry is moving towards smart grids (Georgakopoulos & Quigg, 2017, p. 1441). So, it is still somewhat unclear what kind of applications power grids will consist of and how dependent these systems are from GNSS synchronization signals.

The present literature concerning power grids and GNSS based time synchronization mainly provide some insights for the purposes and applications of time synchronization. There seems to be a lack of in-depth descriptions of how GNSS based time synchronization is utilized in current power grids and planned to be utilized in the future smart grids. Even though many of the technologies that will be used in the smart grids are still under research and development initiatives it is important to identify the planned use cases for them. This information is crucial for determining possible threats and attack vectors based on time synchronization in the power grid environments. This raises the first research question.

Research Question 1: How is the GNSS time synchronization utilized in power grids?

Consequences of cyber-attacks are not only technical by nature. They are important issue for all organizations concerned with economic impacts and interested in protecting themselves, as they potentially have broader implications. Cyber threats are internet-

based attempts to damage, disrupt and access critical information in Information Systems (IS) (Henriques de Gusmão et. al., 2018, p. 248). The threat of cyberattacks against power systems is increasing as cutting-edge smart grid technology is being integrated into existing systems to perform monitoring, control and protection functions. Standardized internet protocols are being deployed to the power system, supervisory control and data acquisition (SCADA) systems are being connected to business networks and to the internet. All these changes introduce new cyber vulnerabilities and open possible backdoors into the systems (Xiang et. al., 2018, p. 368). The increased number of internet users is also contributing to the risk of cyberattacks. Most people accessing the internet do not have the proper training in cybersecurity, which makes them a significant point of weakness for cybersecurity in any system (Henriques de Gusmão et. al., 2018, p. 248).

Due to the advances in cyber-security malicious parties are now developing new more subtle forms of attack. These complex attacks are based on sets of simple attack methods, which individually may not seem dangerous. This poses the challenge of identifying such sets of related attacks, since data may be dispersed, processed at different times, retained in various formats or kept separate due to security policies. This adds difficulty to understand complex attacks. Advanced persistent threats have become a distinct concern, these threats are formed by well-funded organizations like cyber-warfare divisions of different governments. Their goal is to gradually gain more access into a system and remain undetected for as long as possible. These threats are harder to notice than more common types of threats and the gradual approach with attack sequences help the attackers to mask their actual goals (Lundquist et. al., 2014, p. 5). Potential weak spots of the system should be recognized so the early signs of cyber threats could be identified, and risk analysis tools and frameworks are useful to this end.

Risk analysis is an activity of high importance that organizations must perform, so attacks can be prevented, and their consequences negated (Henriques de Gusmão et. al., 2018, p. 248). Risk assessment can be used for tailoring adequate information security policies and protocols for minimizing the potential risks. Threat modeling on the other hand is

one of the most important tasks during the design phase for finding the underlying security issues in the design. GNSS time synchronization is a very specific domain and susceptible to cyber-physical attacks. For this reason, it is crucial to recognize and understand the threats and determine the risks involved, so the adequate security measures can be established for all layers of the system. Recognition and establishment of security measures constitutes the second research question.

Research Question 2: How can attacks on applications utilizing GNSS-based time synchronization be carried out?

Cyber security has increasingly become a concern for the safety of the power grid applications. Even though there is a low probability for continuous large-scale cyber-attacks towards the power grids, the impacts of such attacks would be severe (Huang et. al. 2018, p. 69023). There is a clear relationship between modern power systems and information and communication technology (ICT), that supports the operation and management of power grid. Wide-area monitoring and control (WAMC) systems are envisioned as the future of power grids. At their core they are power system applications, that are supported by infrastructure of intermediary devices and systems which process and store real-time information (Chenine et. al., 2014, p. 633).

Global positioning system (GPS) addresses the need for highly accurate and stable time without extra ground-based infrastructure. Due to this GPS based time synchronization devices are widely used in smart grid monitoring systems and measuring devices equipped with a GPS signal receiver are installed throughout the smart grid systems. The measured data is sampled periodically, and a GPS timing signal received by the device triggers the sampling. By providing a grid-wide reference time for sampling, the system is able to cope with delays in the data transmission and work in synchronous manner (Zhang et. al., 2013, p. 87). The operation performance is a fundamental requirement for the power grid, control and protection functions are designed for fast action, but other qualities like cyber-security cannot be overlooked. Generally, the focus has been placed

on improving the functionality in power grid applications and their supporting systems. Since WAMC systems are real-time by their nature they are vulnerable to variations. (Chenine et. al., 2014, p. 640). Even though GNSS based time synchronization schemes the preferred choice of electric industry, they are heavily interconnected with underlying IT-infrastructure and their signals are vulnerable to various kinds of disruptions. The relationship with IT-infrastructure allows multiple points of entry for malicious attackers and causing disruptions to the GNSS signals is fairly simple, which makes GNSS based time synchronization an appealing target and a considerable security risk.

Research community has shown a lot of interest towards GNSS security. There is a considerable amount of literature on attacks against navigation system signals, most of which focus on GPS as it is the most widely used GNSS. The results from these studies can however be applied to other systems (GLONASS, Galileo, BeiDou), as they all work on same principles and share many common characteristics (Moussa et. al., 2016, p. 1963). GNSS signal and data spoofing have led to design of signal and receiver technologies, which try to address these problems in signal, data and receiver levels. It is imperative for next generation secure GNSS receivers to protect cryptographic functions and keys, software, hardware and data communication to prevent spoofing attempts and data access by hostile parties (Pozzobon et. al., 2010, p. 1). The downside to this is that cybersecurity aspects can have adverse effects to grid operation by disrupting the data flow, but security incursions and their resulting impact can have devastating outcomes (Chenine et. al., 2014, p. 640). Most of the studies concentrating on GNSS security focus on deterring and mitigating the effects of ongoing attacks with distinct well-known methods. Only few studies seem to address how the security threats affect the GNSS time synchronization in general. This forms the basis for the third research question.

Research Question 3: What possible consequences can cybersecurity threats in GNSS based synchronization have?

Even though extensive research on cybersecurity threats has been made before it has not been applied to the field of GNSS based time synchronization in power grids on a system-wide scale. The purpose is to recognize threats and potential weak spots of different systems and assess their risk level by using suitable tools and frameworks. This study aims to find ways to manage and mitigate the identified risks and serves as the basis for the research problem of this study.

Research problem: How could GNSS based synchronization threats be managed and mitigated in electrical distribution systems?

3 Theoretical framework

Risks are involved in all activities of the society. Organizations manage risks by identifying and analyzing them, then evaluating the risks by considering the need for mitigations for reducing the risks to acceptable level. The objective of risk assessment is to support decision-making by identifying and describing the risks, so the potential impacts can be analyzed (Tiusanen, 2008, p. 463).

Comprehensive risk identification is critical, since it is important to consider possible causes and potential consequence scenarios. The proactive analysis and control of risks is growing increasingly important as new innovative digital technologies increase the complexity of systems and there is no failure data available for certain applications. The analysis for new unique technological systems should begin with identification of all potential hazards and assess whether the events are possible or not (Tiusanen, 2008, p. 464). This section describes the theoretical background and methodologies used in this work to identify threats and to evaluate risk.

3.1 Threat modeling

The idea behind threat modeling is to understand potential security risks to a system, so the risks can be determined and appropriate mitigations established. Threat modeling also helps to create awareness of security dependencies and provides the ability to convert technical risk into business impact (Howard, & Lipner, 2006, p. 101). Threat modeling is a method of identifying significant and likely threats for well-defined scenarios, ranking their potential damage and finding cost-efficient ways to mitigate the high priority threats. Threat modeling frameworks and tools are used by various industries, but it is often associated with software development. It is a process which the defender can use to quantify threats, risks and mitigations for comparing the implemented plan against the reality of what occurs (Grimes, 2017, p. 211).

Threat model is a way to anticipate the threats that could affect your system. There are numerous ways to threat model, some of the strategies that can be employed include the modeling of assets, modeling of attackers or modeling of the system (Shostack, 2014, p. 29). Threat modeling reduces risks and makes people consider various threats and risks in a given situation. It allows multiple threats to be assessed against each other, mitigations to be developed and evaluated, and this possibly leads to cost-effective and useful mitigations (Grimes, 2017, p. 211).

There are many different methodologies for threat modeling, they are usually known by their acronyms such as STRIDE, PASTA, VAST etc. Each model attempts to shed some light into the totality of the project under consideration. This is often performed with brainstorming, diagrams and detailed descriptions of the processes. Afterwards all the potential threats are considered and ranked by their likelihood and potential damage. The threats that are most likely to cause significant damage are considered first and then mitigations are developed and assessed according to their suitability and cost-efficiency (Grimes, 2017, p. 212).

3.1.1 Threat modeling process

The main products of threat modeling process are documents that describe background information about the system and define a high-level model of the system, in many cases the high-level model is represented in data flow diagram (DFD). Other artifacts produced during this process are list of assets that require protection, threats ranked by risks and possibly a list of mitigations (Howard, & Lipner, 2006, p. 103).

As problems tend to be caused by the data flow instead of the control flow, the data flow models are ideal for the purposes of threat modeling. DFDs consist of enumerated elements connected by data flows that interact with external elements. Despite the fact that the arrows in DFDs are presented as one way arrows the data flows in two ways in almost all cases (Shostack, 2014, p. 44). The elements of DFD can be seen in the table 1.

Table 1. Elements of DFD (Shostack, 2014, p. 45).

Element	Appearance	Meaning
Process	Rounded rectangle, circle, concentric circle	Any running process
Data flow	Arrow	Communication between processes, or between processes and data stores
Data store	Two parallel lines with a label between them	Things that store data
External entity	Rectangle with sharp corners	People, external processes outside of control etc.

The table above presents the elements of classic DFD model, but DFD has undergone some modernization to make it more usable. Shostack (2014, p. 45) offers some changes to the classic model. Processes are substituted with rounded rectangles and trust boundaries are introduced. A modern version of the model is illustrated in the figure 1.

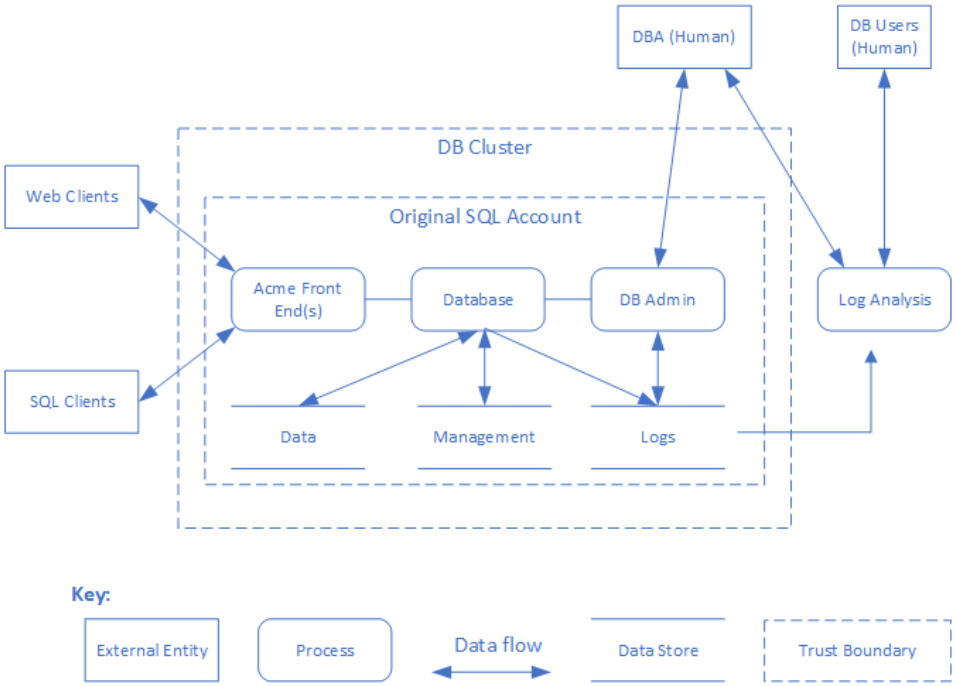

Figure 1. A modern DFD model (Shostack, 2014, p. 46).

After the model of the system has been drawn, there are two ways for adding the boundaries: Known boundaries can be added and additional ones can be sought, or principals (entities with different privileges) can be enumerated and the boundaries can be discovered with their aid. When starting with known boundaries the enforced trust boundaries like data storages, devices, network segments etc. are added and labeled. With principals the starting point should be one end of the privilege spectrum, and the boundaries are added when the entities with different privileges interact with each other (Shostack, 2014, p. 50).

Structured approaches like scenario analysis, pre-mortems and literature reviews can help to bring some structure to threat modeling although they are not great (Shostack 2014, p. 54). Threat modeling is a critically important task for understanding how systems can be attacked and defended. Threat modeling processes can help to systematically uncover threats to applications, rank the risk of threats and to determine appropriate mitigations (Howard, & Lipner, 2006, p. 130).

There are multiple ways to threat model, some of these strategies involve modeling assets, modeling attackers, or modeling software (Shostack 2014, p. 29). Asset-centric strategy concentrates on all the individual assets entrusted to the system, these assets are system or user level resources that are associated with certain value. Modeling attackers focuses on identifying the attackers and their goals, the aim is to predict how the goals can be achieved by the attackers. Software-based strategy involves the design model of the system and focuses on all possible attacks, that target the elements of the model (Martins et. al., 2015, p. 115).

3.1.2 Attack Surface Analysis

Attack Surface Analysis (ASA) concentrates on understanding what constitutes the attack surface for applications and systems. All useful applications provide interfaces for the users and attackers alike and system access offers exploitable vulnerabilities for malicious users. The attack surface is the union of code, interfaces, services and protocols

available for all users (Howard, & Lipner, 2006, p. 78). A system exposing a lot of interfaces presents a larger attack surface than one that presents few (Shostack, 2014, p. 6).

The focus of ASA is on reducing the amount of code that is accessible to untrusted users. The reduction of attacks surface is usually achieved by understanding the system's entry points and the levels of trusts required for access (Howard, & Lipner, 2006, p. 79). Attack surface is a concept closely related to the trust boundaries, it is a trust boundary and direction from which an attack could be launched. For this reason, many people treat the terms as interchangeable (Shostack, 2014, p. 6).

3.1.3 Attack trees

Attack trees are a pragmatic way of describing threats to different systems. They are used for representing one or more attacks and they consist of attacker actions, which aim to a specified goal. Attack trees are widely used in industrial practice and have gained a high popularity, even though they have received a lot of criticism. Since the formal semantics for attack trees were not originally provided, the ambiguity of their meaning has often been questioned. Nowadays this criticism is unfounded since original attack trees and its variants have been clarified and formalized through multiple research articles (Mantel, & Probst, 2019, p. 184).

The purpose of attack trees is to find threats and to organize the ones, that have been already found. They provide a formal and methodical way of describing the security system based on different attacks. The attacks are represented in a tree structure, the root node represents the goal of the attacker and the leaf nodes represent the different ways to attack, so the goal can be achieved (Shostack, 2014, p. 87). An example of an attack tree in the context of ATM machine is shown in the figure 2.

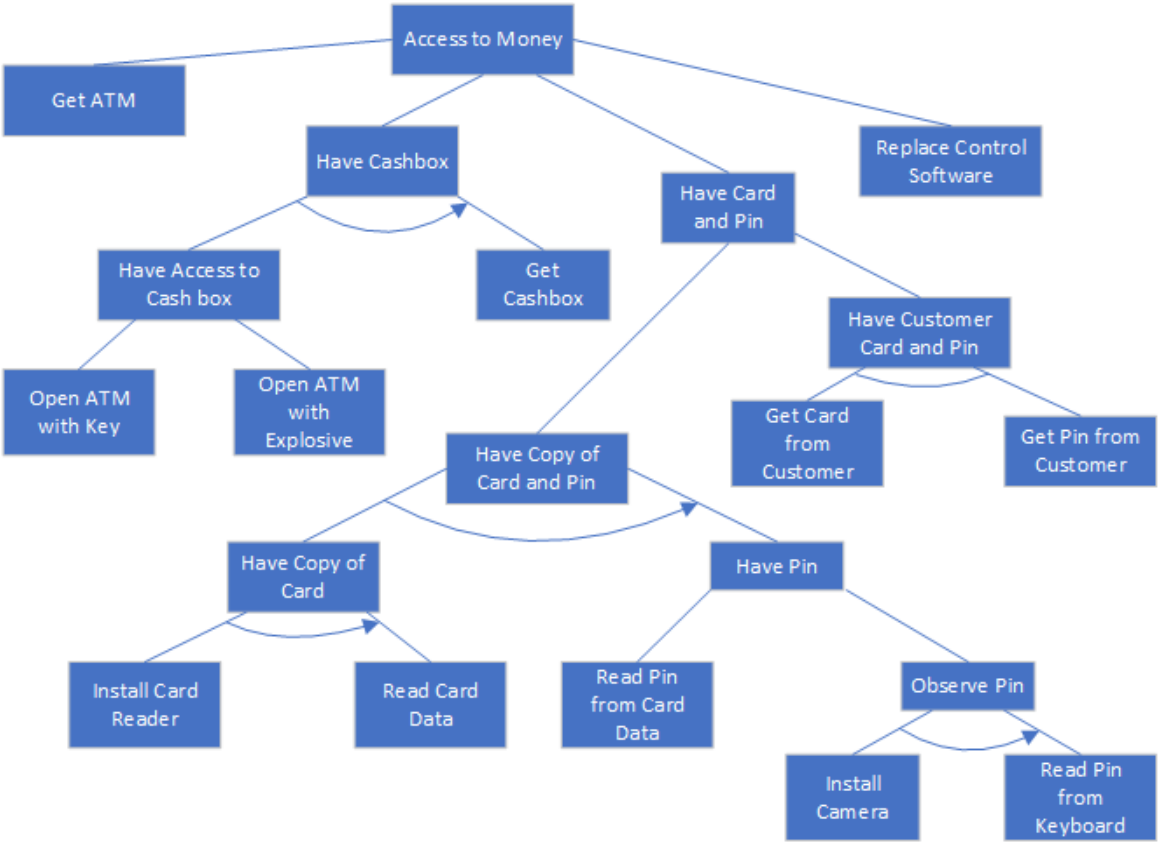

Figure 2: Attack Tree for ATM machine (Mantel, & Probst, 2019, p. 186).

For the purpose of examination premade attack trees can be used for finding threats, if they are relevant to the system under examination. Once the system has been modeled with DFD or some other form of diagram the premade attack trees can be used for analysis. The feasibility of each node in the premade tree is considered and if any of them points to a possible issue the impacts of the attack are evaluated. If there are no usable attack trees available, one can always create a project-specific tree to organize and consider threats. This approach can lead to a single or multiple attack trees and can be a useful way for presenting information about threats. Security experts may find them as a quick and useful way to examine possible threats, but they can be very hard to create at times (Shostack, 2014, 87-88).

When creating a new attack tree, one needs to decide on a suitable form of representation and select a root node. Brainstorming and literature review are useful methods for

finding threats that can be added as nodes to the tree. The completeness of the tree should be considered while the nodes are being added, the tree should not be overly full, and one should make sure that it contains the right threats. When the tree is complete its presentation should be evaluated, so its usefulness to others can be ensured (Shostack, 2014, p. 100).

3.1.4 STRIDE

STRIDE approach was invented by Loren Kohnfelder and Praerit Garg and the acronym stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Shostack, 2014, p. 61). STRIDE is used for analyzing vulnerabilities against system components which can be exploited to compromise the whole system. At first the system has to be decomposed into its logical and structural components. These components can be internal processes within the system or external elements which have access to the system. After this a DFD is plotted for each of the components to visualize the functionality within or outside the system. The next step is to identify the threats from the DFD of each component and place them under the STRIDE categories. The final step to STRIDE approach is to plan effective mitigation strategies, once the threats have been identified and the vulnerabilities causing the threats have been investigated (Khan et. al., 2017, p. 2). Detailed mnemonics of STRIDE can be seen in the table 2.

Table 2. STRIDE mnemonics (Shostack, 2014, p. 62-63).

THREAT	PROPERTY VIOLATED	THREAT DEFINITION	TYPICAL VICTIMS
Spoofing	Authentication	Pretending to be something else than acclaimed	Processes, external entities, people
Tampering	Integrity	Modifying data, that is stored or under processing	Data stores, data flows, processes
Repudiation	Non-Repudiation	Claiming that you didn't do something or were not responsible. Repudiation can be honest or false.	Processes
Information Disclosure	Confidentiality	Providing access to unauthorized information	Processes, data stores, data flows
Denial of Service	Availability	Absorbing resources needed to provide service	Processes, data stores, data flows
Elevation of Privilege	Authorization	Allowing operations for unauthorized entities	Processes

Stride is a useful mnemonic for the purposes of finding threats, but it is not perfect. For this reason, multiple variants have of STRIDE have been devised to address some of its weaknesses. One of these variants is STRIDE-per-element, which makes STRIDE more prescriptive as it denotes that some threats are more prevalent than others in a diagram. This makes finding threats easier by focusing a set of threats against each element (Shostack, 2014, p. 78). Table 3. illustrates STRIDE-per-element approach.

Table 3: STRIDE-per-element (Shostack, 2014, p. 78)**.**

	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data flow		x		x	x	
Data store		x	?	x	x	

STRIDE can be used for finding threats against all kinds of systems, though it is more useful with a set of more detailed threats, that have been already recognized. There are multiple variants of this approach, which can be used to add focus and attention on different details. STRIDE-per-element is a useful example of this, and it can be customized according to the needs (Shostack, 2014, p. 78).

3.2 Data gathering

Data for the analysis is collected through literature review, as stated in subsection 3.2 this is a structured approach to threat modeling. Shostack (2014, p. 33) also suggests that literature review is helpful starting point for threat modeling and to learn what has happened in the past.

High level descriptions of the Global Navigation Satellite Systems, Power grid protection and control systems and the devices involved are provided. This is done in order to gain insight about the systems in place. The literature review will be conducted by using wide variety research articles and books covering these subjects, the collected information is composed into descriptions of the system, subsystems and their components. These descriptions are utilized in constructing system diagrams for the threat modeling and analysis that is performed later. The examination of the systems and their components also serves as source for determining possible consequences, which attacks and involuntary disruptions can have on different systems. This will also help in forming different mitigation strategies and in revealing weak points in the infrastructure.

3.3 Risk assessment

One of the most widely used tools for used for screening risks are the risk matrices. Risk matrix is also known as consequence-probability matrix is utilized for ranking risks based on the risk level. When considerable amount of risks have been identified, the risk matrices are useful for defining which risks need further analysis, which risks need to be handled first or which need the attention of a higher level of management. ISO 12100 standard describes a risk-estimation method, which utilizes risk matrix (Tiusanen, 2008, p. 470). A lighter variant of risk matrix is used on this work, since the method described in ISO 12100 is quite cumbersome. The risk matrix is depicted in the table 4. below and portrays the risk level based on probability and the severity of the consequences in a similar manner as the ISO 12100 risk-matrix.

