Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Gustav Oskar Sivertsen

Observable Effects of Selected Phasor Measurement Unit Time Delay Attacks

Master's thesis in Experience-based Master in Information Security
Supervisor: Prof. Stephen D. Wolthusen
Co-supervisor: Dr. James G. Wright
June 2023

NTNU
Norwegian University of
Science and Technology

Gustav Oskar Sivertsen

Observable Effects of Selected Phasor Measurement Unit Time Delay Attacks

Master's thesis in Experience-based Master in Information Security
Supervisor: Prof. Stephen D. Wolthusen
Co-supervisor: Dr. James G. Wright
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

The traditional electric power grid, which delivers electric power to consumers, is in the process of being transformed from a system that is closed and centrally controlled to a network-controlled automated system for delivering electric power to consumers. As part of this transformation, the control and monitoring subsystems of the classic power grid are transformed from being a location-based closed system, to an Internet-connected Smart Grid. In addition, network-connected devices are distributed that measure and adjust power consumption to the location of power consumers.

The transition described opens up the possibility that the power distribution infrastructure could become an offering for malicious cyber-attacks, with the potential intent of causing power outages, as well as serious damage to critical power grid infrastructure. The topic of my thesis is to investigate the potential effects of setting phasor measurement devices for time delay attacks, by exploiting known vulnerabilities in the IEEE 1588 Precision Time Protocol, observing any consequences such exposure may have on Synchrophasor measurements, as well as attack detection capabilities.

The master's thesis deals with security threats aimed at smart networks for the distribution of electrical energy. As part of the modernization of the power grid to meet future needs, the infrastructure has been connected to the Internet. This entails security challenges, in that malicious actors can carry out internet-based attacks on the infrastructure. In addition, the new infrastructure has an increased need for continuous monitoring, so that the requirement for precision related to monitoring events with a correct time stamp is a key to getting a correct overview of the system's condition. If actors can interfere with the mechanisms that calculate the time stamps of critical distribution components, the operators who monitor and control systems get the wrong decision basis, which can lead to an incorrect response, based on an incorrect basis. The time stamps are calculated based on time data, often obtained from clocks synchronized via GPS, but also via clock synchronization over the network-based PTP protocol. The theme of the master's thesis is the extent to which smart power distribution systems are vulnerable to the fact that targeted modification of the clock signal means that errors in time calculations create operational disruptions based on an incorrect understanding of the situation.

As part of the task, simulations are run in MATLAB and Simulink which show

results that are predictable enough to be optimized in connection with further work.

Sammendrag

Det tradisjonelle elektriske kraftnettet, som leverer elektrisk kraft til konsumenter, er i ferd med å bli transformert fra et system som er lukket og sentralstyrt et nettverksstyrt automatisert system for å levere elektrisk kraft til forbrukere. Som en del av denne transformasjonen transformeres kontroll- og overvåkingsundersystemene til det klassiske strømnettet fra å være et lokasjonsbasert lukket system, til et Internett-tilkoblet Smart Grid. I tillegg distribueres nettverkstilkoblede enheter som måler og justerer strømforbruket til strømforbrukernes plassering.
Overgangen som beskrives åpner muligheten for at kraftdistribusjonsinfrastrukturen kan bli et tilbud for ondsinnede cyberangrep, med den potensielle hensikten å forårsake strømbrudd, samt alvorlig skade på kritisk kraftnettinfrastruktur. Temaet for oppgaven min er å undersøke potensielle effekter av å sette faseormåleenheter for tidsforsinkelsesangrep, ved å utnytte kjente sårbarheter i IEEE 1588 Precision Time Protocol, observere eventuelle konsekvenser slik eksponering kan ha på Synchrophasor-målinger, samt angrepsdeteksjonsevne.
Masteroppgaven omhandler sikkerhetstrusler rettet mot smart nettverk for distribusjon av elektrisk energi. Som en del av moderniseringen av strømnettet for å møte framtidige behov, har infrastrukturen blitt tilknyttet Internett. Dette medfører sikkerhetsmessige utfordringer, ved at ondsinnede aktører kan utføre internettbaserte angrep på infrastrukturen. I tillegg har den nye infrastrukturen et økt behov for kontinuerlig overvåking, slik at kravet til presisjon relatert til åvå hendelser med korrekt tidsstempel er en nøkkel for å få en korrekt oversikt over systemets tilstand. Dersom aktører kan forstyrre mekanismene som beregner tidsstemplene til kritiske distribusjonskomponeneter, får operatørene som overvåker og styrer systemer feil beslutningsgrunnlag, noe som kan føre til feilaktig respons, basert på feilaktig grunnlag. Tidsstemplene blir beregnet basert på tidsdata, ofte hentet fra klokker synkronisert via GPS, men også via klokkesynkronisering over den nettverksbaserte PTP-protokollen. Masteroppgavens tema er i hvilken grad smarte kraftdistribusjonssystemer er sårbare for at målrettet modifisering av klokkesignalet medfører at feil i beregninger av tid skaper driftsforstyrrelser basert på en feilaktig situasjonsforståelse.
Som en del av oppgaven kjøres simularinger i MATLAB og Simulink som viser resultater som er forutsigbare nok til å kunne optimaliseres i forbindelse med videre arbeid.

Acknowledgments

I would first like to sincerely thank my supervisor, **Prof. Stephen D. Wolthusen**, for his invaluable involvement and guidance during the entire duration of my master's thesis project, from the definition of the route for me to take in order to complete the thesis, as well as on the way to project completion.

I would also like to express my thanks to my co-supervisor **Dr. James G. Wright**, for his invaluable support and guidance during the last part of my project.

Figures

Tables

Acronyms

CI Critical Infrastructure. 12, 27

CPG Conventional Power Grid. 4–7, 9

CPS Cyber-Physical System. 6, 7, 12

EU European Union. 8

FN False Negative. 34

FP False Positive. 34

GNSS Global Navigation Satellite System. 20, 21

GPS Global Positioning System. 20

ICS Industrial Control System. 7

IEEE Institute of Electrical and Electronics Engineers. 1

LAN Local Area Network. 12

MitM Man in the Middle. 28

MotS Man on The Side. 28–30

NIST National Institute of Standards and Technology. 1, 8, 9

NTP Network Time Protocol. 21, 23

PDC Phasor Data Concentrator. 2, 13–16, 18, 19, 23, 25

PG Power Grid. 1, 2, 6, 11, 12, 18, 19, 27, 28

PMU Phasor Measurement Unit. 2, 3, 13–15, 18–21, 23–25, 31–33, 36, 39, 45, 73–75

PTP Precision Time Protocol. 3, 4, 16, 19–21, 23, 29–31

SCADA Supervisory Control And Data Acquisition. 1, 2, 6, 11, 12, 15, 23, 24

SE State Estimation. 2, 16, 18

SG Smart Grid. 1–9, 12–17, 19–21, 24, 27, 28, 31, 37

TDA Time Delay Attack. 3, 4, 16, 20, 31, 35

TN True Negative. 34

TP True Positive. 34

WAMS Wide Area Measurement System. 2–4, 8, 9, 13–21, 23–25

Contents

Chapter 1

Introduction and Scope

During the last few centuries, the society has become increasingly dependant on access to a stable and reliant supply of electrical power. The usage of electrical power in order to provide heating, lighting, as well as running various electrical appliances, like washing machines and wireless access points, has created an increased demand for electricity. The increased demand for electricity has transformed the classical Power Grid (PG) infrastructure, initially consisting of local electricity distribution infrastructure, into a nation-wide power distribution infrastructure network, known as the Smart Grid (SG).

1.1 Background

As described in [1], electricity is supplied by the Power Grid infrastructure, consisting of power generating facilities,[1] and transmitted via a high voltage transmission infrastructure, before being converted to lower voltage electrical currents, fed to the distribution infrastructure for distribution to paying consumers.

The classic Power Grid was under manual and centralised control, and monitored through a centralised and unidirectional Supervisory Control And Data Acquisition (SCADA) system. The progressively increasing dependency on a reliable supply of electrical power makes it vital to avoid power outages, which will result in reduced temperature in buildings lacking alternative sources of heating, as well as the absence of vital services, like electronic payments, telecommunications, and transportation. Therefore, several organisations, like the National Institute of Standards and Technology (NIST) and the Institute of Electrical and Electronics Engineers (IEEE)[2] has made considerable efforts in order to produce standards, in order to define the Smart Grid.

[1] like hydro-based facilities utilising water to generate electricity, or nuclear power plants.

[2] amongst others.

1.1.1 The conversion of the Power Grid to the Smart Grid.

In order to address the future demands for electrical power, the uni-directional control mechanisms of the traditional power grid is replaced by the bidirectional flow of information characteristic of the modern SG. The control mechanisms of the modern SG infrastructure is utilising standardised computer networking technology for bidrectional communication. In order to meet the new requirements for monitoring, the PG is connected to the Internet. The authors of [2] describes the transition from the classical power grid to the smart grid as unavoidable.

For the system to meet the Smart Grid monitoring and control capability requirements, the Wide Area Measurement System (WAMS) has been implemented. A number of Phasor Measurement Units are connected to a Phasor Data Concentrator, which transmits synchronised phasors to the WAMS Control Center. The usage of the resulting synchrophasors enables the SG operators to get a more fine-grained view of the operational state of the SG, than obtainable by a classic SCADA system. As part of a modern WAMS system, State Estimation (SE) algorithms has been developed, in order to counter cyber attacks or unintentional PG failures. In addition to the SE algorithms, several security enhancements to relevant SG protocols are being implemented in an attempt to reduce the attack surface available to potential threat actors.

1.1.2 Security vulnerabilities of the Smart Grid WAMS

As a consequence of the Smart Grid infrastructure being connected to the Internet, the infrastructure is becoming vulnerable to cyber attacks. The Smart Grid Wide Area Measurement System is the main control system of the SG and, as such, constitutes a complex system vulnerable to numerous cyber attacks, as identified by several papers, like for instance [3] and [4].

The modern interconnected SG, featuring a WAMS system receiving an increasing number of synchronised phasors,[3] is increasingly dependant on synchronised time. In [5], several types of cyber attacks are identified. Most of the attacks described by Ullmann and Vögeler in [5], with the exception of the "Delay of synchronization messages" attack are, to some extent, being mitigated by various means. The Delay synchronization messages attack however, may[4] prove to be a stealthy attack, thereby avoiding detection. The aim of these sophisticated threat actors would, therefore, be to stay undetected, while creating a substantial amount of disturbance to the operation of the SG.

My thesis will be focusing on time delay attacks against PMUs, and investigate which effects a number of selected delay attacks may have on the PMU output, as visualised by a simulation.

[3] Phasors are synchronised at PMUs, before being transferred via PDCs to the WAMS,

[4] if performed by a sophisticated threat actor having sufficient knowledge of valid traffic patterns.

1.2 Definition of scope

As Moussa, Debbabi and Assi denotes in TABLE II of [6, p. 1959], the paper [5][5] by Ullmann and Vögeler, is lacking experimental verification of the attack, the countermeasures suggested, *as well as any effects of the PTP delay attack*.
Given the unresolved TDA vulnerability of the PTP, in addition to the absence of a description of any effects of the attack, identified by [6] as a disadvantage of [5], my contribution will, specifically, be to investigate possible effects of exposing a Phasor Measurement Unit to a Time Delay Attack.

1.3 Research questions

The main goal of my project, is thus to investigate which potential effects a selection of Time Delay Attacks might have on PMU output.
In order to proceed with the Time Delay Attack vulnerability investigation, I have selected the following research questions:

1. Which effects of the time delay attack simulations covered by this study, is observable on the visualised output of the PMU simulated?
2. For a selected similarity requirement, what delay level could be observed as being within similarity tolerance levels?
3. Which of the delay functions covered would be preferred, in order for the malicious threat actor to stay undetected?

In order to investigate the topic further, I will conduct a theoretical study of relevant concepts, before performing a number of experiments before discussing the results presented, with the aim of being able to conclude on possible answers to the research questions.

1.4 Outline of the rest of the thesis

This introductory chapter is followed by a theoretical part, consisting of a chapter introducing the (smart) power grid, followed by chapters covering topics like the WAMS control system, Smart Grid (SG) power flows status monitoring, and Smart Grid cyber attacks and threat actors.
The remaining chapters covers the experimental investigation of the Time Delay Attack on Phasor Measurement Unit output. The methodology chapter includes a detailed description of the model implementation and usage, before a number of experiments are presented and described in detail. My thesis is finalised by the inclusion of a chapter presenting results, before the discussion and conclusion chapters, including the suggestions for further work, at the end of the thesis.

[5] The paper, entitled "Delay attacks — Implication on NTP and PTP Time Synchronization", is identifiable as reference [13] in [6].

To summarise the content of each of the remaining Chapters:

- Chapter2 presents a brief introduction to Power grids, focusing on the transition from the Conventional Power Grid to the Smart Grid.
- Chapter 3 presents the power grid control system, known as the Wide Area Measurement System (WAMS)
- Chapter 4 Considers the status flow monitoring of th Smart Grid, covering WAMS benefits and security issues.
- Chapter 5 Considers attacks, mainly the PTP Time Delay Attack.
- Chapter 6 Provides the methodological background for the thesis, as well as a description of the model used for running the simulations.
- Chapter 7 Presents and interprets the results
- Chapter 8 Discusses the observed tendencies visible by the results.
- Chapter 9 Finalises, with Conclutions, and suggestions for future work.

Chapter 2

The power grid

2.1 The Conventional Power Grid

The Conventional Power Grid (CPG) is described in several papers, and books like [1], as a uni-directional, manually controlled, power distribution system.

2.1.1 Overview of the Conventional Power Grid

The Conventional Power Grid is a system by which electric power is centrally generated, transmitted, and distributed to industrial, residential,and commercial end users, in order to ensure a reliable access to a sufficient amount of electrical energy. The Conventional Power Grid, as described in [1], consists of the following subsystems, visualised in figure 2.1:

- The **Generation Subsystem** which Generates electric power from various sources of energy, to be transmitted for distribution to Consumers. Some examples of installations generating electrical power are nuclear power plants, as well as hydroelectric power plants, feeding water-driven turbines in order to generate power.
- The **Transmission Subsystem** which transmits electric power from the Generation subsystem to the Distribution Subsystem. The current is transmitted via high voltage power lines, minimising energy loss over longer distances.
- The **Distribution Subsystem** which distributes electric power to end users, after converting the high voltage input into lower voltage levels, suitable for consumption.

2.1.2 Characteristics of the Conventional Power Grid

In order to provide a description of the Smart Grid (SG), a description of the characteristics of the Conventional Power Grid is provided.

As described in [1] by Blume, some of the characteristics of the Conventional Power Grid are:

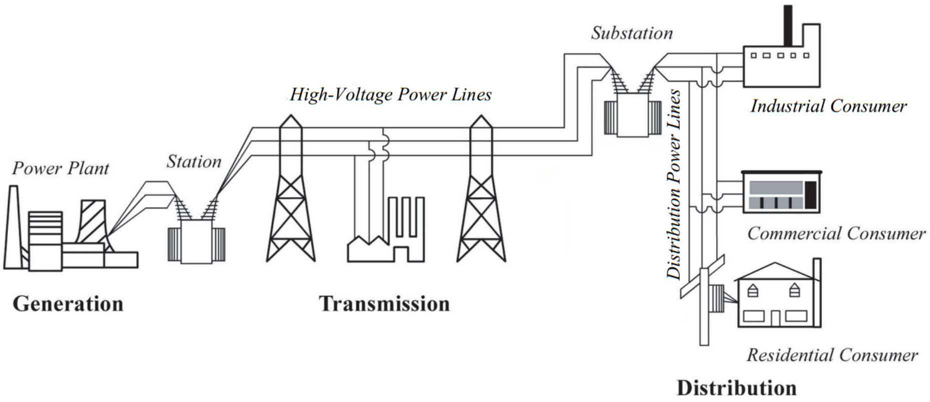


Figure 2.1: Power Grid System Overview , as presented in [1]

- Power is generated in real time. In the event a consumer is "flipping a power switch," the power grid must have sufficient resources in order to keep the voltage levels at an acceptable level.
- The Conventional Power Grid is controlled by a central management facility known as the Supervisory Control And Data Acquisition (SCADA) subsystem. The monitoring and management of the PG is initiated from the Control Center, utilising unidirectional communication channels.
- The Conventional Power Grid Supervisory Control And Data Acquisition subsystem is offline, i. e. not connected to any publicly available computer network, and thus unavailable from the Internet. Therefore, operational duties must be performed by authorised personnel physically located[1] at designated operational sites.

The Conventional Power Grid originates from the local society-serving power generation facilities initiating the supply of electrical power, which over the years were interconnected to form a grid, connecting consumers to a network of several power generating facilities, providing a more flexible power distribution infrastructure. As described in Chapter 2.3 of [7] , the Conventional Power Grid is facing challenges, related to Black Outs adhering to the increased demands for electrical power.

2.2 The Smart Grid

2.2.1 Overview of The Smart Grid

The Smart Grid (SG) is, as described by Humayed, Lin, Li and Luo in [8], the modernisation of the Conventional Power Grid (CPG), into what may be described as an exapmle of a Cyber-Physical System (CPS).

[1] External personnel must physically travel to the site, to perform maintenance tasks, for instance.

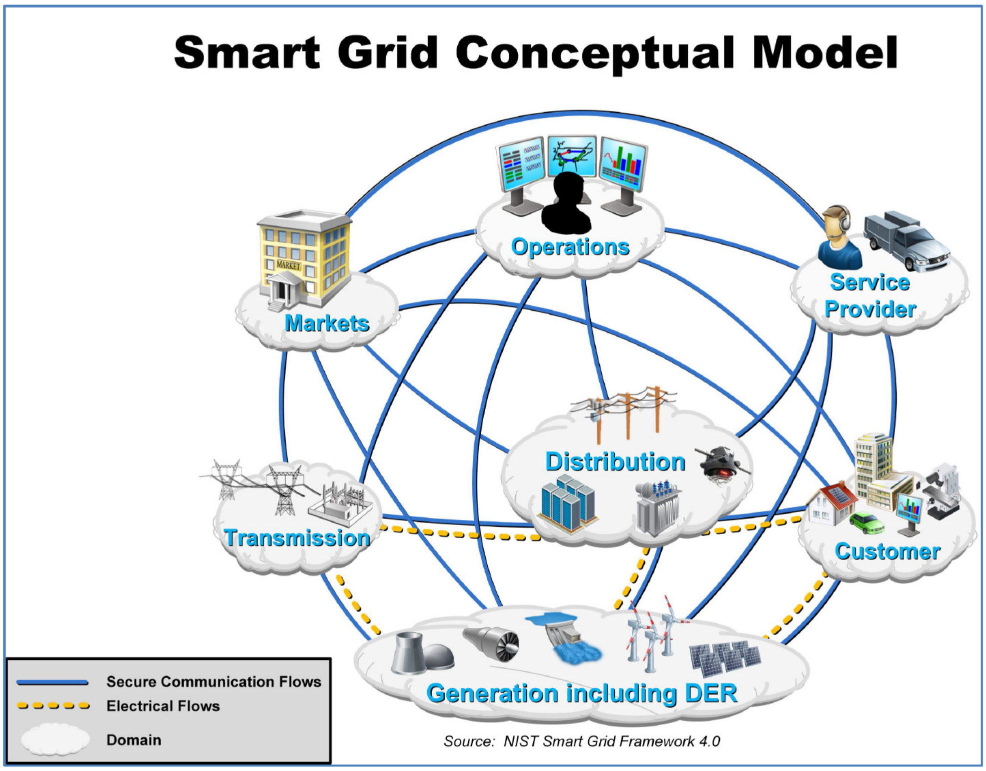


Figure 2.2: Updated Smart Grid conceptual model, as presented in [9, p. 13], Figure 4

Cyber-Physical System

As described by Humayed, Lin, Li and Luo in [8], a Cyber-Physical System (CPS) is characterised by using a computer-based system in order to control and monitor systems of the physical world. The CPS is utilised in order to control physical systems from various fields of applications. Humayed et. al., in [8], describes as various appliances as Industrial Control System (ICS), Medical Devices, and Smart Grid. The Smart Grid, therefore, is an example of a Cyber-Physical System (CPS), consisting of the physical system of a Power Grid, under the control of a network/Cyberspace-connected system.

Due to the shortcomings of the CPG previously[2] covered, the SG might be described as an effort to reduce the risk of blackouts, and to generally make the power distribution system more robust and reliable, meeting the increasing demand for electrical power.

[2] Refer to subsection 2.1.2, and Chapter 2.3 of [7]

	Domain	Roles/Services in the Domain
1	**Customer**	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own sub-domain: residential, commercial, and industrial.
2	**Markets**	The facilitators and participants in electricity markets and other economic mechanisms used to drive action and optimize system outcomes.
3	**Service Provider**	The organizations providing services to electrical customers and to utilities.
4	**Operations**	The managers of the movement of electricity.
5	**Generation Including DER**	The producers of electricity. May also store energy for later distribution. This domain includes traditional generation sources and distributed energy resources (DER). At a logical level, "generation" includes those traditional larger scale technologies usually attached to the transmission system, such as conventional thermal generation, large-scale hydro generation, and utility-scale renewable installations usually attached to transmission. DER is associated with generation, storage, and demand response provided in the customer and distribution domains, and with service provider-aggregated energy resources.
6	**Transmission**	The carriers of high voltage electricity over long distances. May also store and generate electricity.
7	**Distribution**	The distributors of electricity to and from customers. May also store and generate electricity.

Table 2.1: Domains and roles/services in the smart grid conceptual model, as presented in Table 1 of [9]

2.3 Smart Grid models

In order to improve the understanding of a vastly complex system like the Smart Grid, some organisations, like the National Institute of Standards and Technology (NIST), as well as the European Union (EU) commission for SG, is maintaining theoretical models. I have chosen to present a brief overview of the NIST model in order to provide a brief overview of various parts of the Smart Grid, and thereafter focus on the Wide Area Measurement System and related concepts.

2.3.1 The NIST Conceptual model

In order to improve the understanding of a vastly complex system like the Smart Grid, the National Institute of Standards and Technology (NIST) is maintaining the Conceptual model of the Smart Grid. The graphical visualisation of the model, as presented in [9, p. 13], Figure 4, is shown in Figure 2.2. The Smart Grid adds Information and Communication Technology (ICT) to the Conventional Power Grid, in order to transform the unidirectional communication lines of the monitoring and control infrastructure of the Conventional Power Grid, into an infrastructure utilising two-way communication between the various parts of the Smart Grid infrastructure.

The Smart Grid Domains

Table 2.1 gives an overview of the roles and services of the SG domain as presented by NIST in [9].

The Smart Grid is a complex system, involving many aspects like, for instance applications, various kinds of layers and relations between domains, to name a few, topics which it will be beyond the scope of this thesis to cover. My thesis will focus on various aspects of the SG Wide Area Measurement System for the remaining part of the thesis.

Chapter 3

The Power Grid Control System

3.1 The Conventional Power grid control system

The SCADA system constituted the core part of the control center of the classic Power Grid, utilising one-directional communication lines in order to manually control and monitor the operational state of the power grid. Figure 3.1 shows the main components of the SCADA system.

