Resilient Synchrophasor Networks for the Real-Time Monitoring, Protection and Control of Power Grids: from Theory to Validation

THÈSE N^{O} 7724 (2017)

PRÉSENTÉE LE 14 JUILLET 2017
À LA FACULTÉ DES SCIENCES ET TECHNIQUES DE L'INGÉNIEUR
LABORATOIRE DES SYSTÈMES ÉLECTRIQUES DISTRIBUÉS - CHAIRE EOS HOLDING
PROGRAMME DOCTORAL EN ENERGIE

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Marco PIGNATI

acceptée sur proposition du jury:

Prof. D. Dujic, président du jury
Prof. M. Paolone, Dr S.-R. Cherkaoui, directeurs de thèse
Prof. A. Monti, rapporteur
Dr C. Y. Evrenosoglu, rapporteur
Prof. J.-Y. Le Boudec, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Suisse
2017

Beautiful is what we see,
more beautiful is what we know,
most beautiful, by far, is what we don't.
— Nicolas Steno

To my uncle Luca

Acknowledgements

I would like to thank my thesis director Professor Paolone for his constant and unconditional support along the years. In my opinion, his dedication, enthusiasm and passion for each new project are the best example of how to approach research in order to make it move forward.
My sincere gratitude goes also to Dr. Rachid Cherkaoui, Professors Jean-Yves Le Boudec, Cansin Yaman Evrenosoglu and Antonello Monti for the interesting discussions and comments before and during my PhD exam.
The collaboration with brilliant colleagues has been a key element of my PhD. Several are the friends and colleagues that should be named but, among all, I would like to acknowledge Paolo and Lorenzo, now partners in the coming adventure.
A special acknowledgment goes to Marian for her patience and the amazing smiles that made this last year of PhD fly by.
Finally, I am grateful of having such a supportive family: silent listeners of my PhD stories, but always ready to help in case of need. This is my idea of family.

Lausanne, May 7, 2017 Marco Pignati

Abstract

Operational practices of both power transmission and distribution grids are impacted by the increasing connection of renewable energy resources, electric vehicles and energy storage systems. A timely and accurate knowledge of the system state, coupled with a level of automation able to protect or control the system, enables a better operation of the electrical grids. In this respect, synchrophasor networks, might provide system operators with wide-area, synchronized, low latency, high refresh-rate measurements from phasor measurement units (PMUs). This thesis focuses on the design and validation of resilient synchrophasor networks in order to address some of the challenges that are preventing the adoption in real-fields of what proposed by the literature. First, the architectural layers of synchrophasor networks are described with particular focus on the time dissemination techniques suitable for phasor measurement units. Then, we propose a new data-pushing logic able to minimize the latency introduced at the concentration point without increasing the data incompleteness. The data-pushing logic is validated in three real synchrophasor networks adopting different telecom infrastructures (i.e., 4G-LTE, optical fiber links and twisted pairs).

In the context of reliable operation of synchrophasor networks, we propose an algorithm able to deal with intentional or unintentional bad data measurements. We also impersonate an attacker and we show that it is possible to forge delay attacks undetectable by state-of-the-art bad-data detection algorithms that can lead to physical grid damage. We use the proposed bad data algorithm as an effective way of neutralizing these attacks.

The IEEE C37.118 Class-P Std compliant synchrophasor extraction algorithm adopted in the real-fields is also implemented and validated in a GPS-synchronized real-time simulator. The simulated PMUs are used to validate two applications for the real-time protection and control of electrical networks by means of synchrophasor technology. The first one is a protection scheme that relies on PMU-based real-time state estimation processes to detect a fault and identify the faulted line. Then, we validate in a real-time hardware-in-the-loop (HIL) setup, the Grid Explicit Congestion Notification (GECN) voltage control mechanism for distribution networks, already presented in the literature. We show that, by leveraging on the accurate knowledge of the system state, GECN is able to control the state of the system in time-scales of seconds, in order to maintain its voltage level within predefined limits.

Keywords: Phasor measurement unit; WAMPAC; synchrophasor network; phasor data concentrator; state estimation; bad data; time-synchronization; time-attack; fault detection and location; hardware-in-the-loop; field trials.

Résumé

L'exploitation en temps réel des réseaux de transport et de distribution d'électricité est influencée par la pénétration croissante des sources d'énergie renouvelable, des véhicules électriques et des systèmes de stockage d'énergie. Une connaissance précise de l'état du système, associée à un niveau d'automatisation capable de le protéger ou de le contrôler, permettrait un meilleur fonctionnement de celui-ci. À cet égard, les réseaux de synchrophaseur peuvent fournir aux opérateurs du réseau des mesures, sur une grande portée, avec un taux de rafraichissement élevé, et à faible latence à partir d'unités de mesure de phaseurs (PMUs). Cette thèse porte sur la conception et la validation de réseaux de synchrophaseurs résilients afin de répondre à certains des défis qui empêchent encore l'adoption dans le monde réel de tels systèmes comme le propose la littérature. Tout d'abord, les couches architecturales des réseaux de synchrophaseurs sont décrites en mettant l'accent en particulier sur les techniques de diffusion temporelle adaptées aux unités de mesure du phaseur. Ensuite, nous proposons une nouvelle logique de poussée de données capable de minimiser la latence introduite au point de concentration sans augmenter la perte des données. La logique de transmission de données est validée dans trois réseaux réels de synchrophaseurs adoptant différentes infrastructures de télécommunication (c'est-à-dire 4G-LTE, des liaisons à fibres optiques et des paires torsadées).

Dans le contexte du fonctionnement fiable des réseaux de synchrophaseurs, nous proposons un algorithme capable de traiter des mesures intentionnellement ou non intentionnellement erronées. Nous représentons également un système d'attaque et nous montrons qu'il est possible de réaliser des attaques causant des retards indétectables par des algorithmes de détection de données erronées réputés être à la pointe, pouvant ainsi conduire à des dommages physiques au réseau. Nous utilisons l'algorithme de données erronées proposé comme un moyen efficace de neutraliser ces attaques.

L'algorithme IEEE C37.118 classe-P Std compatible avec l'algorithme d'extraction de synchrophaseur adopté dans les applications réelles est également implémenté et validé dans un simulateur GPS synchronisé en temps réel. Les PMU simulées sont utilisées pour valider deux applications pour la protection et le contrôle en temps réel des réseaux électriques au moyen de la technologie de synchrophaseurs. Le premier est un système de protection qui repose sur des processus d'estimation d'état en temps réel basés sur les PMUs pour détecter un défaut et identifier la ligne en défaut. Ensuite, nous validons en temps réel la configuration HIL, le mécanisme de contrôle de tension GECN pour les réseaux de distribution, déjà présenté dans la littérature. Nous montrons qu'en utilisant la connaissance précise de l'état du système, GECN est capable de contrôler l'état du système dans des échelles de temps de l'ordre de secondes, afin de maintenir son niveau de tension dans des limites prédéfinies.

Keywords : Unités de mesure de phaseurs ; WAMPAC ; réseaux de synchrophaseurs ; concentration des phaseurs ; estimation d'etat ; données erronées ; synchronisation temporelle ; attaque temporelle ; détection et localisation des défauts ; hardware-in-the-loop ; essais sur le terrain.

Contents

Acknowledgements **i**

Abstract (English/Français) **iii**

Introduction **1**
- Motivation . . . 1
- Dissertation outline . . . 2
- Contributions . . . 3

1 State of the art in power systems real-time situational awareness **5**
- 1.1 Wide area monitoring protection and control systems . . . 5
  - 1.1.1 Research . . . 6
  - 1.1.2 Operation practices . . . 7
  - 1.1.3 Ongoing challenges . . . 9
- 1.2 Wide area systems adaptations to the case of distribution networks . . . 10
  - 1.2.1 Advantages . . . 11
  - 1.2.2 Ongoing challenges . . . 12

2 Modern synchrophasor networks and their time synchronization **15**
- 2.1 Architectural layers and components . . . 15
  - 2.1.1 Sensing . . . 17
  - 2.1.2 Data communication . . . 21
  - 2.1.3 Data process-and-operation . . . 26
- 2.2 Time synchronization . . . 27
  - 2.2.1 Time-reference and its dissemination . . . 28
  - 2.2.2 Satellite-based time dissemination . . . 30
  - 2.2.3 Terrestrial-based time dissemination . . . 34

3 Time critical functions and applications **39**
- 3.1 Situation awareness functions . . . 39
  - 3.1.1 Phasor data concentrator . . . 39
  - 3.1.2 Real-time state estimation . . . 47
- 3.2 Time critical power system applications . . . 56
  - 3.2.1 Fault detection and faulted-line identification . . . 56

3.2.2 Voltage regulation scheme for distribution networks 63

4 Quality and reliability of PMU-based time critical functions 71

4.1 Bad data detection and identification 71

4.1.1 Post-estimation methods 72

4.1.2 Pre-estimation methods 74

4.1.3 A pre-estimation filtering process of bad data for linear power system state estimators using PMUs 75

4.1.4 Performance evaluation 79

4.2 Undetectable timing attack on linear state-estimation by using rank-1 approximation 87

4.2.1 System Model 88

4.2.2 Undetectable Time-Synchronization Attacks 90

4.2.3 Practically undetectable attack with two delays 93

4.2.4 Practically undetectable attack with more than two delays . . . 96

4.2.5 Performance evaluation 100

4.2.6 Countermeasures 110

5 Experimental activities 115

5.1 The real-time simulator 115

5.1.1 Integration of an IEEE Std. C37.118 compliant PMUs in a RTS . 116

5.2 The field trials 122

5.2.1 Services industriels de Lausanne 122

5.2.2 EPFL campus 125

5.2.3 Alliander - the BML feeder 127

5.3 Phasor data concentrator 130

5.3.1 Real field validation 131

5.3.2 Conclusions 138

5.4 Fault identification and location in RTS 139

5.4.1 Simulation environment 139

5.4.2 Performance Assessment 142

5.4.3 Conclusions 153

5.5 HIL validation of GECN for voltage control 154

5.5.1 HIL Setup and Experiment Design 155

5.5.2 Regression Testing 157

5.5.3 Demonstration Example and Performance Assessment 159

5.5.4 Conclusions 163

Conclusions 165

Appendix 169

List of acronyms 173

Bibliography **175**

Curriculum Vitae **189**

Introduction

Motivation

A power grid is an ever growing complex infrastructure experiencing large changes such as integration of renewable generation, load growth, integration of electric vehicles and energy storage, to name a few. A real-time accurate knowledge of the system state has deemed to be crucial to better operate the grid under such changes, increase the effectiveness of system utilization, ensure the security of supply and prevent blackouts. Driven by these concerns, the deployment of synchrophasor technology is taking place in transmission networks, where these measurements have been considered as the enabler of the so-called wide area monitoring. Although the deployment of a single phasor measurement unit does not pose any particular problems, the operation of the so-called synchrophasor network[1] still presents unique challenges.

At the same time, the concept of wide-area monitoring, protection and control, can be scaled down and adopted in distribution networks to meet the increased reliability requirements of these systems. An augmented level of automation, coupled with low latency, high-refresh rate monitoring, can smooth the impact that distributed energy resources are having on the protection and voltage management practices of distribution systems. For these reasons, major efforts are currently under way to implement synchronized measurement technology in distribution networks enabling distribution network operators to change the operational practices of passive and active distribution networks.

Within this context, this thesis aims at addressing the main challenges that are preventing the adoption in the control rooms of what proposed by the literature on synchrophasor networks. Among the highlighted issues, the time, as fundamental component of any synchrophasor networks, represents the guideline throughout the manuscript.

---

[1] With the term synchrophasor network, we here refer to the architecture that, starting from multiple measurement points, is able to take protection and control actions on the network.

Dissertation outline

This thesis is organized as follows.

Chapter 1 presents the state-of-the-art in power system real-time situational awareness with particular focus on the role played by PMUs. Insight on the status of the current research and operational practices are given, always keeping the focus on the challenges that have still to be addressed. Additionally, the major efforts that are currently under way to implement synchronized measurement technology in distribution networks are presented.

In Chapter 2 the architectural layers of modern synchrophasor networks are presented together with their key-components. Particular focus is given to the importance of the time synchronization and time dissemination in order to meet the stringent latency requirements of some applications. In this context, the time dissemination techniques suitable for synchrophasor networks are introduced together with advantages and drawbacks when adopted in power systems.

Chapter 3 presents functions and applications that we envisioned as time-critical for a successful operation of a synchrophasor network. We propose a new data-pushing logic for data concentrators in order to reduce time latency. Additionally, functions to obtain a reliable estimate of the system's state are given. The second half of the chapter presents two state-estimation-based applications that exploit the availability of PMU data with different time constraints: (i) an application that, in time-scales of hundreds of milliseconds, leverages on the state estimation results to provide protection functions to the monitored network, and (ii) an application conceived to be able to control the state of the system in time-scales of seconds, in order to maintain its voltage level within predefined limits.

Chapter 4 starts with the analysis of state-of-the-art bad data detection and identification methods for power grid situation awareness systems. Then, a novel bad data detection method able to deal with intentional or unintentional tampering of synchrophasor measurements is presented. In the second part of the chapter it is shown that it is possible to forge attacks to the time reference of a number of synchrophasors that are undetectable by state-of-the-art bad data detection methods and, at the same time, lead to physical grid damage. At the end of the chapter, the proposed bad data detection method is tested as a countermeasure to neutralize the attack.

Chapter 5 provides the experimental validation of the functions and applications presented in the previous chapters. The two applications that cope with faults or voltage violations are validated in a GPS synchronized real-time simulation platform. In this respect, the chapter describes (i) the platform and (ii) the implementation and validation of a real IEEE C37.118 Class-P Std compliant synchrophasor extraction algorithm used under these operating conditions. Moreover, three real field trials are described with their characteristics. They are used to experimentally validate the data concentrator pushing logic and the real-time state estimation functionality proposed in the thesis.

A summary of the main outcomes, remarks and future work concludes this dissertation.

Contributions

A list of the original contributions of the thesis can be found here below:

1. We design a phasor data concentrator (PDC) that, in addition to the data-pushing logics suggested by the reference standard, implements a logic that minimizes the latency introduced by the PDC without increasing the data incompleteness. The performance of the data-pushing logic is assessed and compared in terms of reliability, determinism and reduction of the overall latency in three real synchrophasor networks adopting different telecom infrastructures (i.e., 4G-LTE, optical fiber links and twisted pairs). The experimental results show that the proposed logic is indeed characterized by the lowest latency contribution.
2. We define and validate a protection mechanism for fault detection and faulted line identification that relies on PMU-based real-time state estimation processes. We show that, in terms of latency and accuracy, the proposed process is suitable for both transmission or distribution networks (active or passive), with solid-earthed and unearthed neutral, for low- and high-impedance faults of any kind (symmetric and asymmetric) occurring at different locations.
3. We define an algorithm for the pre-estimation filtering of bad data in PMU-based power system linear state estimators. The algorithm is able to assess the reliability of the incoming measurements by leveraging on the confidence in the predicted system state. The algorithm is proven to be computationally efficient and robust against multiple bad data of different nature and magnitudes. Additionally, the algorithm is able to distinguish between actual bad data and unexpected operating conditions and thus suitable for being adopted in real PMU-based state estimators.
4. We show that it is possible to forge delay attacks that are undetectable by state-of-the-art bad-data detection algorithms. We give a closed form for an undetectable attack that imposes two phase offset to two or more PMUs. We also propose different methods for combining two-delays attacks to produce a larger impact. We prove that the attacks are successful and can lead to physical grid damage.
5. Using a hardware-in-the-loop setup, we assess in real-time the performance

of a voltage control mechanism (already presented in the literature) for distribution networks. We model the network, the measurement devices, the data concentration, the real-time state-estimation and the control mechanism in the hardware and software chain. This enables us to assess the performance, in terms of accuracy and latency, of the proposed processes.

1 State of the art in power systems real-time situational awareness

The availability of synchronized measurements, provided by phasor measurement units (PMUs), is able to offer a real-time view of the behavior of a power system. The associated real-time knowledge of the system state has triggered the development of specific applications to better operate the grid, increase the effectiveness of system utilization, ensure the security of supply, and prevent blackouts. At the same time, an integrated architecture capable of enhancing the power system performance has unique deployment challenges. In this chapter, we present the state-of-the-art in power system real-time situational awareness. We give insights on the status of the current research and operational practices always keeping the focus on the challenges that have still to be addressed. Additionally, we introduce the major efforts that are currently under way to implement synchronized measurement technology in distribution networks.

1.1 Wide area monitoring protection and control systems

There is no common definition for a wide area monitoring, protection and control (WAMPAC) system, as it represent a complex infrastructure consisting of different system solutions aimed at meeting various application requirements. The building blocks are: synchrophasor measurements, high precision time synchronization, data communication and concentration, applications, and visualization tools. There is no common design for WAMPAC systems since their architecture is function of the specific applications' needs. On the other hand, a feature that is common for all the WAMPAC systems is the use of system-wide information and their capacity to communicate selected local information to a remote concentration point in order to achieve a given task [1].

The concept of WAMPAC in power systems is usually framed in the context of large - interconnected - transmission systems. Research explored several aspects of WAMPAC

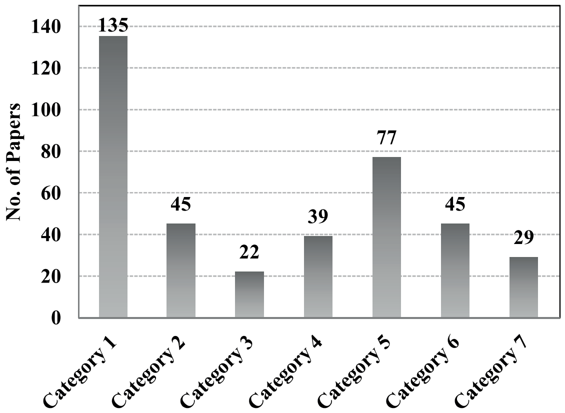


Figure 1.1 – Distribution of papers with respect to each category. Adapted from [2].

systems and real deployments have already taken place at the transmission level as summarized in what follows.

1.1.1 Research

In the latest years, PMUs are rapidly being deployed in electric power networks and consequently WAMPAC systems are emerging as advanced monitoring, protection and control infrastructures. Researchers have investigated a multitude of topics among which the PMU structural design, PMU placement, PMU applications within the substation and various wide-area functionalities. A classification of the publications on these topics on IEEE and IET journals and standards (up to 2014), includes the following categories, as reported in [2] and depicted in Fig. 1.1:

1. PMU algorithms and PMU/wide area monitoring systems (WAMS) structural issues;
2. State estimation consisting of or based on PMU data;
3. Model validation, calibration and extraction via PMU data;
4. Fault/event detection and location using PMU data;
5. WAMS-based dynamic/stability monitoring and prediction;
6. WAMS-based control strategies;
7. WAMS-based protection schemes.

While the early research has been devoted primarily to the PMU algorithms and PMU/-WAMS structural issues, the latest years have been characterized by a growing interest towards the development of robust wide-area-based monitoring, protection and control applications.

As the first requirement for realizing wide-area systems is the time-synchronized sampling over an entire power system, satellite based time dissemination systems have been largely adopted as preferred solution [3, 4, 5]. In this respect, attacks on the time-synchronization receivers have been a major concern in the literature. Indeed, the aim of the National Institute of Standards and Technology (NIST) report [4] is to "identify, analyze and provide guidance on technologies, standards and methodologies for addressing the practical timing challenges that are currently being experienced in wide area time synchronization". The concept of time-synchronization in a synchrophasor network and the related challenges are further expanded in this manuscript.

In addition to PMU algorithms and their time-synchronization, researchers are investigating all the fundamental components of WAMPAC systems. High-performance communication systems and information and communications technology (ICT) architectures have been explored in terms of impact on the reliability of the WAMPAC applications, for example, in [6, 7, 8]. Classical state estimation and bad-data detection techniques have been revised specifically to include PMU data (e.g., [9, 10, 11]). Additionally, state estimators relying entirely on PMU measurements have also been proposed (e.g., [12]). Research efforts are devoted to the PMU-based identification of grid impedance matrices [13] and Thevenin equivalents [14], necessary for the majority of the monitoring and protection algorithms for wide area systems. Researchers have produced a large number of fault detection and location schemes based on PMU data. In general, these schemes leverage on the accuracy and high refresh rate of PMUs. Due to the extent of the literature and the heterogeneity of the fault scenarios, a review on the current practices is given in Chapter 3.2.1.

1.1.2 Operation practices

The outcomes of the research and the success of first prototype systems led to the development and testing in real fields of applications designed to (i) reduce the number and impact of large failures and (ii) detect initiation of disturbances. Nevertheless, as reported in [15], there is still a major confidence gap in the industry between using synchrophasor tools for offline applications and the willingness to rely on synchrophasor tools for real-time critical applications.

Indeed, various publications reported the status of practical applications for different utilities and countries (e.g., [16, 17, 18]). The maturity of elementary applications (i.e., monitoring, model validation) is proven [16, 17, 18, 19]. In contrast, more advanced functions (e.g., control, protections) are still in an early phase. In particular, wide-area control and protection applications are mainly under development and in general not

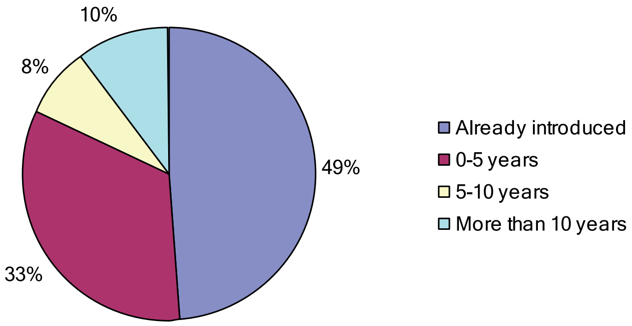


Figure 1.2 – Planned introduction of wide area technology. Adapted from [18].

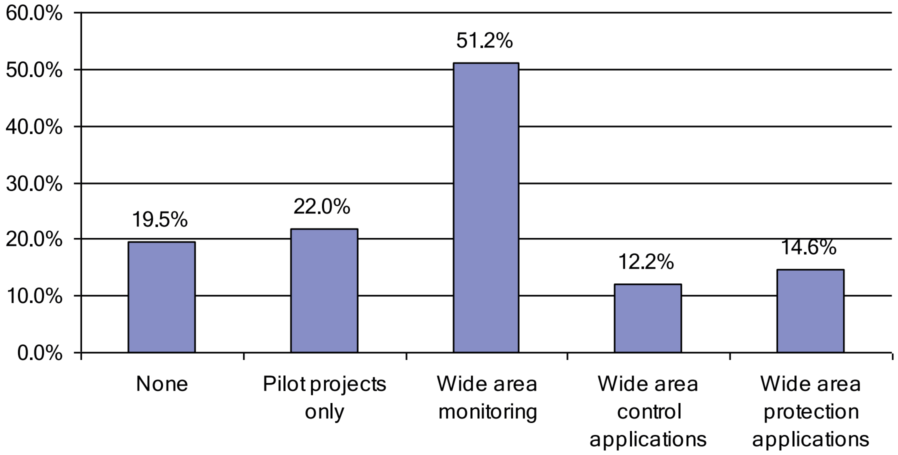
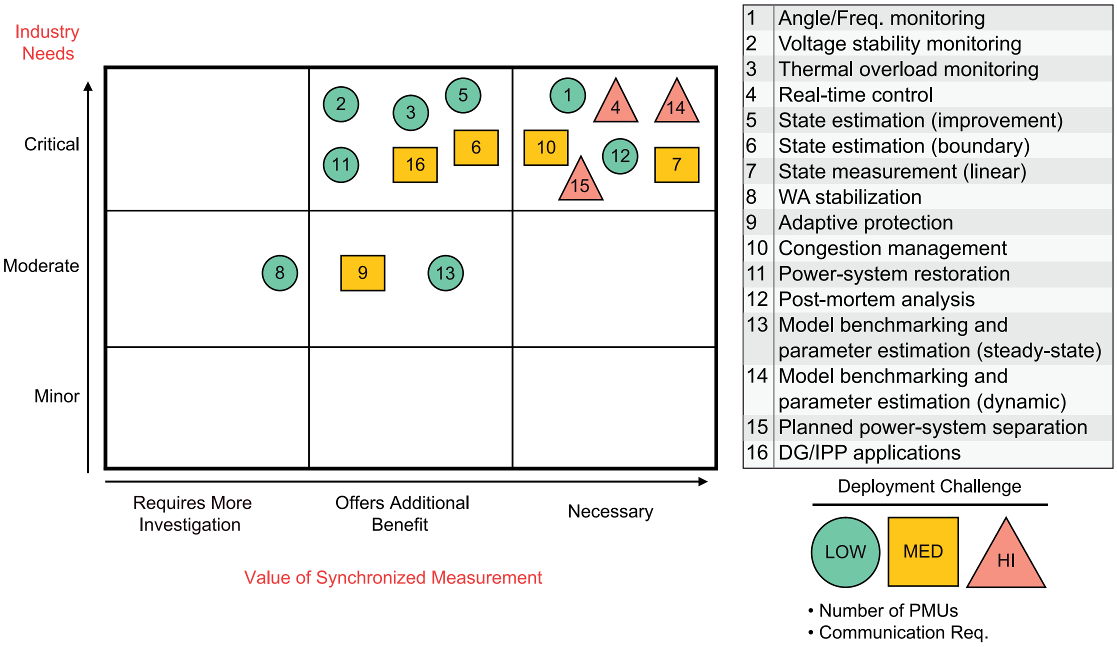


Figure 1.3 – Type of WAMPAC systems in operation. Adapted from [18].

yet mature enough to be considered as consolidated industry products, as described in [18]. A wider deployment of such advanced functions is expected to happen in the near future. In this respect, a survey was distributed to electrical utilities worldwide in order to understand the intentions of network operators to adopt wide area technologies and the current type of WAMPAC system in operations. Fig. 1.2 and 1.3 summarize the outcome of the survey.

In Fig. 1.4 it is illustrated the value that synchronized measurements can bring to the industry in terms of wide area applications. The feasibility of the targeted applications is also shown as function of the deployment challenge (number of PMUs needed, communication and application requirements).

The feasibility of these functions depends on the further advancements in several engineering fields. In what follows we provide an overview on the challenges that are preventing to operate a power system as an unique intelligent wide area system.



1	Angle/Freq. monitoring
2	Voltage stability monitoring
3	Thermal overload monitoring
4	Real-time control
5	State estimation (improvement)
6	State estimation (boundary)
7	State measurement (linear)
8	WA stabilization
9	Adaptive protection
10	Congestion management
11	Power-system restoration
12	Post-mortem analysis
13	Model benchmarking and parameter estimation (steady-state)
14	Model benchmarking and parameter estimation (dynamic)
15	Planned power-system separation
16	DG/IPP applications

Figure 1.4 – Synchronized measurements and industry needs for power transmission systems. Adapted from [20].

1.1.3 Ongoing challenges

The discrepancy between what presented in the literature and what currently in use in real-power systems is due to the following challenges imposed by the real-field deployment:

- *Time synchronization:* Several concerns have been expressed on the dissemination of an accurate time-reference for power system equipment. Issues might arise, for example, from time discontinuities (e.g., leap seconds) or the jamming and spoofing of time-signals [4]. Meanwhile, we are assisting to an increasing proliferation of devices requiring precise time synchronization in power system. This is leading to the exploration of alternative time dissemination methods and towards attempts to increase the robustness of existing technologies [5].

- *Latency of the control signals:* As highlighted in [2], one of the most critical barriers against the implementation of many theoretically-proven control and protection algorithms is the signal latency. This practical challenge has been only marginally discussed in the literature. In the real field, a delayed control signal can degrade or even deteriorate the performance of control/protection systems and thus researchers and real-field deployments have to carefully account for it.

- *Cyber security:* Data spoofing, denial of service, malicious code injection, man-in-the-middle attack, reconnaissance attack, packet injection attack (sniffing).

These are some of the security threats that can induce serious malfunctions in control center applications. Although such threats are common to other measurement devices, they have to be considered prior to a massive deployment of PMUs.

- *Data management and analysis:* Current data management methods could become burdensome for the large amount of data associated to the synchrophasor technology. Large amount of data may represent the bottleneck in exploiting wide area systems especially due to limited communication bandwidth. Additionally, data analysis experts are required to create visualization tools to rapidly extract and display meaningful information for operators in the control centers.
- *Control centers:* Since the advent of wide area infrastructures, it is clear the need to furnish the control centers with new situation awareness tools. The architecture of current control centers has to be revised as specified, for example, in [21]. The overall system has to be scalable and flexible as the number of installed PMUs is expected to increase over time from few units to, potentially, a device per node.
- *User acceptance:* Finally, it is important to guide the user through the learning curve from the installation of a synchrophasor system to their acceptance and use. Control room personnel need to be engaged, trained and committed to use and trust new real-time applications and data outside of post-event analysis.

1.2 Wide area systems adaptations to the case of distribution networks

While the deployment of PMUs at the transmission level is taking place, the possibility of augmenting the level of automation in distribution networks is under exploration at the research level. Studies on research and development priorities for distribution-system PMUs have been carried on, together with the deployment of first demonstrators. In what follows we present the state-of-the-art, advantages and open challenges of adapting the "wide-area" approach to distribution systems.

The deployment of automation systems and advanced technologies in distribution system is driven by the following challenges:

- *Reliability:* As the reliability of the electricity is considered a major concern for the customers, and considering that 90% of customer interruptions originate from distribution systems [22], a fast identification and isolation of faults is crucial. On the other hand, the current lack of monitoring and automation of distribution systems is the result of a trade-off between cost of better infrastructures and cost of manual inspection. Indeed, crews are often involved in the network restoration and therefore some interruptions are lengthy (i.e., in the range of tens of minutes to several hours). Automating the distribution systems would lead to shorter power outages (in average) and thus to increased reliability.

- *Impact of distributed energy resources (DERs):* As more active power sources are being connected (i) distribution networks are no longer purely passive, and this affects protection and voltage management practices; (ii) a disturbance on the load can trigger protection schemes and unnecessarily trip DERs. Details about the impact of DERs in distribution systems, with particular focus on protections of current and future distribution networks are discussed in [23, 24].

Various authors are exploring the possibility of deploying PMUs in distribution systems to address these issues. In particular, the adoption of PMU-based state estimators to develop low-latency and high-refresh rate state estimators for distribution networks is proposed in [25, 26]. The comparison of three-phase distribution system state estimation (DSSE) algorithms is given in [27]. Several contributions focused on the proper meter/PMU placement for DSSE. Placement algorithms have been shown to be able to integrate heterogeneous measurements, keeping the cost at minimum (e.g., [28]). Additional research has proposed robust meter placement with respect to the malfunction of some measurement devices or uncertainty in the distributed generations' (DGs') operative conditions (e.g., [29]).

Reference [22] analyses a number of use cases, suggested by distribution network utilities, where PMUs can provide crucial help (e.g., system reconfiguration to manage power restoration, operation of islanded distribution systems). The findings of report [22] are that "PMUs offer important and irreplaceable advantages over present approaches in the emerging distribution-system issues related to reliability, integration of distributed energy resources, and the changing electrical characteristics of load".

Currently, real deployments of PMUs at the distribution level have taken place mainly on university campuses (e.g, Illinois Institute of Technologies [30], UC Berkeley campus [31], École Polytecnique Fédérale de Lausanne [32] or within research projects (e.g., [33]). As it will be highlighted in the manuscript, in the case of [32] and [33], DSSE is performed. Additionally, PMUs have been used for monitoring purposes during the islanding maneuver of an active distribution network (ADN), significantly facilitating the operator maneuvers [34].

1.2.1 Advantages

The aspects that might facilitate the adoption of PMUs and, in a more general way, of distribution systems oriented towards a "wide area approach", are summarized in what follows:

- *Costs vs. benefits:* On one side, PMU prices and installation costs have dropped markedly since 2010 [15] and the implementation cost is likely to be less than the total cost of multiple, stand-alone measurement systems. On the other side, benefit analysis are showing the crucial role that PMUs might have for the future automation of distribution networks [22]. Indeed, several applications can take advantage of the same sensing and communication infrastructure. As for the case of transmission networks, also at the distribution level, the incremental cost of adding applications is minimal in comparison to the benefits received [18].
- *Sensing:* Currently, distribution networks are characterized by a limited penetration of sensing devices. This leaves room for designing architectures able to meet the applications' requirements. Additionally, the use of electronic sensors (e.g., clamp-on flexible Rogowski coils) enables the deployment of sensing devices rapidly and without affecting the final customers.
- *Limited area:* The area covered by a distribution network is reduced if compared to a transmission one. This calls for a limited number of devices needed to fully monitor the system, with subsequent lower bandwidth requirements for the communication layer. Additionally, a reduced number of cells is sufficient when adopting mobile telecommunication technology over a geographically small area, thus reducing the overall latency.

1.2.2 Ongoing challenges

The real-time monitoring, control and protection of distribution systems needs to cope with additional issues, if compared with transmission systems:

- *Phase angle displacement:* The deployment of PMU devices in distribution systems calls for higher accuracy in the metering systems, because of the limited phase angle displacement. The development and validation of a PMU tailored for distribution systems was the topic of the dissertation [35]. An example of phase displacement between voltage phasors at the beginning and end of a 20 kV overhead line is given in Fig. 1.5.
- *Time synchronization:* As for the transmission systems, the time synchronization of PMUs is a major challenge. The satellite-based time dissemination represents an additional issue for distribution feeders in urban context, due to the limited clear-sky view. Wired based time dissemination may be a valuable alternative. The topic of time synchronization and dissemination is further expanded in Chapter 2.
- *Communication:* The current panorama of the status of communication networks and associated bandwidth is largely non-homogeneous. There are examples of utilities with fiber connecting each substation to the control room. In

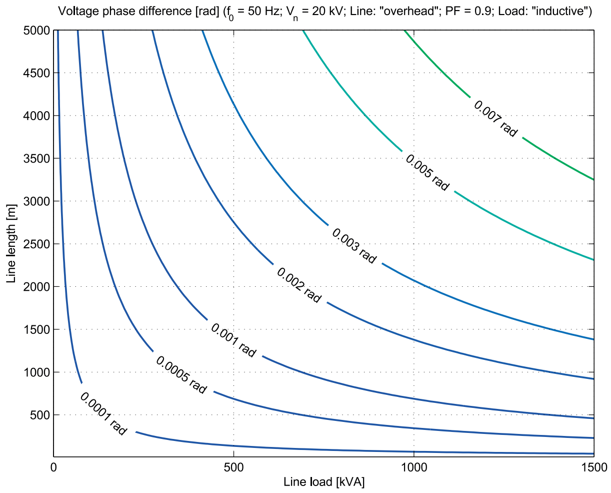


Figure 1.5 – Influence of the line load and line length on the phase difference between voltage phasors measured at the beginning and end of a overhead line, modeled as π-line. Adapted from [35, Chapter 2].

few cases, the fiber extends all the way to the customer [22]. Other utilities have engaged in partnerships with smart-grid demonstration projects and are building communication networks for automation and reliability. However, even if increasing, fiber optic is not currently a common choice, because of its cost. In these cases, wireless technology, Ethernet communication or other wired technologies have to be chosen on a per-substation basis.

- *Network parameters:* Many algorithms (e.g., DSSE) require the knowledge of topology and line parameters. Such information is not always available to the network operator nor fully reliable. Additionally, a direct estimation of the line parameters based on PMU measurements for distribution networks is difficult due to the limited phase angle displacement. The knowledge of the admittance matrix is a constraint for the development of some automation solutions for distribution systems.
- *Proofs of concept:* More research, demonstration projects and information sharing is needed. The development of common testing and calibration platforms as well as standards for PMUs in distribution systems is advised.

Within this context, the manuscript highlights:

- The architectural design of a wide area system adapted for distribution networks;
- The definition of time critical functions with particular reference to situational awareness and fault location/protection tools;

- The resiliency of the above functions with respect to bad data and intentional cyber attacks;
- The experimental validation via real-time digital simulations and real-scale setups.

2 Modern synchrophasor networks and their time synchronization

The *synchrophasor network* has to be able to securely and timely convey measurements, obtained by geographically distributed devices, to a concentration point that eventually performs the following functions: (i) monitor the state of the network under analysis; (ii) modify the state of the network by means of specific control and protection algorithms.

A synchrophasor network is a complex infrastructure and several aspects are crucial for a correct operation of such a system. All the components have to be designed and deployed in order to minimize the possibility of non-secure operation (e.g., data loss, unintentional bad data, malicious attack, etc.) that could compromise the accuracy of the data consumers (e.g., state estimator) and thus lead to non-optimal decisions.

The aims of this chapter are twofold:

- Present the components of a synchrophasor network, the associated time dissemination techniques and their performance;
- Introduce the specific technical nomenclature used in the rest of the dissertation.

2.1 Architectural layers and components

A synchrophasor network can be seen as a combination of layers with dedicated functionalities as shown in Fig. 2.1. The *grid and actuation layer* consists of the actual monitored network together with the actuation devices to be used in case of control / protection. In the *sensing layer*, voltage and current synchrophasors are measured. Accuracy in the synchrophasor phase estimation and possibility of time-stamping of the measurements are guaranteed by the *time dissemination layer*. A telecom network capable of exchanging data frames between the PMUs and the concentration point (or between intermediate concentration points) constitutes the *data communication*

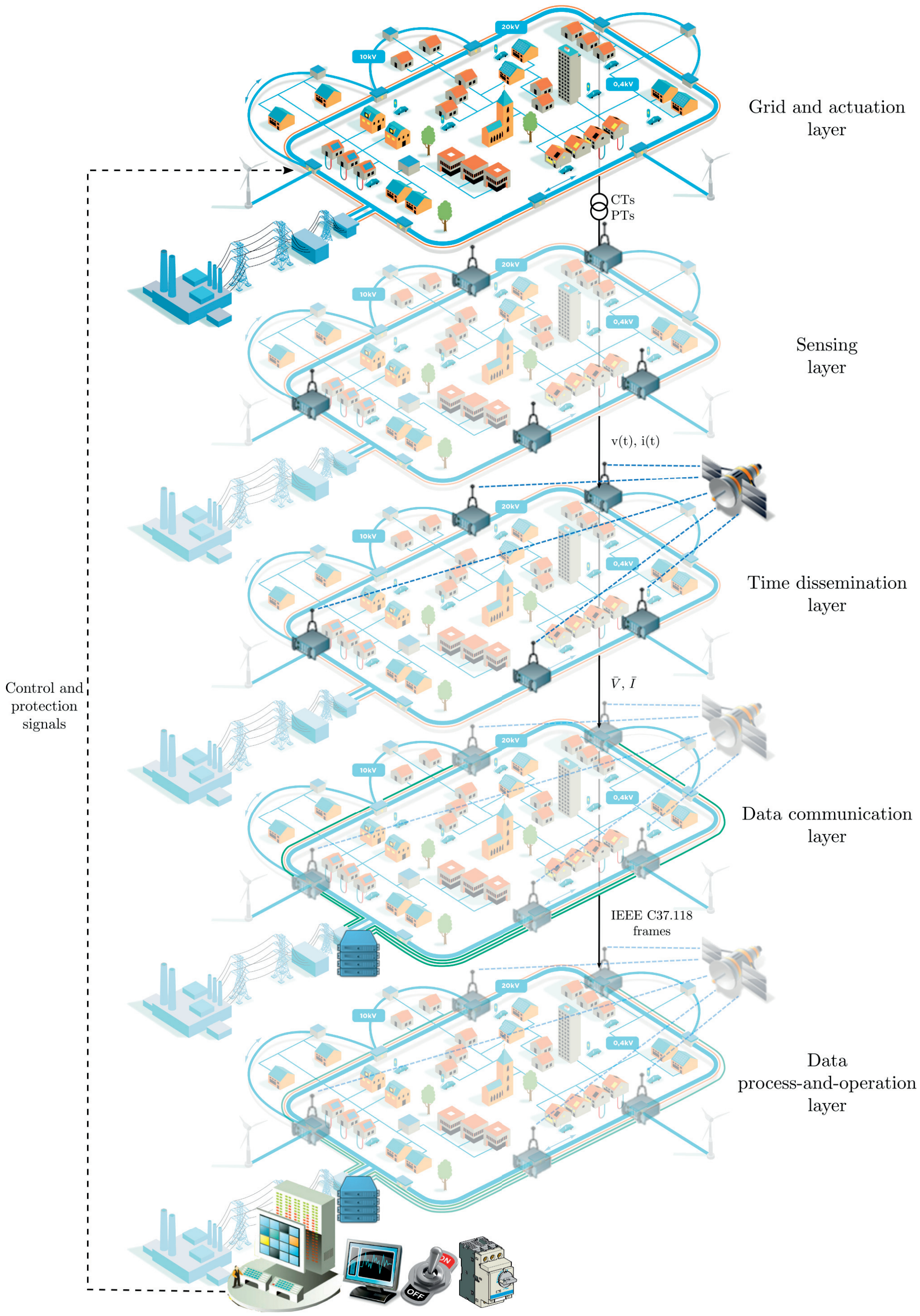


Figure 2.1 – Example of synchrophasor network architecture's layers.

layer. Finally, the *data process-and-operation* layer deals with the data decapsulation, time alignment, monitoring, control and protection applications[1] closing then the loop with the *grid and actuation layer*.

2.1.1 Sensing

The metering infrastructure is mainly composed of two elements: the sensor and the PMU. We refer to sensor as the transducer that scales down the power system voltage or current waveforms to levels appropriate for the PMU analog front-end. The instrument transformers can be classified as follows:

- Conventional current and voltage (potential) transformers
- Low-power (electronic) current and voltage transformers

The choice of a proper sensor is function of many factors (e.g., type of substation insulation, installation constraints, price, accuracy). Additionally, in the synchrophasor network deployment phase, one can often encounter existing sensors for which a replacement is not economically justified. To have an example of the accuracy of such devices, let us consider the case of common standard magnetic core current and voltage transformers (CTs and VTs) of class 0.5%. According to the standards [36] and [37], this sensor introduces, at full scale, a maximum ratio error of 0.5% and a maximum phase error of 6 mrad for VTs and 9 mrad for CTs. This level of uncertainty, in most of the cases, exceeds the one of the connected PMU and thus deteriorates the expected accuracy in the estimation of the magnitude and phase. In this dissertation, we consider the sensors as devices of known characteristics in order to model their contribution to the measurement noise[2] and keeping in mind that, being the first elements in the measurement chain, their accuracy can influence the WAMPAC operations.

The second element composing the metering infrastructure is the PMU. According to the IEEE Std. C37.118.1-2011 [38], a PMU is a device that provides an estimate of the synchrophasors, frequency and rate of change of frequency (ROCOF) of the acquired voltage and/or current waveforms, based on a common coordinated universal time (UTC) reference. The latency introduced by the PMU in order to provide synchrophasors, frequency and ROCOF estimations, is called *PMU measurement reporting latency*. It is defined in [38] as the time difference between the absolute time an event occurs in the power system and the absolute time the same event is reported by the PMU. This delay is mainly influenced by (i) the length of the acquisition window adopted by the

---

[1] We here focus on centralized control and protection applications. Local schemes do not operate on an architecture like the one presented in this chapter.

[2] The importance of the noise covariance matrix in state estimation is discussed in Section 3.1.2.

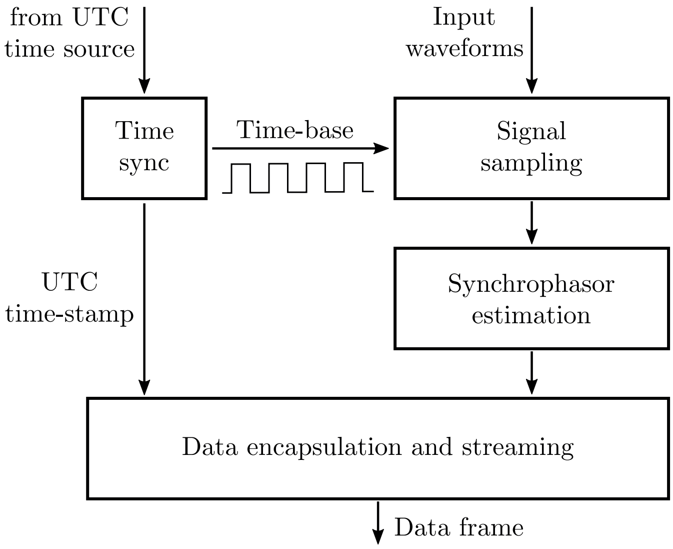


Figure 2.2 – Block scheme of a generic PMU. Adapted from [35].

specific algorithm and (ii) the time needed to estimate the synchrophasors. Therefore, in general, the PMU reporting latency can be reduced by shortening the acquisition window length of voltage and current signals and/or by adopting more performing hardware (for a given synchrophasor estimation algorithm).

UTC Synchronization of the PMUs

In the literature, several methods are proposed to estimate synchrophasors and the associated quantities (e.g., [35]). In this section, instead, we focus on the importance of the time reference for the PMU. Indeed, a *common* UTC time reference enables the comparison of phasor measurements obtained in different locations of the grid. In other words, the concept of *synchronized phasor* (i.e., synchrophasor) allows the definition of a common phase relationship between phasors from remote sites. Obviously, each PMU needs to be equipped with a time-synchronization module capable of receiving and decoding the UTC time (see Fig. 2.2). The UTC time is used to (i) time-stamp the estimated synchrophasor and (ii) discipline the sampling process of the input waveforms. In particular, the time-sync unit generates an internal clock locked to the external UTC time reference. This internal clock, also called “time-base”, may be used by the signal conditioning and A/D conversion unit to discipline the sampling process (i.e., coherent sampling) of the input waveforms. The synchrophasors are then transferred to the encapsulation and streaming processes.

Assume to use a PMU algorithm that estimates the synchrophasor on a set of M samples $\{x(n-M),\dots,x(n-1)\}$ acquired on a window of length T. Assume also that, as common in practice, the synchrophasor's time-stamp $t_s(n)$ is placed in the middle

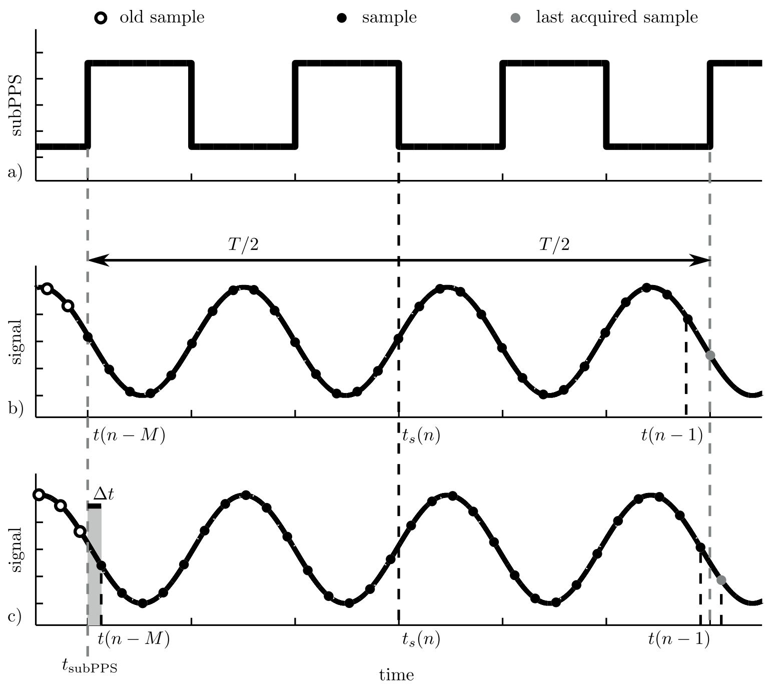


Figure 2.3 – UTC synchronized (b) vs. free running (c) sampling of a waveform. In (c) the delay Δt between the rising edge of the subPPS and the time the first sample of the window is acquired $t\,(n-M)$ is highlighted.

of the acquisition window[3].

A coherent sampling is more advisable because, by directly associating a time-stamp to each sample, the synchronization is automatically achieved. In this case, each sample corresponds to a time-stamp $\{t(n-M),\ldots,t(n-1)\}$ and the synchrophasor's time-stamp can be easily computed as:

$$t_s(n) = t(n-1) + T_s - T/2 \tag{2.1}$$

where T_s is the PMU sampling time (see Fig. 2.3b).

Although common in practice, it is not mandatory nor always feasible to lock the waveform sampling to the common UTC time reference. In this second case, a square waveform, hereafter called subPPS, is internally synthesized. It is aligned to the UTC-PPS (Pulse-Per-Second), shifted back of $T/2$ and characterized by a frequency equal to the PMU reporting rate as in Fig. 2.3a. The rising edge of the subPPS waveform triggers the sampling process. If the clock is free-running the sampling drifts over time and thus the first sample of the window is not aligned to the subPPS (see Fig. 2.3c). Two countermeasures have to be taken in order to correct such drift:

---

[3] The synchrophasor's time-stamp can also be placed in a different position, as specified in [38].