Table 4. Risk matrix

	Probability		
Severity	**Low**	**Medium**	**High**
High	Moderate	High	Critical
Medium	Low	Moderate	High
Low	Negligible	Low	Moderate

3.4 Research process

The actual research process takes an assets-centric approach to threat modeling based on generic use cases. The systems and the components presented in the use cases are modeled as DFDs. The elements in the DFD models are first examined by utilizing the STRIDE-per-element approach. As a result, the different threat types, that the elements are exposed to are recognized. These recognized threat types are used as foundation for identifying more specific threats for the systems, by iterating across the trust boundaries and elements in the DFDs. The identified threats are then presented in a table indexed by the diagram element and threat type, an example can be seen in the table 5.

Table 5. Threats by diagram element and threat type

Diagram element	**Threat Type**	**Threat**
Database	Tampering	SQL injection
Data store	Denial of Service	Filling up the store
Logs	Information Disclosure	Information extracted

The artifacts created are also complemented with attack trees for demonstrating how some of the threats could be realized by the means of an attack. The most prominent threats and their root causes are composed into a list, which serves as a basis for uncovering different kinds of mitigation strategies for the threats. The proposed mitigation strategies are uncovered by investigating a variety of sources through literary review. The utilization and viability of different mitigation techniques is also briefly addressed as they are presented in this study.

4 Global navigation satellite systems

Global navigation satellite system is a generic name for a group of satellite constellations. These satellite constellations broadcast their position and timing information continuously through radio frequencies. GNSS receivers can determine their own position through the radio signals transmitted by the satellite constellation. Being acquainted with GNSS is imperative for engineers, scientists and civilians a like, due to the range of applications. GNSS has been applied for personal and vehicle navigation, aviation, defense, transportation, science, security, telecommunication and survey for example. Its popularity is due to high global availability and continuous service (Swamy, 2017, p. 1155).

Even though there are multiple different GNSS implementations their basic operating principles are essentially the same. In this chapter the basic operating principles of GNSS are introduced and afterwards the most commonly used systems are conversed in more detail. The capabilities and the features of different systems are introduced and compared.

4.1 Functional segments

Architecture of Global Navigation Satellite Systems consists of three functional segments. Each GNSS has their own independent space, control and user segments. Typical GNSS architecture and the different segments can be seen in the figure 3. which is based on the architecture of GPS.

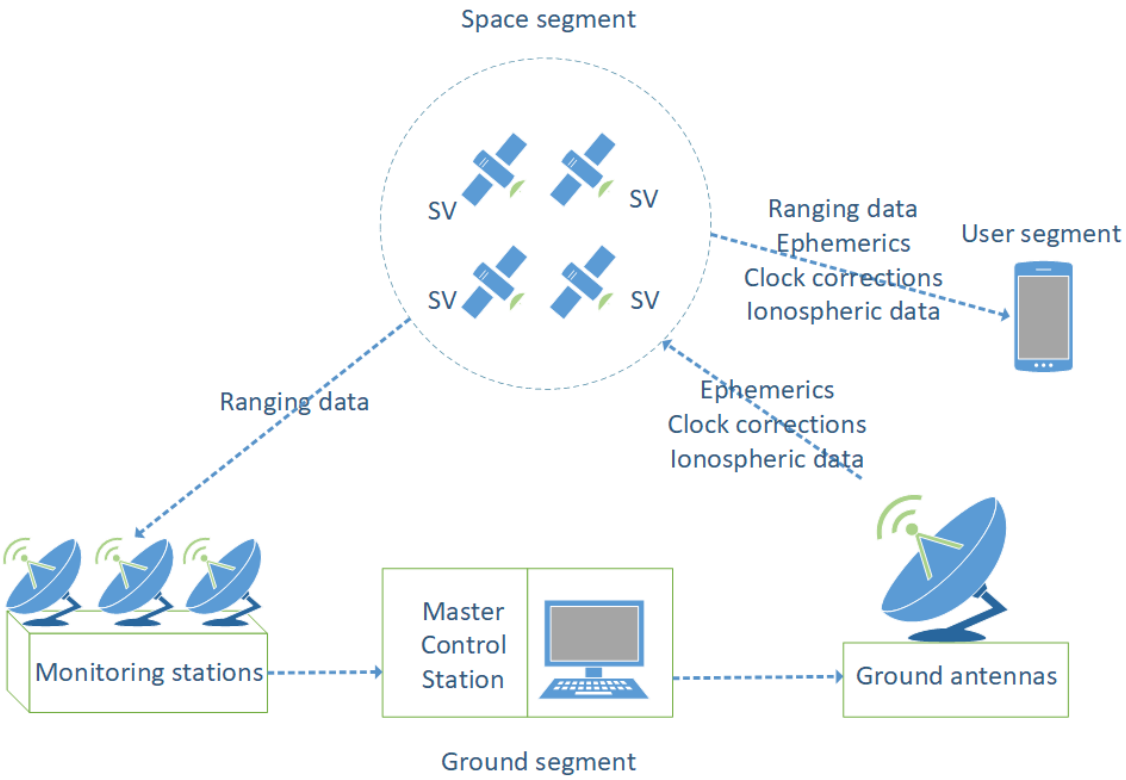

Figure 3. GNSS architecture modelled after GPS (Swamy, 2017, p. 1157).

The space segment consists from satellites which are usually referred to as a constellation. Constellation broadcasts signals which both the control and user segments utilize for their uses (Groves, 2013, p. 162). The satellites reside in medium earth orbit (approximately 20 000 km altitude), even though this varies slightly between different systems. This high altitude allows greater coverage area for the signals and the constellations are arranged in a formation, which allows receivers to pick up signals from at least four satellites at any time (Bhatta, 2010, p. 27). These satellites are referred as Space Vehicles (SV) in some literature. Typically, they weight around 1000 kilograms equipped with solar panels. Fully operational constellations contain at least 24 satellites and constellation has to be distributed across several non-parallel orbital planes (Groves, 2013, p. 162). When compared to geostationary satellites with equatorial orbits the GNSS orbital planes are inclined for better coverage in polar regions as can be seen in the figure 4.

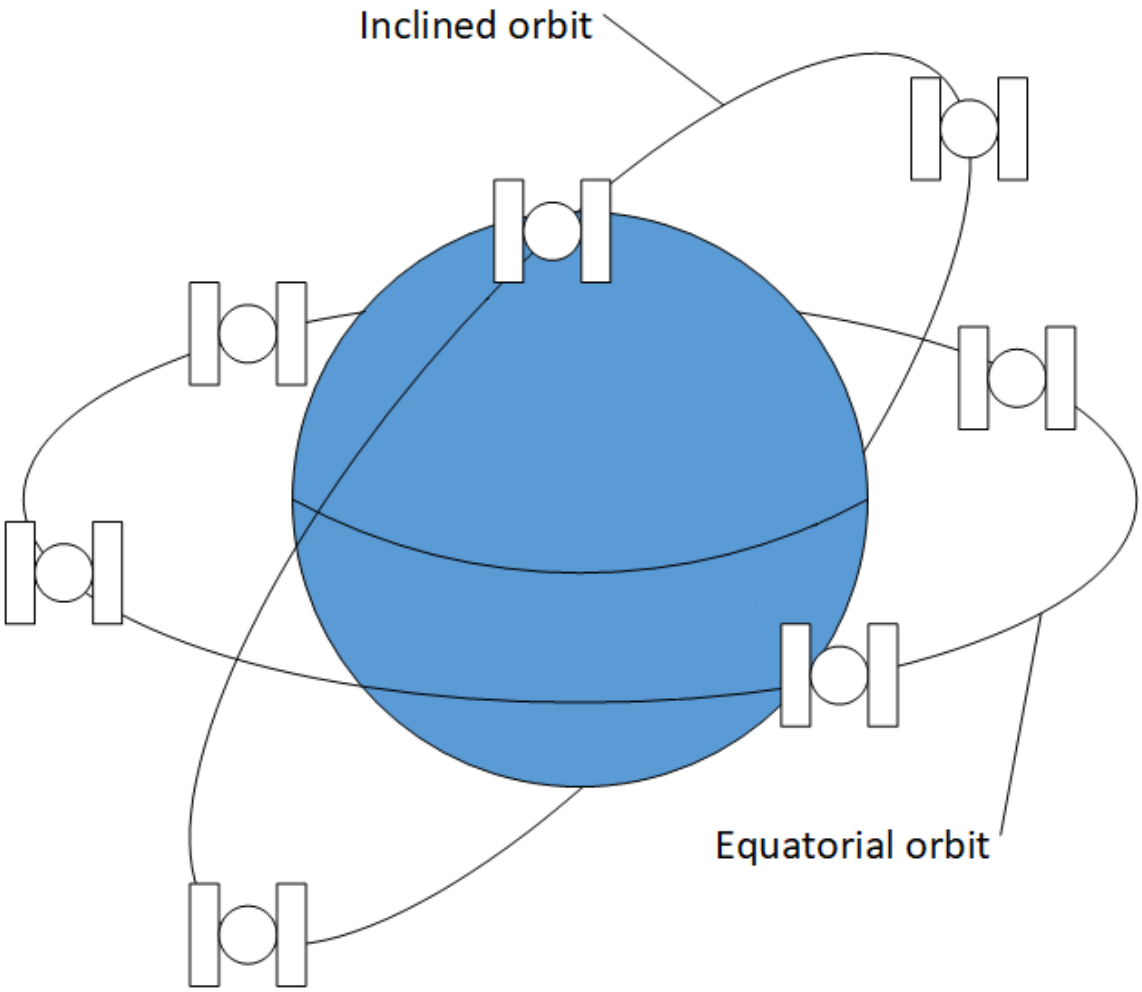

Figure 4. Equatorial and inclined orbits (Groves, 2013, p. 301).

GNSS satellites broadcast signals in several different frequencies. These signals can contain both ranging codes and navigation data messages. Ranging codes enable the user segment to determine the signal transmission time, while the navigation data message contains the data for determining the satellite position (Groves, 2013, p. 162).

The control or ground segment comprises of network of monitoring, control and uplink stations. Monitor stations are responsible for obtaining the ranging measurements from the satellites and relaying these to control stations. The monitoring stations are at precise locations and are equipped with synchronized clocks (Groves, 2013, p. 162-163). Monitoring stations track the satellites constantly and relay the information to a master control station. The information provided is then adjusted with precise orbit and clock

correction coefficients and forwarded to uplink stations (Bhatta, 2010, p. 27). This allows the ranging measurements to be used to determine the satellite orbits and to calibrate the clocks on board the satellites. The control stations compute the navigation data messages for each satellite and determine if some precautionary measures need to be taken. The computed information is then sent to the satellites via uplink stations. Most of the measures taken are small corrections known as station keeping for maintaining the correct orbits of the satellites. Major relocations are only performed during the event of satellite failure, the failed satellite is moved to a different orbit and a new satellite is moved to take its place (Groves, 2013, p. 163).

User segment consists of receiving equipment and GNSS receivers are just a part of the user segment. Antennas are used to convert the received GNSS radio signals into electrical signals, which are the input for the GNSS receivers. The receiver demodulates the signals by using a clock which serves as a reference time. Ranging processor is used to determine the distance between the antenna and the satellites. It also controls the receiver and decodes the navigation messages. Then the navigation processor calculates a position, velocity and time (PVT) from the ranging measurements (Groves, 2013, p. 163).

GNSS user equipment come in various forms due to different applications. They can be supplied as complete units with external or integrated antennas and can support multiple GNSS. The receiver and navigation processor can be supplied as a single module, which is often called original equipment manufacturer (OEM) receiver. OEM receivers require external power supply and an antenna. They may also be supplied as a simple chipset where calculations are performed by the host system's processor. Consumer grade devices are often cheap with a relatively poor accuracy and only support a single frequency. Professional grade devices are designed to be highly accurate and reliable, they often support multiple frequencies and cost a fortune compared to the consumer grade devices. Finally, there are military grade equipment, which are designed to be extremely robust and use separated signals where available (Bhatta, 2010, p. 45-46, 228).

4.2 GNSS Signals

Signals of GNSS are broadcasted within the L-band region (1-2 GHz) of electromagnetic spectrum in most cases. Satellites can transmit signals in several different frequencies and there may be multiple signals transmitted on each frequency (Groves 2013, p. 303). There are two types of information carried by the GNSS signals. Ranging codes, that measure the distance to the satellite and navigation codes also known as data messages. Navigation codes contain status information about the constellation, time information and ephemeris data for calculating the satellite's position. These codes are transmitted on carrier signals and both the codes and carrier signals can be used to determine the ranges (Bhatta, 2010, p. 74).

The basis of GNSS is trilateration, which means distances between satellites and the receiver is calculated to determine the position of receiver. The distance is measured with the signals that are broadcasted from the satellites to the receiver in the microwave area of the electromagnetic spectrum. GNSS could be described as a passive system, since only the satellites transmit signals. This means that there is no limit how many receivers can monitor the signals without causing any disruption. The downside to this is that the GNSS signals have to contain large amounts of information, so the receiver can determine its own position (Bhatta, 2010, p. 82).

Time measurement is critical for GNSS positioning. Since GNSS signals only travel one way to the receiver, the satellite has to mark the departure time of the signal and the receiver has to mark its arrival time. The range measurements depend on the travel duration of the signals, so the elapsed time has to be determined by decoding the signal itself. Since the signal is traveling through the atmosphere, it must also provide some atmospheric delay information to the receiver, so the elapsed time can be estimated more accurately (Bhatta, 2010, p. 82).

GNSS positioning requires ranging information from at least four satellites. Since the receiver must be able to match all the signals it is tracking along the location of the transmitting satellite, the receiver has to be able to identify the source of transmission. This means that the signal has to carry identification information of the satellite and information for finding other satellites as a precaution. The signal also carries health information about the satellite to determine the reliability of received data in case the satellite is malfunctioning (Bhatta, 2010, p. 82). In many cases GNSS signals are a combination of carrier consisting of spreading or ranging code, and navigation data. In majority of the cases, the code and data are arranged to carrier with biphase shift key modulation (Groves 2013, p. 167).

4.3 Timing receivers

GNSS provide atomic Coordinated Universal Time (UTC) time to users and enables precise synchronization for multiple applications. Many of these applications are critical for functioning modern economy and it is likely that there will be even more GNSS-based timing applications as the technology matures (Kaplan & Hagerty, 2017, p. 934). In GPS the current time is determined by the atomic clocks in the satellites and modulated to as a navigation message on top of the coarse acquisition (C/A) ranging code. The receivers generate their own local replicas from the C/A codes received from each satellite and estimate the time delta for aligning the local replicas to the received copy. The receivers also decode the navigation data for calculating the satellites position and clock offsets and this information is used for estimating the 3D position and time (Nighswander et. al., 2012, p. 450).

The standard pulse-per-second (1-PPS) output of GNSS receivers are widely used in timing and time synchronization due to the high accuracy and long-term stability. 1-PPS pulse is used for synchronizing devices to UTC or GNSS system time. In a typical design 1-PPS output signal is locked with the recovery signal of GNSS 1-PPS. (Niu et. al., 2015, p. 141; Jianfeng et. al., 2016, p. 1). The operating principles of numeric controlled oscillator (NCO) based pulse generation is presented figure 5.

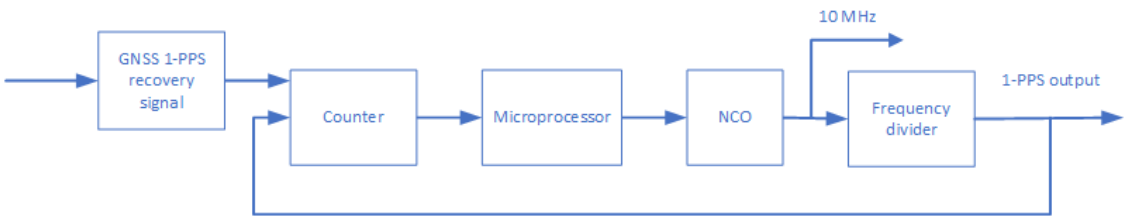

Figure 5. 1-PPS pulse generation (Jianfeng et. al., 2016, p. 1).

The counter represented in the figure 5. measures the difference between NCO 1-PPS and GNSS 1-PPS recovery signals. Microprocessor receives the time difference between the signals and generates control and phase control words for the NCO, which are used for tuning the NCO. The real time 1-PPS phase calibrations are used to compensate the difference between the output signal and GNSS system time (Jianfeng et. al., 2016, p. 1).

Some timing receivers also provide GNSS based time-synchronization through IRIG Time-synchronization signal formats. According to Behrendt & Fodero (2006, p. 4) IRIG-B is a widely used format for distributing time signals to Intelligent Electronic Devices. IRIG-B provides time to devices once per second in a binary coded decimal (BCD) format, which contains seconds through the day of the year. The format allows multiple configurations, by altering attributes which indicate the modulation technique, carrier resolution and the coded expressions. The most used forms for general time synchronization are B122 (seconds through day of the year in BCD on a 1 kHz carrier) and B002 (a level shift format containing seconds through day of the year in BCD).

Even though the GNSS time is considered highly accurate and stable, the GNSS signals are still vulnerable to jammers and Radio-Frequency Interference (RFI) signals, due to the low-power of the transmitted signals. The ever-growing presence of interference sources in urban areas has been highlighted in recent studies (Querol et. al., 2018, p. 155). However, the results of Niu et. al. (2015, p. 149) showed that many of the commercial receivers can provide qualified 1-PPS signal for time synchronization under

nominal signal conditions. The timing accuracy can be maintained at microsecond level even after losing the lock on the GNSS satellite signals often for tens of minutes.

4.4 Navigation satellite systems

This section offers a brief introduction of different navigation satellite systems, that are operating on a global scale. There are currently four different navigation satellite constellations in operation: GPS, GLONASS, Galileo and BeiDou. As mentioned previously, many of the same operating principles apply to all of these systems and some of them are even capable of supporting each other to a limited extent. The major differentiating factors between the systems are the technology they are based on, the composition of their constellations, their operating frequencies, the services they offer and the administrative bodies. The following table 6. displays some of the differences between the systems. The operating frequencies presented in the table were retrieved from an image in Navipedia (Navipedia, 2020).

Table 6. Comparison between different GNSS constellations

System	Administrative bodies	Orbital planes	Planned satellites	Operating Frequencies	Services
GPS	GPS directorate	6	30	1176,54 MHz 1227,60 MHz 1575,42 MHz	SPS PPS
GLONASS	Roscosmos	3	24	1246,00 MHz 1602,00 MHz	ST VT
Galileo	European Commission European Space Agency	3	30	1176,45 MHz 1207,14 MHz 1278,75 MHz 1575,42 MHz	OS HAS PRS SAR
Beidou	China National Space Administration	3	35	1176,45 MHz 1207,14 MHz 1268,52 MHz 1561,098 MHz 1575,42 MHz	RNNS RDSS

4.4.1 Global positioning system

NAVSTAR GPS was developed for the purposes of United States military as a navigation system. The system is controlled by GPS directorate, which is operating under United States Department of Defense. Even though the development was started in 1973 the initial operational capacity was reached in 1993 and the full operational capacity at the end of year 1994. GPS offers two varieties of navigation services. Standard Positioning Service (SPS) is open for all the users and the Precise Positioning Service (PPS) which has encrypted signals and is only available for users licensed by the United States' government (Groves, 2013, p. 213).

The GPS constellation consists of 24 satellites, even though there are 28-30 satellites in the GPS space segment. The additional satellites improve the accuracy of the positioning by providing more measurement data and serve as spare satellites for the constellation. In GPS there are six near-circular orbits where the satellites are placed at the nominal altitude of 20200 kilometers. The orbits have approximately 55 ° inclination relative to equator and are separated by 60 ° right ascension. Four of the satellites on each of the six orbital planes are positioned in a way, that a receiver on earth can always receive signals from at least four satellites, and there are always 12 satellites on either side of the hemispheres. There are multiple different generations of GPS satellites, which coexist on the orbit as can be seen in the table 7. As a result of this the capability and functionality of the satellites vary (Bhatta, 2010, p. 29).

Table 7. Present and Future Generations of GPS satellites (Groves, 2013, p. 172)

GPS Satellite Block	Launch Dates	Number of Satellites
Block IIA	1990-1997	19
Block IIR	1997-2004	12
Block IIR-M	2005-2009	7
Block IIF	2010-2015	12
Block III	2015-2024	24 (planned)

The latest generation of satellites in GPS is Block III, also known as GPS III. GPS III satellites will change the existing operational paradigms of the system. It will improve operator capabilities as new uplink/downlink and crosslink communication architecture is introduced. Crosslink communication makes it possible to contact all satellites through one satellite, which enables continuous connectivity and near real-time navigation updates and monitoring. When fully operational, GPS III will provide significant operational advantages for the system operators and users L-band signals. The whole system's responsiveness and flexibility will improve and some of the features will provide better positioning and timing performance for all users when compared to previous generations. GPS III will also boost the signal power and enable improvements to user equipment, which will improve the performance under stressed environments e.g. when the received signal is being disrupted by jamming. The system will also include NAVWAR spot-beam antenna for directed higher power Military-Unique signals (Luba et. al., 2005, p. 12-14). GPS III will also feature new signals L1C and L2C for civilian users, M-code for military usage and L5 safety of life signal.

L1C is a new signal that will maintain backwards compatibility with old L1 C/A signal. It will feature Multiplexed Binary Offset Carrier scheme, which enables international cooperation by interoperability with other satellite navigation systems. L1C was originally developed by the United States and Europe as a common civil signal for GPS and Galileo to enable interoperability. L2C is specifically designed for commercial needs and in combination with L1 C/A signal through dual-frequency receiver it enables ionospheric correction to boost the accuracy. The existing dual-frequency operations will receive faster signal acquisition, improved reliability and greater operating range by providing higher power than L1 C/A signal. First satellite featuring L2C was launched in 2005, but it remains pre-operational and caution should be employed while using it before it is declared operational. L5 signal is designed for the demands of safety-of-life transportation and high-performance applications. It is reserved for aviation safety services and features higher bandwidth and advanced signal design. In combination with L1 C/A it will

improve the accuracy and the robustness of the system. At the moment L5 is also considered as pre-operational (National Coordination Office for Space-Based Positioning, Navigation, and Timing, 2019). GPS III will improve the accuracy, integrity and the availability for both civil and military users, once it is fully operational (Bhatta, 2010, p. 33).

4.4.2 GLONASS

The Global Navigation Satellite System (GLONASS) is the Russian Federation's counterpart to GPS. Like GPS the GLONASS program was also initiated to support military needs in mid-1970s by the Soviet Union and the system was declared to be fully operational in 1996. Although soon after its completion the constellation degraded as some of the older satellites failed in orbit. The restoration process back to full global service took until 2011 to be completed (Kaplan & Hagerty, 2017, p. 191-192).

The constellation of GLONASS is composed of 24 active satellites and six spares. The satellites are positioned in a 19100-kilometer orbit and have an inclination of 54,8 °. They are uniformly located in three orbital planes and each plane contains eight satellites. The current orbital configuration and system design provides navigation service up to 2000 kilometers above Earth's surface and the 24-satellite provides continuous four satellite visibility for over 99 % of the Earth's surface. (192) The GLONASS constellation is populated with two types of satellites: Glonass-M which is a modernized version of the satellites launched between years 1982 and 2005, and Glonass-K first launched in 2011. There are also plans to launch more advanced Glonass-K2 satellites in the future (Kaplan & Hagerty, 2017, p. 192-194).