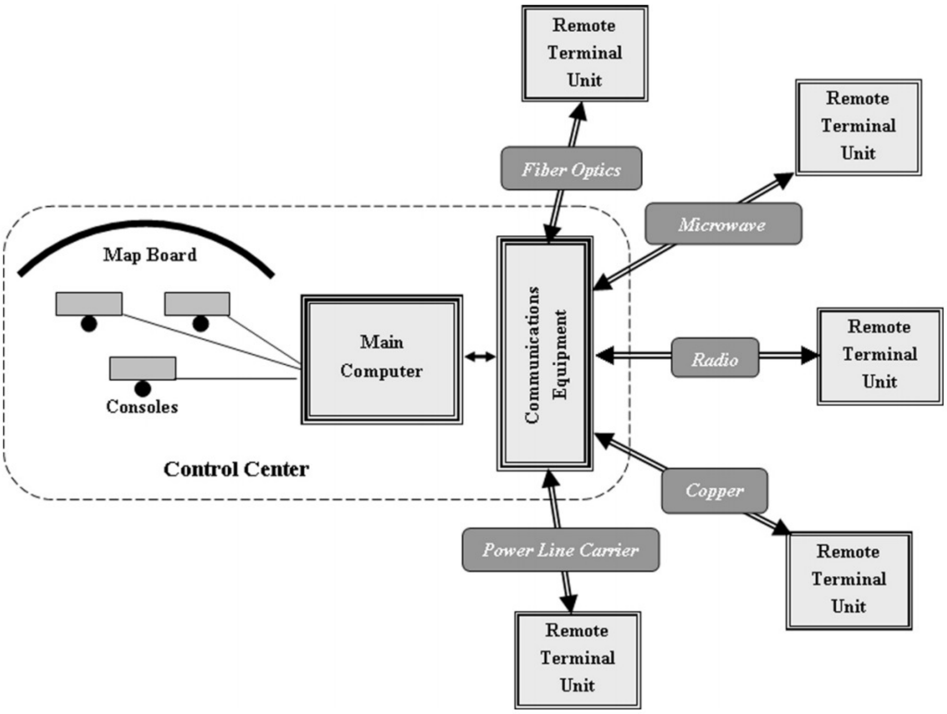


Figure 3.1: SCADA system , as presented in [1]

A centrally located control center, optionally being backed up by control centers at one or more locations for redundancy, displays status information from the equipment at the associated substations, received for monitoring purposes. As a response to alarms indicating operational issues, commands enabling remote control of affected infrastructure is issued in order to address the issue, in order to resolve the issue and receive updated status information clearing the alarm.

3.2 The Smart Grid Control System

Analogous with the modernisation of the classic Power Grid into the Smart Grid, the SCADA subsystem of the PG is the predecessor of the control system of the modern Smart Grid. Therefore, a description of the SCADA system, evolving from the centralised subsystem controlling the Classic PG, to the modernised version of the SCADA subsystem, initiates the description of the Smart Grid Control System.

The characteristics of the three generations of SCADA system described by Alcaraz, Fernandez and Carvajal in [10], may be summarised below:

1. A Monolithic SCADA system utilises a centralised offline control center infrastructure, in order to monitor and control the physical system by proprietary control mechanisms.
2. A Distributed SCADA system utilises a networked, but centralised control center in order to monitor and control the physical system by proprietary control mechanisms.
3. A Networked SCADA system utilises a networked, and online control center in order to monitor and control the physical system by standardised control mechanisms.

3.2.1 The Modernised SCADA system

The SCADA system isa system utilised to supervise and control Critical Infrastructure (CI) systems, including PG infrastructures. Initially designed in order to control physical infrastructure systems like the classic Power Grid, the Monolithic SCADA system emerged into the Distributed SCADA system. The transition from a Monolithic SCADA system to a Distributed SCADA system transforms, as indicated by , the central management center from a centrally controlled mainframe environment, to a networked server environment controlled by operators connected through a Local Area Network (LAN)
The SG control center emerged from the Distributed SCADA system, into the Networked SCADA system used in order to control modern Cyber-Physical Systems, like the SG.

However, as explained by Zamani, Panahi, Abyaz and Alhelou in [11], the SCADA system has a number of shortcomings, making it unsuitable for a SG enegy distribution monitoring system:

- The data polling rate is once every 2-10s, which is not sufficient in order to get real-time measurements.
- No time-stamps are attached to samples, making it hard to monitor rate of change over time
- State Estimation is not performed with sufficient frequency, if at all.
- The ability to observe dynamics is not supported by the system.

In order to address these shortcomings, the Wide Area Measurement System (WAMS) system[1], described next, was invented.

3.3 Wide Area Measurement System

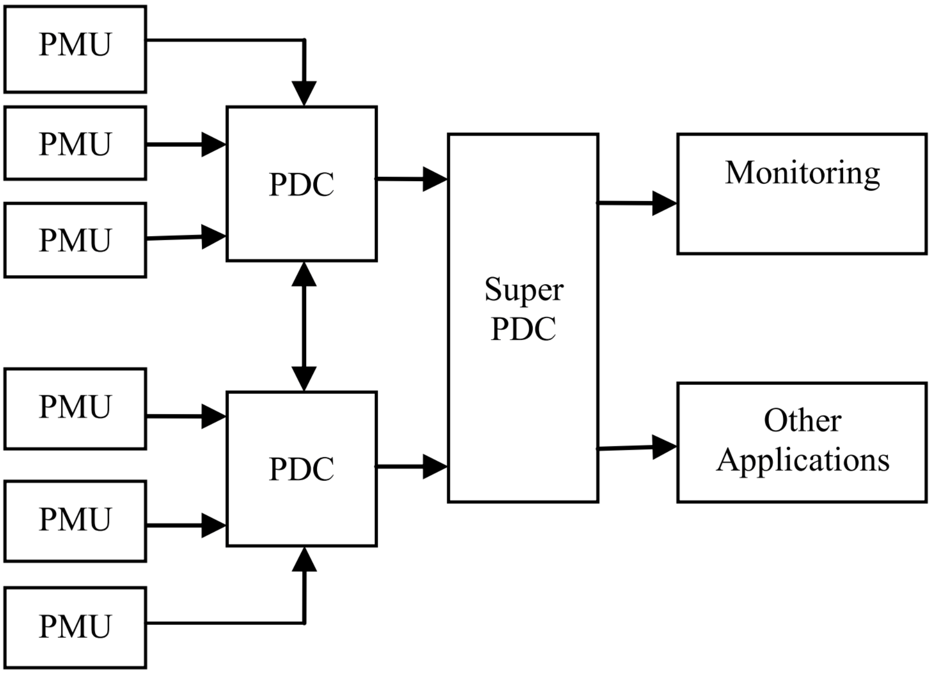


Figure 3.2: WAMS architecture, as presented in [12]

In order to ensure the continuous monitoring of the modern Smart Grid energy distribution system, the Wide Area Measurement System (WAMS) is utilised. An overview of the WAMS architecture, as presented in [12], is shown as Figure 3.2:
The WAMS is, as described in [12], a system, consisting of:
(1) PMUs, (2) PDCs, (3) The super PDC, and (4) Communication networks.
The various components might be described as follows, from (4) to (1):

- The **Communication Networks**, providing data transport between WAMS components, as required.

[1] WAMS is also known as the Wide Area **Monitoring** System

- The **Super PDC** controls several PDCs constituting a distributed WAMS.
- The **Phasor Data Concentrator (PDC)** is responsible for collecting and interpreting PMU measurements, before synchronising the measurements according to timestamps, in order to get more complete status information based on a combination of measurements.
- The **Phasor Measurement Unit (PMU)** is an intelligent measuring device, responsible for registering sensor measurements, performing calculations like, for instance, phase angles, as well as voltage and current magnitudes. The data registered and processed by the PMU, is transferred to the nearest PDC.

3.4 Smart grid Monitoring

The Smart Grid system constitutes a complex system of subsystems, which proper operation is a prerequisite for the successful transmission of electric energy from producers to consumers. In order for the WAMS to receive status monitoring data, a controlled process for retrieving and transmitting sensor data, is a prerequisite for proper system operation.

3.4.1 Description of the Smart Grid Monitoring system

Electricity is produced according to the current demand for energy, as controlled by the Demand Management system, dynamically adjusting the energy supply accordingly. In order to successfully reply to the dynamically changing demands for energy, a close monitoring of the production, transmission and distribution of energy is required. In order for the monitoring system to obtain status information, the proper transmission of monitoring data from power status sensors to the WAMS is essential. For the transmission of monitoring data to flow as flawlessly as possible, proper time synchronisation of the system components is mandatory. In order for the WAMS to receive the monitoring data required, the correct operations of the PDC and the PMUs, described next, is essential.

Phasor Measurement Units

The Phasor Measurement Unit (PMU) is a system which receives samples from a number of sensors monitoring real-time power line status, related to the electrical Voltage and Impedance the of the infrastructure being monitored. The entities monitored are known as electrical phases, most often part of a three-phase system, where each phase is separated by 120^0. Each PMU is continuously calculating the phasor values of all sensors, aligning all values corresponding to a time stamp as synchrophasors, before transmitting a synchrophasor record for each timestamp to the single Phasor Data Concentrator (PDC) to which the PMU has a TCP or UDP network connection.

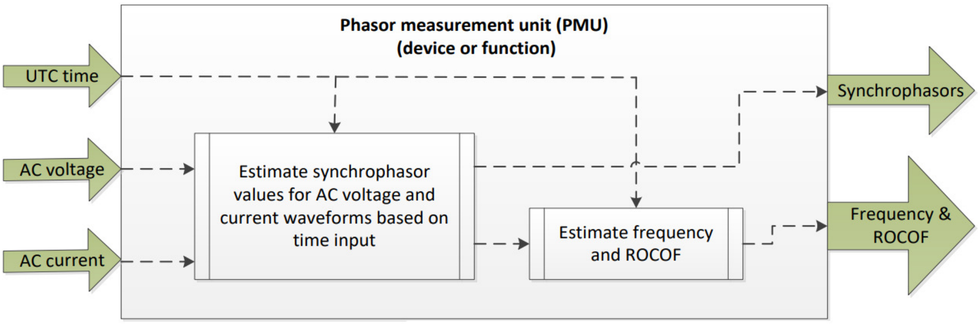

Phasor measurement unit (PMU)
(device or function)
UTC time
AC voltage
AC current
Estimate synchrophasor values for AC voltage and current waveforms based on time input
Estimate frequency and ROCOF
Synchrophasors
Frequency & ROCOF

Figure 3.3: PMU inputs and outputs, as presented in [13, p.12]

Phasor Data Concentrator

The Phasor Data Concentrator (PDC) is a networked system responsible for forwarding synchronised phasor data from as number of PMUs , to a more centralised PDC, most often denoted a Super PDC. The PDC processes each time stamp, awaits for synchrophasors for that time stamp to arrive from any PMU from which the PDC is reachable. A syncrophasor for a time stamp is required to be transferred to the destined PDC within a specified time frame, for it to be included in the data transmitted from the PDCto the Super PDC. Any remaining syncrophasor originating from a PMU is lost , resulting in a small piece of status information to be missing.

3.5 Advantages

The WAMS system adds great value to the monitoring of system status for the Smart Grid. Prior to the introduction of the synchronised phasors, the main component of the system for status monitoring, was the SCADA system, capable of updating status information at a significantly lower frequency of updates, measured in seconds rather than the current rate of a few milliseconds. Analogous to the transition of computers from being few and huge, to the current situation of them being numerous and tiny, the distribution of PMUs has increased the granularity of monitoring devices substantially. The increase in granularity of devices in the monitoring system has obvious advantages, considering the details available for status monitoring. The transition from the old system, however has some security issues, described next.

3.6 Security Issues

The Smart Grid (SG) Wide Area Measurement System (WAMS) is a SG subsystem enabling SG system operators to monitor the state of SG energy flow, and general system state. A vital requirement for the view of the current state of the SG energy distribution to be correct is, as described in previous sections, the ability of the WAMS Super PDC to utilise synchrophasors collected from the PDCs to produce a view of the system state. In order for the view to be correct, however, the correctness of the timestamps is critical. Therefore, in order to produce correct time stamps, the reliability of the Time Synchronisation source is of Critical importance. At the same time, risks of being the victim of Cyber Attacks is a consequence of the transition from the old, offline[2], to the new, online system, At the end of the day, this leads us to a vulnerability of the WAMS, as a potential victim of a Cyber Attack, caused by a successful Attack on any vulnerable time sycronisation protocol used in order to transmit the synchrophasors required for the status information to be correct and reliable. I describe the concept of Precision Time Protocol Time Delay Attacks in Section 5.3.

3.7 State Estimation

In order to detect abnormalities, or errors, in the monitoring data received, the WAMS includes applications capable of validating the quality of the state information received. Various State Estimation (SE) implementations exist, giving alerts on dubious system state based on comparisons with known good system states. State estimation systems increases the risk of attack detection, thus lowers the probability of a threat actor being capable of pulling off a stealthy attack. The assumed detection rate of the SE system, as explained early in subsection 6.8.3, is the basis for a stealthiness measurement in the form of the **tolerance levels** covered later in subsection 6.8.3.

[2] A system being offline is not available from public networks.

Chapter 4

Smart Grid Power Flow Status Monitoring

The SG consists of a vast number of both conventional and modern, more dynamic, production facilities, which requires thorough monitoring in order to ensure the optimal distribution of electrical energy. The requirement of a consistently stable and reliable supply of energy is constant, while the amount of energy demanded is dynamically changing according to the demand for power at any time.

Therefore, the proper Smart Grid operation might be considered virtually impossible without a close monitoring of current power flow, as well as the ability to instantly adjust the supply of power according to present needs, without the risk of causing power surges or blackouts. For this purpose, the Wide Area Monitoring System analyses the levels of electrical power as monitored by sensors, continuously sampled and forwarded to the WAMS, through a networked infrastructure continuously time-synchronised within a fraction of a second tolerance, for the less demanding subsystems. The correctness of this time source is critical to the reliability, and therefore, the proper operation of the monitoring system, constituting the primary decision criteria for actions controlling the supply of power.

4.1 Time Synchronisation

In order to be able to synchronise events in time, it is mandatory to adjust the clock of each participating actor, analogous to the classic pre-operational physical watch-synchronisation meetings in the physical domain. The SG time synchronisation requirements are, to say the least, a bit more demanding than a simultaneous(-ish) press on buttons to start timing from a common time reference. Several articles, of which [14] may serve as an example, stresses the importance of utilising a precise and reliable times source.

4.1.1 System Operations Benefits of proper Time Synchronisation

In [15], Dagle states the following aspects as the benefits for Smart Grid operation, of ensuring correct time synchronisation:

- **Situational Awareness and Wide-Area Monitoring** The improved quality of Syncrophasor data makes life easier for system operators, getting a more detailed overview of system state. The real-time state of the monitoring data presented, enabled the operators to react proactively to any status issues, before the underlying system state is allowed to a potential system blackout.
- **Real-Time Operations** PG system operators are using Phasor Measurement Unit data in order to pinpoint potential locations possibly hosting faulty equipment, enabling the early remediation of a potential issue capable of disturbing proper grid operatuion.
- **Power System Planning** The more detailed situational awareness obtainable from the usage of Synchrophasor data, gives the grid system operators a tool which enables them to ensure the optimal power asset utilisation, while at the same time being able to improve State Estimation systems, explained in Section 3.7, as well as testing for compliance standards.
- **Forensic Event Analysis** In the case of black-outs and other disturbance events, the availability of fine-grained Synchrophasor data, time-stamped to μ-second accuracy, be a good tool for any post-event investigations aiming to conclude on the events leading to the event to be investigated.

4.1.2 Possible effects of Time Synchronisation Data Impairment

In [16], Martin and Chen lists a number of side-effects which could result form the absence of high-quality data material from the WAMS.

- **Data loss** due to delayed, or otherwise erroneous, transmission of Syncrophasor data from the PDCs and PMUs covered in the previous chapter, will pprevent the WAMS from obtaining a correct snapshot og the current System State at any time. The missing data will give the operators system state information that is incomplete, and possibly erroneous, on which to base their actions in order to cope with possible system state issues.
- **Data corruption** causes the WAMS, and ultimately the grid operators, to be unable to interpret the affected data in any meaningful way, possibly loosing valuable system information. Data corruption could occur at any stage of the transmission from the sensors, caused by sensor malfunction, via the PDCs and, indeed, even by some issues with the proper phasor calculation at the Phasor Measurement Unit (PMU).
- **Inaccurate representation** of engineering quantities like specialised PG networking equipment like transducers, or devices used to record or display the data. The inaccuracy could be caused by wrong scaling or timing, as well as interference and noise.
- **Lack of precision**, will render the available data less useless for monitoring

purposes, when compared with a situation of receiving data of sufficient precision. The lack of precision negatively affects data accuracy, which may ultimately result in a situation where the operators may have an inaccurate situation stare awareness. The possible situation of added noise which could be a result of increasing the precision is not relevant for Syncrophasor data not containing a significant level of noise.

- **Incorrect identification** of measurements could be caused by the wrong labeling of any sensors to be used in order to monitor any equipment located in the PG. Incorrect data identification could also be an issue caused by a Syncrophasor data having erroneous identifiers of any related equipment.
- **Excessive or inconsistent latency** may cause the various system components, to fail to provide the data required in order to ensure displaying the proper system state to some part, or application, residing in the Wide Area Measurement System.

4.1.3 WAMS Time Synchronisation

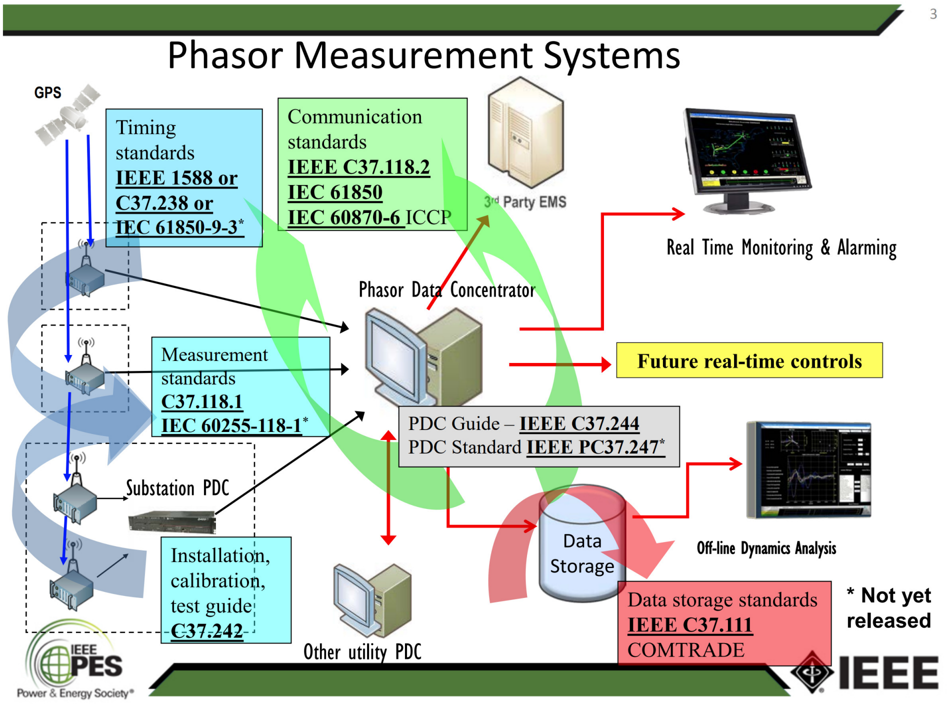
The Wide Area Measurement System is critically dependant on precise Time Synchronisation, as a Time Synchronisation error of a few μ-seconds may result in SG monitoring instability. The time stamps produced by Synchrophasors, pinpointing the exact time of any system event, is vital in order to ensure precise and reliable system state information. In the event of a system alert being triggered by erroneous system state Information, corrective actions by operators might have undesired effects. In order to synchronise the samples received from the PMU, the PDC, as well as the PMU devices producing the samples, is vitally dependant on precise timing adjustments, in order to establish a precise and correct overview of system state. Incorrect synchronisation of measurements caused by erroneous timing information, will produce an equally wrong system state overview, as presented in the SG WAMS.

4.2 Protocols

A large number of protocols are defined, in order to standardise the operation of the Smart Grid. Figure 4.1 provides an overview of standards relevant for the specified areas relevant for the Phasor Measurement System. Of these, I will focus mainly on a couple of protocols, seen in the upper left part of the figure:

- For the protocols in the timing standards, my main focus will be on the Precision Time Protocol (PTP) standard, IEEE 1588.
- for the protocols in the communications standards, my main focus will be on the Synchrophasor standard IEEE c37.118.2[1]

[1] For the IEEE C37.118 revision of 2011, the standard IEEE c37.118 was separated in two parts. IEEE c37.118.1 standardises communications, whereas IEEE c37.118.2 standardises measurements.



3

Phasor Measurement Systems

Timing standards
IEEE 1588 or
C37.238 or
IEC 61850-9-3*

Communication standards
IEEE C37.118.2
IEC 61850
IEC 60870-6 ICCP

Measurement standards
C37.118.1
IEC 60255-118-1*

PDC Guide – **IEEE C37.244**
PDC Standard **IEEE PC37.247***

Future real-time controls

Installation, calibration, test guide
C37.242

Data storage standards
IEEE C37.111
COMTRADE

* Not yet released

Figure 4.1: Phasor Measurement Systems, as presented in [17] Slide 3

In my thesis, concerning Time Delay Attacks, I am going to focus on the IEEE 1588 protocol, used in order to provide time synchronisation of devices residing in a Precision Time Protocol-enabled network, supported by PMUs not[2] relying on Global Navigation Satellite System (GNSS) systems, like the Global Positioning System (GPS) for time synchronisation.

4.3 Time Synchronisation Protocols

Time Synchronisation protocols are used in order to synchronise the time of interconnected devices in need of synchronised time for various purposes. In the case of synchrophasor devices, the devices needs to be time synchronised in order for SG WAMS operators to get a correct overview of the system state.

4.3.1 Time Synchronisation Protocols Precision Requirements

Time synchronisation protocols are controlling the synchronisation of time between various devices of the grid, like the PMUs, collecting Phasor Measurements from a defined number of measuring devices. Synchronised time is crucial in order to

[2] PTP are now common in recent years as an alternative to GPS for PMU time synchronisation.

ensure each PMU is able to put the correct time stamp on each Phasor Measurement, before transmitting the resulting Synchrophasor for each time stamp, to the destined PDC device.

In the event one of the Synchrophasors have an erroneous time stamp, an error affecting the integrity of the Synchrophasor data is introduced. As described in [6], Precision Time Protocol Synchronisation network , as well as Global Navigation Satellite System based synchronisation networks, are both capable of producing the precision required by the Synchrophasor protocols, as opposed to the more common Network Time Protocol (NTP) commonly used in ordinary computer networks. As my thesis covers PTP time synchronisation only, my description of time synchronisation protocols is limited to the Precision Time Protocol (PTP).

Precision Time Protocol services

The Precision Time Protocol (PTP) is a network-based time protocol, enabling the time difference between devices to be synchronised within a fraction (in the order of a few μs) of a second, satisfying the requirements of the SG WAMS for the precise time synchronisation ensuring the reliable and robust transmission of synchrophasors from the PMU to the WAMS.

Description of PTP time synchronisation

A device, being synchronised by the PTP protocol, reads its system time from a clock which is continuously synchronised by a network of one or more slave clocks, being periodically synchronised via various types of hybrid[3] clocks, ultimately synchronised with a Grand Master Clock.

The time of the slave clock, is being adjusted according to the following process, as visualised in figure 4.2, and described in [18, p. 51]:

> " The basic sequence in synchronizing a slave clock to a master clock is:
>
> - The master clock sends a Sync message to all directly connected slave clocks. The master clock generates a timestamp t_1 based on the master's local clock, indicating the Sync message sending time at the master clock.
> - A slave clock receives the Sync message and generates a timestamp t_2 based on the slave's local clock, indicating the Sync message receipt time at the slave.
> - The master clock communicates the Sync message sending timestamp t_1 to the slaves as a data field in a Follow Up message.

[3] Hybrid clocks are a master clock for some clocks, while being a slave clock for others.