1. Compensate the time-stamp value t_s and the estimated phase by accounting the time difference between the subPPS rising edge and the first sample of the window. This contribution could have a large impact on the estimated phase angle. For example, if we assume a sampling frequency F_s = 50 kHz on a 50 Hz system, the uncertainty due to the position of the first sample with respect to the subPPS rising edge could account for up to 2πmrad in the phase estimation error. Such uncertainty can be removed by freezing the UTC time stamp of the first sample of each acquisition window and calculating its time delay with respect to the rising edge of the subPPS waveform.

   $$\Delta t = t(n-M) - t_{\text{subPPS}} \tag{2.2}$$

   where $t(n-M)$ and t_{subPPS} are the absolute time of the first sample of the window and the absolute time of the rising edge of the subPPS square waveform.

2. Measure and compensate for the actual window length (not exactly T as the sampling clock drifts). Indeed, the free running sampling clock is usually obtained with a quartz crystal oscillator that does not exactly run at the frequency specified by the data-sheet. The actual frequency is function of the manufacturing process, the surrounding temperature and other variable conditions. This small difference, if accumulated over time, largely affects the estimation of the synchrophasors. As an example, let consider the maximum drift declared by a typical quartz oscillator to be ± 50 ppm. For a 50 kHz sampling clock on a M = 3000 sample window (60 ms), this correspond to a misestimation of the length of the window of 3 µs. Because PMUs are equipped with accurate time reference units, the sampling clock drift can be measured in real-time over a long observation window (i.e. in the order of seconds) and compensated [39]:

   $$\varepsilon_{clock}(n) = \frac{t(n) - t(n-M)}{M \cdot t_s} - 1 \tag{2.3}$$

   where $t(n)$ and $t(n-M)$ are the absolute times corresponding to the samples at the end and the beginning of the observation window respectively and t_s is the nominal sampling time.

It is intuitive to understand that even by carefully compensating for such drift, the adopted time source and dissemination technology, affect the sampling process. In particular the alignment of the subPPS to the UTC-second rollover and thus the accuracy of the sampling time might be negatively impacted. This uncertainty can have non-negligible effects on the overall measurement accuracy, in particular on the estimation of the phase. For this reason, in Section 2.2 details about the accuracy, stability and time dissemination techniques available for synchrophasor networks are presented.

Table 2.1 – Comparison of bandwidth requirements for C37.118.2 and IEC 61850-90-5. Adapted from [18].

Reporting rate (Hz)	IEEE C37.118.2	IEC 61850-90-5
50	66400 bps	102800 bps

2.1.2 Data communication

The data communication for synchrophasor networks is an intermediate layer that has to allow a *secure* and *robust* connection in order to achieve a *low latency* exchange of messages between the PMUs and the data process-and-operation layer. The synchrophasor system communications includes data, commands and configuration information. Additionally, the communication layer might be used to disseminate the time (see Section 2.2.1).

Ideally, a traffic study should be conducted to evaluate communications requirements: the volume and path of data, the acceptable time delay and jitter, the error rate, the reliability of the paths and various other characteristics. From the collected information, an appropriate communication scheme can be selected (e.g., wired or wireless, public or private). Such studies are rarely performed on distribution systems because of cost and due to the still limited number of PMU-based applications available at the moment.

One of the most important parameters to consider when designing the communication infrastructure is the *end-to-end (ETE) time delay* also known as *communication network latency*. It is defined as the time difference between the instant the PMU transmits a data frame and the instant the same data frame reaches the network interface of the data process-and-operation layer (typically the concentration point). Together with the PMU measurement reporting latency, it defines the so-called *synchrophasor data latency*. Depending on the adopted ICT (e.g., 3G-4G networks), this contribution might introduce relatively high delays and non-deterministic latency variations.

The communication network protocols for synchrophasors data are essentially two. The IEEE Std C37.118.2-2011 [40] and the IEC/TR 61850-90-5 [41]. The IEEE Std C37.118.2-2011 is largely the most adopted communication standard in existing synchrophasor networks as reported in [3], due to the reduced message size if compared to IEC/TR 61850-90-5. In this respect, Table 2.1 compares the bandwidth requirements of IEEE C37.118.2 and IEC/TR 61850-90-5 when transmitting 8 synchrophasors (phase values and positive sequence), frequency, rate of change of frequency (ROCOF), 2 Analogs and a Digital word, with a reporting rate of 50 Hz.

Table 2.2 provides the average End-to-End (ETE) time delay of a IEEE C37.118.2 and

Table 2.2 – Average ETE time delay of IEEE C37.118.2 and IEC 61850-90-5 under different links for modified IEEE 30 bus system. Adapted from [42].

Type of link		Average ETE time delay (ms)			
		IEEE C37.118.2		IEC 61850-90-5	
		No backgr. traffic	With backgr. traffic	No backgr. traffic	With backgr. traffic
51.84 Mbps	PMU to PDC	8.6	13.0	15.2	22.2
	PDC to Central PDC	14.0	32.0	39.0	46.0
155.52 Mbps	PMU to PDC	2.1	3.0	6.3	8.3
	PDC to Central PDC	6.0	8.0	12.0	15.0
622.08 Mbps	PMU to PDC	2.0	2.2	4.5	5.1
	PDC to Central PDC	4.2	4.5	8.5	9.2

IEC 61850-90-5 based PMU communication under different links for a modified IEEE 30 bus system (see [42] for details). It is assumed that the test system is spread over an area of 1000 km by 1000 km and thus the communication delays play an important role. It is worth mentioning that each study available in the literature (e.g., [42, 43]) is based on assumptions about the measurements, the protocols, the data format, routing algorithm, data rate and communication infrastructure. In this context, the values provided in Table 2.2 give an insight on the order of magnitude of the expected delays. The ETE time delays for each specific synchrophasor network have to be obtained on a case to case basis.

Concerning the reliable and timely data exchange, the classic approaches to reliable communication through coding and retransmission (TCP/IP) are not compatible with the hard delay-constraints of some applications. For this reason, although supported by the standards, real-time applications typically use UDP. Additionally, TCP does not support IP multicast. Research is now focusing on increasing reliability through replication over multiple fail-independent paths [44].

In order to achieve cyber security of the ICT, there are a number of standards that help security practices, as summarized in [45]. In few words, they aim at improving (i) *availability* of the measurements by increasing the redundancy to prevent denial of service attacks, (ii) *integrity and authenticity* by means of digital signatures or various authentication codes and (iii) *confidentiality*, by preventing inadvertent disclosure of information.

Information-centric networking for power systems

Traditionally the information network infrastructure for power grids is based on a one-to-one client-server communication that, in some particular cases, could be one-to-many [46]. The client is the data producer (e.g., PMU) and the server is the data consumer (e.g. concentration point). Both end-points need to be aware of each other and this lead to complexity that could limit the normal operations of a synchrophasor network. In particular, by using a client-server communication:

- Each device needs to be configured with communication parameters (e.g., IP addresses, port number). Additionally, each server needs to be configured to accept traffic only from trusted clients.
- In case of unavailability of a server (e.g., maintenance), all its clients need to be re-configured in order to establish a communication with backup servers.
- Adding a new client forces to reconfigure the access control of the server in order to include the new device among the trusted clients.
- Anomalies (e.g., faults) in the power grid may trigger a change in the grid topology in order to restore the normal operation. In this case, a PMU device needs to direct its data flow to a different PDC and thus an individual re-configuration of each PMU device is needed.
- When different data receivers request different rates of the same data flow, the down-sampling is normally performed on the server side. This lead to waste in network resources.
- Exposing the IP addresses, in order to establish a client-server communication, makes the network vulnerable to denial-of-service (DoS) attacks.

Driven by these concerns, recent research projects have focused on the possibility of adopting information-centric networking (ICN) architectures that are by design more secure, resilient, scalable, and flexible than conventional information systems. The ICN has to support massive integration of renewables and a heterogeneous set of co-existing smart grid applications providing multiple benefits for utilities [47]. The ICN establishes a communication built on the information/data. Indeed, the information consumers (subscribers) are mainly interested in the information itself (i.e., *what* the message is) rather than the explicit location (i.e., *where* the message goes or comes from). Such an approach decouples in time and space the communicating devices as data producers and consumers are not aware to where and when the data will be consumed/produced by their counterparts. The ICN is based on the well known mechanism of publish/subscribe shown in Fig. 2.4. The core components are: (i) Publisher or data producer (e.g., PMU), (ii) Subscriber or data consumer (e.g.,

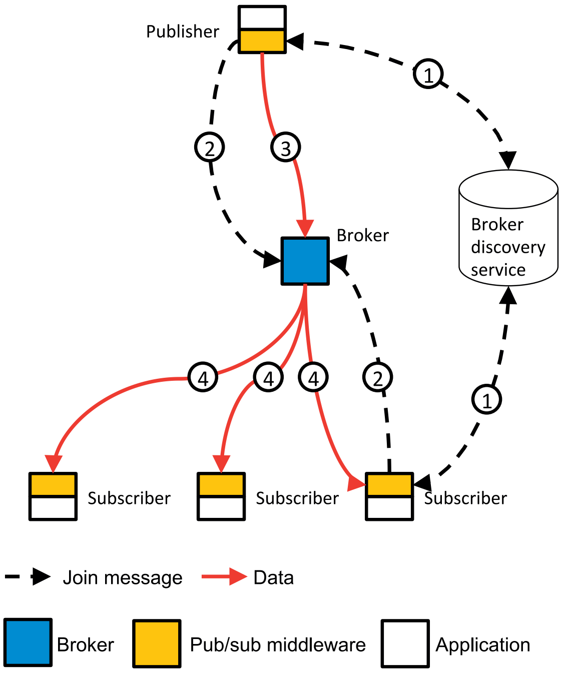


Figure 2.4 – Publish-subscribe mechanism. Adapted from [33].

data concentration, applications), (iii) Broker for storage and data forwarding and (iv) Broker discovery service to assign brokers to publishers and subscribers. The sequence of operation, according to the numbering in Fig. 2.4, is the following:

1. Publisher (subscriber) ask the broker discovery service what broker to use to publish (subscribe to) data of a certain topic;
2. Publisher (subscriber) requests to join the broker;
3. Publisher publish to broker;
4. Broker stores and forwards data to subscriber(s) with the pace required by the subscriber, if any.

An example of ICN based middleware platform with a topic-based publish-subscribe engine, was developed in the context of the EU FP7 project Cyber-secure DAta and control cloud for power grids (C-DAX) [33]. The project aimed at providing a cyber-secure distributed information infrastructure to the energy distribution networks. Validation in the field, showed the suitability of the platform for data communication in ADNs even when characterized by large penetration of PMU devices [48, 49]. The C-DAX architecture is shown in Fig. 2.5.

Fundamentally, C-DAX consists of a control and a data plane, with the former being responsible for handling topic-based communication sessions while the latter being

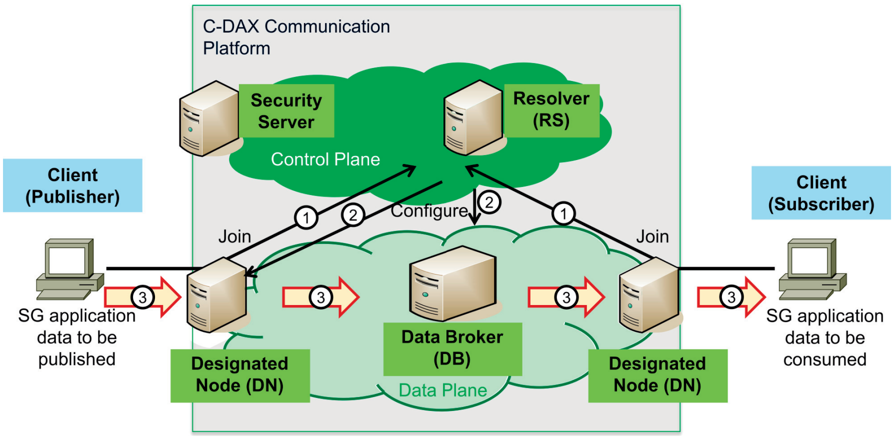


Figure 2.5 – The C-DAX architecture. Publishing steps include: (1) client join, (2) data plane configuration, and (3) topic data transmission. Adapted from [49].

dedicated to the forwarding of the PMU streaming data.

In the *data plane*, designated nodes (DNs) provide access for PMUs, as legitimate data publishers, to the C-DAX platform. They act as first point of contact and are responsible for forwarding topic data to and from the plane. A second entity in the data plane is the data broker (DB) that stores and forwards topic data to DNs. It acts acts as a rendezvous point connecting the publishers and the subscribers of a specific topic. Multiplicity of DBs under a common topic is allowed for scalability and resilience. Additionally, DBs can (i) configure PMUs, (ii) cache data for further usage, (iii) adapt the data rate towards subscribers with heterogeneous data rate requirements.

In the *control* plane, the topic resolver (RS) entity maps topic names to DBs so that join requests can be sent to appropriate DBs. Additionally, it answers topic-mapping requests of DNs. There may be several RSes for resiliency reasons. Security-related functionalities (e.g., DNs local authentication of publishers / subscribers) are enabled by the presence of a security server in the control plane that deals with functionalities like authentication, authorization, and key distribution.

To summarize, the ICN-based architecture benefits the synchrophasor network data communication layer by addressing the intrinsic issues in a client-server based communication, in particular:

- It simplifies the establishment and re-configuration of communication flows, limiting the error-prone manual settings and additionally taking care of setting up new devices interested in the published data.
- Facilitates traffic management decisions, selecting one or more DBs based on the underlying transmission capabilities, application requirements, network conditions, topology characteristics, and so on.

- Enables network management of smart grid data, including caching and processing such as rate adaptation, aggregation, filtering, and so on.
- Enhances resilience of information delivery to protect the grid against anomalies/power failures and subsequently minimize power distribution disruption.
- Enhances security by avoiding the exposure of critical components' network locations.

2.1.3 Data process-and-operation

Data concentration

In a synchrophasor network, the data concentration is typically performed by the so-called phasor data concentrator (PDC). The PDC collects data from several PMUs or PDCs at a lower hierarchical-level, gathers them by time-stamp and feeds out a single measurement set to further applications or to higher-level PDCs [46]. A design characteristic of any PDC is its ability to provide synchrophasor data fast enough to meet the destination's needs. For instance, low data latency is crucial for fast control applications because delayed data may be useless. Slower application (e.g., visualization) can tolerate higher data latency. Finally, applications like data logging can tolerate the highest latencies due to their intrinsic non-real-time nature. Extensive details about data concentrations together with a novel data-pushing logic for low-latency PDCs are given in Chapter 3.1.1.

Data elaboration

The data elaboration consists of all the applications relaying, totally or partially, on synchrophasor measurements. A non-comprehensive list of possible applications includes tuning of system parameters (e.g., protection relays), estimation of the nodal equivalent (e.g., loads) parameters, line/transformer congestion management, fault detection and fault location [1].

Table 2.3 summarizes some of the possible PMU wide area monitoring control and protection applications, providing an estimate for the reporting rate and latency requirements as reported in the literature. The values are obtained by means of (i) simulations focusing on the view point of the application [43] (i.e., what is needed by the application to successfully operate), (ii) surveys aimed at collecting the expectation of the network operators about WAMPAC applications [50] and (iii) literature's review [42, 51]. Due to the heterogeneity of the sources, the values provided in Table 2.3 are intended to provide an overview only on the latency requirements for WAMPAC applications.

Table 2.3 – Estimated latency for different PMU wide area monitoring, control and protection applications.

Application	Reporting rate [Hz]	Latency	Reference
Out of step protection	> 10	50 ms	[42, 51]
Adaptive relaying	> 10	50 ms	[42, 51]
Synchrocheck	> 4	100 ms	[42]
PMU-only state estimation	> 10	100 ms	[51]
Oscillation detection	> 10	200 ms - 1 s	[43, 50, 51]
Frequency instability	>1	250 ms - 5 s	[50]
Conventional state estimation	< 1	1 s - 5 s	[42, 43]
Voltage instability	> 1	1 s - 30 s	[43, 50]
Situational awareness	>1	5 s	[42]
Line temperature monitoring	< 1	1 s - 10 min	[50]

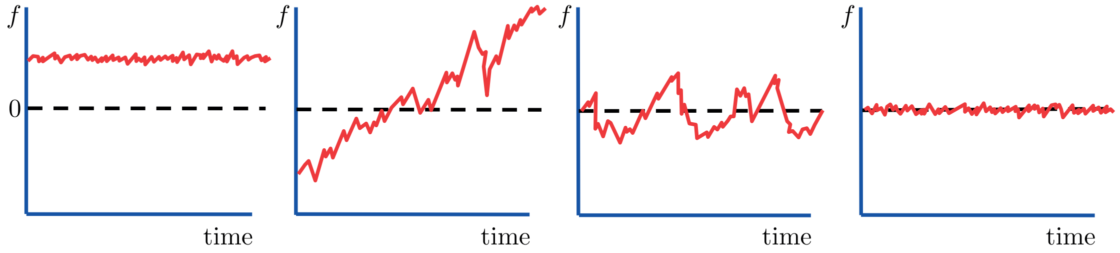
Depending on the chosen application, the latency requirements can vary between tens of milliseconds for the so-called *hard real-time* applications, (e.g., fault management) to few tens of seconds, i.e., *soft real-time* applications (e.g., voltage control [52]) up to minutes for applications like line temperature monitoring[4]. Extensive details about data elaboration functions and applications are given in Chapter 3. A real-time state estimation functionality is presented. Additionally, two state-estimation-based applications characterized by different time constraints (i.e., hard and soft real-time) are described.

2.2 Time synchronization

Synchrophasor measurements have the peculiarity of being UTC time-stamped and thus synchronization to an UTC time-reference is needed. As previously shown, a common UTC time-reference among different devices allows a meaningful estimation and comparison of the phase of the main fundamental frequency component of the acquired signals. Other components of the synchrophasor network may also exploit the possibility of an UTC synchronization. For instance, an UTC synchronized PDC enables the operator to (i) obtain the UTC arrival time of the incoming synchrophasors thus detecting bottlenecks in the communication layer, if any; (ii) detect and discard measurements with an erroneous time-stamp (e.g., measurement coming from the future). In what follows, we elaborate on time-referencing technologies and we provide an overview on possible time dissemination techniques for synchrophasor networks.

---

[4] The terms *hard* and *soft real-time* are used in this manuscript to indicate the type of latency constraint that the specific application has to meet.



Stable but not accurate

Not stable and not accurate

Not stable but accurate (bounded uncertainty so finite accuracy)

Stable and accurate

Figure 2.6 – Stability and accuracy concepts.

2.2.1 Time-reference and its dissemination

A time-reference is an oscillator with a known initial time t_0 [53]. Its task is to produce a periodic oscillating signal that, ideally, should not be affected by aging, temperature, shocks, or other external conditions. The quality of an oscillator is often expressed by using the terms *accuracy* and *stability* (see Fig. 2.6). *Accuracy* is the degree of conformity of a measured or calculated value to its definition [53]. In other words, accuracy indicates the closeness of agreement between a measured value and the true value of the measurand. For example, the accuracy of an oscillator embedded in a PMU can be defined by the difference between a measured on-time pulse and an ideal on-time pulse that coincides exactly to UTC. Accuracy defines how well an oscillator has been set on time or on frequency. On the other hand, *stability* indicates how well an oscillator can produce the same time or frequency offset over a given time window. To be noted that stability does not indicate whether the time or frequency is “right” or “wrong” but only whether it changed over the observation interval.

Referring once again to the oscillator embedded in a PMU, it is worth to note that whereas the accuracy can be compensated by initial calibrator of the oscillator and regular adjustments of its unavoidable drift, the stability identifies the reproducibility of the PMU estimates and thus it is inherently related to the PMU’s quality. As a consequence, stability can be considered to be the most important parameter to be used when selecting a PMU time-reference oscillator.

Although each PMU embeds an oscillator, the synchronization of the components of a synchrophasor network is usually achieved by using external time-sources for the following reasons:

- An oscillator does not intrinsically have the *absolute time information*, this needs to come from an external UTC-synchronized source;
- An embedded oscillator, independently of its quality, needs an adjustment of its

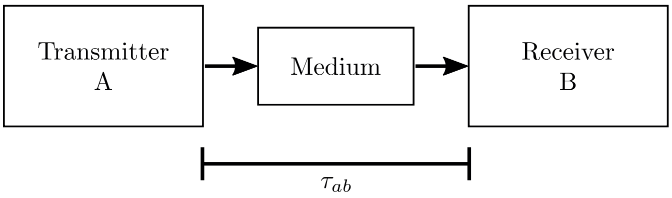


Figure 2.7 – Unidirectional time transfer. τ_{ab} is the time delay.

drift due to its finite stability. This is typically done with external and more stable time-references;

- A single external unit can synchronize multiple instruments without the need of replicating the time source.

As seen, synchrophasor network components require clocks or oscillators at different locations to be set to the same time. Time dissemination technologies can use signals broadcast through many different media, including coaxial cables, optical fiber, radio signal, telephone lines and the internet. The synchronization is achieved by sharing a on-time pulse and a time code. In general, the information sent from a transmitter reaches a receiver after a time τ_{ab} called *path delay*. There are two ways to compensate for such a delay: (i) the transmitter estimates τ_{ab} and sends the time out early by this amount or (ii) τ_{ab} is computed and applied on the receiver side. The correction factor can be computed if the position of the transmitter and the receiver, together with the medium type are known. When the transmitter is moving (a satellite, for example) it must broadcast its position in addition to broadcasting the time.

As reported in [45], the criteria to select the proper time dissemination technology are the following:

- *Accuracy*: degree of conformance between measured synchronization signal and its true value.
- *Availability*: capability of the synchronization system to provide usable timing services within the specified coverage area.
- *Continuity*: probability that the synchronization system will be available for the duration of a phase operation, presuming that the system was available at the beginning of that phase of operation.
- *Reliability*: probability that a synchronization system will perform its function within defined performance limits for a specified period of time under given operating conditions.
- *Integrity*: ability of the synchronization system to detect the timing signals' degradation and provide timely warnings to users.

- *Coverage*: geographical area in which the application-specific synchronization system requirements for accuracy, availability, continuity, reliability, integrity and coverage parameters are satisfied at the same time.

How to disseminate the time information is the focus of the next subsection. Satellite- and terrestrial-based technologies are presented together with advantages and disadvantages when employed in synchrophasor networks. Among all the time dissemination techniques available nowadays, only the ones that meet the accuracy required by synchrophasor networks are presented.

2.2.2 Satellite-based time dissemination

In power systems, it is common practice to adopt the time derived from a global navigation satellite system (GNSS) as UTC time reference. The best known among the GNSSs is the Global Positioning System (GPS), an U.S. Department of Defense satellite-based radio navigation system. Other GNSSs are the Russian GLONASS, the Chinese BeiDou and the European Galileo[5].

The satellites are typically located in the so-called medium earth orbit and have an approximate period of 12 hours. They are equipped with atomic clocks to derive the time information from a ground-based UTC referenced primary clock. The dissemination is done using carrier signals over dedicated frequency channels. The mechanism through which the GPS, and in general all the GNSSs, are able to disseminate the time is largely discussed in the literature and thus will not be treated in details in this section. What is only marginally given in the literature, instead, is a list of advantages and disadvantages that such a technology presents when adopted in power systems, in particular for synchrophasor networks.

Advantages: A cheap GPS receiver (few dollars) can infer the UTC time with an uncertainty of 100 ns (3σ) and a position uncertainty of <10 m [53]. The success of the GPS for time and frequency transfer is due to its reliability and exceptional results with minimal effort. A GNSS receiver synchronizes its on-time pulse to the received signals and it is then able to produce time-of-day and date information. In terms of hardware to be installed in the substation, the GNSS requires an antenna and the proper cabling to reach the GNSS receiver.

Disadvantages: Relying on wireless information transfer, the received GNSS signal is characterized by weak power level, therefore GNSSs are vulnerable to radio-frequency interference (RFI). Disruption mechanisms that could limit the GNSSs performance can be classified as unintentional or intentional interference.

---

[5] BeiDou and Galileo are not fully operational at the time of writing.

- Unintentional interference: examples are RFI caused by electronic equipment radiating in the GNSS band (above 1 GHz) or restricted line of sight to satellites in all the cases where there is not a clear view of the sky (e.g., in urban areas or near foliage).
- Intentional interference: in this case, the GNSS signals are deliberately jammed by radio interference. The levels of interference needed to jam a typical GNSS receiver are quite low, thus jamming equipment can be small.
- The GPS included the so-called selective availability that allowed the U.S. department of defense to intentionally add time varying errors to the signal, thus inserting a non-controllable delay in the accuracy of the synchronized device. This possibility lead to the development of an alternative common European system (i.e., Galileo Navigation Satellite System).

In what follows, we present some of the reliability issues characteristics of GNSSs that could undermine their usage in synchrophasor networks.

Spoofing of GNSS

Spoofing of a GNSS consists in broadcasting false signals with the aim that the victim receiver will misinterpret them as authentic. The victim might deduce a false position fix, a false clock offset, or both. At the time of writing, spoofing has been used to send a hovering drone in an unplanned dive and to steer a yacht off course (in controlled experiments). Other claims of GNSS spoofing have been reported, although none of them directly affected power system equipment yet. According to the literature (e.g., [54]), off-the-shelf receivers have only rudimentary defense against spoofing and this defense mechanism is easily deceived. A possible sequence of attack is shown in Fig. 2.8. The spoofer exploits the knowledge of the true GNSS signal and its location relative to the victim. It aligns its spoofed signal with the true signal (1). The attack starts at low power and ramps its power until it captures the receiver's tracking loops (2-3). Afterwards, it smoothly drags the victim off to a false position/timing fix (4-5).

For power systems and especially for synchrophasor networks, several publications have dealt with the issue of GNSS spoofing (e.g., [55, 56, 57]). Chapter 4.2 focuses on the detectability of timing attacks on linear state-estimators. It shows that it is possible to forge delay attacks that are undetectable by using classic bad-data detection techniques and, at the same time, have large impact on the state estimation results.

Leap second

Although the terrestrial time is based upon the earth's rate of rotation, the latter slowly changes over time. A one-second adjustment (i.e., leap second) to the UTC time is

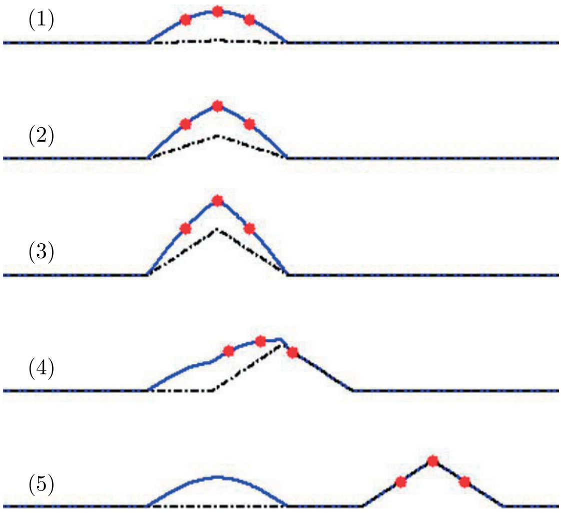


Figure 2.8 – Spoofing attack sequence viewed from a victim receiver channel. Spoofer: black dash-dotted curve; sum of spoofer and truth: blue solid curve; receiver tracking points: red dots. Adapted from [54].

Table 2.4 – Leap second insertion occurred on December 31st 2016.

Date	Time	Comment
2016 December 31	23h 59m 59s	
2016 December 31	23h 59m 60s	extra leap second
2017 January 1	00h 00m 00s	

thus needed to ensure that precise scientific time remains in synch with observed astrological time [58]. The UTC time is usually adjusted on June 30 or December 31 and the leap seconds events are announced about 6 months before the event occurs.

Incorrect GPS or PMU handling of leap seconds, poor interoperability between clocks and PMUs have caused several issues in the past leap second events, as reported in [58].

- Duplicated or missed measurements;
- Erroneous interpretation of PMU data;
- PMU or clock failures from second to hours;
- PMU measurements dropped at the concentration point.

If PMU data are used for missing-critical operations, such failures could cause problems as simple as lessened system visibility or as significant as undesirable actions such as triggering system protection schemes or wide area control schemes that could compromise grid reliability [58].

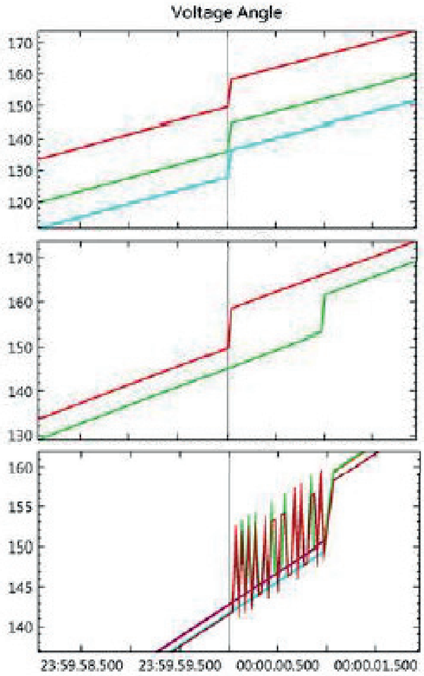


Figure 2.9 – Example of voltage angle misestimation due to incorrect handling of leap second for different PMUs. Adapted from [58].

GPS glitch

On January 26th 2016, some GPS receivers suddenly began to output erroneous time signals at different time. The disruption lasted for approximately 12 hours and was later acknowledged to be due to an erroneous time correction parameter upload to GPS satellites. The receivers have been affected by an abrupt 13 µs time jump in their PPS time synchronization output, as it can be seen in Fig. 2.10. Indeed, a certain number of GPS satellites, while declaring themselves "healthy", broadcast a wrong UTC correction parameter. A 13 µs time error corresponds to approximately 4 mrad misestimation of the phase angle for a 50 Hz system. The error affected a large number of PMU devices and these multiple coherent erroneous measurements are difficult to detect and eliminate with state-of-the-art bad data methods (see Chapter 4.1 for details), therefore synchrophasor network applications are negatively impacted from such events.

Countermeasures

Possible countermeasures proposed in the literature to cope with the aforementioned issues when using GNSS as time synchronization are constituted of, but not limited to:

- Redundancy of the timing signal and local oscillators to increase reliability and

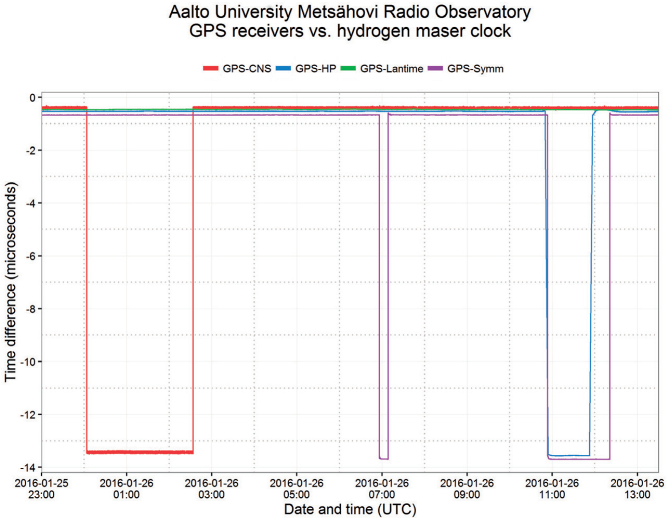


Figure 2.10 – Time difference between Metsähovi H maser and four different GPS receivers, for the duration of the disruption. Adapted from [59].

accuracy [45, 54];

- Protection of the GNSS receiver from RFI, to reduce the possibility of intentional or unintentional interference [45, 54];
- Adoption of International Atomic Time (TAI) time (i.e., a time scale continuously and monotonically incremented, never discontinued) instead of UTC for power systems as proposed by the Swiss National Committee;
- Definition of timing event performance tests and of a single correct method for handling the leap second [58].

2.2.3 Terrestrial-based time dissemination

The above mentioned reliability issues of GNSS led to the IEEE recommendation to pursue an alternative method of synchronization using terrestrial system as stated in [4, 45]. Few of the available terrestrial-based time dissemination technologies guarantee the accuracy level required by synchrophasor networks. Recently, Packet-Based Time-Synchronization Protocols (PBTSPs) like the precision time protocol version 2 (PTPv2) [60] raised the interest of some PMU developers due to the increased accuracy with respect to its predecessors. Still, the higher cost of such a time dissemination infrastructure (the network needs to be deployed if not in place) does not yet attract many PMU developers. The PTPv3 (also known as White rabbit [61]) is expected to largely increase the synchronization accuracy (i.e., in the order of sub-nanoseconds) and thus make terrestrial-based time dissemination appealing also for synchrophasor networks.

PPS

A simple way to synchronize two clocks is to use a train of positive pulses at a rate of one pulse per second (1 PPS). The rising edge of the pulses coincides with the seconds change in the clock and provides a very precise time reference (better than 100 ns). Because the PPS signal does not provide any indication of the date or time of day, it has been largely replaced by the IRIG-B.

IRIG-B

According to a 2014 survey on synchrophasor system networks [3], the IRIG-B [62] is the second most spread technology to synchronize synchrophasor networks after GPS. The unmodulated IRIG-B code can deliver accuracy limited only by the slew rate of the digital signal, usually better than 1 µs and, with care, even 100 ns. The IRIG-B includes control bits that enable its support for real-time applications thanks to the inclusion of leap second, daylight savings or summer time status, year of the century and time quality. These assignments extend IRIG-B to a complete time message as needed by the PMUs. The IRIG-B suffers from a limitation: the time dissemination is performed either with twisted pair wires or coaxial cables. This means that data exchange and time synchronization are over two different infrastructures. This limitation is overcome by the precision time protocol.

Precision time protocol

IEEE Std 1588-2008 [60] allows sub-microsecond time accuracy for devices connected via a network such as Ethernet. IEEE Std C37.238-2011 [63] specifies a subset of IEEE 1588 functionality to be supported for power system protection, control, automation and data communication applications using an Ethernet communication architecture.

The IEEE Std 1588 specifies a way to evaluate the link delay between two nodes (master and slave) through the exchange of time-tagged messages, see Fig. 2.11. The master node sends a Sync message to the slave and stamps it with a time-stamp t_1 as it leaves its networking interface. The message is received at time t_2 in the slave's time base. The process is then reversed, with a message Delay_Req sent from the slave at time t_3 and received in the master at time t_4. The Follow_Up and Delay_Response messages are used to transport the timestamps recorded at the master clock to the slave clock, so that the slave has the information needed to adjust its time. Indeed, assuming the one-way delay through the network is exactly half of the two-way delay, the offset of the slave's clock with respect to the master is:

$$\delta = \frac{(t_2 + t_3 - t_1 - t_4)}{2} \tag{2.4}$$

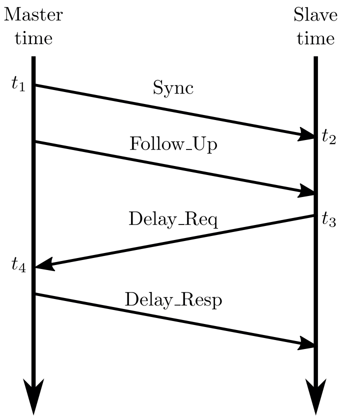


Figure 2.11 – Simplified PTP message exchange diagram.

Following the same principles, the grandmaster clock at the top of the time distribution chain, synchronizes the clocks in the entire system to UTC. Each device in the time distribution chain (including Ethernet switches) is required to support IEEE C37.238-2011 to achieve 1 µs time accuracy. Ethernet switches supporting IEEE C37.238-2011 should perform measurements and corrections for cable delay and queuing time. IEEE C37.238 offers the use of the same communication infrastructure (Ethernet) for PMU/PDC data and time distribution, and reduced use of GPS connectivity whenever possible.

Advantages: The adoption of the IEEE Std 1588-2008 in power system enables:

- The automatic time compensation for the dynamic changes of path (dynamic delays);
- The automatic choice of the grandmaster clock thanks to the Best Master clock algorithm. Additionally, the protocol selects the backup clocks in case of failure of the grandmaster;
- The usage of existing network cabling;
- Additionally, all protocol adaptations relevant for the electric power industry are taken care of in the so-called Power Profile IEEE C37.238-2011 [63].

Disadvantages:

- Special network switches (i.e., transparent clocks) are needed to achieve the sub-microsecond accuracy;
- Need to compensate for the time delay between the GPS antenna and the master clock (if grandmaster is not integrated in the antenna).

- Time-stamping by means of dedicated hardware. A software-only time-stamping allows an overall accuracy in the range of 20 to 100 μs.

White Rabbit

The White Rabbit (WR) project was initiated at CERN in 2008. The idea is to deliver the following functionality while using (or improving) existing standards. As reported in [64], the functionality are:

- Sub-nanosecond accuracy in synchronization and stability better than 50 ps;
- Coverage over distances of 10 km (proven nowadays to be able to cover more than 100 km);
- Ability to serve more than 1000 nodes;
- Guaranteed upper bound in the overall latency;
- Open hardware, firmware and software [61].

To achieve sub-ns accuracy, in addition to an improved version of the PTPv2 protocol, the WR operates the so-called Layer-1 syntonization. Indeed, typical PTP implementations use free-running oscillators in each node. This means that the time base of each node drifts during the time interval between two calculations of δ in Equation (2.4). The Layer-1 syntonization ensures equal clock frequencies in all nodes, therefore eliminating this drift. Because all the system clocks oscillate at the same rate, it is possible to compensate for the phase shift between two clock signals. This is achieved by means of a phase-shifting circuit in the slave that creates a phase-compensated clock signal despite the delay introduced by the fiber link.

Disadvantages:

- Requires optic links and dedicated switches;
- Not standardized (although in the process of standardization).

In terms of performance, WR has been proven to be able to reach synchronization accuracy in the order of 200 ps with standard deviation of approximately 6 ps for 15 km links (e.g., [64]). A large number of applications is currently taking advantage of the WR performance. Recent literature has considered WR as the future synchronization method for PMU-based power systems (e.g., [65, 66]).

Table 2.5 – Summary of the accuracy of time dissemination technologies for synchrophasor networks.

Technology	Typical accuracy
GNSS	100 ns
1PPS	100 ns
IRIG-B (unmodulated)	$\sim$ 1 µs
PTPv2 (HW)	< 1 µs
White Rabbit	< 0.5 ns

3 Time critical functions and applications

This chapter presents functions and applications that we envisioned as time critical for a successful operation of a synchrophasor network. The chapter starts by describing two functions that enable the network operator to (i) collect meaningful data from its geographically distributed measurement devices and (ii) obtain a reliable estimate of the state of its network. Since several applications can exploit the availability of PMU data, the second half of the chapter presents two state-estimation-based applications with different time constraints. First, a *hard real-time* application is described. It leverages on the state estimation results to provide protection functions to the monitored network, in time-scales of hundreds of milliseconds. As a second example, a *soft real-time* application is described. It is conceived to be able to control the state of the system in time-scales of seconds in order to maintain its voltage level within predefined limits.

Original contributions of this chapter:

- Definition of a data-pushing logic for synchrophasor data concentration;
- Definition of a protection mechanism relying on PMU-based state estimation processes.

3.1 Situation awareness functions

3.1.1 Phasor data concentrator

The content of this section is based on [67]. The Phasor Data Concentrator (PDC) is defined by the IEEE Std C37.244-2013 [46] as a key component of the synchrophasor network collecting data from several PMUs or PDCs at a lower hierarchical-level, gathering them by time-stamp and feeding out a single measurement set to further applications or to higher-level PDCs. Depending on the requirements of the application being served by the PDC and the layout of the synchrophasor network, the PDC provides additional features like (but not limited to) data quality checking, data conversion to different formats, etc.

The most relevant functionalities of a PDC, identified by the IEEE Std C37.244-2013 [46], are *data aggregation* and *data pushing*. Data aggregation enables to concentrate data coming from multiple PMUs into a single, usually time-aligned[1], dataset. This functionality mitigates the latency variations introduced by the components of the synchrophasor network as data frames coming from different PMUs and characterized by the same time-stamp, never reach the PDC simultaneously. The data pushing, forwards the dataset to subsequent applications. It is triggered by the so-called *PDC wait time* that represents the amount of time the PDC has to wait for data frames with a given time-stamp. Reference [46] defines two logics for setting the PDC wait time: an *absolute* time logic, where the data pushing is performed once a specific UTC time is reached, and a *relative* time logic, in which the PDC waits for a specified relative time triggered by an event, which may be the arrival of the first data with a specific time-stamp.

Acting as a bridge between measurements and applications, the PDC has to be properly designed in order to reliably operate without introducing unnecessary delays or data loss. Nevertheless, few contributions have dealt with the design, implementation and testing of PDC architectures to meet the requirements dictated by the applications in term of speed and reliability. Reference [68] and [69] highlight the inconsistencies that might arise from an inaccurate PDC implementation and how they could affect wide area operations. In reference [70] and [71] the functional and communication requirements of a generic PDC are shown together with proposed test methodologies to validate the PDC core features. A possible design for a PDC that integrates synchrophasor data logging and a graphical user interface is given in [72]. Other works focus on maximizing the throughput of synchrophasors in order to use the PDC for specific applications (e.g., wide-area damping control [73, 74, 75]). How different settings for the relative wait time affect the incompleteness and timeliness of the outgoing dataset in a WAMS, is shown in [76].

However, the above-listed literature does not explore the possibility of having different data pushing logics than the ones defined in [46]. Moreover, the results available in the literature that aim at assessing the PDC's performance are all obtained in simulated environments. On the contrary, the performance of the method here proposed is assessed in real field installations, as shown in Chapter 5.

---

[1] The time-alignment is not mandatory, but it is usually present to leverage the PMU time-stamped measurements.

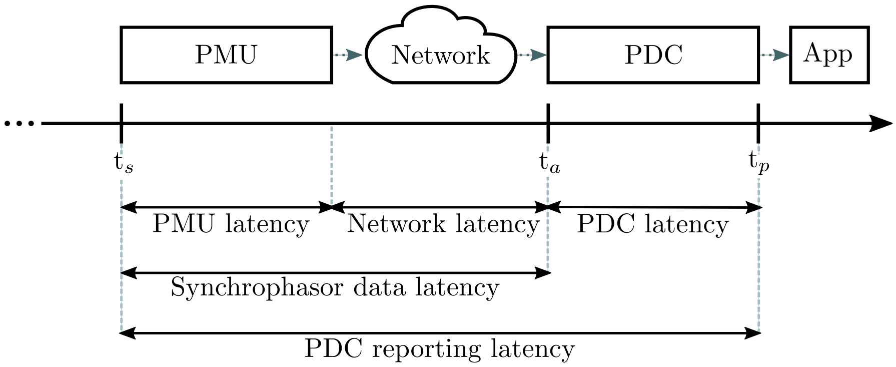


Figure 3.1 – The PDC reporting latency decomposed in its individual contributions. The synchrophasor time-stamp t_s, the data frame arrival time t_a and the time-aligned dataset push time t_p are highlighted.

PDC Reporting Latency Analysis

The PDC reporting latency is defined as the difference in time between the moment a set of synchrophasors characterized by a specific time-stamp is pushed towards the subsequent application and the time-stamp itself. As mentioned in Chapter 2, this parameter can vary between milliseconds to tens of seconds (hard real-time, soft real-time, respectively) depending on the targeted applications (e.g., protection, voltage regulation, etc.)

The PDC reporting latency is a result of several contributions shown in Fig. 3.1.

- The *PMU measurement reporting latency* is defined in [38] as the time delay between the instant a specific event occurs in the power system and the instant the same event is reported by the PMU.
- The *communication network latency* corresponds to the time difference between the instant a data frame leaves the PMU and the moment it reaches the PDC. Based on the type of communication technology adopted (i.e., wired, wireless) this layer may introduce high delays and non-deterministic latency variation in the overall PDC reporting latency.
- The *PDC latency* is defined as the time difference between the instant a dataset with a certain time-stamp is pushed to the desired applications and the instant the first message with the same time-stamp reaches the PDC. The PDC latency itself is the sum of two contributions:
  - *PDC wait time:* accounts for the time between the moment the first synchrophasor with a certain time-stamp reaches the PDC and the instant the last measurement arrives or the timeout expires;

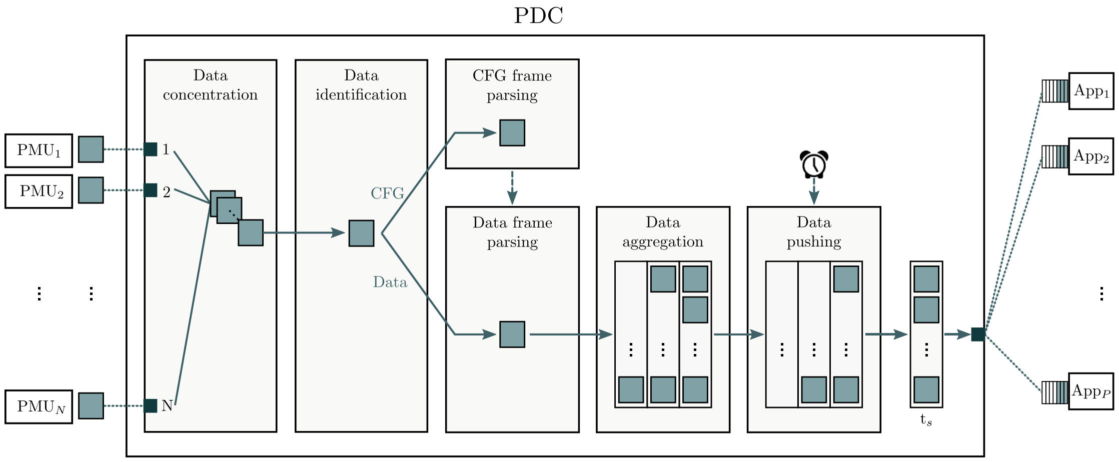


Figure 3.2 – Architecture of the proposed PDC collecting data frames from N PMUs and pushing time-aligned datasets to P applications. Adapted from [67].

  - *PDC processing time:* accounts for the time needed by the PDC to produce an aggregated dataset from the single measurements and push it to the application.

To be noted that the former contribution outweighs by far the latter.

References [45] and [46] do not explicitly state the maximum or minimum values for the latency contribution defined above. Their value should be coherent with the requirements set by the targeted application.

What follows focuses mainly on the aspects affecting the PDC latency. A data-pushing logic that allows to reduce the contribution of the PDC to the total latency of the synchrophasor network is given. Indeed, additional work can focus on the reduction of the contributions of PMU and communication layer, but these are not a direct subject of this work. See [77] for details on how to reduce the PMU contribution to the synchrophasor latency. Reference [78] suggests a proper engineering of the real-time traffic in order to reduce the communication network latency.

Proposed PDC Architecture

The time-alignment functionality is not mandatory, but it is usually present to leverage the PMU time-stamped measurements. On the other hand, it is possible to imagine applications able to sequentially process measurements characterized by a specific time-stamp (e.g., sequential discrete kalman filter). In this case, one could envision an architecture where the PDC is not present, and the application itself, the applications

The architecture of the proposed PDC is shown in Fig. 3.2. It is developed to meet the requirements dictated by [46] and it implements a large number of the optional and

Table 3.1 – List of functionalities implemented in the proposed PDC.

Functionality
Data aggregation
Data pushing (3 logics)
Selective data forwarding
Data communication - TCP/IP or UDP (multicast)
Data validation
IEEE Std C37.118.2-2011 support
Data format and coordinate conversion
Data latency calculation
Reporting rate down-conversion
Configuration management
Data logging

mandatory functionalities there described. A list of the functionalities implemented is given in Table 3.1. However, in what follows, we focus only on the functionalities that affect the PDC latency and the completeness of the pushed dataset.

For each PMU, the PDC opens a TCP/IP or UDP socket. It continuously listen to incoming PMU frames. When a new packet is received, the data validation process discards invalid frames. The frames are then categorized in configuration frames or dataframes and they are treated differently according to their type. Configuration frames are needed to parse the dataframes and are typically streamed once per minute or upon request. Once a configuration frame is received from a specific PMU, the subsequent dataframes coming from that PMU are parsed. The PDC time alignes the data and pushes the aggregated dataset to the subsequent applications. Time-aligned data aggregation and pushing operations are based on a circular fixed-size data buffer, shown in Fig. 3.3. The buffer can be seen as a 2D array, with N columns representing the N PMUs and M rows, indicating the buffer-depth. Each row corresponds to a stored time-stamp. The buffer depth and the PMU reporting rate allow to compute the so-called buffer history length T_h.

$$T_h = M/F_r = M \cdot T_r \tag{3.1}$$

where $F_r = 1/T_r$ is the PMU reporting rate and T_r the PMU reporting interval. A pointer p indicates the next line to be pushed to the applications and it is always in the smallest time-stamp t_{min}. The time-stamps are monotonically increasing within the circular buffer starting from the pointed line, therefore the largest time-stamp $t_{max} = t_{min} + T_h$ lies always in the previous line position (modulo the buffer depth M). New data overwrite the old one thus avoiding to rotate the buffer's elements when data are released. This structure is suitable for data buffering purpose because it allocates a

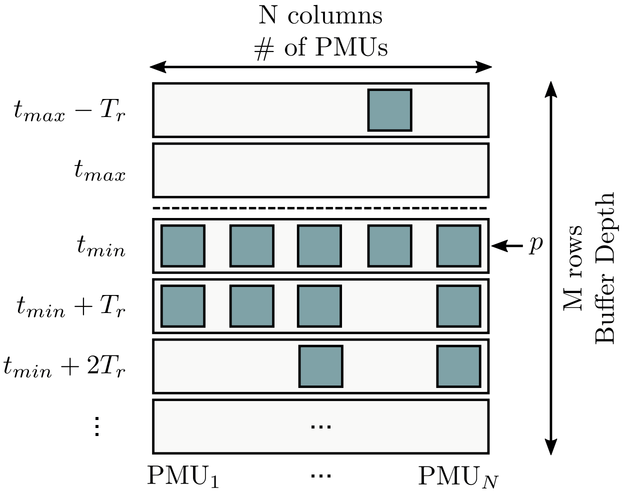


Figure 3.3 – Layout of the circular buffer used to aggregate and time-align the incoming data flows generated by N PMUs. It can store up to M time-aligned datasets characterized by time-stamps in the range $t_{min} < t_s < t_{max}$. A pointer p points to the next line to be pushed to the supplied applications.

fixed amount of memory when created and it does not lead to memory leaks.