GLONASS also offers an authorized military navigation service and an open civil service like its GPS counterpart. Both services utilize L1 and L2 frequency bands on their transmissions and the more modern satellites also provide civil service in the L3 frequency band. The high accuracy service is known as VT and is reserved for the military, this signal is not encrypted but is nevertheless equipped with anti-spoofing capability. Since VT is reserved strictly for military use there is little information available on it. The designation

for the open service is ST and is used for military, civilian and commercial purposes. Russia has also developed several types of GLONASS differential services, which improve the performance of positioning or timing by using radio beacons (Kaplan & Hagerty, 2017, p. 203-207; p. 709).

4.4.3 Galileo

Galileo is a navigation satellite system, which is governed by the European Union (EU). As the executive body of the EU, the European Commission (EC) acts as the Program Manager for the European GNSS program, while the European Space Agency (ESA) functions as the technical design authority for the Galileo navigation system. In 1999 EC and ESA recognized the need for an independent European GNSS, and based on previous experience on the European Geostationary Navigation Overlay Service (EGNOS) and consultations with global stakeholders the key objectives for the European GNSS were identified. These objectives were analyzed by ESA as part of Galileo comparative system studies during the years 1999 and 2000. This led to the recommendation to develop Galileo with similar design as the existing GPS, making Galileo interoperable with other SATNAV systems (Kaplan & Hagerty, 2017, p. 218).

Galileo has been specifically designed for the worldwide civilian use and has been developed with incremental approach. The major implementation phases of Galileo include in-orbit validation (IOV) and full operational capacity (FOC) phases. The IOV phase provided the end-to-end validation of the Galileo system concepts with incomplete satellite constellation and a ground segment prototype. This allowed the testing of fundamental system concepts before the development of elements for the final system was complete. As the IOV Test Campaign was completed all the objectives of IOV phase were accomplished and all the core functions of the final system have been successfully tested (Kaplan & Hagerty, 2017, p. 218).

The complete constellation of Galileo will consist of 24 active satellites on three orbital planes, with two spare satellites on each plane. The satellites are placed in the nominal

altitude of 23222 kilometers and the orbital planes are equally spaced with 56 ° inclination relative to the equator. The driving factor for the orbit selection of Galileo constellation has been the optimal operation of EGNOS Safety of Life (SOL) service, another factor being high service availability. The constellation is currently composed of two generations of satellites. The first four satellites were launched to form the space segment for the IOV phase. The second generation consists of 22 satellites which form the core of the Galileo FOC constellation. Although the two generations of the satellites differ from each other by design they still share similar components and architecture between themselves (Kaplan & Hagerty, 2017, p. 233-234).

Once completed Galileo system is expected to meet a variety of user needs. The services specified for Galileo form the basis of the system design and operations and have been used for consolidating the main features of the system. Although the scope of defined services is limited, the Galileo system will serve a much larger range of applications. The reference services envisioned for the system in full operational capacity include Open Service (OS), High Accuracy Service (HAS), Public Regulated Service (PRS) and Search and Rescue Service (SAR) (Kaplan & Hagerty, 2017, p. 219; European Global Navigation Satellite Systems Agency, 2020).

The Galileo Open Service will provide public PVT information to users through ranging signals on three frequencies designated as E1, E5a and E5b. The OS is targeted for mass-market applications such as in-car navigation. The OS will also encompass a navigation message authentication service (OS-NMA) that entails an authentication mechanism that allows Galileo user equipment to verify the authenticity of the GNSS information and of the entity transmitting it, to ensure that it comes from a trusted source and to combat malicious spoofing of SATNAV signals (Navipedia, 2021; Cozzens, 2021). The High Accuracy Service will allow the development of professional applications and features the dissemination of value-added data in real time on a dedicated commercial service signal in the E6 band. The currently planned services provided with HAS signal are related to high accuracy and authentication. The Public Regulated Service is targeted for

government authorized users, who require higher level of protection. PRS will provide PVT capabilities with encrypted signals in the E1 and E6 bands. The access to the service will be controlled through government-approved secure key distribution mechanism and is only accessible with receivers containing the PRS security module with a valid decryption key. The Search and Rescue Service includes Forward Link Alert Service (FLS) for accurate emergency beacon alert information detection and Return Link Service (RLS) for delivering short messages to emergency beacons. RLS enables return link messages to the SAR users and can provide them with rescue operation information (Kaplan & Hagerty, 2017, p. 219-220).

4.4.4 BeiDou

BeiDou is a Chinese global navigation satellite system which is interoperable with other GNSS constellations. The BeiDou project follows a three-phase development plan advancing from regional operation to global and switching from active service to passive. The project began in 1994 as BeiDou Navigation Satellite Experimental System to provide positioning, timing and short message service to China and its surrounding environments. The first two experimental satellites of BeiDou-1 System (BD-1) were launched in the year 2000 and short after the launch the initial operational capacity was declared. The third satellite was launched in year 2003 and later that year the system was declared to have reached the full operational capacity, making China the third country to own a navigation satellite system. In 2004 the phase 2 of BeiDou development named BeiDou-2 System (BD-2) was initiated and in 2012 the BD-2 space segment was completed and began offering regional services to China and Asia-Pacific region. The development of phase 3 started in 2013 with the goal of extending the services from regional to global. The extended system is named BeiDou Navigation Satellite System (BDS) (Kaplan & Hagerty, 2017, p. 273-279).

According to the official BDS documents the global constellation will consist of 5 GEO satellites and 30 non-GEO satellites. The GEO satellites will operate on equatorial orbits on altitude of 35786 kilometers, the non-GEO satellites will include 27 MEO satellites

and 3 IGSO satellites. The MEO satellites will be evenly positioned in three orbital planes on the altitude of 21500 kilometers with an inclination angle of 55 °. The IGSO satellites will operate at the altitude of 36000 kilometers placed on three different orbits with inclination angles of 55 ° (Kaplan & Hagerty, 2017, p. 283).

Upon its completion BDS will provide users with global positioning, velocity and timing services, it will also provide wide-are differential services with better positioning accuracy for users in China and surrounding areas. Basic navigation service will be provided through RNNS service utilizing multiple frequencies with free open service for global users and authorized service for authorized users. RDSS service is a unique feature for BDS including rapid positioning, short-messaging and precision timing through the GEO satellites for the users in China and surrounding areas. RDSS was the only service type provided by the initial BD-1 system but will be incorporated in BDS with improved performance. Unlike other GNSS BeiDou will have an augmentation service integrated to its design through the multiple GEO satellites (Kaplan & Hagerty, 2017, p. 292).

5 Power grid protection and control

The purpose of power system protection is to detect faults and abnormalities to engage in corrective actions (Horowitz et. al., 2014, p. 25). Switchgear, cables, transformers, overhead lines and other electrical equipment need devices to protect them during fault conditions. The function of protection is not to prevent the faults themselves, but to take immediate action upon the recognition of the fault (Bayliss, & Hardy, 2011, p. 287).

A complex network of transmission and distribution lines and equipment are necessary for moving the electric energy from generation units to the consumer loads. The secure operation of the network is dependent on bus voltage magnitudes and angles being within tolerance (Richter, 2012, p. **21**-3). Substations are the points where transmission lines and distribution lines are connected to each other by circuit breakers or switches. This allows the control of power flows and switching operations for maintenance (Bayliss, & Hardy, 2011, p. 93). The primary plant in substations is composed of high-voltage equipment including bus bars, circuit breakers, isolators, power transformers, current transformers (CT) and voltage transformers (VT). The control equipment for the primary plant is called substation automation system (SAS) and it includes protection, control and automation devices. The connecting links between the primary plant and SAS are called process connections and they mainly compose of copper multicore cables with analog voltages and currents or digital signals (Lundquist et. al., 2012, p. 1173).

Modern substations have adopted new technology that increase the reliability of the installations and reduce their size and cost. Large amount of integration has taken place due to this and it has resulted that more conventional devices have been replaced with IEDs and SAS. IEDs are compact and cost-effective solutions that can cover protection, local control, recording, monitoring and communication in one device. Communication standards like IEC 61850 make communication protocols and formats compatible between various vendors and pave the way towards IED inter-operability. These advancements have made it possible to reduce the number of panels and wiring in a substation,

and it is not uncommon that these devices hold a large number of protection functions (Bayliss, & Hardy, 2011, p. 359).

A modern substation is designed to have one or more IEDs per High Voltage bay connected to current transformers, voltage transformers, circuit breaker, isolators etc. and communicating through Ethernet with a Substation Automation system. The protection and control system also communicates with SCADA systems as can be seen in figure 6. Though some installations segregate control and protection from each other for security reasons (Bayliss, & Hardy, 2011, p. 358).

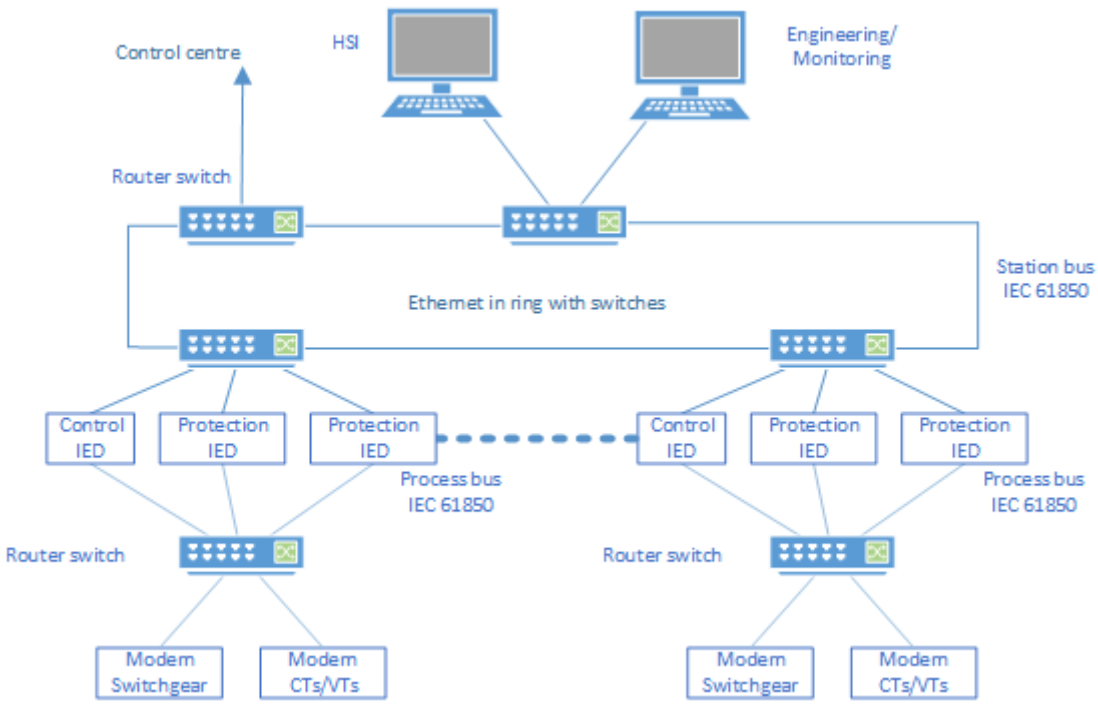

Figure 6. IEC 61850 based substation (Bayliss, & Hardy, 2011, p. 358).

Currently most of the power system protection schemes are designed around individual components, while system-wide disturbances are becoming a frequent problem. Major disturbances require coordinated protection and control to minimize the impacts in the system. Wide-area monitoring and control with advanced measurement and communication technologies are expected to provide better ways to detect and control emergency situations (Begovic, 2012, p. **4**-1).

Wide-Area Measurement Systems (WAMS) complement the traditional data acquisition functions of protection relays, fault recorders and SCADA systems. In substations protection relays and fault recorders process measurements with high data rates of thousands of samples per second, but SCADA systems usually operate on the rate of few seconds (Cai et. al., 2005, p. 1). Since actions based on conditions and events are not always enough to control the power system stability, it is possible to utilize wide-area monitoring, protection and control for more adaptive detection and control strategies. The modern wide-area monitoring systems allow advanced protection and control strategies that can be applied through implementation of new analytical tools and extensive studies (Terzija et. al., 2011, p. 81).

Increased use of WAMS is expected to result in a more efficient and reliable use of corrective actions in cases of system-wide disturbances, but this requires accurate phasor and frequency information from multiple synchronized devices. The concept of wide-area monitoring, protection and control (WAMPAC) involves the use of system-wide information to counteract large disturbances (Terzija et. al., 2011, p. 81). A generic architecture of a Wide-Area Monitoring based protection and control system can been in the figure 7.

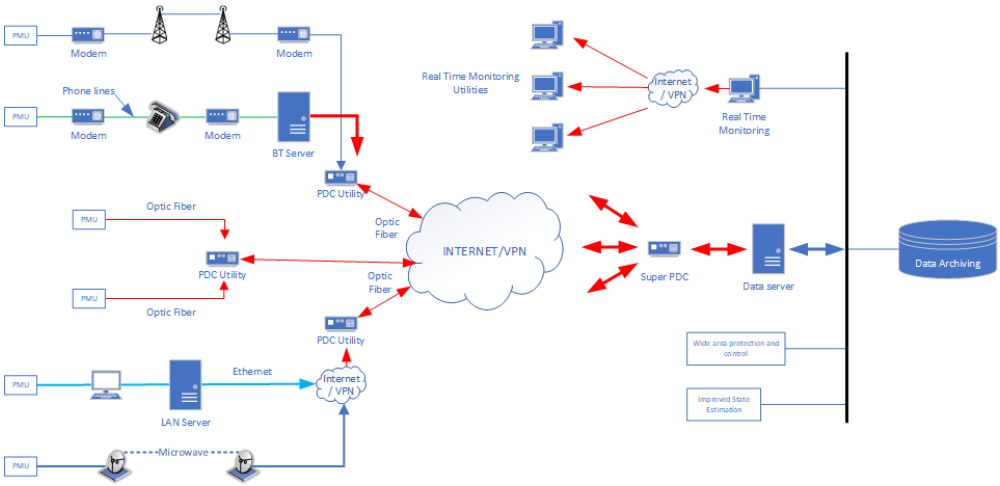

Figure 7. WAMPAC Architecture (Terzija et. al., 2011, p. 82).

The objective of WAMS is to provide real-time monitoring capabilities and to improve the situational awareness of the grid interconnection. It is an evolving infrastructure that consists of measurements from all over the grid providing grid operators with an enhanced view of grid conditions of the interconnections and facilitate confident decision making for ensuring the grid reliability (Parashar et. al., 2012, p. **15**-3).

5.1 IEC 61850 Standard

IEC 61850 is a standard that has been accepted world-wide for Ethernet-based communication in substations and it consists of 14 parts. It takes advantage of comprehensive object-oriented data model and Ethernet technology bringing reductions to the configuration and maintenance costs (Elgargouri et. al., 2013, p. 1). The IEC 61850 standard has been identified as key component for protection, automation and control for the smart grids by The International Electrotechnical Commission (IEC). The main goal of standardization of substation automation with IEC 61850 is to supply interoperable communication standards, which can achieve the current needs and support further developments in technology (Ingram et. al., 2012, p. 1173).

IEC 61850 provides high requirements for IEDs inside SA, like high-speed communication, guaranteed delivery times, multi-vendor interoperability, etc. The standard is also designed to meet the main requirements of smart grids, such as reliability, efficiency, flexibility and interoperability. The added value of using IEC 61850 is mainly linked to reduced installation, commissioning and configuration costs, but it also improves the flexibility of the grid. The standard enables new capabilities that are not viable with legacy protocols. It makes Wide-area protection schemes much more viable as the devices are already connected to a network (Elgargouri et. al., 2013, p. 3-4). Even though IEC 61850 does not actually belong to the scope of this thesis, a quick introduction for it was necessary. The standard sets certain limits and defines some concepts, which will be referred in the course of this thesis.

5.2 GNSS in power grids

Many modern applications in power systems rely on common and precise time between different IEDs that run them. Some examples of applications that require submicrosecond accuracy for time synchronization are Synchrophasors, Sampled Values (IEC 61850-9-2) and traveling wave fault location (Watt et. al., 2015, p. 1). Intelligent Electronic Devices with special functions like line differential protection can be provided with GPS information to achieve highly reliable microsecond accuracy time stamps (Bayliss, & Hardy, 2011, p. 359). Using an external synchronizing pulse which is obtained from GPS receiver a common time reference can be placed for the measurements in any computer-based relay (Begovic, 2012, p. **4**-7).

Already various devices and applications in the power grids are utilizing GNSS receivers and signals in the power grid. As is the case with previously discussed WAM systems, which depend on highly accurate information provided by multiple synchronized devices. This section aims to provide more detailed information about different the devices, applications and functions, which can take advantage of GNSS or are associated with it to some extent.

5.2.1 Phasor measurement unit

Phasor measurement unit (PMU) is a device, which is used for power grid health determination from the electrical waves it measures from the power system. PMU can be a dedicated device, or it can be integrated in some other device. It measures both the magnitude and phase angle of the sine waves in electricity. PMUs utilize GPS to achieve common time source between the devices and can be installed in dispersed locations in the power system (Bayliss, & Hardy, 2011, p. 1070). PMU provides synchronized phasor magnitude, and angle, frequency and Rate of Change of Frequency (ROCOF). All these measurements are time-tagged by using an absolute time refence in UTC-format and the measurements are encapsulated in IEEE C37.118.2 compliant data packets (Castello et. al., 2018, p. 78).

The first prototype for PMU was developed in 1988 and it is a descendant of the Symmetrical Component distance relay. GPS satellite system made precise synchronization of sampling clocks possible. Even though the accuracy of the synchronization was not precise in the early implementations, it is possible to achieve accuracies of 1 p or better these days. Since one microsecond equals approximately 0,022° in 60 Hz signal, the accuracies are perfect for power frequency voltage and current measurements (Phadke, 2002, p. 477).

The GPS receiver is an integral part of a PMU. Analog input signals are first filtered to remove interfering signals and then anti-aliasing filters are applied. The timing pulse provided by GPS receiver is used for producing a phase-locked oscillator at the required sampling rate. PMU continuously computes arriving data samples and the measured phasors are time stamped to Coordinated Universal Time (UTC) with the signals that the GPS receiver provides. Since the frequency in the power system varies constantly PMUs must take these variations into account and apply required corrections to the estimated phasor (Parashar et. al., 2012, p. **15**-9). A generic PMU is presented in the figure 8.

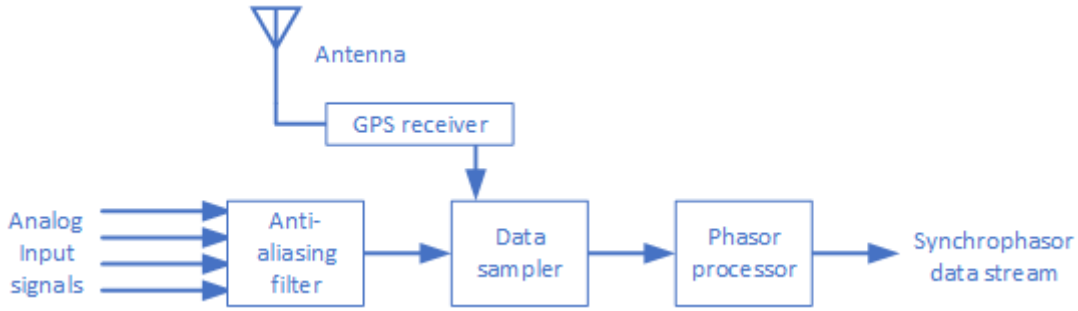

Figure 8. Representation of generic PMU (Parashar et al, 2012, p. **15**-9).

The obtained phasors are presented in a synchrophasor representation, where the time signal is used for defining the instant when the measurement is made. Common timing signal makes it possible to combine multiple phasors from different locations on a common phasor diagram (Parashar et al, 2012, p. **15**-9).

The IEEE standard for Synchrophasor measurements for Power Systems (IEEE C37.118.1-2011) specifies the requirements for PMUs. The Total Vector Error (TVE) combines three possible error sources: magnitude, phase and timing. TVE factor guarantees, that the uncertainties in magnitude and time synchronization errors are bound within certain limits. The standard specifies this limit to 1 %, which corresponds to phase angle error 0,573 ° or a time synchronization inaccuracy of 31,8 µs at 50 Hz (Almas et. al., 2018, p. 4601-4602; Shepard et. al. 2012, p. 148).

PMU's are utilized in Wide-Area Measurement Systems (WAMS), which complement the traditional data acquisition functions of protection relays, fault recorders and SCADA systems. In Phasor data computation the rates range between 10 to 60 phasors per second for systems which include PMUs. Typical applications which utilize synchronized phasor measurements in North America include relaying applications and improvement of SCADA-based state estimation (Cai et. al., 2005, p. 5).

5.2.2 Phasor data concentrator

Phasor data concentrator (PDC) is a function combining synchrophasor data from multiple sources for further processing. The original purpose of PDC was to combine the synchrophasor measurements from PMUs into a single time synchronized data stream, but it includes monitoring for the overall measurement system as well. As the measurement system and the deployment of different applications have grown, so have the functionalities of PDCs also expanded to include more data handling, processing and storage capabilities. PDCs can be consider as a function instead of stand-alone device as it can be integrated into other systems and devices (The Institute of Electrical and Electronics Engineers, 2013, p. viii).

PDCs collect data packets that PMUs send and compose the data into suitable streams which are forwarded to a control center. There are different applications that utilize the PMU data and this data can be used for real-time analysis or stored for offline analysis.

PDCs are designed to collect and align the measurements with same timestamp and to forward the data to the upper levels of architecture. This makes PDC the first element of the system with a complete view of an entire portion in the power system (Castello et. al., 2018, p. 78).

Simple synchrophasor networks consist of PMUs and phasor data concentrators as the figure 9. demonstrates. Typically, PMUs are located in key substations and gather phasor data, which they send in real time to a PDC at location where the data is aggregated. The collected data can be sent to other PDCs and synchrophasor systems and then used to support different applications, that provide sophisticated functionality for analytics, controls and protection. For example, dynamics monitoring applications use full-resolution real-time data combined with grid models to support operating and planning functions in power grid environments (The Institute of Electrical and Electronics Engineers, 2013, p. 5).