- The slave clock sends a Delay Req message to the master clock. The slave clock generates a timestamp t_3 based on the slave's local clock, indicating the Delay Req sending time at the slave clock.
- The master clock receives the Delay Req message and generates a timestamp t_4 based on the master's local clock, indicating the Delay Req receipt time at the master clock.
- The master clock communicates the Delay Req receipt timestamp t_4 to the slave as a data field in a Delay Resp message.
- The slave uses the four timestamps t_1, t_2, t_3, and t_4 to compute the offset between the slave and master clocks. "[18, p. 51]

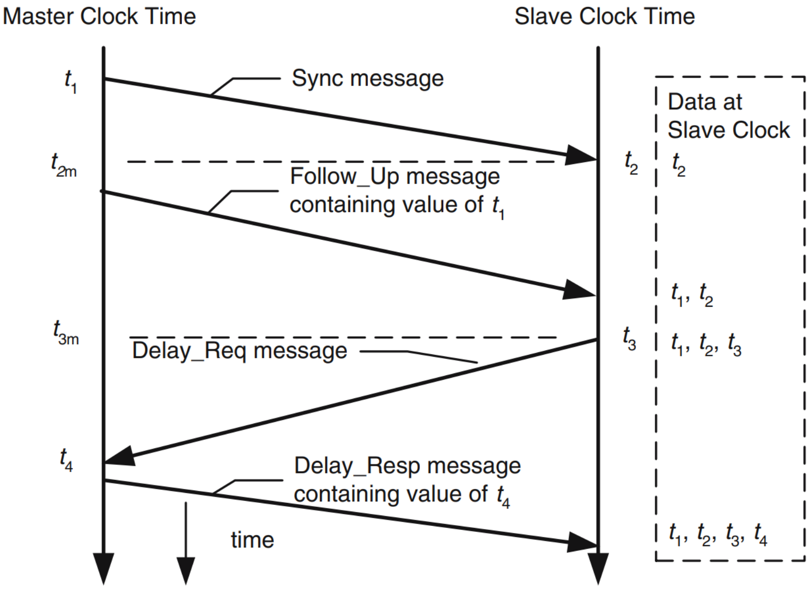


Figure 4.2: As presented in [18, p. 51]: Timing diagram for synchronization messages.

Following the message exchange visualised by Figure 4.2, the Slave clock uses the time offset $offset$ from the Master clock time, calculated by Equation 4.4, in order to synchronise with the Master clock. One fundamental

$$t_1 = t_0 + offset + d_1 \tag{4.1}$$

$$t_3 = t_2 - offset + d_2 \tag{4.2}$$

$$d_1 = d_2 = d \tag{4.3}$$

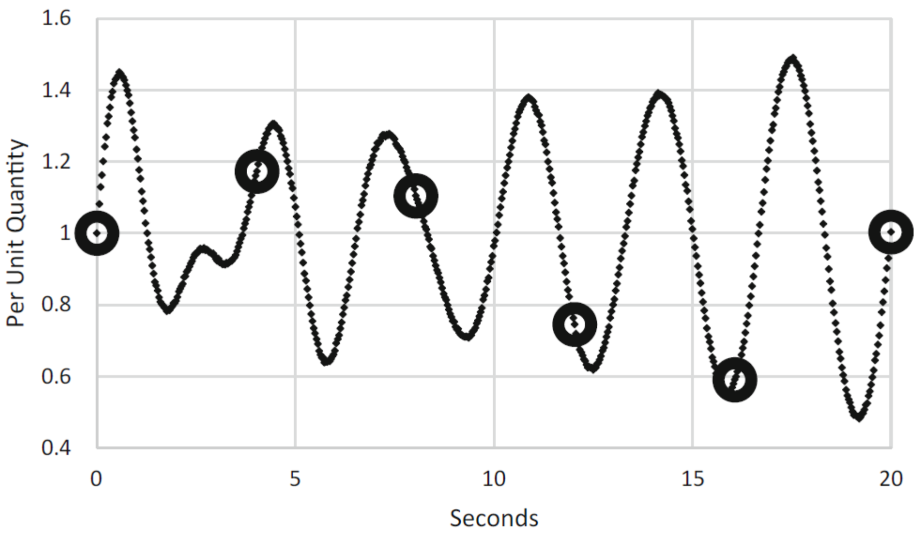


Figure 4.3: As presented in [15, p. 3]: Notional representation of the difference between synchrophasor and SCADA measurement. Figure credit: Dagle.

$$offset = \frac{(t_2 - t_1) + (t_4 - t_3)}{2} \tag{4.4}$$

In order to be able to achieve the time difference required, the PTP, as described by Eidson, in [18], is dependant on:

- Timestamped network events, messages, which is used for synchronisation.
- A method of timestamp transmission as required for synchronisation.
- Overcoming any timing impairments introduced by system components.

As is discussed by several papers, including [5], a vulnerability of PTP, and similar protocols like the "NTP protocol, is the assumption given in equation 4.3 of d_1 being equal to d_2, assuming symmetrical packet transmission delay delay between the Synchronisation target and the corresponding Synchronisation source.

4.3.2 Synchrophasors

A number of protocols has been developed and maintained, in order to standardise the format of the synchronised phasors to be transmitted, as well as the actual method of transmission used in order to transfer the standardised data. The PMU is receiving values from sensors, on which it is able to calculate voltage level and phase angle of the energy flow. It is utilising a time-source to pinpoint measurements in time, producing synchrophasors, to be transmitted to the nearest PDC. As described in [15], the data received from traditional SCADA systems are timestamped after arriving at the control station. The synchrophasors of the WAMS on

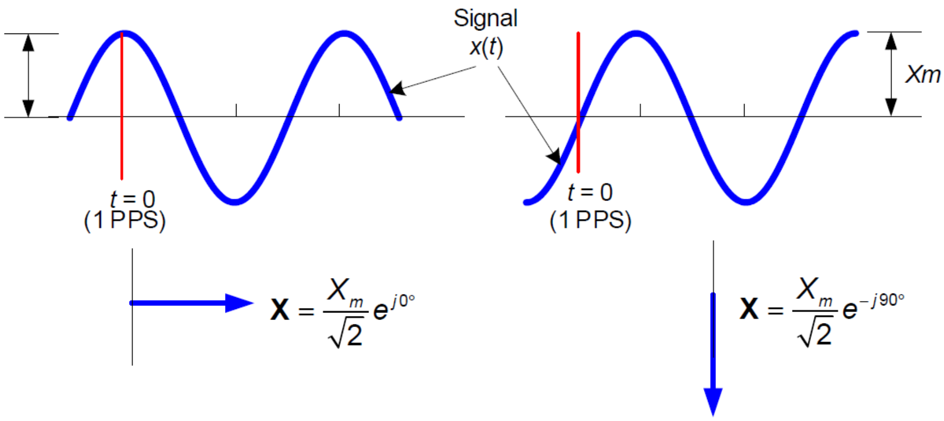

Signal
$x(t)$
Xm
$t = 0$
(1 PPS)
$t = 0$
(1 PPS)
$\mathbf{X} = \frac{X_m}{\sqrt{2}} e^{j0°}$
$\mathbf{X} = \frac{X_m}{\sqrt{2}} e^{-j90°}$

Figure 4.4: As presented in [20]: Convention for synchrophasor representation.

.

the other hand are, as described in [19], being time-stamped by the PMU in real-time before being transferred to the control system. The sampling rate of the PMU, results in synchrophasor data enabling operators of the WAMS to get real-time visualisation of critical elements, like the state of energy flow of the Smart Grid. The increased granularity of the measurement system allows for the detection of anomalies undetectable by traditional SCADA systems, as illustrated by Figure 4.3. The increased sampling rate, of the synchrophasors of the WAMS systems enables a more fine-grained view of energy distribution system state changes. However, in order for the WAMS system to get the correct system state information, correct time stamps is critical. Therefore, the time-synchronisation mechanisms of the PMU system is of critical importance.

The Synchrophasor

As explained in [20], the Synchrophasor is defind as:

$$X = \frac{X_m}{\sqrt{2}} e^{j\phi} \tag{4.5}$$

The signal $x(t)$ is a periodic signal given by the function:

$$x(t) = x_m cos(\omega t + \phi) \tag{4.6}$$

The equations and formulae of the Synchrophasor has been modified over the years,as new editions of the standard have been published.

4.3.3 Synchrophasor Protocols

As described in [21] and [22], the communication and data exchange from the PMU to the PDC was standardised by the introduction of the IEEE 1344 standard in 1995, which was established as the standard communication protocol for synchrophasor data exchange. According to [14], the IEEE 1344 was revised in 2001 , before the introduction of the IEEE C37.118 in 2005. The IEEE C37.118 protocol was derived from the IEEE 1344 standard, and has undergone a number of revisions, over the years. In [21], Martin, Brunello, Adamiak, Antonova, Begovic, Benmouyal, Bui, Falk, Gharpure, Goldstein *et al.* describes the history of the IEEE C37.118-series of standards. The characteristics of the various generations, might be summarised as:

- The IEEE C37.118-2005, introduced the transmission hierarchy of PMU to various levels of PDCs, and super PDCs.
- The IEEE C37.118-2011, introduced the separation of the standard into two parts:
    - The IEEE C37.118-2011-1, which covers masurements and performance requirements.
    - The IEEE C37.118-2011-2, which covers communications, and realtime transfer of data to via PDCs, to the WAMS.
    - The IEEE Std. C37.118.1a-2014 is, according to [20] an ammendment to the 2011 verisons of the standard.

The IEEE C37.118 series of protocols has, although not designed with security in mind, been updated with security extensions in order to ensure a trustworthy connection less vulnerable to attack on integrity and availability.

Chapter 5

Smart Grid Cyber attacks

The Smart Grid (SG) is a complex system delivering electrical power to a society more dependant on electricity then ever, given the transition from traditional sources of energy to electrical energy on areas like agriculture, industrial production, heating, and more recently, transportation. The transition of the electrical grid from the classic Power Grid to the Smart Grid exposed, as previously described, the Critical Infrastructure of the power grid to attacks from remote locations via the Internet.

5.1 Attack via time protocols

Computer systems reachable[1] from the outside world, are potential targets of Cyber attacks. The eventual recoveries of the initial Cyber Attacks was followed up by defence actions, resulting in more advanced attack techniques, has evolved to a continuous battle of control between attackers and defenders.

Threat Actor Types

There are numerous Threat Actors of various skill levels, from so-called "Script Kiddies" to professionals, aiming to get unauthorised access to systems, for fun, fame, or for more serious reasons, like terrorism or financial gain.

- The **Internal attacker** has privileged access to, at least parts of, the internal infrastructure of the target, enabling the ability to take malicious actions not available to non-internal attackers.
- The **External attacker** is limited to attacking the targeted infrastructure from the outside, typically through network connections.
- The **Traffic Injector attacker** adds network packages to the benign traffic of the networks of the target, in order to produce the desired effects on the state and operation of the targeted infrastructure.

[1] Systems could ultimately be targeted utilising USB sticks, if not accessible from the Internet.

- The **MitM attacker** interrupts the communication between the two parties A and B, impersonating as B to A and vice-versa.
- The **MotS attacker** are able to eavesdrop on communications, without any privileged access to enable the direct modification of any data transmitted.

The various types of attackers possesses various malicious action capabilities, which they may use in order to attack their intended target in numerous ways.

5.1.1 Examples of Cyber attacks

As described in [23], a number of security incidents targets the SG specifically, like the 2015 BlackEnergy3 attack on the Ukranian Power Grid, the StuxNet worm of 2010, as well as the watering-hole remote access trojan attack of 2014. Any online SG infrastructure containing vulnerabilities, is equally inflicted by attacks not specifically targeting Smart Grid (SG) like the WannaCry ransomware cryptoworm of 2017, targeting the EternalBlue vulnerability of unpatched windows computers.

5.2 Cyber Attacks targeting Smart Grid

The two-way communication lines of theSmart Grid systems opens the possibilities of communication between the networks of energy distributors and the networks of consumers, serving purposes as automatic measurement of energy consumption, as well as dynamic adaption of energy production according to variations in demand for energy over the hours of the day. The transition from networks managed by closed communication channels to networks communicating over IP-based networks, exposesSmart Grid networks to Cyber attack vulnerabilities. Malicious threat actors having privileged access to the infrastructure, is able to perform various kinds of internal attacks.

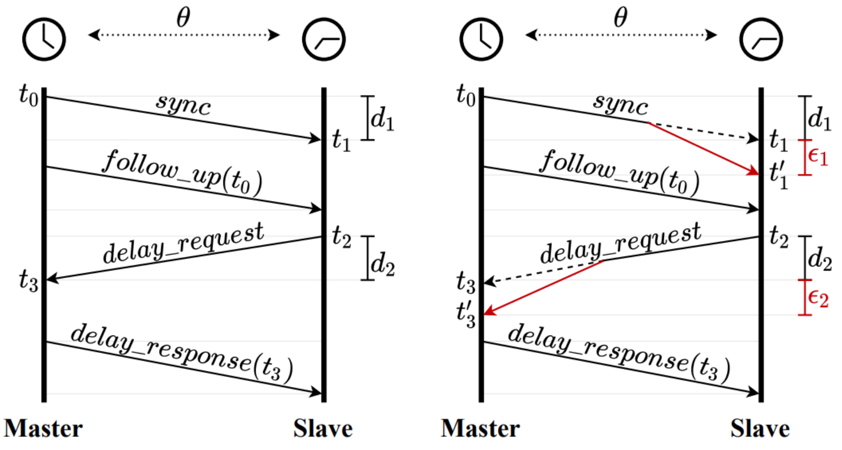
Traditionally, anyone aiming to attack the Power Grid infrastructure, was obliged to get physical access to the premises, from which the infrastructure in question was controlled. Following the transition to the online SG, the network connecting the grid to the outside might be utilised in order to execute any Cyber attack requiring internal privileged access from the outside.

5.2.1 External Attacks

External attacks is characterised by malicious actors attacking the infrastructure from the outside, without having the privileged access required in order to target internal system vulnerabilities.

5.2.2 Internal Attacks

The distinction between external and internal attacks, is the level of access required in order to perform the attack in question.



a) Normal PTP

b) PTP with delay attack

Fig. 2: PTP message flow with timestamping to minimize the clock offset θ (a). When the attackers are able to delay either the *snyc* or *delay_request* message (b), they can introduce asymmetric path delays that will break the synchronization.

Figure 5.1: As presented in [24], figure 2. Comparison of PTP delay attack synchronisation with normal PTP synchronisation.

Man on The Side (MoTS) Attack

The Man on The Side (MotS) attack is a type of attack requiring minimal privileges and system access in order to be successfully executed.

5.3 PTP delay Attacks

Several attacks which targets the Precision Time Protocol utilises vulnerabilities in the PTP, as explained by [24]:
Based on the equations related to the regular PTP synchronisation, in [24] stated as:

$$t_1 = t_0 + \theta + d_1 \tag{5.1}$$

$$t_3 = t_2 - \theta + d_2 \tag{5.2}$$

$$d_1 = d_2 = d \tag{5.3}$$

$$\theta = \frac{(t_1 - t_0) - (t_3 - t_2)}{2} \tag{5.4}$$

$$d = \frac{(t_1 - t_0) + (t_3 - t_2)}{2} \tag{5.5}$$

The PTP delay attack uses the following equations:

$$t_1' = t_0 + \theta + d_1 + \epsilon_1 \tag{5.6}$$

$$t_3' = t_2 - \theta + d_2 + \epsilon_2 \tag{5.7}$$

Using the equation 5.5, we arrive at the following equations:

$$\theta' = \frac{(t_1 - t_0) - (t_3 - t_2)}{2} - \frac{\epsilon_1 - \epsilon_2}{2} \tag{5.8}$$

$$d' = \frac{(t_1 - t_0) - (t_3 - t_2)}{2} - \frac{\epsilon_1 + \epsilon_2}{2} \tag{5.9}$$

and accordingly:

$$\theta' = \theta - \frac{\epsilon_1 - \epsilon_2}{2} \tag{5.10}$$

and

$$d' = d - \frac{\epsilon_1 + \epsilon_2}{2} \tag{5.11}$$

For the attack, Finkenzeller, Wakim, Hamad and Steinhorst further describes, the attacker has the option to set the desired (erroneous) clock offset value at will, as well as being able to control the offset direction. choosing vvalues of ϵ_1 and ϵ_1 as $\epsilon_1 < \epsilon_2$ for setting the slave behind, whereas the reverse is true for the case of $\epsilon_1 > \epsilon_2$.

Thus the PTP delay is a realistic attack. Some of the various flavors of the attack should be obtainable for an attacker having limited access to the Target of the attack, like a Man on The Side (MotS) attacker.

Chapter 6

Method

6.1 Introduction

As a background for the thesis, assume a threat actor is in a preliminary phase of an attack. The decision to initiate a phase of attack simulation is made, with the aim of gathering useful information in order to learn more about possible risks of being detected, as well as to gain some empirical background for the evaluation of possible consequences of a successful attack. The potential outcome of the simulation may be used in order to prepare for attacking the actual infrastructure with attacks with a low attack detection probability and, to the best possible knowledge, with foreseeable consequences of the attack. As described previously, the aim of the thesis is to investigate any observable effects of specific time delay attack simulations. Such simulations could be executed in a preparation phase, preparing for the execution of an actual time delay attack. Some papers, like for instance [5] and [25], describes a number of varieties of the PTP delay attack, while other papers, like for instance [26], describes Cyber Attacks, like the Time Delay Attack, to have severe consequences to the SG infrastructure. The primary goal of the actual attack is to stay undetected, while exposing the infrastructure under attack to an attack having the most severe consequences possible, while still avoiding detection.

6.2 Research Design

In order to be able to observe the effects of exposing a PMU to a time delay attack, the real attack is dependant on getting access to expensive equipment, like a PMU as well as the interconnected infrastructure. As previously discussed, a time delay attack on Synchrophasors imposes a high risk of causing damage to the infrastructure targeted. Given the high potential for damage, a good option for visualising any potential effects a time delay might have on the values produced by a PMU under attack, would be to simulate the attacks. There exists a number of projects which utilises MATLAB and SIMULINK in order to model power grid components

in general and, specifically, PMUs.
My selected approach, however is to produce a SIMULINK model, using standard components from the Simscape Electrical addon to MATLAB/SIMULINK. The simulation produces pair-wise (original, delayed) PMU output values for each of the channels Magnitude, Angle and Frequency, making them available for comparison and further analysis.
As the final part of the thesis, a theoretical discussion, aiming to provide answers to the research questions, will be conducted.

6.3 Research Methods

As the thesis includes both a theoretical, as well as a more practical phase, the methods are dependant on the phase in question.

6.3.1 Theoretical phase

As part of the introductory studies of the topic selected, a couple of searches on the NTNU literature search facilities returned a number of books, like [1] and [27], covering introductory chapters on Power Grid and Smart Grid. The introductory chapters heavily relies on descriptions from relevant book chapters.

6.3.2 Practical phase

In order to provide theoretical evidence on which to answer the research questions, a literature study will be conducted. For any experimental results, experiments will be described, implemented and executed.

6.4 Measurements

The simulations to be defined and executed provides examples of Phasor Measurement Unit output, where two identical PMUs are given a signal from a simulated power source as input. One of the PMUs are fed the original power source signal, whereas the other PMU is fed a delayed version of the original power source signal. The resulting PMU output measurements may be compared for similarity.
Where possible, experimental investigations reported by articles selected will be provided as relevant examples, in order to support any discussion arguments for the purpose of reaching conclusions.

6.5 Sample

The samples for my literature study will be papers relevant for the discussions, in order to provide answers to the research questions.

Any execution of experiments will provide experimental samples, with the aim of supporting discussions and conclusions. The samples originating from the experiments, consists of:

- Three channels of PMU output, denoted **Magnitude**, **Frequency** and **Angle**
- Two arrays of numerical values for each channel of PMU output: One for the original signal, the other for the delayed signal.

6.6 Validity and Reliability

In order to increase the validity and reliability, a number of articles will be included as the foundation for any conclusions. My personal selection of papers deemed relevant for my discussion, will be selected highlighting on articles being included as relevant articles by survey papers, as well as papers gaining a high relevance score on literature search sites.[1] Another selection criteria aiming to increase validity and reliability will be a focus on selecting articles receiving a high number of quotations ratings on sites like Google Scholar.

For the experimental parts, my project is utilising a selection of PDC and PMU simulator packages. In order to validate the phasor data generated, the included validation capabilities of the simulator packages are utilised.

6.6.1 Validation of the model

A experiment of running the simulation with a delay leve of 0, could serve two purposes:

- Validation of the delay function
- Validation of the two copies of the PMU as being identical.

As a hypothesis, running the simulation with a delay of zero should produce identical channel-wise output.

A $d = 0$ test result producing identical output for the who PMUs , would increase the confidence of the model both being valid and reliable.

Another criterion for a valid model would be for the data to show alterations which could be explained by a change of delay level.

6.7 Infrastructure used during experiments

In order to provide practical results on which to base the discussions and conclusions, the following tools will be utilised;

- MATLAB, R2023a, with SIMULINK added, is used for running the simulation.

[1] ... like the NTNU ORIA site (`https://innsida.ntnu.no/litteratur`).

- Simscape Electric, and its dependency Simscape, are required in order to build, and run, the simulations.
- The Simulation is executed by running a MATLAB script.
- A Windows 10 laptop is being used for the simulations

6.8 Simulating a Time Delay attack

6.8.1 Scenarios

For the experimental part of my thesis, a number of attack scenarios will be required. The aim is to investigate various attack vectors which might be used by a sophisticated man-on-the-side threat actor in order to execute an attack while staying undetected.

6.8.2 Assumptions

A number of assumptions is stated, in order to narrow the scope of the thesis:

- **Attacker Policy:**
  A sophisticated threat actor would most likely want to avoid detection by anyone protecting the targeted infrastructure. Therefore, executing an attack which may be detected should be avoided at all costs. As a consequence, any decisions related to actually executing the attack should be as a result of promising results following a stealthiness assessment process. Simulations of possible effects could be part of the stealthiness assessment process.
- **Attack Prerequisites:**
  A stealthy attack with small impact is preferred over an attack having more severe impacts, at a higher risk of detection. The ideal attack would be an attack having maximal impact on the target, while the risk of detection being minimal.
- **Attack Design Policy:**
  A part of the challenge would be to design an attack producing a high impact on the target, while staying undetected.

6.8.3 Approach Selected for the Attack:

Consider targeting a system able to detect PMU output deviations exceeding a specified threshold. The detection system may classify a suspicious PMU output pattern as one of four categories, analogous to the classification categories described in [28, p. 5]:

- True Positive (TP): Output pattern correctly classified as an attack.
- True Negative (TN): Output pattern correctly classified as no attack.
- False Positive (FP): Output pattern incorrectly classified as an attack.
- False Negative (FN): Output pattern incorrectly classified as no attack.

A viable strategy could be to focus on a few optional tolerance levels. Even without knowing the detection threshold of the system targeted, the attacker could benefit from being able to predict any consequences of a future attack. Three levels of tolerance could cover three potential scenarios:

1. A tolerance level of 1% may impose a high attack detection risk before the attacker is able to do much harm.
2. A tolerance level of 12% may impose a lower detection risk, enabling the attacker to do more harm
3. A tolerance level of 50% will impose an even lower detection risk, enabling the attacker to do even more harm, than in the previous case (Item 2.).

It may also be a good approach to determine any effects of a small increase in delay level, versus executing the attack using a fixed delay level.

6.8.4 Attack scenarios

In order to provide experimental results in order to answer the Research Questions stated, a number of attack scenarios are defined. The main method of simulation would be a delayed forwarding of values, where a specified number of delayed samples, d, is applied to the PMU input. The value of d is used to replace any sample $s(i)$ with the sample value $s(i-d)$, simulating[2] clock drift, producing effects similar to a Time Delay Attack. The simulation could be performed using a number of delay functions. For the thesis, two types of approaches are used:

- The **Instant Delay Attack**, Increases the delay level to the targeted level at attack initiation. The attack maintains a constant delay level for the entire duration of the attack.
- The **Step-wise Delay attack**, increasing the delay level by one sample each second, until the targeted delay level is reached. The attack maintains a constant delay level for the remaining duration of the attack.

Attack characteristics

In order to investigate some specific effects of the attack, the following characteristics are selected:

1. In order for the model to stabilise[3], data used for visualisation does not include the first second of the simulation ($t < 1$).
2. In order to be able to conclude on the effect of delay cancellation, knowledge of the system state prior to the attack is required. Therefore, each simulation is executed with a delay level of 0 for the next second ($1 < t < 2$).
3. The Instant Delay Attack involves raising the delay level instantly to a level $d > 0, d \in \mathbb{N}$, at the time $t = 2$.

[2] A specific SIMULINK delay module is performing the simulated delay of samples.

[3] The PMU needs some samples of input before being able to stabilise the output values.