Data Aggregation logic

The data aggregation is performed with time-alignment. Before inserting the data frame in a specific buffer position, the buffer is updated depending on the received time-stamp t_s. If $t_s < t_{min}$, the data frame is discarded. If $t_{min} \leq t_s \leq t_{max}$ the buffer time-stamps are not updated. If $t_s > t_{max}$, the oldest lines are fed to the applications and then replaced by the new ones. In this case, a set of $((t_s - t_{max})/T_r) \in \mathbb{N}$ empty lines, characterized by newer time-stamps up to t_s, overwrites the older ones[2]. This data aggregation logic is completely independent of the adopted data-pushing logic.

Absolute and Relative Time Data-Pushing logics

The implementation of the absolute and relative time data-pushing logics in the developed PDC is described in what follows. For the sake of comprehension, let us consider the aggregation and data-pushing processes of data frames characterized by time-stamp t_s coming from N PMUs as shown in Fig. 3.4. Let us define with $t_{a,i}$ and $t_{a,j}$ the arrival time at the PDC of the first and last data frames characterized by the time-stamp t_s and sent by the i-th and j-th PMUs, respectively.

---

[2] If a data-frame characterized by a time-stamp greater than the actual UTC time is received (i.e., a time-stamp coming from the future), the data frame is discarded. This plausibility check is possible only by synchronizing the PDC to an absolute time reference.

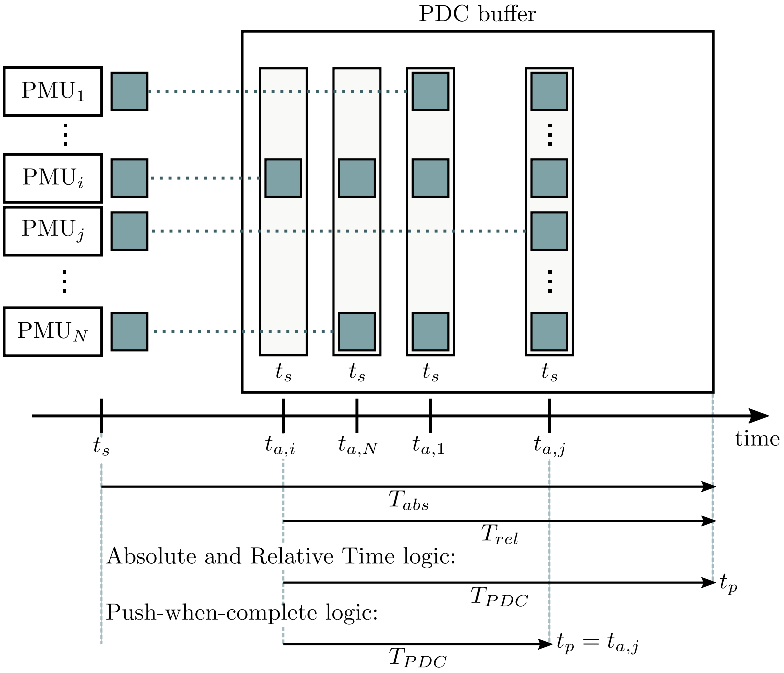


Figure 3.4 – Comparison between the various data pushing logics in the case of a PDC gathering dataframes from N PMUs characterized by time-stamp t_s. The arrival times of the first and the last data frame characterized by the time-stamp t_s are indicated by $t_{a,i}$ and $t_{a,j}$, respectively.

If an absolute time data-pushing logic is adopted, the wait time is linked to the data frame time-stamp t_s and it elapses at

$$t_p = t_s + T_{abs}, \tag{3.2}$$

where t_p is the PDC push time and T_{abs} is the absolute PDC wait time. To be noted that in order to push the dataframes at time t_p, the PDC must be synchronized to an absolute time reference. This logic implies that the dataset supplied to the application is characterized by high determinism.

In case a relative time data pushing logic is adopted, the wait time counter is triggered by the reception of the first data frame characterized by a time-stamp t_s and elapses at time

$$t_p = t_{a,i} + T_{rel}, \tag{3.3}$$

being T_{rel} the relative PDC wait time. In this case, it is not mandatory to synchronize the PDC with the absolute time, since it has only to count up to T_{rel} from the trigger event. Additionally, it is evident that for this data-pushing logic, the variations in the arrival time of the dataframes, largely affect the determinism of the dataset supplied to the subsequent applications.

Irrespectively of the data-pushing logics, at time t_p the aggregated dataset is pushed to the supplied applications and the pointer p is incremented. The pushed dataset is replaced by an empty one characterized by a time-stamp equal to $t_{max} + T_r$. Yet, for both the data-pushing logics, the pushing at time t_p is operated even if the dataset is characterized by missing information. In this case, the missing data is flagged according to what specified in [46]. It is the task of the subsequent applications to cope with possible incomplete datasets by using techniques able to replace the missing information (e.g. [79, 80]). A delayed packet that reaches the PDC when its corresponding dataset has already been pushed, is discarded and it is no longer available for further applications.

From what specified above, it is evident that the PDC wait time plays an important role in the PDC design. Its value must be selected as trade-off between the completeness of the dataset provided to the applications and the latency requirement of the application itself. For a *soft real-time* application, the wait time can be set to a large value with the consequent increase of the overall latency of the system. Conversely, for a *hard real-time* application the wait time has to be minimized as a function of the number of missing information accepted by the subsequent applications.

A proper value of T_{abs} can be set according to the measured synchrophasor data latency in order to push time-aligned datasets that are mostly complete. In this case, the minimum buffer depth for the absolute time data-pushing logic is

$$M = \left\lceil \frac{T_{abs} - T_{min}}{T_r} \right\rceil + 1 \tag{3.4}$$

where $\lceil \cdot \rceil$ represents the ceiling function and T_{min} the minimum possible PMU reporting latency.

In case of relative time data-pushing logic, T_{rel} has to be set according to the measured time needed to receive all data frames of a specific dataset. The resulting buffer length is computed as[3]

$$M = \left\lceil \frac{T_{rel}}{T_r} \right\rceil + 1. \tag{3.5}$$

Push-when-complete logic

For a deterministic and well designed synchrophasor network, with a PDC wait time properly defined, most of the datasets are completed before the timeout elapses. In this specific cases, and according to the logics presented so far, the dataset would wait for the timeout to elapse before being pushed, even if the dataset is already completed.

---

[3] Note that the $+1$ in (3.4) e (3.5) is needed to handle dataframes arriving at the PDC at the same instant when the corresponding dataset is being pushed.

In this respect, a data pushing logic that pushes the dataset as soon as it is complete, regardless of the wait time, contributes in actively reducing the PDC latency without affecting the completeness of the dataset. The majority of the datasets are pushed according to this logic, unless data frames are lost or delayed. In such a case, the absolute or relative time logics would overtake and push uncompleted datasets only once the PDC wait time has elapsed.

As mentioned, the *push-when-complete* logic has the main advantage of minimizing the PDC reporting latency, which is practically reduced to the synchrophasor data latency of the latest received data frame plus the negligible PDC processing time. This allows to increase the time budget allocated for the other functionalities. On the other hand, the drawback of such an approach is that the data pushing time t_p is linked with the data frames arrival time and thus it jitters. Hence, the supplied applications should be designed in order to properly cope with non-deterministic datasets arrival. A solution for this issue is to embed dedicated FIFO (First-In-First-Out) data structures in the supplied applications, in order to eliminate the non-deterministic synchrophasor data latency (see Fig. 3.2).

The validation of the performance of the proposed PDC with the associated data-pushing logics is given in Chapter 5.

As a side note, it is worth mentioning that, although the time-alignment of synchrophasors is performed in the large majority of the cases, one could imagine to feed the time-stamped measurements directly to the applications. In this scenario, the PDC is only used as a data concentration and decapsulation point and it does not perform any time-alignment nor implements any particular data pushing logic. This avoids that the PDC waits for a delayed data that does not bring a critical information for the subsequent application. It is then the task of the application itself to implement a proper sequential data-processing logic that, having a global view on the data that is currently available and the missing ones, decides to provide or not its outputs. Following this strategy, whenever a redundant or non critical measurement is missing, the output of the application is still provided without the need for the PDC wait time variable to elapse, leading to a reduction of the overall latency. The validation of such alternative approach is not described in this manuscript and will be the focus of future research.

3.1.2 Real-time state estimation

As an example of situation awareness function, we present the real-time state estimation, where with *system state* we indicate the voltage phasors at all the network buses. The knowledge of the system state allows to infer the system operating conditions thus enabling the usage of several fundamental functions, such as security assessment, voltage control and stability analysis. Until the mid 1970s, the system state was obtained by using the raw voltage measurements of magnitude and power injections by means of a load flow. The drawback of this *modus operandi* was that the loss of even only one measurement made the calculation impossible and, additionally, error in the measurements highly impacted the load flow solution.

These limitations were overcome when the load flow theory was combined with a statistical processing of the collected information to obtain the likelihood system state. The associated state estimation (SE) process consists in an optimization problem able to process the measurements together with the network model in order to determine the likelihood state of the system. The benefits of such a technique are several. First of all, the measurements are not restricted to voltage magnitudes and powers but all the type of measurements are allowed (e.g., voltage and current magnitudes, nodal power injections and flows, synchrophasors) and their consistency is evaluated by using the network model. Moreover, a sufficient measurement redundancy allows to cope with measurement losses, detect and identify measurements and parameters errors and filter out the measurement noise. The importance of the foregoing properties is perceived differently according to the final goal of the user of the state estimation results. For example, the aim of the system operator is to have a trustful output from the SE and thus its main interest is to have a reliable identification of inconsistent or erroneous measurements. On the other hand, automatic regulation functions and protections need also to exploit the capacity of the SE to filter out the measurement noise in order to take accurate and proper control actions.

Traditionally, SE was performed by using measurements coming from remote terminal units (RTUs)[4]. As a result, the SE was characterized by a refresh-rate that could be in the range of minutes [81]. The advent of PMUs in transmission and afterwards in distribution systems, is leading to better accuracy performance and a significant increase in the SEs refresh-rates that now are in the sub-second range.

Since the works of Schweppe on power system SE in the early ’70s [82, 83, 81], the research mainly focused on the so-called *static estimators*, largely based on the weighted least squares (WLS) [84, 85, 86]. A static estimator uses a single set of measurements belonging to the current time-step and the network topology to obtain the most likely estimate of the system state. Subsequent research led to the formulation and development of the so-called *recursive estimators*, such as the Kalman filter (KF). These estimators, in addition to the measurement set at the current time-step and the network model, also predict the system state by modeling its time evolution. This prediction component comes at the price of introducing an additional source of uncertainty that, if not properly quantified, might worsen the accuracy of the estimated state. For this reason, the ability of recursive estimators to better filter out the measu-

---

[4] An RTU is a device, installed at the substation level, that is used to send (usually non-synchronized) measurements to the network operation and control center. The measurement set generally consists of voltage and current magnitudes as well as active and reactive powers.

rement noise could not be exploited in the past due to the low refresh rate between two consecutive SE outputs and thus due the high uncertainty in the state prediction. Thanks to the adoption of PMUs characterized by a high reporting rates, the usage of recursive estimators has been reconsidered.

In what follows, the measurement and process models used by static and recursive estimators, are described because they are functional with respect to the applications described in the rest of the chapter. For the same reasons, this section also provides the analytic formulation of two linear estimators: the so-called linear weighted least squares estimator (LWLS) and the discrete Kalman filter (DKF).

Measurement model

The link between the system state variables and the measurements, together with the measurement noise is expressed by the measurement model. In power systems, the measurement model is represented by the network model that is composed of (i) the network topology and (ii) the electrical parameters of the various components of the power system (e.g., line, transformers). Depending on the type of measurement chosen, the measurement model can be either linear or nonlinear. When using measurements coming from RTUs or hybrid set of RTUs and PMUs, the measurement model is nonlinear. On the other hand, when the SE uses only measurements coming from PMUs composed of voltage and/or current phasors, the SE can be formulated in a linear way. The latter is the formulation described in the rest of the section and used throughout the whole manuscript.

In general, the state variables are represented by the phase-to-ground nodal voltages. Nevertheless, there are cases in the literature where the state variables are represented by the nodal current injections, by the current flows, or a mix of them (provided that they are independent state variables). If we define with $\mathcal{S}$ the set of network buses, the number of network buses is equal to $s =\mid \mathcal{S} \mid$, where the operator $\mid \ \mid$ denotes the cardinality of a set. The state of a three-phase (3-ph) network with s buses is denoted by $\mathbf{x} \in \mathbb{R}^n$, where $n = 3 \cdot 2s$ is the number of states that compose the set of states variables $\mathcal{N}$. Also, if we define with $\mathcal{B}$ the set of network branches or lines, the number of branches is equal to $b =\mid \mathcal{B} \mid$. An exact linear measurement model is obtained by expressing measurements and states in rectangular coordinates. Hence, the state vector is:

$$\mathbf{x} = [\mathbf{V}_{1,re}^{a,b,c}, \dots, \mathbf{V}_{i,re}^{a,b,c}, \dots, \mathbf{V}_{s,re}^{a,b,c}, \mathbf{V}_{1,im}^{a,b,c}, \dots, \mathbf{V}_{i,im}^{a,b,c}, \dots, \mathbf{V}_{s,im}^{a,b,c}]^T \tag{3.6}$$

where

$$\begin{aligned}\mathbf{V}^{a,b,c}_{i,re} &= [V^a_{i,re}, V^b_{i,re}, V^c_{i,re}]\\ \mathbf{V}^{a,b,c}_{i,im} &= [V^a_{i,im}, V^b_{i,im}, V^c_{i,im}]\end{aligned} \tag{3.7}$$

are respectively the real and imaginary parts of the voltage phasor at bus *i* in the three phases. To be mentioned that PMU measurements eliminate the need of choosing a reference bus[5]. Unlike the conventional SE formulation, when using PMUs, the phase angle or the imaginary part of the voltage is estimated at every bus.

In order to provide an example of linear measurement model, and without loss of generality, let us assume that the SE is fed with measurement coming only from PMUs. Suppose that the measurements consist of nodal voltage phasors, current injection phasors and current flow phasors. Identify with $\mathcal{D}_1$ ($d_1 =\mid \mathcal{D}_1 \mid$) the set of buses where PMUs measure nodal voltage phasors, with $\mathcal{D}_2$ ($d_2 =\mid \mathcal{D}_2 \mid$) the set of buses where current injection phasors are measured and with $\mathcal{D}_3$ ($d_3 =\mid \mathcal{D}_3 \mid$) the set of branches where current flow phasors are measured. Hence, the set of measurements $\mathcal{M}$ is composed of:

- $3d_1$ phase-to-ground voltage phasors;
- $3d_2$ injected current phasors;
- $3d_3$ branch current phasors;

and its cardinality is equal to $m = 2 \cdot (3d_1 + 3d_2 + 3d_3)$. Therefore, the measurement array $\mathbf{z} \in \mathbb{R}^m$ is equal to:

$$\mathbf{z} = \left[\mathbf{z}_V, \mathbf{z}_{I_{\text{inj}}}, \mathbf{z}_{I_{\text{flow}}}\right]^T \tag{3.8}$$

where

$$\begin{aligned}\mathbf{z}_V &= \left[\mathbf{V}^{a,b,c}_{1,re}, \ldots, \mathbf{V}^{a,b,c}_{d_1,re}, \mathbf{V}^{a,b,c}_{1,im}, \ldots, \mathbf{V}^{a,b,c}_{d_1,im}\right]\\ \mathbf{z}_{I_{\text{inj}}} &= \left[\mathbf{I}^{a,b,c}_{\text{inj},1,re}, \ldots, \mathbf{I}^{a,b,c}_{\text{inj},d_2,re}, \mathbf{I}^{a,b,c}_{\text{inj},1,im}, \ldots, \mathbf{I}^{a,b,c}_{\text{inj},d_2,im}\right]\\ \mathbf{z}_{I_{\text{flow}}} &= \left[\mathbf{I}^{a,b,c}_{\text{flow},1,re}, \ldots, \mathbf{I}^{a,b,c}_{\text{flow},d_3,re}, \mathbf{I}^{a,b,c}_{\text{flow},1,im}, \ldots, \mathbf{I}^{a,b,c}_{\text{flow},d_3,im}\right].\end{aligned} \tag{3.9}$$

The measurements and the system state variables are linked by the following equation:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{3.10}$$

---

[5] A reference bus, is a bus where the phase angle or the imaginary part of the voltage it is assumed to have a known value (usually equal to zero) and therefore it is not included in the state vector.

where $\mathbf{H}$ is a $m \times n$ matrix that represents the link between the measurements and state variables and $\mathbf{e}$ is the measurement noise. Note that, when using a linear SE, $\mathbf{H}$ does not introduce approximation in the measurement model since it is exact. The measurement noise $\mathbf{e}$ is assumed to be white and Gaussian, with a distribution:

$$p(\mathbf{e}) \sim \mathcal{N}(0, \mathbf{R}) \tag{3.11}$$

where $\mathbf{R}$ is the measurement noise covariance matrix. The normality of PMU errors is based on experimental evidences of error distributions of actual PMUs (e.g., [87]). The diagonal entries of $\mathbf{R}$ represent the variances of the measurements, which correspond to the cumulative accuracies of the metering systems[6]. The off-diagonal entries account for eventual correlation between the measurements that occurs if mutual influence among meters is present. However, as discussed in [26] we here recall why the presence of off-diagonal terms is unlikely to occur:

- Measurements provided by different meters can be reasonably considered independent [88], and it is assumed to use no 3-ph multifunction meters [89];
- The sensors are typically installed separately in each of the three phases and the cross-talk interferences are assumed to be negligible;
- The voltage and current magnitudes measured by the same PMU can be usually considered uncorrelated [88];
- As demonstrated in [88], neglecting PMU correlations (both in magnitude and phase) in the estimator model does not lead to a significant decrease of the SE accuracy.

For the case of power networks, matrix $\mathbf{H}$ of (3.10) is derived from the network topology and the electrical parameters of the various network components. The derivation of the linear matrix $\mathbf{H}$, when using rectangular coordinates, is available in several works in the literature (e.g., [26, 90]) and therefore it is not provided here.

Process model

As mentioned in the introduction, recursive state estimators use a process model in addition to the measurement model. The process model is used to describe the time evolution of the system state as a function of (i) the previous system states, (ii) the controllable inputs, (iii) the process noise.

---

[6] With metering system, we here refer to sensors as the transducers (e.g., voltage or current instrument transformers) that scale down the input voltage and current signals in order to interface the meters (represented in this case by PMUs) with the electrical network.

The considered linear discrete-time process model can be formulated as in [91]:

$$\mathbf{x}_t = \mathbf{A}\mathbf{x}_{t-1} + \mathbf{B}\mathbf{u}_t + \mathbf{w}_t \tag{3.12}$$

where:

- t is the time-step index;
- $\mathbf{x} \in \mathbb{R}^n$ represents the system state;
- $\mathbf{u} \in \mathbb{R}^{u_c}$ represents a set $\mathcal{U}_c$ $(u_c = \mid \mathcal{U}_c \mid)$ of known controllable variables;
- $\mathbf{w} \in \mathbb{R}^n$ represents the process noise;
- $\mathbf{A}$ is an $n \times n$ matrix that links the system state $\mathbf{x}$ at time-step $t-1$ with the one at the time-step t, for the case of null controllable variables and null process noise;
- $\mathbf{B}$ is a $n \times u_c$ matrix that links the system state with the controllable variables $\mathbf{u}$, for the case of null process noise.

In general, matrices $\mathbf{A}$ and $\mathbf{B}$ might change at each time-step. Several works in the literature focused on the estimation the state transition matrix $\mathbf{A}$ to increase the prediction model (e.g., using Holt's exponential smoothing [92], regression analysis [93]). Nonetheless, for sake of simplicity, in what follows we leverage on the high frame rate of the PMUs (e.g., 50 fps in a 50 Hz system) and thus we assume that, between two consecutive time-steps, the system state exhibits small variations. For this reason, we adopt a unity state transition matrix as in its original formulation in [94]. Additionally, power systems are not typically controllable thus $\mathbf{B}$ is set equal to the null matrix $\mathbf{0}$. For these reasons, from (3.12) by imposing $\mathbf{A} = \mathbf{I}$ and $\mathbf{B} = \mathbf{0}$ a suitable process model for the case of power system SE with PMUs is obtained. It is called Autoregressive Integrated Moving Average - ARIMA (0,1,0) and it is given by:

$$\mathbf{x}_t = \mathbf{x}_{t-1} + \mathbf{w}_t \tag{3.13}$$

The process noise $\mathbf{w}_t$ is assumed to be a Gaussian white sequence:

$$p(\mathbf{w}_t) \sim \mathcal{N}(0, \mathbf{Q}_t) \tag{3.14}$$

where $\mathbf{Q}_t$ is the *process noise covariance matrix*.

The application of the process model (3.13) to power system SE using KF was proposed in the 1970 by Debs and Larson [94]. The main advantage of such a formulation is that only $\mathbf{Q}$ has to be assessed. An heuristic method for the assessment of $\mathbf{Q}$ in the context of power system SE is proposed in [95]. It uses a sliding time windows of the last K estimated states to directly infer the distribution of the process noise covariance matrix. In particular, being at time t, the forecast of $\mathbf{Q}_{t+1}$ is performed using the last K estimated states (from t to $t-K$). The K process noises $\mathbf{w}^{(j)}$ with $j=(1,\ldots,K)$ are computed as

$$\mathbf{w}^{(j)} = \mathbf{x}^{(j)} - \mathbf{x}_{t-K} \tag{3.15}$$

Finally, the process noise covariance matrix $\mathbf{Q}_{t+1}$ is obtained by computing the variance of every row of $\mathbf{w}$. This heuristic method is used in this thesis to assess the $\mathbf{Q}$ of the chosen recursive state estimator (i.e., Kalman Filter). For additional details, refer to [95].

Observation. In most cases, including power system SE, it is reasonable to assume that the process and measurement noises are uncorrelated, that is:

$$\mathbb{E}[\mathbf{w}\mathbf{e}^T] = \mathbf{0} \tag{3.16}$$

Weighted Least Squares

The weighted least squares (WLS) estimator is used when measurements are characterized by different accuracy. Indeed, the WLS method is able to weight the measurements according to their accuracy. It relies on the following assumptions:

1. The measurement noises are Gaussian-distributed with null mean value;
2. The measurement noises are uncorrelated, therefore the measurement noise covariance matrix $\mathbf{R}$ is diagonal;
3. The measurement matrix $\mathbf{H}$ that links the measurements with the states is full rank, so that the network is observable.

The objective of the WLS-SE is to compute the *most likely* system state, given a set of measured quantities. The measurement noises are assumed to have known Gaussian probability distributions with zero mean and variances reported in the diagonal elements of $\mathbf{R}$. The *measurement residual* vector $\mathbf{r}$ is defined as:

$$\mathbf{r} = \mathbf{z} - h(\mathbf{x}) \tag{3.17}$$

where we consider the measurement function $h(\mathbf{x})$ truly linear, as in (3.10). The objective of the WLS optimization problem is to minimize the weighted sum of the squares of the measurement residuals as explained, for example, in [86]:

$$J(\mathbf{x}) = \mathbf{r}^T\mathbf{R}^{-1}\mathbf{r} \tag{3.18}$$

The assumption #2, enables us to write Equation (3.18) as:

$$J(\mathbf{x}) = \sum_{i=1}^{m} \frac{r_i^2}{R_{ii}} \tag{3.19}$$

It can be seen that the reciprocal of the measurement noise variances represent the weights assigned to each measurement, so that a higher measurement accuracy corresponds to a higher weight.

In the case of Linear Weighted Least Squares (LWLS), the exact linear measurement model of (3.10) is used. The measurement residual vector at a given time instant *t* is given by:

$$\mathbf{r}_t = \mathbf{z}_t - \mathbf{H}\mathbf{x}_t \tag{3.20}$$

where matrix **H**, a part from containing no approximations, it is also constant in time for a given network model.

The minimum of the function J in correspondence of the *estimated state* $\widehat{\mathbf{x}}$ can be computed analytically as:

$$\left.\frac{\partial J(\mathbf{x}_t)}{\partial(\mathbf{x}_t)}\right|_{\widehat{\mathbf{x}}} = \left.\frac{\partial(\mathbf{r}_t^T \mathbf{R}_t^{-1} \mathbf{r}_t)}{\partial(\mathbf{x}_t)}\right|_{\widehat{\mathbf{x}}} = 0 \tag{3.21}$$

that yields:

$$\mathbf{H}^T \mathbf{R}_t^{-1} (\mathbf{z}_t - \mathbf{H}\widehat{\mathbf{x}}_t) = 0. \tag{3.22}$$

Solving for $\widehat{\mathbf{x}}_t$ yields:

$$\widehat{\mathbf{x}}_t = \mathbf{G}_t^{-1} \mathbf{H}^T \mathbf{R}_t^{-1} \mathbf{z}_t \tag{3.23}$$

where **G** is the so-called *Gain Matrix* that is defined as:

$$\mathbf{G}_t = \mathbf{H}^T \mathbf{R}_t^{-1} \mathbf{H} \tag{3.24}$$

The covariance matrix of $\widehat{\mathbf{x}}_t$ is:

$$\text{cov}(\widehat{\mathbf{x}}_t) = \mathbf{G}_t^{-1} \tag{3.25}$$

To be noted that, while **H** is constant in time for a given network model, **R** may change at each time-step because:

- The measurement errors are calculated with respect to the measured values.
- The measurement errors are given in polar coordinates while the state is ex-

pressed in rectangular coordinates. The projection from polar to rectangular coordinates needs to be performed at each time-step. The derivation of the analytical relationship that allows to express the phasor uncertainties in rectangular coordinates as a function of the measurements is given in [90]. To be noted that the measurement errors transformed in rectangular coordinates are Gaussian-distributed only if the standard deviation of the magnitude and phase errors are small [90]. Hence, we assume that the sensors used throughout the manuscript satisfy this constraint.

Kalman Filter

The Kalman Filter (KF) was presented in 1960 as a recursive solution to the discrete data linear filtering problem. Since then it has been further improved and used in different fields including power systems SE. The KF relies on the following assumptions:

1. The process and measurement noises are Gaussian white sequences;
2. The process and measurement noises are uncorrelated, as indicated by (3.16);
3. The measurement matrix $\mathbf{H}$ that links the measurements with the states is full rank, so that the network is observable.

Among the several KFs that have been deployed, the Discrete Kalman Filter (DKF) is used when it is possible a linear formulation of the SE, as in our case. In what follows, the DKF is described as it is one of the estimators used in this thesis.

As mentioned above, the estimator has to face and manage two main sources of error formally included in (i) the measurement noise covariance matrix $\mathbf{R}$ and (ii) the process noise covariance matrix $\mathbf{Q}$. The former takes into account the noise $\mathbf{e}$ added by the measurement devices. The larger the coefficients of $\mathbf{R}$, the lower the filter trusts the measurements model (3.10). The $\mathbf{Q}$ matrix, instead, comprehends every approximation introduced in the process model, therefore it gives an indication of how much the filter trusts the process model (3.13).

As known (e.g., [91]), DKF consists of two different parts, the so-called *time-update* (*prediction*) and the *measurement-update* (*estimation*). The prediction equations obtain an a-priori estimate $\widetilde{\mathbf{x}}_t$ of the true state $\mathbf{x}_t$, using the observations available up to and including time-step $t-1$. The estimation equations incorporate the new measurements obtained at time-step t into the a-priori estimate and obtain an improved a-posteriori estimate $\widehat{\mathbf{x}}_t$ of the true state $\mathbf{x}_t$.

The derivation of the formulation for the DKF-SE is not the focus of the chapter and thus it is not provided. The prediction and estimation equations for the optimal

Kalman Gain are reported in the following for reference:

1. Time-update (prediction):

$$\widetilde{\mathbf{x}}_t = \widehat{\mathbf{x}}_{t-1} \tag{3.26}$$

$$\widetilde{\mathbf{P}}_t = \widehat{\mathbf{P}}_{t-1} + \mathbf{Q}_{t-1}. \tag{3.27}$$

2. Measurement-update (estimation):

$$\mathbf{K}_t = \widetilde{\mathbf{P}}_t \mathbf{H}^T (\mathbf{H}\widetilde{\mathbf{P}}_t \mathbf{H}^T + \mathbf{R}_t)^{-1} \tag{3.28}$$

$$\widehat{\mathbf{x}}_t = \widetilde{\mathbf{x}}_t + \mathbf{K}_t(\mathbf{z}_t - \mathbf{H}\widetilde{\mathbf{x}}_t) \tag{3.29}$$

$$\widehat{\mathbf{P}}_t = (\mathbf{I} - \mathbf{K}_t\mathbf{H})\widetilde{\mathbf{P}}_t. \tag{3.30}$$

where:

- $\widetilde{\mathbf{P}}_t$ is a $s \times s$ matrix that represents the a-priori estimate error covariance;
- $\widehat{\mathbf{P}}_{t-1}$ and $\widehat{\mathbf{P}}_t$ represent the a-posteriori estimate error covariance matrices at time-step $t-1$ and t, respectively;
- $\mathbf{K}_t$ is a $s \times m$ matrix that minimizes the a-posteriori estimate error covariance. It is the so-called “Kalman gain”.

3.2 Time critical power system applications

As introduced in Chapter 2, the so-called *data process-and-operation* layer, is often composed of applications that, taking advantage of the PMU measurements, are able to achieve several specific tasks. A non-comprehensive list of possible applications includes tuning of system parameters (e.g., protection relays), estimation of the nodal equivalent (e.g., loads) parameters, congestion management, fault detection and fault location [1]. It is clear that these applications, although based on the same architecture, are characterized by very different time-scales. In what follows, we present two applications that, with different time-scales, aim at protecting and controlling the power system.

3.2.1 Fault detection and faulted-line identification

The content of this section is based on [96] and it is a shared contribution with L. Zanni that is the other main author of the work.

Introduction

The fundamental problem in power system protection is to define the quantities that allows to differentiate between normal and abnormal (faulty) operating conditions. This is complicated by the fact that, for a relay device, a normal operating condition can also be the one where a disturbance exists, but it is outside of the zone of protection [97]. Regardless of the chosen method, the *fault detection* and subsequent protection of a power system is not a trivial task. The network operator always needs to deal with:

1. *Definition of zones of protection*: the region of a power system for which a given relay or protective system is responsible.
2. *Selectivity of protections*: the setting of time-delays and coordination between relays belonging to the same or different zone of protection.
3. Increasing *number of protection devices installed*: each type of relays covers for a subset of possible faults. This leads to increased complexity in terms of installation and maintenance.

In the recent years, studies have shown that the network operator can highly benefit from PMUs and the associated synchrophasors in order to improve its existing protection schemes [98].

Traditionally the fault detection (with the associated relaying schemes) and fault location functionalities have been considered as separate processes since the latter usually requires computational efforts that do not fit the time latencies needed by the protections.

While the protection of the system from faults has to be achieved within time-scales of tens of / hundred milliseconds, the identification of the faulted component (i.e., *fault location*) is usually performed offline. Fault location methods can relay on impedance-based techniques [99], exploit the characteristics of fault-generated traveling waves (e.g., [100, 101, 102]) or use synchrophasor measurements (e.g., [103, 104]).

In distribution systems, the protection of the feeders is typically achieved by means of breakers often installed only at the root of each feeder. In a very basic scheme, the fault location is then performed by repairing crews, leading to outages that might last hours. As discussed in Chapter 1, the increasing integration of DGs, is leading to changes in monitoring and automation of existing distribution systems. An accurate and fast fault location is the next step to accelerate the service restoration. In this respect, the literature has proposed a number of methods for fault location in distribution networks based on impedance measurements [105], traveling waves [106] and synchrophasors [107].

This section discusses the possibility of merging the relaying and fault location functionalities in any power system network by using PMU-based real-time SE. Indeed, beside their capability of bad data filtering, real-time state estimators are characterized by high rejection of measurement noise [86] and low time latency [32]. The former property improves the assessment of the fault position, whilst the latter supports the stringent time requirements of protections. In the literature, the papers that aim at localizing faults by means of PMU-based state estimation is limited to [108] and [109]. In [108] the fault is detected by using bad data identification techniques. An augmented state vector, that includes the voltage and the fault position, is used to estimate the fault location. Reference [109], follows a similar approach by using estimated and/or actual voltage and current measurements at the extremities of the faulted line to infer, by means of a WLS, the fault position.

The method proposed in this section relies on the outcomes of a LWLS synchrophasor-based SE to identify, in real-time, the line affected by the fault, the fault type and the current drained by the fault. For this reason, differently from existing methods, the proposed method does not change regardless to the type of network, the type of fault, the fault impedance or the presence of DG. This flexibility theoretically enables the network operator to adopt the proposed approach as a single protection and fault-location scheme for any power system.

Proposed method

The proposed faulted-line identification[7] method represents one of the possible applications based on synchrophasor networks data and therefore:

- There is no need to implement any coordination between relays, but time-deterministic communication is required with the data process-and-operation layer (i.e., PDC and applications).
- It is based on PMUs that implicitly enable the operator to perform voltage and synchronization checks before operating a reclosing maneuver.
- A part from the sensors, the method does not share other components with the existing protection relays and thus it might be used as a backup remote protection for the deployment and testing phase.

The proposed fault detection and faulted line identification methodology strongly relies on the state estimation theory and in particular on the WLS formulation given in Section 3.1.2. It relies on the following assumptions:

---

[7] Henceforth in this manuscript, the term faulted-line identification is used interchangeably with the term fault location

1. Knowledge of the network admittance matrix (i.e., $\mathbf{H}$ is exact). This implies the knowledge of (i) network topology and (ii) line parameters. For (i), it has to be noted that the standard [40] allows PMUs to record and stream digital values with the synchrophasor data. The digital values may correspond to the status of the breaker connected to the lines departing from a PMU-monitored substation. The status of all the breakers in the observed system allows to obtain the incidence matrix and thus the network topology. Indeed, the possibility of streaming the breaker's status together with the synchrophasor is a further advantage of the PMUs for protection. It allows to reconstruct and time-tag the topology changes with the same latency as the measurement set. If, due to installation constrains, not all the PMUs can measure the status of the breakers in the substation, the literature provides several methods to estimate the topology or detect topology errors, with or without using PMU measurements (e.g., [110, 111, 112]. Concerning (ii), distribution and transmission networks are usually composed of overhead lines and cables that have a standard configuration with known electrical parameters. Therefore, we suppose that these characteristics are known. By knowing the incidence matrix and the line parameters, the admittance matrix $\mathbf{Y}$ can be obtained.

2. Knowledge of the noise covariance matrix $\mathbf{R}$. This assumption holds in power systems because the characteristics of the measurement devices (e.g., sensor's class) are usually known. See Section 3.1.2 for details about the measurement model.

3. PMUs are installed in every bus. In the current literature, it is evident the growing interest in deploying PMUs and associated applications. Recent publications have dealt with PMUs installation in every bus, even at the distribution level [30, 32].

4. Bad data are not present in the dataset. The targeted application sets stringent time requirements. For this reasons, it is assumed that bad data are removed from the measurement set by using the pre-estimation filtering of bad data as described in Chapter 4.1.

Fault modeling: A generic fault on a line is an event that can be modeled by adding an additional three-phase bus (hereafter called *virtual bus*) on the line affected by the fault. The virtual bus absorbs the fault current and it increments by one the total number of three-phase buses in the monitored network.

Let us consider a s-buses and b-lines network equipped with PMUs at every bus, measuring injected currents. We can imagine to feed b parallel SEs with the same dataset. Each one of the b-SEs has a slightly different topology from the others. The difference is due to the presence of the virtual bus on a specific line. The j^{th} SE

($j = 1, ..., b$) considers the existence of a virtual bus *in the middle* of the j^{th} line. This leads to an augmented state vector $\underline{\mathbf{x}}$. The state vector thus becomes:

$$\underline{\mathbf{x}} = [V_{1_{re}}^{a,b,c}, ..., V_{s_{re}}^{a,b,c}, V_{s+1_{re}}^{a,b,c}, V_{1_{im}}^{a,b,c}, ..., V_{s_{im}}^{a,b,c}, V_{s+1_{im}}^{a,b,c}]^T \tag{3.31}$$

where $V_{s+1_{re}}^{a,b,c}$ and $V_{s+1_{im}}^{a,b,c}$ represent the real and imaginary parts of the nodal voltage phasor in the virtual bus. The measurement matrix $\mathbf{H}$ is modified accordingly for each SE.

In normal operating conditions, the b-virtual buses do not absorb any current and thus the different topology among the SEs does not play a role in the b estimated states. In this case, the minimization of the objective function returns similar results for each of the b-SEs:

$$\underline{\mathbf{x}}^j \backsimeq \mathbf{x}_{\text{true}} \quad \forall j \tag{3.32}$$

Assume now the existence of a generic fault (i.e., phase to ground, phase to phase or three phase) in the line delimited by buses #h and #u. The fault consists in a current (i.e., fault current) being drawn from an unknown position between buses #h and #u. Assume the f^{th} SE is the one, among the b parallel SEs, with the virtual bus placed in the middle of the line that connects bus #h and #u. It is intuitive to understand that the topology of the f^{th} SE is the closest to real network one. This is true even if the fault is not located exactly in the middle of the line, that is, in correspondence of the virtual bus for the f^{th} SE. In this case:

$$\begin{aligned} &\underline{\mathbf{x}}^f \backsimeq \mathbf{x}_{\text{true}} \\ &\underline{\mathbf{x}}^j \neq \mathbf{x}_{\text{true}} \quad \forall j \neq f \end{aligned} \tag{3.33}$$

As the position of the fault is not known a priori, it is necessary to distinguish among the b-SEs the one providing the best estimated state. The weighted measurement residuals (WMR) are used as the metric to determine the best SE (the one characterized by the smallest topology error):

$$\text{WMR}^j = \sum_{i=1}^{m} \frac{|\mathbf{z}_i - \widehat{\mathbf{z}}_i^j|}{\boldsymbol{\sigma}_{z_i}} \quad j \in [1, \ldots, b] \tag{3.34}$$

where $\widehat{\mathbf{z}}^j = \mathbf{H}^j \widehat{\mathbf{x}}^j$.

During normal operating conditions, the b-WMRs are all close to each other because the SEs have the same dataset as input and each virtual bus is not absorbing any current so it is seen as a zero-injection bus[8]. By the time a fault occurs, $b - 1$ SEs converge to a solution far from the true state and their WMRs suddenly increase. The SE that has the virtual bus placed in the faulted line has the lowest WMR, allowing

---

[8] A zero-injection bus is defined as a bus where no load or generation is connected.

an immediate *identification* of the faulted line. Moreover, the state returned by the SE characterized by the lowest WMR, is used, together with its admittance matrix, to estimate the fault currents. The phases of the virtual bus in which the estimated current differs from zero are the ones affected by the fault, so that also the type of fault is identified.

The analysis of the WMRs allows also the *detection* of the fault. Let us call WMR_{mean} the mean of all the WMRs at a certain instant in time. When the difference between the WMR_{mean} of two consecutive time-steps has a sudden increase, a fault is detected (one example of the time evolution of the WMRs before and during a fault is provided in Section 5.4.2, Fig. 5.17).

A pseudo-algorithm that summarizes the proposed method is given in Algorithm 1. For every new data set coming from the PMUs, we compute the WMRs of the parallel SEs and also their mean WMR_{mean}. Comparing the WMR_{mean} of two consecutive time-steps, we detect the presence of a fault. If a fault is detected, the index f of the SE associated to the minimum WMR identifies the faulted line. Finally, we can use the estimated state returned by the f^{th} SE to identify the fault type and estimate the fault current.

Algorithm 1 Pseudo-algorithm of the proposed fault detection and line identification method.

```
function IDENTIFY FAULT (LINE,CURRENT,TYPE)
    for each time-step $t$ do
    compute $\text{WMR}_j \quad \forall j$
    if $\text{mean(WMRs)}\Big|_t \gg \text{mean(WMRs)}\Big|_{t-1}$ then
        Fault detected ← true
        $f$ = index of min(WMRs)
        Faulted line ← $f$
        $I^f = Y^f E^f$
        Fault current ← $I^f_{\text{virtual bus}}$
        Fault type ← phases where Fault current $\neq 0$
    end if
    return Fault detected, Faulted line, Fault current, Fault type
end function
```

For sake of clarity, a flowchart summarizing the proposed method has also been added in Fig. 3.5.

In summary, the proposed method allows to:

- detect the existence of a fault;
- identify the faulted line;

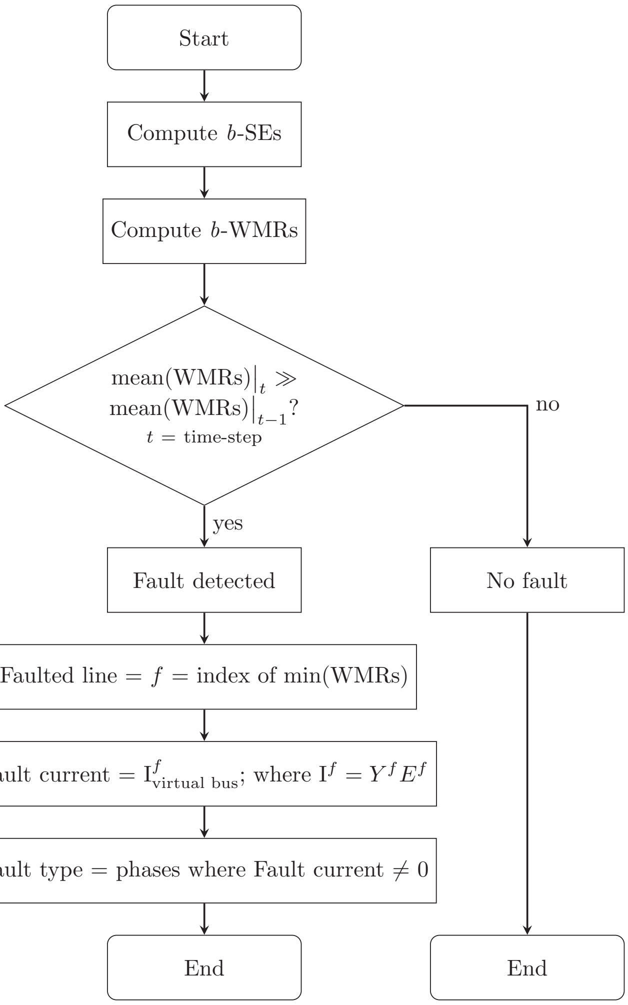

Start
Compute b-SEs
Compute b-WMRs
$\text{mean(WMRs)}\big|_t \gg \text{mean(WMRs)}\big|_{t-1}$?
t = time-step
no
yes
Fault detected
No fault
Faulted line = f = index of min(WMRs)
Fault current = $I^f_{\text{virtual bus}}$; where $I^f = Y^f E^f$
Fault type = phases where Fault current $\neq 0$
End
End

Figure 3.5 – Flowchart of the proposed fault detection and line identification method, performed at each time-step t.

- identify the fault type (1-ph, 2-ph or 3-ph);
- estimate the fault current.

Although not presented in this manuscript, the methodology described here can also be applied to estimate the location of the fault along the faulted line. The virtual bus is moved in discrete steps along the faulted line and state estimation is subsequently performed. The position of the virtual bus that minimizes the WMR corresponds to the most likely position of the fault along the line.

The validation of the proposed fault detection and faulted-line identification method in a real-time simulation environment is given in Chapter 5.4.

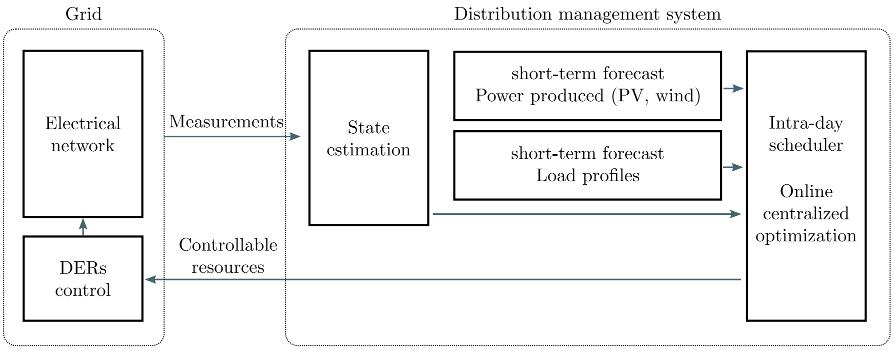

Grid
Distribution management system
Electrical network
DERs control
Measurements
Controllable resources
State estimation
short-term forecast Power produced (PV, wind)
short-term forecast Load profiles
Intra-day scheduler
Online centralized optimization

Figure 3.6 – Scheme of a generic centralized DMS for ADNs. Adapted from [114].

3.2.2 Voltage regulation scheme for distribution networks

As mentioned in Chapter 1, the past years have seen a large increase in the connection of DERs that resulted in violation of operational constraints at the distribution level. This leads to the need of developing optimal control strategies tailored for distribution grids. It is worth noting that optimal control solutions are of interests only if they meet the time constraints imposed by the stochasticity of DERs, in particular photovoltaic units (PVs), largely present in these networks. The synchrophasor network architecture presented so far, if well designed, meets these time constraints and may enable the deployment of processes for optimal control of distribution networks (e.g., voltage control, line congestion management).

This section starts with an overview on a centralized distribution management system (DMS) for ADNs. Then, framed within this control architecture, the Grid Explicit Congestion Notification (GECN) mechanism, firstly presented in [113], is recalled together with the formulation of the optimal voltage control problem.

Distribution management system for active distribution networks

A control architecture, aiming at operating in distribution networks, needs to take into account the multi-phase unbalanced nature of the network, the non-negligible R/X ratio for longitudinal line impedance as well as the influence of the transverse capacitance[9], and thus the existing control strategies have to be upgraded to meet such constraints.

Let us consider an ADN equipped with a number of distributed controllable energy resources, a monitoring infrastructure like the one presented so far and a centralized DMS. A possible architecture of the DMS is shown in Fig. 3.6, and its main modules are:

---

[9] The line shunt parameters are non-negligible especially in presence of coaxial cables. These types of cables are often present, for instance, in urban context.

- *State estimation*: This DMS module has been described in Section 3.1.2. The real-time SE has to be able of assessing the system state with a latency of few tens/hundreds of milliseconds with relatively high levels of accuracy and refresh rate. Once the voltage phasors are known, it is straightforward to compute the nodal power injections and the line power flows.
- *Short-term forecasts*[10]: This DMS module incorporates algorithms able to provide short-term forecast for loads and DERs. An accurate forecast of load and DER generation is useful when the DNOs is requested to contribute to ancillary services, or for demand-response actions [115, 116].
- *Online centralized optimization*: This DMS module formulates and solves the optimization problem in order to obtain the new operation set points. Examples of objective functions can be the minimization of the losses, or of the voltage deviation, the minimization of the cost of the energy supply or the management of lines congestions. Once the new set points are obtained, the module communicates them to the controllable DERs with a time-scale that is set by the controlled application [114, 117].

In what follows we give the necessary background on the Grid Explicit Congestion Notification (GECN) mechanism. The GECN mechanisms was discussed in the Ph.D. dissertation [118]. We briefly recall the functionalities of the *centralized GECN network controller* and the design of the *GECN load controller* for the case of thermostatically controlled loads (TCLs). These two components constitute the necessary background to fully understand the validation of the GECN mechanism in a real-time simulation environment, given in Chapter 5.5.

GECN mechanism

A control mechanisms that implements a direct control of each single resource, is not a viable approach when the resources are numerous and diverse, as in the distribution networks where the controlled systems are represented, for instance, by thermostatically controlled loads (TCLs) or distributed storage. Such control scheme would results in algorithms that cannot scale in the number of network buses and controllable resources. Additionally, a customized architecture for the control of a specific type of energy resource, renders the control problem difficult in presence of heterogeneous resources. The GECN mechanism was designed in order to address such issues. GECN is a unified control mechanism that provides grid ancillary services by controlling heterogeneous energy resources via low bit-rate broadcast-control signals [113]. It is conceived to avoid individual point-to-point communication from the DNO to every

---

[10] This functionality is mentioned for the sake of completeness but it is not used in the manuscript. It is mainly used for energy management purposes.

controllable resource and uses state estimation as feedback channel. The control architecture is essentially composed of two parts:

- The first part is a centralized network controller that, based on the system state, computes optimal power active and reactive nodal power set-points that steer the system to the desired voltage level. The optimal set-points are then translated to broadcast signals, henceforth called GECN signals, that are communicated to the buses where the controllable DERs are connected.
- The second component of the GECN architecture is the local controller that interprets the GECN signals and acts on the DERs according to the device's capabilities and internal state constraints.