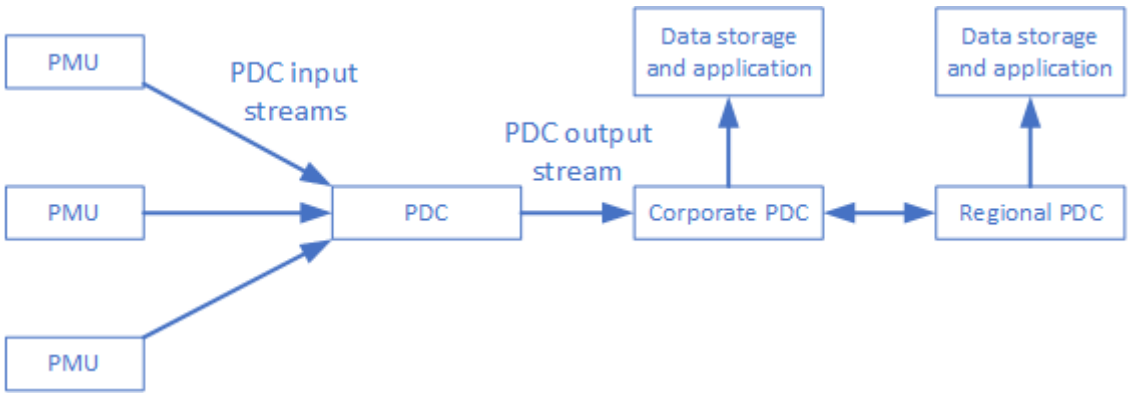

Figure 9. PDC network (The Institute of Electrical and Electronics Engineers, 2013, p. 6).

A PDC serves as a node in communication network, where the incoming data is processed and sent out as a single stream to higher level PDCs and applications. Synchrophasor data is processed by timestamp to create a system-wide measurement set. A structured hierarchy of distributed PDCs can follow the system's hierarchy: substation, utility, control area, reliability coordinator, and interconnection level. PDCs are also able to interact with each other on a peer-to peer basis and each layer of the distributed PDC

hierarchy can have its own data requirements (e.g., latency, quality, resolution). Local PDCs represent a single point of failure in the system, so bypass options and backups are necessary for mitigating the possible failures (The Institute of Electrical and Electronics Engineers, 2013, p. 7). Current commercial PDCs, which are suitable for electrical transmission system monitoring can receive hundreds of incoming streams. PDCs can apply different mathematical functions (power calculations, evaluation of sequence components) for the incoming streams and the can contain other utilities such as alarms that are specific for electric substations (Castello et. al., & Sulis, 2018, p. 78).

5.2.3 Precision Time Protocol

The IEEE 1588 Precision Time Protocol standard is an emerging candidate for addressing increasing timing requirements in networks. PTP standard defines distributed network of clocks, which are arranged into master-slave hierarchy and the protocol measures and compensates delays in the network (DeCusatis et. al., 2019, p. 1). PTP enables submicrosecond synchronization accuracy in packet-based networked systems, but in order to achieve this precision specific design principles and adherence to the protocol is necessary (Watt et. al., 2015, p. 2).

IEEE 1588 was initially released in 2002, but later revised in 2008 as version 2. These versions of the protocol are not compatible with each other, so it is impossible to combine devices using different versions in the same network (Watt et. al., 2015, p. 2). Both IEC Smart Grid Strategy Group and the National Institute of Standards recommend Precision Time Protocol version 2 (PTPV2) for precision timing in substation automation. PTPV2 can achieve timing errors of less than 100 ns providing the greatest accuracy for network-based time transfer systems (Ingram et. al., 2012, p. 1173). The standard defines five device types: ordinary clocks, boundary clocks, end-to-end transparent clock, peer-to-peer transparent clock and management nodes (Watt et. al., 2015, p. 2). Example of PTP topology can be seen below in figure 10.

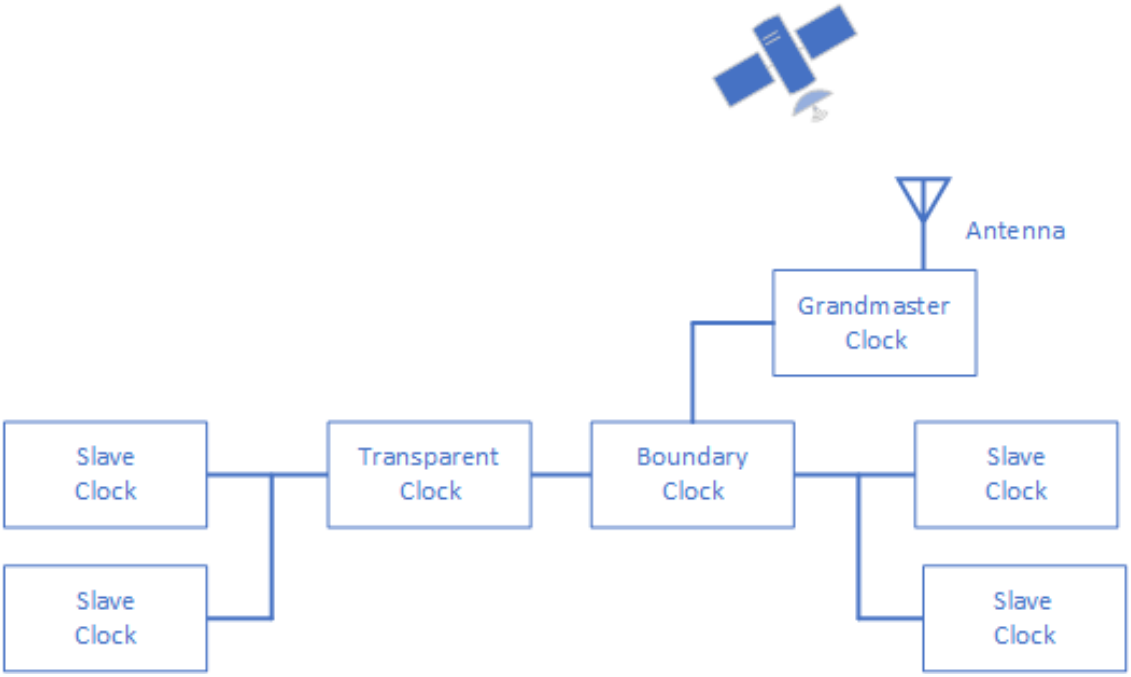

Figure 10. PTP network topology (Watt et. al., 2015, p .2).

An ordinary clock communicates on the network through a single PTP port and it either synchronizes to time or serves the time to other devices in the network. It is called grandmaster clock if it serves time to the entire network and it acts as the ultimate source for the time for all the other devices. If an ordinary clock is synchronized by another clock it is called a slave clock (Watt et. al., 2015, p. 2). As GPS has proven to be an excellent tool for time transfer, it is expected that most of the master clocks in substations will be synchronized to International Atomic Time (TAI) via GPS (Ingram et. al., 2012, p. 1174).

A boundary clock is a device with multiple PTP-ports and synchronizes other devices to reference time through these ports. One of the ports serves as a slave and the rest operate as master ports. Boundary clocks are usually integrated into PTP-aware network devices like switches, bridges and routers. Boundary clocks enable the PTP network to support large numbers of slave clocks, and they can be used to scaling up the network as they service the slave clocks instead of the grandmaster clock (Watt et. al., 2015, p. 2).

An end-to-end transparent clock is a multiport device for routing PTP messages and it measures the time, which PTP messages spend in the device. The delay information is added to correction field of the message and the message is sent to its destination. This functionality is usually performed by PTP-aware switches and its purpose is to eliminate variations and asymmetry that the device can introduce in the transfer process (Watt et. al., 2015, p. 2).

A peer-to-peer transparent clock is a multiport device, which measures the link delay for each port and adds it along with the residence time to the messages, that are passing through it. As with the end-to-end transparent clock, the intention is to eliminate asymmetry and variations, but peer-to-peer transparent clocks also allow scaling of the network as slave devices don't need to rely on grandmaster clock for measuring the end-to-end delay. Instead the slave devices can measure the delay to its peers and work out the overall delay as PTP messages always contain the delay experienced in the network (Watt et. al., 2015, p. 2). The relationship between end-to-end and peer-to-peer delay measurements can be seen in figure 11.

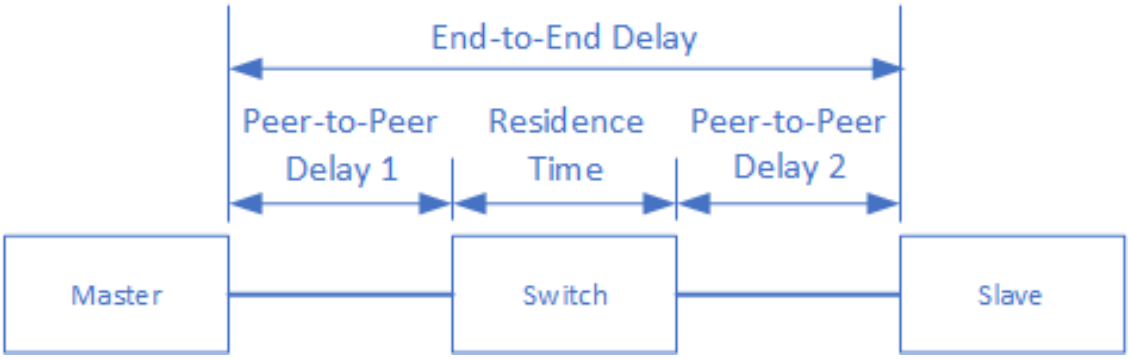

Figure 11. End-to-end and peer-to-peer delays (Watt et. al., 2015, p. 2).

A management node can be any device and it does not have to be PTP-aware. Management nodes are used for configuring and monitoring PTP devices. They are typically just ordinary computers with appropriate software (Watt et. al., 2015, p. 2).

PTPV2 provides means to compensate for propagation delay, absolute time and a way to distribute time across a substation. Many suppliers stock PTPV2 slave clocks that can generate 1-PPS signal. Though native support for PTPV2 is desirable, since utilizing 1-PPS signal means loss of most of the extra data, including accuracy information, absolute time and date (which can be included in Sampled value or synchrophasor messages) and details of the clock source (Ingram et. al., 2012, p. 1175).

5.2.4 Sampled Values (IEC 61850-9-2)

Sampled value (SV) protocol specified in IEC 61850-9-2 is a specific communication service mapping and it provides an interface to the IEC-61850-based data model. A time synchronization system is a requirement for SV, though the details for it are not defined in the standard (Ingram et. al., 2012, p. 1173). The process bus architecture specified in IEC 61850-9-2 was proposed to reduce the complexity of copper wiring between instrument transformers and SAS. It offers data formatting and dedicated communication network with timestamp for digitizing the sampled values (Adrah et. al., 2018, p. 84). SV is suited for thousands of updates per second and has been designed for the rapid publication of information to many subscribers. This has been achieved through connectionless multicasting by implementing publisher/subscriber model (Ingram et. al., 2012, p. 1174).

SV are digitized instantaneous values of power system quantities; these measurements are transmitted to SAS at a sampling rate of 80-265 samples/cycle (Adrah et. al., 2018, p. 84). Currently SV is used for sending instantaneous current and voltage samples from CTs and VTs, but in future it may also be used for sending Boolean or transduced data. The process bus carries data (voltage and current samples, transformer temperature, and circuit breaker status) from the primary plant to the SAS. Data (circuit breaker tripping and closing commands) is also carried out from the SAS to the primary plant through the process bus. Merging units collect or sample the output of three to four CTs and VTs and the collected data is transmitted forward in a standardized form. The data must be

accurately timestamped for each sample, if IEDs like protection relays are to use the SV data gathered from multiple MUs (Ingram et. al., 2012, p. 1174).

The content and rate of data that is transferred in SV through Ethernet is not explicitly defined. To address this problem a guideline was developed by the UCA International User Group in 2004. This guideline is commonly referred as 9-2 Light Edition (9-2LE) and it specifies the datasets that are transmitted, sampling rates, time synchronization requirements, and physical interfaces. The physical interface for time synchronization in 9-2LE is based upon 1-PPS signals. The accuracy requirement of ±1-µs is derived from the T4 timing class (overall timing error within ±4 µs) defined in IEC 61850-5. A higher time performance class T5 also exists with overall accuracy requirement of ±1 µs, which is the stretch target for substation timing systems (Ingram et. al., 2012, p. 1174).

5.2.5 Merging Unit

The main function of Merging unit (MU) is to collect sampled values from 12 channels of electronic voltage and current transformers and transmit the data to secondary devices synchronously in a specified format. Process bus is one of the architectural components of IEC 61850 substation automation system. The process bus is an isolated network segment for carrying SV streams of process data between MUs and other IEDs implementing monitoring, protection and control for the secondary equipment in the SAS. MU is the applied foundation for electronic transformers in intelligent substations and IEC 61850 communication protocol is integral part of MUs (Wei-ming et. al., 2011, p. 1238; Honeth et. al., 2013, p. 1).

MUs must provide SV packets with magnitude and accuracy corresponding to that which is provided by conventional acquisition methods in order to keep the requirements of the system. They also must provide stable samples in relation to the timestamps. Meaning that for example in nominal frequency of 60 Hz and sample of 80 frames/cycle, every sample must be sent within 208 microseconds. It is also imperative that the first sample of the second is as close to PPS turnover as possible. These characteristics define the

good stability of the MU and they are strongly dependent of the performance of the time synchronization of the acquisition system (Dutra et. al., 2014, p. 1). Due to this strong dependency between time synchronization and MUs, they are often synchronized with GPS clock sources or PTP network connected to GPS clock source.

5.2.6 Traveling wave fault location

Accurate fault location provides great value for power transmission asset owners and operators. Traveling wave fault location (TWFL) systems are also important applications for resilient smart grids providing better guarantees for safe operation. Impedance-based fault location systems utilize voltage and current measurements at the frequency of the system combined with different assumptions about the system, which leads to different methods for fault location like Takagi and Schweitzer methods (Li et. al., 2011, p. 1631; Schweitzer et. al., 2016, p. 114).

Fault location system is based of high-accuracy clock synchronization, the precise positioning of the whole network can be achieved by recording the arrival time of traveling wave in each substation. When a fault occurs, the traveling wave signals are generated in the fault point and are registered in the both ends of the transmission line. The fault location system detects the arrival of the traveling waves and is able to position it according to the recorded arrival time (Li et. al., 2011, p. 1631). A fault at any point of the voltage wave except for the voltage zero launches a step wave, which travels to both directions from the location of the fault as can be seen in figure 12. A common time reference is used in the devices capturing the fault and by exchanging the local timestamps, the distance (m) to the point of fault can be calculated (Schweitzer et. al., 2016, p. 115).

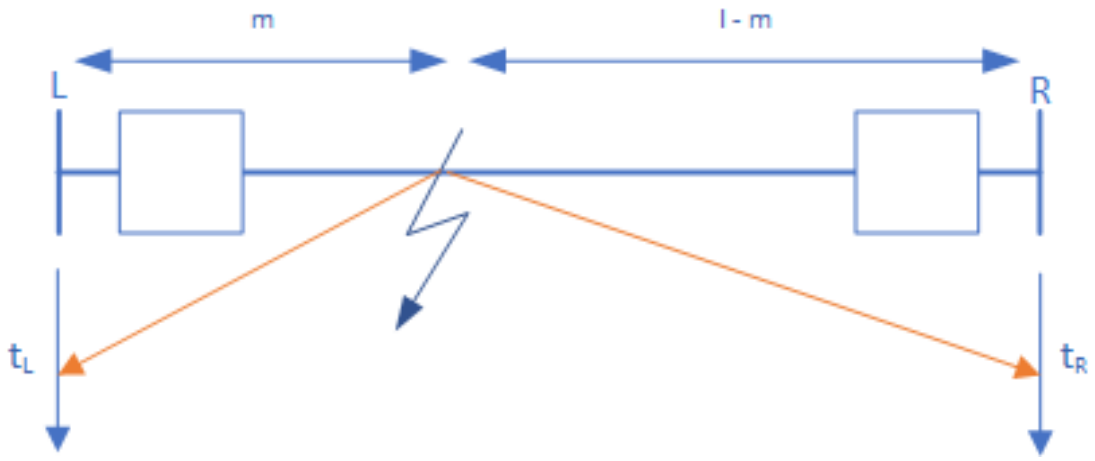

Figure 12. Fault location in transmission line (Schweitzer et. al., 2016, p. 115).

With the development of smart grid, the traveling fault location systems have put forward ever increasing requirements for the time synchronization. GPS has been widely adopted as the synchronization source these days, due to its high precision. Installing GPS clock to every site of the traveling fault location system has proved to be expensive. PTP which also relies on GNSS timing signals has been proposed as an alternative synchronization source to reduce the installation costs of TWFL systems (Li et. al., 2011, p. 1631).

5.2.7 Protection and Control Relays

Protection and control relays are the first level of intelligent electronic devices in power system substations, they have a critical role in protection, control and monitoring of the systems. These devices have a first-hand access to the power system and are in the bottom of the hierarchical communication network. Relays isolate faulty sections of the subsystems from the rest of the grid and actively participate in the power restoration after a fault has occurred. IEDs also play a part in the optimized management of substation devices and in the overall transmission and distribution of the power network, which is an integral part of the smart grid vision of the future (Sukumara et. al., 2018, p. 1).

First micro-processor based IEDs were introduced in the early 1980s. These IEDs provided greater functionality and resulted in better problem-solving capabilities, higher reliability and cost savings, when compared to traditional devices. The first generation of numerical protection relays already integrated several protective functions and metering into one device (Duncan, & Bailey, 2004, p. 33).

Modern protection relays allow design of specific protection and control schemes. Microprocessor-based protection relays emulate the physical behavior of the previous generations of protection relays. The Integration of programmable logic functions has eliminated the need for several external devices and control logic. IEDs can provide in-plant metering with appropriate accuracy as they include voltage inputs, voltage-based functions and calculated energy metering. This in turn eliminates the need for separate meters and yields significant cost savings and simplifies the required wiring for the system. IEDs are capable of fulfilling unique system requirements by combining the internal programmable logic controller (PLC) capabilities and metering functions within the same device (Duncan, & Bailey, 2004, p. 35).

The introduction of Ethernet-based protocols to relays has brought multiple benefits to them from the operational perspective through information exchange over communication networks. The communication of relays in substation and distribution automation systems occurs through Ethernet and TCP/IP based protocols nowadays. This development has introduced cyber security issues to power grids, which previously only concerned office environments and enterprise IT systems (Sukumara et. al., 2018, p. 1).

6 Known threats and disruptions

This section provides a brief introduction to some different threats and disruptions that are known to have adverse effects on GNSS-based applications. These threats come in various forms, they can be naturally occurring phenomenon, unintentional interference or intentional attacks. Disruptions hindering the GNSS signal receiving are quite common and often unintentional by nature, intentional attacks on the other hand might target specific the receiving equipment and applications with severe consequences.

6.1 Natural phenomenon

Threats caused by natural phenomenon are usually related to the physical qualities of the GNSS signals. Space weather can cause irregular propagation delays to the signals traveling through the atmosphere, the growth of the vegetation or newly erected buildings can block or the reflect the signals. Most of these threats can be coped with by appropriate preparation and receiver antenna siting, though in case of strong disturbances caused by space weather preparation might mean planned downtime for some services.

6.1.1 Ionospheric scintillation

GNSS receivers may be unable to track one or more visible satellites for short periods of time due to Ionospheric scintillation. This phenomenon is caused by irregularities in the ionospheric layer of Earth's atmosphere, the region from roughly 50 km up to several Earth radii. In this region the solar radiation separates small fractions of normally neutral constituents into positively charged ions and free electrons (Kaplan & Hagerty, 2017, p. 588).

The maximum density of free electrons is located at an altitude of approximately 350 km above Earth's surface during daytime. The free electrons in the atmosphere mainly cause some delay to the GNSS signals, but the irregularities of the density can also cause major

interference to the signals. These irregularities are most common and severe after sunset in the equatorial region, but high-latitude regions also experience scintillation which is less severe but can persist for long periods of time (Kaplan & Hagerty, 2017, p. 588-589). This phenomenon can be troublesome for receivers that are making carrier-phase measurements, and the results may be inaccurate, or the position information can be lost completely due to scintillation - code only receivers are less susceptible for ionospheric scintillation but can still be affected by it (Rama Rao et. al., 2009, p. 2101).

6.1.2 Geomagnetic storms

Solar disturbances can cause changes in Earth's magnetic field and space weather resulting in geomagnetic storms. They occur in conjunction with ionospheric storms and usually start out with the initial phase, which increases the earth magnetic field. This is followed by the main phase which lasts for couple of days and causes a large decrease in the magnetic field, afterwards a recovery phase starts and usually last somewhat longer than the initial phase. Geomagnetic storm caused by a solar flare starts with a sudden increase of the Earth's magnetic field, which is called sudden commencement storm. This is caused by High Speed Solar Wind Stream (HSSWS). The gradual commencement storm which HSSWS causes starts off gradually and overtakes the Earth's magnetic field (Rama Rao et. al., 2009, p. 2101).

Space weather phenomenon affect navigational systems that utilize radio-wave signals by reflecting from or propagating through the ionosphere. GPS, as also other GNSSs, in particular is vulnerable for changes in space weather, since it relies on constellation of earth orbiting satellites. The radio signals used by GPS must pass through the ionosphere. This introduces propagation delay, that depends upon the Total Electron Content (TEC) of the ionosphere and the above horizon elevation angles of the satellites (Rama Rao et. al., 2009, p. 2101).

Study conducted by Sikirica et. al. (2018, p. 181) demonstrates that the variability of the GPS positioning error increases with development of geomagnetic and ionospheric disturbance. Considerable performance degradation was experienced especially when the GPS pseudoranges were uncorrected or inappropriately corrected. Rama Rao et. al. (2009, p. 2109) also observed, that the number of carrier phase slips detected in GPS receivers increased significantly during the time of geomagnetic storm. These phase slips also resulted in loss of locks by the GPS receivers due to phase fluctuations, which were caused by rapid changes in TEC.

6.1.3 Signal blockage

Signal blockage occurs when the electromagnetic waves encounter physical objects in the path between the transmitter and the receiver. This effect may be negligible when the objects obstructing the path are small enough, but large buildings for instance can absorb or reflect the waves and make even the most sensitive GNSS receivers useless. This phenomenon is also known as shadowing and the actual results may vary significantly from the available predicted models. Due to this applying significant amounts of margin is important when assessing performance of the GNSS (Kaplan & Hagerty, 2017, p. 591-592).

Vegetation is a source of signal blockage which is typically a combination of branches and trunks along with foliage or leaves. They can cause combination of refraction and diffraction resulting in delay spread as small-scale multipaths. They can also cause multiple angles of arrival and attenuation due to absorption and reflection of energy. Terrain can be considered as a signal blockage source, that is impervious for electromagnetic waves at L-band, which the GNSS signals utilize. When signal blockage is caused by the terrain, any signal energy arriving to the receiver is due to bending of waves or diffraction over the terrain. Man-made structures also cause additional propagation losses, if either the transmitter or the receiver are inside them. These losses should be added to the propagation losses of the prediction models. The losses caused by buildings vary significantly depending on the materials used on the construction and from the location of the

receiver in the building. Considerable multipathing is also often experienced within buildings alongside the signal propagation losses (Kaplan & Hagerty, 2017, p. 592-598).

6.1.4 Multipath

Multipath occurs when GNSS receivers receive multiple reflected or diffracted replicas of the desired signal as well as the direct path signal. Multipath signals are delayed in relation to the direct path signal, since they always travel longer distances. When the delay of multipath signals is large the receivers are usually able to resolve and reject the signals. If the receiver is able to track the direct path signal, which always arrives before multipath signals, the effect of resolvable signals on performance is minor (Kaplan & Hagerty, 2017, p. 599).