4. The Step-Wise Delay Attack involves raising the delay level in steps of one each second, from $t = 2$ until reaching the level d at $t = 1 + d$.
5. In order to be able investigate any effects of attack cancellations, the targeted PMU is exposed to a delay attack for a limited time, thus reducing the delay level d to 0 before reaching the last second of the pre-set simulation running time.

6.8.5 Attack Simulation Implementation

A number of physical investigations related to the effects of any attacks on the intended targets, would increase the knowledge of a potentially complex target, increasing the probability of staying undetected during the attack. As previously explained, those investigations will be done in a simulation environment.

6.9 Creating a Simulation environment

Simulations are designed, in order to investigate the attack scenarios previously described. The planned attack is implemented using a combination of Simulink and MATLAB. The simulation produces three pairs of PMU channel output, one pair for each of the **Magnitude**, **Angle** and **Frequency** channels. Each pair consists of the native[4] and delayed PMU output signals. The execution of each simulation will, after the completion of the execution of the SIMULINK model, produce corresponding graphical output, included in the thesis as figures. The graphical representations are used to illustrate any visible effects the attack may have on the system. The graphs enable visual pair-wise comparison of the output produced by the attack. In addition, the graphical result of a numerical check for tolerance compliance is presented for visual inspection. A PMU may include output channels for both Voltage and Impedance PMU input. The simulation covers both Voltage and Impedance pMU input.

6.9.1 Modelling a PMU

As the plan of the threat actor is to expose a number of PMUs to a time delay attack, the plan is to build a model of a PMU, allowing the model to be run for both Instant and Step-Wise attacks involving various time delay levels, in order to investigate any observable effects on the output from the PMU.

6.9.2 Model Description

The SIMULINK model implemented consists of two SIMULINK Subsystems:

- The **PowerSource** Subsystem, consists of a number of SimScape Electric components, producing simulated three-phase signals for both Voltage and Impedance.

[4] Native PMU output equals the PMU output with no input delay.

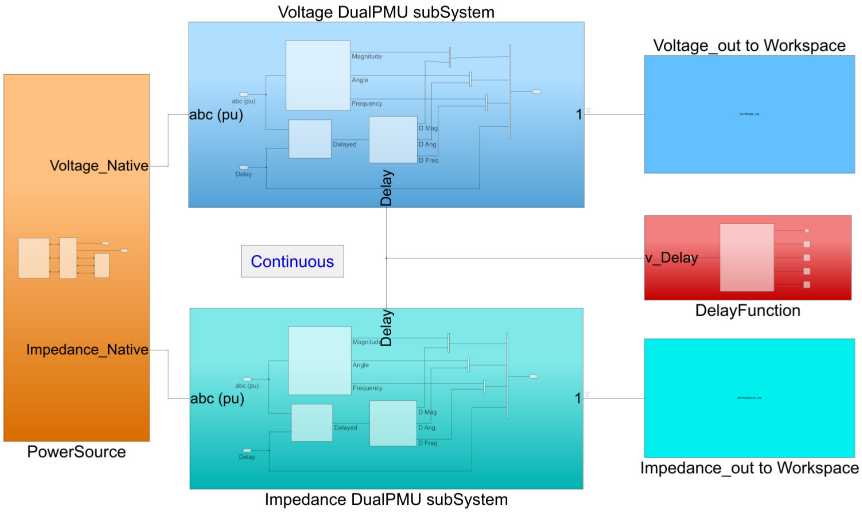


Figure 6.1: A SIMULINK model for the simulation of PMU Time Delay Attacks.

- **The DualPMU** Subsystem, accepts a simulated three-phase power input, and a delay level, and produces a six-channel signal for external processing.

The model, shown in figure 6.1, consists of one PowerSource Subsystem, connected to two DualPMU subsystems, one for each of the Voltage and Impedance PowerSource outputs.

The PowerSource subsystem

The main components of the sub system is available from the component libraries of the Simscape Electic addition to the SIMULINK/MATLAB software suite.

- **Three-Phase source**
- **Three-Phase V-I Measurement** Providing Voltage and Impedance levels.
- **Three-Phase Parallel RLC Load**. Documentation at [29].

In addition, two signals are provided as output from the subsystem to be used as PMU inputs:

1. **Voltage_ Native**: The non-delayed voltage signal.
2. **Impedance_Native**: The non-delayed Impedance signal.

The composition of the PowerSource Subsytem is visualised in figure 6.2. There may be alternatives for configuring the power source, in order for it to be more realistic for a Smart Grid environment. For the simulation designed and executed as part of the thesis, however, the aim has been to investigate any visible effects of exposing a standard PMU model to a time delay attack. Redesigning the DualPMU and PowerSource Sub systems are suggested as possible future work at the end of the thesis.

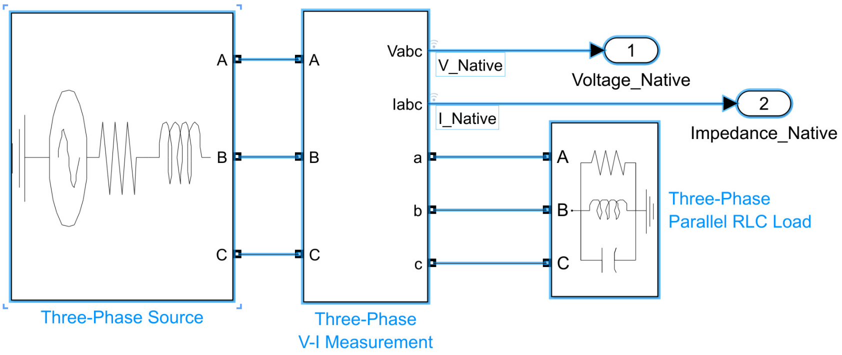


Figure 6.2: PowerSource: Generating V and I PMU Input to DualPMU.

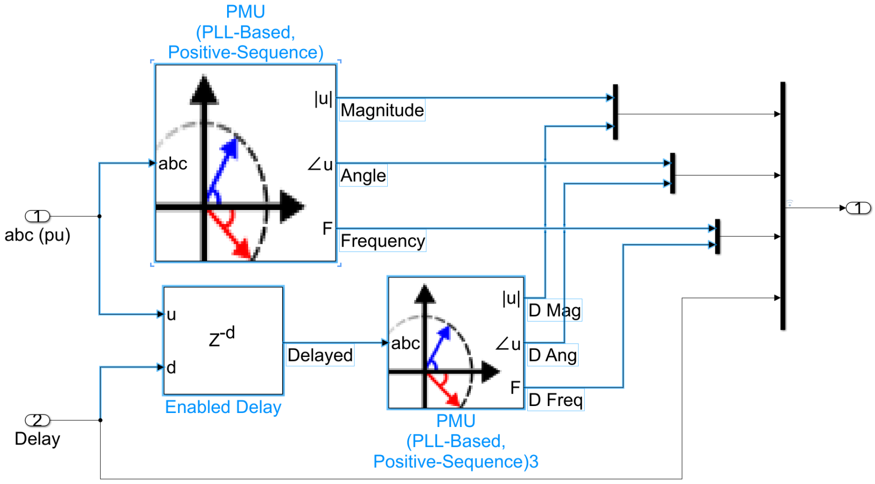


Figure 6.3: DualPMU: Generating PMU output from V or I from PowerSource.

The DualPMU subsystem

The composition of the DualPMU Subsytem is visualised in figure 6.3.

The DualPMU subsystem consists of the following components:

- A three-phase input, as provided by the Voltage or, alternatively, Impedance output of the PowerSource subsystem previously described.
- A numeric integer input, representing the delay level by which to use during the Delay level attack.
- A **Delay** SIMULINK block, which produces a delayed signal from the PowerSystem Output, delayed by the value **d**, received at DualPMU Delay input from the DualPMU delay input port.
- Two identical PMUs are part of the DualPMU system: One accepting the original PMU input signal, the other accepting the delayed pMU input signal.
- The PMU blocks in the model, are available from the library of the **Simscape Electric** add-on to the Simulink/MATLAB environment.
- Three 2to1 MUxes, collecting one PMU channel output pair each.
- One 4to1 MUX, collecting the combined PMU outputs from the three 2to1 muxes, one for each of the channels Magnitude, Frequency and Angle.
- The fourth MUX input is connected to the unmodified delay input, in order to store the corresponding delay function for each simulation session, enabling its inclusion in the figures.

In addition to the PowerSource and the DualPMU subsystems, there are also some additional components included in the SIMULINK Model:

- The Delay function, listed in Table 6.1, is implemented as a MATLAB function, which dependant on the value of a variable, calculates a step-wise delay level, alternatively sets a constant delay level, according to the rules for delay initiation and termination.
- Two SIMULINK blocs of type **to Workspace**:
  - **Voltage_out** storing the output from the Voltage DualPMU subsystem to a MATLAB workspace variable, for further processing.
  - **Impedance_out** storing the output from the Impedance DualPMU subsystem to a MATLAB workspace variable, for further processing.

6.9.3 Experimental Procedure

In order to execute the simulation, each step should be completed, as required.

1. Start Matlab
2. Open a MATLAB script, named **PMUsimScript.m**.
3. Inspect and modify a selection of variables.

Variable	Purpose
d_level	Delay Level: numeric
d_step	Step-Wise if true, Instant otherwise.

Table 6.2: Selected variables for tuning the simulation

The execution of the script will produce:

a. Output data logged to workspace for each of the DualPMU subsystems voltage(V) and Impedance(I), to be further processed by the script at the end of each execution of the SIMULINK model.
b. For each variation of PMU type (V/I), and channel (Magnitude/Angle/-Frequency), a numeric comparison is followed by a corresponding colored (Red) similarity classification.
c. One figure for each channel, PMU type, Delay function type, and Delay Level, is produced.
d. Each figure is showing, for the specific configuration, a combined plot of the original and delayed signals. A number of plots, one for each of the tolerance levels of 0.01 (1%), 0.12 (12%), and 0.5 (50%), is included in the same figure.
e. The tolerance plots, shows tolerance compliance information for a level, as well as a visualisation of the Delay function, and the normalised ([0,1]) difference between the native and delayed signals, for the signals in the plot above.
f. Failure to comply to the tolerance level is visualised as red portions on the time scale.

4. During script execution, each figure is displayed on screen for visual inspection, before being automatically saved at a specified location.

6.9.4 Definition of Experiments

The experiments will focus on various levels of assumed detection thresholds.

1. **Immediate delay** Square pulse signal: Starting off, turning constant-delay on, before dropping to 0 before simulation end.
2. **Step-wise delay** Increasing to delay level specified, in step-wise increase of delay level by one each second, before dropping to 0 before simulation end.

Additionally, the **No delay (, no[5]) Attack**, running the simulation on a constant delay level of 0 for the entire duration of the simulation, will be executed in order to produce output for model validation purposes.

[5] At least, if considering the attack with No Delay an attack, it will be pretty harmless.

```
function y = vDelay(timeStamp, d_Start, step, duration, d_Delay)
% Calculates a delay level, given input parameters
%
   % The delay level is calculated using a step-wise function
   % gradully approacing a level of one during the attack duration.
   % this function is multiplied by d_Delay/steps in order to reach the
   % specified delay level of d_Delay in an number of steps specified
   % by the variable "steps".
   %
% y: calculated delay level.
% timestamp: The timestam to calculate the delay for.
% d_start: The initiation time of the delay.
% step: Make setep-wise delay if true, otherwise the delay is instant.
% duration: The length of the active delay, in seconds.

    if ((d_Delay == 0 ) || ...
            ((timeStamp < d_Start) || (timeStamp >= (d_Start+duration))))
        % No delay 8d_Delaydelay = 0) in any of these cases:
        % * d_Delay== 0: The delay level is explicitly set to zero.
        % - (timeStamp < d_Start): Time before d_start.
        % - (timeStamp >= (d_Start+duration)): Time after specified time
        % frame of attack

        y=0; % Set the delay level equal to Zero.

    else % There should be a delay level greater than Zero.

        if (step == false) % The attack should not be Step-wise:
            % Use one step to reach the specified delay level.
            steps=1;

        else % Use n steps to reach a delay level of n
            steps=d_Delay;

        end
       % The delay level is calculated using a step-wise function
       % gradully approacing a level of one during the attack duration.
       % this function is multiplied by d_Delay/steps in order to reach the
       % specified delay level of d_Delay in the number of steps specified
       % by the variable "steps".
       %
       y=ceil(rem((timeStamp-d_Start),(d_Start+duration)) )*d_Delay/steps;

       % In case the formula results in a too high delay level
     if (y > d_Delay)
         % limit the delay level to the specified level
            y = d_Delay;
     end

   end
end
```

Table 6.1: Code Listing of the Delay Function

Chapter 7

Results

The following sections presents the results for each attack type, with subsections for the detection threshold levels selected, as defined in section 6.9.4 For each attack type defined, a number of attacks specifying various delay levels, specified as a number of samples, are covered. For each delay level, a number of figures are produced by running the simulation. A figure showing a combined view of all three components, displaying the delayed and original signals, as well as a signal indicating the actual difference between the two signals. Three more detailed figures follows, comparing the original and delayed signal to a similarity measure for each of the three PMU output components.

The delay functions defined, delays the input signal by the specified number of samples, in one or more steps.

Comments on the results are included for selected figures, whereas, interpretation of the results are deferred to Chapter 8

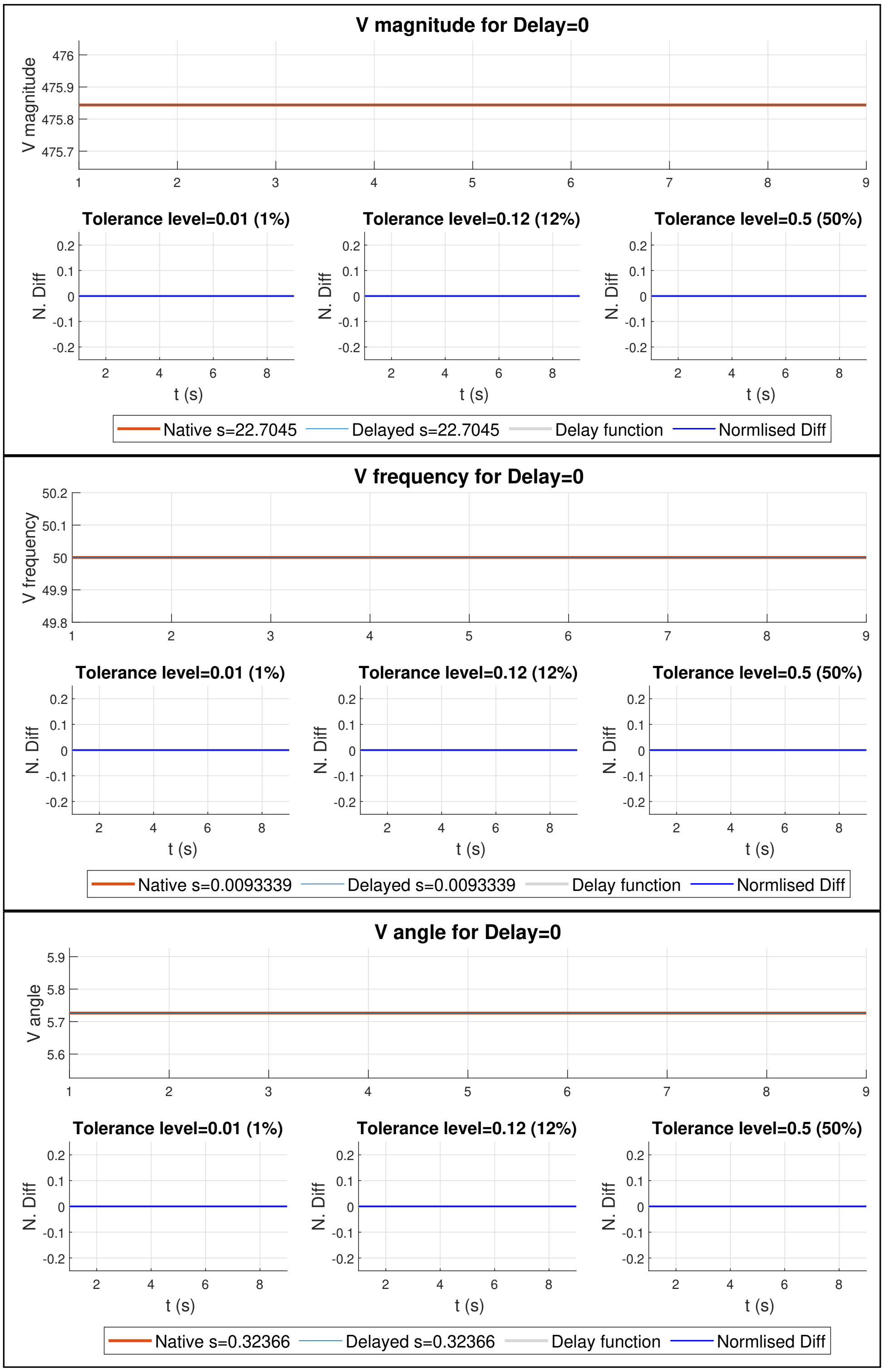


Figure 7.1: Results for Voltage Output for Delay equal to Zero

- The delayed signal overlaps the original signal, producing a straight line colored in a different color from any of the colors in the associated legends.
- The blue Normalised diff signal also overlaps the grey Zero delay function, with similar effects on the color of the line.

7.1 The Delay Level of Zero

For model verification purposes, the output for the delay level of zero is included. One could possibly dispute the relevance of including an attack producing a zero delay level, but the simulation is intended to serve two purposes, as previously explained in subsection 6.6.1:

1. The design of the **DualPMU** subsystem, as visualised in figure 6.3, appears to include two instances of Phasor Measurement Units of the same PMU implementation, the SimScape Electric PMU library module, as previously described in subsection 6.9.1.
2. The delay function, listed in 6.1, is presumably correct. Running a simulation with a constant delay level of Zero should produce the same result as for identical Phasor Measurement Unit (PMU)s, showing identical, and indistinguishable PMU output, as displayed in the resulting figures.

No matter how identical the PMU implementations of the **DualPMU** subsystem appears to be: If the delay function erroneously introduces a delay, the resulting output of the simulation is unlikely to produce a correct result,
The reverse argumentation also sounds reasonalbe:
No matter how perfect the delay function might be, if the simulation produces deviating results, erroneously indicating a, possibly random, delay, the PMU implementations of the **DualPMU** subsystem is unlikely to be correct.

Result for delay Zero:

On the next, as well as the previous page, the results of running the simulation with a delay level of Zero is presented. Comments are located underneath the name of each figure.

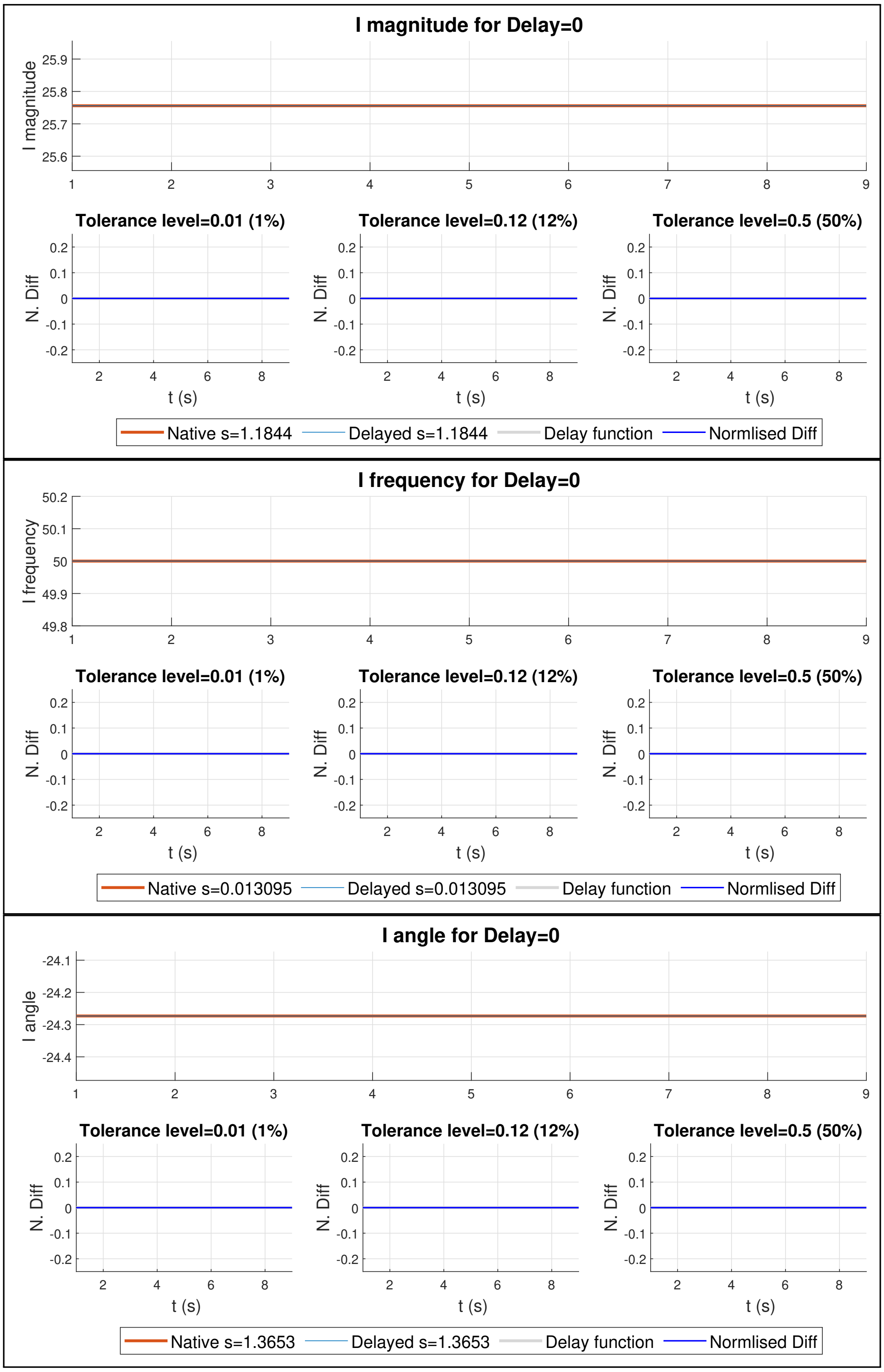


Figure 7.2: Results for Impedance Output for Delay equal to Zero

- The delayed signal overlaps the original signal, producing a straight line colored in a different color from any of the colors in the associated legends.
- The blue Normalised diff signal also overlaps the grey Zero delay function, with similar effects on the color of the line.

7.2 Instant Delay Simulations

Instant delay simulations are characterised by the delay level instantly raises to the specified level, staying at the same constant level for the entire duration of the simulation, before instantly dropping to zero at the specified attack termination time. The simulation focuses on:

- Observing the situation prior to the attack for the purpose of comparing system state at attack termination with the pre-attack system state.
- observing the effect of a prolonged attack of constant level:
-
- What is the effect of a instant rise of the delay level for various delay levels?
- What is the effect of a instant drop of the delay level for various delay levels?

On a suitable number of next pages, the figures showing the results of running the Instant Delay Simulations of levels One trough Six are available for inspection of the results.
Comments are located underneath the name of each figure.