An interesting feature of such mechanism is the inherent ”separation of concerns" between the centralized GECN network controller and the GECN local controllers. The GECN network controller is agnostic with respect to the nature and the actual state of the controlled resources. On the other hand, the local resource controller is specific for each type of DER and simply acts on the resource it is coupled to, as a function of its GECN input signals and the resource's internal state without having a view of the whole system.

GECN network controller

The control mechanism is based on the closed loop depicted in Fig. 3.7[11]. A deviation from the day-ahead forecast power profiles $\left(P_i^f(t+1), Q_i^f(t+1)\right)$ is penalized and thus the aim of the DNO is to match them as closely as possible to reduce the costs of operation associated to the acquisition of reserve at transmission level (e.g., [119]). At the same time, the DNO has to ensure a voltage profile within acceptable operating limits $\left(E_0 - \delta \leq |\bar{E}_i(t+1)| \leq E_0 + \delta\right)$, where δ denotes the voltage deviation from the rated value E_0 that the DNO tolerates.

At each time-step t, and for each bus i, the DNO observes the state of the network $\bar{E}_i(t)$ and the aggregated active and reactive power injection $P_i(t)$, $Q_i(t)$. Additionally the DNO computes the mismatch between forecast power and aggregated one, in absence of control, as $\Delta P_i^f(t) = P_i^f(t+1) - P_i(t)$ and $\Delta Q_i^f(t) = Q_i^f(t+1) - Q_i(t)$.

The voltage sensitivity coefficients with respect to absorbed/injected power of a bus ℓ [120, 113] are:

$$K_{P,i\ell}(t) := \frac{\partial|\bar{E}_i(t)|}{\partial P_\ell},\ K_{Q,i\ell}(t) := \frac{\partial|\bar{E}_i(t)|}{\partial Q_\ell}, \tag{3.35}$$

---

[11] Fig. 3.7 shows the closed loop for the control of the active power. In case the controllable resources have reactive power capabilities, a similar feedback control loop is adopted.

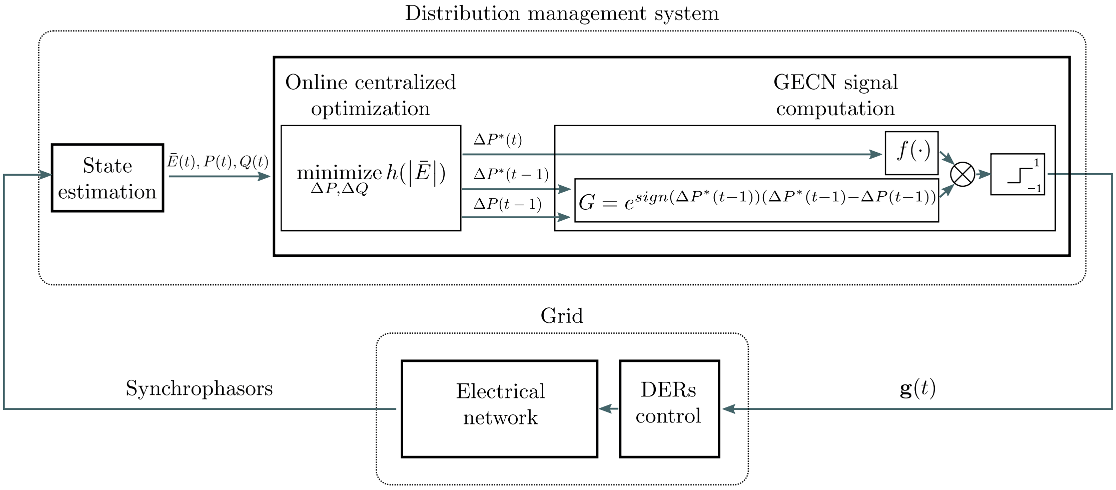


Figure 3.7 – Control loop for the computation of the GECN signal $\mathbf{g}(t)$ for the control of active power. Adapted from [113].

This allows for a local linearization of the voltage deviation $\Delta|\bar{\mathbf{E}}(t)| = (\Delta|\bar{E}_i(t)|)_i$:

$$\Delta|\bar{\mathbf{E}}(t)| \approx \mathbf{K_P}(t)\Delta\mathbf{P}(t) + \mathbf{K_Q}(t)\Delta\mathbf{Q}(t). \tag{3.36}$$

Next, using the computed sensitivity coefficients, the DNO solves the following convex optimization problem (i.e., the online centralized optimization block shown in Fig. 3.7) to compute optimal nodal power adjustments $(\Delta\mathbf{P}^*(t), \Delta\mathbf{Q}^*(t))$ for the buses with controllable loads, in order to steer the system towards the desired operating set-point for voltage control:

$$\begin{aligned} &\min_{\Delta\mathbf{P},\Delta\mathbf{Q}} \sum_i \left(\Delta P_i(t) - \Delta P_i^f(t)\right)^2 + \sum_i \left(\Delta Q_i(t) - \Delta Q_i^f(t)\right)^2 \\ &\text{subject to:} \quad \gamma_i \leq \cos\varphi_i \leq 1 \\ &\qquad\qquad\qquad E_{min} \leq |\bar{E}_i(t)| + \Delta|\bar{E}_i(t)| - E_0 \leq E_{max} \end{aligned} \tag{3.37}$$

where γ_i is the constraint on the power factor of the i-th bus.

To be noted that the optimal control problem reported here has been modified compared to [113]. In particular, in this case the limits on the voltage deviations are explicitly inserted as constraints of the optimization problem. Additionally, we apply the penalty method to transform the problem above into an unconstrained optimization problem and we use a gradient descent iterative scheme to compute the optimal solution of the control problem [121]. Adopting such a method allows us to have control over the solution of the optimization problem in real-time as shown in Section 5.5.

The resulting optimal set points, $(\Delta\mathbf{P}^*(t), \Delta\mathbf{Q}^*(t))$ are mapped to the GECN signal $\mathbf{g}(t)$

as shown in Fig. 3.7. A saturation function f maps $\Delta P_i^*(t)$ to a value in $[-1, 1]$.

$$f(\Delta P_i^*(t)) = sign(\Delta P_i^*(t))(1 - e^{-\left|\Delta P_i^*(t)\right|/b_i}) \tag{3.38}$$

where b_i is a parameter that affects the slope of the saturation function (i.e., the smallest the b, the steepest the slope). A exponential parameter G, function of the mismatch between optimal and actual set point computed at the previous time-step $t-1$ is then used to weight the outcome of (3.38) as shown in Fig. 3.7:

$$G = e^{sign(\Delta P^*(t-1))(\Delta P^*(t-1) - \Delta P(t-1))} \tag{3.39}$$

Note that, in case the controllable resources have also reactive power capabilities, it is sufficient to replace $\Delta P_i^*(t)$ with $\Delta Q_i^*(t)$ in (3.38) and (3.39) to compute the GECN signal for the control of reactive power.

The GECN signals are broadcasted to the network buses and particularly to the load controllers. In what follows we describe how the load response has been represented.

Load response representation

In this thesis we consider TCLs whose state is given by their temperature (e.g., air conditioners or refrigerators). In particular, we describe the behavior of a cooling thermostatic device. A more detailed load representation, including also storage systems can be found in [118].

A TCL operates in binary mode $\mathcal{X} = \{0, 1\}$, and its internal state is given by the cooling compartment temperature, constrained in the form of a deadband $\Theta = [\theta_{\text{min}}, \theta_{\text{max}}]$. The internal temperature of these kinds of loads can be modeled as in [122]:

$$\theta(t+1) = \epsilon\theta(t) + (1-\epsilon)\left(\theta_0 - \eta\frac{X(t)P_r}{A}\right) + \omega(t) \tag{3.40}$$

where θ_0 is the ambient temperature, $\epsilon = e^{-\tau A/m_c}$ describes the inertia of the appliance, τ is the time-step and m_c is the thermal mass, η is its coefficient of performance, and A is the thermal conductivity. The process $\omega(t)$ is a noise process-modeling of the random external heat injections in the thermostatically controlled loads having a distribution that follows hourly data. A typical duty-cycle function (Fig. 3.8) is:

$$\begin{aligned} h(X=0,\theta) &= \mathbb{1}_{\{\theta \geq \theta_{\text{max}}\}} \\ h(X=1,\theta) &= \mathbb{1}_{\{\theta \geq \theta_{\text{min}}\}} \end{aligned} \tag{3.41}$$

As in [118], we assume at each network bus i a population of the aforementioned TCL appliances, each one having a state evolving as in (3.40) and a duty cycle described by

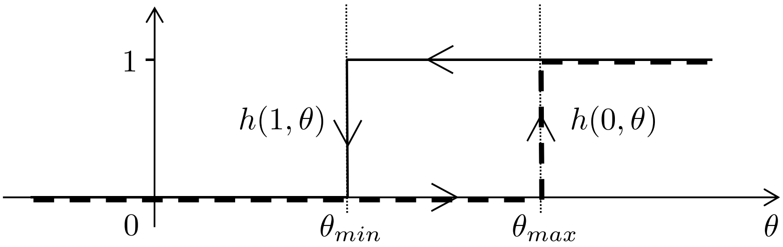


Figure 3.8 – Duty-cycle for appliances with deadband-constrained state. Adapted from [118].

(3.41). In addition to the controllable loads, in each network bus, non-elastic demand represented by typical 24-h load profiles is considered. The combination of elastic and non-elastic loads at the bus level, represents the so-called ”aggregated power".

GECN local controller

All the elastic appliances connected to a network bus i receive at the time-step t the GECN control signal $g_i(t)$ broadcast by the DNO. The signal represents a real number $g_i(t) \in [-1, 1]$. The control signal $g_i(t)$ is proportional to the DNO's desire to inhibit consumption: a positive g_i inhibits consumption, a negative g_i encourages consumption, whereas $g_i = 0$ does not impact the behavior of the appliance. The local controller decides the action to be taken based on the internal state of the resource and on the value of the received signal.

The normal operation of a TCL appliance is an on-off mode, with the temperature moving in a dead-band. When on, the TCL absorbs active power, and via a fixed power factor, a proportional amount of reactive power. For this reason, the target of the GECN local controller is to control the active power injection by switching mode, if necessary and allowed by the internal state of the TCL. A flow chart that summarizes the design and control actions of the local resources-controller is shown in Fig. 3.9[12]. In particular, a TCL reacts with a probability equal to the magnitude of the g_p signal received. Therefore, a larger magnitude of the signal would result in more appliances participating in the control action. If the TCL reacts, the controller turns on or off the appliance with a probability that is function of the signal and on the internal state of the fridge (i.e., internal temperature). Finally, if the appliance switches mode due to the g_p signal received, it ignores ignores all subsequent control signals for a predetermined number of time-steps. This avoids operation in mini-cycles thus preserving the compressor's lifetime.

As for all the other topics presented in this chapter, the validation in a real-time simulation environment of the GECN mechanism here recalled, coupled with its

---

[12] A more detailed description of this load controller is given in [118].

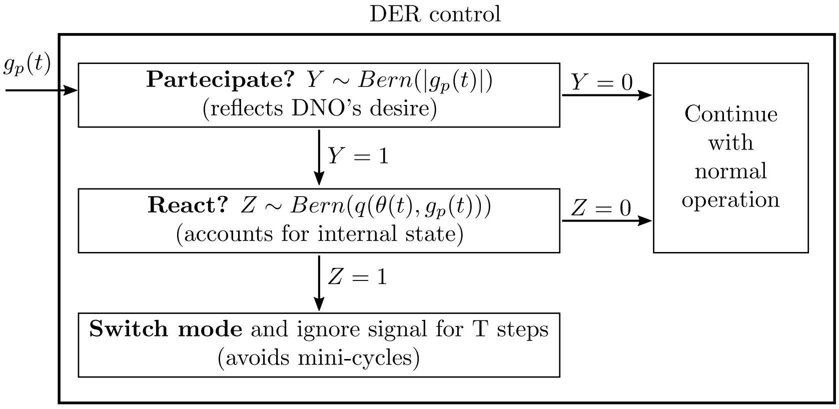

DER control
$g_p(t)$
Partecipate? $Y \sim Bern(|g_p(t)|)$
(reflects DNO's desire)
$Y = 0$
$Y = 1$
React? $Z \sim Bern(q(\theta(t), g_p(t)))$
(accounts for internal state)
$Z = 0$
$Z = 1$
Continue with normal operation
Switch mode and ignore signal for T steps
(avoids mini-cycles)

Figure 3.9 – State model representing the local controllers for TCLs. Adapted from [123].

functional blocks (e.g., PMU-based state estimation), is given in Chapter 5.

4 Quality and reliability of PMU-based time critical functions

This chapter starts with the analysis of state-of-the-art bad data detection and identification methods for power grid situation awareness systems. Then, a novel bad data detection method able to deal with intentional or unintentional tampering of synchrophasor measurements is presented. In the second part of the chapter it is shown that it is possible to forge attacks to the time reference of a number of synchrophasors that are undetectable by state-of-the-art bad data detection methods and, at the same time, lead to physical grid damage. At the end of the chapter, the proposed bad data detection method is tested as a countermeasure to neutralize the attack.

Original contributions of this chapter:

- Definition and validation of an algorithm for the pre-estimation filtering of bad data that leverages on the confidence in the predicted system state. The algorithm is also able to distinguish between actual bad data and unexpected dynamic phenomena;
- Closed form formulation of an attack to the time-reference of selected PMUs that is undetectable by state-of-the-art bad data detection methods and leads to physical grid damage.

4.1 Bad data detection and identification

As mentioned in Chapter 3.1.2, sufficient measurement redundancy allows SE to cope with measurement losses and to detect and identify measurements errors. These are the so-called *bad data* (BD). Detection indicates the ability of recognizing the *existence* of a BD in the measurement set whereas the identification pinpoints the specific corrupted measurement(s) in the set. BD always deteriorates the accuracy of the estimation output, although a large measurement redundancy and the employment of robust state estimators can mitigate this impact. In power systems, BD are not rare due to the large amount of collected measurements and the complexity of the sensing and communication layers.

An example of BD are the so-called gross errors. They are measurements characterized by a large difference from their expected value (e.g., negative magnitude values) that can be identified with simple plausibility checks. Data conditioning algorithms can be used to analyze the incoming measurements seeking gross errors, missing data, or to refine the raw measurements (e.g., [80]).

Other BD require more advanced methods to be detected and identified as the measurement error magnitude is only a few times larger than the expected standard deviation. These types of errors impact the accuracy of the estimated state and can be generated, for instance, by electromagnetic interference.

Several different algorithms are available in the literature for BD detection (BDD) and identification as summarized in [124]. They can be mainly classified in *post-estimation* and *pre-estimation* filtering processes according to the position in the state estimation chain where the detection of the BD takes place. As an alternative, one may rely on the so-called least absolute value (LAV) estimator that falls in the category of the *robust state estimators*. The LAV possess intrinsic bad-data rejection capability and does not need a separate bad-data process. When used in combination with PMU only estimators, it is possible to reduce its computation time and at the same time address its vulnerability against leverage measurements[1]. Nevertheless, as the robust state estimators are largely discussed in the literature, they are not included in this thesis.

In what follows, we provide the general background on post- and pre-estimation method for BD identification. Then, we present a novel BD detection and identification algorithm that falls into the category of the pre-estimation methods.

4.1.1 Post-estimation methods

Being executed after the static state estimator, the post-estimation methods enable the network operator to exploit the statistical properties of the SE outputs. The analysis is typically carried out on the measurement estimation residuals as they provide a quantification of the quality of the fitting between measurement set and network model. Following the nomenclature given in Chapter 3.1.2, the measurement estimation residual vector and its covariance matrix are:

$$\widehat{\mathbf{r}}_t = \mathbf{z}_t - \mathbf{H}\widehat{\mathbf{x}}_t \tag{4.1}$$

$$\mathrm{cov}(\widehat{\mathbf{r}}_t) = \mathbf{C}_t = \mathbf{R}_t - \mathbf{H}\mathbf{G}_t^{-1}\mathbf{H}^T \tag{4.2}$$

---

[1] A measurement that, although not critical, is characterized by a small residual even in presence of a large error.

A well-known post-estimation BD detection method is the χ^2-test. It leverages on the assumption that each measurement residual $\widehat{r}_{t,i}$ is a randomly-distributed zero mean Gaussian variable (assumption valid, for instance, in WLS and DKF SE presented in Chapter 3.1.2). Indeed, the objective function $J(\widehat{\mathbf{x}})$, being the sum of m normally-distributed random variables, has a χ^2-distribution with $(m-n)$ degrees of freedom. The detection of BD in the set of measurement is triggered if $J(\widehat{\mathbf{x}}) > \chi^2_{(m-n),\zeta}$, where ζ is the chosen detection confidence probability (e.g. 95% or 99%). A part from performing only detection and no identification of BD, this method also usually fails to detect BD for errors lower than twenty standard deviations as reported in [86, 125].

Another widely-used post-estimation method that allows both detection and identification of BD is the largest normalized residual (LNR) test. It requires the calculation of the *normalized measurement estimation residual* vector $\widehat{\mathbf{r}}_t^N$. The i^{th} element of $\widehat{\mathbf{r}}_t^N$ is computed as:

$$\widehat{r}_{t,i}^N = \frac{\mid \widehat{r}_{t,i} \mid}{\sqrt{C_{t,ii}}}. \tag{4.3}$$

Each normalized residual should be distributed as $\sim \mathcal{N}(0,1)$, therefore the LNR test detects BD if at least one element of $\widehat{\mathbf{r}}_t^N$ exceeds a certain threshold (e.g. 3 or 4). The largest $\widehat{r}_{t,i}^N$ is identified as BD, removed from the data set, and the SE is performed again. This procedure is iterated until no BD are detected. The LNR test limits its identification capability to a single BD or multiple non-interacting BD, that is multiple BD appearing simultaneously whose residuals are not correlated [86, 125].

Finally, the hypothesis testing identification (HTI) method [126, 127] is able to avoid several successive state estimation cycles, differently from the post-estimation methods presented so far. Additionally, the method is able to deal with multiple interacting BD. The HTI is based on the selection of a set s of suspected measurements and the computation of their estimation error $\hat{e}_s$. The identification of the BD in the set is performed according to statistical properties of each $\hat{e}_{s,i}$ in order to decide whether to accept the hypothesis H_0 (i.e., the measurement is valid), or H_1 (i.e., the measurement is corrupted). Although the latter method seems to solve some of the issues that characterize post-estimation methods (e.g., iteration in the state estimation solution), it has to be taken into account that its performance is influenced by the choice of a proper suspected measurement set. The set s should be:

- Large enough as to contain all the BD;
- Small enough to ensure accuracy in the estimate of $\hat{e}_s$;
- Formed by independent and non-critical measurements[2].

---

[2] A critical measurement is a measurement that makes the network unobservable if removed; a critical pair is composed of two measurements that make the network unobservable if removed simultaneously.

The choice of the elements of s is usually performed by using the LNR test that, as specified above, does not provide optimal results when dealing with multiple interacting BD. The difficulty in choosing a proper set s have limited the adoption of HTI method in real applications in favor of simpler, although not always reliable, LNR test.

To conclude, some general remarks concerning the use of post-processing BD methods:

- All the methods here introduced cannot identify BD in critical measurements or critical pairs, since their residuals are always equal to zero [86]. High measurement redundancy is therefore advised in real-field installations.
- A common assumption of post-estimation methods is the exact knowledge of the network model therefore any inconsistency between measurements and network model is associated to the existence of BD. However, network parameter errors have an impact on the state estimation residuals similar to BD. BD processes may misinterpret a network parameter error as a BD. An effective method to distinguish between BD and network parameter errors with or without synchrophasor measurements is presented in [128] and further expanded in [129].
- Although the post-estimation methods do not always succeed in presence of interacting BD, they are characterized by a relatively high reliability and accuracy. These characteristics come at the expense of computational time, because, after the identification of BD, the state has to be re-estimated iteratively until no more BD are detected. In this respect, one can take advantage of a predicted system state in order to obtain a consistent set of predicted measurements to be compared with the real ones, as usually done by the pre-estimation BD methods.

4.1.2 Pre-estimation methods

Pre-estimation methods analyze and filter the set of measurements before proceeding with the state estimation. The high refresh rate of PMU-based SE allows to effectively use prediction models as the ARIMA(0,1,0) already defined in (3.13). This raised the interest in coupling pre-estimation methods, as well as data conditioning of raw measurements, with recursive state estimators.

Pre-estimation methods are usually based on statistical procedures or simply logical checks that typically involve the examination of the so-called innovation vector, defined as the difference between the most recent set of measurements and a predicted one inferred by using previous estimations [130]

$$\boldsymbol{\nu}_t = \mathbf{z}_t - \mathbf{H}\widetilde{\mathbf{x}}_t. \tag{4.4}$$

The innovation vector is a Gaussian white sequence whose covariance matrix is:

$$\mathbf{S}_t = \mathbf{R}_t + \mathbf{H}\widetilde{\mathbf{P}}_t\mathbf{H}^T \tag{4.5}$$

An useful indication of presence of BD may come from the *normalized* innovation vector $\boldsymbol{\nu}_t^N$. The i^{th} element of the normalized innovation vector is computed as:

$$\nu_{t,i}^N = \frac{\mid \nu_{t,i} \mid}{\sqrt{S_{t,ii}}}. \tag{4.6}$$

Setting a threshold for some elements of the innovation vector is not a sufficient condition to detect the existence of BD. Sudden variations in the system state (e.g., inrushes, faults and disconnection of loads or generators) may also lead to a mismatch between predicted and actual measurements. In some works in the literature (e.g. [131]), the discrimination between BD or other possible anomalies is performed by analyzing the skewness γ_t of the distribution obtained by the normalized innovation vector $\boldsymbol{\nu}_t^N$ and comparing it yet with another threshold γ_{max} (to be assessed off-line based on previous data-series):

$$\begin{cases} \text{Bad data} & \text{if } |\gamma_t| \geq \gamma_{max} \\ \text{Other anomaly} & \text{if } |\gamma_t| < \gamma_{max} \end{cases} \tag{4.7}$$

It is clear that more robust methods, that do not fully rely on customized thresholds, are needed. Additionally, the methods have to be able to distinguish between BD and variation in the system state, taking the proper countermeasures for the two cases. In order to overcome this limitation, the method described in the next section has been proposed by the authors in [79].

4.1.3 A pre-estimation filtering process of bad data for linear power system state estimators using PMUs

The section presents a pre-estimation method that examines the measurement innovations for each new received set of measurements in order to locate anomalies and apply countermeasures. The incoming measurement from a PMU is marked as reliable or not, according to a dynamic threshold defined as a function of the confidence of the predicted state estimated by using an ARIMA(0,1,0) process model. A fast and reliable heuristic boolean logic routine is provided to detect the presence of BD and discriminate it from measurements recorded during fault conditions. The detection and identification scheme is based on the following inputs: (i) the forecast state of the network obtained by means of a Kalman filter, (ii) the current network topology, (iii) the accuracy of the measurement devices and (iv) their location.

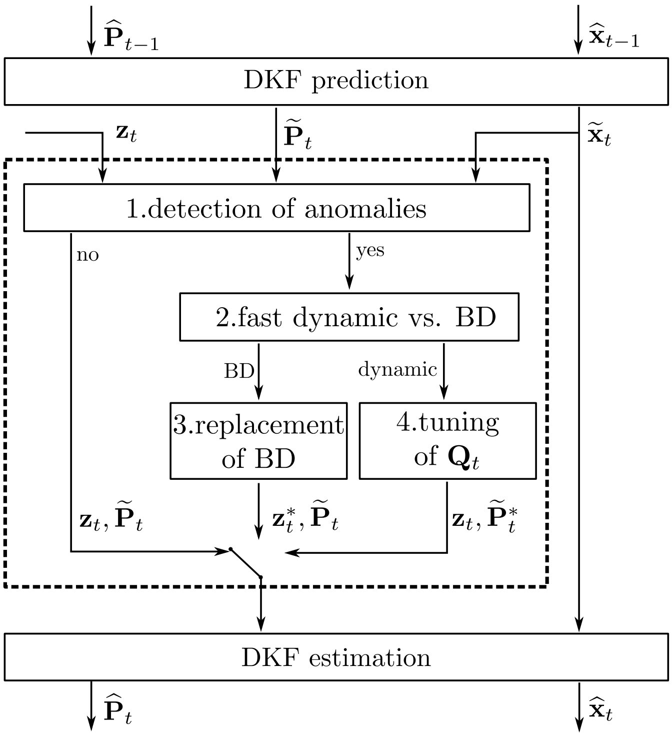

$\widehat{\mathbf{P}}_{t-1}$
$\widehat{\mathbf{x}}_{t-1}$
DKF prediction
$\mathbf{z}_t$
$\widetilde{\mathbf{P}}_t$
$\widetilde{\mathbf{x}}_t$
1.detection of anomalies
no
yes
2.fast dynamic vs. BD
BD
dynamic
3.replacement of BD
4.tuning of $\mathbf{Q}_t$
$\mathbf{z}_t, \widetilde{\mathbf{P}}_t$
$\mathbf{z}_t^*, \widetilde{\mathbf{P}}_t$
$\mathbf{z}_t, \widetilde{\mathbf{P}}_t^*$
DKF estimation
$\widehat{\mathbf{P}}_t$
$\widehat{\mathbf{x}}_t$

Figure 4.1 – Steps of the bad data algorithm process.

An analysis on the impact of single and multiple BD of different nature and magnitudes is given. Furthermore, the algorithm is also tested against faults to show its robustness and the help it provides to the state estimator during these peculiar operating conditions. The speed of the process itself is also taken into account since the BD processing is supposed to introduce a negligible time latency.

We suppose the measurements consist of phasors of bus voltages and nodal-injected current sent by a certain number of PMUs deployed in the network to guarantee its observability. We adopt the linear Discrete Kalman Filter (DKF) whose formulation is given in Section 3.1.2.

A set of measurements might differ from the expected ones for two main reasons: a sudden change in the system operating point or BD. Generally speaking, there might be errors in the meter-communication or in the network configurations (e.g. faulty switch breaker status information). The algorithm propose here only considers meter-communication errors and it is able to discriminate a BD from data recorded during a fault, a fast dynamic in the system or other unexpected conditions. The probability of simultaneous occurrence of a BD and a fault is assumed to be negligible.

The proposed BD method might be seen as a process inserted in between the prediction and estimation parts of the DKF. It is divided in four basic steps as shown in Fig. 4.1. In Step #1, called *detection of anomalies*, the innovation vector is checked against a specific threshold that is analytically defined in what follows. If one or more anomalies are detected, the algorithm goes to the second step, otherwise the estimator proceeds to the estimation part. In Step #2, *fast dynamic vs. BD*, the algorithm infers whether the previously identified anomaly is due to a sudden change in the network conditions (e.g., fault, inrush of a load, etc.) or to a set of incoming measurements affected by BD. In case a BD is identified, the algorithm proceeds to Step #3, *replacement of BD*, where the wrong measurement is substituted with its predicted value (pseudo-measurement), obtained by using the ARIMA (0,1,0) process model combined with the outcome of the DKF. When the anomaly is found to be due to a sudden change in the network state or a fault in a bus, the algorithm enters in Step #4, *tuning of* $\mathbf{Q}_t$ in order to help the estimator to keep track of the quickly changing state of the network.

Step #1: detection of anomalies

Let suppose the availability, at time-step $t-1$, of the a-posteriori estimated state $\widehat{\mathbf{x}}_{t-1}$ and its associated error covariance matrix $\widehat{\mathbf{P}}_{t-1}$. A BD is now inserted between time-step $t-1$ and t so that the set of measurement $\mathbf{z}_t$ is affected. By means of (3.26) and (3.27), $\widetilde{\mathbf{x}}_t$ and $\widetilde{\mathbf{P}}_t$ are obtained. The innovation vector, its covariance matrix and the normalized innovation vector can be then obtained as already shown in (4.4), (4.5) and (4.6), respectively. Thanks to the statistical properties of $\boldsymbol{\nu}_t^N \sim \mathcal{N}(0,1)$, it is now possible to define a threshold for each element of the normalized innovation vector that should not be exceeded during normal operating conditions. Therefore, each i^{th} element of $\boldsymbol{\nu}_t^N$ should satisfy the following equation:

$$|\nu_{t,i}^N| \leq \epsilon \tag{4.8}$$

where $|\nu_{t,i}^N|$ is the absolute value of the i^{th} element of the innovations $\nu_{t,i}$ and ϵ defines the confidence interval, usually taken equal to 3 or 4 for Gaussian noises. The definition of this threshold is close to the threshold usually set for LNR tests.

It is important to note that the use of bus voltage and nodal-injected current phasors establishes a linear relation between measurements $\mathbf{z}_t$ and state $\mathbf{x}_t$. Therefore, in the calculation of matrix $\mathbf{S}_t$ in equation (4.5), no approximations are introduced. This eliminates the need of augmenting the ϵ in order to include the approximations introduced by the linearization process as done, for instance, in [132].

The first step of the detection of anomalies is therefore to check each $\nu_{t,i}^N$ using (4.8) and raise a flag for those elements who do not satisfy it. In this way, the $\boldsymbol{\nu}_t^N$ is associated to a Boolean vector $\boldsymbol{\beta}_t$ that is filled with zeros or ones according to the absence or presence of anomalies, respectively.

Step #2: discrimination between fast dynamic and BD

The second step discriminates whether the previously identified anomalies are in fact BD or they are due to an unpredictable fast dynamic in the system. A reliable logic routine is implemented to distinguish between the two possibilities. The idea is simple: assuming that a sudden change in the system is occurring in a certain region of the network, an unexpected variation in correlated variables has to be detected by different PMUs, especially from those who are deployed in a region nearby the anomaly. Obviously, it is assumed that network topology and substations where the PMUs are installed, are known. A function takes as input the adjacency matrix[3] and the PMU locations and provides, for each PMU, the indices, in the normalized innovation vector $\boldsymbol{\nu}_t^N$, of the neighbor measurement devices. In this case, the term neighbor devices indicates the PMUs that are closer to the one whose measurements are under analysis. Each anomaly detected for bus voltage or nodal-injected current phasors in the Step #1, is then checked against the corresponding quantity of the neighbor PMUs. If at least one of the neighbor devices is recording the same anomaly, it is a symptom of the presence of a fast network dynamic at time-step t, otherwise the anomaly is marked as definitive BD. A simplified pseudo-algorithm that summarizes this process is provided in Algorithm 2.

Algorithm 2 Pseudo-algorithm for discrimination between BD and dynamics.

```
Input: PMU index $i$ at time $t$ such that $\beta_{t,i} \neq 0$
J = set of neighbors of $i$
if ($\exists j \in J, \beta_{t,j} \neq 0$) then
    $z_{t,i}$ = dynamic
else
    $z_{t,i}$ = bad data
end if
```

When the anomaly is detected on an injected current, the comparison described in Algorithm 2 is performed with the corresponding voltage phasors of the neighbor PMUs. This is due to the relatively low influence that a fast dynamic has on the injected currents whereas the voltage profile is more affected by sudden changes in the power flows.

Step #3: replacement of BD

The previous step has enabled the discrimination between BD and sudden changes in the operating point of the network. The measurements that have been identified as wrong, are simply replaced with their prediction avoiding to impact the observability of the system. The new set of measurements $\mathbf{z}_t^*$ (see Fig. 4.1) is fed to the estimation part

---

[3] In power system, the adjacency matrix provides an indication of which are the neighboring buses of each bus.

of the DKF. The variance associated to the pseudo-measurements is indeed larger than the one of the incoming set, because it includes the uncertainty added in the prediction step. Therefore, the outcoming $\widehat{\mathbf{P}}_t$, resulting from the state estimation at time-step t, will have larger values for those elements obtained by using the pseudo-measurements.

If the BD is not temporary, the uncertainty in the innovation terms, especially for those buses whose state is strongly based on the pseudo-measurements, will eventually be so large that a BD could fall again within the confidence interval that defines the acceptable measurements and, therefore, it could be fed again to the DKF. Concerning this point, it has to be clarified that the replacement of the corrupted measurement is advisable in presence of BD on a critical measurement. In all the other cases, the measurement can be safely discarded.

Step #4: tuning of process noise covariance matrix ($\mathbf{Q}_t$)

As anticipated, even when the anomalies are identified as originated by a fault, the algorithm has to take further actions before proceeding with the estimation part. As explained, the $\mathbf{Q}_t$ gives an indication of how much the DKF trusts its process model and thus its previous estimations. Provided that the process model is correctly defined, a diagonal $\mathbf{Q}_t$ with elements in the range $\left[10^{-4}, 10^{-10}\right]$ is usually selected (e.g., [95, 133]) meaning that high belief is given to the previous estimations to infer the next ones. A fault in the network, instead, eliminates completely the correlation between the previous estimation and the current state. In order to take into account the above considerations, it is necessary that, once a fault is detected, the elements of the $\mathbf{Q}_t$ are increased to values large enough[4] to strongly rely on the measurements only until the estimator has tracked the new faulty state. At that point, the $\mathbf{Q}_{t+n}$ can be decreased again to the pre-fault values trying to re-enhance the accuracy of the estimation. An appropriate value of n for a BD process coupled with PMUs and a DKF working at 50 fps is $n \geq 3$.

After having detected a fault and increased the $\mathbf{Q}_t$, the BD algorithm, has also to compute an updated version of the a-priori estimated covariance $\widetilde{\mathbf{P}}_t^*$ (see Fig. 4.1) that incorporates the changes in the $\mathbf{Q}_t$ matrix. The set of measurements can then be forwarded to the estimation part of the DKF.

4.1.4 Performance evaluation

The performances of the pre-estimation filtering of BD are tested on a fully unbalanced distribution network based on a modified version of the IEEE 13-bus test feeder [135] shown in Fig. 4.2. The choice of a distribution system rather than a transmission network is driven by the increasing interest the PMUs are raising when installed in the

---

[4] Note that the assessment of the most suited value of $\mathbf{Q}_t$ during sudden changes is addressed in [134].

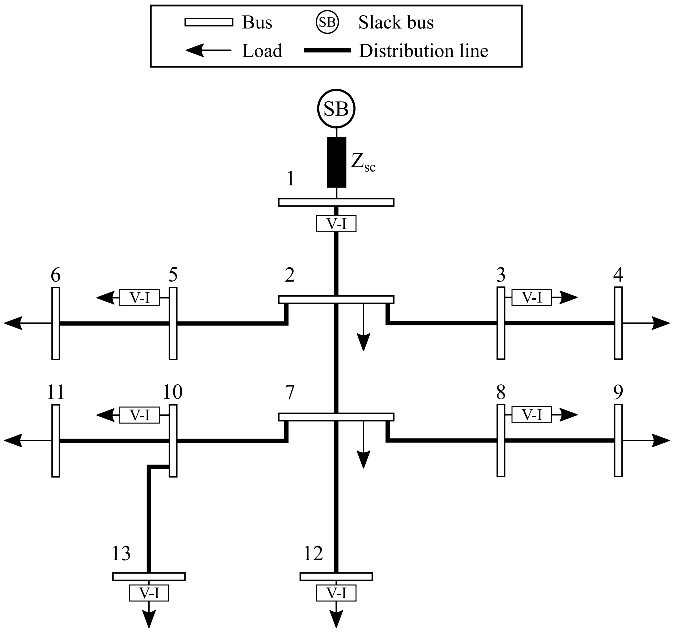


Figure 4.2 – The simulated IEEE 13-bus distribution test feeder.

challenging active distribution networks context (e.g.,[136]). From the point of view of the algorithm definition, there are no differences when dealing with transmission or distribution networks. Differently from what it is defined in [135], here the network rated voltage is assumed to be 15 kV, the lines are unbalanced and correspond to the #602 line conductor configuration of [135]. With reference to Fig. 4.2, bus #1 represents the connection to the sub-transmission network. This point is modeled as an ideal generator imposing the nominal voltage and frequency in series with its internal short-circuit impedance ($S_{sc} = 300$ MVA, balanced $R_{sc}/X_{sc} = 0.1$).

The network is implemented inside a phasor-domain simulator to reproduce different test conditions and save the corresponding *true* phasors of voltage and currents (see Chapter 5.1 for details about the real-time simulation platform). The sets of measurements are saved every 20 ms, so that it is possible to simulate incoming synchrophasors streamed at 50 fps from a certain number of PMUs deployed in the field. A Gaussian noise with zero mean is added to the measurements in order to simulate the use of class 0.1 CT and VT as described in [36] and [37]. The noise added by the PMUs is neglected since it is a few orders of magnitude smaller than the one added by the sensors [39]. For this reason the PMU's accuracy is not inserted in the model of the system. As for the measurements, also the true state of the network is saved every 20 ms in order to allow an offline accuracy assessment of the SE performances when pseudo-measurements are inserted in the DKF process. The power profiles of loads and DGs are unbalanced and they come from measurements taken in a real distribution network located in the South-East region of Switzerland. Data refers to residential and commercial buildings for the loads and PVs and mini-hydro power plant for the DGs.

Tests are run with the network in normal operating conditions and also when affected by fast dynamics like the ones characterizing single or multi-phase faults. The algorithm has to identify the eventual presence of single or multiple BD during the normal operating conditions, and detect the sudden change in the network state in case of faults without replacing the unexpected, but correct, received measurements.

Both DKF and the BD algorithm here presented are fully implemented in LabVIEW. A library of potential BD is developed in order to simulate the meter devices behavior when affected from several types of BD. The library includes: offset in magnitude and phase for each phasor of every PMU, single or multiple packet losses from one or more PMUs due to communication failures, drift in the phase estimation that might affects PMUs after the loss of the absolute time reference, etc.

A total of 7 PMUs are assumed to be installed in bus #1, #3, #5, #8, #10, #12, #13 and every PMU estimates 6 synchrophasors (three nodal voltages phasors and three injected/absorbed nodal current phasors). This number of PMUs guarantees the observability of the system. For simulation purposes, this number of PMUs, together with the absence of other meters, creates a system with very low redundancy: removing only one PMU from the set, would make the system not fully observable. We have decided to use this critical measurement configuration since no PMU data can be dropped without losing the observability of a certain area of the network. The importance of an effective replacement in case of a telecommunication system failure is therefore highlighted. The matrix $\mathbf{R}_t$ is diagonal and it is assumed to be constant. Each element is equal to $0.1 \cdot 10^{-6}$ that corresponds to the variance of real and imaginary part of the current and voltage sensor measurements [36, 37]. The elements of matrix $\mathbf{Q}_t$ are set to 10^{-9} during normal operating conditions, following a probabilistic assessment of the process-noise covariance matrix described in [95].

The algorithm is tested against several scenarios of BD present in everyday life of power systems. Some characteristic results are reported in what follows. All the plots are shown in per unit with reference to the following base voltage and current values: $V_b = 15$ kV, $I_b = 666.6$ A.

Gross errors

This test simulates a temporary communication failure from the PMU placed in bus #1. At time $t = 0.5$ s, all the information coming from bus #1 is lost and the communication is supposed to be re-established after 1 s. The gross BD is identified with no delay and replaced with pseudo-measurements. Fig. 4.3 shows the replacement for real and imaginary part of the voltage phasors of phase *c*. A similar behavior is recorded for all the missing synchrophasors. As it can be seen, the replacement with pseudo-measurements, increases the confidence interval for which an incoming measurement

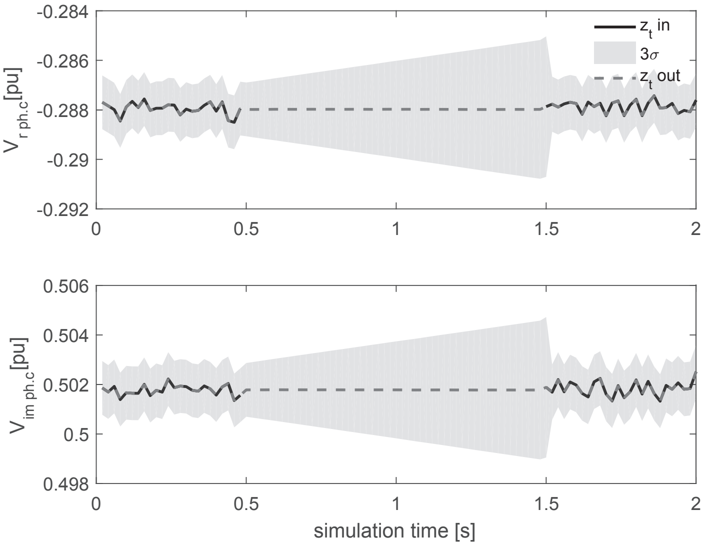


Figure 4.3 – Replacement of synchrophasors due to temporary communication failure. The grey area represents the 3σ confidence interval.

is defined as acceptable or not. This is due to the growing uncertainty associated to the pseudo-measurements when they are constantly replacing the missing ones.

Fig. 4.4 shows the absolute value of the error in the estimation of the real and imaginary components of the state for the bus affected by the specific BD and its neighbors. The error is plotted as a function of the bus position and the simulation time. The packets are missing between the two red dotted lines. As it can be noticed, the replacement does not worsen the accuracy in the estimated state for all the surrounding buses since the errors of the estimated state after the BD event are comparable with the ones before the event.

In case of damage of one of the PMU's components, the device can stream synchrophasors largely different from the real ones. This scenario was also tested and the algorithm performs well even in this case without affecting the quality of the estimations for the neighbor buses.

Small deviations

The algorithm is able to identify and detect BD even when the deviation from the true value is small. Fig. 4.5 shows a temporary offset of 0.004 p.u. in the voltage magnitude of phase *b* streamed by the PMU in bus # 10. The BD is properly detected and replaced.

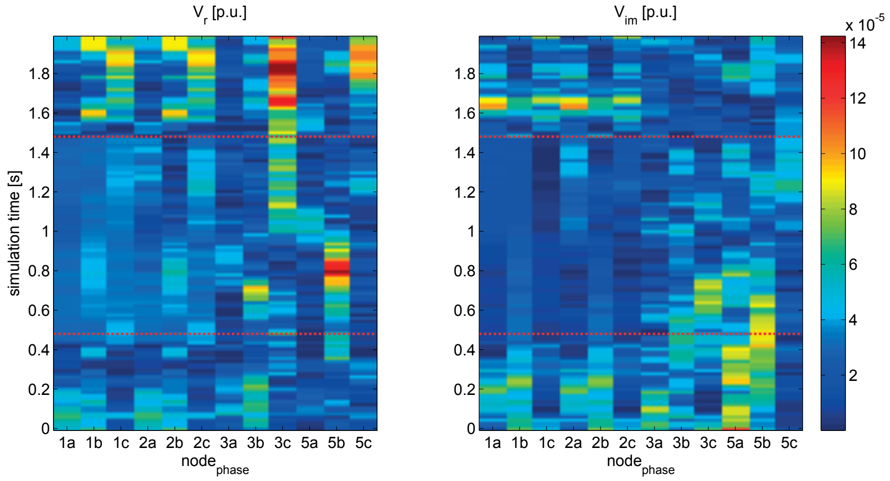


Figure 4.4 – Missing packets: Absolute value of the estimation error for real and imaginary part in bus #1 and its neighbor buses.

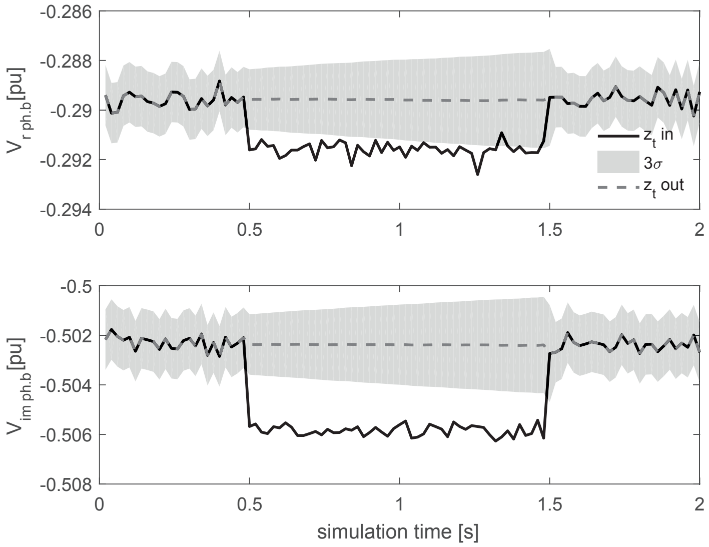


Figure 4.5 – Phasors replacement due to an offset in the voltage magnitude value.

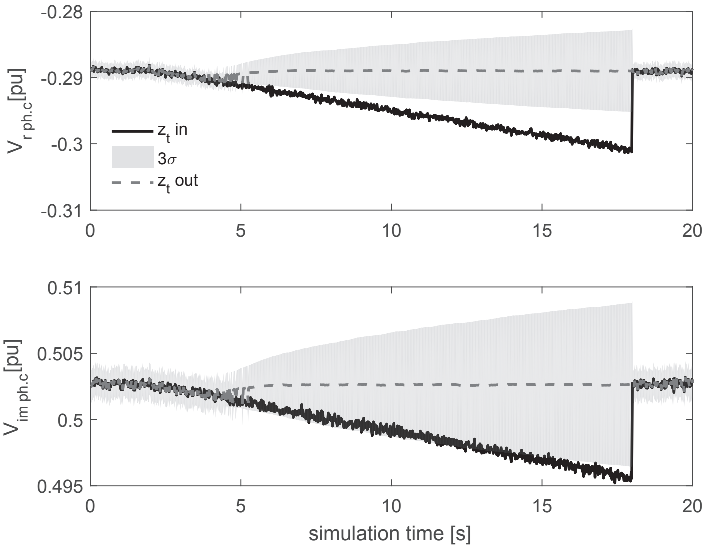


Figure 4.6 – Detection of a phase drift in bus #10 due to loss of time synchronization.

Phase Drift

This is a BD specific for PMUs that could appear when the device loses its time synchronization due to unintentional or intentional interference. The BD causes a phase drift in all the synchrophasors estimated by the PMU. In this specific case, the PMU deployed in bus #10 is supposed to be affected by a deviation in the estimated phases of 1.5 mrad/sec. The drift begins at time $t = 2$ s and it continues until $t = 18$ s when the PMU is re-synchronized with a valid absolute time source. As shown in Fig. 4.6, for the first two seconds, the BD does not detect the anomaly since the obtained residuals are within the bounds defined by (4.8). As soon as this condition is not satisfied, i.e. at $t = 4$ s, the BD is correctly identified. Due to the slow deviation, the identification is not immediate and this results in a temporary worsening in the accuracy of the estimated state, especially for bus #10 and #11 as shown in Fig. 4.7. The replacement of the wrong measurements brings the accuracy back to its usual values even if the PMU is still not time-synchronized.

Multiple BD

The presence of multiple BD coming from a single or several PMUs is also simulated. The algorithm correctly identifies and replaces them as long as they are not highly correlated. In fact, the simultaneous presence of BD on the same phasor quantities in two or more PMUs belonging to the same region, might deceive the algorithm of the existence of a fast dynamic in the region itself. It should be noted that such concurrent events are not likely to happen, if not intentionally.

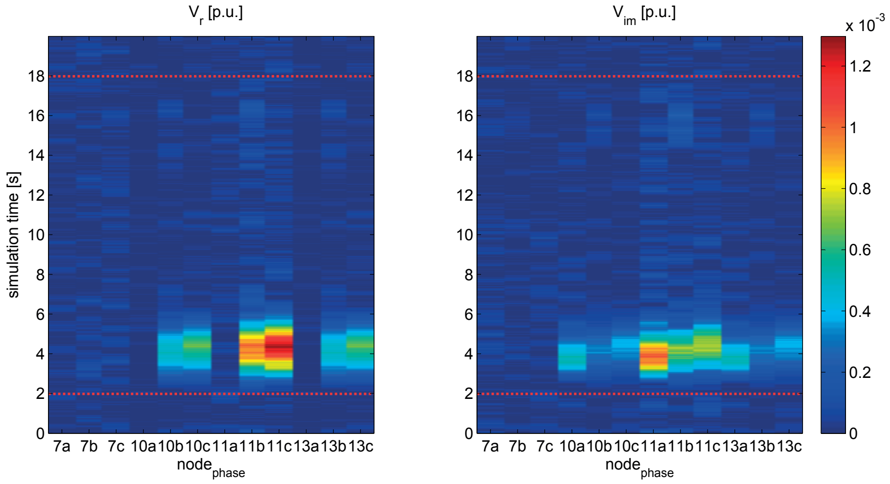


Figure 4.7 – Phase drift: Absolute value of the estimation error for real and imaginary part in bus #10 and its neighbor buses.