Multipath reflections from nearby objects or grazing multipaths reflected from distant objects may be received after a short delay from the direct path signal. These multipaths distort the correlation function between the received composite signal and the locally generated reference of the receiver. This also distorts the phase of the composite signal and introduces errors in pseudorange and carrier phase measurements producing errors in position, velocity and time. If blockage or shadowing of the direct path occurs among with multipath, the received power of multipath can be greater than the received power of the direct path as illustrated in figure 13. This situation may also occur indoors, when the direct path signal is significantly attenuated by wall, ceiling and roof while the multipath is reflected by another obstacle and arrives through a window or opening (Kaplan & Hagerty, 2017, p. 599).

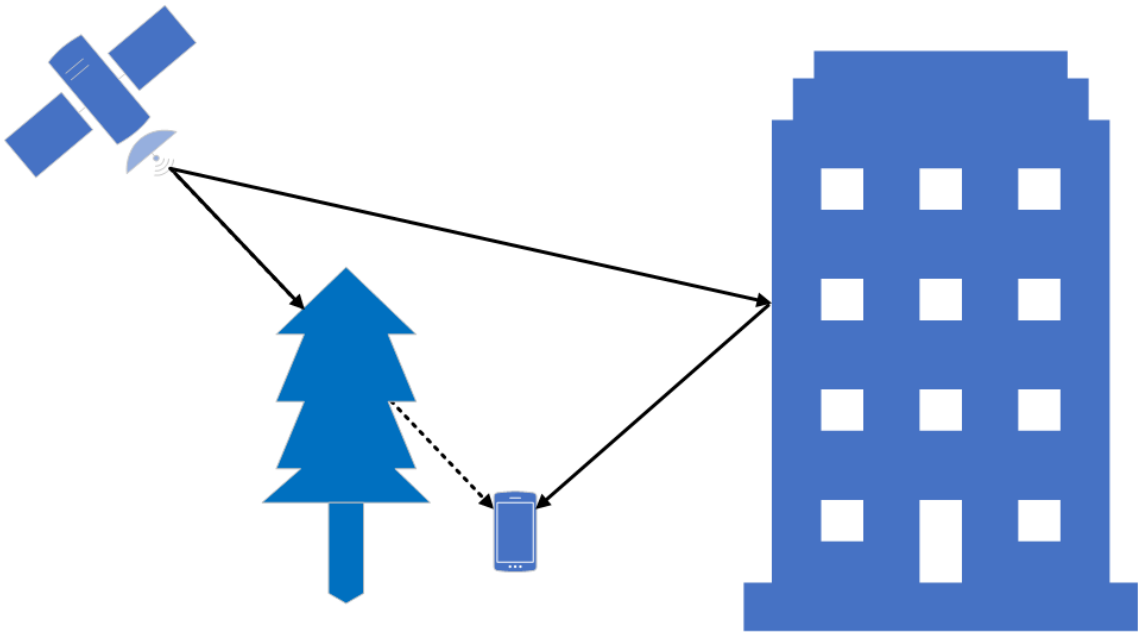

Figure 13. Outdoor multipath and shadowing (Kaplan & Hagerty, 2017, p. 600).

Shadowing of the direct path and multipath has combined effect on the amplitudes of direct path and multipaths. It is possible, that the shadowing is so severe that the receiver only tracks multipaths. The error introduced by multipaths depends on their delays, power and carrier phase relative to those of direct path in situations, where the receiver can track the direct path. When the signal power of received multipaths is minimal compared to the direct path, then also the distortion and error produced by the multipaths is minimal (Kaplan & Hagerty, 2017, p. 599-600).

6.2 Unintentional threats

Unintentional jamming is caused by devices transmitting radio frequency signals. The strength of the disturbances caused by these interference sources can substantially vary in strength and duration. The reasons behind these interferences also vary greatly, they can be generated by malfunctioning devices, transmissions from adjacent frequency bands or they can be intentionally targeted against other GNSS applications.

6.2.1 RF interference

Since GNSS receivers rely on external RF signals they are vulnerable to interference caused by sources of RF interference. The overcrowding of frequency spectrum furthers the appearance of unintentional RFI events originating from GNSS near-band services. The likelihood of these events is increasing due to broadband technologies like 5G, which utilizes the RF spectrum intensively. This can cause the degradation of navigation accuracy and complete loss of tracking (Kaplan & Hagerty, 2017, p. 550; Querol et. al., 2018, p. 155).

Low levels of unintentional interference for any GNSS receiver is to be expected for practically anywhere on Earth. There are large numbers of other systems which rely on transmissions within L-band. It is also inevitable that out-of-band energy from the signals in adjacent bands will at times fall within range of utilized frequencies. Strong RF signals can deteriorate the performance even when the interfering signals are not within the nominal band. RF equipment misuse and malfunctions can also lead to high levels of interference causing for example harmonics that become in-band RF interference. This kind of interference source has to be located and corrected so the normal operation of GNSS receivers in the vicinity can resume (Kaplan & Hagerty, 2017, p. 551-554).

6.2.2 Unintentional Signal Jamming

Jamming is the emission of radio frequency with enough power and features to effectively prevent the tracking of GNSS signals. Even low power devices can act as efficient sources of GNSS signal jamming due to the low power level on which the signals are transmitted to the ground (Faria et. al., 2018, p. 2-3). The effects of jamming on receivers are evaluated with the J/S relationship (Jamming/Signal). This is the difference between the power of interfering signal and power of the received signal expressed in decibels. A J/S level of 27 dB is enough to prevent the phase acquisition of GPS receivers, which only use C/A signals. This however only prevents the tracking process, it requires J/S of 47 dB to prevent the generation of PNT (Position, Navigation and Timing) information as a

whole. So, the 27 dB is only enough to block the acquisition process of the receiver (Faria et. al., 2018, p. 3).

A low power jamming device can corrupt GNSS signal over a wide area range, this is especially true for chirp-like signals, which affect the GNSS signal spectrum with high time frequency dynamics. Several studies have indicated that the combination of highly sensitive GPS receivers and the low signal of GPS makes the system very vulnerable to jamming. Unintentional cases of GNSS jamming are also quite commonplace. For example, in 2007 the US Navy was conducting an experiment on radio signal jamming in San Diego harbor, and accidentally disrupted the GPS reception over a large part of the city (Gao et. al., 2016, p. 1328; Glomsvoll, & Bonenberg, 2017, 34).

6.3 Intentional threats

Intentional threats target specific applications and receiver equipment. These attacks vary in aims and the level of sophistication of the attack. Simple attacks can be launched by anyone having access to proper equipment while the most sophisticated attacks require technical prowess and knowledge about the targeted system.

6.3.1 Intentional Signal Jamming

There are two main motives for intentional GNSS signal jamming. One is to purposefully disturb the use of GNSS by others and the other one is to defend one's privacy. The availability of low-cost GNSS jamming devices has presented a serious threat to GNSS systems and has increased the likelihood of GNSS outages (Gao et. al., 2016, p. 1327). GNSS interference is relatively simple and inexpensive to accomplish and there are various methods available in the market. Though being illegal in most countries, it is very easy to find GNSS jamming and spoofing equipment available for purchase in the internet (Faria et. al., 2018, p. 2).

The GNSS outages which South Korea has been experiencing since 2010 is an example of fully intentional GNSS jamming. These outages were caused by North Korea's ability to jam GPS signals near the border with an operational range that is enough to affect civilian flights. More than 319 aircraft were affected by a similar cyber-attack in 2012. Personal privacy devices (PDD) are the second type of intentional jamming. PDDs are used to overpower weak GNSS signal to prevent tracking (Gao et. al., 2016, p. 1327).

The most frequent targets of GPS jamming are currently the central fleet management platforms used by transportation companies. The motive for these attacks is often the desire to use the company car and hide the illicit use of the vehicles. Other motivations are for example the circumvention of road toll systems and theft of high-end cars (Hunkeler et. al., 2012, p. 1). In July 2013, GPS signals around the London Stock exchange were unavailable for nearly 10 minutes each day. The cause for this turned out to be a delivery driver, who was hiding from the management (Gao et. al., 2016, p. 1378). This indicates that signal jamming is often caused by vehicles, and thus pose a viable risk to the power grid environments when passing by a substation utilizing GNSS based time synchronization.

6.3.2 Spoofing attacks

The aim of spoofing attacks is to fool the victim receiver to false position or time via fake signals. Existing attacks can be classified into three categories: simplistic attack, intermediate attack and sophisticated attack. Simplistic attacks do not take account of any specific information about the targeted receiver. Intermediate attacks are based on the GPS signal received by the target. The attacker generates a fake signal utilizing the information extracted from the authentic signal. The fake signal is then used for spoofing the target receiver to a false location and time. Sophisticated attacks employ several antennas in coordination to emulate the spatial signal domain, thus reducing the pseudorange and Doppler variation correlation, which makes it more difficult to detect the attack (Wei & Sikdar, 2019, p. 1155).

Current GPS receivers, that have been embedded to time synchronized measuring devices use civilian GPS signal, which does not require authentication. GPS receivers can be misled to acquire a fake GPS signal, this can be achieved by initiating a two-step spoofing strategy. The first step for the attacker is to launch certain interference, which causes the GPS receiver to lose track of its current signals. In the second step a spoofed GPS signal is sent while the GPS receiver is acquiring new signals to replace the lost ones. The receiver will start to track the spoofed signal due to its higher correlation peak, since the counterfeit signal has a higher Signal-To-Noise ratio (SNR). This is caused by the way how the GPS signal acquisition is implemented, during the acquisition the highest correlation peak in the code-phase-carrier frequency is being searched out (Zhang et. al., 2013, p. 89).

Alternatively, the attacker can scan the code-phase-carrier frequency until the fake correlation peak overlaps with the authentic one. The first stage is the scanning, where the attacker launches a fake peak close to the authentic peak and starts moving the fake peak towards the true peak. In the second stage the fake correlation peak is moved to a position where the fake peak overlaps with the true peak. This captures the GPS receiver with a counterfeit signal due to the fake signal's higher SNR. The third stage consists of moving the fake correlation peak slowly to a desired point, at this point the true correlation peak is considered as noise by the receiver (Zhang et. al., 2013, p. 89).

Spoofing attacks are a specific type of an attack which fabricate the data used for calculating the pseudoranges. These attacks do not target the GNSS receivers themselves but feed the receiver with false input data. The targeted receivers operate correctly, but these attacks modify the pseudoranges of the satellites in view with some fractional amount (Nighswander et. al., 2012, p. 450-451).

6.3.3 Time synchronization spoofing attacks

The existing GPS spoofing methods have mainly focused on changing GPS satellite's position information by manipulating the ephemerides data or shifting the signal time with

delay. Time synchronization spoofing attacks (TSSA) have only recently become a relevant concern. In these attacks the GPS receivers are deceived by broadcasting forged GPS signals or simply by rebroadcasting GPS signals which have been captured at another time (Wei & Sikdar, 2019, p. 1156; Almas et. al., 2018, p. 4601).

The time of the GPS receiver is dependent on the time deviation, signal propagation time and the signal transmitting timestamp. This means that there are theoretically three ways to spoof the time of the targeted receiver: changing the propagation time, changing the GPS timestamp, and the combination of both. Serious GPS spoofing can be conducted with low errors on pseudorange and location by fabricating the GPS timestamp. Negligible pseudorange and constant location errors can also be achieved by inserting the same amount of delay to all GPS signals. These low error attacks can be difficult to detect, but inserting a random delay into each signal on the other hand can be quite obvious since the pseudorange and location errors can be thousands of meters (Wei & Sikdar, 2019, p. 1156, 1160).

6.3.4 Data Layer attacks

Spoofing attacks can also be used for producing different kinds of data at higher levels such as a navigation message with a valid GPS signal. The data layer attacks can cause more damage compared to the straight-forward spoofing attacks. In data layer attacks the spoofed signal carries malicious data stream, which targets the software applications running inside the receiver. These attacks exploit specific vulnerabilities in the applications, which form the navigation solution or in other downstream applications interfacing or utilizing the navigation solution. Data level attacks could also target other applications running on separate devices which utilize the receiver data and obtain it over a network (Nighswander et. al., 2012, p. 451, 453-454).

Nighswander et. al. (2012, p. 456) performed a series of attacks on GPS receivers, one of them was called **Middle-of-the-Earth Attack**, in which they fed multiple different receiv-

ers ephemeris data, which corresponded to telling the receiver that a satellite was located in the middle of the earth. All the receivers excluding one rejected the bogus data they were fed. The one which accepted the data entered into an infinite reboot cycle when attempting to resolve the error. This device only recovered after a full hardware reset was manually performed. This attack basically served the purpose of Denial of Service (DoS) attack achieving similar goal as jamming attacks. But unlike jamming this attack does not have to be continuous and the bogus data needs to be fed until the receiver decodes the ephemeris, which typically takes about 30 seconds.

GPS receivers do date calculations by using Z-count, which consists of 10-bit Week Number (WN) and 9-bit Time of Week field. This can be utilized for **Vulnerable Week Number Attack** by first setting the week number to be one past the current week without changing any other data in the navigation message. When the ephemeris expired all the receivers except for one accepted the new week number, after that the week number could be set to any value in the 10-bit range (Nighswander et. al., 2012, p. 456).

Date De-synchronization Attack exploits the rollover of the 10-bit WN**.** Rollover is an expected event which occurs approximately on every 19,7 years. The original GPS specification leaves the handling of rollover events up to manufacturer's discretion, so the results may vary depending on the manufacturer. The rollover event can be simulated by alternating between the high (all 10 bits set), low week numbers (1-5 bits set), and medium week numbers (8-9 bits set) in WN. After this the setting of IODC and IODE parameters with arbitrary values tells the receiver, that new data has been issued and should be decoded. After which the receiver should use an internal clock for deciding if it is reasonable for a rollover event to occur. Only one of the tested receivers was vulnerable for this attack, but it suffered permanent damage rendering it useless as a sub-microsecond accurate time source (Nighswander et. al., 2012, p. 457).

6.3.5 Receiver software attacks

As GNSS receivers are computers they also share common vulnerabilities with other microprocessor-based devices. Low-end receivers run on basic operating system stacks and contain simple software. High-end receivers have additional networking capabilities and run software like webservers, which makes them significantly more complex. Since the receivers are often treated as devices instead of computers, their vulnerabilities are more likely left unpatched which poses serious threat to critical applications (Nighswander et. al., 2012, p. 451).

Nighswander et. al., (2012, p. 457-458) were able to identify the operating systems from three of the devices they attempted attacks against. This gave the researchers the ability to access some services and exploit certain security flaws, which for example allowed them to gain root access to one device. They were also able to upload executable files through USB and SD card slots meant for updating the GPS maps and device firmware. This enabled them to run arbitrary code in the devices, which could lead installation of malware or identification of new software vulnerabilities, that can be exploited on the Data Layer.

Identification of the operating system which the GNSS receivers utilize opens the possibility for devising system dependent attacks. Operation systems have known vulnerabilities, which can be exploited on an attack. For instance, a spoofing attack with Date desynchronization and vulnerable week number attacks could be attempted in order to exploit system specific timestamp vulnerabilities (Nighswander et. al., 2012, p. 458).

6.4 Possible consequences

If the signal spectrum of GNSS systems is compromised around power grid environment a wide variety of possible consequences can follow in its wake. The consequences vary from minor nuisance to severe system-wide instability depending from the nature of the threat and the affected applications. Accurately targeted attack could bring down major

portions of the entire power grid, while minor interference can introduce some error into measurement data. Theoretically the power grid time synchronization could also be exploited for DoS attacks.

Pure jamming attacks can be generally considered as a minor threat, but they do constitute as DoS attacks if the jamming goes on for long enough. According to Seth & Kazi (2018, p. 2), when the GPS signals are jammed, and since almost all PMUs have internal clocks, which can produce synchronization signal when the 1-PPS signal is unavailable, the PMUS are able to deliver reliable data for several minutes. In the experimental setup of Almas et. al. (2018, p. 4609) the maximum allowed Total Vector Error (TVE) of 1 % was exceeded within 24 minutes by all the PMUs in the setup, when the synchronization signal was disconnected.

Even though the internal oscillators of the PMUs provide some margin, intentional jamming can be a severe threat, if the jamming continues and the source of the signal cannot be located. Long-term jamming attack could incapacitate entire substations by leaving the field devices to rely on their internal oscillators, if the substations were designed solely around the utilization of IEC 61850-9-2 sampled value process bus. Ingram et. al. (2012, p. 1173) state that China has already commissioned full-scale process-bus-based substations, but they do not provide any information about precautionary measures against DoS attacks on time synchronization.

Spoofing attempts have even more severe implications than jamming, this is especially true if the attempted attack remains undetected. Shepard et. al. (2012, p. 152) observed that GPS spoofing attack can introduce timing errors, which violate the IEEE C37.118 standard for synchrophasors. Synchrophasor-based control schemes can be utilized for identifying fault conditions, one example of such control scheme is in the Chicoasén-Angostura electricity transmission line in Mexico. This scheme monitors the angular instability experienced by hydroelectric generators with two PMUs, which have been deployed to each end of the transmission line. If the phase angle difference measured by

the PMUs exceeds 10 ° the generators will automatically trip. Spoofing attack to a similar system could be used to trip a generator. Alternatively, an attack could aim at preventing the tripping by leading the phase angle to opposite direction, such an attack could damage the generators and the remaining transmission lines. Almas et. al. (2018, p. 4611) also noted, that TSSA can result in faulty activation of protection schemes. In their research a TSSA of around 450 µs caused a false activation of anti-islanding protection and separated the distributed generation from the rest of the power system.

Almas et. al. (2018, p. 4611, 4608, 4610) also remark that any application requiring phase angle measurements will provide misleading information if the PMUs are subjected TSSA. If for example Phase Angle Monitoring (PAM) produces misleading information, it can result in false corrective actions by the automation systems or the grid operators. TSSA also results delay in the feedback control loop degrading the performance of oscillation damping controllers which process synchrophasors. PMUs also need to resynchronize their internal oscillators to the spoofed synchronization signal when they are subjected TSSA. During the resynchronization period the PMUs report a large phase angle computation error, which can lead to undesirable operation of monitoring, protection and control applications. Though there is a more sophisticated spoofing attack, which involves the jamming of authentic signal before the spoofing. During such an attack the internal oscillator goes through a smoother transition, which can be harder to detect especially if the induced time synchronization error is small.

GNSS spoofing attacks targeting the receiver time have also other implications, which seem to be rarely discussed in the studies on the matter. According to Malhotra et. al. (2016, p. 2) several authors have observed that Network Time Protocol (NTP) could be used for undermining the security of TLS certificates. An NTP attacker could send clients back in time and force the acceptance of certificates, that have been revoked or alternatively send clients back in time when cryptographically weak keys were still valid. Similar principles could be applied to power grid environments that rely on IEEE 1588 PTP for

time synchronization. Nighswander et. al. (2012, p. 457) were able to change a GPS receiver's perceived time years into the future permanently with date de-synchronization attack. Vulnerabilities like this could be exploited on PTP grandmaster's GPS receiver to invalidate device certificates. This could prevent the formation of secure connections between different devices due to expired certificates and effectively serve as a DoS attack, if the devices adhere to strict security policies.

7 Threat analysis

This section examines the threats, which GNSS based attacks can pose to the power grid applications and environments. The examination is carried out by utilizing threat modeling techniques for three different use cases. The use cases depict typical power grid applications, which rely on GPS based time synchronization schemes. Since the focus of this thesis is on GNSS based threats, the models mainly address attacks launched from a single entry point, thus limiting different aspects that are considered during the analysis of the models.

The system overview of each use case is presented in the following subsections. The analysis for each use case is performed based on these overviews by utilizing the methods described in section 3.1. The outcome of each analysis is a collection of threat modeling artifacts, which consist of DFD, STRIDE-per-element analysis, list of recognized threats and attack trees demonstrating how different attacks could be executed.

7.1 Synchrophasor-based generation-shedding

This use case is based on the Chicoasén-Angostura electricity transmission line in Mexico already mentioned in the section 6.4. In this application the phasor measurement and control units (PMCUs) communicate directly with each other exchanging syncrophasor data and processing it for protection purposes. The system overview is composed from the available information and is represented in the figure 14.

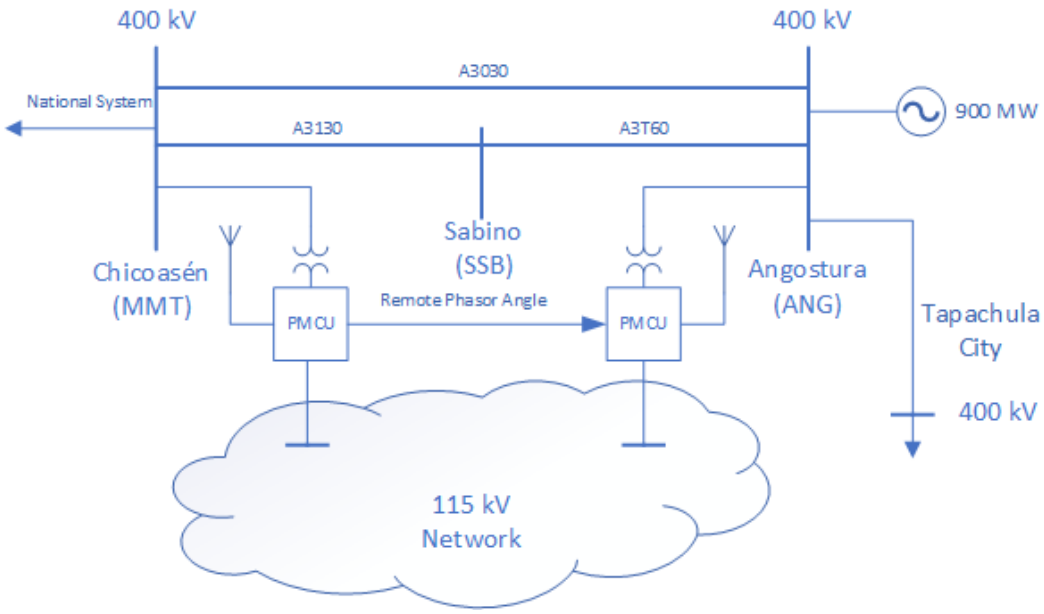

Figure 14. Chicoasén-Angostura system overview (Schweitzer et. al., 2010, p. 1-2).

If the 400 kV transmission link between Chicoasén and Angostura is lost, the generators located at Angostura may experience angular instability, which will overload the 115 kV network. The relays exchanging synchrophasor data calculate the angle difference between Angostura and Chicoasén and measure the local 400 kV bus voltage. The relay at Angostura time-aligns the local phasor data with the remote phasor data and calculates the angle difference. If the angle difference exceeds the threshold this will cause a generator trip at Angostura (Schweitzer et. al., 2010, p. 1-2).

7.1.1 DFD and STRIDE

The system overview and the details provided in the previous section were used for composing a DFD of the system. The GPS receivers and the power generation systems were recognized as the major trust boundaries. The receivers provide time synchronization information for the power generation systems based on the internal clocks of the receivers, which are disciplined with GPS signals. The phasor angle data in both substations is affected by the time synchronization. This data is utilized by the protection scheme which computes the difference between the phasor angles for determining the current state of the overall system. The DFD of the system can be seen in the figure 15. below.