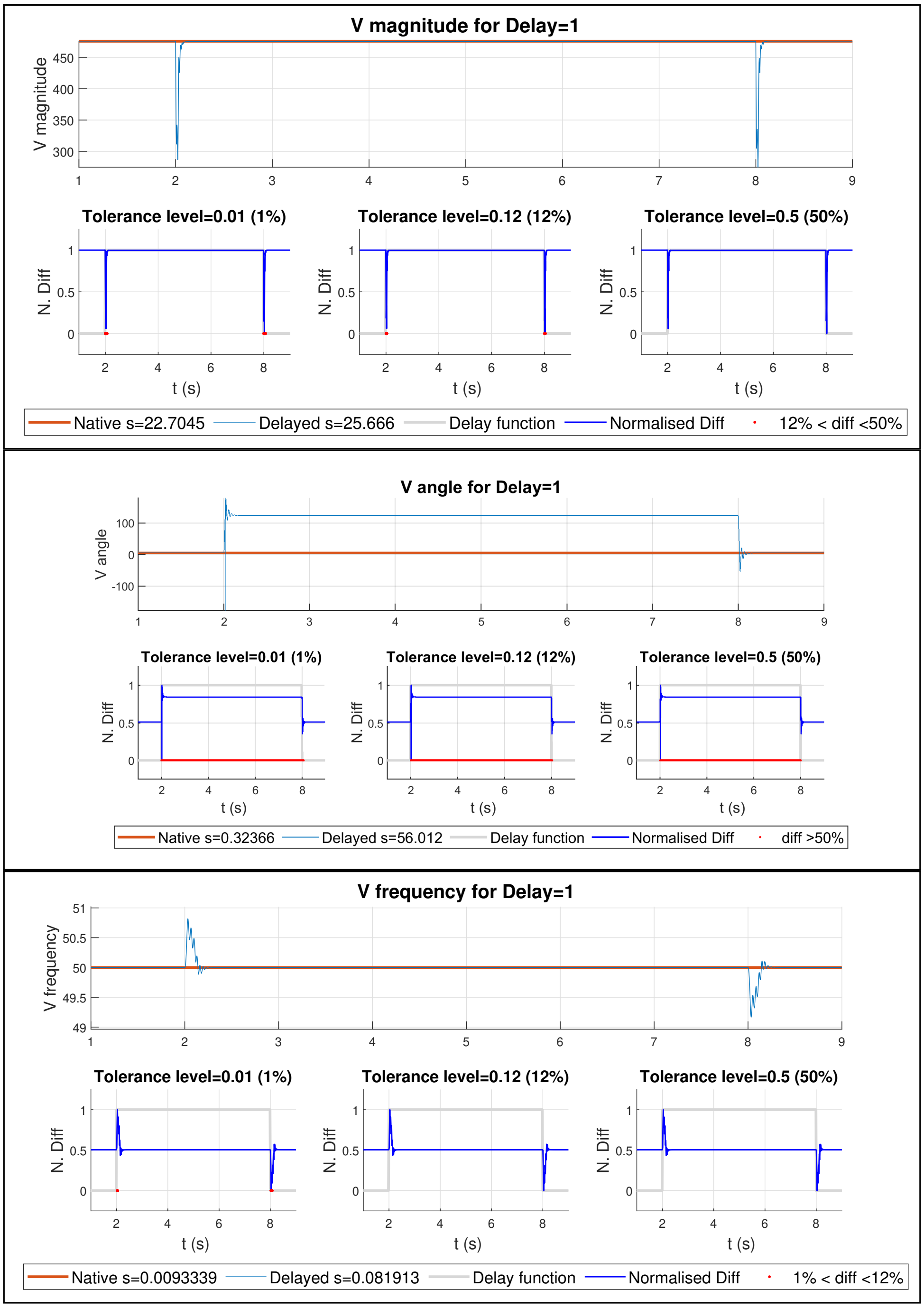


Figure 7.3: Results for Voltage Output for Instant Delay equal to One

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly 120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

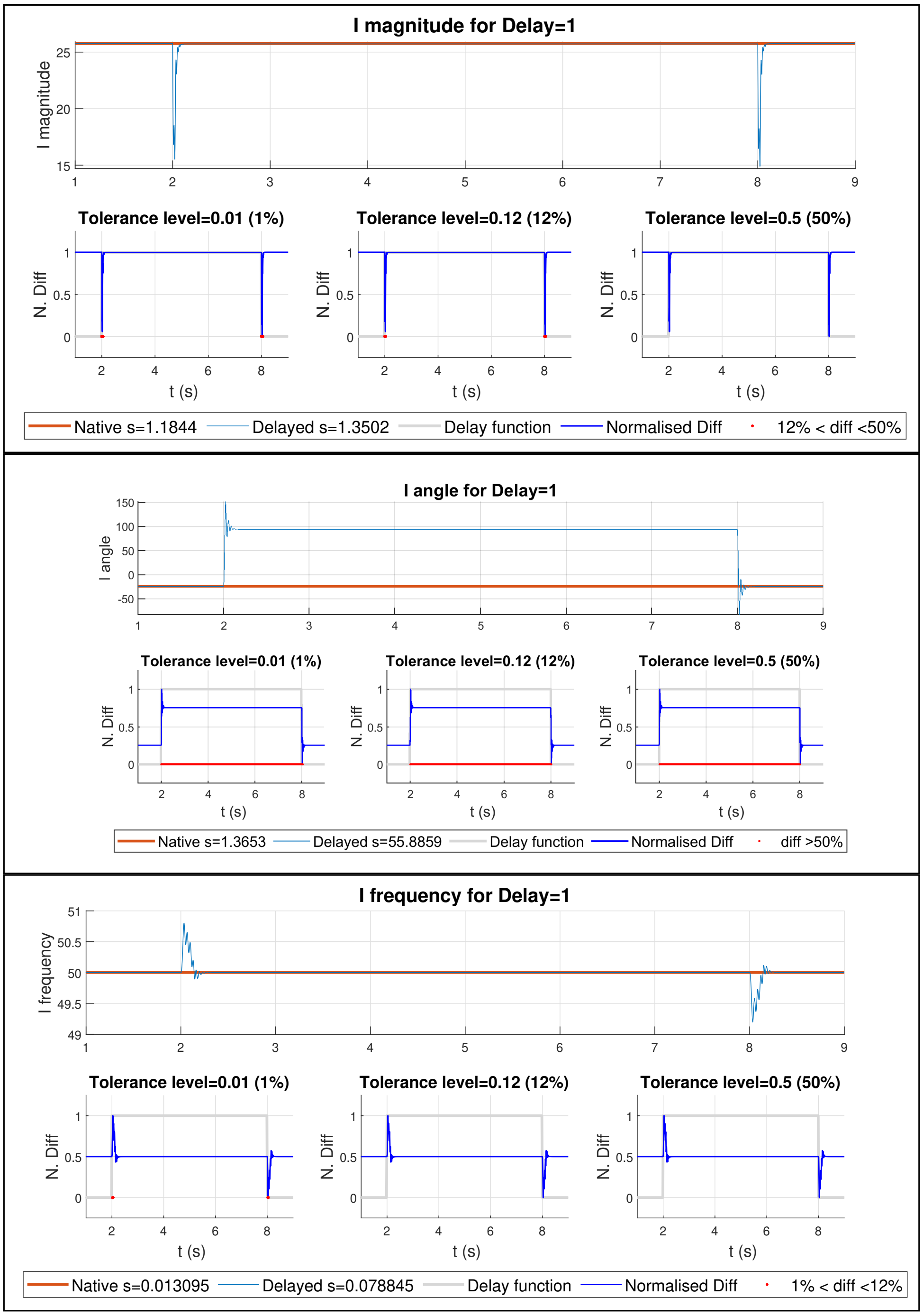


Figure 7.4: Results for Impedance Output for Instant Delay equal to One

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly 120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

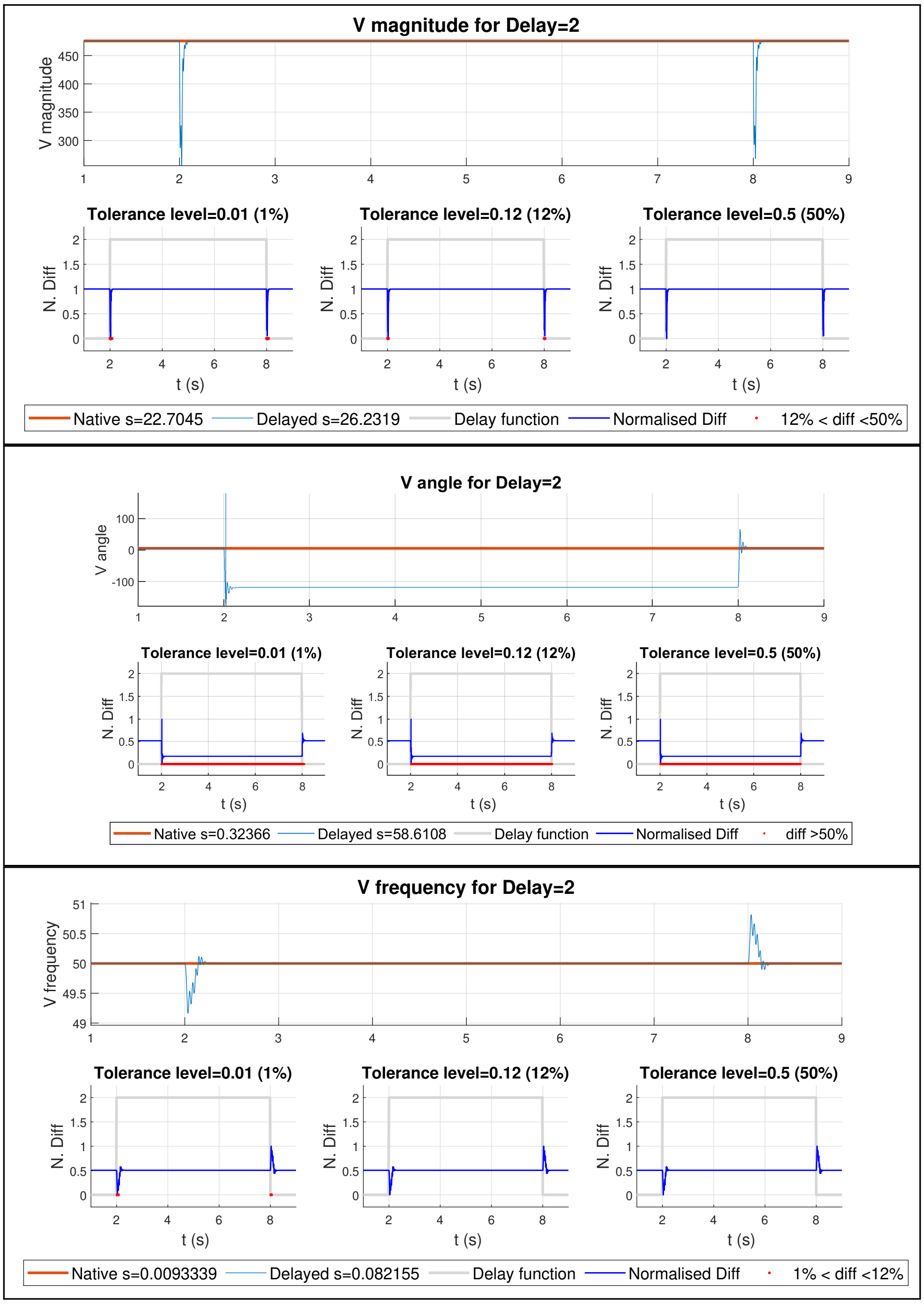


Figure 7.5: Results for Voltage Output for Instant Delay equal to Two

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

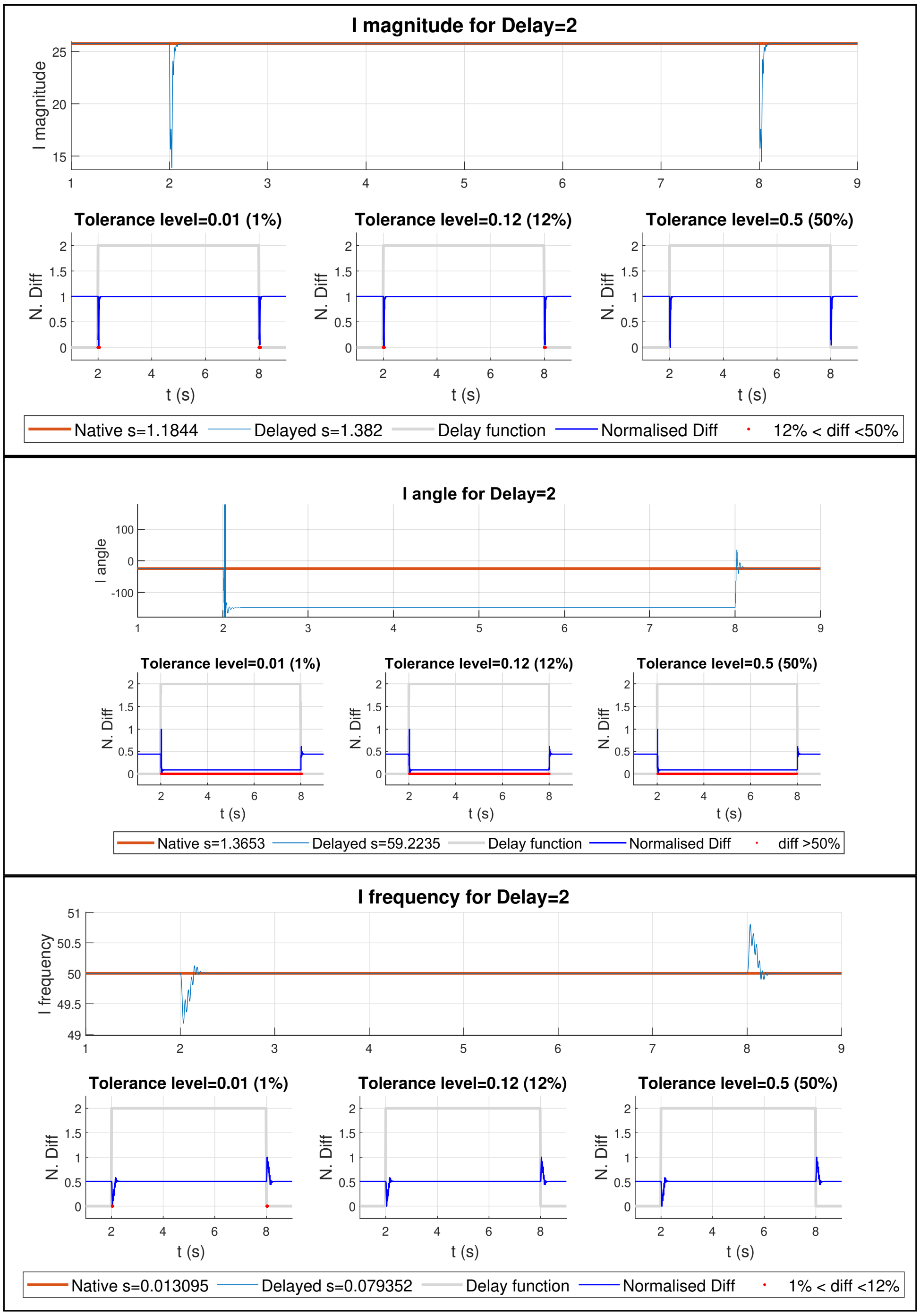


Figure 7.6: Results for Impedance Output for Instant Delay equal to Two

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

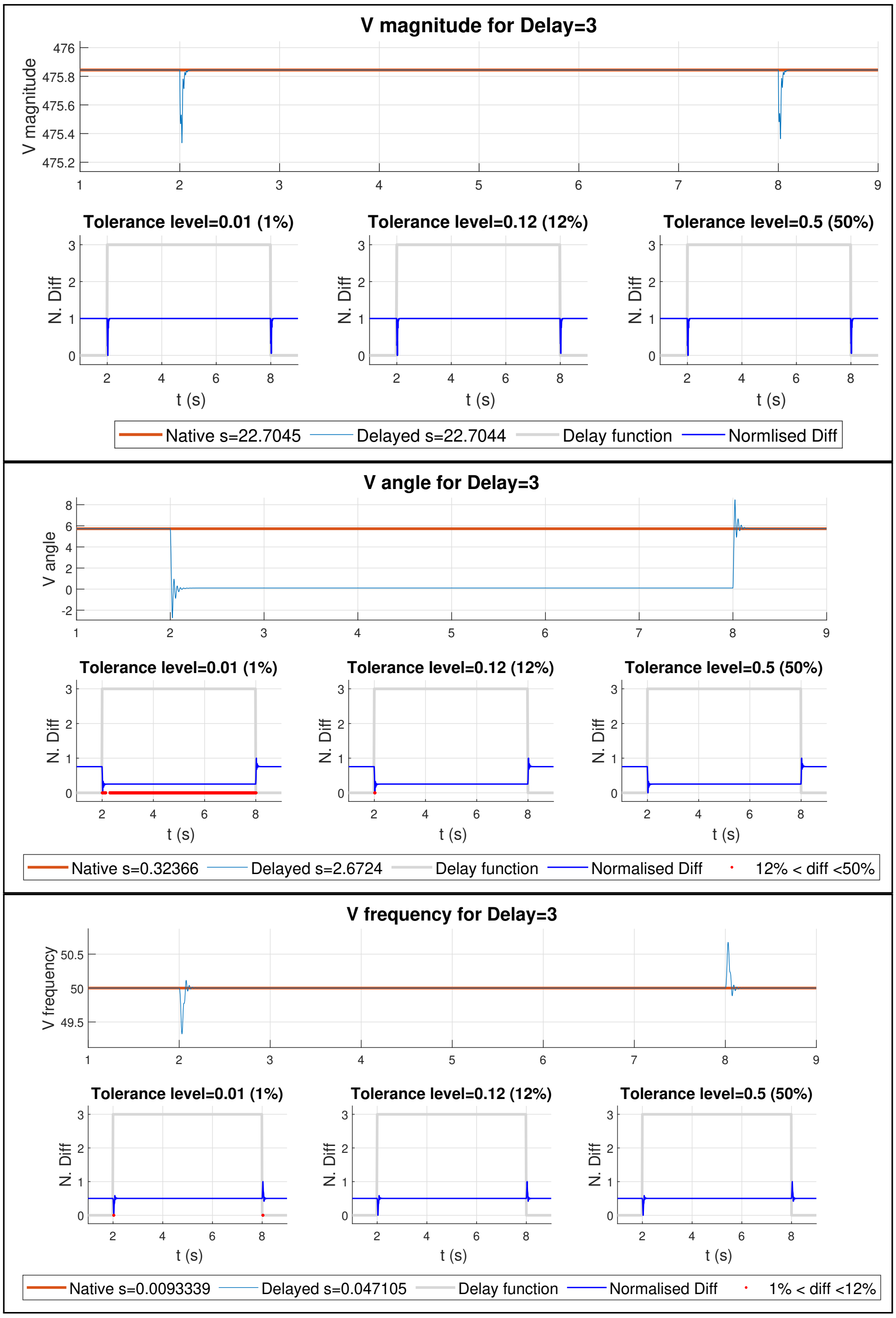


Figure 7.7: Results for Voltage Output for Instant Delay equal to Three

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -10^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

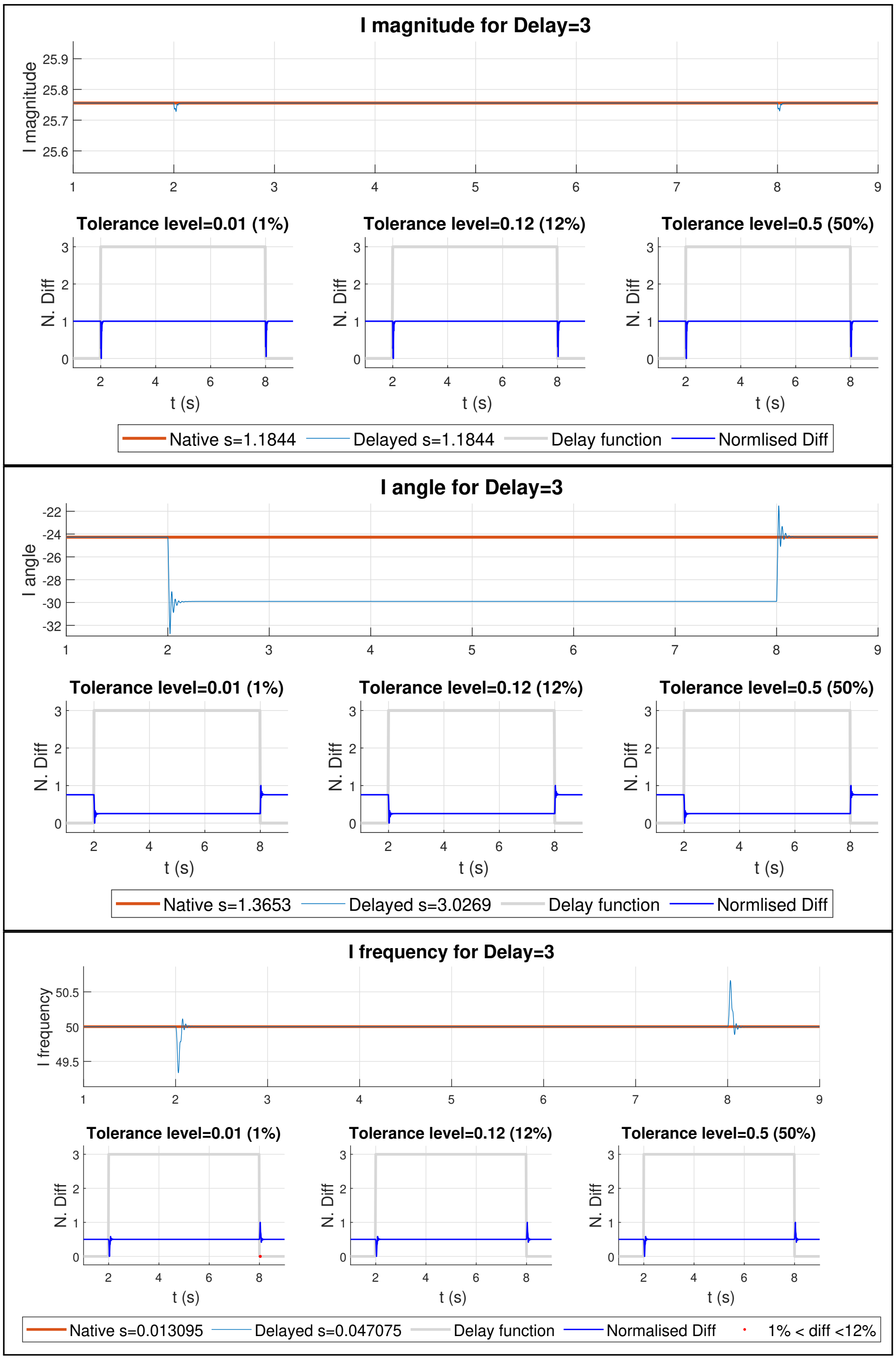


Figure 7.8: Results for Impedance Output for Instant Delay equal to Three

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -10^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