Tracking of faults

Tests with single and multi-phase faults on different buses are performed to check whether the BD algorithm takes the proper countermeasures described in Section 4.1.3. The case illustrated in Fig. 4.8 consists in a 3-ph fault on bus #7 with a fault impedance of $1\ \Omega$. The fault begins at time $t = 1$ s and it is assumed to be cleared after 500 ms. As it can be seen, the fault is correctly distinguished from a BD since it is not classified as such. The process noise covariance matrix $\mathbf{Q}_{t=1\text{s}}$ is increased to an appropriate value for $n = 3$ iterations and then it is set back to the original value of 10^{-9}. The same happens at $\mathbf{Q}_{t=1.5\text{s}}$. Thanks to this expedient, the SE keeps following the state, with only a slight worsening in the accuracy performance immediately after the begin and the end of the 3-ph fault. This test is repeated for different faults types and fault impedances with the same positive results.

Timing assessment

Fig. 4.9 shows the cumulative distribution function (CDF) of the time added by the BD process here described (red line) and also the CDF of the whole process (prediction, BD assessment and estimation). The test was run on a Intel core i7, 8GB of RAM. This result is only indicative and shows that BD detection obviously adds a latency to the SE. It can be seen that the latency is approximately one third of the total time that is taken to perform the complete estimation. The specific figure refers to the test where complete sets of incoming measurements are lost, and therefore replaced with pseudo-measurements, for one second. Obviously, the latency for both SE and BD algorithm is proportional to the number of measurements to be processed. In addition, the latency of the BD layer is also slightly dependent on the number of BD which are

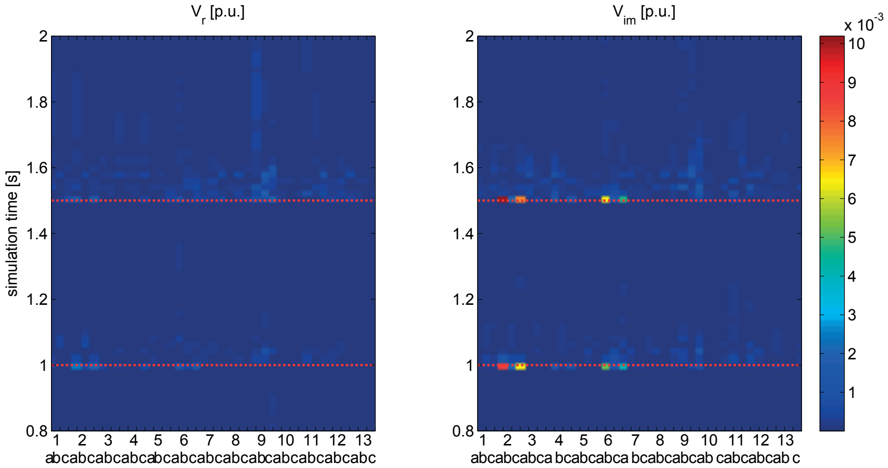


Figure 4.8 – Absolute value of the estimation error for real and imaginary part in every bus, during a 3-ph fault at bus #7.

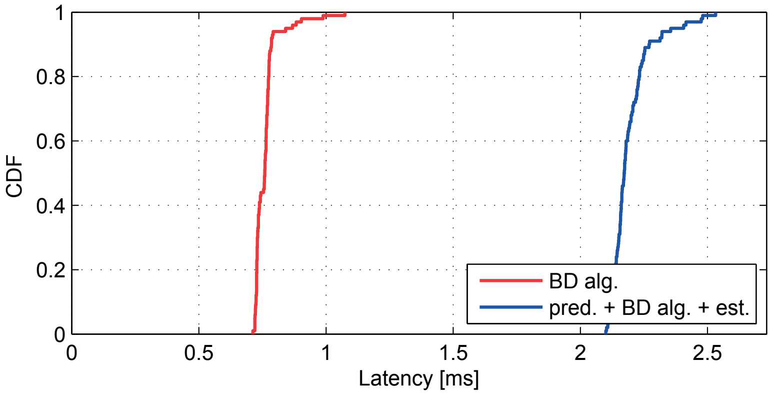


Figure 4.9 – CDF of the time latencies for the BD algorithm and the whole SE process.

not likely to occur simultaneously.

Conclusion

A pre-estimation filtering process of bad for PMU-based linear state estimators has been discussed and validated. The proposed algorithm is coupled with a DKF state estimator that uses only PMU measurements. The detection of potential anomalies relies on a set of dynamic thresholds inferred by predicted measurements using an ARIMA (0,1,0) process combined with the outcome of the adopted DKF state estimator. If a potential bad data is detected, it is compared with adjacent PMU data in order to verify whether it is a real bad data or a non-predictable fast dynamic appearing in the network (for instance, a fault). Additionally, we provided a way to replace the bad data with pseudo-measurements obtained by a prediction process fed by the state estimation itself. The variance associated to these pseudo-measurements is computed using the a-priori error covariance of the DKF. The algorithm is validated against single and multiple bad data of different nature and magnitudes, namely: gross errors, small synchrophasors-magnitude deviations and synchrophasors phase-drifts. Furthermore, the algorithm has been tested against faults to show its robustness during these unexpected operating conditions. The performance assessment of the proposed algorithm allows to conclude that it appears robust and compatible with the real-time nature of the considered state estimation process enabling the use of this functionality also to observe fast network dynamics.

As a final remark, we would like to point out that the algorithm here presented does not rely on any statistical property of the residuals. For this reason, the algorithm is agnostic to the existence of critical measurements, differently from the methods presented in Section 4.1.1.

4.2 Undetectable timing attack on linear state-estimation by using rank-1 approximation

The content of this section is based on what published in [137]. As discussed in Chapter 2, smart-grid applications based on synchrophasor measurements strongly rely on the usage of a proper time synchronization technology and are vulnerable to timing attacks. A fundamental question is whether timing attacks could remain undetected by bad-data detection (BDD) algorithms used in conjunction with state-of-the-art situation-awareness state estimators. In this section, we analyze the detectability of timing attacks on linear state-estimation. We show that it is possible to forge delay attacks that are undetectable. We give a closed form for an undetectable attack; it imposes two phase offsets to two or more synchrophasor-based measurement units that can be translated to synchrophasors' time delays. We also propose different methods for combining two-delays attacks to produce a larger impact. We simulate the attacks on a benchmark power-transmission grid, we show that they are successful and can lead to physical grid damage. To prove undetectability, we use classic BDD techniques such as the largest normalized residual (LNR) and the χ^2-test, described in Section 4.1.

Recent works show that both GPS and packet-based time-synchronization protocols (PBTSPs) can be attacked (e.g., [56, 138]). As civilian GPS satellite signals are not authenticated, they can be spoofed by superimposing a fake signal with a higher signal-to-noise ratio, which would enable an attacker to manipulate a GPS clock [56]. In the case of PBTSPs, an attacker could inject a malicious offset in the time signal by delaying messages, which is feasible because in any PBTSP it is impossible to measure asymmetries in the propagation delay [139]; for this reason, any notion of asymmetry needs to be provided to the protocol (e.g., PTPv2 assumes that propagation delays are symmetric). As the attack involves only delaying messages, such an attack would work even if synchronization messages are encrypted and/or authenticated.

In what follows, we analyze the effect of tampering with the common time reference of PMUs used for linear state estimation of a transmission network, applying the well-known WLS. We show that by manipulating the time reference only, it is possible to perform an attack that does not change the measurement residuals, and thus it bypasses the BDD methods used in state-of-the-art state estimators. We show that a successful attack requires tampering with at least two different angles, and we provide a method to compute attacks that maximize damage while remaining undetectable. We illustrate the findings with respect to a PMU-based linear state-estimator applied to the 39-bus IEEE-benchmark power system. We demonstrate that in given transmission lines, the attack can produce a large mis-estimation of the power flows while passing the χ^2 and LNR tests.

Our work assumes that the only manipulation concerns the time reference used by PMUs. As shown for example in [140], such attacks may be possible without compromising any cryptographic security system. To the best of our knowledge, there is no work that addresses how to perform an undetectable attack on linear state-estimators by maliciously manipulating only the time reference of a set of PMUs.

4.2.1 System Model

State Model

We consider a one-phase direct-sequence equivalent of a three phase transmission network with N_b buses, and we let $\mathcal{N}$ be the set of all buses (with $N = N_b$ elements). The system state is $x \in \mathbb{C}^N$. We assume nodal injected-current phasors and/or nodal voltage-phasors measurements coming from PMUs only. We count separately measurements for voltages and for currents. At a bus where both voltage and current are measured, we count two measurement points; at a bus where only voltage (resp. current) is measured, there is a single measurement point. We denote by $\mathcal{M}^V \subseteq \mathcal{N}$ the set of measurement points for voltage, and by $\mathcal{M}^I \subseteq \mathcal{N}$ the set of measurement points for nodal currents. Let $\mathcal{M} = \mathcal{M}^V \cup \mathcal{M}^I$ be the set of all measurement points, and $M = |\mathcal{M}|$. The measurement vector is $z \in \mathbb{C}^M$.

Let Y be the $(N \times N)$ single-phase complex admittance-matrix, and H be the $M \times N$ complex measurement matrix. We have

$$\begin{aligned} H_{m,m} &= 1,\ m \in \mathcal{M}^V \\ H_{m,n} &= 0,\ m \in \mathcal{M}^V, m \neq n \\ H_{m,n} &= Y_{m,n},\ m \in \mathcal{M}^I, n \in \mathcal{N}. \end{aligned}$$

The measurement model is recalled in equation

$$z = Hx + e, \tag{4.9}$$

where $x \in \mathbb{C}^N$ is the system state, $e \in \mathbb{C}^M$ is the complex measurement-error with a distribution discussed in Section 4.2.5. Define the verification matrix F as

$$F \triangleq H(H^\dagger H)^{-1}H^\dagger - I \tag{4.10}$$

We denote with $H^\dagger$ the conjugate transpose of H. Note that $Fz = 0$ if and only if there exists some state x with $z = Hx$. If $Fz = 0$, there is a unique complex vector x that solves $z = Hx$ and it is given by $x = (H^\dagger H)^{-1}H^\dagger z$. In general (i.e., when $Fz \neq 0$), $x = (H^\dagger H)^{-1}H^\dagger z$ is the least-square estimator of the state. Note that we assume that the state estimation uses the WLS in rectangular coordinates instead of complex numbers. The reason for using complex numbers becomes apparent in the next sections, where we find closed form expressions that could not be found otherwise.

Attack Model

The goal of the attacker is to create a mis-estimation of the state of the grid while maintaining the residuals of the state-estimator unaffected. As illustrated by the attack in Fig. 4.10, this goal can be achieved using various attack vectors. We consider an attacker that is an insider to the utility, thus he has access to the network topology and to the admittance matrix, but he is not able to physically tamper with any PMU or transducer (sensor). We assume the attacker is able to observe, but cannot forge the measurement vector z, which is consistent with the security standards for synchrophasor data transmission, as those mandate only authentication but not encryption [141]. We thus consider that the attacker can add an offset to the time reference of some PMUs, which will be seen as an offset in the synchrophasor estimation. An attack against the time reference can be done with moderate effort for both PTP and GPS synchronization schemes [142]. For the case of PTP, many overhead lines contain an optical fiber with physical layer repeaters placed every few kilometers on the line poles, and it is also common to have unmanned facilities with repeaters. For an attacker it would be sufficient to disconnect a cable and to insert a delay box to attack PTP [140]. In the case of GPS, spoofing GPS transmitters can be built from low-cost components and can be coordinated easily [56, 143].

As a result of the attack, the PMU shifts the time window for which the synchrophasor is computed. Therefore, besides the incorrect estimation of the phase, the attack affects the estimation of the phasor's amplitude, the frequency of its main tone and the ROCOF estimation. As we are considering a transmission network, it follows that the estimation of the phase angle is the one that is most affected by the attack, thus this is the only error we consider in this manuscript.

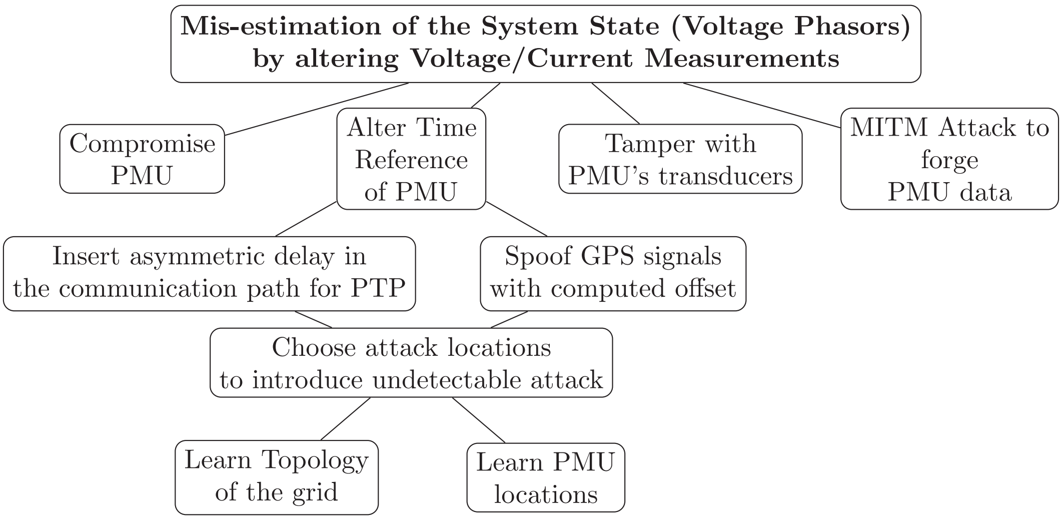

Mis-estimation of the System State (Voltage Phasors) by altering Voltage/Current Measurements
Compromise PMU
Alter Time Reference of PMU
Tamper with PMU's transducers
MITM Attack to forge PMU data
Insert asymmetric delay in the communication path for PTP
Spoof GPS signals with computed offset
Choose attack locations to introduce undetectable attack
Learn Topology of the grid
Learn PMU locations

Figure 4.10 – Attack-tree for attacking the time reference of a PMU measurement infrastructure.

4.2.2 Undetectable Time-Synchronization Attacks

In what follows we present a theory of undetectable attacks, which forms the basis for the practical methods presented in Sections 4.2.3 and 4.2.4.

Absolutely Undetectable Attack

Let p be the number of time references manipulated by the attacker, α_i the i^{th} phase angle difference between the attacked and the original synchrophasor measurement and $\mathcal{A}_i$ the set of measurement points to which the angle difference α_i is imposed, $i = 1{:}p$.

For all $m \in \mathcal{M}$, define $\Delta z_m = z'_m - z_m$ where z_m is the value of the m^{th} measurement that would be obtained if there would be no attack and z'_m is the value obtained when the timing attack is present. We have:

$$\begin{aligned}
\Delta z_m &= z_m(u_i - 1), \ \text{if } m \in \mathcal{A}_i \\
\Delta z_m &= 0, \ \text{if } m \in \mathcal{M} \setminus \bigcup_i \mathcal{A}_i \\
\text{with } u_i &= \cos\alpha_i + j\sin\alpha_i = e^{j\alpha_i}, \ i = 1{:}p.
\end{aligned}$$

By the definition of F, an attack that produces a change $\Delta z = (\Delta z_m)_{m=1:M}$ to the true observation vector z is absolutely undetectable if and only if

$$F\Delta z = 0. \tag{4.11}$$

Let Ψ be the attack-measurement indicator matrix, defined by

$$\Psi_{m,i} = 1 \text{ if } m \in \mathcal{A}_i \text{ and } \Psi_{m,i} = 0 \text{ otherwise,} \tag{4.12}$$

with $m = 1{:}M$ and $i = 1{:}p$. Then Δz can be re-written as

$$\Delta z = (u_1 - 1) \operatorname{diag}(z)\Psi_{:,1} + ... + (u_p - 1) \operatorname{diag}(z)\Psi_{:,p} \tag{4.13}$$

where $\Psi_{:,i}$ denotes the i-th column of matrix Ψ and diag(z) is the $M \times M$ diagonal matrix with diag$(z)_{m,m} = z_m$. By (4.11), the attack α is absolutely undetectable if and only if

$$\sum_{i=1}^{p}(u_i - 1)F \operatorname{diag}(z)\Psi_{:,i} = 0. \tag{4.14}$$

We can make (4.14) more tractable by introducing the *attack-angle matrix* W, which is a $p \times p$ hermitian-complex matrix defined as

$$W \triangleq \Psi^T \operatorname{diag}(z)^\dagger F^\dagger F \operatorname{diag}(z)\Psi \tag{4.15}$$

or in other words

$$W_{i,j} = \sum_{l,m,n\in\mathcal{M}} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m \tag{4.16}$$

with $i, j = 1{:}p$. We use $\bar{F}_{n,l}$ to denote the conjugate of $F_{n,l}$. Note that the dimension of the matrix W is $p \times p$, where p is the number of different delays imposed by the attack; it is particularly interesting to use W when p is small.

Theorem 1. *The attack* $\alpha = (\alpha_1, \dots, \alpha_p)$ *is absolutely undetectable if and only if*

$$W(\vec{u} - \vec{1}) = 0 \tag{4.17}$$

with $\vec{u} = (u_1, ..., u_p)^T, \vec{1} = (1, ..., 1)^T$.

Proof. First recall that the attack is absolutely undetectable if and only if equation (4.14) holds. Second, we prove that for any complex vector $y \in \mathbb{C}^p$:

$$Wy = 0 \Leftrightarrow F \operatorname{diag}(z)\Psi y = 0. \tag{4.18}$$

The $\Leftarrow$ side of the implication directly follows from the definition of W. Conversely, assume that $Wy = 0$ for some $y \in \mathbb{C}^p$. Then

$$\begin{aligned} \Psi^T \operatorname{diag}(z)^\dagger F^\dagger F \operatorname{diag}(z)\Psi y = 0 \\ \Rightarrow y^\dagger\Psi^T \operatorname{diag}(z)^\dagger F^\dagger F \operatorname{diag}(z)\Psi y = 0 \\ \Rightarrow \|F \operatorname{diag}(z)\Psi y\|^2 = 0 \\ \Rightarrow F \operatorname{diag}(z)\Psi y = 0 \end{aligned}$$

In the above, $\|\cdot\|$ denotes the ℓ^2 norm, defined for $y \in \mathbb{C}^p$ by $\|y\| = \sqrt{\sum_{i=1}^{p} |y|_i^2}$. □

Timing attack with a single delay ($p = 1$)

Consider that the attacker can only induce a single delay, i.e., $p = 1$ and $\alpha = (\alpha_1)$. Then the matrix W is a single complex number $W = (W_{1,1})$, and Theorem 1 becomes

$$W_{1,1}(u_1 - 1) = 0 \tag{4.19}$$

with $W_{1,1} = \sum_{l,m \in \mathcal{A}_1, n \in \mathcal{M}} \bar{F}_{n,l} F_{n,m} \bar{z}_l z_m$. It is very unlikely that $W_{1,1} = 0$, thus undetectability requires $u_1 = 1$ (i.e. $\alpha_1 = 0$), namely there is no attack. Thus this case is of no interest.

Timing attack with two delays ($p = 2$)

Consider now that the attacker can induce two delays (e.g., with two GPS coverage zones or two different communication paths in a PTP network), i.e., $p = 2$ and $\alpha = (\alpha_1, \alpha_2)$. Observe that for $p = 2$ the matrix W is 2×2, and Theorem 1 becomes

$$\begin{aligned} W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) &= 0 \\ W_{2,1}(u_1 - 1) + W_{2,2}(u_2 - 1) &= 0. \end{aligned}$$

Before we formulate our theorem, we propose the following Lemma.

Lemma 1. *Let $a, b \in \mathbb{C}$. If $a + b \neq 0$ then the solutions of the system of equations*

$$\begin{cases} a(u-1) + b(v-1) = 0 \\ |u| = |v| = 1 \end{cases}$$

with unknowns $u, v \in \mathbb{C}$ are

$$u = v = 1 \text{ and } u = \frac{\bar{a}(a+b)}{a(\bar{a}+\bar{b})}, \quad v = \frac{\bar{b}(a+b)}{b(\bar{a}+\bar{b})}.$$

If $a + b = 0$, there are infinitely many solutions, given by $u = v$, $|u| = 1$.

Proof. We can interpret the system of equations as follows. Denote with S^1 the unit circle in the complex plane, i.e., $S^1 = \{u \in \mathbb{C}, |u| = 1\}$. When $u \in S^1$, $z = a(u-1)$ is a point in the circle of center $-a$ and radius $|a|$; similarly, $z = -b(v-1)$ is a generic point in the circle of center b and radius $|b|$. Solutions to the equations are given by the intersection of these two circles, if they intersect. Now they intersect because $u = v = 1$ is a solution. Therefore, there is exactly one other solution, except in the special case where the two circles are tangent or when the two circles are identical. □

Theorem 2. *For $p = 2$, if rank$(W) = 1$ there is one non-trivial absolutely undetectable attack vector $\alpha = (\alpha_1, \alpha_2)$, given by*

$$\begin{aligned} \alpha_1 &= 2\arg(W_{1,1} + W_{1,2})(\textit{mod}\, 2\pi) \\ \alpha_2 &= -2\arg(W_{1,2}) + 2\arg(W_{1,1} + W_{1,2})(\textit{mod}\, 2\pi) \end{aligned} \tag{4.20}$$

Proof. With rank$(W) = 1$, the system of equations derived from Theorem 1 is equivalent to

$$W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) = 0 \tag{4.21}$$

where the unknowns are $u_1, u_2 \in \mathbb{C}$ with the constraints $|u_1| = |u_2| = 1$. This system of equations can be precisely solved by applying Lemma 1 to (4.21) and obtain a single non-trivial attack, given by

$$\begin{aligned} u_1 &= \frac{W_{1,1} + W_{1,2}}{W_{1,1} + \bar{W}_{1,2}} \\ u_2 &= \frac{\bar{W}_{1,2}(W_{1,1} + W_{1,2})}{W_{1,2}(W_{1,1} + \bar{W}_{1,2})} \end{aligned}$$

from where we derive the attack vector α, using the fact that $W_{1,1}=\bar{W}_{1,1}$ because W is hermitian. □

For the case rank$(W) = 2$, there is only one solution $u_1 = u_2 = 1$, i.e., there are no absolutely undetectable attacks.

As we show next, Theorem 2 forms the basis for practical attacks because, even when W is full rank, it can often be well approximated by a rank-1 matrix.

4.2.3 Practically undetectable attack with two delays

In this section we describe a strategy for performing a practically undetectable attack when W is full rank and $p = 2$. We assume that each attacking-angle affects a single PMU, i.e., we attack two PMUs in total. In [144] it is shown that attacking at least two PMUs is enough to perform an undetectable attack.

Attack based on Rank-1 matrix approximation

Recall that the W matrix is hermitian, thus we can diagonalize W as $W = U\Lambda U^\dagger$, with $UU^\dagger = U^\dagger U = I$ and Λ is a diagonal matrix with real, nonnegative and descending-ordered eigenvalues. Let us construct $\tilde{\Lambda} = \mathrm{diag}\,(\Lambda_{1,1}, 0)$, with $\Lambda_{2,2} = 0$ and we define $\tilde{W} = U\tilde{\Lambda}U^\dagger$, i.e., we replace the smallest eigenvalue by 0. The approximate attack is one that satisfies

$$\tilde{W}(\vec{u}-\vec{1})=0, \tag{4.22}$$

and the attack vector α is then given by (4.20) with $\tilde{W}$ in lieu of W.

The IoS criterion

The effectiveness of using $\tilde{W}$ instead of W depends on the value of $\Lambda_{2,2}$ and whether or not zeroing this value is a good approximation. To investigate this, we use the index of separation (IoS) of the matrix W, which is classically defined as

$$\text{IoS}=\frac{\lambda_{\max}}{\sum_i \lambda_i}=\frac{\Lambda_{1,1}}{\Lambda_{1,1}+\Lambda_{2,2}}. \tag{4.23}$$

We obtain the two eigenvalues of W as roots of the characteristic polynomial:

$$\Lambda_{1,1}=\frac{1}{2}\left(\operatorname{trace}(W)+\sqrt{\operatorname{trace}(W)^2-4\det(W)}\right)$$
$$\Lambda_{2,2}=\operatorname{trace}(W)-\Lambda_{1,1}$$

and using $\Lambda_{1,1}$ and $\Lambda_{2,2}$ in (4.23) we get

$$\text{IoS}=\frac{1}{2}+\frac{1}{2}\sqrt{1-4\frac{\det(W)}{\operatorname{trace}(W)^2}}. \tag{4.24}$$

Note that for an attack with two delays ($p=2$), IoS(W) $\in[0.5,1]$ and IoS(W) $=1 \implies$ rank(W) $=1$.

An attacker should therefore look for attack locations such that IoS(W) ≈ 1. In general, for a given choice of locations, IoS(W) depends on the measurement vector z; however, it is possible to avoid this dependency by computing the *minimum index of separation* (IoS*), defined as the minimum value of IoS(W) taken over all values of $z\in\mathbb{C}^M$. If IoS$^*\approx 1$ for a given choice of locations, then the delay attack given by (4.20) with $\tilde{W}$ in lieu of W is undetectable, regardless of the value of the measurements. The following theorem provides a closed-form expression for IoS*.

Theorem 3. *For an attack with two delays ($p=2$), and one attacked measurement point per delay ($\mathcal{A}_1=\{z_1\}$ and $\mathcal{A}_2=\{z_2\}$), the minimum index of separation (IoS*) is equal to*

$$IoS^*=\frac{1}{2}+\frac{|f_{12}|}{2\left(f_{11}f_{22}\right)^{\frac{1}{2}}} \tag{4.25}$$

with

$$f_{i,j}=\sum_{l,m}\sum_{n}\Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m} \tag{4.26}$$

where Ψ is defined as in (4.12)*. Note that IoS* depends only on the measurement matrix*

H and the location of the attacked PMUs.

Proof. We want to find the minimum of (4.24). First we need to compute the elements $W_{i,j}$ of W to find $\det(W)$ and $\operatorname{trace}(W)$ as a function of attacked measurements z_1 and z_2. We use (4.16) with $p = 2$ and one attacked measurement per delay

$$\begin{aligned}
W_{1,1} &= \sum_{l,m,n} \Psi_{l,1}\Psi_{m,1}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = |z_1|^2 f_{11}\\
W_{1,2} &= \sum_{l,m,n} \Psi_{l,1}\Psi_{m,2}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = \bar{z}_1 z_2 f_{12}\\
W_{2,1} &= \sum_{l,m,n} \Psi_{l,2}\Psi_{m,1}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = \bar{z}_2 z_1 f_{21}\\
W_{2,2} &= \sum_{l,m,n} \Psi_{l,2}\Psi_{m,2}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m = |z_2|^2 f_{22}.
\end{aligned} \tag{4.27}$$

The trace and determinant of W are given by

$$\begin{aligned}
\operatorname{trace}(W) &= |z_1|^2 f_{11} + |z_2|^2 f_{22}\\
\det(W) &= |z_1|^2 f_{11} |z_2|^2 f_{22} - |z_1|^2 |z_2|^2 f_{21} f_{12}\\
&= |z_1|^2 |z_2|^2 \left(f_{11} f_{22} - |f_{12}|^2\right).
\end{aligned} \tag{4.28}$$

Note that $f_{21} f_{12} = |f_{21}|^2 = |f_{12}|^2$. Using (4.24) and (4.28) we can express the problem as

$$\min_{z_1, z_2} \quad \frac{1}{2}\sqrt{1 - 4\frac{|z_1|^2|z_2|^2\left(f_{11}f_{22} - |f_{12}|^2\right)}{\left(|z_1|^2 f_{11} + |z_2|^2 f_{22}\right)^2}}. \tag{4.29}$$

Note that the objective function can be simplified if we substitute $s = \frac{|z_2|^2}{|z_1|^2}$ in (4.29), which brings

$$\min_{s} \quad \frac{1}{2}\sqrt{1 - 4\frac{s\left(f_{11}f_{22} - |f_{12}|^2\right)}{\left(f_{11} + s f_{22}\right)^2}}.$$

By analyzing the sign of the derivative with respect to s we find a minimum when $s = \frac{f_{11}}{f_{22}}$, and substituting this in (4.24) we obtain the value of IoS* given in the theorem. □

Theorem 3 can be used to find pairs of PMUs that can be attacked undetectably by finding that the corresponding IoS$^* \approx 1$. This is computationally simpler than the algorithms in [144] or [145].

For locations where Theorem 3 does not provide IoS$^* \approx 1$, depending on the operating conditions of the grid, the following result shows than an attacker could still find alternative attack locations to produce an undetectable attack.

Theorem 4. *For an attack with two delays ($p = 2$), one attacked measurement per delay ($\mathcal{A}_1 = \{z_1\}$ and $\mathcal{A}_2 = \{z_2\}$), and rank(W) $= 2$, there is still a possibility of performing* *a practically undetectable attack if the ratio between the magnitude of the attacked measurements is either very small or very large.*

Proof. By analyzing (4.24), it follows that IoS$(W) \approx 1$ if and only if IoS$(W) \approx 1 \Leftrightarrow \operatorname{trace}(W)^2 >> \det(W)$. By using (4.28) we can express the inequality as

$$\begin{aligned} \left(|z_1|^2 f_{11} + |z_2|^2 f_{22}\right)^2 &>> |z_1|^2 |z_2|^2 \left(f_{11} f_{22} - |f_{21}|^2\right) \\ \left(\frac{|z_1|}{|z_2|} f_{11} + \frac{|z_2|}{|z_1|} f_{22}\right)^2 &>> \left(f_{11} f_{22} - |f_{21}|^2\right). \end{aligned} \tag{4.30}$$

Define $d = \frac{|z_2|}{|z_1|}, d \geq 0, d \in \mathbb{R}$; substituting d in (4.30)

$$\left(\frac{1}{d} f_{11} + d f_{22}\right)^2 >> \left(f_{11} f_{22} - |f_{21}|^2\right) \tag{4.31}$$

If we take the left-handside of (4.31) and plot it as a function of d, we can observe that it has a quadratic behavior with minimum in $d^* = (f_{11}/f_{22})^{\frac{1}{2}}$ and expands to $+\infty$, both when $d \to 0$ and when $d \to +\infty$, i.e., if the ratio between the magnitude of the attacked measurements is either very small or very large. ☐

In summary, an attacker can compute IoS* for arbitrary pairs of locations; this requires only the knowledge of H. If he finds location pairs with IoS$^* \approx 1$, he has obtained candidate locations where an undetectable attack is possible; he can then test the effect of such attacks. If, in contrast, there is no location with IoS$^* \approx 1$, the attacker can rely on Theorem 4 to assess the candidate measurements to be attacked, and pick two measurements with smallest or largest magnitude ratio and still perform a practically undetectable attack.

4.2.4 Practically undetectable attack with more than two delays

In this section we consider the problem of computing attacks with more than two delays, i.e., finding a solution to the problem in Theorem 1 for $p > 2$. In what follows, we show how to combine attacks against two delays ($p = 2$) to obtain an attack with $p > 2$ delays.

Combining Attacks on Disjoint Pairs of PMUs

As a first step, we consider that there is a set of disjoint PMU pairs ($p = 2$) that can be attacked using the algorithm proposed in Theorem 2, i.e., pairs of PMUs for which the IoS is close to 1. In what follows we show that even though an attack modifies the apparent measurements (and the apparent system state), when the attacked pairs of

PMUs are disjoint, the attacks can be computed independently in parallel.

Theorem 5. *Consider a collection of* K *attacks, and let* $\mathcal{A}_i^{(k)}$ *be the set of measurements affected by the* i^{th} *angle of the* k^{th} *attack. Let* z_m *be the* m^{th} *measurement value when no attack is performed and let* $W^{(k)}$ *be the matrix given by* (4.15) *when it is only attack* k *that is performed. Then*

(i) the matrix $W^{(k)}$ *depends only on the values* z_m *for* $m \in \cup_i \mathcal{A}_i^{(k)}$.

Assume furthermore that the sets $\mathcal{A}_i^{(k)}$ *are disjoint, i.e. any measurement point appears in some* $\mathcal{A}_i^{(k)}$ *for at most one* k *and at most one* i. *Then*

(ii) if each attack k *is absolutely undetectable if performed on its own, then so is any combination of the attacks, performed sequentially or simultaneously.*

Proof. By (4.16),

$$
\begin{aligned}
W_{i,j}^{(k)} &= \sum_{\ell,m\in\mathcal{M}} \bar{z}_\ell z_m \mathbb{1}_{\{\ell\in\mathcal{A}_i^{(k)}\}} \mathbb{1}_{\{m\in\mathcal{A}_j^{(k)}\}} g_{\ell,m} \\
&= \sum_{\ell\in\mathcal{A}_i^{(k)}} \sum_{m\in\mathcal{A}_j^{(k)}} \bar{z}_\ell z_m g_{\ell,m}
\end{aligned}
$$

with $g_{\ell,m} = \sum_n \bar{F}_{n,\ell} F_{n,m}$. Note that $g_{\ell,m}$ depends only on the verification matrix F and is thus independent of the measurements and of the attack. Statement (i) follows.

Now assume that the attacked sets of measurements $\mathcal{A}^{(k)} = \cup_i \mathcal{A}_i^{(k)}$ are disjoint. The matrix $W^{(k)}$ for attack k depends only on the values of z_m for $m \in \mathcal{A}^{(k)}$. An attack $k' \neq k$ affects only the measurement sites in $\mathcal{A}^{(k')}$ and $\mathcal{A}^{(k')} \cap \mathcal{A}^{(k)} = \emptyset$ therefore for $m \in \mathcal{A}^{(k)}$, the values of z_m remain the same before or after attack k'. Therefore $W^{(k)}$ also remains the same before and after attack k' is performed. $\square$

The above result implies that for a set of disjoint PMU pairs with IoS ≈ 1 a practically undetectable attack can be performed by attacking each pair of PMUs simultaneously with the angles given by (4.20).

Combining Attacks on Overlapping Pairs

Let us now consider attacks on overlapping pairs of PMUs. Unfortunately, we cannot apply the previous result because the W matrix of an attack now may depend on the apparent measurement values due to another, overlapping attack. However, as we show next, it is possible to combine attacks *sequentially*, provided that the effect of the previous attack in the sequence is accounted for.

Theorem 6. *Consider a sequence of $k = 1{:}K$ attacks, computed one after the other. The pairs of PMUs attacked may be overlapping. Let $z_m^{(0)} = z_m$ be the true value of measurement m, and $z_m^{(k)}$ the apparent value after the k^{th} attack. Let attack k be constructed so as to be absolutely undetectable assuming that the measurements are $z_m^{(k-1)}$. Then the combination of the K attacks is absolutely undetectable.*

Proof. Note that, by assumption, the k^{th} attack, resulting in $z^{(k)}$, is undetectable, i.e., by (4.11) it satisfies

$$F\left(z^{(k)} - z^{(k-1)}\right) = 0$$

where F is the verification matrix, which is independent of the measurements. Summing all these equations for $k = 1{:}K$ gives:

$$F\left(z^{(K)} - z^{(0)}\right) = 0$$

which shows that the combination is undetectable. □

The theorem implies that if a sequence of attacks on pairs of PMUs is practically undetectable, then so is their combination. One may think that it is difficult to predict, in the general case, whether a sequence of attacks is practically undetectable, since the undetectability condition (IoS$^{(k)} \approx 1$) depends on the matrix $W^{(k)}$ which itself depends on the result of the previous attack. As we show next, this is not the case, as the IoS of a pair of PMUs does not change due to an attack against a subset of those PMUs.

Theorem 7. *Consider a pair of PMUs, with matrix W given by* (4.16) *derived using the original measurements z. Assume that an attack is performed that affects a subset of this pair of PMUs, producing an apparent measurement z'. Let W' be the matrix given by* (4.16) *computed using the apparent measurements z'. Then IoS(W) = IoS(W').*

Proof. Observe that by (4.23) and (4.28), IoS(W) depends only on the modulus of the complex measurements z_m. Since an attack modifies only the angle of the measurements, the modulus are unchanged, and so is IoS(W). □

The practical implication of the above results is that an attacker can identify an arbitrary set of pairs of PMUs with IoS ≈ 1 based on the true measurement values, or a set of pairs of PMUs with IoS$^* \approx 1$. The attacker can then take an arbitrary sequence of these PMU pairs, computes the angles of the k^{th} attack using (4.20) and with matrix $W^{(k)}$ updated to account for the effect of the preceding $k-1$ attacks in the sequence, and in this way the attacker obtains an undetectable attack. In the example studied in Section 4.2.5 we consider a case where 10 pairs of PMUs have IoS$^* \approx 1$, and we found that, in general, every sequence of attacks gives a different set of attack angles.

A special case of interest is if we repeatedly attack a particular pair of PMUs (that has IoS ≈ 1). The effect of doing so is that the second attack restores the original measurement, i.e., it undoes the first attack. To see why, let z be the original measurement value, $z^{(1)}$ the apparent measurement after the first attack and $z^{(2)}$ the apparent measurement after the second attack (computed using the updated matrix $W^{(1)}$). We have $z^{(2)} \neq z^{(1)}$ by construction of the second attack. By Theorems 6 and 7, the sequential combination is an undetectable attack on z, which has produced an apparent measurement $z^{(2)}$. Nonetheless, by Theorem 1 there is only one non trivial undetectable attack, therefore $z^{(2)} = z$.

A Greedy Heuristic

In the previous subsections we have shown how to find a potentially very large number of undetectable attacks. In this section we propose a greedy heuristic for computing an attack that aims at optimizing a certain attacker objective.

We assume that the attacker has an objective that it wants to maximize; for example he might want to underestimate the apparent-power flow of a transmission line (with the potential consequence of burning it). The attacker has access to the admittance matrix Y, the PMU measurement type and locations and the measurement vector z. The attacker's goal is to mount an undetectable delay attack that induces a forged measurement vector z' that maximizes the attacker's objective, say $J(z')$.

A greedy algorithm for achieving this objective is as follows.

1. Establish a list $\mathcal{L}$ of pairs of PMUs that have IoS ≈ 1 given the measurement vector z. Alternatively, the list $\mathcal{L}$ can be computed using IoS* ≈ 1, in which case it is independent of the measurement z.
2. Let $z^{(0)} = z$ and $k = 0$;.
3. $k = k + 1$. Find the pair $j_k \in \mathcal{L}$ that maximizes $J(z^{(k)})$ where $z^{(k)}$ is the forged measurement obtained after applying the attack to the pair j_k and to the measurement $z^{(k-1)}$.
4. If $k < K_{max}$ and $J(z^{(k)}) - J(z^{(k-1)}) > \varepsilon$ go to 3) else exit and output $j_1, j_2, ...$

In other words, the algorithm finds at every step, among all the possible attacks, the one that gives the largest damage. It then updates the measurement vector z based on the attack, and continues until no new attack can increase the damage in the line or a maximum number of iterations is reached. The attack to be mounted is then given by the sequence of pairs of PMUs $j_1, j_2, ...$ By the theorems in the previous section, this combined attack is practically undetectable. In Section 4.2.5 we provide numerical results for testing undetectability of the resulting attack. Additionally, we compare the apparent-power flow mis-estimation obtained by this method versus an undetectable attack on a single pair of PMUs.

4.2.5 Performance evaluation

In this section we illustrate how the previously presented attack method can be applied to the IEEE 39-bus system, a benchmark for power transmission grids [146]. We show in particular how the computation of IoS* can be used to easily find attack locations. We also demonstrate that the attacks are non detectable by BDD methods based on residuals.

The performance evaluation was entirely done in MATLAB 2015b-64 bit, on a PC with Intel® core i7-5500U, 2.40GHz and 8 GB of RAM. The procedure consisted in:

1. Every 20 ms, a load flow is computed in order to determine the true state of the network;
2. The synthetic measurements forwarded to the state estimator are obtained by perturbing the true quantities inferred from the previous step with randomly-generated Gaussian noise characterized by the cumulated standard deviation of the PMUs and their sensors;
3. Computation of the attack vector according to the presented algorithm;
4. WLS estimation;
5. WLS estimation with attacked measurements;
6. Comparison of the detectability for step 5 with respect to step 4;
7. Comparison of estimated apparent power flows for steps 4 and 5.

The computational cost of the attack is compatible with the delays involved in a typical PMU-measurement flow. For instance, with the adopted software and hardware, an attacker needs an average of 0.4 ms with a max of 1.3 ms over a 300 s attack window to compute the attack vector when $p = 2$.

Analysis of Residuals

We here describe how residuals are analyzed in order to detect the existence of the attack. WLS cannot be expressed easily using complex matrix operations as we use in Section 4.2.1, because the measurement errors cannot be assumed to have circular symmetry, as we discuss later. This is why in what follows we have to introduce a slightly different formalism than in Section 4.2.1 in order to project from complex to rectangular coordinates.

The error covariance matrix R is defined as

$$R = \mathbb{E}\left(ee^{\dagger}\right) \tag{4.32}$$

where e is the measurement error vector from (4.9), assumed to be Gaussian. Note that if PMU errors in polar coordinates are relatively small, their projection in rectangular coordinates result into a Gaussian distribution [147]. R is a complex hermitian matrix, namely $R^{\dagger} = R$. In order to work with rectangular coordinates, we need to move from $R \in \mathbb{C}^{M\times M}$ to a matrix $R' \in \mathbb{R}^{2M\times 2M}$. Let $e = a + jb \in \mathbb{C}^M$ and define $e' = \begin{pmatrix} a & b \end{pmatrix}^T \in \mathbb{R}^{2M}$. Then, using the same expression as in (4.32) it follows that

$$R' = \mathbb{E}\left(e'e'^T\right) = \begin{pmatrix} R_{aa} & R_{ab} \\ R_{ba} & R_{bb} \end{pmatrix}$$

Note that $R_{aa}, R_{bb} \in \mathbb{R}^{M\times M}$ are diagonal matrices. As the hypothesis of independent measurement errors was justified in Section 3.1.2, then $R_{ab} = R_{ba} = 0$. R' is therefore diagonal and can be expressed as

$$R' = \begin{pmatrix} R_{aa} & 0 \\ 0 & R_{bb} \end{pmatrix} = \operatorname{diag}\left(\sigma^2_{e'_1}, \ldots, \sigma^2_{e'_{2M}}\right) \tag{4.33}$$

where $\sigma_{e'_m}$ $(m = 1, \ldots, 2M)$ is the standard deviation of the m^{th} measured quantity. (Note that if we would have $R_{bb} = R_{aa}$, then e would have circular symmetry and we could do least square estimation in complex numbers, but such an assumption cannot usually be made.)

At this point, we can perform the WLS in rectangular coordinates as described in Section 3.1.2. The WLS residuals are analyzed by using the χ^2 and LNR tests described in Section 4.1.1.

Recall that the undetectable attack is structured such that the distribution of the residuals, and their values after the attack, remain unchanged when compared with the values obtained without the attack. Hence, all the detection methods based on the normality of the residuals are expected to fail in identifying the attack. This is shown numerically in Section 4.2.5.

Electrical model

The validation of the attacks is performed on the IEEE 39-bus system shown in Fig. 4.11. We assume Bus #31 as the connection point to the external grid with a short-circuit

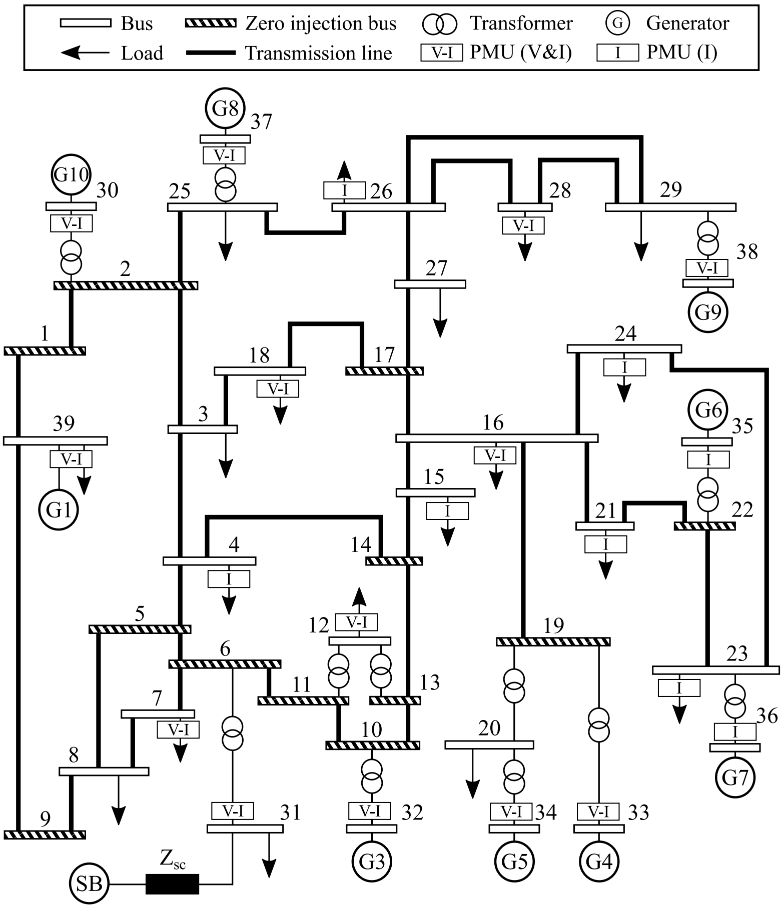


Figure 4.11 – Benchmark IEEE 39-bus transmission system and PMU locations.

power of S_{sc} = 50 GVA. The ratio between the real and imaginary parts of the short-circuit impedance is R_{sc}/X_{sc} = 0, as usually assumed for transmission networks. We assume the network has 13 PMUs that measure voltage and injected-current phasors and 8 PMUs that measure injected-current phasors only, for a total of 21 PMUs installed. Network observability (i.e., matrix H of full rank) is the only criterion followed when selecting measurement type (i.e., nodal voltage and injected-current phasors vs. injected-current phasors only) and PMU locations. These PMU locations, their measurement type, together with the presence of 12 zero-injection buses[5], are sufficient conditions to guarantee the observability of the system state. Note that other combinations of PMU locations and measurement type would affect the verification matrix F and all the quantities computed from it such as the attack-angle matrix W and the minimum index of separation IoS* defined in equations (4.15) and (4.25), respectively. In summary, this would mean different attack-locations as the ones showed in this analysis.

PMU measurements are generated by adding a white Gaussian noise to the amplitude and phase of the ideal phasors obtained by running a load flow. The standard deviation of the measurements is compatible with class 0.1 current and voltage sensors as described in [36, 37].

The load profiles are obtained from real measurements taken at 50 frames-per-second by real PMUs installed in the 125-kV sub-transmission network of Lausanne, Switzerland (more details about the field-trial in Section 5.2.1.). For this reason, the load profiles present time-domain behavior typical of transmission networks. This sub-transmission network is constituted by five 3-ph loads. In order to obtain values for the 19 1-ph equivalent loads available in the IEEE 39-bus system, some of the load profiles have been replicated. It is worth mentioning that the load profiles are then adapted to match the values provided in [146]. Moreover, as we do not use the transformer tap changers, the power at three selected buses (#7, #8 and #12) is adapted so that, in all the buses, the voltage stays within the $\pm$ 5% range of the rated voltage. In order to verify the effectiveness of the attack during non-steady-state conditions of the grid, we use a time window in which a sudden reactive power drop takes place at Bus #4 (see Fig. 4.12).

Results for undetectability of the attacking methods

We applied Theorem 3 to all possible combinations of attack locations, with $p = 2$, one measurement per delay, and taking PMUs that measure only injected currents. Table 4.1 shows the results for the IoS* at each location pair. Any pair that has an IoS* = 1, allows an undetectable attack regardless of the measurement values.

---

[5] A zero-injection bus is defined as a bus where no load or generation is connected therefore this information can be exploited as a so-called virtual measurement.

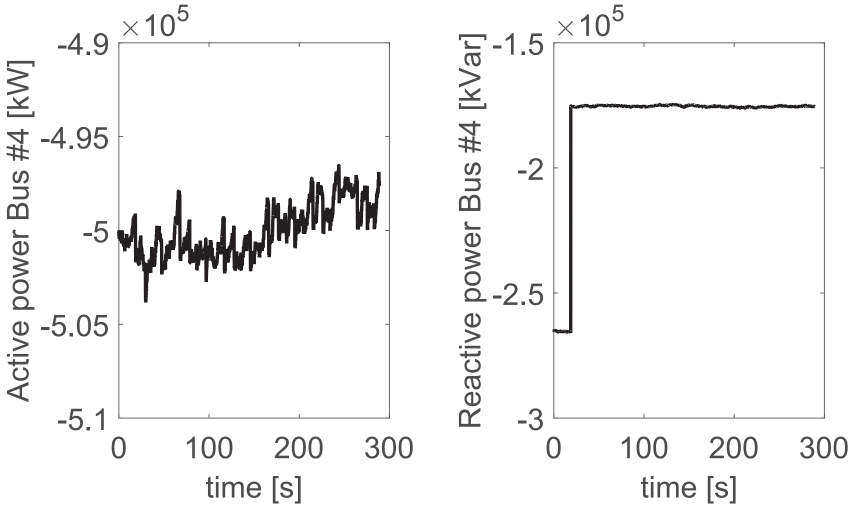


Figure 4.12 – Reactive power drop in Bus #4.

Table 4.1 – IoS* for all the two-delays attack combinations for buses with current measurements only in Fig. 4.11.