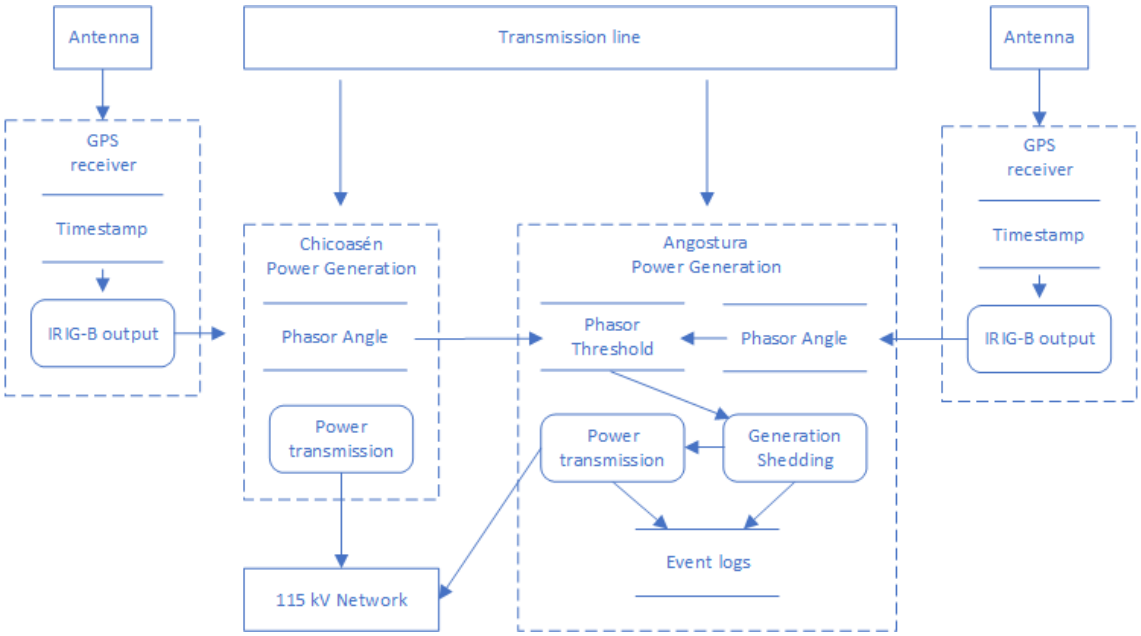

Figure 15. Chicoasén-Angostura generation-shedding scheme data flow diagram

The elements recognized during the DFD modeling process were utilized for STRIDE-per-element analysis. GPS signal disruptions and spoofing expose many of the elements to threats that could be described as tampering. Some of the entities are also susceptible to denial of service. The table 8. below presents the types of threats, that the different elements were recognized to be susceptible to.

Table 8. STRIDE-per-element analysis for generation shedding scheme

Diagram element	S	T	R	I	D	E
Antennas	x	x			x	
Timestamp		x			x	
IRIG-B output		x				
Chicoasén Phasor Angle		x				
Chicoasén Power Transmission						
Angostura Phasor Threshold						
Angostura Phasor Angle		x				
Angostura Generation Shedding		x			x	
Angostura Power Transmission		x			x	
Angostura Event Logs		x			x	

The STRIDE-per-element analysis formed the basis for further threat analysis for the system. The different threat types recognized per element were utilized for considering actual threats for the elements. The threats recognized during this process can be seen in the 9. below, where the identical elements are treated as a single element.

Table 9. Threats affecting the generation shedding scheme

Diagram element	Threat Type	Threat
Antenna	Spoofing	Receiving fake GPS signals
	Denial of Service	GPS signal jammed
Timestamp	Tampering	Time drifted
	Denial of Service	Timestamp based on internal clock
	Denial of Service	Loses internal clock discipline
IRIG-B output	Tampering	Outputs incorrect timestamp
Chicoasén Phasor Angle	Tampering	Provides incorrect angle measurement values
Angostura Phasor Angle	Tampering	Provides incorrect angle measurement values
Angostura Generation Shedding	Tampering	Trigger the protection scheme
	Denial of Service	Prevent the protection scheme from triggering
Angostura Power Transmission	Tampering	Stop power transmission during normal operation conditions
	Denial of Service	Prevent generator tripping during fault conditions
Angostura Event Logs	Tampering	Logs false entries (warnings etc.)
	Tampering	Logs entries with incorrect timestamps
	Denial of Service	Logging of actual events and warnings is prevented

7.1.2 Potential attacks

This kind of protection scheme could be quite easily abused for causing harm with an intentional attack. Schweitzer et. al. (2010, p. 2) state, that double-line outage produces 14 degrees phase angle difference between the Chicoasén and Angostura sites and the detection threshold has been set to 10 degrees, and when this threshold is exceeded the

power generation is shed. The power transmission to the 115 kV network can be stopped simply by misaligning the phase angle and timestamps in either of the substations located in Angostura and Chicoasén. The attack tree presented in the figure 16. below demonstrates how this kind of an attack could be launched via GPS spoofing.

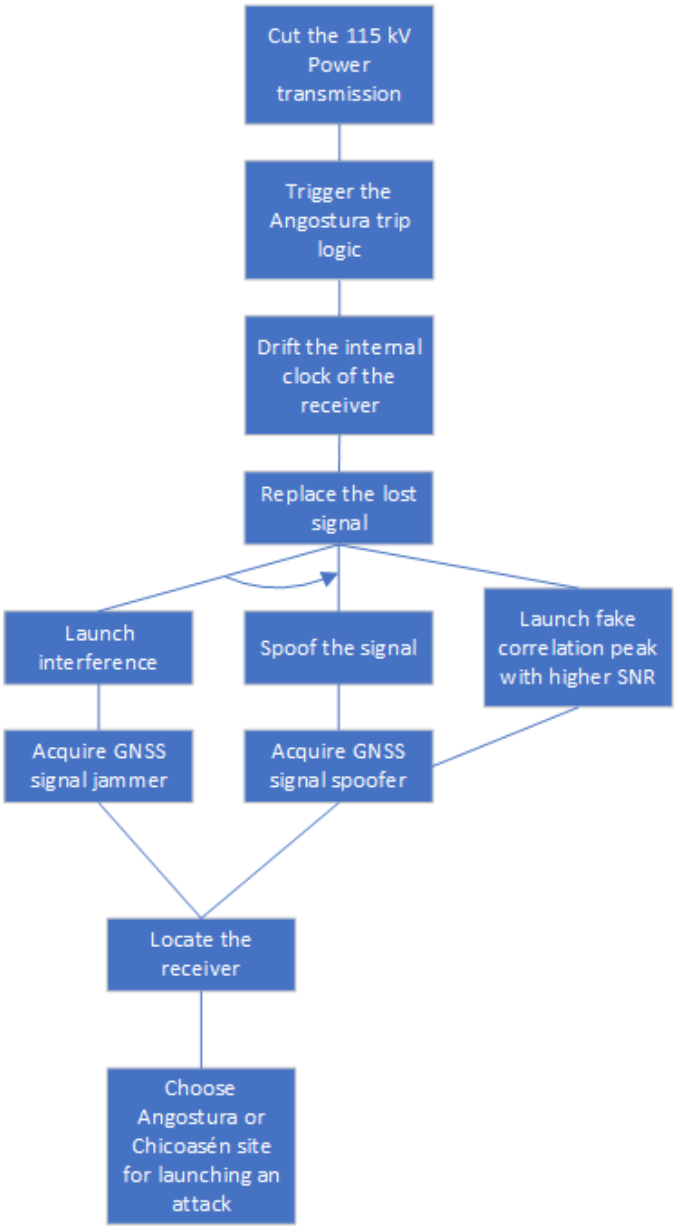

Figure 16. Attack tree for tripping the Angostura generators

There is also a theoretical possibility for damaging the generators in Angostura site, even though this is a highly unlikely situation. The tripping of generators could be prevented

with a forged GPS signal by drifting the clock signal to the opposite angle direction from the phase angle transmitted from Chicoasén. An attack tree for this kind of an attack can be seen in the figure 17.

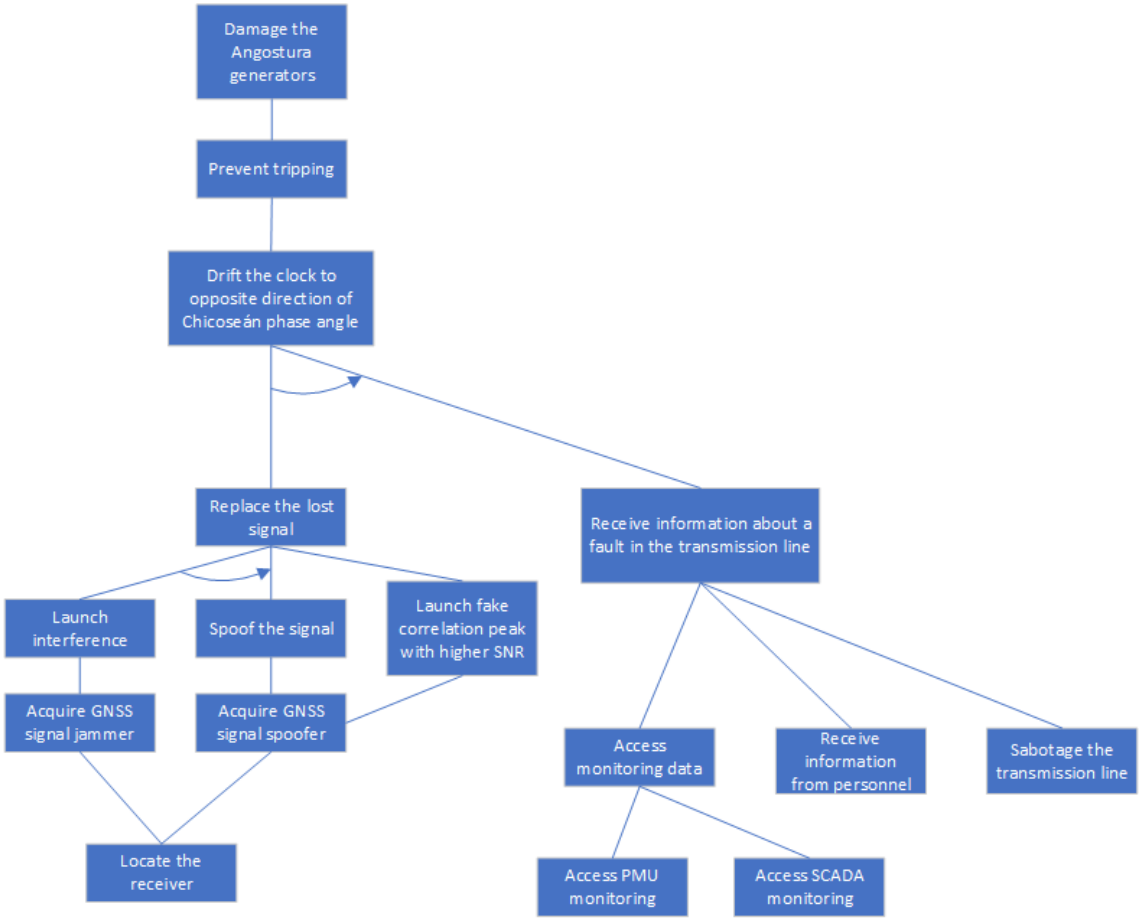

Figure 17. Attack tree for an attack aimed at the Angostura generators

As the attack tree demonstrates, this sort of an attack would require a lot of preparation. The GPS signal would have to be captured in advance and information channel must be secured first. The fake timestamp has to be fed through ephemeris data at the right moment, so the generators won't trip during the attack. This kind of attack could of course be commenced without relying on any outside information source, just by constantly feeding fake signal directing the receiver's internal clock to wrong direction. But without any additional information about the phase angles and the system state, the forged

timestamp would likely cause the generators to trip at some point before the actual objective is met.

7.2 Line current differential protection

The threat model presented here is based on quite generic line current differential protection scheme. Conventional line current differential protection consists of multiple microprocessor-based relays operating independently and exchanging information through a communication channel. Each relay samples its input currents and transmits the local current data through the Data Exchange Channel. As the relays have collected a full set of current data from the local and remote substations, the differential trip equation is executed for determining the potential fault location (Liu et. al., 2011, p. 521). If the relay identifies a fault, the circuit breaker (CB) is signaled to cut-off the faulty section of the transmission line. The overview of typical line current differential protection system can be seen in the figure 18.

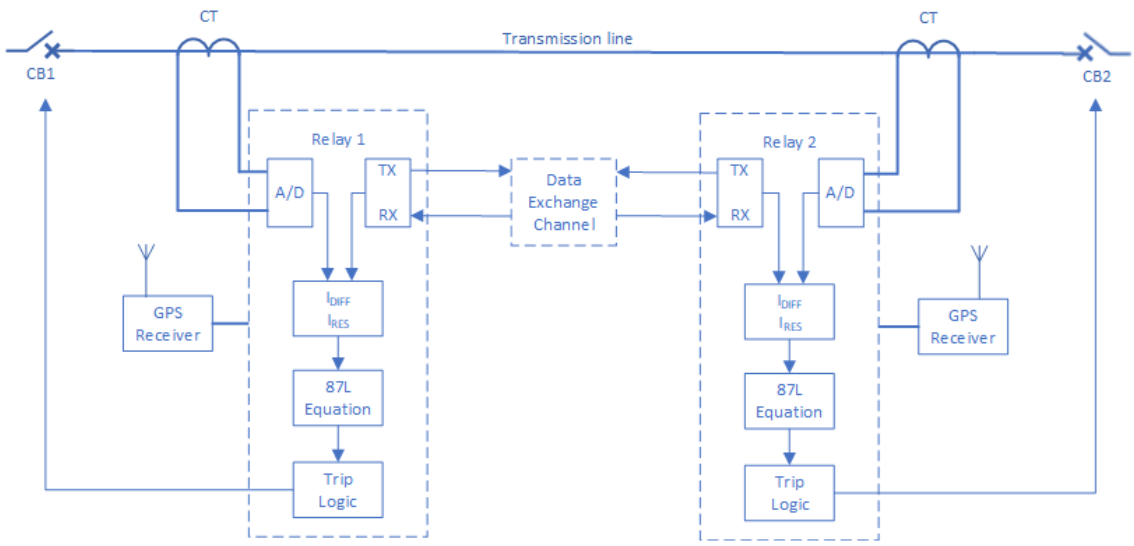

Figure 18. Line current differential protection overview (Liu et. al., 2011, p. 521).

Data synchronization is a crucial part of line current differential protection schemes. If the communication channel is symmetrical, it is possible to use channel-based synchronization known as Ping-Pong algorithm. If the channel symmetry cannot be guaranteed, then GPS can be used as an alternative for the channel-based synchronization, as it offers

a practical way for providing common timing across wide areas based on external time reference (Liu et. al., 2011, p. 521).

7.2.1 DFD and STRIDE

The DFD shown below in figure 19. depicts a conventional current differential protection system based on the system overview presented in the figure 18. The current transformer provides the local current sample for the relays, the sample is appended with timestamps and transmitted to the remote relay. When both local and remote datasets have been completed, the relay feeds them to the 87L Equation for comparison between differential and restraining currents. The result is assessed by the Current Protection logic and a trip signal to the circuit breaker is sent when required.

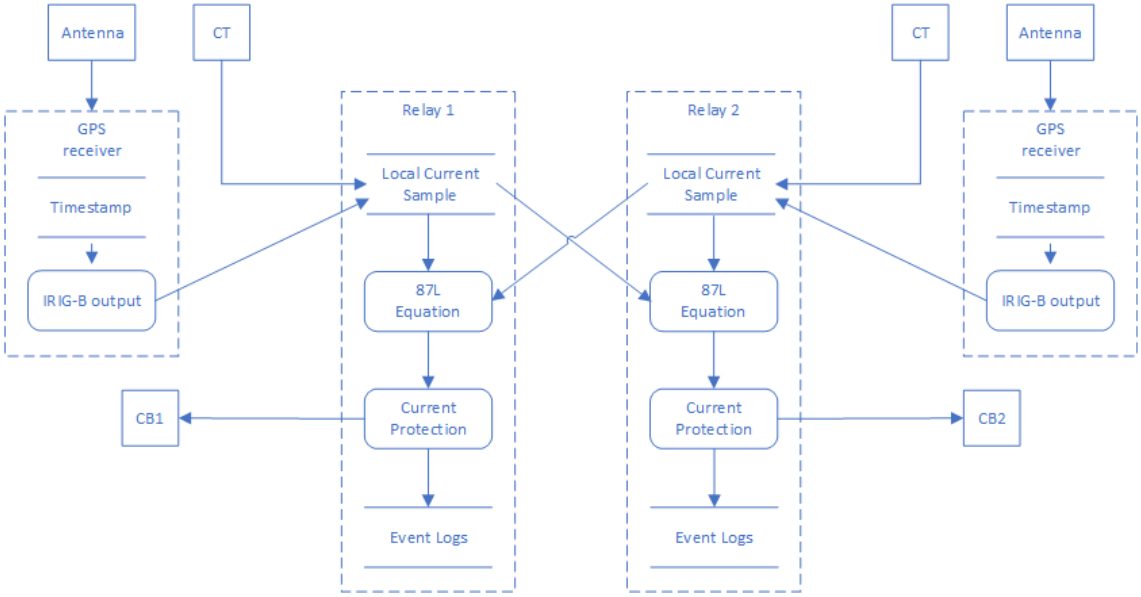

Figure 19. Line current differential protection dataflow diagram

The STRIDE per-element analysis performed for the different elements of figure 19. can be seen in the table 10. Since the system depicted in figure 19. is completely symmetrical the identical elements are displayed as a single entity in the table. The most prevalent threat affecting all the parts of the system was tampering, but many of the elements were also susceptible to denial of service.

Table 10. STRIDE-per-element for line current differential protection

Diagram element	S	T	R	I	D	E
Antenna	x	x			x	
Recovery Signal		x				
1-PPS output		x				
Local Current Sample		x				
87L Equation		x				
Current Protection		x			x	
Event Logs		x			x	

In-depth analysis for the elements was carried out by inspecting the different threat types affecting the elements. The list of exact threats was composed by utilizing the different threat types found with STRIDE-per-element analysis. The table 11. describes the threats, that were recognized during the inspection of different threat types.

Table 11. Threats affecting Line current differential protection

Diagram element	Threat Type	Threat
Antenna	Spoofing	Receiving fake GPS signals
	Denial of Service	GPS signal jammed
Timestamp	Tampering	Time drifted
	Denial of Service	Timestamp based on internal clock
	Denial of Service	Loses internal clock discipline
IRIG-B output	Tampering	The output is based on inaccurate timestamp
Local Current Sample	Tampering	Providing incorrect Sample values
87L Equation	Tampering	Providing false result due to local sample
	Tampering	Providing false result due to remote sample
Current Sample	Denial of Service	Prevent the protection scheme from triggering
	Tampering	Trigger protection scheme
Event Logs	Tampering	Logs false entries (warnings etc.)
	Tampering	Logs entries with incorrect timestamps
	Denial of Service	Logging of actual events and warnings is prevented

7.2.2 Potential attacks

Protection relays often have limited internal capabilities for logging events and for recording different disturbances and faults. Depending from the relay manufacturer and the relay configuration, the logs may behave in differ manner. Some devices might overwrite previous data, some might record and log events to certain limit etc. and in worst case even fill up the entire non-volatile memory of the device. GPS signal spoofing and current line differential protection functions could be utilized in an attack to fill the internal stores of protection relays. Filling the logs might be the actual motivation behind the attack or it could be done in order to prevent an analysis of actual attacks. The figure 20. below showcases how such an attack could be staged.

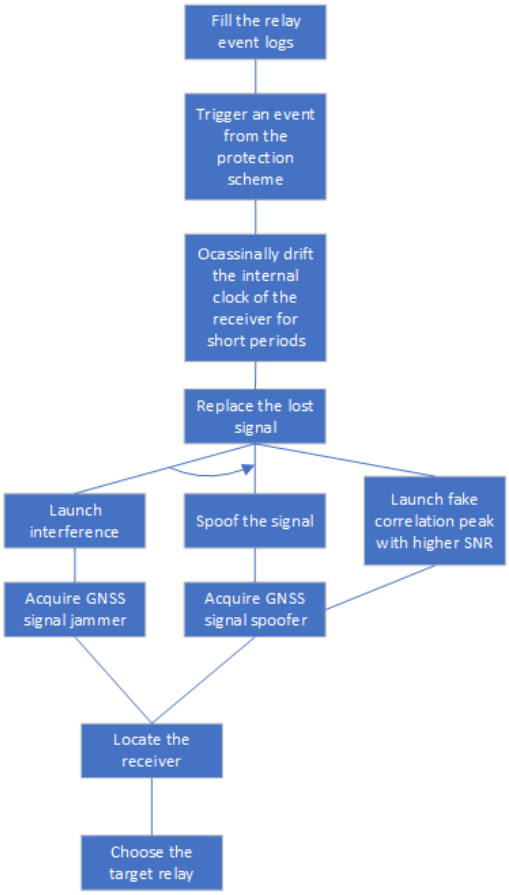

Figure 20. Attack tree for filling event logs

One of the most obvious attacks against current line differential protection scheme via GPS is the triggering of the protection scheme itself. The protection is highly reliable on accurate time synchronization, so attacking either of the relays in charge of the protection would either reroute the transmission or cut the transmission line from the rest of the network. This kind of an attack could be carried out by using signal jamming or by drifting the internal clock of the receiver via GPS spoofing, the attack tree for such an attack can be seen in the figure 21.

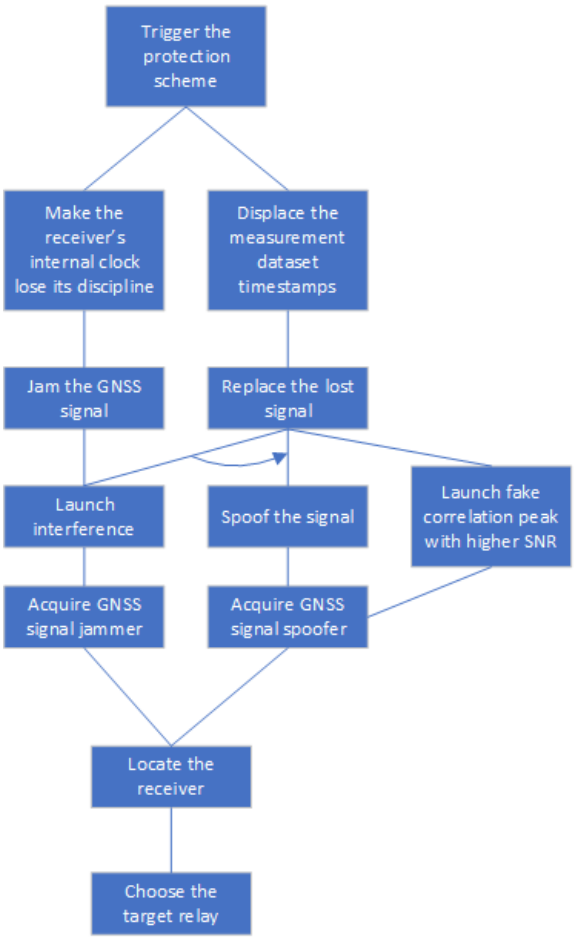

Figure 21. Attack tree for triggering the current line differential protection

Triggering the protection scheme is fairly simple to realize and it can have harmful consequences at least for a short period of time, if the source can be located or the attacks are not carried out constantly. Tampering the event logs and recordings by themselves

are unlikely to cause any noticeable harm, but attacks aimed at the relay logging capabilities can be used for distraction purposes. The aim these kinds of attacks could be diverting attention away from an actual attack or to prevent the analysis of an attack.