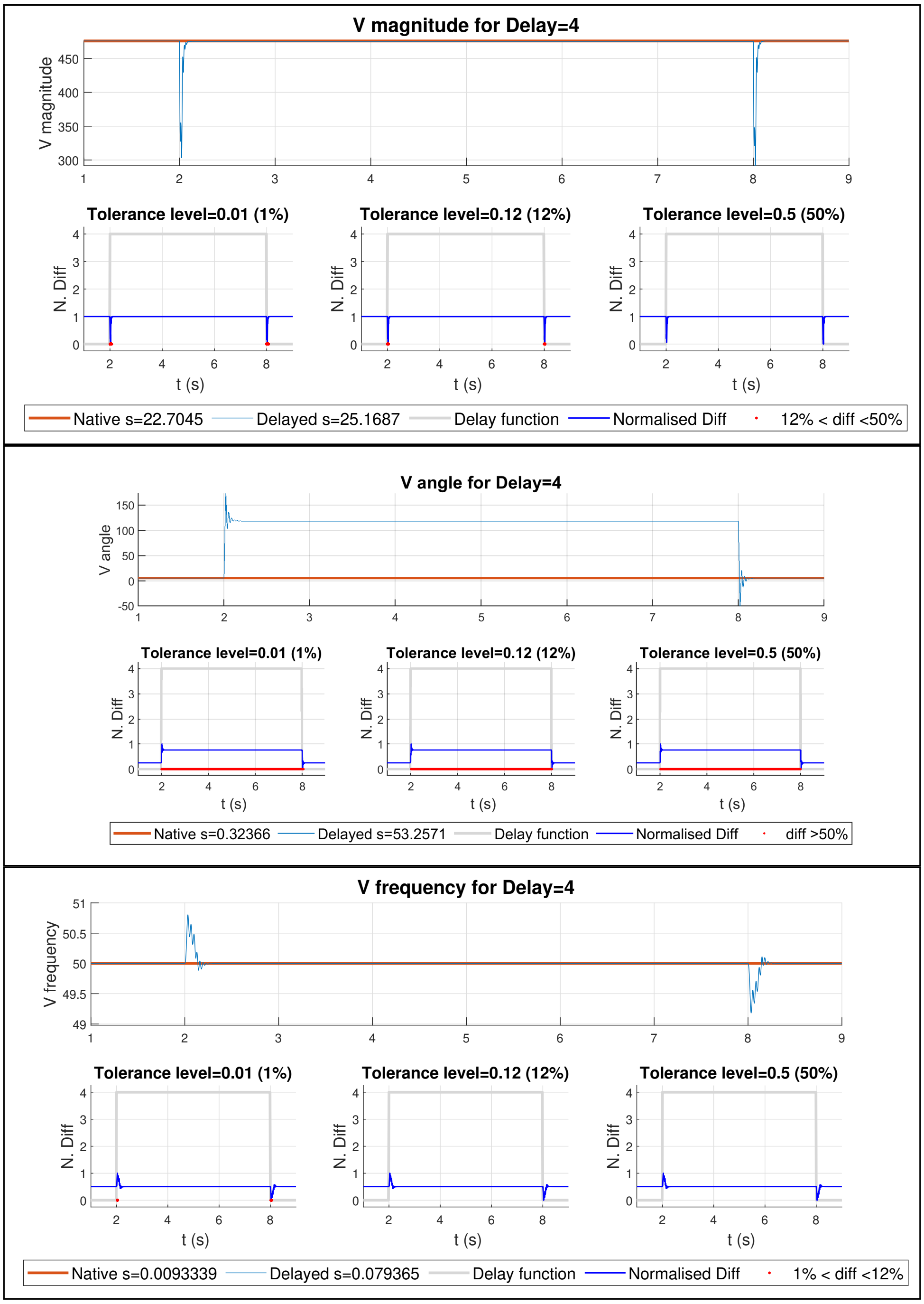


Figure 7.9: Results for Voltage Output for Instant Delay equal to Four

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

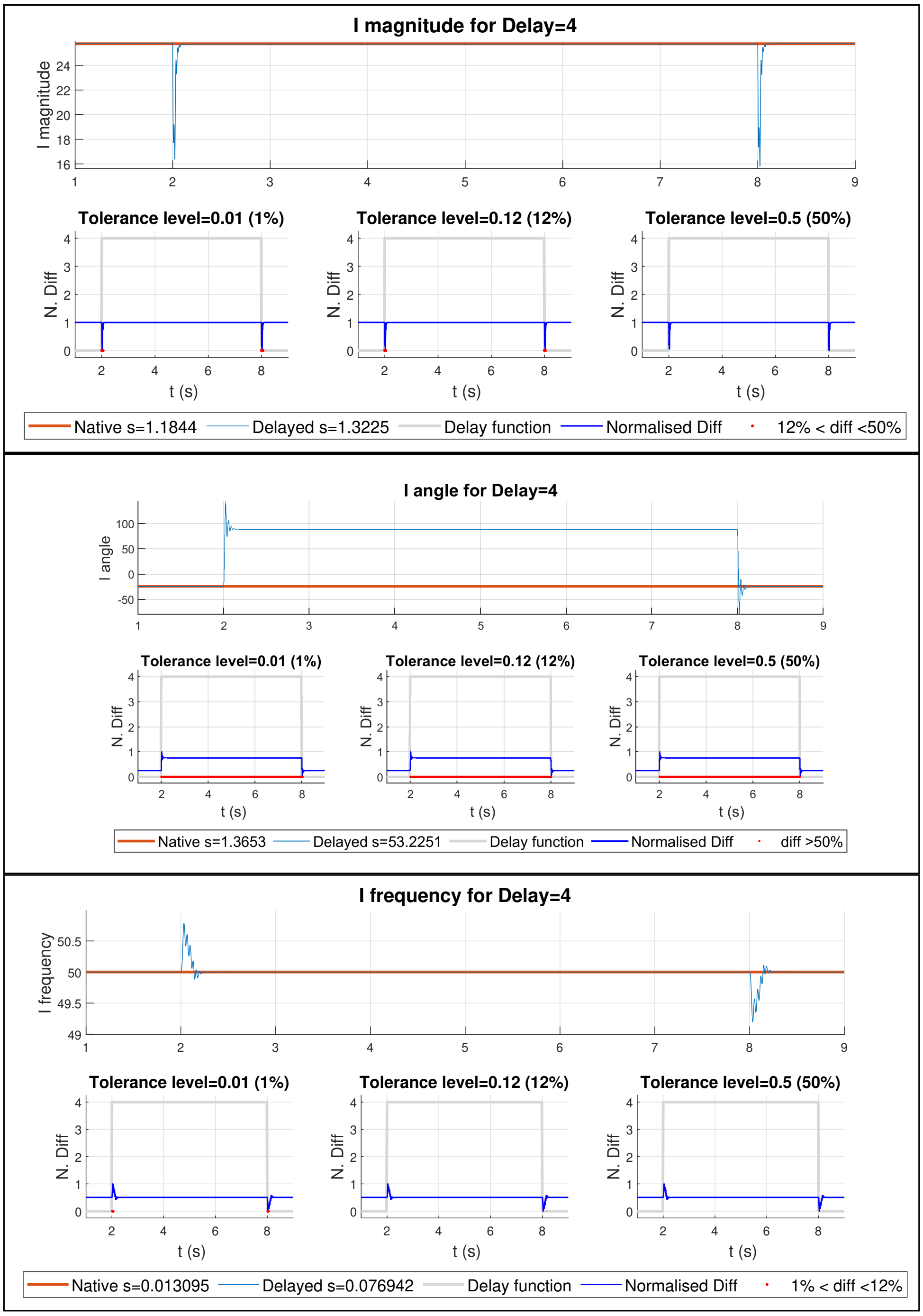


Figure 7.10: Results for Impedance Output for Instant Delay equal to Four

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly 120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

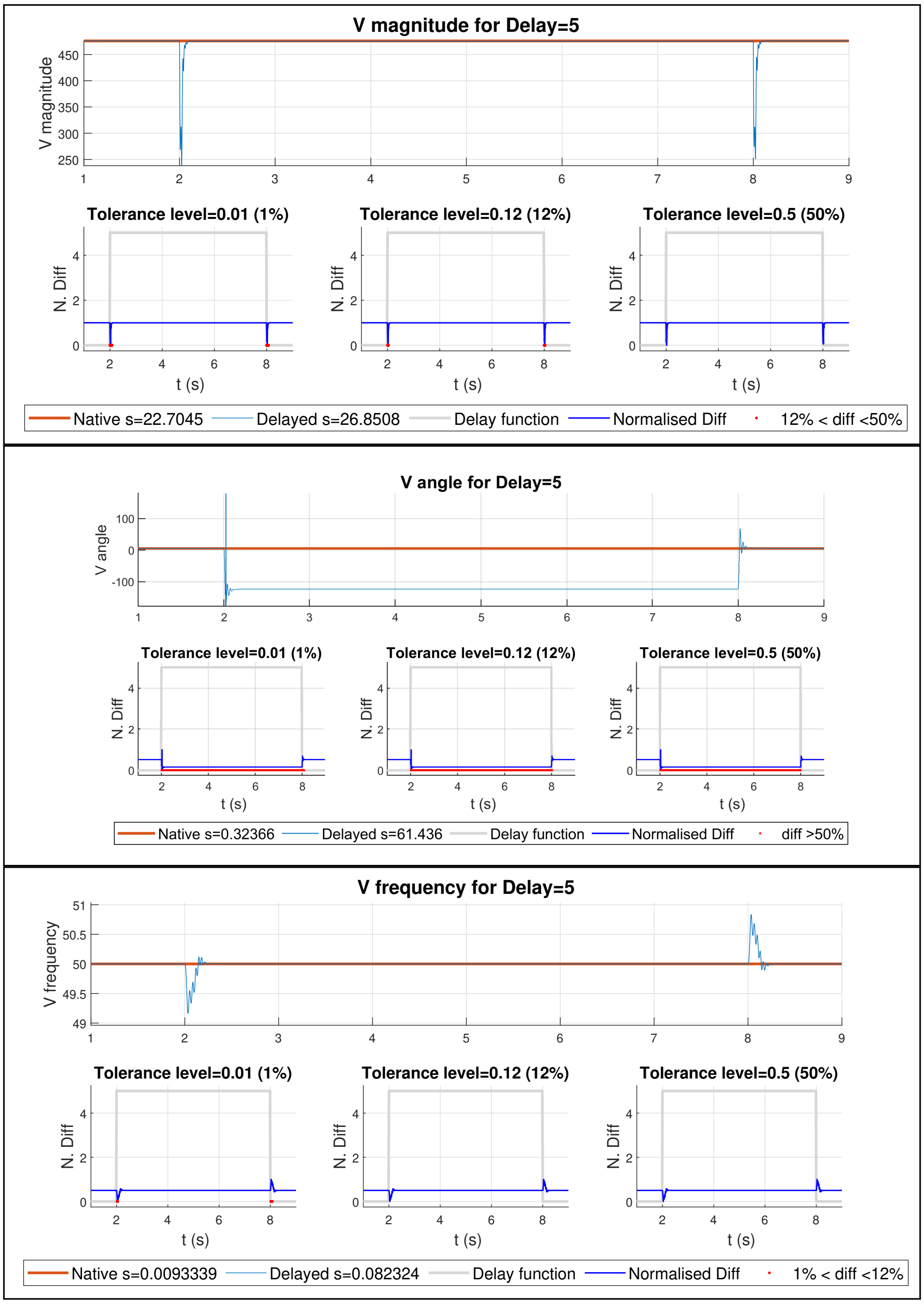


Figure 7.11: Results for Voltage Output for Instant Delay equal to Five

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

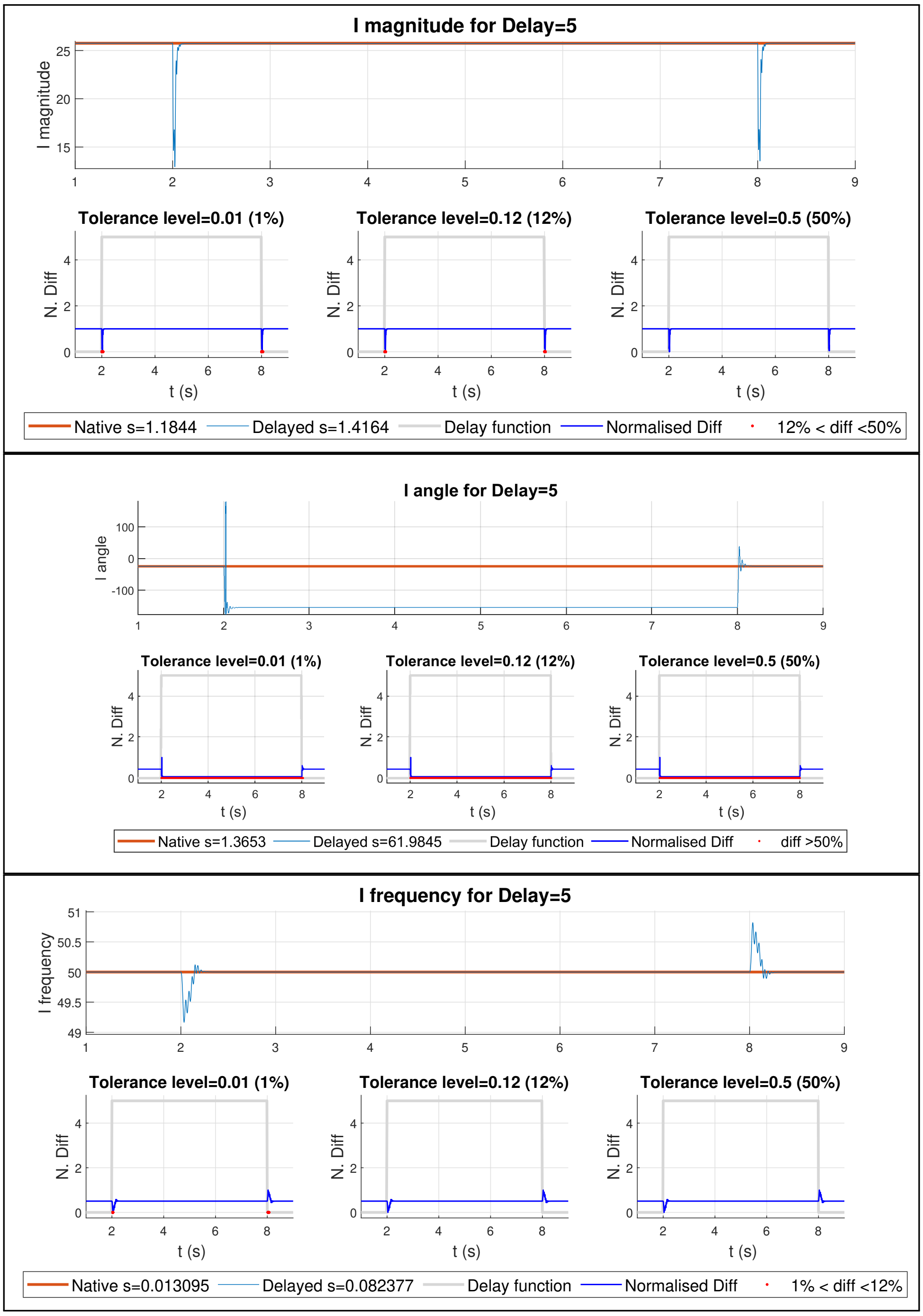


Figure 7.12: Results for Impedance Output for Instant Delay equal to Five

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -120^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

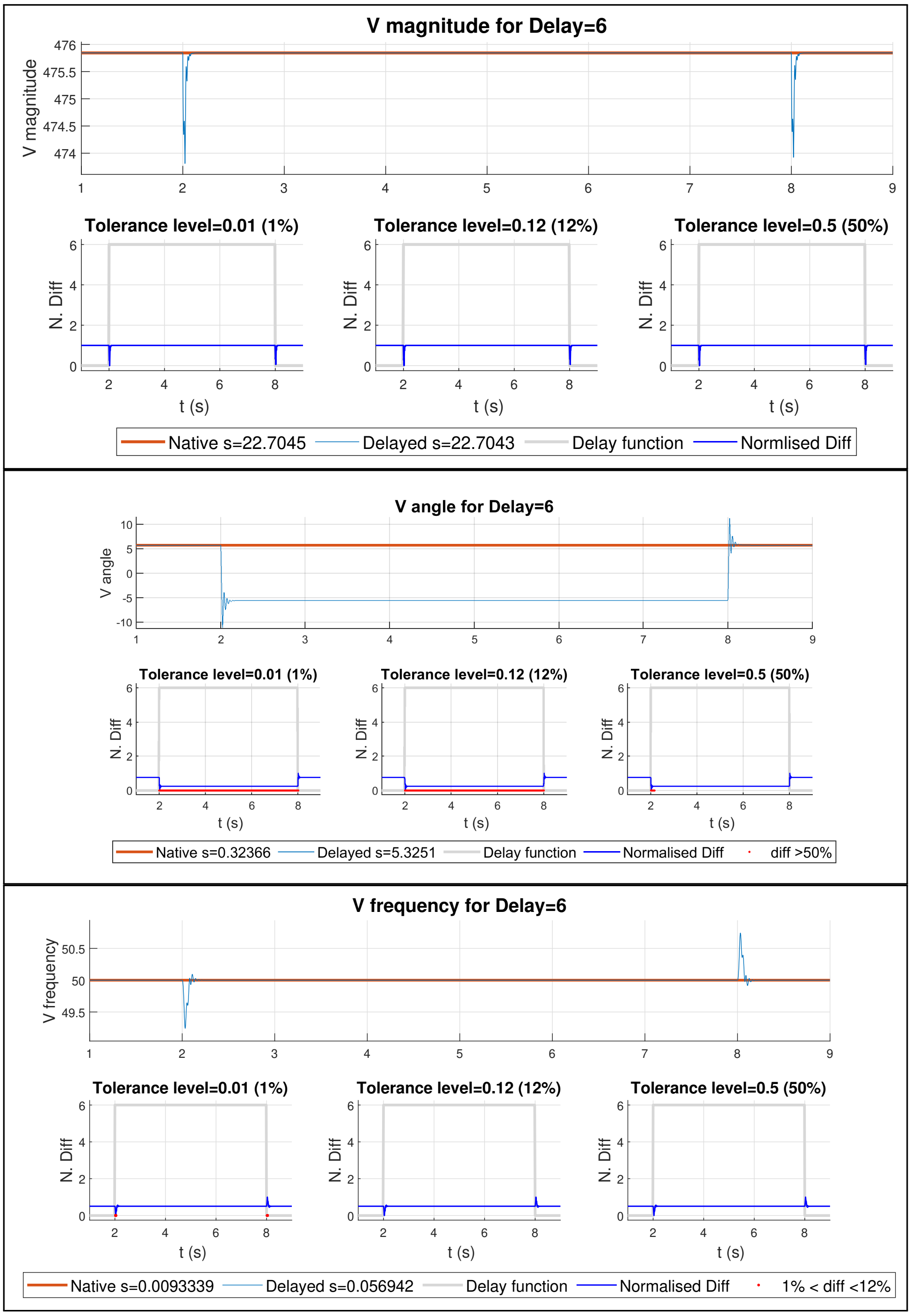


Figure 7.13: Results for Voltage Output for Instant Delay equal to Six

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -6^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

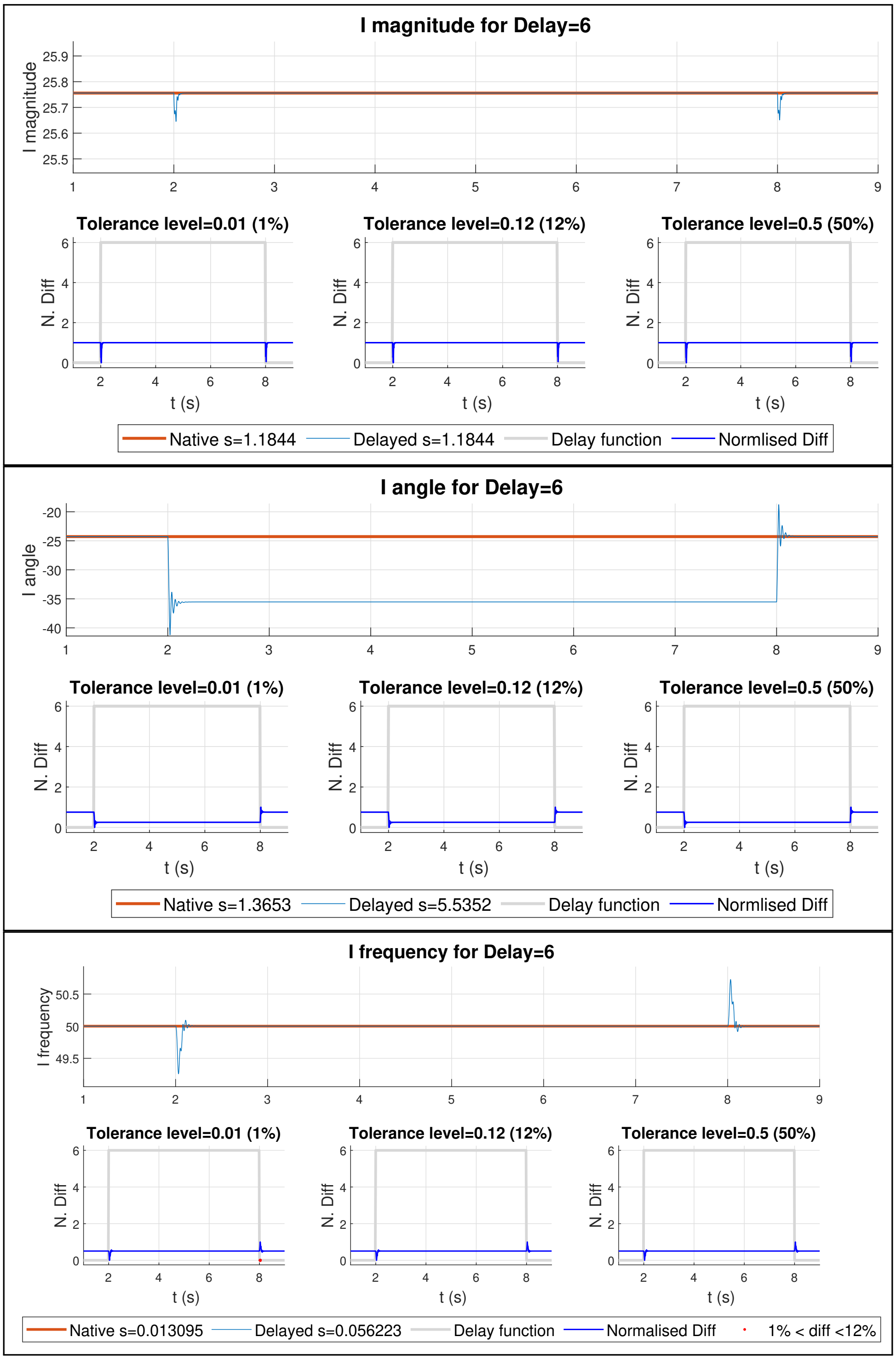


Figure 7.14: Results for Impedance Output for Instant Delay equal to Six

- Apparently identical spikes are present for the magnitude graph, at initiation and termination of attack.
- Similar, but mirrored, spikes are apparent for the frequency, whereas the spikes for angle differs.
- A small constant shift of angle, possibly -6^0, is apparent, whereas the magnitude and frequency shows no constant alteration of value during the main period of the attack.

7.2.1 Conclusive remarks on instant delay simulations

Instant Delay Level of One

Figures 7.3 and 7.4 shows the result of the Instant delay attack of level One.

Instant Delay Level of Two

Figures 7.5 and 7.6 shows the result of the Instant delay attack of level Two.

Instant Delay Level of Three

Figures 7.7 and 7.8 shows the result of the Instant delay attack of level Three.

Instant Delay Level of Four

Figures 7.9 and 7.10 shows the result of the Instant delay attack of level Four.

Instant Delay Level of Five

Figures 7.11 and 7.12 shows the result of the Instant delay attack of level Five.

Instant Delay Level of Six

Figures 7.13 and 7.14 shows the result of the Instant delay attack of level Six.

7.3 Step-Wise Delay functions

The other flavour of delay attack considered, the step-Wise delay attack, focuses on effects caused by a slower rise of the delay level towards a pre-determined target level of delay. As there are no step-wise attack for delay level one, this category of attacks initiates the sequence of attacks by starting with a delay level of two.
The attack focuses on the following

- What are the effects of repetitive increases of the delay level by one for different number of repetitions?
- Are there any patterns observable:
    - Do the termination of the attack cancel the effect of the attack
    - Do the next level of increase produce corresponding effects?

On a suitable number of next pages, the the figures showing the results of running the Step-wise Delay Simulations of levels One trough Six are available for inspection of the results.
Comments are located underneath each figure.