Bus1	Bus2	IoS*	Bus1	Bus2	IoS*
4	15	0.8437	21	24	1.0000
4	21	0.6613	21	26	0.8395
4	23	0.6613	21	35	1.0000
4	24	0.6613	21	36	1.0000
4	26	0.5282	23	24	1.0000
4	35	0.6613	23	26	0.8395
4	36	0.6613	23	35	1.0000
15	21	0.9516	23	36	1.0000
15	23	0.9516	24	26	0.8395
15	24	0.9516	24	35	1.0000
15	26	0.7669	24	36	1.0000
15	35	0.9516	26	35	0.8395
15	36	0.9516	26	36	0.8395
21	23	1.0000	35	36	1.0000

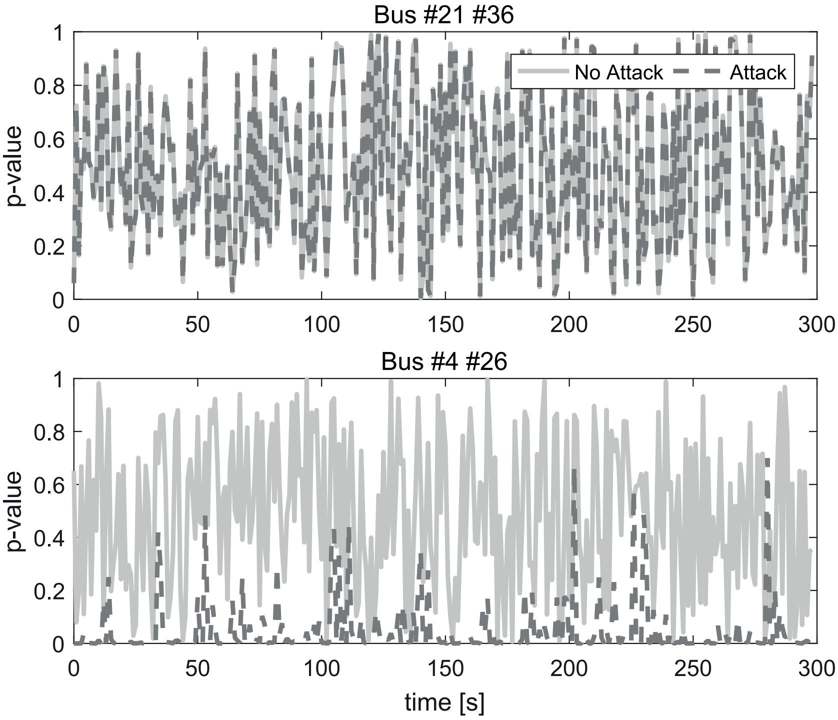


Figure 4.13 – Comparison of p-values for the χ^2-test applied to two attack locations.

To demonstrate the undetectability of an attack at a pair of PMUs where IoS$^* = 1$, we perform the χ^2-test for BD in the non-attacked and attacked scenarios with a detection confidence of 99%, and we confirm the results by performing the LNR test in the same scenarios. For both tests we adopted the approach described in [86] and recalled in Section 4.1.1. We attack the pair of Buses [#21, #36] as a representative of an attack where IoS$^* = 1$; we use the pair [#4, #26], as it has the lowest IoS*, as a basis for comparison.

Fig. 4.13 shows the p-values of the χ^2-test. At the top of Fig. 4.13 we observe that the p-values of the χ^2-test for the pair of Buses [#21, #36] are not modified by the attack, making the attack undetectable. In the bottom of Fig. 4.13, we show result for the pair [#4, #26], and the p-values for non-attacked and attacked scenarios are largely different, meaning that the χ^2-test detects the attack.

In Fig. 4.14 we show the LNR-test results for the attacks shown in Fig. 4.13. For each pair of PMUs, we plot LNR $= \max_m |r_m^N|$, with r_m^N computed as defined in equation (4.3) and $m = 1 : M$. The dotted line shows the threshold corresponding to a confidence of 99.73 %, which maps to a 3σ deviation for a single measurement. It can be seen that when attacking the undetectable location pair (top), the normalized residuals are invariant. Conversely, if we attack the second location pair (bottom), the majority of the LNRs are above the identification threshold making the attack easily detectable. Note that the reactive power drop in Fig. 4.12 has no effect on the LNR after the attack,

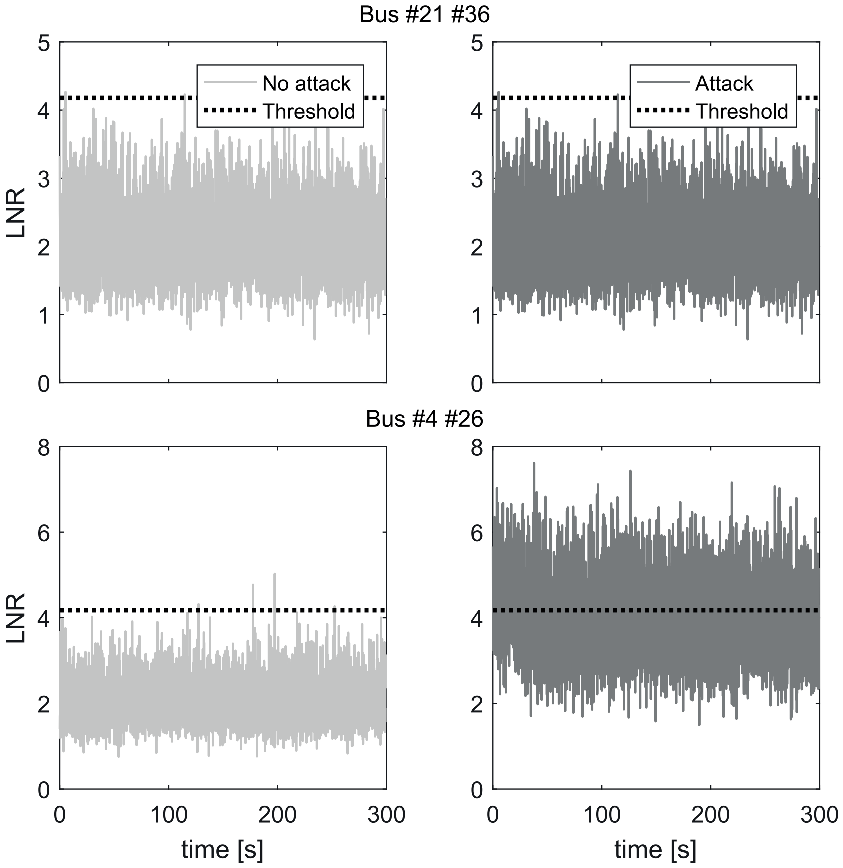


Figure 4.14 – LNR test applied to two different attack locations for the no-attack and attack scenarios.

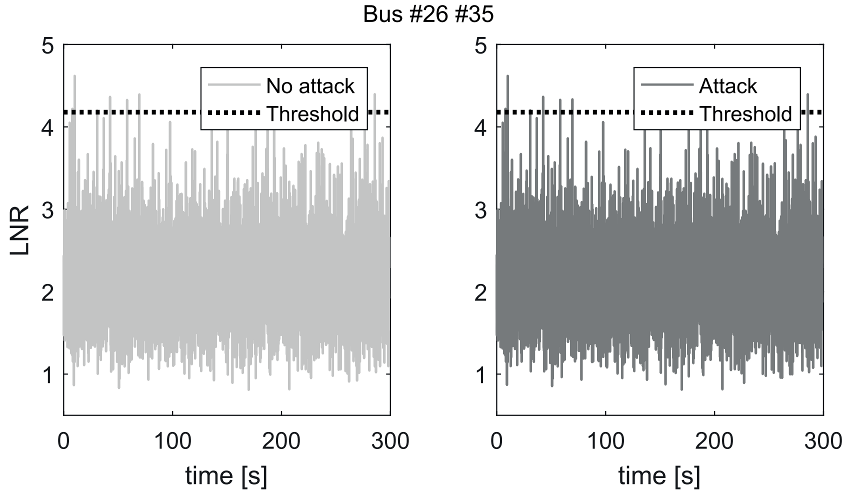


Figure 4.15 – Undetectability of a pair of PMUs that have large measurement-magnitude ratio, with IoS* < 1.

when the attack location has an IoS* $= 1$. This behavior holds under any transient.

To numerically illustrate Theorem 4, in Fig. 4.15 we show the LNR-test results for Buses [#26, #35], which have an IoS* $= 0.8395$, for a case when the magnitude of the measurement in Bus #35 is 9 times larger than that in Bus #26. The figure illustrates the LNR-test results before and after the attack, and shows that the attack remains undetectable despite the fact that IoS* < 1.

To illustrate Theorem 5, we show results for $p = 6$, for the disjoint PMU pairs [#21, #36], [#26, #35] and [#23, #24] for which either IoS* $= 1$ (first and third pairs), or Theorem 4 can be applied (second pair). The attack is performed in parallel, and Fig. 4.16 shows the results of the LNR-test, comparing attacked and non-attacked measurements. We can observe again that the results are statistically indistinguishable from the non-attacked case.

Finally, we use the greedy algorithm described in Section 4.2.4 with the objective of under-estimate the apparent power flow for the line between Buses #16 and #24. The algorithm finds the maximum underestimation with $p = 10$, attacking pairs [#21, #36], [#23, #24], [#24, #35], [#23, #36], [#21, #23]. We can see the LNR-test applied to the measurements before and after the attack in Fig. 4.17, which shows that the sequential attack on pairs of PMUs that give an undetectable attack, is also undetectable.

Results on power-flows mis-estimation

To illustrate the potential impact of time synchronization attacks, we show results for an attack against a pair of PMUs (i.e., [#21, #36]), which leads to over- and under-

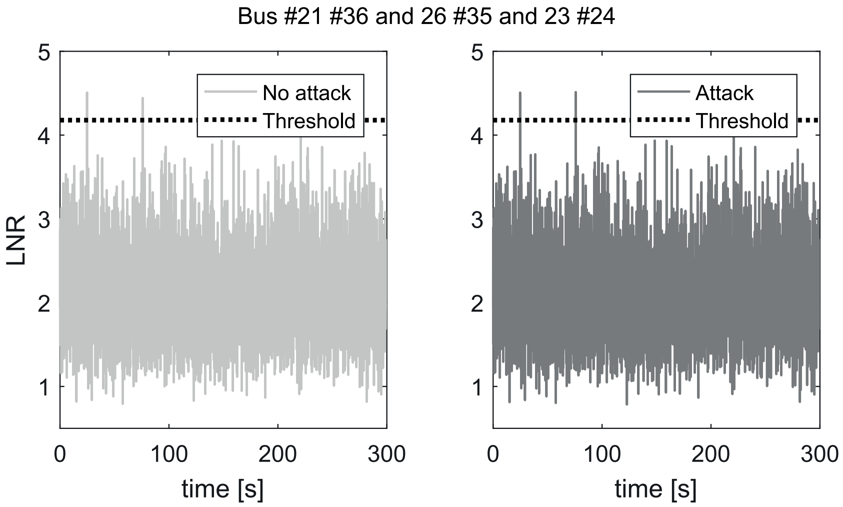


Figure 4.16 – LNR-test applied to an attack on three disjoint pairs ($p = 6$), following the method described in Theorem 5.

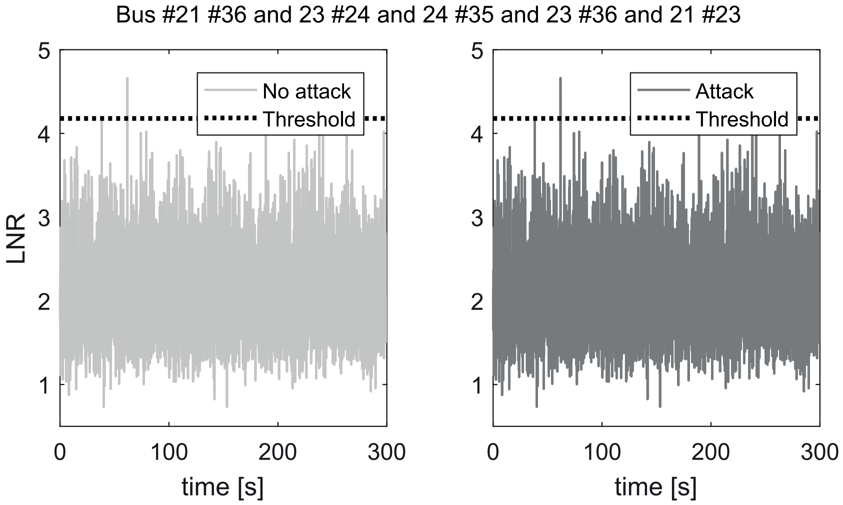


Figure 4.17 – LNR-test on a sequential attack with $p = 10$, using the greedy algorithm strategy.

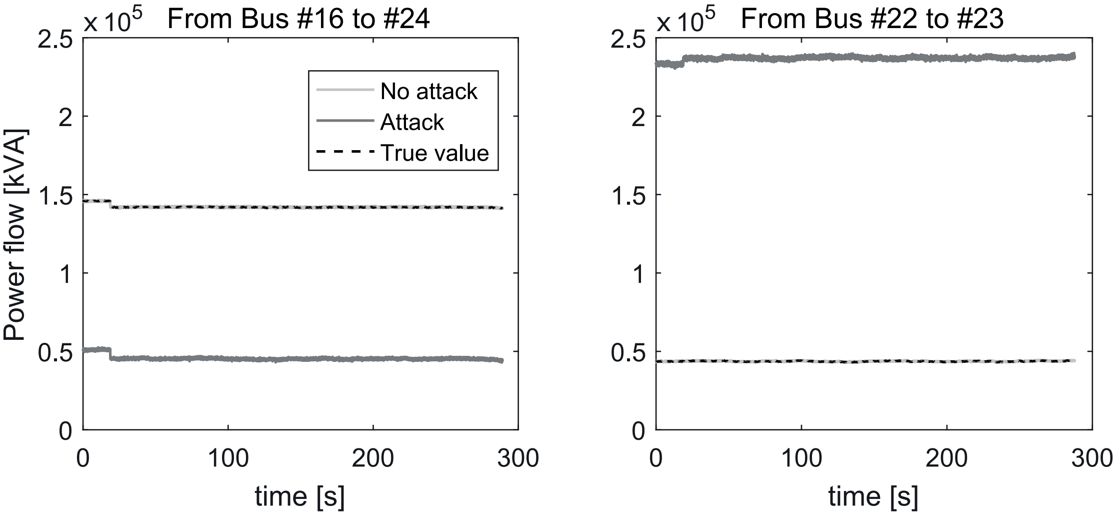


Figure 4.18 – Comparison of the true apparent-power flow in two lines and the estimated apparent-power flow for the no-attack and attack scenarios.

estimation of power flows in the power system. The attack angles computed are $\alpha_1 = 1.14$ rad for Bus #21 and $\alpha_2 = 0.57$ rad for Bus #36, and they increased of 0.02 rad after the reactive power drop.

We applied the same random numbers for generating the measurement noise to the scenarios with and without attack, ensuring that any difference in the state-estimation results is only due to the attack.

The attack worsens the estimated voltages, hence all the inferred quantities from there are affected (e.g., injected currents, current flows, active and reactive powers, etc.), with errors going above 500 %, as shown in the right side of Fig. 4.18. In this case, the system operator believes that the power flowing in the line between Buses #22 and #23 is much higher than it really is, therefore the system operator could decide to shed some loads or to reconfigure the network when this is not necessary. On the contrary, in the left side of Fig. 4.18, the system operator under-estimates the power flowing in the line between Buses #16 and #24 thus exposing the line to power flows larger than those it is designed for (in all the cases where the true power flow is close to the line's ampacity limit).

Fig. 4.19 compares the under-estimation of the apparent-power flow on the line between Buses #16 and #24 obtained by different attacks. We compare (i) the attack on a single pair of PMUs (i.e., [#21, #36]); (ii) the attack on disjoint pairs of PMUs described in Theorem 5 and (iii) the heuristic greedy algorithm described in Section 4.2.4. Although we see that adding extra pairs appears to increase the impact of the attack, the assertion does not always hold (e.g., attacking twice the same pair of PMUs cancels the attack, as mentioned before). In general, it is the attacker that, by knowing the IoS*

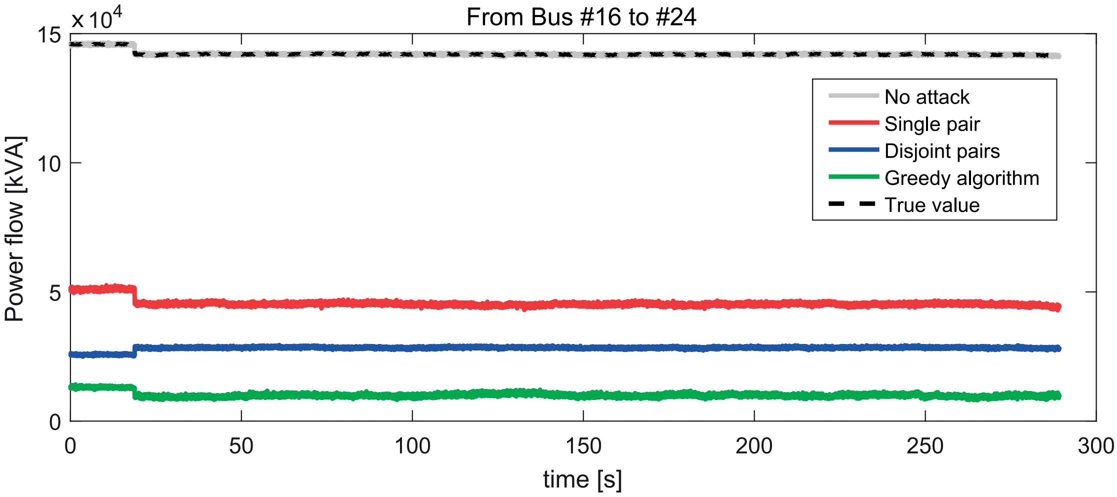


Figure 4.19 – Comparison of the under-estimated power flow in a transmission line, for different attack scenarios.

criterion, can build a strategy to best achieve its objective.

4.2.6 Countermeasures

The methodology of the attack presented here does not have any influence on the value of the residuals, hence the BD cannot be identified and removed from the measurement set by applying the classic BDD algorithms. A possible countermeasure is discussed in [148], where the authors propose strategies to maintain integrity of measurements, and describe a BDD technique based on a comparison between measurements from PMUs and measurements from SCADA (from other remote terminal units (RTUs)). Notwithstanding, the differences between these types of measurements could make ineffective the use of SCADA measurements to validate the integrity of PMU measurements. Indeed, typical SCADA measurements are available every 4 seconds and are not time synchronized, while PMUs can provide 50 or 60 synchrophasors per second.

Successful countermeasures capable to identify the GPS spoofing need to be implemented at the device level. The recent literature has discussed potential countermeasures using this approach. Additional features need to be added in the GPS controller embedded in the PMU to detect, and eventually mitigate, the GPS spoofing. Reference [149] has discussed these techniques that can be clustered as follows:

- Detect changes of power-related parameters of the GPS hardware (e.g., carrier-to-noise density ratio, absolute received signal power, power variations, etc);
- Observe time-related parameters of the GPS receiver like the length of interval

between phase transitions, the delay between signals transmitted on different frequencies;

- Analyze multiple signals with the same direction of arrival using multi-antenna receivers;
- Add secondary sources of time synchronization like, for instance, precision time protocol (e.g., PTPv2, White Rabbit).

Note that the attacks here presented require knowledge of the measurement vector, thus integrity or authentication mechanisms are not sufficient for mitigation. Given the impact of the attacks, and how simple and useful the IoS* criterion is, we strongly suggest that confidentiality of PMU measurements be mandated by the standards.

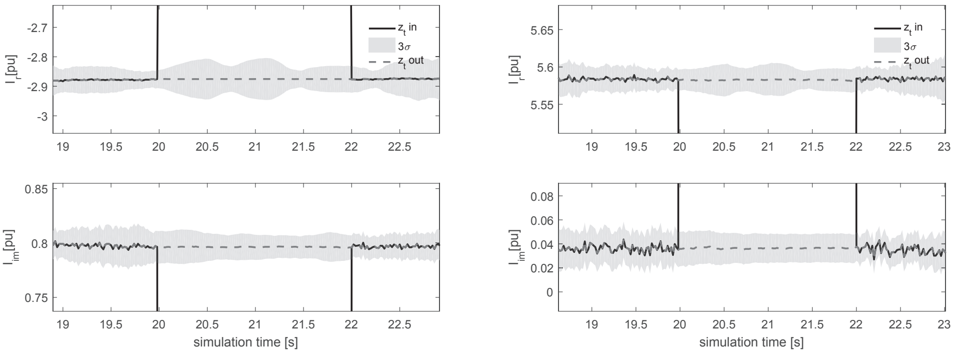
Timing attacks under clock-drift conditions

The clock of any PMU has an internal oscillator that is controlled by a clock-servo. A clock-servo is a filter that prevents the clock from making abrupt changes in time and has a stiffness that depends on the manufacturer. The described attacks in the paper could cause a change in time which could produce an alarm in the clock-servo, making the attack detectable. Taking the clock-servo described in [150] as an example, the total attack's time-adjustment would require to be divided in "chunks" of 5 µs/s (corresponding to a phase shift of 1.57 mrad/s at 50 Hz) to avoid an overfeeding to the clock-servo that could trigger an alarm. Further research in this direction could consider proposing an optimal attack with a constraint in the derivative of the attack-angle calculation of the form $|\alpha_i(t+\Delta t)-\alpha_i(t)| \leq \eta_{att}$ with Δt being the refresh rate of PMU measurements and η_{att} the maximum incremental step in time to avoid a clock-servo alarm.

Pre-estimation filtering vs. undetectable timing attack

We assess the performance of the pre-estimation filtering process of BD, presented in Section 4.1.3, as a countermeasure for the undetectable timing attack. Differently from the validation of the pre-estimation filtering process of BD carried out in Section 4.1.4:

- The transmission network of Fig. 4.11 does not present several critical measurements. For this reason, a non-critical measurement affected by BD may be discarded. Nevertheless, we chose to replace any corrupted measurement for sake of comparison with the previous results;
- In what follows, the process noise covariance matrix **Q** is assessed following the heuristic method presented in [95] and briefly recalled in Chapter 3.1.2;



(a) Bus #21

(b) Bus #36

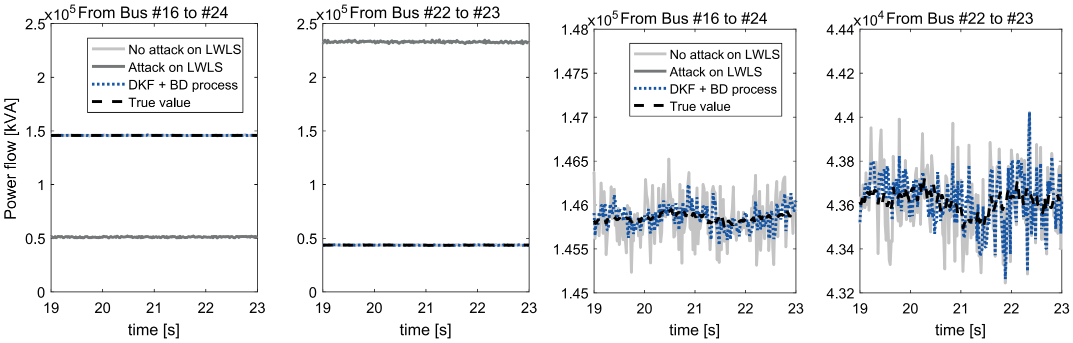
Figure 4.20 – Replacement of the attacked measurements by the pre-estimation filtering of BD process.

- The attack is inserted at time t=20 s for a duration of 2 s.

As an example, let us take the undetectable attack to Bus #21 and #36 previously described. In Fig. 4.18 it was shown that this attack led up to 3 times underestimation and 5 times overestimation of the power flows, in two specific lines. Fig. 4.20 shows the real and imaginary parts of the current measurements (in p.u.) during the attack to the PMUs in the two buses. The continuous black line represents the measurement affected by the undetectable attack (from t=20 s), the grey dashed line represents the output of the BD process. The BD method correctly detects the BD and replaces the corrupted measurements. For the sake of completeness, we list and briefly discuss the main reasons for the success of the BD process:

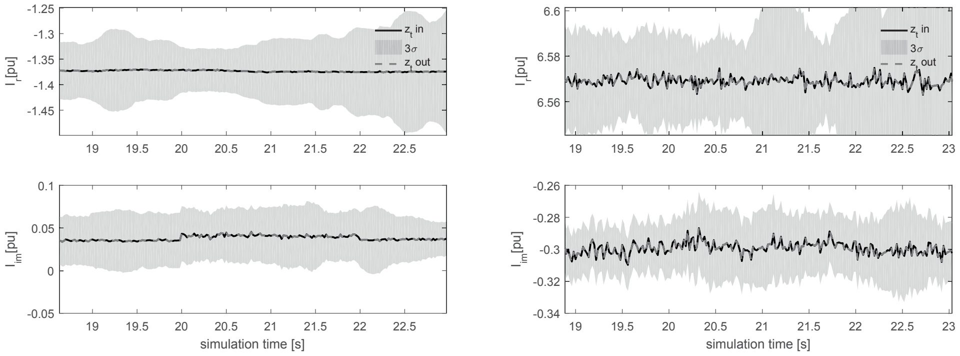
1. The angles computed to obtain an undetectable attack are large ($\alpha_{21} \approx 1.14$ rad and $\alpha_{36} \approx 0.57$ rad), thus the attacked measurements fall largely beyond the threshold (grey area in Fig. 4.20).
2. The change in the angles is assumed to be instantaneous. This assumption was already discussed at page 111. On the other hand, a slow change would be detectable by residual-based BD algorithms.
3. The pre-estimation of BD assumes to compare anomalies in injected currents with anomalies in voltage. Due to the nature of the timing attack, PMU measuring current-only are the target of the attack. BD are therefore not present in voltage measurements and this facilitates the comparison with the neighbor PMU and the subsequent BD identification.

Fig. 4.21 shows the impact that the attack has on 2 specific lines. Differently from



(a) Estimated power flows. (b) Detail on the accuracy of the DKF + BD.

Figure 4.21 – Comparison of the estimated power flows for two lines. The BD process neutralizes the attack.



(a) Bus #26. (b) Bus #35.

Figure 4.22 – Failure in replacing the attacked measurements by the pre-estimation filtering of BD process.

Fig. 4.18, the power estimated by the DKF coupled with the BD process is also given. As it can be noticed, the BD replacement neutralizes the impact of the attack.

As mentioned, the success of the BD process is function of the computed angle α. The larger α, the more probable the detection of the attack is. This was tested on all the attacks presented in Section 4.2.5. As an example of missed detection, let us consider the attack at Bus #26 and #35. In this case, the resulting angles are $\alpha_{26} \approx 3$ mrad and $\alpha_{35} \approx 0.3$ mrad. Such angles fall below the threshold and thus the attack is not identified as shown in Fig. 4.22.

At the same time, such small angles do not have a visible impact on the estimated power flows. Indeed, an analysis of the the estimated powers in all the lines has shown that such angles do not impact the accuracy of the state estimator. The DKF and LWLS provide comparable results to the non-attacked case, as shown in Fig. 4.23. For sake of

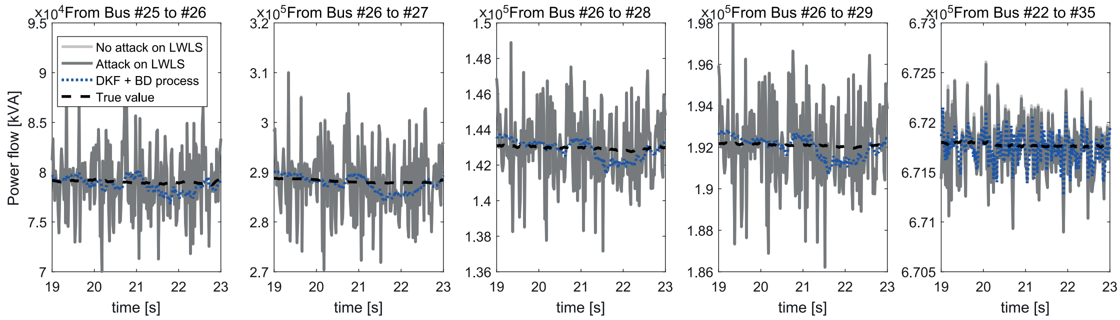


Figure 4.23 – Comparison of the estimated power flows for the lines departing from the attacked buses. Due to the small angles, the undetectable attack does not lead to a misestimation of the power flows.

space, only the estimated power flows in the lines departing from Bus #26 and #35 are given.

Conclusions

In this section we have shown that, by manipulating the time reference of one pair of PMUs, it is possible to perform attacks in PMU-based linear state estimators that are undetectable by state-of-the-art residual based BDD methods. We introduced a criterion to find location pairs where the attack is undetectable and provided a closed-form expression to compute the attack angles. We also provided an additional criterion to identify attackable locations regardless of the measurement values. We mounted attacks with more than two delays and showed that attacks on disjoint pairs can be superimposed such that the attack is performed in parallel. Furthermore, we showed how combined sequentially attacks are possible and can be used with a greedy algorithm in order to damage transmission lines. We also showed that when performing a sequence of attacks, it is possible to know whether each attack in the sequence will be undetectable before computing the attack. We used simulations to verify the attacks and to demonstrate their efficacy. Finally, we discussed possible countermeasures, with particular focus on the performance of the pre-estimation filtering of bad data proposed in Section 4.1.3. We have shown that this process might represent an effective way to identify and neutralize the PMU timing attacks.

5 Experimental activities

This chapter illustrates the experimental validation of the functions and applications presented in the manuscript. In this respect, the chapter starts by describing a GPS synchronized real-time simulation platform and the implementation and validation on this platform of a real IEEE C37.118 Class-P Std compliant synchrophasor extraction algorithm. We then describe three field trials where we assess and compare the performance of the proposed PDC data-pushing logics. Finally, in the real-time simulation platform, we validate a protection mechanisms relying on PMU-based state estimation and by means of a HIL setup, we validate a voltage control mechanism.

Original contributions of this chapter:

- Deployment and performance validation in a GPS-synchronized real-time simulator of a realistic IEEE C37.118 Class-P Std compliant synchrophasor extraction algorithm;
- Validation of data-pushing logics for synchrophasor data concentration in three real field installations;
- Validation in a real-time simulator of a protection mechanism relying on PMU-based state estimation;
- Validation of the GECN voltage control mechanism by means of a time synchronized HIL setup.

5.1 The real-time simulator

It is crucial to validate the behavior and performance of new protection schemes or new control mechanisms prior to their deployment in real networks. Indeed, in the real field, the assessment of the performance of the protection scheme or control mechanism is practically impossible as the true state is hidden by the measurement noise and bias.

Additionally, emergency situations such as contingencies or disturbances might result in unpredictable protection/control actions that were not foreseen in the development phase. These limitations can be tackled by first validating the protection or control mechanisms in a laboratory environment using Real-Time Simulators (RTSs) within a Hardware-in-the-Loop (HIL) setup.

5.1.1 Integration of an IEEE Std. C37.118 compliant PMUs in a RTS

The content of this section is based on [151]. The connection of real PMU devices to the RTS might presents technical and economical drawbacks typically represented by: (i) the limited number of available analog outputs to interface large number of PMUs (e.g., several tens/hundreds) and (ii) the potential high cost of such a kind of devices. To overcome these obstacles, PMUs might be virtualized and directly embedded inside the model running into the RTS. This enables the usage of a number of PMUs limited only by the computational resources of the RTS with respect to the selected integration time-step and the model complexity. Despite the evident advantages of such an approach, its application is limited by the computational resources typically required by the RT simulation of the majority of synchrophasor estimation algorithms.

In this respect, few works explored the possibility of virtualizing PMUs in RTSs [152, 153, 154, 155] and the synchrophasor estimation performance was always a compromise between accuracy and complexity. In what follows, instead, we show the deployment and validation into a RTS of a virtual PMU characterized by a synchrophasor estimation algorithm that, associated to a PMU prototype, has demonstrated its compliance with the class-P requirements defined in the IEEE Std. C37.118.1-2011 [38] and with most of the accuracy requirements defined for class-M PMUs with the exception of out of band interference tests. To the best of our knowledge, this is the first work that presents the integration of a standard compliant PMU into a RTS.

The focus of the section is on (i) the time synchronization of the platform that allows the RT-virtualized PMU to exchange messages to real-world applications and (ii) the assessment of its performance. The formulation of the deployed synchrophasor estimation algorithm, the so-called enhanced Interpolated Modulated Sliding DFT (e-IpMSDFT), is widely documented in the literature and thus it is not reported in this work. The algorithm has been first formulated in [39] and further extended in [156] in order to reduce the measurement reporting latencies and, consequently, increase the reporting rates (see Fig. 5.1). Moreover, the same algorithm is currently deployed in PMU prototypes installed in real electrical grids [32, 47].

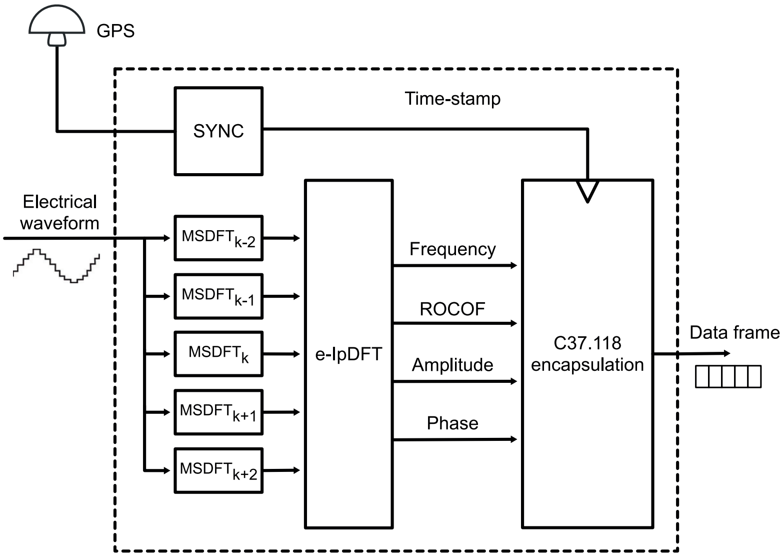


Figure 5.1 – Block scheme of the proposed e-IpMSDFT-based virtual PMU.

The platform

The adopted platform is the Opal-RT eMEGAsim PowerGrid Real-Time Digital Simulator [157]. Such a platform consists of a multi-core processor hardware able to perform operations within an integration time-step generally of some tens of microseconds. Simulink is used to create the models that, by means of the software platform RT-Lab are compiled and transferred in the CPUs to run in RT. Additionally, the RTS is also equipped with a set of Analog and Digital I/Os to allow the connection with external devices for HIL setups.

The setup is shown in Fig. 5.2 and it consists of one industrial PC (12 cores), a Spartan3 FPGA board and a Dolphin DXE410 Expansion Chassis. The RT simulated model runs in the industrial PC, the FPGA is used to lock the integration time-step to a more stable clock. The DXE410 module enables the communication between the two elements. In addition to this, in order to have access to a stable and reliable UTC-time reference needed to simulate any PMU, the industrial PC has been equipped with a hardware GPS-synchronization module from Spectracom (Tsync-PCIe express board [158]). This board is used to provide (i) the UTC time-stamp for PMU data-frames (ii) the Pulse-per-Second (PPS) to a clock adapter in order to generate a GPS synchronized clock. The reason for having such a setup is clarified in the next section where the time-synchronization of the setup is described.

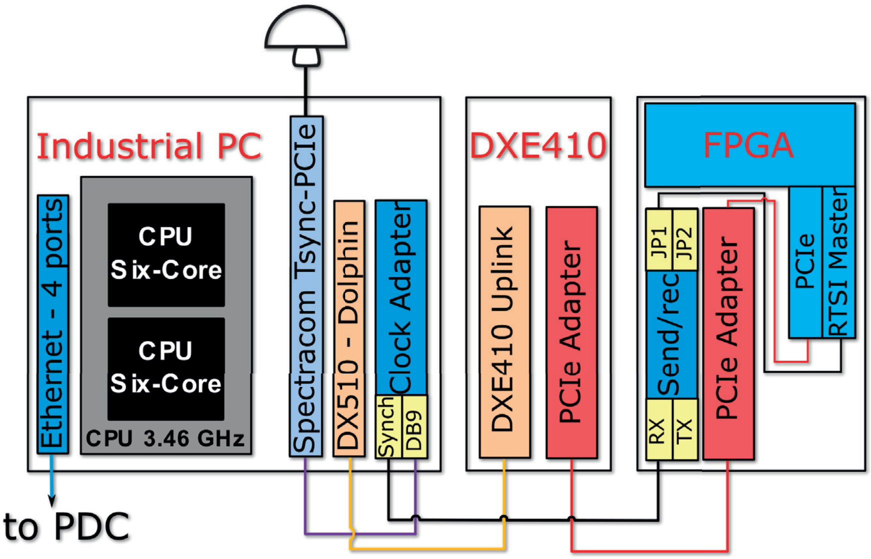


Figure 5.2 – Setup of the eMEGAsim PowerGrid RTS.

Time-synchronization of the setup

Both real or simulated PMU, need to report to the outside world the estimated values at regular time-intervals defined by the adopted reporting rate and at reporting times aligned with the UTC-second rollover. The PDC is also usually synchronized to a traceable UTC-time source as shown in Fig. 5.3a. The experimental validation of PMU-based monitoring and control schemes by using HIL setup needs to include at least: (i) a RTS integrating the RT-models of the simulated electrical grid and PMUs; (ii) a PDC coupled with the monitoring or control algorithms under test.

In such context, it is clear that the RTS needs to integrate a proper GPS receiver, or equivalent UTC-time source, to bring synchronization to the simulated PMUs and, in this respect, two main possibilities exist. The first one refers to a sort of ideal operating condition for the RTS that wants to integrate one or more virtual PMUs. In such a setup, the CPU clock used to derive the RTS integration time-step is disciplined by a UTC-stable time reference (see Fig. 5.3b). This condition allows to considerably simplify the PMU design by directly synchronizing the PMU sampling and reporting processes to UTC and guarantees that the RTS simulation time would not drift over time. In the case of the adopted RTS, such synchronization can be achieved by taking advantage of the setup described and shown in Fig. 5.2. The Spectracom board generates a pulse at the frequency corresponding to the inverse of the integration time-step configured in the simulated model. The pulse is constantly aligned with the PPS of the GPS source so that it does not drift in time and it is fed to the FPGA board. In correspondence of each pulse, a FPGA counter register is incremented. The model developed by the authors polls on the same FPGA counter and uses its increment to determine the exact

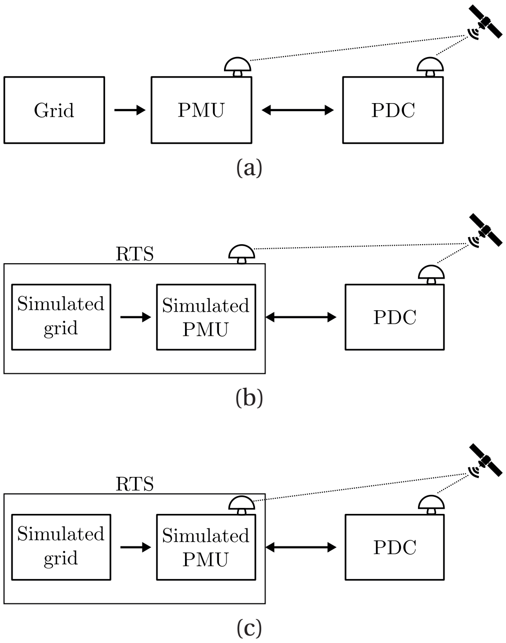


Figure 5.3 – Time synchronization of possible validation setups. To be noted the position of the GPS antenna. (a) Real field, (b) Simulation in a GPS synchronized RTS (both grid and PMUs), (c) Simulation in a non-synchronized RTS (simulated PMU is GPS synchronized for packet time-stamping).

instant to proceed to the next calculation step. In other words, since the FPGA counter increment is driven by a GPS disciplined pulse, the model integration time-step will not drift over time.

The second possibility (see Fig. 5.3c) refers to a very common configuration where the CPU clock, and therefore the RTS integration time-step, cannot be disciplined to any stable time reference. This condition might happen, for instance, when the setup does not include a FPGA board. As a consequence the integration time-step can only be directly derived from the free-running CPU clock and will therefore be affected by a slow but relevant time-drift (for the specific setup, the drift has been measured to be approximately 9 µs/s). On the other hand, the reporting of PMU measurements is automatically synchronized to UTC by means of the built-in C37.118 data encapsulation library by Opal-RT. More specifically, every time the GPS-derived UTC time hits a specific reporting time, the data frame is built using the e-IpMSDFT estimations and streamed out of the RTS. As a consequence, the PDC receives a synchronous PMU data flow from the RTS but the estimated synchrophasors are obtained by means of a CPU clock that is drifting with respect to a generic UTC time-reference. In order to illustrate the effects of this drift, let consider, for the sake of simplicity, a simple setup where a single-channel PMU is directly connected to a simulated 50 Hz steady-state signal generator. Since the signal generation and the PMU sampling processes are running at the same speed, the simulated PMU will not notice the CPU clock time drift and will measure consistent data with respect to the signal generation settings. Nevertheless, the frequency and phase estimation received at the PDC will not be consistent due to the RTS's clock drift with respect to the UTC time reference. The consequence is that the PDC will receive a drifting phase from the simulated PMU with a constant 50 Hz frequency estimation. In order to cope with the drift in time of a non-synchronized RTS, the PMU estimations of frequency and phase have been opportunely compensated. In particular, the RTS sampling clock error is computed in real-time inside the simulated PMU as follows:

$$\varepsilon(n) = \frac{t_p - t_{p-Z}}{Z \cdot T_s} - 1 \tag{5.1}$$

where T_S is the integration time-step and the equivalent PMU sampling time, Z is the measurement window length (expressed as an integer number of input samples) over which the clock error is computed (for the specific case of this simulated PMU we have adopted a 10 seconds window length) and t_p is the UTC start time of the p-th integration time-step. Every time the CPU clock error is computed, the frequency estimation can be properly updated (see [39] for more details about this aspect). In addition to this, another correction takes place into the simulated PMU when the integration time-step is derived from the free-running CPU clock. This second correction compensates the phase uncertainty related to the PMU sampling time T_s by measuring the time distance between the specific reporting time and the first sample of the time-window used to estimate the synchrophasor. Such an uncertainty corresponds, for a sampling rate of 10 kHz and a rated system frequency of 50 Hz, to 10 πmrad (1.8 deg), a value that definitely needs to be compensated particularly for PMUs conceived for distribution networks (see [39] for further details).

Once deployed in the Opal-RT eMEGAsim PowerGrid Real-Time Digital Simulator, the simulated PMU has been experimentally validated with respect to: (i) the accuracy of the algorithm during the static and dynamic testing conditions dictated by the IEEE Std. C37.118.1-2011; (ii) the computational load of the developed PMU model. The validation concerns the configuration shown in Fig. 5.3b since it allows a straightforward UTC-time synchronization of the RTS and thus of the PMU model.

Accuracy assessment

Typically the validation of the performance of any synchrophasor estimation algorithm deployed in a real hardware always includes additional sources of errors dependent on (i) the PMU A/D converters resolution, (ii) the sampling process time-stability and (iii) the adaptation of the developed SE algorithm to the adopted hardware platform. In the case of the simulated PMU model these error sources are not included. In particular, the sampling process is perfectly synchronous with respect to the simulated power system and its jitter can be, therefore, neglected. Similarly the influence of the A/D

Table 5.1 – Performance assessment of the e-IpMSDFT algorithm (the meaning of the symbols is the one in [38]).

Test type	Test range	Maximum Error	
		TVE [%]	FE [Hz]
Single tone	$f_0 \pm 5$Hz	$5.71e^{-4}$	$6.90e^{-4}$
Multi tone	10% each harmonic up to 50^{th}	$9.24e^{-12}$	$4.83e^{-13}$
Ampl. modulation	Mod. frequency 0.1 to 5Hz, $k_x = \pm 0.1$	$6.29e^{-1}$	$7.96e^{-2}$
Phase modulation	Mod. frequency 0.1 to 5Hz, $k_a = \pm 0.1$	$5.69e^{-1}$	$1.85e^{-2}$
Frequency ramp	$\pm$1Hz/s ramp, $f_0 \pm 5$Hz	$3.71e^{-2}$	$6.95e^{-4}$
Test type	Test range	Response Time [s]	
		TVE	FE
Ampl. step	Magnitude = $\pm 10\%$, $k_x = \pm 0.1$	0.031	0.051
Phase step	Angle = $\pm 10^\circ$, $k_a = \pm \pi/18$	0.026	0.048

converters and of the specific implementation of the SE algorithm are minor since the PMU model is directly coupled with the simulated voltage/current signals and the SE algorithm has been implemented using floating point precision (64 bits). As a consequence, the PMU accuracy assessment, carried out on the RTS, allows an analysis of the performance of the e-IpMSDFT synchrophasor estimation algorithm only (thus, eliminating all the sources of additional uncertainty). In this respect, the validation is performed by applying static and dynamic signals to the PMU as defined by the IEEE Std [38] and verifying its compliance with the same standard. Table 5.1 provides the performance assessment in terms of Total Vector Error (TVE), Frequency Error (FE) and response time. For each test type, the results shown in Table I, are obtained by using the more demanding testing conditions among those defined for class-P PMUs. The specified range refers to a PMU with a reporting rate of 50 fps, but other reporting rates were tested as well. The errors and response times are always within the limits and the TVE in steady state conditions is compatible with distribution system applications. The measurement accuracy is verified to be compatible with the one presented in [39].

Computational requirements

Further tests were performed to verify the computational resources of the proposed SE algorithm when running in RT in the eMEGAsim target. In this respect, when selecting the integration time-step, it should be taken into consideration the fact that the MSDFT methods assumes that, for each new sample, every DFT bin needs to be updated in order not to compromise the next DFT estimation. This computation must be performed before the acquisition of the next sample, over the whole set of PMU input channels, in order to correctly estimate the corresponding synchrophasors.

Table 5.2 – Computational requirements of the virtual PMU into the Opal-RT eMEGA-sim RTS.

Integration time-step	Number of virtual PMUs per RTS core		
	1-channel	6-channel	12-channels
100 µs	16	9	5

Following these considerations, the integration time-step (i.e. the PMU's sampling time) must be carefully selected to avoid overruns in the RTS target. In what follows, this parameter has been set to 100 µs.

Indeed, a virtual PMU is seldom simulated alone. Typically, a simulated electrical grid might integrate several tens of PMUs. In this respect, several virtual PMUs were included in the same model in order to assess the maximum number of PMU that can be simulated by a single core of the RTS. The test results are presented in Table 5.2 and refer to an integration time-step of 100 µs and to 3 different virtual PMU models, equipped with 1, 6 and 12 input channels respectively.

To conclude, let us recall that:

- The synchrophasor estimation algorithm implemented in the simulated PMU is also embedded in PMU prototypes deployed in three field trials to assess the performance of the PDC data-pushing logic. Results are given in Section 5.3.
- The assessment of the performance of the protection scheme and control mechanism is provided in Section 5.4 and 5.5, respectively. The results are obtained by using simulated PMUs and the setup here described.

5.2 The field trials

As anticipated at the beginning of the chapter, this section presents the field trials in which the functions described in this manuscript have been deployed and validated.

5.2.1 Services industriels de Lausanne

The Services industriels de Lausanne (SiL), the Network Operator of the city of Lausanne, has deployed a PMU-based advanced and upgradable monitoring system on its 125 kV sub-transmission network that eventually will constitute the backbone of their future SCADA system.

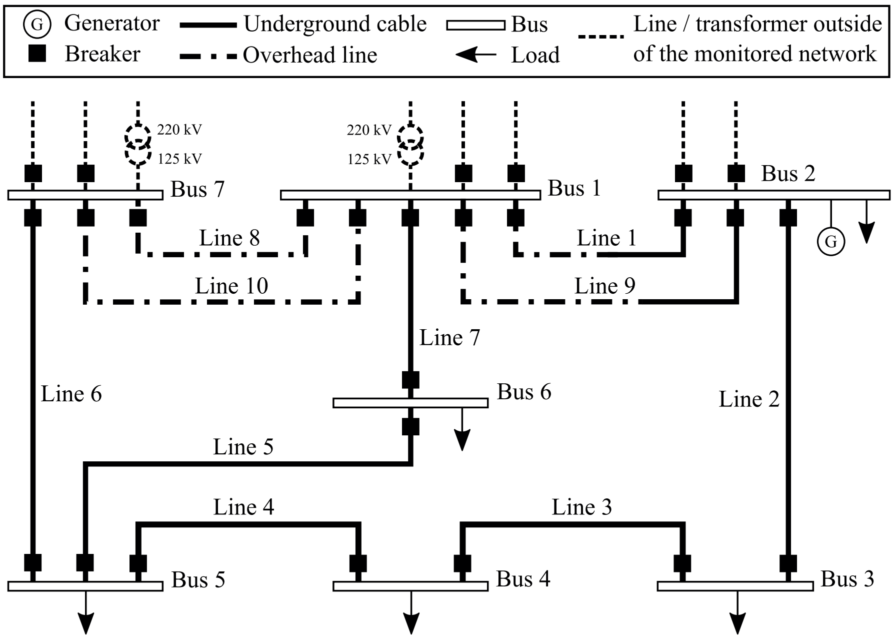


Figure 5.4 – Network topology of the monitored portion of the 125 kV power network of Lausanne city, together with the breaker position.