7.3 Traveling wave fault location system

The use case presented here is a wide-area traveling wave fault location system located in Hubei province, China. According to Chen et. al. (2013, p. 1208) this system consists of traveling wave data acquisition devices, which have been installed in substations for capturing traveling wave analysis information. When these units are triggered, they send the acquired data to master station through a communication network. The master station runs analysis software and can compute the distance to the disturbance point. The master station constitutes of a communication server, a database server, a web server, and a workstation. The recorded data is collected by the communication server, it calculates the distance to the disturbance point and stores the data in the database server. The system infrastructure can be seen in the figure 22. below.

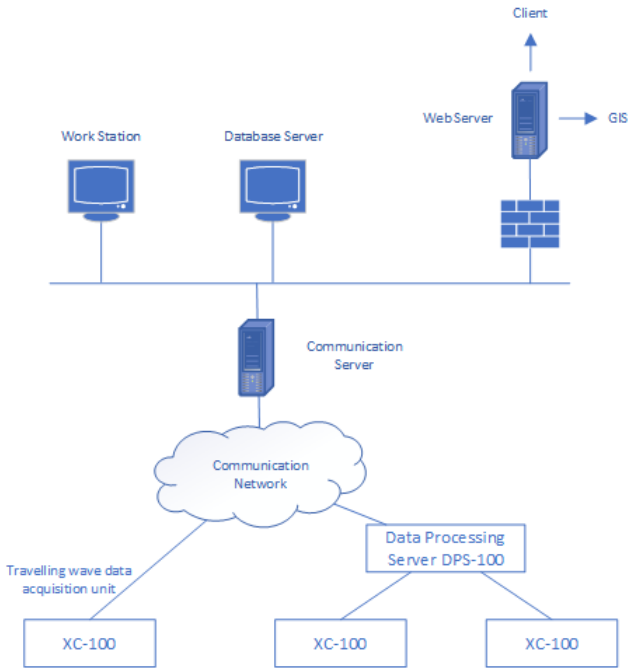

Figure 22. Wide-area traveling wave location system (Chen et. al., 2013, p. 1208)

The master station obtains the wide-area traveling wave data from the traveling wave data acquisition units in the substations. The station can determine the location of the disturbance point by utilizing the arrival time and the information about the monitored network topology. The application is divided into fault location function, disturbance recording function, input and output functions and interface function, which contains setting, logging and data storing (Chen et. al., 2013, p. 1208-1209). An example of TWFL network topology with a disturbance point displayed in it can be seen in the figure 23. below.

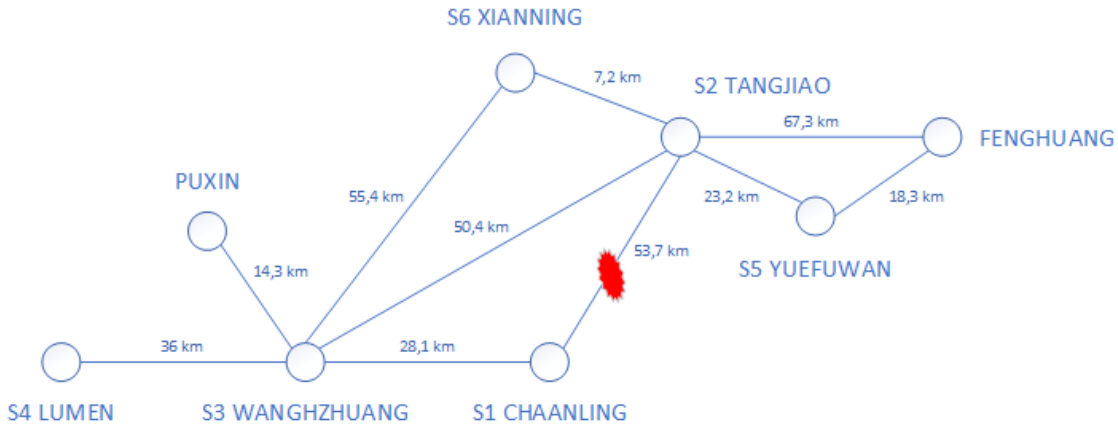

Figure 23. TWFL network topology (Chen et. al., 2013, p. 1214).

The algorithm used in this application first determines, if the records gathered from all the substations belong to a same set of records. This is done by comparing the arrival times of the collected records to the record of the first substation, which detected the disturbance. After the preliminary selection of the dataset, the valid area for calculation is determined by utilizing a weighted adjacency matrix representing the power grid and traveling wave propagation characteristics. The shortest path search is applied to the valid calculation area and the faulty line and the disturbance point is then identified (Chen et. al., 2013, p. 1211-1212).

7.3.1 DFD and STRIDE

The system overview and the information that Chen et. al. (2013, p. 1211-1212) provide about the algorithm was used as a basis for this DFD. The DFD portrays only the interactions between single data acquisition unit and the master station, as every data acquisition unit works independently from each other. In reality the master station is connected to multiple units through the network and the wide-area TWFL algorithm compares the input from multiple sources. The DFD for the wide-area TWFL system can be seen in the figure 24. below.

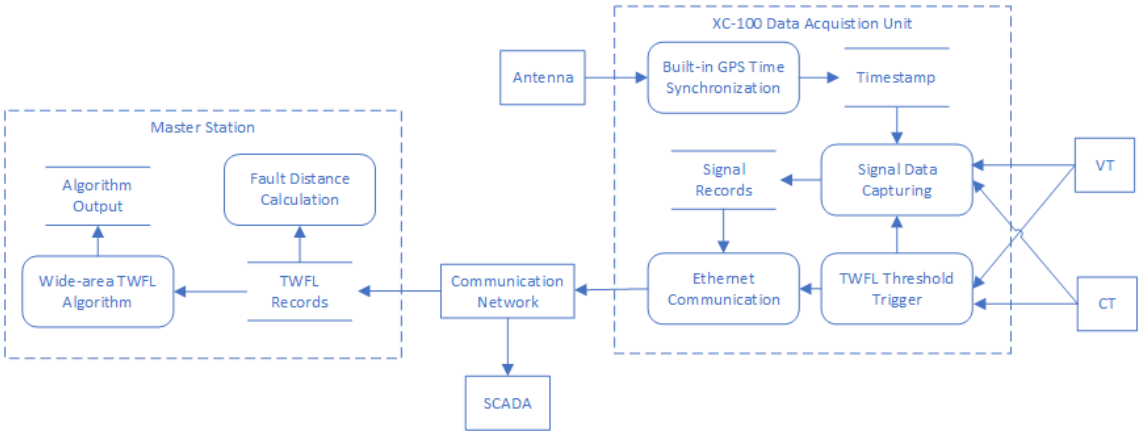

Figure 24. Wide-area TWFL system dataflow diagram

Table 12. contains the results of STRIDE-per-element analysis, which was performed for the DFD in figure 24. Spoofing and jamming of GPS signals expose several elements of the system to threats that could be classified as tampering and denial of service. Due to the nature of the wide-area TWFL algorithm a well-placed attack against a single substation could alter the result of the Algorithm Output drastically.

Table 12. STRIDE-per-element analysis for TWFL system

Diagram element	S	T	R	I	D	E
Antenna	x	x			x	
Built-in GPS Time Synchronization		x			x	
Timestamp		x			x	
Signal Data Capturing		x			x	
Signal Records		x				
Ethernet Communication		x				
Communication Network		x				
TWFL Threshold Trigger						
TWFL Records		x				
Fault Distance Calculation		x				
Wide-area TWFL Algorithm		x				
Algorithm Output		x				

The STRIDE-per-element analysis was used for performing more comprehensive threat analysis for the TWFL system. The results of this analysis can be seen in the table 13. containing the list of different types of threats that were recognized. Most of the recognized threats could be considered as tampering, affecting especially the elements, which are responsible for data storing and transfer.

Table 13. Threats affecting TWFL

Diagram element	Threat Type	Threat
Antenna	Spoofing	Receiving fake GPS signals
	Denial of Service	GPS signal jammed
Built-in GPS Time Synchronization	Tampering	Time drifted
	Denial of Service	Synchronization based on internal clock
Timestamp		Forged timestamp
		Timestamp generated by internal clock
Signal Data Capturing	Tampering	Disturbance captured with forged timestamp
	Denial of Service	Disturbance captured with timestamp based on internal clock
Signal Records	Tampering	Records contain inaccurate information
Ethernet Communication	Tampering	Transmitting incorrect records and events
Communication Network	Tampering	Forwarding incorrect records and events
TWFL Records	Tampering	Records contain incorrect data
Fault Distance Calculation	Tampering	Incorrect distance calculation due to corrupt data set
Wide-area TWFL Algorithm	Tampering	Incorrect disturbance fault and disturbance point identified
Algorithm Output	Tampering	Outputs incorrect disturbance fault and disturbance point identified

7.3.2 Potential attacks

The TWFL algorithm uses the substation which first detects the initial traveling wave as the central point between the other substations detecting the wave. The point of disturbance can be determined by the stations first detecting the wave, and the substations neighboring it can be used for confirming that the fault occurred on the transmission line between the stations which initially detected the fault. The preliminary selection of the dataset is based on preset threshold value of arrival times, if the arrival time is less than the threshold value the record is considered belonging to the same set (Chen et. al., 2013, p. 1210-1211). This information can be exploited for dropping a substation record out of the algorithm's input dataset. In the figure 23. the fault occurs in the line

between substations S1 and S2. The Attack tree presented in the figure 25. depicts a low-error TSSA for disqualifying a substation disturbance record from the algorithm's dataset in the TWFL system presented in the figure 23.

Figure 25. Attack tree for invalidating a substation record in TWFL system

The substation first detecting the traveling wave could also be changed with very similar attack. The only major differences are that the clock has to be drifted behind in time, the drift must not exceed the set threshold and the travel time of the wave also has to be

taken into account. If the spoofed substation record's timestamp is earlier than the substation's which really detected the disturbance first, then the algorithm considers the spoofed record as the central point for the calculation.

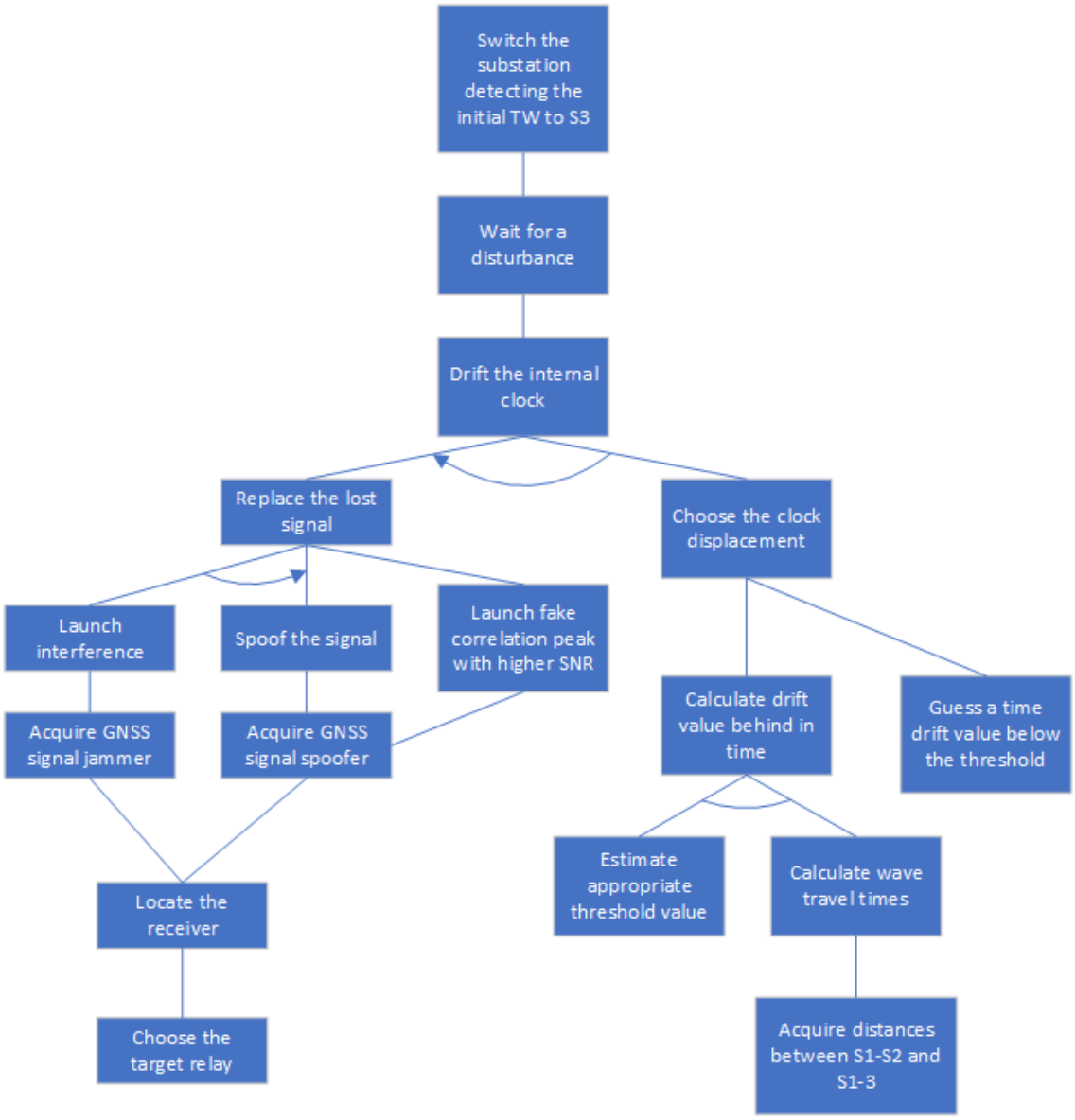

Figure 26. Attack tree for switching the initial detection substation

Neither of these attacks would actually prevent the algorithm from providing the correct result, but they affect the degree of confidence for the calculation. Preventing the algorithm from outputting the correct result, would require spoofing or jamming of multiple substations. In the latter case the algorithm would actually accept the record from S3 as

an input but would dismiss it during the calculation of confidence coefficients. The algorithm is an improvement an over typical double-end fault location as it provides safeguards against scenarios like this.

8 Mitigating GNSS based threats

This section attempts to provide threat mitigation techniques for GNSS based applications in power systems, but the mitigations presented here may also apply for other applications as well. The different root causes recognized during the literature review and threat analysis of the use cases are utilized as the foundation for different mitigations for the threats presented in this section. The table 14. contains the root causes and the mitigations proposed for them.

Table 14. Root causes and mitigations of GNSS based threats

Root Cause	Mitigation
GNSS spoofing	Encrypted signal Multi-antenna receiving architecture Adding redundancy Increase of detection capabilities GNSS receiver firmware updates Precautionary planning
GNSS jamming	Frequency switching Adaptive beamforming Multi-antenna receiving architecture Barriers Adding redundancy Increase of detection capabilities GNSS receiver firmware updates Precautionary planning
Ionospheric scintillation	Adaptive beamforming Adding redundancy Precautionary planning
Geomagnetic storms	Frequency switching Precautionary planning
Signal blockage	Antenna siting Removal of obstructive objects
Multipath	Antenna siting Removal of obstructive objects RF-absorptive coating Choke ring antennas
RF interference	Frequency switching Adaptive beamforming Barriers Adding redundancy

The mitigation propositions themselves are addressed separately in the following subsection. The mitigations presented here center only in options, which are viable in current industrial production environments. Kaplan & Hagerty (2017) and Morales-Ferre et. al. (2019) for example provide several different more experimental mitigation techniques, which are not readily available in commercial products at the time of writing. Since the applications utilizing GNSS in power grid environments are mainly concerned with the time synchronization the techniques presented here also contain mitigations solely addressing the loss of time synchronization in the said environments.

A risk evaluation was also performed for the recognized threats during the threat analysis of the use cases. The different threats were first generalized between the different use cases and treated by their root causes. The risk level of each threat by root cause was evaluated by utilizing the risk matrix presented in the section 3.3. The table containing the risk analysis is included in appendix 1.

8.1 Mitigation techniques

Encrypted signal would be the most obvious choice for mitigating the effects of spoofing by preventing it altogether. Switching over to encrypted signal would eliminate the chance of GNSS signal spoofing nearly completely as spoofing would require access to the encryption key. Unfortunately, currently the only encrypted signals available are reserved only for government and military use. This might change in the future though, as Galileo system shows promise of encrypted commercial signal known as High Accuracy Service, which will provide higher accuracy and encryption capabilities. Switching over to HAS and upgrading current devices to Galileo compatible receivers and time synchronization equipment might be an option to consider for the added security in the future. Also the future Galileo OS-NMA authentication mechanism will allow GNSS receivers to verify Galileo PNT information and it will work on a comparable basis to everyday encryption (Cozzens, 2021).

Multi-antenna receiving architecture is according to Morales-Ferre et. al., (2019, p. 268-269) the best candidate for detecting the presence of forged signals generated from the same source, by detecting the angle of arrival (AoA) of signals. Multi-antenna receiving can detect different pseudo-random noises (PRN) by using multiple receiving chains and by manipulating the post-correlation measurements for detecting the counterfeit signals arriving from the same direction. The multiple receiving chains can be implemented with array of multiple antennas or it can be emulated by moving a single antenna. Though multi-antenna receivers most often just add redundancy against signal jamming and only few vendors have multiple antenna receivers with spoofing detection capabilities available for purchase.

Frequency switching is effective countermeasure against GNSS jamming, but unfortunately is not effective against spoofing attacks. The technique relies on switching to an alternative frequency, when the primary band is affected by interference. It has been shown by a probabilistic analysis, that it is improbable that both L1/E1 and L5/E5 frequencies of GPS/Galileo systems are affected by interference and hopping between them is recommended. Frequency switching however requires a receiver capable of utilizing multiple frequencies and there are no guarantees, that the jammer is not jamming all GNSS frequency bands (Morales-Ferre et. al., 2019, p. 272-274). Rapid changes in the TEC also affect the GNSS signals during geomagnetic storms. The delays of pseudorange and carrier phase measures can be eliminated for the most part with dual frequency receiver equipment (Danson, 2011, p. 61).

Adaptive beamforming suppresses the direction interfering signals by controlling the antenna array and steering the remaining power towards GNSS satellites. The same technique is widely used in controlled radiation pattern antennas (CRPAs). There exist multitude of beamforming algorithms, but several of them require an estimate of the interference AoA for mitigating the effects of interference and ionospheric scintillation (Morales-Ferre et. al., 2019, p. 274; Kaplan & Hagerty, 2017, p. 591). The downside to this method is that it requires specialized smart antenna array.

Antenna siting is important for mitigating the effects of signal blockage and multipath. Kaplan & Hagerty (2017, p. 612-613) state that the **removal of obstructive objects** and **RF-absorptive coating** of reflective structures near the antenna can yield significant benefits. In environments like open fields, placing the antenna closer to the ground can decrease the amount of multipath errors, as the antenna receives reflections with shorter excess path delays. When there are obstacles near the horizon, the opposite approach is often beneficial as raising the antenna decreases the effects of multipath produced by dominant reflectors. **Choke ring antennas** have also been effective for mitigating multipath arrivals from the ground or low-elevation scatters.

Barriers can also be utilized as mitigations for RFI and jamming. Kaplan & Hagerty (2017, p. 585) provide few examples of using barriers as a mitigation. As a part of a military strategy handheld receiver antenna is operated below ground level in a foxhole, which permits the visibility of the SVs, but masks the antenna from ground level jammers. Another coincidental example is an antenna located on top of an aircraft. The aircraft body provides some protection from the ground-based RFI, though the barrier is not significant against strong ground-based jammers.

Adding redundancy can also mitigate the risks concerning time synchronization. The time synchronization can be switched to network-based time synchronization provided by IEEE 1588 and common time reference can be distributed through the network to other devices. Multiple GNSS synchronized master clocks can be installed into the network and if the spoofing or jamming of the current grandmaster clock is detected one of the non-compromised master clocks can take care of the time synchronization. Accurate atomic clocks, which are able to keep their clock discipline for extended periods of time can also be placed as a backup clock sources.

Increase of detection capabilities in the system allows carrying out pre-emptive measures like rerouting of the power transmission or steering the system towards safer

state, if the early signs of an attempted attack are detected. The less sophisticated attacks often expose themselves in various ways, Wei & Sikdar (2019, p. 1160) observed that random delays in timestamps can cause noticeable errors on the receiver location. Almas et. al. (2018, p. 4611) on the other hand note, that when PMUs are subjected to TSSA their internal oscillators need to resynchronize to the spoofed signal and report a large computation error in the phase angle.

GNSS receiver firmware updates are mostly undermined, since the receivers are often treated devices instead of computers as Nighswander et. al. (2012, p. 451) note. Updates often fix exploitable software flaws within the system. They can also contain enhancements for example to spoofing detection capabilities and even improvements to the signal processing or utilization of new and modernized signals. Attacks against outdated receiver software can potentially halt the services provided by the receivers for extended periods of time.

Precautionary planning is highly advisable for any situation and some threats like geomagnetic storms can be anticipated to some extent. Forecasts of solar activity for instance should be monitored and the activities planned accordingly for the periods of high solar activity. Predetermined emergency plans should also be devised for different scenarios of more imminent threats like spoofing and jamming, so the system can be brought down safely if needed.

9 Discussion and conclusions

The main objective of this thesis was to identify different kinds of GNSS based threats to power grid environments and find ways to mitigate them. The investigation was conducted through extensive literature review concentrating on how global navigation satellite systems work and how they are applied in power grid environments. The different threats presented in this work were identified by utilizing threat modeling techniques on use cases, which were found during the literature review. The identified threats served as a foundation for examining different options for mitigating GNSS based threats from available literature. The results of this study are the threat modeling artifacts based on the use cases, the risk evaluation for the generalized forms of identified threats and the proposed mitigations for these threats.

The examination of literature on the subject and the threat modeling process revealed, that there are various threats that can affect the GNSS based signal transfer and lead to severe consequences in power grid environments, as was to be expected. Some of these threats are naturally occurring like geomagnetic storms, some unintentional and others malicious in their intent. While most of the threats affecting GNSS signals only cause local disturbances, some of them can have system wide effects in power grid. Impacts of these threats can vary from minor monitoring errors to economically significant and possibly life-threatening large-scale blackouts.