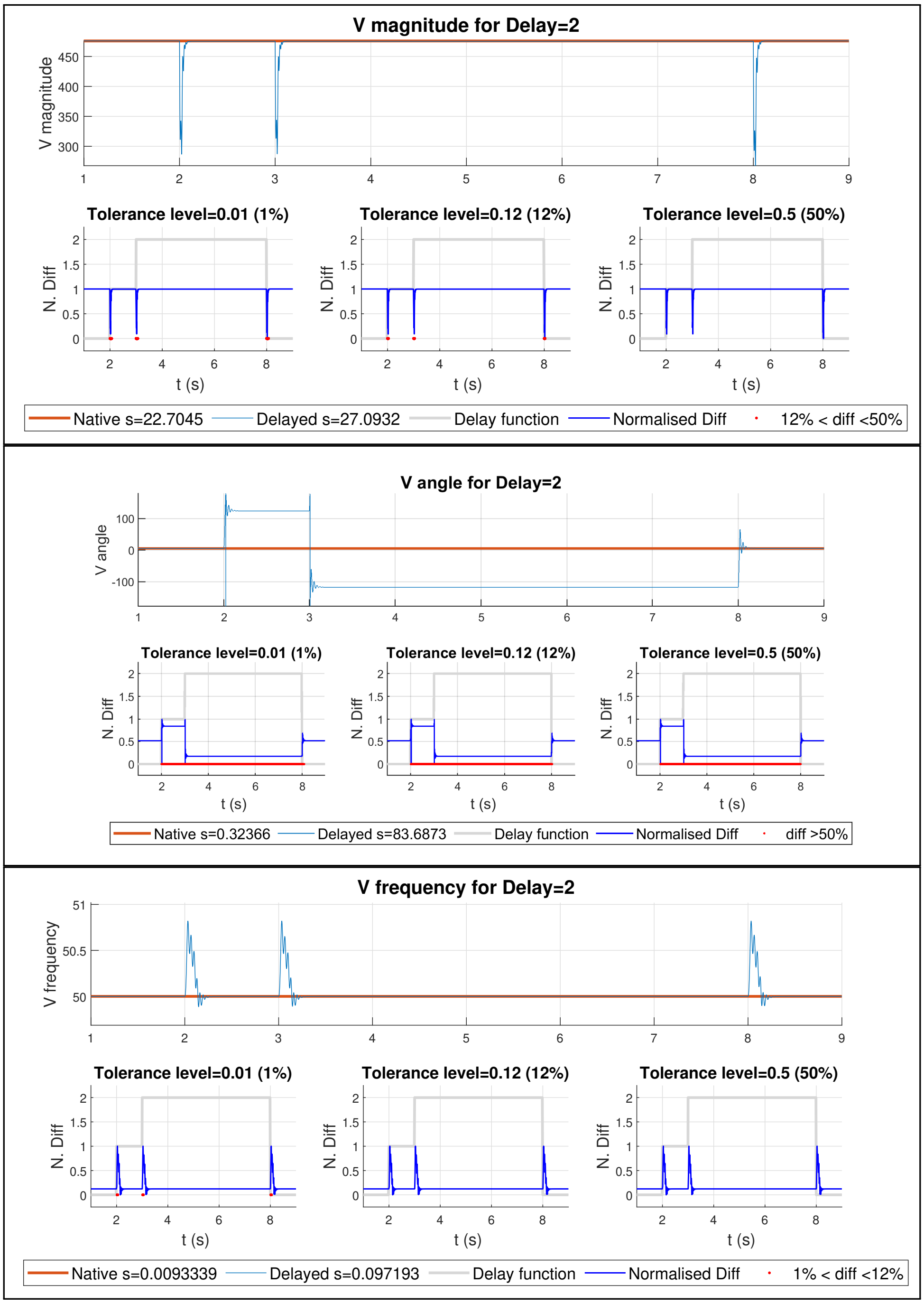


Figure 7.15: Results for Voltage Output for Step-Wise Delay equal to Two

Component **Main Observations**

The component graphs shows combinations of the results for the instant delay simulations of levels one and two.

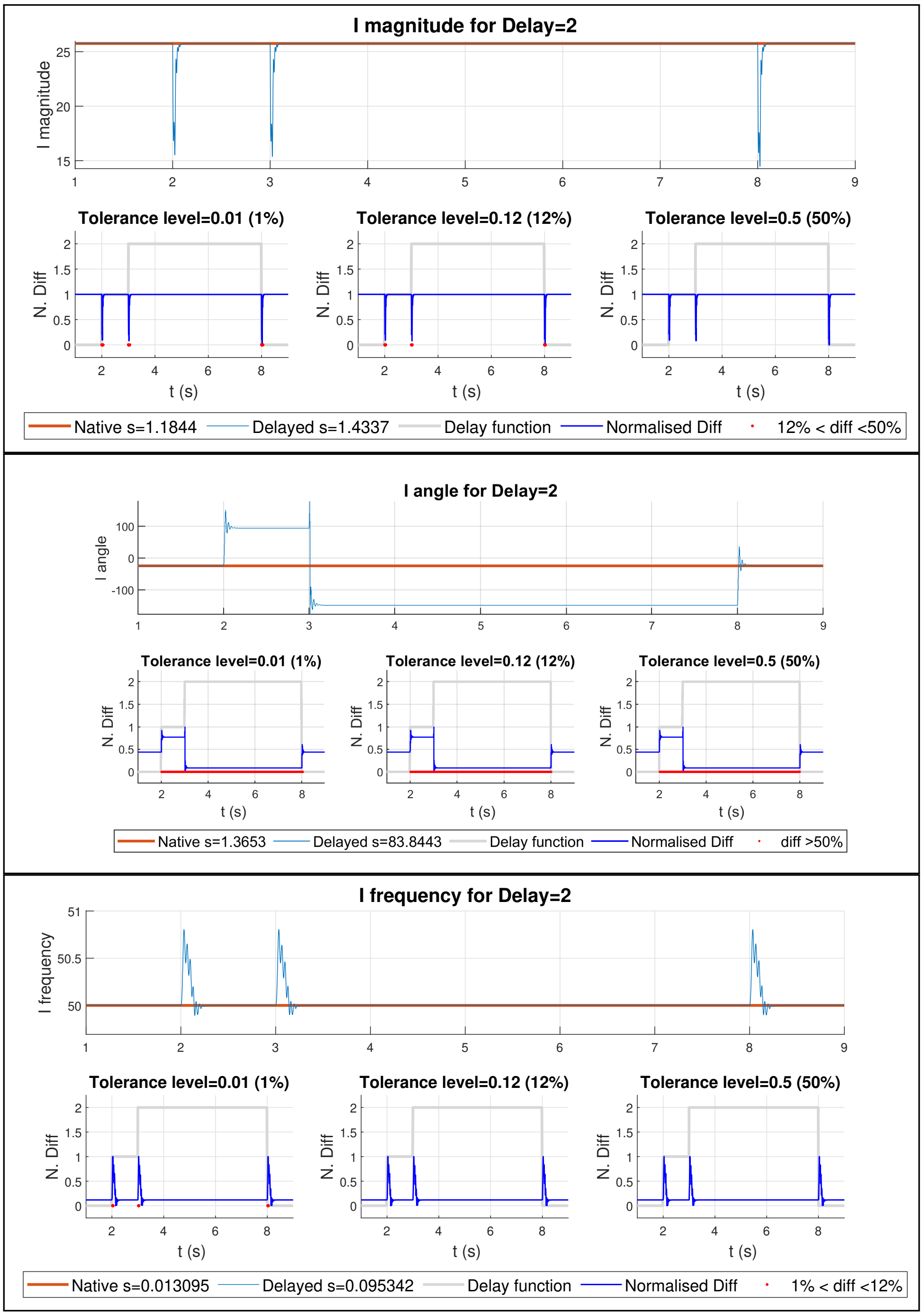


Figure 7.16: Results for Impedance Output for Step-Wise Delay equal to Two

Component	**Main Observations**
	The component graphs shows combinations of the results for the instant delay simulations of levels one and two.

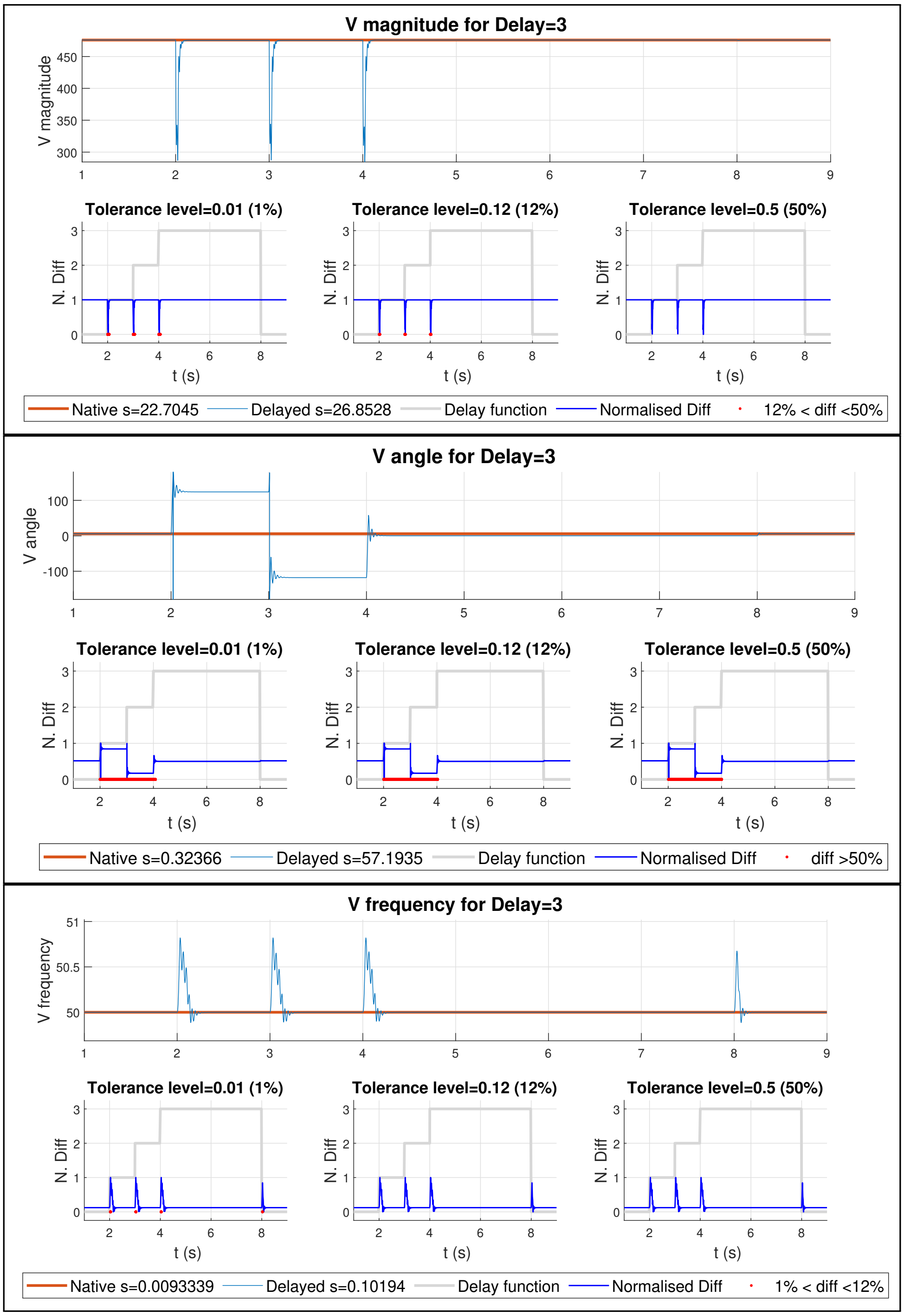


Figure 7.17: Results for Voltage Output for Step-Wise Delay equal to Three

Component	Main Observations
	The component graphs shows combinations of the results for the instant delay simulations of levels between one and three.

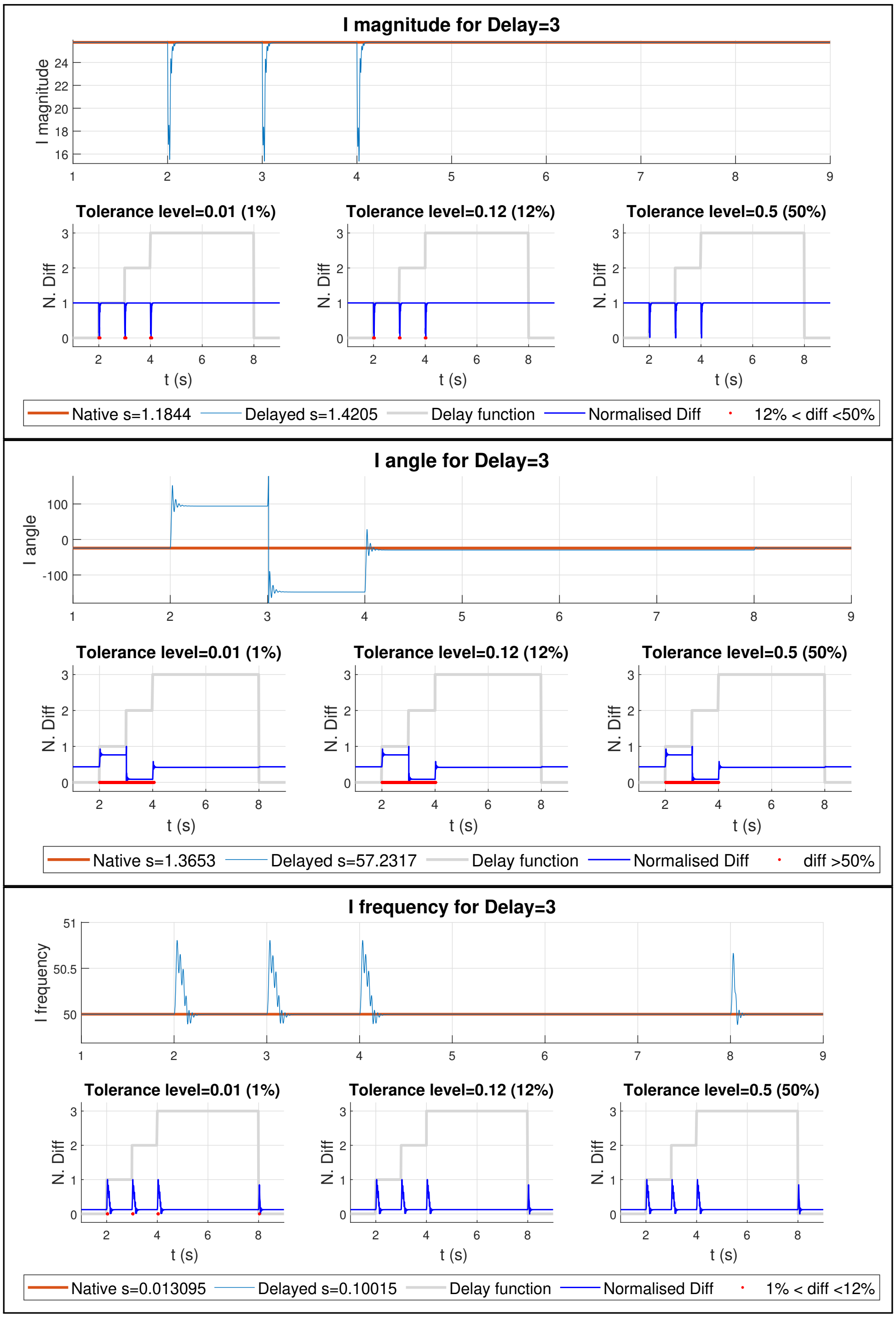


Figure 7.18: Results for Impedance Output for Step-Wise Delay equal to Three

Component	**Main Observations**
	The component graphs shows combinations of the results for the instant delay simulations of levels between one and three.

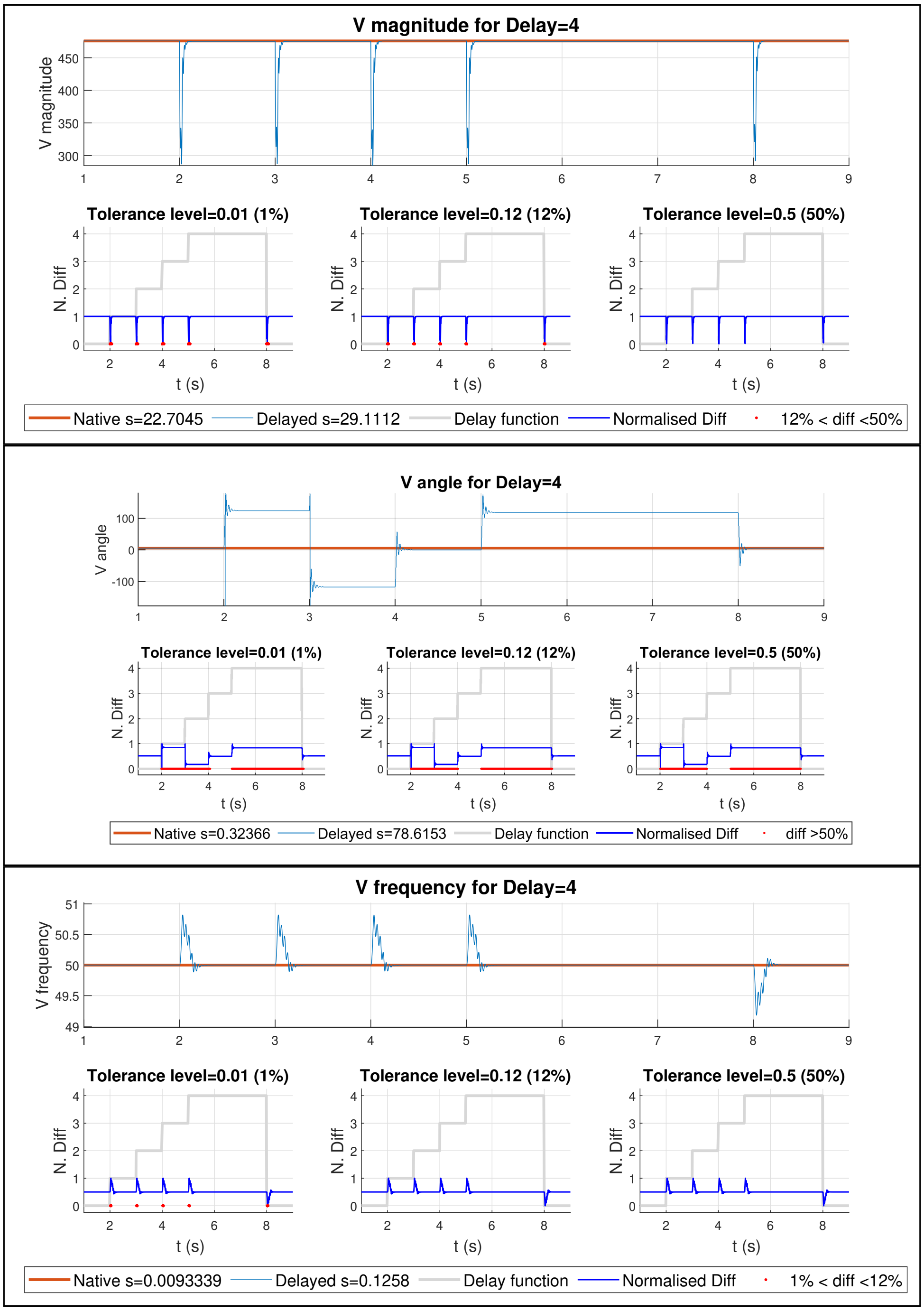


Figure 7.19: Results for Voltage Output for Step-Wise Delay equal to Four

Component	Main Observations
	The component graphs shows combinations of the results for the instant delay simulations of levels between one and four.

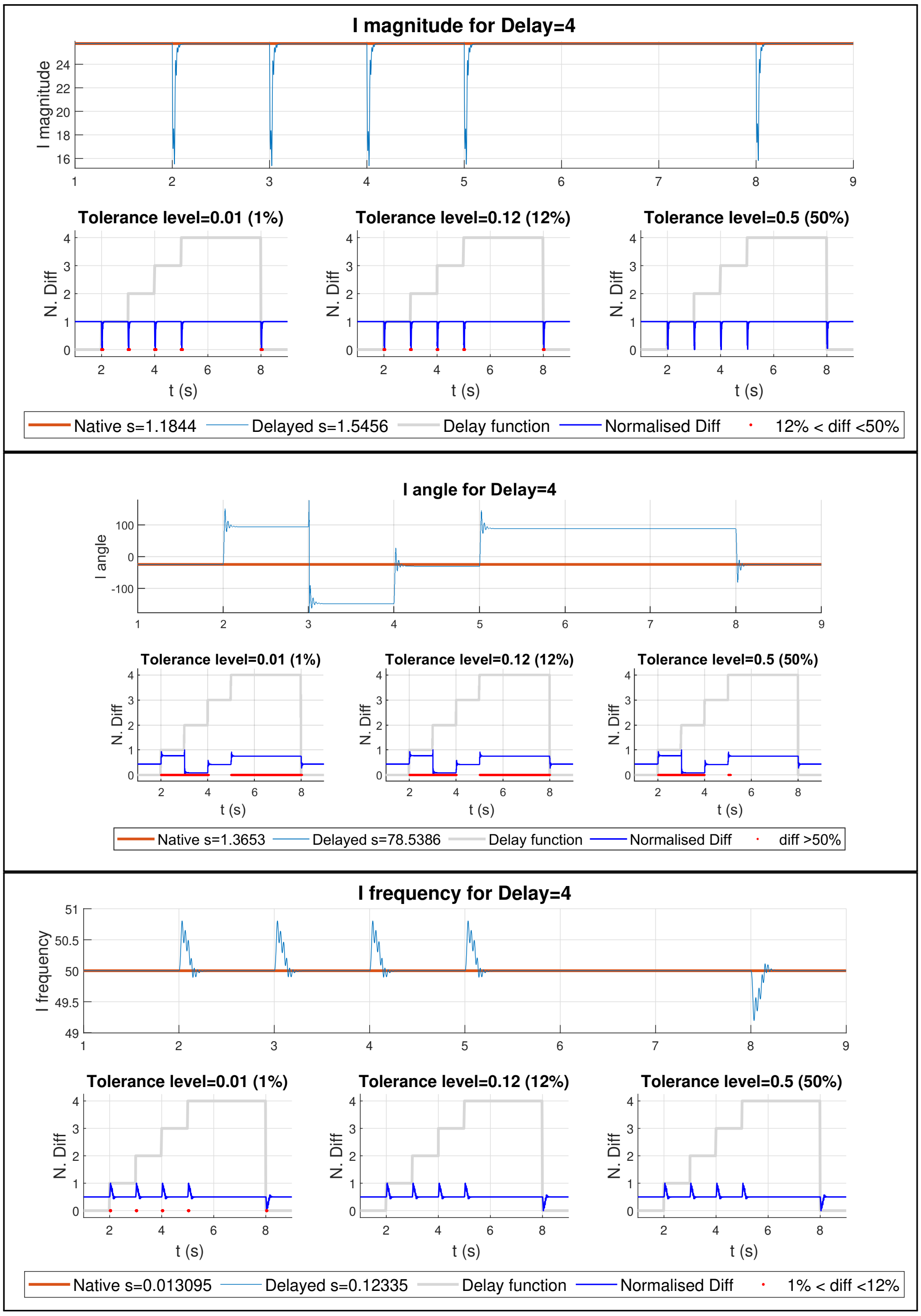


Figure 7.20: Results for Impedance Output for Step-Wise Delay equal to Four

Component	Main Observations
	The component graphs shows combinations of the results for the instant delay simulations of levels between one and four.