Power network and sensing

The electrical network is composed of 7 electrical substations as shown in Fig. 5.4. The lines are mainly underground cables with the exception of: (i) Line 8 and 10 (two parallel overhead lines), and (ii) Line 1 and 9 (two parallel lines) that are split in two sections: starting from bus #1, they are composed of 3.682 km of overhead line and 1 km of underground cable (see Table 28 in Appendix 5.5.4 for details about the line parameters). No zero-injection buses are present. The points of connection to the 220 kV grid are buses 1 and 7. The local distribution network is fed by step-down transformers from buses 2, 3, 4, 5 and 6. Additionally, a non-monitored portion of the 125 kV network departs at buses 1, 2 and 7.

The voltage and current signals fed to the PMUs are obtained from standard potential (PTs) and current transformers (CTs). The PT and CT accuracy-classes (0.2- or 0.5-class) are specified in Table 29 in Appendix 5.5.4. The PT and CT full-scales are 125 kV and 600 A, respectively. The ratio errors and phase displacements are derived from the accuracy class by using the Standards [36] and [37].

Each PMU is equipped with 8 voltage and 8 current channels, therefore it can be connected to maximum 2 three-phase (plus neutral) power lines. A PMU is installed at both ends of each line and measures the nodal-voltage and current-flow synchrophasors in each of the three phases, for a total of 15 PMUs deployed in the network. This corresponds to a very large measurement redundancy of 5.7. The PMUs are based

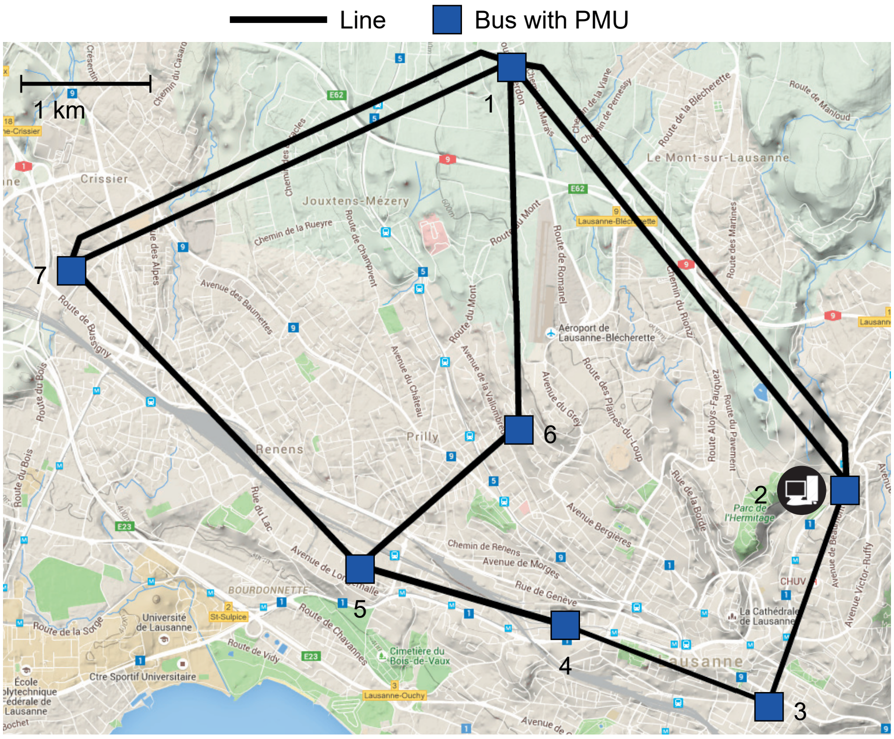


Figure 5.5 – Network topology of the SiL 125 kV sub-transmission grid showing the PMUs and PDC locations.

on the National Instruments Grid Automation System, a programmable CompactRIO platform with PMU capability that meets the IEEE Std. C37.118.1-2011 measurement requirements for both classes P and M. The PMUs are configured to meet the P-class performance requirements, implementing the synchrophasor estimation algorithm presented in [39]. Each PMU is also equipped with an 8-channels digital-input module to monitor in real-time the status of breakers and switches[1] whose location is also represented in Fig. 5.4.

Data communication

The PMUs stream UDP frames with a reporting rate of 50 fps. The total UDP frame size can vary depending on the number of lines that are effectively monitored by each PMU. The size is 134 bytes when streaming a single set of phasors (together with frequency, ROCOF and power values) and 198 bytes when streaming 2 sets of phasors.

The telecommunication physical channel is the legacy optical fiber of SiL. Each substation is equipped with a switch connecting the optical fiber and the PMUs through an Ethernet cable. The communication is established through a dedicated Virtual LAN.

---

[1] The presence of a line breaker at both ends of each line and the possibility of including its status in the PMU packet, enables us to obtain in real-time the network topology.

Data process-and-operation

The PDC is equipped with a GPS receiver that provides the absolute time with a resolution of 1 ms due to the limited precision of the LabVIEW *get time* function. The PDC is running on a workstation placed in the control room of SiL (see Fig. 5.5) equipped with an Intel Xeon Processor at 2.4 GHz, 8 GB of RAM and running Windows Server 2008. The PDC supplies at a constant reporting pace (i.e., 50 fps) a real-time linear state estimator of the sub-transmission grid of Lausanne, a user interface that displays in real-time both the measured and the estimated values and a local database.

5.2.2 EPFL campus

The power grid of the EPFL campus is a particularly challenging distribution network where all the peculiarities of ADN are present. The lines are short (most of them below 100 m), and the load demand is largely variable in function of the hour of the day and the weather conditions. Moreover, active power injections are present as 2 MW of photovoltaic panels are installed together with 6 MW of combined heat and power generation units. These conditions, and the large use of power electronics, heavily affect the voltage and current profiles which makes the EPFL campus a challenging test bed for the developed infrastructure. Indeed, the analysis carried out in [35] has shown that PMUs deployed in distribution network need to be characterized by an accuracy well below the 1% TVE dictated by the reference Standard [38].

Power network and sensing

The electrical network is composed of 5 electrical substations as shown in Fig. 5.6. The lines are underground cables, the parameters are reported in Table 30 in Appendix 5.5.4. Each substation is equipped with a class-P PMU prototype [39] based on the National Instruments CompactRIO 9068, composed by a reconfigurable Artix-7 FPGA and a dual-core ARM Cortex-A9 processor and equipped with a customized Linux-RT OS. The chassis has been equipped with a stationary GPS unit (NI-9467) for the synchronization to the UTC-time and two analog input modules (NI-9215) characterized by an input range of $\pm$ 10 V and a sampling frequency of 50 kHz. The synchrophasor extraction algorithm is the same as the one deployed in the RTS, as shown in Section 5.1.1.

The 3-ph nodal voltages and nodal injected currents are transformed to low voltage signals by means of Altea CVS-24, that consists of 0.1-class capacity voltage dividers and 0.5-class Rogowski coils [159]. The connection between the sensors output and the PMU is obtained by means of dedicated shielded-cables of equal fixed length for all the substations. The connection between the GPS antenna mounted on the rooftop and the PMU is made using RG213 cables in order not to attenuate the GPS signal also with more than 100 meters of cables. The cable length delay is suitably compensated

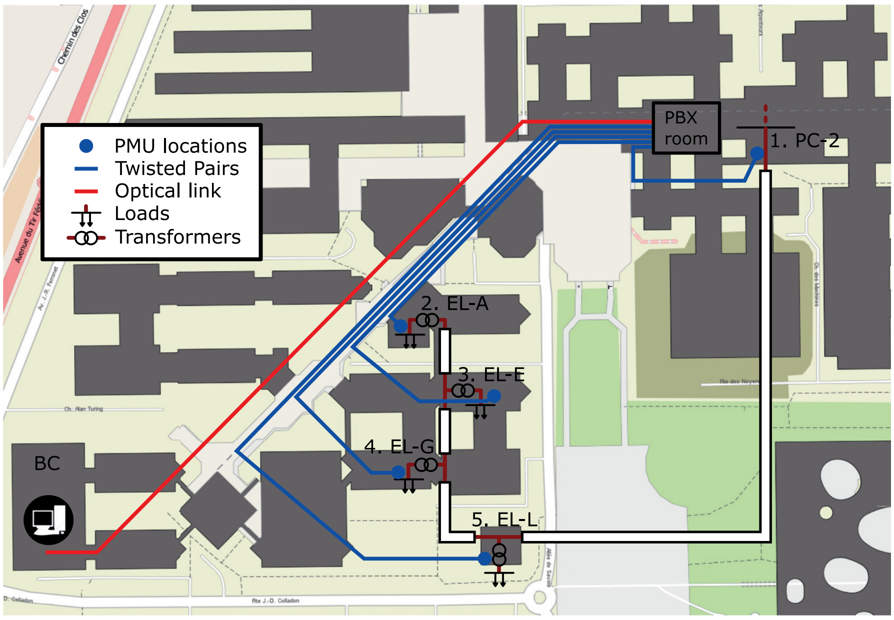


Figure 5.6 – Network topology of the power distribution feeder of the EPFL campus, together with the adopted PMU placement and PDC location.

on the PMU side. An example of elements composing a typical substation setup is shown in Fig. 5.7.

Data communication

The PMUs stream UDP frames with a reporting rate of 50 fps. The total UDP frame size can vary between 66 and 138 bytes according to the number of transformers to monitor. To avoid packet losses, the communication network is duplicated by means of a parallel redundancy protocol called IPRP. UDP packets are duplicated at the PMU side and the duplicates are removed once they reach the PDC. The design and implementation of the protocol are given in [44]. Expensive cable deployments are avoided by re-using existing twisted pair cables (2 Mb/s), originally installed for telephony. The cables are passive and are stare-wired from a central point, the "PBX room" in Fig. 5.6. For communication from this room to the location where the PDC is installed, an optical fiber at 100 Mb/s is used. The whole network is resilient to up to 8 hours of power outage. Additionally, security mechanisms are also in place to ensure that the ICT infrastructure is robust to insider and outsider cyber-attacks, following the security solutions and best practices for ADNs given in [160].

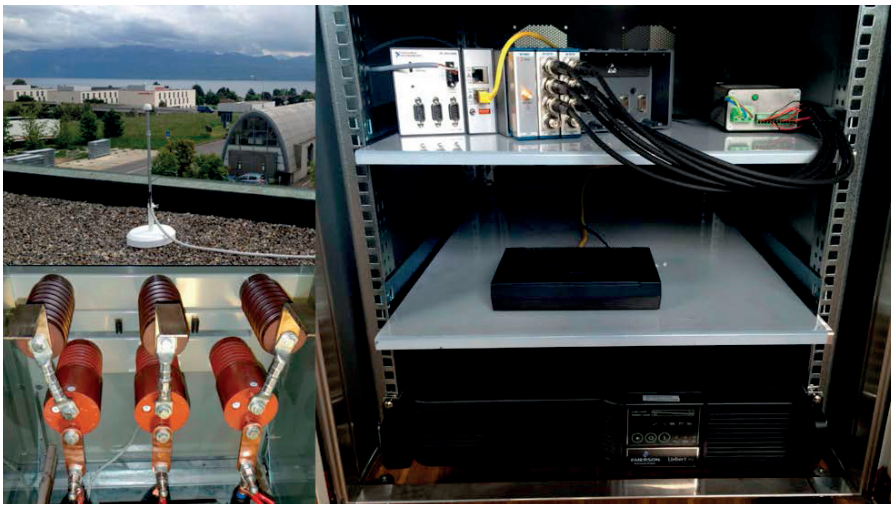


Figure 5.7 – Components installed in the equipped EPFL-campus substations: GPS antenna (top left), Altea CVS-24 current and voltage sensors (bottom left) and rack containing: the PMU (top shelf), the SHDSL modem (middle shelf) and the UPS (bottom shelf).

Data process-and-operation

A GPS-synchronized PDC (2 processors quad-core, 2.7 GHz) runs in a Scientific Linux 7 operating system. The same machine is also hosting a DKF estimator. Raw measurements and state estimator outputs, as well as the historical data, are made public through a web interface[2]. Every stored file contains one hour of data; it is a self-explanatory text file that is digitally signed. Other research institutes have already used the provided historical data for different purposes [161, 162].

5.2.3 Alliander - the BML feeder

Alliander, one of the DNOs of the Netherlands, has deployed, in the framework of the FP7 project C-DAX [33], a PMU-based monitoring system on a medium voltage (10 kV) distribution feeder.

Power network and sensing

The BML feeder is composed of a primary substation supplying multiple feeders including the monitored one composed of 17 secondary substations supplying the surroundings of the city of Huissen. The substations are connected as shown in Fig. 5.8 by means of underground cables with cross sections from 95 to 240 mm^2. The line parameters are provided in Table 31 in Appendix 5.5.4. A total of 10 class-P PMUs, based

---

[2] http://smartgrid.epfl.ch/

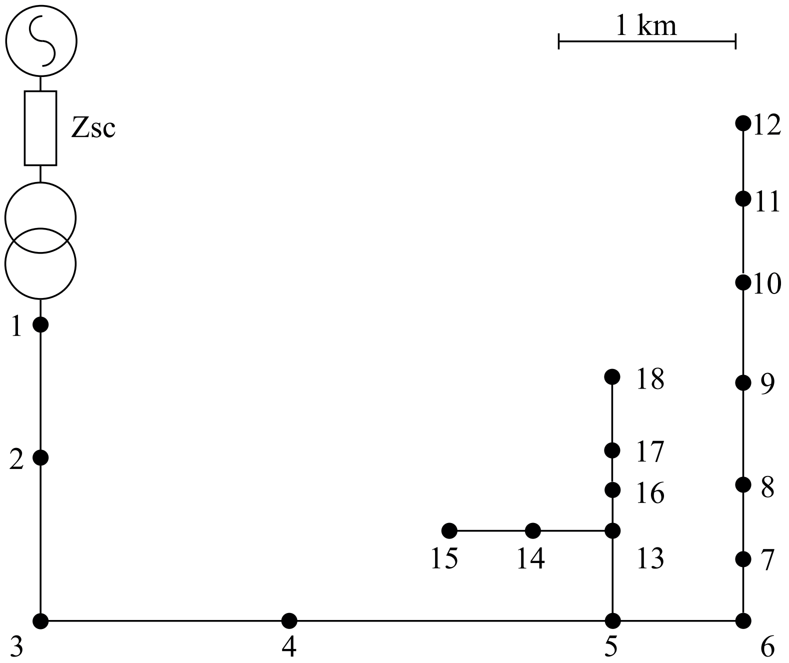


Figure 5.8 – Network topology of the Alliander 18-bus power distribution feeder, together with the adopted PMU placement. Line lengths are in scale.

on the same platform and synchrophasor extraction algorithm adopted in the EPFL campus, have been installed in 10 buses. The PMU location depends on installation constraints set by the DNO, as well as on the network observability. In the primary substation (i.e., bus #1) a PMU measures nodal-voltage and current flow, in all the secondary substations where PMUs are installed, they measure nodal voltage and injected current synchrophasors.

Data communication

The PMUs stream two sets of phasors, together with frequency and ROCOF, for a total UDP frame size of 116 bytes.

PMU data are streamed through a public 4G LTE network, provided by the local service provider Vodafone, to a PDC running in the Alliander data center in Haarlem (see Fig. 5.9).

In order to support the PMU data stream, each PMU has been connected to dedicated 4G routers through the CompactRIO Ethernet switched interface. The Wide Area Network (WAN) interface of the routers connects to the Vodafone network through a dedicated IP address range without any specific service level implemented, so that the PMU traffic is not prioritized. The advantages of such a wireless solution are its high availability, its cost-effectiveness and its easy deployment. Nevertheless, the main dra-

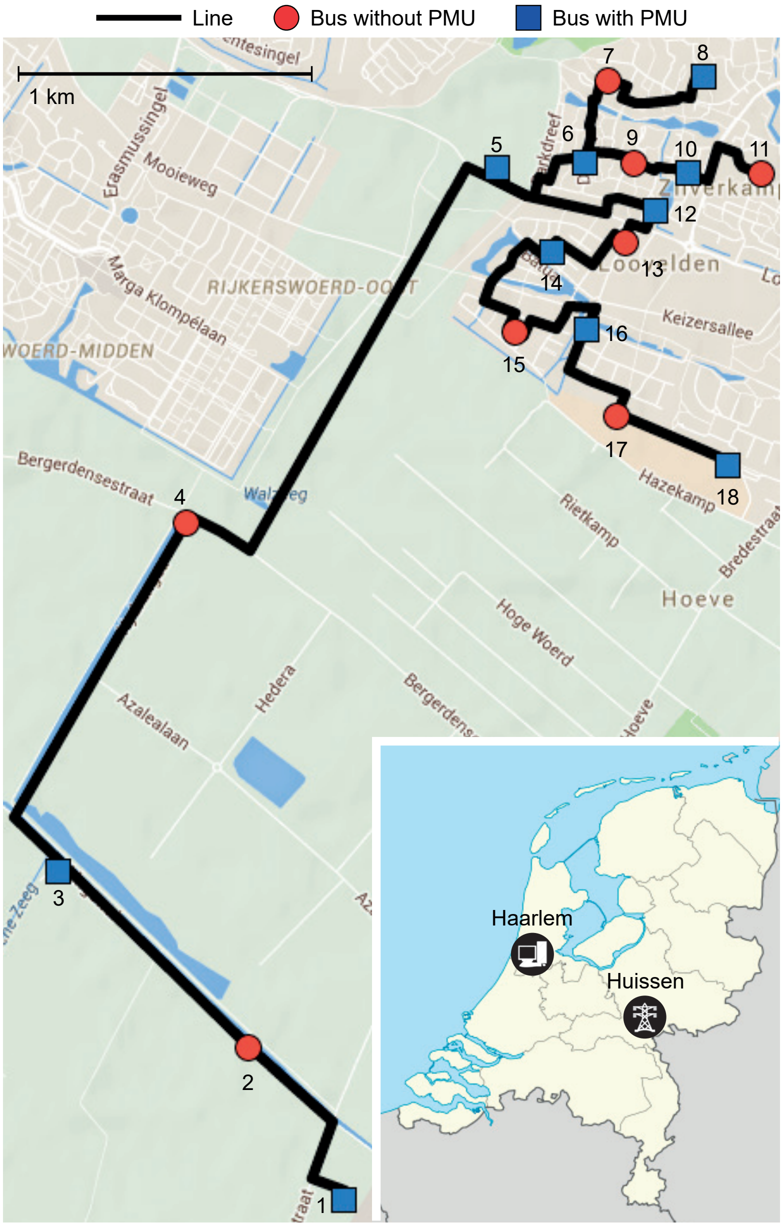


Figure 5.9 – Network topology of the Alliander 10 kV feeder showing the PMUs and PDC locations.

Table 5.3 – Summary of the three presented field trials.

	Network			PMU		Communication type
	V_n [$kV_{rms_{LL}}$]	# nodes	# lines	#	Class	
SiL	125	7	10	15	P	fiber
EPFL	20	5	4	5	P	twisted pairs and fiber
Alliander - BML	10	18	17	10	P	4G

wback is that the latency depends on the real-time availability of the wireless physical mean and on the instantaneous network load, which leads, to short-term variations of the network latency and eventual data incompleteness or packet reordering (discussed in Section 5.3.1).

Data process-and-operation

The PDC is equipped with a GPS receiver that provides the absolute time with a resolution of 1 ms due to the limited precision of the LabVIEW *get time* function. The PDC is integrated in a Linux RedHat server equipped with an Intel Xeon CPU at 2.00 GHz and 64 GB of RAM that supplies, at 50 fps, a real-time state estimation process used to monitor the nodal voltage and line power flow variations of the feeder.

The main characteristics of the field trials in which the PDC data pushing logics are validated, are summarized in Table 5.3. Additionally, by leveraging on the synchrophasor networks here described, real-time state estimation (RTSE) has been deployed and experimentally validated. This enabled the network operators to monitor the state of their electrical networks with latency in the order of tens-hundred ms and a refresh rate of 20 ms. Details about the validation of the RTSE in the presented field trials in [32, 47].

5.3 Phasor data concentrator

The PDC architecture and the three data-pushing logics presented in Chapter 3.1.1 were deployed and experimentally validated in the SiL, EPFL and BML field trials.

The data flow is tracked along the whole process by measuring the data frame timestamps t_s, their arrival times t_a and the PDC push time t_p[3]. The synchrophasor data latency of each data frame and the PDC reporting latency of each time-aligned dataset are computed for the various data pushing logics presented in Section 3.1.1. In parti-

---

[3] A Real-Time Operating System (RTOS) would provide more deterministic performance. However, neither of the field trials implemented the PDC on a RTOS.

cular, four different data pushing logics are examined over an observation window of 24 hours:

1. absolute time logic (hereafter referred as Logic 1);
2. absolute time integrating push-when-complete logic (hereafter referred as Logic 2);
3. relative time logic (hereafter referred as Logic 3);
4. relative time integrating push-when-complete logic (hereafter referred as Logic 4).

For each field trial, the experimental results are presented by means of three histograms representing the probability density function (PDF) of the following quantities:

a) the aggregated synchrophasor data latencies from all PMUs;
b) the comparison between the PDC reporting latency in Logics 1 and 2;
c) the comparison between the PDC reporting latency in Logics 3 and 4.

Also, for each data pushing logic, the dataset incompleteness is presented by means of a table showing the percentage of incomplete datasets pushed by the PDC during the 24 hours observation window.

In order to properly set the PDC wait time, a preliminary test is performed to measure the characteristic synchrophasor data latencies of all the field trials together with their jitter over a time window of 24 hours. This quantity has then been set to guarantee the collection of the majority of the data frames with a particular time-stamp, independently of the adopted data pushing logic. The adoption of a constant PDC wait time represents the most classic approach to define a proper PDC wait time. Nonetheless, other approaches are available in the literature. For example, the PDC wait time could be adapted along the day based on recent PMU traffic delay patterns, as proposed in [75].

5.3.1 Real field validation

SiL field trial

The experimental results are presented in Fig. 5.10. Both the absolute and relative PDC wait time are set by analyzing the aggregated synchrophasor data latencies from all PMUs measured along an interval of 24 hours, as shown in Fig. 5.10a. The histogram

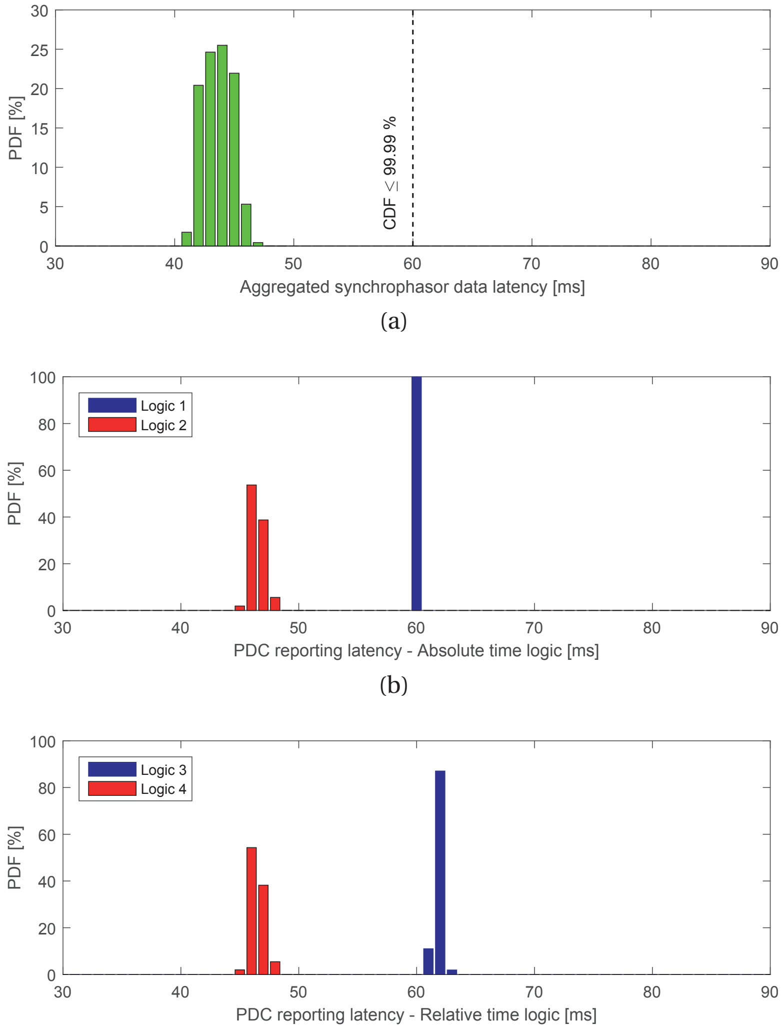
Table 5.4 – Dataset incompleteness when adopting different data pushing logics in the SiL field trial.

	% of incomplete datasets			
Missing data frames	Logic 1	Logic 2	Logic 3	Logic 4
1	$2.3 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$	0	0
2	0	0	0	0
3	$6.8 \cdot 10^{-5}$	$6.8 \cdot 10^{-5}$	$4.5 \cdot 10^{-5}$	$4.5 \cdot 10^{-5}$
>3	$1.5 \cdot 10^{-3}$	$1.5 \cdot 10^{-3}$	$5 \cdot 10^{-4}$	$5 \cdot 10^{-4}$
Total	$1.6 \cdot 10^{-3}$	$1.6 \cdot 10^{-3}$	$5.4 \cdot 10^{-4}$	$5.4 \cdot 10^{-4}$

represents the aggregated data, because an analysis by PMU data stream showed no significant differences among the various PMUs. As it can be noticed, they are characterized by a mean value of 44 ms and standard deviation of 2 ms. Nevertheless, as more than 99.99% of the packets is received with a latency smaller than 60 ms, the absolute PDC wait time T_{abs} is set to this value. Besides, the average amount of time needed to receive all data frames with specific time-stamp is 3 ms, whereas more than 99.99% of datasets take less than 20 ms to complete. Hence, the relative PDC wait time T_{rel} is set to 20 ms.

The comparison between Logics 1 and 2 (Fig. 5.10b) shows the improvement introduced by adopting the push-when-complete logic, that enables to reduce the PDC reporting latency by 14 ms. Nevertheless, the latter increases the jitter of the PDC reporting latency that is less deterministic compared to Logic 1 as it is always influenced by the arrival time of the last-received data frame with a specific time-stamp. The push-when-complete logic also reduces the PDC reporting latencies when adopting a relative time data pushing logic, with an average improvement of 15 ms (see Fig. 5.10c comparing Logics 3 and 4). In such a case the PDC reporting latency jitter is slightly improved by adopting Logic 4 but it is still non-deterministic as in case of Logic 1.

Based on the adopted PDC wait time setting (T_{abs} =60 ms, T_{rel} =20 ms), the incompleteness of the time-aligned datasets is presented in Table 5.4. As expected, when transmitting data frames through a dedicated wired telecom infrastructure, the dataset incompleteness is negligible and in the order of few parts per million regardless of the adopted data pushing logic. Nevertheless, occasionally, the PMU data frames are simultaneously delayed by a considerable amount of time and do not reach the PDC before the expiration of the absolute PDC wait time. This causes the PDC to push empty data-sets in case of Logics 1 and 2, yielding to a total data-set incompleteness that is one order of magnitude higher compared to Logics 3 and 4.

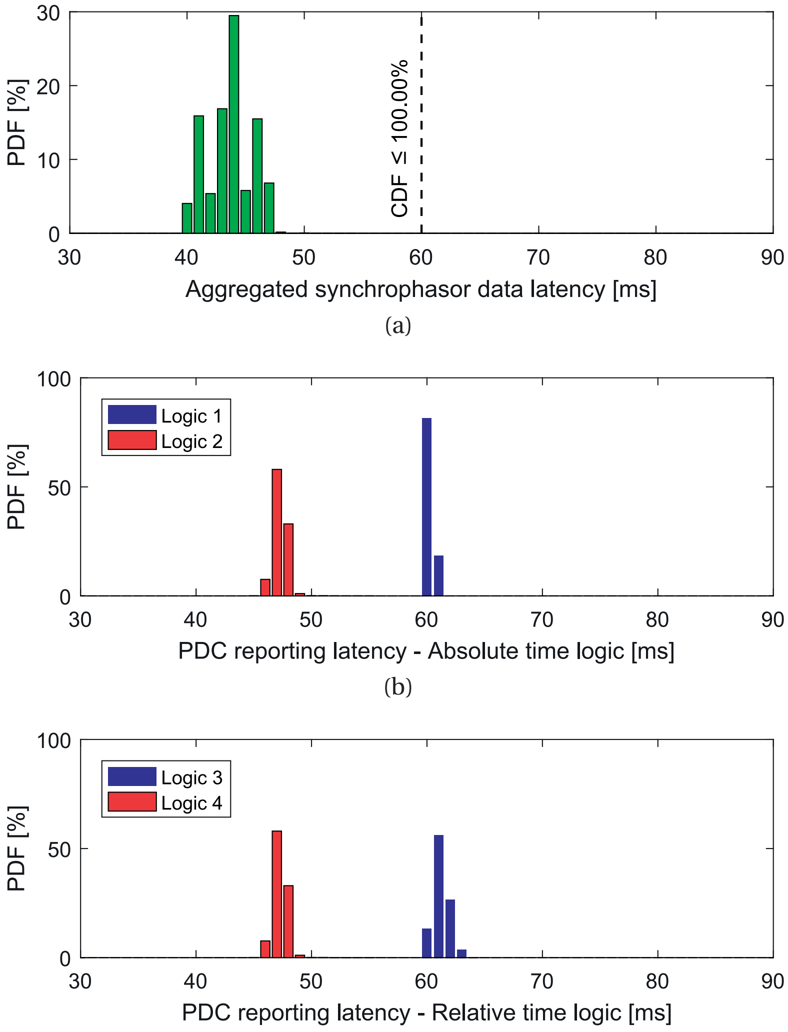


(a)

(b)

(c)

Figure 5.10 – Experimental results in the SiL field trial showing the PDF of: (a) the combined synchrophasor data latencies; (b) the PDC reporting latency when adopting an absolute time logic (Logic 1) and when integrating it with a push-when-complete logic (Logic 2); c) the PDC reporting latency when adopting a relative time logic (Logic 3) and when integrating it with a push-when-complete logic (Logic 4).



(a)

(b)

(c)

Figure 5.11 – Experimental results in the EPFL field trial showing the PDF of: (a) the combined synchrophasor data latencies; (b) the PDC reporting latency when adopting an absolute time logic (Logic 1) and when integrating it with a push-when-complete logic (Logic 2); c) the PDC reporting latency when adopting a relative time logic (Logic 3) and when integrating it with a push-when-complete logic (Logic 4).

Table 5.5 – Dataset incompleteness when adopting different data pushing logics in the EPFL field trial.

	% of incomplete datasets			
Missing data frames	Logic 1	Logic 2	Logic 3	Logic 4
1	$2.9 \cdot 10^{-2}$	$2.9 \cdot 10^{-2}$	$2.8 \cdot 10^{-2}$	$2.8 \cdot 10^{-2}$
2	$9.2 \cdot 10^{-5}$	$9.2 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$
3	$6.9 \cdot 10^{-5}$	$4.6 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$
>3	$2.3 \cdot 10^{-5}$	$4.6 \cdot 10^{-5}$	0	0
Total	$2.9 \cdot 10^{-2}$	$2.9 \cdot 10^{-2}$	$2.8 \cdot 10^{-2}$	$2.8 \cdot 10^{-2}$

EPFL field trial

The experimental results are presented in Fig. 5.11. Both the absolute and relative PDC wait time are set by analyzing the aggregated synchrophasor data latencies from all PMUs measured along an interval of 24 hours, as shown in Fig. 5.11a. The histogram represents the aggregated data. The aggregated data are characterized by a mean value of 44 ms and standard deviation of 2 ms. The SiL and EPFL communication networks are both wired, so we decided to set the absolute PDC wait time T_{abs} to 60 ms as for the SiL case. Besides, the average amount of time needed to receive all data frames with specific time-stamp is 4 ms, whereas more than 99.99% of datasets take less than 20 ms to complete. Hence, the relative PDC wait time T_{rel} is set to 20 ms.

The comparison between Logics 1 and 2 (Fig. 5.11b) shows the improvement introduced by adopting the push-when-complete logic, that enables to reduce the PDC reporting latency by 13 ms. Nevertheless, the latter increases the jitter of the PDC reporting latency that is less deterministic compared to Logic 1 as it is always influenced by the arrival time of the last-received data frame with a specific time-stamp. The push-when-complete logic also reduces the PDC reporting latencies when adopting a relative time data pushing logic, with an average improvement of 14 ms (see Fig. 5.11c comparing Logics 3 and 4). In such a case the PDC reporting latency jitter is slightly improved by adopting Logic 4 but it is still non-deterministic as in case of Logic 1.

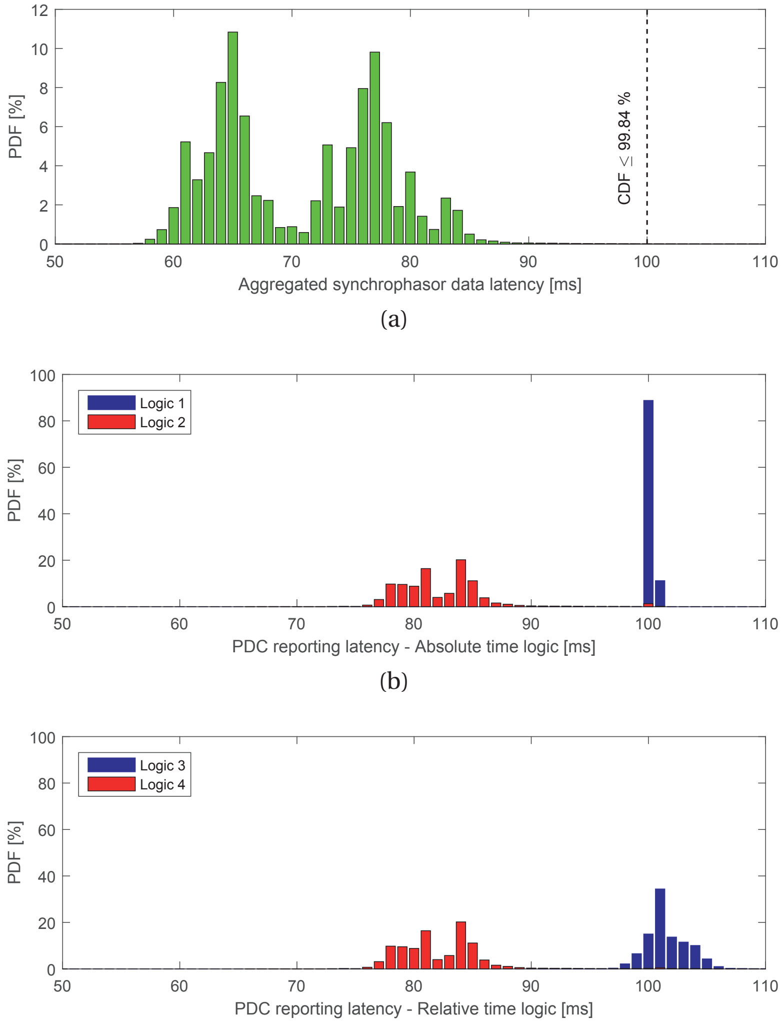
Based on the adopted PDC wait time setting (T_{abs} =60 ms, T_{rel} =20 ms), the incompleteness of the time-aligned datasets is presented in Table 5.5. As expected, the wired telecom infrastructure ensures an almost negligible dataset incompleteness regardless of the adopted data pushing logic. Nevertheless, occasionally, a single PMU data frame does not reach the PDC before the expiration of the absolute and relative PDC wait time. This causes the PDC to push data-sets with a single missing data frame regardless of the adopted data pushing logic.

Alliander - BML field trial

Fig. 5.12 shows the experimental results for the Alliander field trial. The absolute and relative PDC wait times have been set according to the measured synchrophasor data latencies shown in Fig. 5.12a. As it can be noticed, by adopting a 4G telecom infrastructure, the measured synchrophasor data latency shows a bimodal distribution characterized by a mean value of 70 ms that, as expected, is higher than the SiL case. The same distribution can be observed by analyzing each PMU data stream separately. Such a behavior could be attributed to the varying conditions of the wireless medium (e.g., interference, noise, congestion, etc.) across the duration of the measurement. However, as the public 4G network operator did not provide any additional detail on the network topology and data traffic, a deeper investigation is not possible. Moreover, the measured distribution highlights a behavior that is typical of 4G LTE networks, that is the presence of several outliers scattered through time and through PMU data stream, characterized by a synchrophasor data latency up to 1 second (not visible in Fig. 5.12a). For this reason, the absolute PDC wait time has been set to 100 ms, as a trade-off between the lowest achievable PDC reporting latency and an acceptable dataset completeness. In particular, within 100 ms, more than 99.84% of data frames are received at the PDC, which is acceptable for the supplied applications, whereas augmenting the threshold up to 1 second would not bring a significant improvement. Besides, the average amount of time needed to receive all data frames with specific time-stamp is 22 ms, and more than 98.91% of datasets are completed within 40 ms. Hence, the relative PDC wait time T_{rel} is set to 40 ms.

The improvements introduced by adopting the push-when-complete logic are visible for both absolute and relative time logics. In particular, Fig. 5.12b and 5.12c show an average reduction of the PDC reporting latency of 18 and 19 ms respectively. This comes at the price of a higher jitter of the PDC reporting latency that, in such a case, is highly affected by the real-time variation of the 4G network latency. Looking at the same figures, it is also evident how the only logic that guarantees a certain determinism in the PDC reporting latency is Logic 1 as it is the only one that is not influenced by the data frame arrival time.

Finally, the dataset incompleteness is presented in Table 5.6. Compared to the SiL and EPFL cases, the 4G network performance, and particularly its latency variations, considerably affect the dataset completeness that is strongly influenced by the choice of the absolute and relative PDC wait time. In particular, based on the adopted PDC wait time settings, (T_{abs} =100 ms, T_{rel} =40 ms), the reported cumulative data incompleteness is around 1.4% in the case of Logics 1 and 2 and around 1.2% in the case of Logics 3 and 4.



(a)

(b)

(c)

Figure 5.12 – Experimental results in the Alliander field trial showing the PDF of: a) the aggregated synchrophasor data latencies from the 10 PMUs; b) the PDC reporting latency when adopting an absolute time logic alone (Logic 1) and when integrating the push-when-complete logic (Logic 2); c) the PDC reporting latency when adopting a relative time logic alone (Logic 3) and when integrating the push-when-complete logic (Logic 4).

Table 5.6 – Dataset incompleteness when adopting different data pushing logics in the Alliander field-trial.

	% of incomplete datasets			
Missing data frames	Logic 1	Logic 2	Logic 3	Logic 4
1	1.295	1.295	1.193	1.192
2	0.027	0.027	0.018	0.018
3	0.009	0.009	0.005	0.005
>3	0.042	0.042	0.013	0.013
Total	1.372	1.372	1.229	1.229

5.3.2 Conclusions

In this section we experimentally validated the architecture of a PDC that integrates both the absolute and relative time data pushing logics together with a third one that enables to minimize the PDC latency without decreasing the data completeness. We have assessed the performance of the developed PDC and related logics within the context of three real PMU installations that adopt different communication infrastructures (i.e., optical fiber links, combination of twisted pairs and optical link and wireless 4G LTE public network).

The assessment of the PDC performance has quantified the influence of the adopted telecom infrastructure and PDC data pushing logic on the achievable PDC reporting latency. In particular the experimental validation has demonstrated that the push-when-complete logic is characterized by the lowest PDC latency, that is only influenced by the synchrophasor data latency: in the case of optical fiber links the PDC latency is on average 3 ms, whereas in the case of a 4G network, this value increases to 12 ms. Nevertheless, the latency reduction introduced by this logic involves a reduced determinism of the outgoing PDC data flow. As a consequence, in order to correctly operate, this logic has to be properly coupled with dedicated FIFO structures to mitigate the variations in the PDC reporting latency.

On the contrary, the only logic that, independently of the network characteristics, is capable of guaranteeing a constant PDC reporting latency and the consequent mitigation of the synchrophasor data latency variations is the absolute one. In such a case, the PDC reports time-aligned datasets at a constant reporting rate (corresponding to the PMU one) with a PDC reporting latency that is fixed and coincides with the absolute PDC wait time. In such a case, the average PDC latency is approximately 16 ms in the case of optical fiber links (SiL) and twisted pairs coupled with an optical link (EPFL) and 30 ms in the case of 4G network (Alliander).

Finally, the experimental validation has highlighted the importance of properly selecting the PDC wait time due to its influence on the PDC reporting latency and the dataset completeness. The latter, particularly in the case of non-deterministic networks, might be degraded up to values that do not enable to exploit any longer the availability of synchrophasor data. More specifically, regardless of the adopted data pushing logic, in the case of wired links the cumulative dataset incompleteness is in the order of few parts per million, whereas in the case of 4G network is in the order of 1%.

5.4 Fault identification and location in RTS

The PMU-based fault detection and faulted line identification method presented in Chapter 3.2.1 is experimentally validated by means of the RTS setup described in Section 5.1. In order to reproduce realistic conditions into the RTS, we have adopted the following working hypothesis:

- Noise levels derived from PMU measurements recorded in the distribution feeder of the EPFL campus have been used;
- A real PMU synchrophasor extraction algorithm, as described in Section 5.1.1, has been adopted.
- The method has been validated for both transmission and distribution networks, as its performance is not dependent on (i) network voltage level and configuration (e.g., transmission or distribution, radial or meshed); (ii) presence of DG; (iii) neutral connection (i.e., solid-earthed or unearthed neutral); (iv) type of fault (symmetric and asymmetric); and (v) its impedance (i.e., low- or high-impedance).

5.4.1 Simulation environment

In order to assess the accuracy and time latency of the proposed method we have modeled in the RTS both the Alliander distribution feeder described in Section 5.2.3 and a commonly used test transmission network. In what follows, details about the modeling of the networks and the adopted measurement noise models are given.

Network description

Distribution network: The Alliander field trial (i.e., the BML distribution feeder) described in Section 5.2.3 has been modeled in SimPowerSystem$^{\text{TM}}$. The lines are modeled with the equivalent PI circuit, the upstream grid has a short-circuit power of 1000 MVA and it is modeled with the short-circuit impedance Z_{sc} (we assumed a resistance to reactance ratio R_{sc}/X_{sc}=0.1). The high to medium voltage transformer can be either

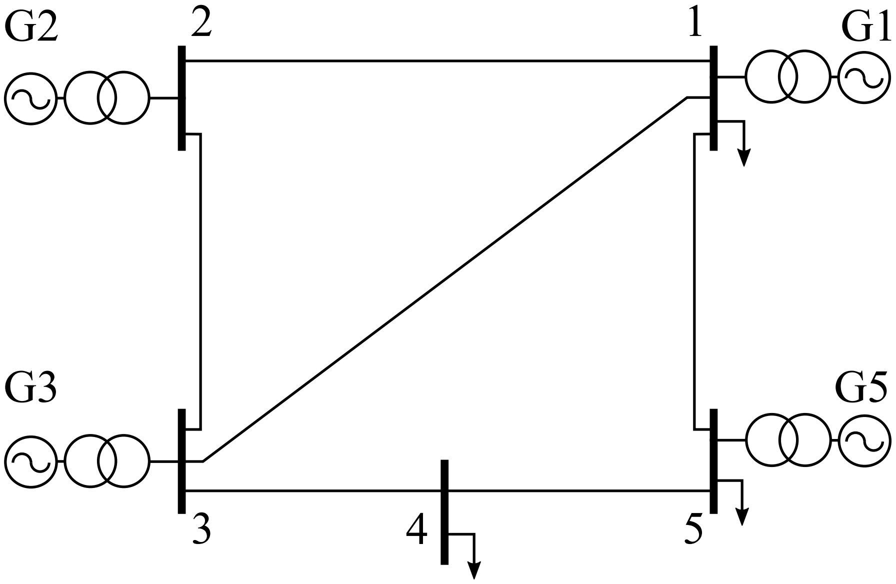


Figure 5.13 – Network topology of the 5-bus transmission test network adopted for the validation.

Yg-Yg or Yg-Y, according to the simulation scenario that might request earthed or unearthed neutral networks, respectively. The loads are modeled as star connections of impedances. In normal operating conditions they absorb approximately 1/4 of the rated power of the real transformers to which they are connected (see Table 32 in Appendix 5.5.4 for details about the rated powers of the transformers).

Transmission network: The network used is a modified version of the PJM 5-bus system. Its layout is reported in Fig. 5.13. The injected/absorbed powers together with the line parameters are provided in [163]. The network has been modeled in SimPowerSystem$^{\text{TM}}$. The lines are modeled with the equivalent uncoupled PI circuit. The medium to high voltage transformers are Yg-Yg, a common choice in transmission networks. The loads are modeled as star connections of impedances. In normal operating conditions they absorb the active and reactive power provided in [163]. Loads are connected to buses 1, 4 and 5.

Adopted PMUs vs. common practice

The modeled networks have been equipped with PMUs at every bus measuring nodal voltage and injected current phasors. The implementation of the synchrophasor extraction algorithm in the RTS have been already shown in Section 5.1.1. The use of simulated PMUs makes the validation of the proposed method more realistic compared to the common practice of using synchrophasors generated from the true state. Indeed, the adoption of a real synchrophasor estimation algorithm enables us to include in the analysis the response time of the PMU during transients. The latter is mainly affected

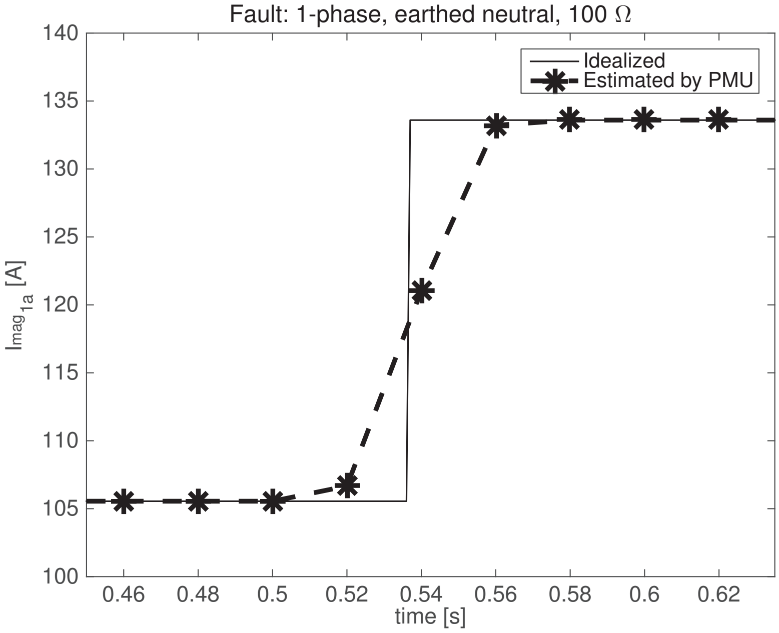


Figure 5.14 – Comparison between the current phasor magnitude estimated by the simulated PMU in bus #1 of the BML feeder during a fault versus the idealized current phasor magnitude.

by the window length used by the algorithm and the position of the time-stamp within the window. A comparison of the time evolution of the current phasor magnitude estimated by the modeled PMU in bus #1 of the BML feeder during a fault versus the idealized current phasor magnitude is given in Fig. 5.14. It can be seen that for this specific class-P PMU characterized by a window length of 3 periods and the time-stamp centered in the window, the magnitude estimate takes 4 time-steps to reach the pre-fault accuracy level. This aspect is taken into account in Section 5.4.2 to assess the total latency of the proposed method.

Measurement noise model

In the literature, the robustness of fault detection and location algorithms is tested with respect to the measurement noise [164]. The simulated PMU introduces only the noise due to the synchrophasor estimation algorithm. It is then needed to superimpose a measurement noise to the synchrophasors estimated by the simulated PMU. The noise should also include the effect of the sensor interfacing the PMU to the network. In order to generate a realistic noise, real-field data have been used.

We have considered real measurements taken in the EPFL campus. Fig. 5.15 shows the magnitude and phase of nodal voltage and injected current measurements. Note that these measurements include the noise introduced by the combination of sensor and

PMU. The corresponding standard deviations (stds) are:

$$\begin{aligned} \sigma_{V_{mag}} &= 1.6 \cdot 10^{-3}\% \qquad & \sigma_{V_{ph}} &= 5.1 \cdot 10^{-5}[\text{rad}] \\ \sigma_{I_{mag}} &= 4.0 \cdot 10^{-1}\% \qquad & \sigma_{I_{ph}} &= 5.8 \cdot 10^{-3}[\text{rad}] \end{aligned} \tag{5.2}$$

Furthermore, Fig. 5.16 shows that the Gaussian assumption of the measurement noises is fulfilled. The voltage and current phases are referred to the phase of another quantity (see Fig. 5.15b and 5.15d) because the phase is continuously changing due to the fact that the real system frequency is not exactly 50 Hz. The std of the voltage phase is $1/\sqrt{2}$ of the one of $(E_{ph_{1a}} - E_{ph_{5a}})$ since we assume that the two voltage noises have the same std and are uncorrelated (the same assumption holds for the voltage magnitude noise). On the contrary, we entirely attribute the noise of $(I_{ph_{1c}} - E_{ph_{1c}})$ to the current phase. We assume the measurement noise to be the same for transmission and distribution networks. Indeed, it is important to observe that the graphs of Fig. 5.15 include both the measurement noise and the network dynamics, therefore the computed stds are overestimated for transmission networks that are usually considered in quasi steady-state.