During the course of this study multiple ways to mitigate GNSS based threats in power grid environments were uncovered. Redundancy can be built by using different satellite systems for time synchronization and precise on-site atomic clocks can be used as backup time sources. Multi-antenna architecture and beamforming can be utilized for eliminating the effects of interfering signals. Galileo's Public Regulated Service even shows promise, that spoofing attempts can be prevented nearly completely as encrypted signals become available for commercial use in future. Of course, none of these techniques are completely secure, some of them are more effective than others and some of them might be too expensive for any practical use when compared against the actual risks

involved. Nevertheless, the likelihood of unintentional interference from different consumer devices and services is growing rapidly, so implementing at least some forms of mitigations should be considered for reducing the risks involved.

One of the main motivations behind this thesis was to acquire concrete experience about analyzing security flaws by utilizing threat modeling techniques. The threat analysis for large cyber-physical systems proved out to be a challenging task as new elements to be considered constantly came up during the process. STRIDE-per-element performed adequately when a single point posing different threats was considered, but if combined threats (GNSS, Ethernet, physical sabotage etc.) were to be analyzed on similar systems, the outcome would likely be too vague and hard to interpret. Although analyzing combined threats with any STRIDE variant might require building multiple different threat models concentrating on different aspects of the system. The asset-centric STRIDE-per-element is a useful way for finding out the elements which are exposed to threats in a system, but STRIDE-per-interaction could provide a better alternative when developing protection strategies for large cyber-physical systems as Khan et. al. (2017) have already suggested in their work.

Based on the experience gained during this study, a more structured approach to threat modeling is proposed for any party actively analyzing threats on complex cyber-physical systems. Producing a rough STRIDE-per-element analysis for all the major components and subsystems reveals more interfaces that are exposed, potentially making the analysis more comprehensive. Compiling a library of common components and extending them when necessary assists the threat modeling process of the system under analysis and provides foundation for future modeling efforts, which consist of similar components and subsystems. As threat modeling is generally applied only in software development, this paper suggests further research on how threat modeling affects the system design of cyber-physical systems.

A number of ways for mitigating GNSS based threats in power grid environments were presented in this study. This work intentionally left out many mitigation techniques, which are theoretical or still under work, as the emphasis was on techniques which could be instantly taken into use without excessive effort and research. This subject still demands further investigation and the communities in electrical engineering, global navigation satellite systems and cyber-security are encouraged to collaborate with each other to figure out the problems and challenges that GNSS based threats pose to existing applications and systems.

References

Adrah, C. M., Kure, O., Yellajosula, J., Paudyal, S., & Mork, B. (2018, August). *A Methodology to Implement and Investigate Performance of Sampled Values for Wide-Area Protection*. Paper presented at 2018 2nd International Conference on Smart Grid and Smart Cities (ICSGSC), Kuala Lumpur, Malaysia 12.-14.8.2018. doi: https://doi.org/10.1109/ICSGSC.2018.8541290

Almas, M. S., Vanfretti, L., Singh, R. S., & Jonsdottir, G. M. (2018). Vulnerability of Synchrophasor-Based WAMPAC Applications' to Time Synchronization Spoofing. *IEEE Transactions on Smart Grid,* 9(5), 4601-4612. doi: https://doi.org/10.1109/TSG.2017.2665461

Bayliss, C. R., & Hardy, B. (2011). Transmission and Distribution Electrical Engineering (4. edition). Oxford: Elsevier Science & Technology. doi: https://www.doi.org/10.1016/C2009-0-64342-7

Begovic, M. M. (2012). System Protection. In Grigsby, B. L. L. (Ed.), Power System Stability and Control (3. Edition, p. **4**-1 - **4**-10). Boca Raton: CRC Press LLC. doi: https://doi.org/10.4324/b12113

Behrendt, K., & Fodero, K. (2006, May). *The Perfect Time: An Examination of Time-Synchronization Techniques.* Paper presented at 60th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, USA 3.-5.5.2006. Retrieved 2020-11-6 from https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/ 6226_PerfectTime_KB_20060309_Web.pdf?v=20180604-230308

Bhatta, B. (2010). Global Navigation Satellite Systems Insights into GPS, GLONASS, Galileo, Compass, and others. Global Media. ISBN:978-6612798924

Cai, J.Y., Huang, Z., Hauer, J.F., & Martin, K. (2005, August). *Current Status and Experience of WAMS Implementation in North America*. Paper presented at 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific, Dalian, China 18.8.2005. doi: https://doi.org/10.1109/TDC.2005.1546889

Castello, P., Muscas, C., Pegoraro, P. A., & Sulis, S. (2018, April). *Low-Cost Implementation of an Active Phasor Data Concentrator for Smart Grid.* Paper presented at 2018

Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy 16.-18.4.2018. doi: https://doi.org/10.1109/METROI4.2018.8428312

Chen, Y., Liu, D., & Xu, B. (2013). Wide-Area Traveling Wave Fault Location System Based on IEC61850. *IEEE Transactions on Smart Grid*, 4(2), 1207-1215. doi: https://doi.org/10.1109/TSG.2012.2233767

Chenine, M., Ullberg, J., Nordström, L., Wu, Y., & Ericsson, G. N. (2014). A Framework for Wide-Area Monitoring and Control Systems Interoperability and Cybersecurity Analysis. *IEEE Transactions on Power Delivery,* 29(2), 633-641. doi: https://doi.org/10.1109/TPWRD.2013.2279182

Cozzens, T. (2021). Tests begin of Galileo's OSNMA signal authentication service. *GPS World*, February 2021. Retrieved 2021-03-04 from https://www.gpsworld.com/tests-begin-of-galileos-osnma-signal-authentication-service/

Danson, E. (2011). Managing solar effects in GNSS operations. *PositionIT*, 33, 60-63. Retrieved 2020-12-16 from https://www.ee.co.za/wp-content/ uploads/legacy/ posit11/PositionIT_Aug-Sep11_60-63.pdf

DeCusatis, C., Lynch R. M., Kluge, W., Houston, J., Wojciak, P., & Guendert, S. (2019). Impact of Cyberattacks on Precision Time Protocol. *IEEE Transactions on Instrumentation and Measurement (Early Access)*, 1-13. doi: https://doi.org/ 10.1109/TIM.2019.2918597

Duncan, B. K., & Bailey, B. G. (2004). Protection, Metering, Monitoring, and Control of Medium-Voltage Power Systems. *IEEE Transactions on Industry Applications,* 40(1), 33-40. doi: https://doi.org/10.1109/TIA.2003.821809

Dutra, C. A., Cruz, I. H., Franzen, T. A., Matos, R. R., Neves, F. C., Oliveira, L. B., & Krefta, G. (2014, March). Paper presented at 12th IET International Conference on Developments in Power System Protection (DPSP 2014), Copenhagen, Denmark 31.3.-3.4.2014. doi: https://doi.org/10.1049/cp.2014.0008

Elgargouri, A., Elfituri, M. M., & Elmusrati, M. (2013, October). *IEC 61850 and smart grids.* Paper presented at 2013 3rd International Conference on Electric Power and

Energy Conversion Systems, Istanbul, Turkey 2.-4.10.2013. doi: https://doi.org/10.1109/EPECS.2013.6713080

European Global Navigation Satellite Systems Agency (2020). Galileo Services. Retrieved 2020-09-24 from https://www.gsa.europa.eu/galileo/services

Faria, L. A., Silvestre, C. A. M., Correia, M. A. F., & Roso, N . A. (2018). GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments. *Journal of Aerospace Technology and Management*, 10: e0618. doi: https://doi.org/ 10.5028/jatm.v10.870

Gao, G. X., Sgammini, M., Lu, Mingquan., & Kubo, Nobuaki (2016). Protecting GNSS Receivers From Jamming and Interference. *Proceedings of the IEEE,* 104(6), 1327-1338. doi: https://doi.org/10.1109/JPROC.2016.2525938

Georgakopoulos, D. & Quigg, S. (2017). Precision Measurement System for the Calibration of Phasor Measurement Units. *IEEE Transactions on Instrumentation and Measurement,* 66(6), 1441-1445. doi:https://doi.org/10.1109/TIM.2017. 2653518

Glomsvoll, O., & Bonenberg, L. K. (2017). GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea. *Journal of Navigation*, 70(1), 33-48. doi: https://doi.org/10.1017/S0373463316000473

Grimes, R. A. (2017). *Hacking the Hacker: Learn from the Experts Who Take down Hackers* (1. edition). Indianapolis: John Wiley & Sons, Inc. doi: https://doi.org/10.1002/9781119396260

Groves, P. D. (2013). Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems (2. edition). Boston: Artech House. ISBN: 978-1-60807-006-0

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara E Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management,* 43, 248-260. doi: https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Honeth, N., Khurram, Z. A., Zhao, P., & Nordström, L. (2013, June). *Development of the IEC 61850–9–2 software merging unit IED test and training platform.* Paper

presented at 2013 IEEE Grenoble Conference, Grenoble, France 16.-20.6.2013. doi: https://doi.org/10.1109/PTC.2013.6652385

Howard, M., & Lipner, S. (2006). *The Security Development Lifecycle* (1. edition). Redmond: Microsoft Press. ISBN: 978-07356-2214-2

Horowitz, S. H., Phadke, A. G., & Niemira J. K. (2014). *Power System Relaying*. Chichester: John Wiley & Sons, Inc. doi: https://doi. org/10.1002/9780470758786

Huang, X., Qin, Z., & Liu, H. (2018). A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access,* 6(2018), 69023-69035. doi:https://doi.org/10.1109/ACCESS.2018. 2879996

Hunkeler, U., Colli-Vignarelli, J., & Dehollain, C. (2012, June). *Effectiveness of GPS-jamming and counter-measures*. Paper presented at 2012 International Conference on Localization and GNSS, Starnberg, Germany 25.-27.6.2012. doi: https://doi.org/10.1109/ICL-GNSS.2012.6253115

Ingram, D. E., Schaub, P., & Campbell, D. A. (2012). Use of Precision Time Protocol to Synchronize Sampled-Value Process Buses. *IEEE Transactions on Instrumentation and Measurement,* 61(5), 1173-1180. doi: https://doi.org/10.1109/TIM.2011. 2178676

Jianfeng, W., Yonghui, H., Hongchung, L., Zaimin, H., Wenhe, Y. & Lulu, Y. (2016, April). *Research on the zoom technique of GNSS timing signal granularity*. Paper presented at 2016 European Frequency and Time Forum (EFTF), York, United Kingdom 4.-7.4.2016. doi: https://doi.org/10.1109/EFTF.2016.7477758

Kaplan, E. D., & Hegarty, C. J. (2017). *Understanding GPS/GNSS - Principles and Applications* (3. edition). London: Artech House.

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017, September). *STRIDE-based Threat Modeling for Cyber-Physicshoal Systems*. Paper presented at 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Torino, Italy 26-29.9.2017. doi: https://doi.org/10.1109/ISGTEurope.2017.8260283

Li, R., Zeng, X., & Wang, Y. (2011, October). *The application of precision clock synchronization technology based on PTP(IEEE1588) in traveling wave fault*

location system. Paper presented at 2011 International Conference on Advanced Power System Automation and Protection, Beijing, China 16.-20.10.2011. doi: https://doi.org/10.1109/APAP.2011.6180541

Liu, Y., Gao, H., Gao, W., Li, N., & Xiang, M. (2011, September). *A Design Scheme of Line Current Differential Protection Based on IEC61850.* Paper presented at 2011 IEEE Power Engineering and Automation Conference, Wuhan, China 8.-9.9.2011. doi: https://doi.org/10.1109/PEAM.2011.6134989

Luba, O., Boyd, L., Gower, A., & Crum, J. (2005). GPS III system operations concepts. *IEEE Aerospace and Electronic Systems Magazine,* 20(1), 10-18. doi: https://doi.org/10.1109/MAES.2005.1396789

Lundquist, D., Kunpeng, Z., & Ouksel, A. (2014, September). *Ontology-Driven Cyber-Security Threat Assessment Based on Sentiment Analysis of Network Activity Data.* Paper presented at 2014 International Conference on Cloud and Autonomic Computing, London, United Kingdom 8-12.9.2014. doi: https://doi.org/10.1109/ICCAC.2014.42

Malhotra, A., Cohen, I. E., Brakke, E., & Goldberg, S. (2016, February). *Attacking the Network Time Protocol*. Paper presented at 2016 The Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA 21-24.2.2016. doi: https://doi.org/10.14722/ndss.2016.23090

Mantel, H., & Probst, C. W. (2019, June). *On the Meaning and Purpose of Attack Trees*. Paper presented at 2019 IEEE 32nd Computer Security Foundations Symposium (CSF), Hoboken, NJ, USA 25-28.6.2019. doi: https://doi.org/10.1109/CSF.2019.00020

Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Cheeyee, T., & Candell, R. (2015, August). *Towards a systematic threat modeling approach for cyber-physical systems*. Paper presented at 2015 Resilience Week (RWS), Philadelphia, PA, USA 18-20.8.2015. doi: https://doi.org/10.1109/RWEEK.2015.7287428

Morales-Ferre, R., Richter, P., Falletti, E., de la Fuente, A., & Lohan, E. S. (2019). A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and

Unmanned Aircraft. *IEEE Communications Surveys & Tutorials*, 22(1), 249-291. https://doi.org/10.1109/COMST.2019.2949178

Moussa, B., Debbabi, M., & Assi, C. (2016). Security Assessment of Time Synchronization Mechanisms for the Smart Grid. *IEEE Communications Surveys & Tutorials,* 18(3), 1952-1973. doi: https://doi.org/10.1109/COMST.2016.2525014

National Coordination Office for Space-Based Positioning, Navigation, and Timing (2019). New civil signals. Retrieved 2019-09-13 from https://www.gps.gov/systems/gps/modernization/civilsignals/

Navipedia (2020). File:GNSS All Signals.png. Retrieved 2020-11-25 from https://gssc.esa.int/navipedia/index.php/File:GNSS_All_Signals.png

Navipedia (2021). Galileo Open Service Navigation Message Authentication. Retrieved 2021-03-04 from https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication

Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012, October). *GPS Software Attacks*. Paper presented at 2012 ACM conference on Computer and Communications Security, Raleigh, NC, USA 16-18.10.2012. doi: https://doi.org/10.1145/2382196.2382245

Niu, X., Yan, K., Zhang, T., Zhang, Q., Zhang, H., & Liu, J. (2015). Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers. *GPS Solutions*, 19(1), 141-150. doi: https://doi.org/10.1007/s10291-014-0375-7

Parashar, M., Giri, J. C., Nuqui, R., Kosterev, D., Gardner, R. M., Adamiak, M. Trudnowski, D., Chakrabortty, A., Menezes de Moreaes, R., Madani, V., Dagle J., Sattinger, W., & Novosel, D. (2012). Wide-Area Monitoring and Situational Awareness. In B. L. L. Grigsby (Ed.), Power System Stability and Control (3. edition p. **15**-1-**15**-41). Boca Raton: CRC Press LLC. doi: https://doi. org/10.4324/b12113

Phadke, A. G. (2002, October). *Synchronized phasor measurements ~ a historical overview.* Paper presented at 2002 IEEE/PES Transmission and Distribution Conference and Exhibition, Yokahama, Japan 6-10.10.2002. doi: https://doi.org/10.1109/TDC. 2002.1178427

Pozzobon, O., Wullems, C., & Detratti, M. (2010, December). *Security considerations in the design of tamper resistant GNSS receivers*. Paper presented at 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, Netherlands 8-10.12.2010. doi: https://doi.org/10.1109/NAVITEC.2010.5708066

Querol, J., Camps, A Manfredini, E. G., & Piriz, R. (2018, July). *An anti-jamming system for GNSS timing applications.* Paper presented at 2018 European Frequency and Time Forum (EFTF), Turin, Italy 10.-12.7.2018. doi: https://doi.org/ 10.1109/EFTF.2018.8409021

Rama Rao, P. V. S., Gopi Krishna, S., Vara Prasad, J., Prasad, S. N. V. S., Prasad, S. V. V. D., & Niranjan, K. (2009). Geomagnetic storm effects on GPS based navigation. *Annales Geophysicae,* 27, 2101-2110. doi: https://doi.org/10.5194/angeo-27-2101-2009

Richter, C. W. (2012). Generation Control: Economic Dispatch and Unit Commitment. In B. L. L. Grigsby (Ed.), Power System Stability and Control (3. edition p. **21**-1 - **21**-18). Boca Raton: CRC Press LLC. doi: https://doi. org/10.4324/b12113

Schweitzer, E. O., Guzmán, A., Altuve H. J., & Tziouvaras D. A., Needs, J. (2010, March). *Real-Time Synchrophasor Applications for Wide-Area Protection, Control, and Monitoring.* Paper presented at 10th IET International Conference on Developments in Power System Protection (DPSP 2010), Manchester, UK 29.3.-1.4.2010. doi: https://doi.org/10.1049/cp.2010.0343

Schweitzer, E. O., Guzman, A., Mynam, M. V., Skendzic, V., Kasztenny, B., & Marx, S. (2016). Protective Relays with Traveling Wave Technology Revolutionize Fault Locating. *IEEE Power and Energy Magazine,* 14(2), 114-120. doi: https://doi.org/10.1109/MPE.2016.2543123

Seth, N., & Kazi, F. S. (2018, December). *Vulnerability of Intelligent Electronic Devices (IED) to Time Synchronization Spoofing in Power Grid and Jamming of GNSS Receiver*. Paper presented at 2018 IEEE 8th Power India International Conference (PIICON), Kurukshetra, India 10.-12.12.2018. doi: https://doi.org/10.1109/POWERI.2018. 8704422

Shepard, D. P., Humphreys, T. E., & Fansler, A. A. (2012). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4), 146-153. doi: https://doi.org/10.1016/j.ijcip.2012.09.003

Shostack, A. (2014). *Threat Modeling: Designing for Security* (1. edition). Indianapolis: John Wiley & Sons, Inc.

Sikirica, N., Špoljar, D., Lawon, B., & Rabiu, B. (2018, September). *Impact of Geomagnetic Storm on GPS Positioning Performance.* Paper presented at 60th International Symposium ELMAR-2018, Zadar, Croatia 16.-19.9.2018. doi: https://doi.org/10.23919/ELMAR.2018.8534673

Sukumara, T., Starck, J., Vellore, J., Kumar, E., & Harish, G. (2018, March). *Cyber security — Securing the protection and control relay communication in substation.* Paper presented at 2018 71st Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA 26.-29.3.2018. doi: https://doi.org/10.1109/CPRE.2018.8349788

Swamy, K. (2017). Global navigation satellite system and augmentation. *Resonance,* 22(12), 1155-1174. doi: https://doi.org/10.1007/s12045-017-0579-6

Terzija, V., Valverde, G., Cai, D., Regulski, P., Madani, W., Fitch, J., Skok, S., Begovic, M., Phadke, A. (2011). Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. *Proceedings of the IEEE*, 99(1), 80-93. doi: https://doi.org/10.1109/JPROC.2010.2060450

The Institute of Electrical and Electronics Engineers (2013). *IEEE Guide for Phasor Data Concentrator Requirements for Power System Protection, Control, and Monitoring* (IEEE Std C37.244™-2013). doi: https://doi.org/10.1109/IEEESTD.2013.6514039

Tiusanen, R. (2008). Qualitative Risk Analysis. In Möller, N., Hansson S. O., Holmberg, J., & Rollenhagen, C. (Ed.), Handbook of Safety Principles (Vol. 9, p. 463-492). Hoboken, NJ: John Wiley & Sons, Inc. ISBN: 978-1-11895-069-2

Watt, S. T., Achanta, S., Abubakari, H., Sagen, E., Korkmaz, Z., & Ahmed, H. (2015, December). *Understanding and Applying Precision Time Protocol.* Paper

presented at 2015 Saudi Arabia Smart Grid (SASG), Jeddah, Saudi Arabia 7.-9.12.2015. doi: https://doi.org/10.1109/SASG.2015.7449285

Wei, X., & Sikdar, B. (2019, February). *Impact of GPS Time Spoofing Attacks on Cyber Physical Systems*. Paper presented at 2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, Australia 13.-15.2.2019. doi: https://doi.org/10.1109/ICIT.2019.8755016

Wei-ming, W., Xiong-ying, D., & Yan, L. (2011, July). *The research and development of an intelligent merging unit based on IEC61850-9-2*. Paper presented at 2011 4th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Weihai, Shandong, China 6.-9.7.2011. doi: https://doi.org/10.1109/DRPT.2011.5994084

Xiang, Y., Wang, L., & Zhang, Y. (2018). Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. *International Journal of Electrical Power and Energy Systems,* 96, 368-379. doi: https://doi.org/10.1016/j.ijepes.2017.10.004

Yao, L., Jianjuan, W., & Yunlong, L. (2012, August). *The Research Of Time Unified System In Smart Grid*. Paper presented at 7th International Conference on Communicationsand Networking in China, Kung Ming, China 8-10.8.2012. doi: https://doi.org/ 10.1109/ChinaCom.2012.6417453

Zhang, Z., Gong, S., Dimitrovski, D. D., & Li, H. (2013). Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Transactions on Smart Grid,* 4(1), 87-98. doi: https://doi.org/10.1109/TSG.2012.2227342

Appendices

Appendix 1. Risk evaluation for identified threats

Threat	Root Cause	Severity
Protection scheme triggers	GNSS spoofing	High
	GNSS jamming	High
	Ionospheric scintillation	Moderate
	Geomagnetic storms	Low
	Signal blockage	Low
	Multipath	Low
	RF interference	Moderate
Protection scheme failure	GNSS spoofing	High
	GNSS jamming	Low
	Ionospheric scintillation	Low
	Geomagnetic storms	Low
	Signal blockage	Negligible
	Multipath	Negligible
	RF interference	Negligible
Monitoring disturbed	GNSS spoofing	High
	GNSS jamming	High
	Ionospheric scintillation	Moderate
	Geomagnetic storms	Low
	Signal blockage	Low
	Multipath	Low
	RF interference	Low
False events in event log	GNSS spoofing	High
	GNSS jamming	Moderate
	Ionospheric scintillation	Low
	Geomagnetic storms	Low
	Signal blockage	Low
	Multipath	Low
	RF interference	Moderate
Events unlogged in event log	GNSS spoofing	Moderate
	GNSS jamming	Moderate
	Ionospheric scintillation	Negligible
	Geomagnetic storms	Negligible
	Signal blockage	Negligible
	Multipath	Negligible
	RF interference	Low

Time synch. drifted	GNSS spoofing	High
	GNSS jamming	Moderate
	Ionospheric scintillation	Low
	Geomagnetic storms	Low
	Signal blockage	Low
	Multipath	Negligible
	RF interference	Low
Time synch. Lost	GNSS spoofing	Low
	GNSS jamming	High
	Ionospheric scintillation	Low
	Geomagnetic storms	Moderate
	Signal blockage	Low
	Multipath	Low
	RF interference	Moderate
False monitoring data	GNSS spoofing	High
	GNSS jamming	Low
	Ionospheric scintillation	Negligible
	Geomagnetic storms	Negligible
	Signal blockage	Negligible
	Multipath	Negligible
	RF interference	Low
False control data	GNSS spoofing	High
	GNSS jamming	Low
	Ionospheric scintillation	Low
	Geomagnetic storms	Low
	Signal blockage	Low
	Multipath	Low
	RF interference	Low