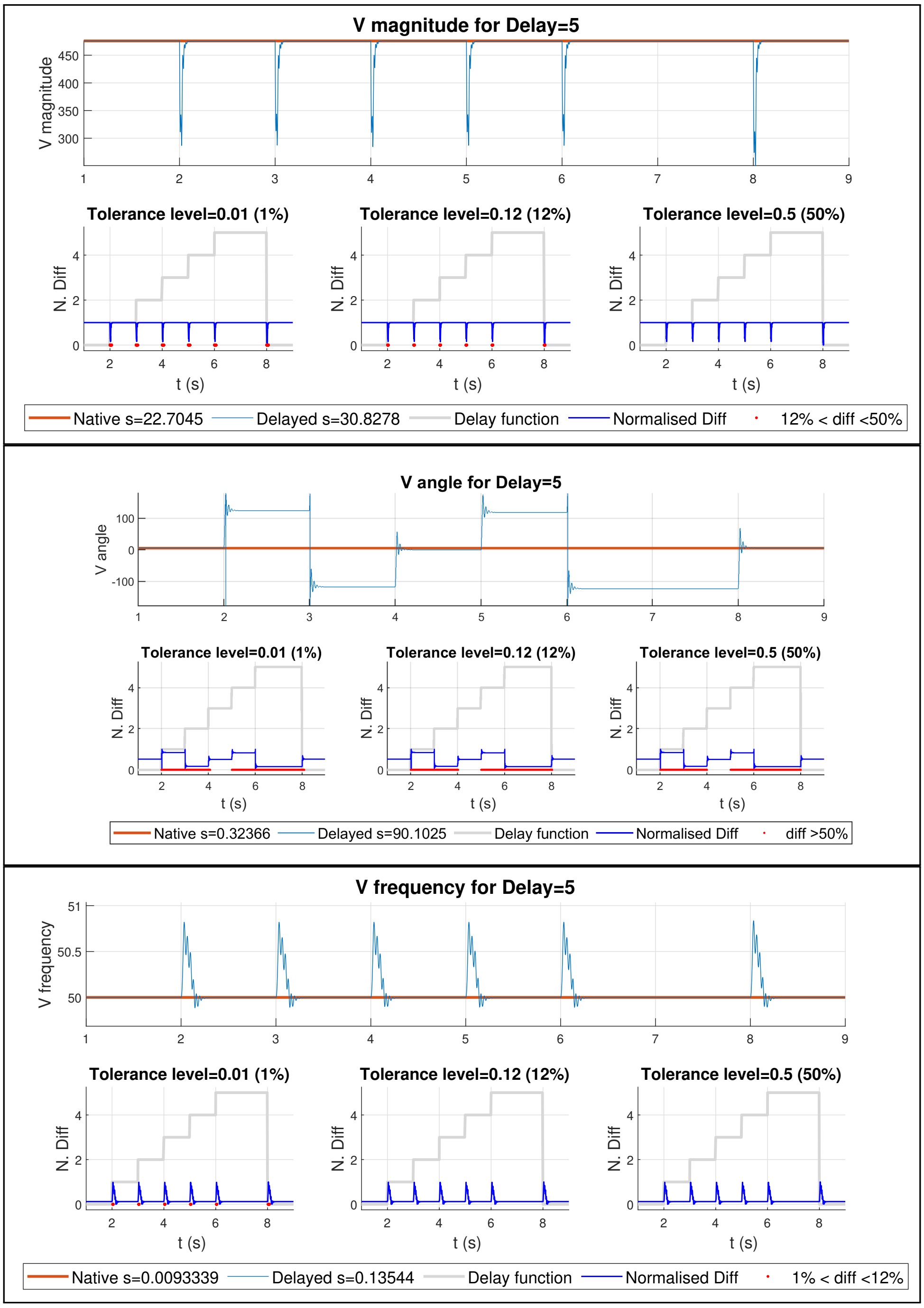


Figure 7.21: Results for Voltage Output for Step-Wise Delay equal to Five

Component	Main Observations
	The component graphs shows combinations of the results for the instant delay simulations of levels between one and five.

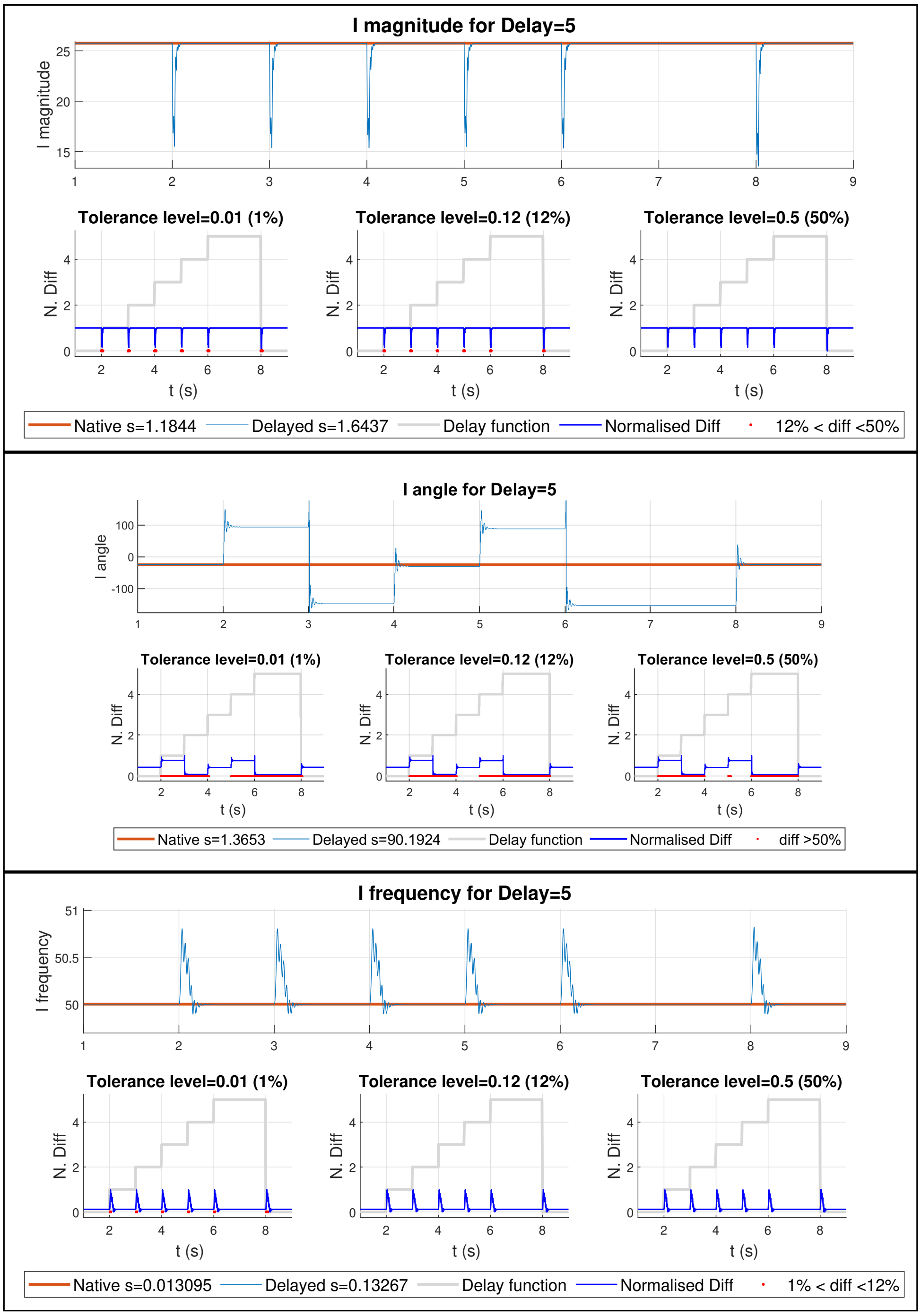


Figure 7.22: Results for Impedance Output for Step-Wise Delay equal to Five

Component **Main Observations**

The component graphs shows combinations of the results for the instant delay simulations of levels between one and five.

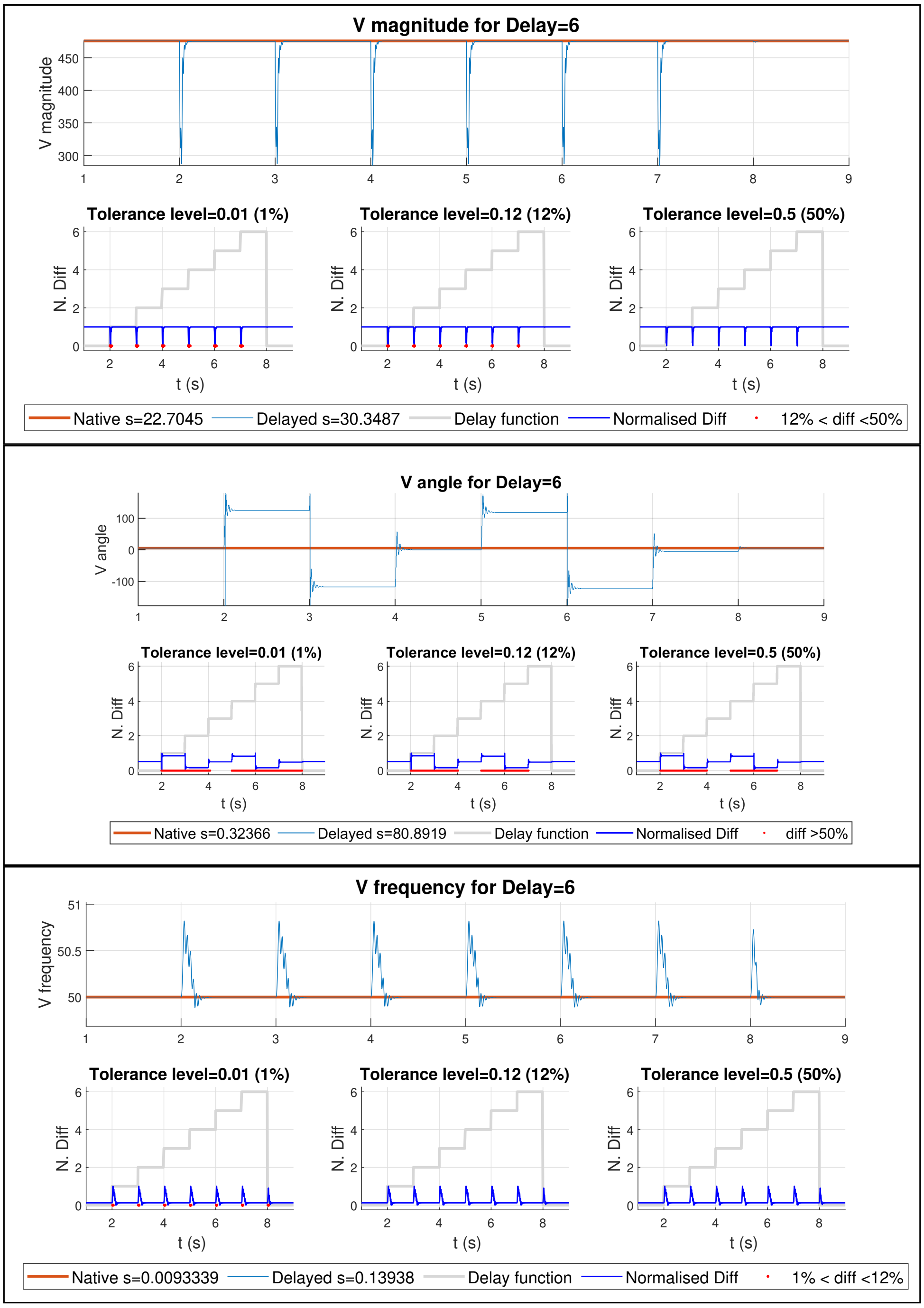


Figure 7.23: Results for Voltage Output for Step-Wise Delay equal to Six

Component	**Main Observations**
Magnitude	Drop in level at times of delay increase, no drop at reset to 0.
Angle	Periodic reduction of difference for delay levels 3 and 6. Alternating +/- differences for each increase of one
Frequency	Similar spikes at any time of delay change, even from 6 to 0 The component graphs shows combinations of the results for the instant delay simulations of levels between one and six.

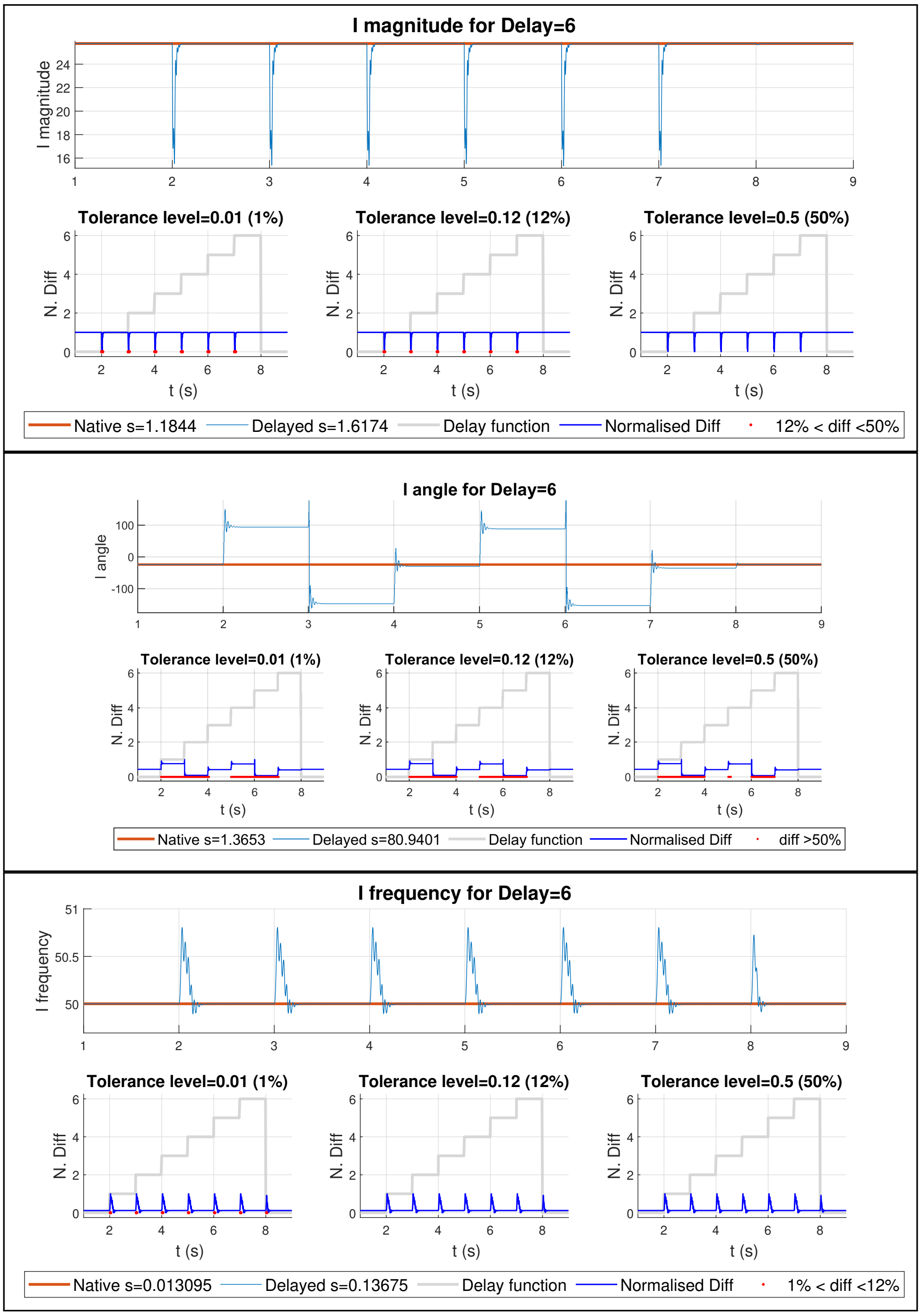


Figure 7.24: Results for Impedance Output for Step-Wise Delay equal to Six

Component	Main Observations
Magnitude	Drop in level at times of delay increase, no drop at reset to 0.
Angle	Periodic reduction of difference for delay levels 3 and 6. Alternating +/- differences for each increase of one
Frequency	Similar spikes at any time of delaly change, even from 6 to 0 The component graphs shows combinations of the results for the instant delay simulations of levels between one and six.

7.3.1 Conclusive remarks on running Step-Wise delay simulations

Step-Wise Delay Level of Two

Figures 7.15 and 7.16 shows the result of the Step-wise delay attack of level Two.

Step-Wise Delay Level of Three

Figures 7.17 and 7.18 shows the result of the Step-wise delay attack of level Three.

Step-Wise Delay Level of Four

Figures 7.19 and 7.20 shows the result of the Step-wise delay attack of level Four.

Step-Wise Delay Level of Five

Figures 7.21 and 7.22 shows the result of the Step-wise delay attack of level Five.

Step-Wise Delay Level of Six

Figures 7.23 and 7.24 shows the result of the Step-wise delay attack of level Six.

Chapter 8

Discussion

8.1 Introduction

8.1.1 Verification of model

For verification purposes, results for the delay level of 0 is presented. In this case, the original and delayed graphs should be identical.

Comments on the result:

The results of running the simulation with a delay of Zero produces a number of figures of pMU output consisting of indistinguishable signal graphs for the Native and Delayed output, with identical standard deviation, and no traces of red parts in the graphs showing degree of tolerance, for any PMU output Component under study. The result may be regarded as indicative of a correctly working delay function, as well as the dualPMU being a correctly designed PMU subsystem.

8.2 Comments on various aspects related to the results

For the Instant delay attack of levels above two, a tendency of small variations for Delay Level three and Six seems to be visible.

- A delay of One alters the value for the **Angle** component of around 120^0 compared to the value for the native, undelayed, PMU output.
- A delay of Two alters the value for the **Angle** component of around -120^0 compared to the value for the native, undelayed, PMU output.
- A delay of Three alters the value for the **Angle** component a small number, like -6^0 for the level of three, compared to the value for the native PMU output.

Even though no simulations for levels above six are performed, there seems to be a pattern related to the angular component value. This phenomena may possibly be related to the 120^0 separation between the three phases of the PMU input signal.

From my inspection of the figures presenting the results, it seems to be cases of a combination of results obtained during some of the instant delay attack simulations. The Step-Wise delay attack with a Delay level of Two, for instance, is initiated the same way as the Instant Delay attack of a Delay Level of one.

Regardless of the attack being Instant or Step-wise, the termination of the attacks involves an instant drop of delay level from the delay level specified, to Zero. Therefore, the finals second of the simulation using the step-wise attack should be the same as that of the corresponding Instant delay attack.

8.2.1 Similarity Requirements

There seems to be a consistent tendency of graphs showing smaller distance between the delayed output and the native PMU output, and the lower values for ranges of the diff variable being compared with the tolerance levels in the plots located in the lower part of each figure.

Chapter 9

Conclusion

- After running the initial simulation, with a delay level of Zero, for model-validation, the remaining results seems to provide consistent results, making it possible to get some ideas, at least, on which delay level, and attack type to use for optimising the stealthiness versus the possible harm don to the attack target.
- The simulations constitutes an initial attempt to differentiate between a number of parameters for attack, like the similarity measures, as well as the delay level.
- The Step-wise attack seems to be a nice tool in order to observe the effects of a small variation of delay level, whereas the instant delay level may show the effects of greater increases of delay level.

9.1 Summary

From the results present, i wold summarise my conclusions as follows.

- The data material present in the results chapter provides sufficiently good evidence of the simulation model being consistent enough to produce predictable effects on the output values.

9.2 My contribution:

Given the conclusion the simulation produces predictable effects, the thesis has resulted in the availability of a system capbele of determinig effects of a simulated Time Delay attack on PMU input values.

9.3 Considerations related to future work

The initial values for tolerance levels of 1%, 12%, and 50%, may be tuned for any future investigations, in order to be able to find realistic and reliable stealthiness thresholds. It seems like there is not enough data in order to draw any reliable conclusions on the optimal values.

Bibliography

[1] S. W. Blume, *Electric power system basics : For the nonelectrical professional*, eng, Hoboken, N.J, 2007.

[2] I. Colak, R. Bayindir and S. Sagiroglu, 'The effects of the smart grid system on the national grids,' in *2020 8th International Conference on Smart Grid (icSmartGrid)*, IEEE, 2020, pp. 122–126.

[3] F. Li, X. Yan, Y. Xie, Z. Sang and X. Yuan, 'A review of cyber-attack methods in cyber-physical power system,' in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, IEEE, 2019, pp. 1335–1339.

[4] R. Kateb, P. Akaber, M. H. Tushar, A. Albarakati, M. Debbabi and C. Assi, 'Enhancing wams communication network against delay attacks,' *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2738–2751, 2018.

[5] M. Ullmann and M. Vögeler, 'Delay attacks — implication on ntp and ptp time synchronization,' in *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, IEEE, 2009, pp. 1–6.

[6] B. Moussa, M. Debbabi and C. Assi, 'Security assessment of time synchronization mechanisms for the smart grid,' *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1952–1973, 2016.

[7] M. Rihan, 'Applications and requirements of smart grid,' in Nov. 2018, pp. 47–79, ISBN: ISBN 978-981-13-1767-5. DOI: 10.1007/978-981-13-1768-2.

[8] A. Humayed, J. Lin, F. Li and B. Luo, 'Cyber-physical systems security—a survey,' *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[9] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, D. Wollman *et al.*, *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology ..., 2021.

[10] C. Alcaraz, G. Fernandez and F. Carvajal, 'Security aspects of scada and dcs environments,' in *Critical Infrastructure Protection*, Springer, 2012, pp. 120–149.

[11] R. Zamani, H. Panahi, A. Abyaz and H. H. Alhelou, ‘Introduction to wams and its applications for future power system,’ in *Wide Area Power Systems Stability, Protection, and Security*, Springer, 2020, pp. 45–69.

[12] S. Kumar, M. Soni and D. Jain, ‘Monitoring of wide area power system network with phasor data concentrator (pdc),’ *International Journal of Information Engineering and Electronic Business*, vol. 7, no. 5, p. 20, 2015.

[13] I. 6.-.-1.-.-1. 2018, *Measuring relays and protection equipment, part 118–1: Synchrophasor for power systems–measurements*, 2018.

[14] B. Appasani and D. K. Mohanta, ‘A review on synchrophasor communication system: Communication technologies, standards and applications,’ *Protection and control of modern power systems*, vol. 3, no. 1, pp. 1–17, 2018.

[15] J. Dagle, ‘Importance of synchrophasor technology in managing the grid,’ in *Power System Grid Operation Using Synchrophasor Technology*, Springer, 2019, pp. 1–11.

[16] K. Martin and K. Chen, ‘Impact of phasor measurement data quality in grid operations,’ in *Power System Grid Operation Using Synchrophasor Technology*, Springer, 2019, pp. 13–40.

[17] A. Johnson, ‘Standards associated with synchrophasors,’ 2018, `https://www.naspi.org/sites/default/files/2017-03/01_sce_johnson_Standards_Associated_with_Synchrophasors_20161019.pdf` (visited: 2023-05-14).

[18] J. C. Eidson, *Measurement, control, and communication using IEEE 1588*. Springer Science & Business Media, 2006.

[19] S. Ali, M. Jawad, B. Khan, C. Mehmood, N. Zeb, A. Tanoli, U. Farid, J. Glower and S. Khan, ‘Wide area smart grid architectural model and control: A survey,’ *Renewable and Sustainable Energy Reviews*, vol. 64, pp. 311–328, 2016.

[20] D. Schofield, F. Gonzalez-Longatt and D. Bogdanov, ‘Design and implementation of a low-cost phasor measurement unit: A comprehensive review,’ in *2018 Seventh Balkan Conference on Lighting (BalkanLight)*, IEEE, 2018, pp. 1–6.

[21] K. Martin, G. Brunello, M. Adamiak, G. Antonova, M. Begovic, G. Benmouyal, P. Bui, H. Falk, V. Gharpure, A. Goldstein *et al.*, ‘An overview of the ieee standard c37. 118.2—synchrophasor data transfer for power systems,’ *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1980–1984, 2014.

[22] I. Ali, M. A. Aftab and S. S. Hussain, ‘Performance comparison of iec 61850-90-5 and ieee c37. 118.2 based wide area pmu communication networks,’ *Journal of Modern Power Systems and Clean Energy*, vol. 4, no. 3, pp. 487–495, 2016.

[23] A. Sundararajan, T. Khan, A. Moghadasi and A. I. Sarwat, 'Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies,' *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449–467, 2019.

[24] A. Finkenzeller, T. Wakim, M. Hamad and S. Steinhorst, 'Feasible time delay attacks against the precision time protocol,' in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, IEEE, 2022, pp. 3375–3380.

[25] W. Alghamdi and M. Schukat, 'Advanced methodologies to deter internal attacks in ptp time synchronization networks,' in *2017 28th Irish Signals and Systems Conference (ISSC)*, IEEE, 2017, pp. 1–6.

[26] G. De Pace, Z. Wang, J. Benin, H. He and Y. Sun, 'Evaluation of communication delay based attack against the smart grid,' in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, IEEE, 2020, pp. 1–6.

[27] E. Kabalci and Y. Kabalci, *Smart Grids and Their Communication Systems*. Springer, 2019.

[28] Y. N. Kunang, S. Nurmaini, D. Stiawan and B. Y. Suprapto, 'Attack classification of an intrusion detection system using deep learning and hyperparameter optimization,' *Journal of Information Security and Applications*, vol. 58, p. 102 804, 2021.

[29] *Implement three-phase parallel RLC branch - Simulink - MathWorks Nordic — se.mathworks.com*, `https://se.mathworks.com/help/sps/powersys/ref/threephaseparallelrlcbranch.html`, [Accessed 25-May-2023].

NTNU

Norwegian University of
Science and Technology