Further assumptions have to be made for distribution networks in order to simulate the realistic behavior of the sensing system:

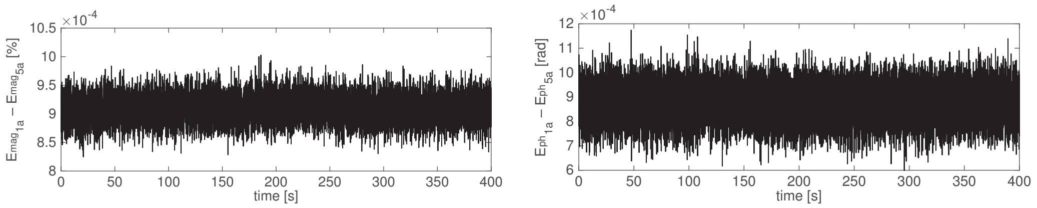
1. We use current protection sensors in bus #1 of the BML feeder to measure the current during the fault. Their accuracy is assumed to be 10 times worse than the one defined in (5.2).
2. The 1-phase low impedance fault in an unearthed neutral network leads the voltage in the faulted phase to drop to around 0.6 % of the rated value. In this specific case, we consider an accuracy of these voltage measurements to be 100 times worse than the one defined in (5.2).

In the next section we carry out a sensitivity analysis of the proposed fault location algorithm with respect to the measurement noise.

5.4.2 Performance Assessment

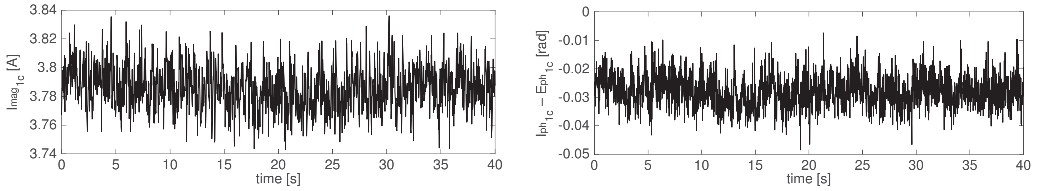
This section provides the performance assessment of the method with respect to the considered scenarios.

The accuracy of the proposed method in identifying the line affected by the fault has been extensively tested. The scenarios refer to different combinations of the following factors:



(a) Voltage magnitude

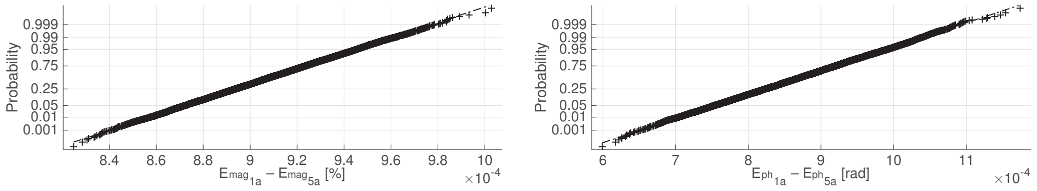
(b) Voltage phase



(c) Current magnitude

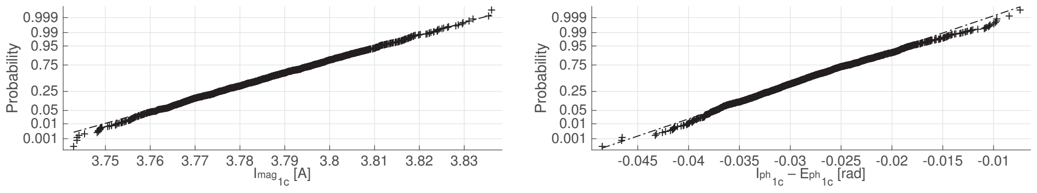
(d) Current phase

Figure 5.15 – Real voltage and current measurements taken in the EPFL campus. The signals include the noise introduced by the combination of sensor and PMU. The noise stds inferred from the signals are shown in (5.2).



(a) Voltage magnitude

(b) Voltage phase



(c) Current magnitude

(d) Current phase

Figure 5.16 – Normal probability plots of the measured quantities shown in Fig. 5.15. The normality assumption of the measurement noises is satisfied.

- Transmission network or distribution network operated with earthed or unearthed neutral;
- Low, high or very high impedance faults (1 Ω, 100 Ω or 1000 Ω);
- Symmetric (3-ph) or asymmetric (1-ph-to-ground and 2-ph) faults;
- Fault at 1/4 or 1/2 of the line length. Three lines are considered: $L_{4,5}$, $L_{9,10}$, $L_{13,16}$ for the distribution network and $L_{1,3}$, $L_{3,4}$, $L_{1,5}$ for the transmission network;
- Presence of DG and different network operating conditions.

Faulted line identification

For a given fault scenario (e.g., 1-ph-to-ground low impedance fault, at 1/4 of a specific line, on a distribution network operated with earthed neutral, without DG), the procedure used to assess the accuracy of the proposed fault location method is the following:

1. The model is implemented and run. The synchrophasors estimated by the PMUs at 50 frames-per-second are recorded.
2. M sets of measurements are obtained by perturbing the quantities inferred in step 1 with randomly-generated Gaussian white noise characterized by the stds given in (5.2). We set $M = 10000$ in order to get results that are statistically significant. Note that the phase noise std is in radians, while the magnitude noise std is in percentage of the quantity X of step 1. Therefore, the magnitude and phase of the synchrophasor measurement X_{meas} are calculated as follows:

$$\begin{aligned} X_{meas_{mag}} &= X_{mag} + N(0, \sigma_{X_{mag}} \cdot X_{mag}) \\ X_{meas_{ph}} &= X_{ph} + N(0, \sigma_{X_{ph}}) \end{aligned} \tag{5.3}$$

3. Each set of measurements computed in step 2 is given to the b parallel SEs that return the b estimated states. The latter are compared with the set of measurements in order to obtain b WMR values. The index of the SE exhibiting the lowest WMR identifies the inferred faulted line. The proposed fault location method is successful if the inferred faulted line coincides with the real faulted line.
4. The accuracy of the fault location method is represented by the percentage of success in correctly identifying the faulted line. It is computed as:

$$\text{accuracy} = \frac{M_s}{M} \cdot 100$$

where M_s indicates the number of times the faulted line is correctly identified.

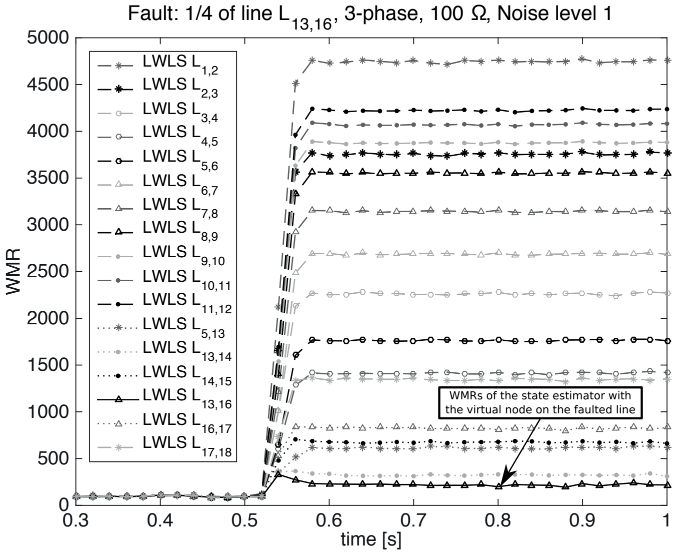
The accuracy of the proposed fault location method for each scenario is given in Tables 5.7-5.24. The tables also contain an analysis of the sensitivity of the proposed fault location method accuracy with respect to the noise level (details about the noise levels in Appendix 5.5.4):

- *Noise level 1*: the noise stds are the ones presented in Section 5.4.1, which are obtained from real 0.1-class voltage and 0.5-class current sensors;
- *Noise level 10*: the noise stds related to the *measurement* sensors and the current *protection* sensors are respectively 10 and 3 times larger than the ones presented in Section 5.4.1. These values refer to significantly worse sensors and were chosen in order to represent a worst, but still realistic, scenario.

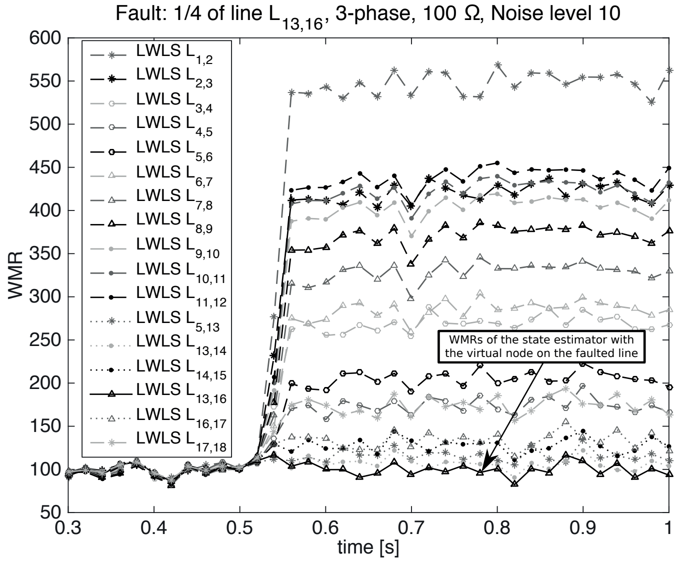
Note that the *Noise level 10* corresponds to a very high noise for transmission networks (see Tables 33 and 33 in Appendix).

Distribution network: In what follows, the method is validated on the simulated Alliander distribution network. Fig. 5.17a shows the WMRs of the b-SEs as a function of time for the specific case of a 3-ph fault at a quarter of line $L_{13,16}$, with fault impedance of 100 Ω and *Noise level 1*. The fault occurs between 0.5 and 0.52 seconds. The quick separation of the WMRs in the following time-steps allows the detection of the fault according to the algorithm presented in Section 3.2.1. After three time-steps (see Figs. 5.14 and 5.18), it is evident that the LWLS with the virtual bus in line $L_{13,16}$ maintains the lowest WMR, therefore the fault location algorithm correctly identifies the fault in line $L_{13,16}$. It is worth observing that the fault in line $L_{13,16}$ is the most challenging to be identified among the three considered lines. This is due to the fact that line $L_{13,16}$ and its neighbor lines ($L_{5,13}$, $L_{13,14}$ and $L_{16,17}$) are short (218 to 510 m), and the virtual buses positioned in these lines are close to the fault. Indeed, we can see from Fig. 5.17a that the WMRs of the SEs using these virtual buses are quite close to each other. As a consequence, when we apply a high level of measurement noise, the WMRs become more noisy (see Fig. 5.17b), leading to a possible misestimation of the faulted line. However, it is important to point out that in the time-steps where the algorithm fails, it locates the fault in one of the lines adjacent to the faulted one.

Tables 5.7 and 5.8 refer to symmetric faults, namely 3-ph. The low-impedance fault is characterized by a fault impedance of 1 Ω and leads to fault currents in the order of thousands of Amperes. The high-impedance fault is assumed to have a fault impedance of 100 Ω that produces a fault current limited to tens of Amperes. Consequently, the high-impedance faults are very difficult to identify and locate. Unlike conventional schemes, the proposed method guarantees a correct fault detection and location in case of realistic noise level (i.e. *Noise level 1*). If we increase the noise level (i.e. *Noise level 10*), the percentage of success decreases for the case of high impedance faults. Indeed, high impedance faults cause less perturbation in the network state compared



(a) Noise level 1.



(b) Noise level 10.

Figure 5.17 – WMRs of the b-SEs in case of a 3-ph high impedance fault at a quarter of line $L_{13,16}$ of Fig. 5.8 occurring between 0.5 and 0.52 seconds. Two noise levels are shown: (a) *Noise level 1*; (b) *Noise level 10*. In (b), the noisy WMRs worsen the accuracy of the fault location method. At some time-steps, it does not locate the fault on the faulted line, but on one of the adjacent ones.

Table 5.7 – Distribution: 3-ph fault, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	100%
	1/2	100%	100%
$L_{9,10}$	1/4	100%	100%
	1/2	100%	100%
$L_{13,16}$	1/4	100%	100%
	1/2	100%	100%

Table 5.8 – Distribution: 3-ph fault, 100 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	99.27%
	1/2	100%	99.85%
$L_{9,10}$	1/4	100%	98.54%
	1/2	100%	99.90%
$L_{13,16}$	1/4	100%	84.65%
	1/2	100%	99.74%

to the low impedance ones. The WMRs of the various SEs are closer to each other and the method becomes more sensitive to the noise, as already explained above. However, even with the high noise level and the high fault impedance, the proposed method exhibits a quite high number of correct fault location estimates.

We can also notice that the algorithm is always less accurate in locating faults at a quarter of a line compared to the ones in the middle of a line. Indeed, the presented methodology assumes that each virtual bus is in the middle of a given line. However, in the experimental validation, the position of the fault was changed along the line (i.e. 1/2 or 1/4 of the line length) but always keeping the virtual bus of the SEs in the middle of the line. When the actual fault happens to be exactly in the virtual bus of one of the SEs (i.e. in the middle of the line), the network topology and the admittance matrix used by that SE match perfectly the simulated faulted network. For this reason, we achieve higher accuracy when the fault is in the middle of the line. However, we have shown that even for fault locations not on the virtual bus, we do achieve the correct identification of the faulted line.

The same considerations about symmetric faults can be extended to the other scenarios. We can further observe that the proposed fault location method has slightly reduced performance in locating a low impedance fault only in case of a 1-ph fault in an unearthed neutral network with *Noise level 10*. The reason is that the voltage drops significantly in the faulted phase. As already mentioned in Section 5.4.1, for this specific case we have used stds of the voltage magnitude and phase measurements in the faulted phase which are 100 times larger than the ones defined in Section 5.4.1.

Transmission network: The method is further validated on the transmission test bed. Tables 5.17-5.24 provide the percentage of success in identifying the fault for symmetric and asymmetric faults, with *Noise level 1* and *Noise level 10* for three selected lines at 1/4 and 1/2 of their lengths. What commented for the distribution network holds true also for the transmission network. On the other hand, it has to be highlighted that, in

Table 5.9 – Distribution: 2-ph fault: earthed neutral, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	100%
	1/2	100%	100%
$L_{9,10}$	1/4	100%	100%
	1/2	100%	100%
$L_{13,16}$	1/4	100%	100%
	1/2	100%	100%

Table 5.10 – Distribution: 2-ph fault: earthed neutral, 100 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	92.48%
	1/2	100%	92.91%
$L_{9,10}$	1/4	100%	89.56%
	1/2	100%	95.09%
$L_{13,16}$	1/4	100%	68.43%
	1/2	100%	91.73%

Table 5.11 – Distribution: 2-ph fault: unearthed neutral, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	100%
	1/2	100%	100%
$L_{9,10}$	1/4	100%	100%
	1/2	100%	100%
$L_{13,16}$	1/4	100%	100%
	1/2	100%	100%

Table 5.12 – Distribution: 2-ph fault: unearthed neutral, 100 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	92.41%
	1/2	100%	92.83%
$L_{9,10}$	1/4	100%	89.38%
	1/2	100%	95.20%
$L_{13,16}$	1/4	100%	67.57%
	1/2	100%	92.32%

Table 5.13 – Distribution: 1-ph-to-ground fault: earthed neutral, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	100%
	1/2	100%	100%
$L_{9,10}$	1/4	100%	100%
	1/2	100%	100%
$L_{13,16}$	1/4	100%	100%
	1/2	100%	100%

Table 5.14 – Distribution: 1-ph-to-ground fault: earthed neutral, 100 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	83.78%
	1/2	100%	99.99%
$L_{9,10}$	1/4	100%	95.05%
	1/2	100%	99.23%
$L_{13,16}$	1/4	100%	96.06%
	1/2	100%	99.36%

Table 5.15 – Distribution: 1-ph-to ground fault: unearthed neutral, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	69.84%
	1/2	100%	87.28%
$L_{9,10}$	1/4	100%	72.69%
	1/2	100%	77.82%
$L_{13,16}$	1/4	100%	72.08%
	1/2	100%	79.33%

Table 5.16 – Distribution: 1-ph-to ground fault: unearthed neutral,100 Ω

Fault Position		Noise Level	
		1	10
$L_{4,5}$	1/4	100%	70.95%
	1/2	100%	99.66%
$L_{9,10}$	1/4	100%	89.99%
	1/2	100%	97.94%
$L_{13,16}$	1/4	100%	87.56%
	1/2	100%	95.74%

Table 5.17 – Transmission: 3-ph fault, 1 Ω

Fault Position		Noise Level	
		1	10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	100%
	1/2	100%	100%

Table 5.18 – Transmission: 3-ph fault, 100 Ω

Fault Position		Noise Level	
		1	10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	67.54%
	1/2	100%	100%

general, the noise affects less the state estimation results in transmission networks due to larger phasor displacements. This is reflected in an overall better performance of the method especially in case of *Noise level 10*.

As a conclusion, we can state that the proposed algorithm is able to correctly detect the fault and locate the faulted line irrespectively of the type of network, the neutral connection, fault type, fault impedance and fault position. The method is robust against realistic noise levels since, during the experimental validation, it never failed when using noises directly inferred from real-field data. The fault location accuracy decreases, but not significantly, only when we apply a noise level 10 times larger. However, this noise level is considerably larger than the real one and the success percentage of proposed method remains above 66% for both the networks under test.

In order to further test the proposed fault location method in distribution networks we have carried out another simulation with a higher fault impedance of 1 kΩ. This is commonly considered one of the highest possible fault impedances since it refers to

Table 5.19 – Transmission: 2-ph-to ground fault, 1 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	100%
	1/2	100%	100%

Table 5.20 – Transmission: 2-ph-to ground fault, 100 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	59.59%
	1/2	100%	100%

Table 5.21 – Transmission: 2-ph fault, 1 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	100%
	1/2	100%	100%

Table 5.22 – Transmission: 2-ph fault, 100 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	96.75%
	1/2	100%	100%

Table 5.23 – Transmission: 1-ph-to ground fault, 1 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	100%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	100%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	100%
	1/2	100%	100%

Table 5.24 – Transmission: 1-ph-to ground fault, 100 Ω

Fault Position		Noise Level 1	Noise Level 10
$L_{1,3}$	1/4	100%	99.99%
	1/2	100%	100%
$L_{3,4}$	1/4	100%	99.86%
	1/2	100%	100%
$L_{1,5}$	1/4	100%	87.19%
	1/2	100%	100%

Table 5.25 – Distribution: 1-ph-to ground fault: unearthed neutral, 1000 Ω

Fault Position		Noise Level
		1
$L_{4,5}$	1/4	80.94%
	1/2	99.99%
$L_{9,10}$	1/4	95.92%
	1/2	99.30%
$L_{13,16}$	1/4	95.93%
	1/2	99.32%

the typical electrical resistance of a biological body. The performance of the proposed method has been assessed considering a 1 kΩ 1-ph-to-ground fault in an unearthed neutral network. The reason motivating this choice is that, for this case, the fault current is limited in amplitude by the high network zero-sequence impedance, so that its value becomes comparable to the currents absorbed by the loads. Indeed, the simulation results show that fault location is more difficult in unearthed networks. We consider the case of *Noise level 1* in order to match the realistic noise measured in the real network. The results are provided in Table 5.25. It can be seen that, also for this extreme scenario, the proposed methodology is capable to identify the faulted line and type of fault in the large majority of the cases.

Faulted buses

The fault on a bus has not been discussed so far because we assume to have a PMU installed in every substation. Hence, the faulted bus and the fault type are easily detected by using the measurements of the PMU installed in the faulted bus. For example, in case of 1-ph fault in a bus of an unearthed neutral network: (i) the voltage zero-sequence component has a non-null value; (ii) the current magnitude in the faulted phase has a sudden jump of tens of Amperes.

Distributed generation

The performance of the method has been also assessed when dealing with faults in distribution networks characterized by a large penetration of DG. The loads in bus #4, #10 and #17 have been coupled with variable pitch wind turbine models driving 160 kW squirrel cage asynchronous generators running at nominal speed. The power requested by the loads has been varied in order to create three different scenarios. *Case 1*: a passive network where the loads absorb approximately 1/4 of the rated power

Table 5.26 – Distribution: presence of DG, unearthed neutral: Fault at 1/4 of $L_{13,16}$, 100 Ω

Scenario	Fault Type	Noise Level 1	Noise Level 10
Case 1	3-ph	100%	82.73%
	2-ph	100%	66.66%
	1-ph	100%	80.74%
Case 2	3-ph	100%	83.08%
	2-ph	100%	67.43%
	1-ph	100%	82.34%
Case 3	3-ph	100%	84.62%
	2-ph	100%	69.71%
	1-ph	100%	83.40%

of the real secondary substation transformers and the DG does not cover the load demand. *Case 2*: an intermediate scenario where the loads absorb 50 % of the power of *Case 1*, but the network is still passive. *Case 3*: the loads absorb 10 % of the power of *Case 1* so that the DG production is abundantly larger than the load demand making the feeder exporting power towards the upstream grid. For these tests, we have used the case characterized by the worst accuracy performance, that is a high impedance fault (100 Ω) on line $L_{13,16}$ in an unearthed neutral network. Table 5.26 shows the fault location accuracy for different fault types and noise levels. As expected, these results are close to the ones referring to the same fault conditions shown in Tables 5.8, 5.12 and 5.16. Indeed, the presence of DG does not change the performance of the proposed method since state estimation is inherently not affected by the nature of the loads/generators.

Computation time and latency

The assessment of the speed of the algorithm in identifying the faulted line is a metric of interest when comparing the proposed method to existing fault location algorithms. In what follows we focus on two time latencies: (i) the computation time of the proposed method and (ii) the overall latency of the system to identify the faulted line.

The former is basically the time needed to compute the parallel SEs and then to go through the flowchart shown in Fig. 3.5. The computation time is function of the size of the network, the number of measurements, and the type of state estimation technique employed. Comparing the two networks under test, the distribution one presents a larger number of measurements and unknown states and thus a larger computation time. The latency assessment that follows refers to the distribution network. The proposed method has been implemented in an Apple MacBook Pro with a 2.6 GHz CPU, 8 GB RAM, and MATLAB® 2014b. The SEs are implemented in series and the computation time to run all the b-SEs is 11.0 ms with a std of 0.8 ms.

The overall latency represents the time between the occurrence of the fault and its identification. It is worth noting that, in order to obtain a reliable and correct post-fault synchrophasor estimate, the PMUs have to process a dataset of raw-sampled waveforms that does not contain the instant in which the fault occurred. To clarify this aspect, Fig. 5.18 shows that whenever a fault occurs (e.g., in the grey area), three acquisition windows (W_1,W_2,W_3) are always corrupted. We remind that the adopted synchrophasor estimation algorithm uses a window containing three periods of the fundamental frequency. Then, W_4 contains the post-fault waveform without any step and the associated synchrophasor is correctly estimated. The total latency is therefore the sum of four contributions:

1. T_1 that is the time between the fault event and the first sample of window W_4. Depending on when the fault occurs in the grey area of Fig. 5.18, T_1 can vary between 0 and 20 ms;
2. T_2 that corresponds to half of the acquisition window length used by the synchrophasor estimation algorithm. For the synchrophasor estimation algorithm used, T_2 is equal to 30 ms at 50 Hz;
3. T_3 is the time between the center of the acquisition window and the moment the set of measurements is pushed to the fault detection and location application. In Section 5.3.1 it was shown that for wired communication networks (SiL and EPFL), this value was approximately 47 ms. In case of wireless links T_3 may become more important.
4. T_4 is the computation time needed to run the b-SEs. For the case considered in this paper, where the b-SEs are implemented in series, T_4 is equal to 11 ms with a std of 0.8 ms.

Therefore, the overall latency can vary between 88 and 108 ms, depending on the instant the fault occurred. This value of latency matches with the requirements of protective relaying, so one can ideally envision its adoption in the context of protection.

5.4.3 Conclusions

A novel PMU-based fault detection and location method for power systems based on real-time state estimation has been proposed. It consists of parallel SEs characterized by different and augmented network topologies in order to include a floating fault

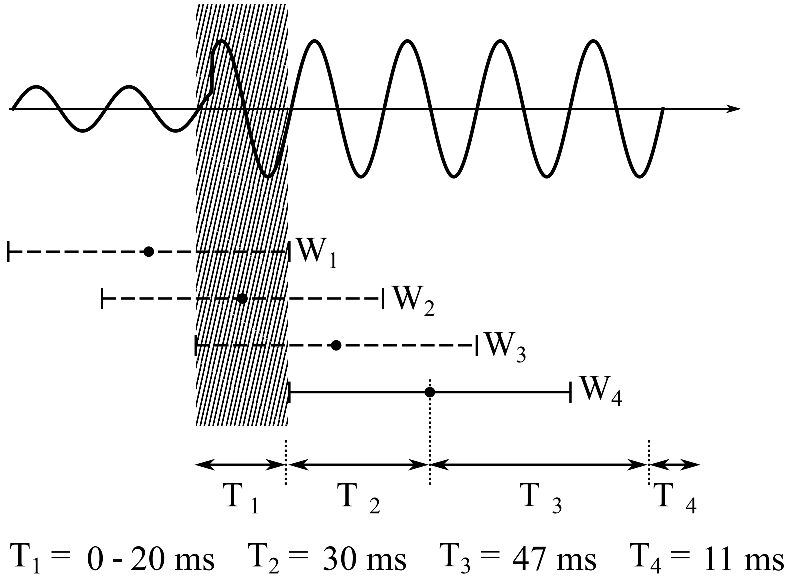


Figure 5.18 – Overall latency of the proposed method in identifying faults.

bus. By comparing the weighted measurement residuals of all the SEs, we are able to detect the presence of a fault and identify the faulted line with a latency ranging from 88 to 108 ms. The validation has been carried out on a distribution and transmission networks equipped with PMUs at every bus. The electrical networks and the PMUs are simulated in the time-domain by using a RTS. We have also implemented the PMU synchrophasor estimation algorithm in order to reproduce the real PMU behavior. The measurement noises have been inferred from real-field PMU data. The proposed method correctly identifies the faulted line irrespectively of network type, neutral connection, fault type, fault impedance and fault position along the line. It has also been proven to be significantly robust against noise. Additionally, the fault location accuracy is not influenced by the presence of DG since the method is based on state estimation, which does not inherently depend on the nature of the loads/generators.

Although the results here presented show an accuracy and latency that match the requirements of protection schemes, a massive deployment of the presented fault detection and faulted-line identification method needs to be preceded by additional studies. In particular, researchers need to investigate on the sensitivity of the method, especially with respect to errors in the line parameters and its robustness against communication issues.

5.5 HIL validation of GECN for voltage control

In this section, we present the experimental validation of the GECN mechanism when applied to the case of thermostatically controlled loads to provide voltage control. The

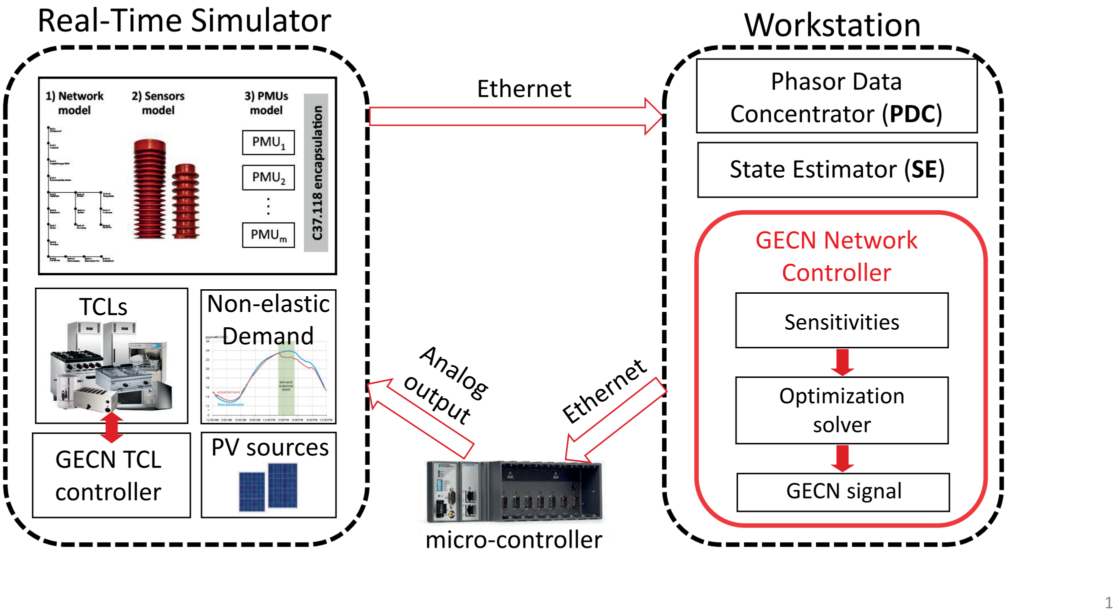


Figure 5.19 – The proposed HIL setup for the validation of GECN.

GECN is described in [118] and its basic concepts are recalled in Chapter 3.2.2 of this manuscript. What follows is based on [123].

5.5.1 HIL Setup and Experiment Design

The HIL setup that has been designed and implemented for the experimental validation of the GECN control scheme is shown in Fig. 5.19. It consists of a RTS that communicates via the local Ethernet network with a workstation. In the RTS, we have developed specific models to represent the electrical network, the PMUs, the TCLs and the GECN load controllers. In addition to the controllable resources, non-dispatchable production coming from distributed solar panel units and non-controllable demand are also included in the RTS.

It is worth noting that the developed set-up corresponds to the Alliander distribution network presented in Section 5.2.3 and the PMUs' location corresponds to the real installation of these devices in the electrical network. The PMUs estimate the synchrophasors of nodal voltages and injected/absorbed currents, encapsulate them according to the IEEE Std. C37.118.2-2011 and stream via Ethernet to the workstation.

In the workstation, a specific LabVIEW interface comprises a PDC, a RTSE, as well as the GECN network controller. PDC and DKF-based RTSE have been already explained in this manuscript. We rely on a PMU-based RTSE that surely matches the timing requirements for the control of ADNs. However, the control approach here described can be extended to the case of RTU-based SE (i.e., relying on measurements coming

Table 5.27 – Parameters of the elastic appliances and the load controller

Parameter	Value
Temperature deadband, $\Theta(^{o}\mathrm{C})$	[1,6]
Ambient temperature, $\theta_0(^{o}\mathrm{C})$	19
Thermal conductivity, A(kW/^{o}C)	10.563
Coefficient of performance, η	3
Rated power, P_r(W)	150
Time-step, τ(s)	1
Time constant, $T_c = m_c/A$(h)	$\sim U$(1.326,2.778)
Controller time counter, T_0(s)	480
Internal state parameter, ξ	0.4
Appliance power factor, $\cos\varphi$	0.85

from smart meters).

Once the estimated state is available, it is received by the GECN network controller block that uses this information to compute the broadcast control signals. To this end, first the voltage sensitivity coefficients are computed as in [120] and next, the optimal control problem presented in Section 3.2.2, equation (3.37) is solved. Finally, the GECN broadcast control signal is computed. The operation of the GECN network controller is triggered every 16 sec as in [113]. In order to close the control loop, the GECN signal is sent via Ethernet to a micro-controller where it is transformed to an analog voltage signal and transmitted via dedicated analog outputs back to the network buses in the RTS. There, each signal is received by all the GECN load controllers that are connected to a single network bus. The local controllers change the state of the TCLs according to the received signal and, consequently, the state of the network.

At each of the buses equipped with PMUs, apart from bus #1, we consider a population of 400 controllable refrigerators. The characteristics of the elastic appliances, as well as the TCL controller parameters are shown in Table 5.27. In addition to the controllable resources, real measurements of 24 h curves of consumption and production coming from distributed PV units are considered in each network bus. The aggregate active and reactive power injections profiles of all the network buses are shown in Fig. 5.20[4].

In what follows, we first verify that the RT implementation of GECN is the same as the off-line event-driven simulation in MATLAB by performing a regression testing. Then, we evaluate the performance of GECN in terms of voltage optimality and we characterize its time requirements.

---

[4] These aggregate data come from measurements taken at a different feeder.

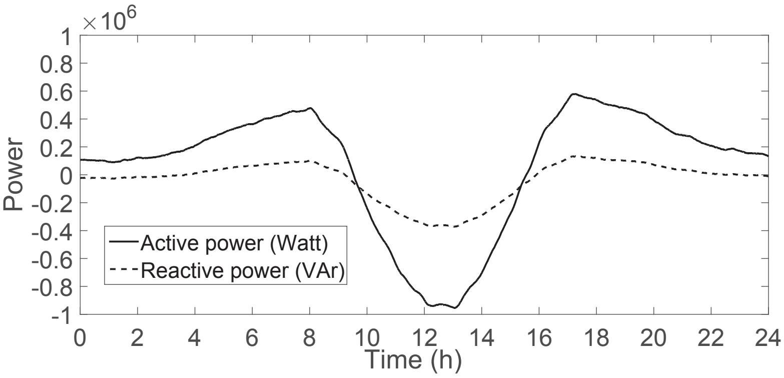


Figure 5.20 – Aggregated non-controllable active and reactive power injections of all network buses.

5.5.2 Regression Testing

In this section we want to verify that the implementation of the GECN control mechanism in real-time is identical to the off-line version in MATLAB used for the simulations in [113]. For this purpose, the goal is to run the same test-case in MATLAB off-line and in real-time and obtain identical resulting voltage profiles, as well as aggregated power of the TCLs. However, there are several factors that render such a comparison difficult:

- The probabilistic nature of the GECN local controllers and the noise introduced by the analog signals do not allow to obtain a deterministic output of the controllable loads between different simulations;
- The finite integration time-step of the RTS involves truncation errors caused by the RTS solver that are different from the event-driven simulator developed in MATLAB that, instead, uses the power flow calculus.

For these reasons, we choose to test and compare separately the operations of the GECN network controller and the load controllers as described next.

For the validation of the GECN network controller, we perform the following test. We first run a 24 h off-line MATLAB simulation and we store every second the network state, i.e., the nodal voltage phasors, the nodal power injections, as well as the computed GECN signals for each network bus. Then, we use the nodal voltage phasors and power injections as input to the LabVIEW implementation of the GECN network controller block shown in Fig. 5.19. In this way, we can compare the 24 h GECN signals computed in MATLAB with the ones obtained from the GECN network controller that is used in the experimental set-up. The results of this test are shown in Fig. 5.21-5.22. In these figures we plot the difference between the 24 h GECN signal computed off-line in MATLAB and the one computed by the RT implementation in LabVIEW. For the sake of brevity we show only the signals sent to bus #3, which is the controllable bus

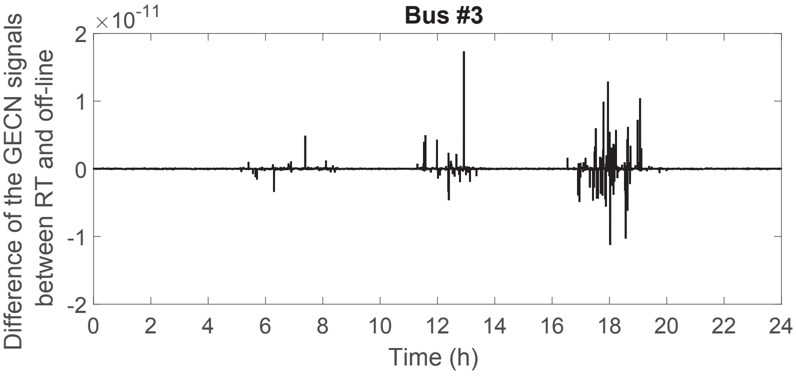


Figure 5.21 – Difference between the 24 h GECN signals sent to bus #3 computed by the MATLAB off-line and the LabVIEW RT implementation of the GECN network controller.

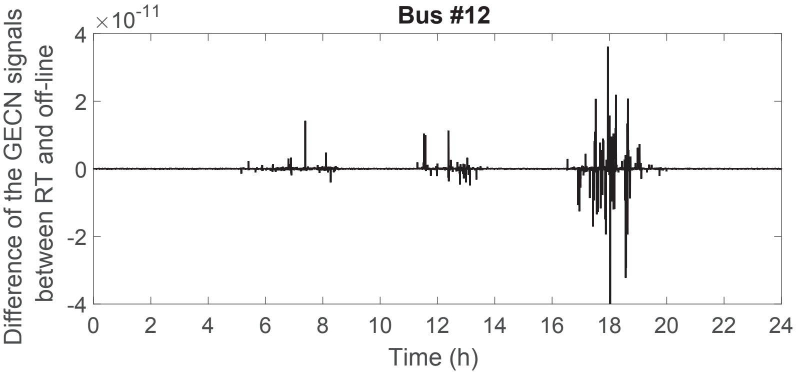


Figure 5.22 – Difference between the 24 h GECN signals sent to bus #12 computed by the MATLAB off-line and the LabVIEW RT implementation of the GECN network controller.

closest to the slack bus and bus #12 which is the furthest one. As it can be observed, the difference between the GECN signals is negligible, in the order of 10^{-11}, which indicates that the implemented GECN network controller is behaving in RT as the event-driven one developed in MATLAB.

For the validation of the local controllers of the TCLs we adopt a similar procedure. We run a 24 h off-line simulation in MATLAB and we store the GECN signals sent to the MV network buses, as well as the aggregate power of the controllable resources. Then we use the control signals as input to the RT TCL controller which is implemented in Simulink and we observe the aggregate TCL power at each MV bus. In both the RT and the off-line simulations we make sure to set the seed of the random number generator so that the same sequence of random numbers is produced in the two simulations. By doing so we are able to compare the two different implementations of the local resources controller in the two different software platforms. Fig. 5.23 and 5.24 show the aggregate TCL power of bus #3 and #12 respectively computed in the off-line

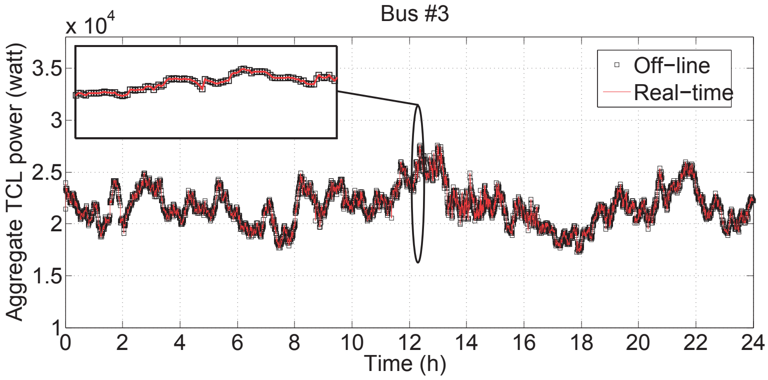


Figure 5.23 – Aggregate power consumption of TCLs connected to bus #3 in MATLAB off-line (black squares) and in RT simulation (red line).

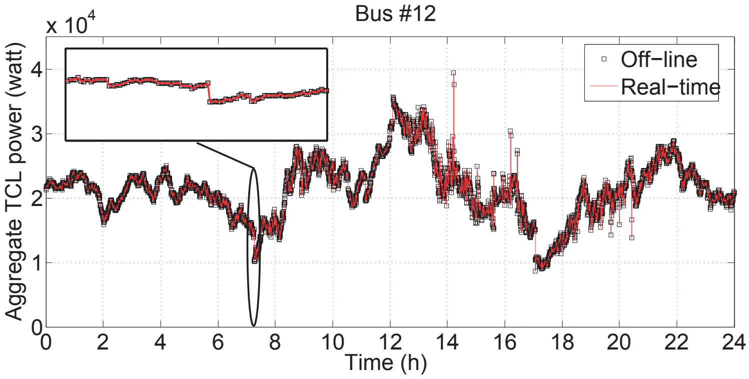


Figure 5.24 – Aggregate power consumption of TCLs connected to bus #12 in MATLAB off-line (black squares) and in RT simulation (red line).

simulations (black squares) and in real-time (red line)[5]. As it can be observed in these figures the aggregate powers of the TCLs are exactly superposed, indicating that the TCL controller, as well as the TCL model are behaving in RT exactly as the ones in MATLAB.

5.5.3 Demonstration Example and Performance Assessment

In this section we evaluate the performances of GECN as a RT primary voltage controller in ADNs. To this end we use the Alliander distribution feeder and the HIL set-up described in detail in Section 5.5.1.

First, we run a 24 h RT simulation without enabling the GECN network controller in order to obtain the base-case voltage profile, as well as the uncontrolled aggregate consumption of the TCLs. The results of this simulation for the voltage are shown in

---

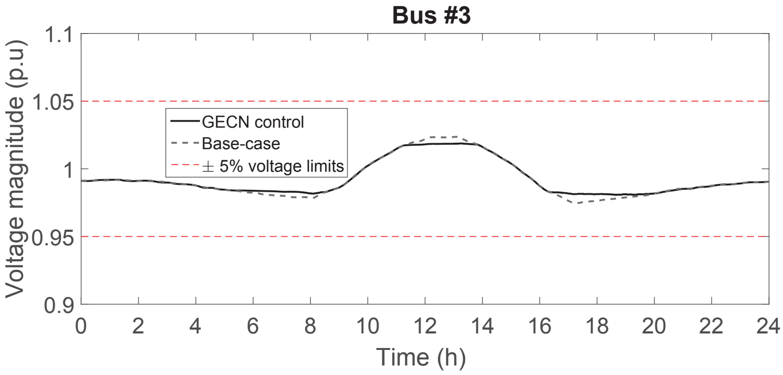
[5] Note that in this case we do not show the differences between the aggregate powers computed in the two implementations as they are exactly zero for the whole 24 h period.

the dashed black lines in Fig. 5.25a-5.26a.

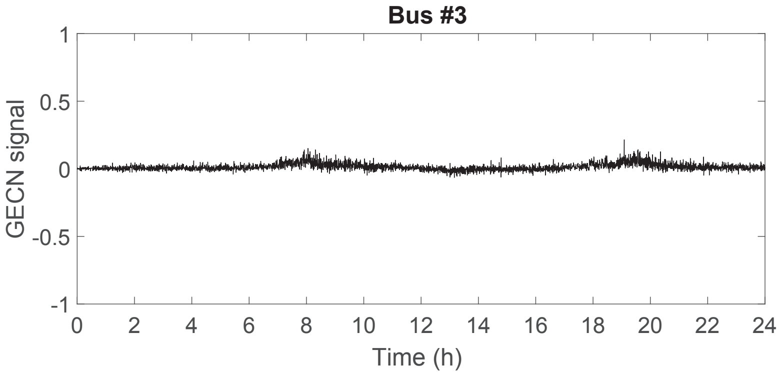
For the sake of brevity, we show the network voltage profiles that exhibit the minimum and maximum voltage variations, namely the one of bus #3 and bus #12 that are the closest and the furthest away from the slack bus respectively. It is worth observing that for bus #12, the absence of a suitable control produces voltages below the allowed limit of 0.95 p.u. in correspondence of the peak consumption periods, i.e., hours 7-8 and 17-18. Moreover, over-voltages above 1.05 p.u. occur in the middle of the day during the peak production of the PV units, i.e. hours 12-13. In Fig. 5.25c-5.26c the aggregate power of the refrigerators in buses 3 and 12 respectively are shown for the base-case in red.

Next, we run a 24 h RT simulation where GECN control is enabled. The improvement in the voltage profile of buses 3 and 12 due to the application of GECN is shown in Fig. 5.25a-5.26a (black curves). It is worth noting that the GECN is able to control in real-time the network voltage guaranteeing that the resulting profiles remain for the whole 24 h period within the allowed $\pm 5\%$ limits shown in the dashed red lines. The GECN signals that correspond to this improvement in the voltage profiles are shown in Fig. 5.25b-5.26b for bus #3 and #12 respectively. As expected, the signal sent to bus #12 exhibits larger magnitudes caused by the larger voltage variations in this bus, whilst GECN signals are close to zero for bus #3. In fact, the three peaks of the signal observed in Fig. 5.26b correspond to the time periods when under-voltages and over-voltages occur in Fig. 5.26a, i.e., hours 7-8, 12-13 and 17-18. The GECN signals cause variations of the aggregate TCL power of the controllable buses that can be observed in Fig. 5.25c-5.26c in black. Compared to the base-case consumption (red curves) the TCLs consume less during hours 7-8 and 17-18, responding correctly to the positive GECN signal that dictates there is a peak in consumption that causes under-voltages. On the contrary, the TCLs consume more during hours 12-13 in order to locally compensate the peak in the PV power production and decrease the corresponding over-voltages. Overall, these results indicate that the GECN control mechanism is able to selectively control the aggregated demand per bus and successfully provide real-time primary voltage control in active distribution networks.

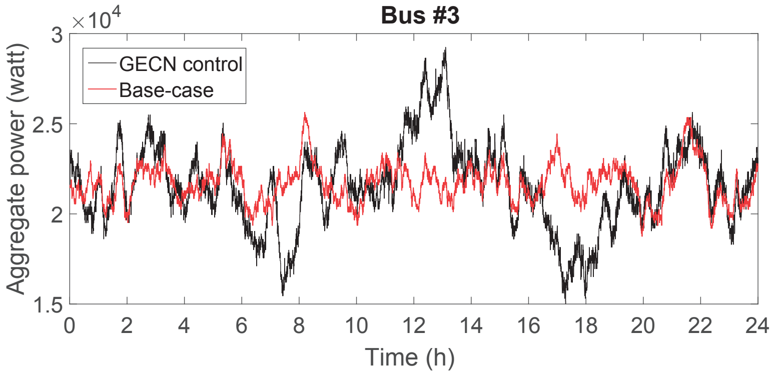
In addition to the performance evaluation of GECN in terms of voltage optimality, it is interesting to assess the time latencies of the control process. In Fig. 5.27 we show the time required by the GECN network controller to solve the centralized optimization problem throughout the 24 h period. It is worth noting that even during the time-periods when voltage control is required in the network, the solution time of the optimization problem is in the order of few ms. Furthermore, Fig. 5.28 shows the CDFs of the time required to solve the centralized optimization problem off-line, using the solver fmincon of MATLAB and in RT, using the gradient descent method. It is worth noting the significant improvement of the adopted solution method in RT which is in the order of 10 times faster. In particular, the median value of the solution time is



(a) 24 h voltage profile of bus #3 before (black dashed line) and after (black continuous line) the GECN control.

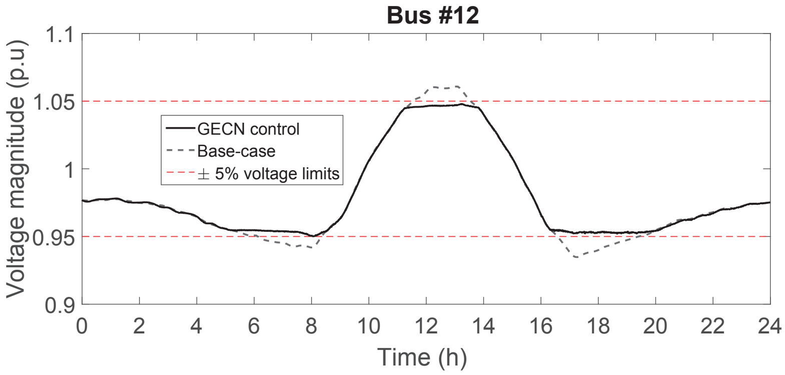


(b) 24 h GECN signal sent to bus #3.

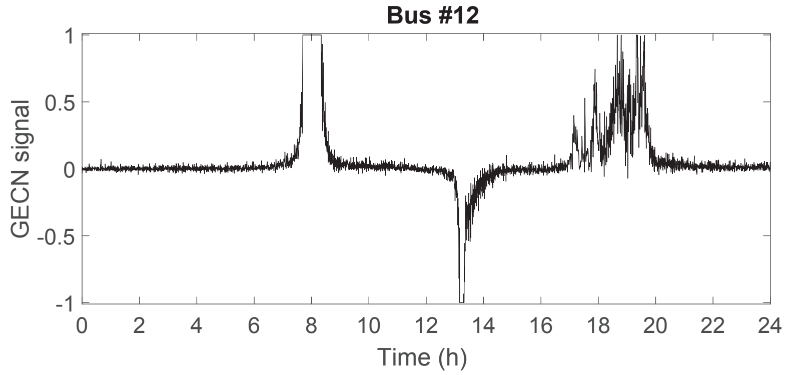


(c) 24 h aggregate power consumption of the TCLs connected to bus #3 before (red curve) and after (black curve) the GECN control.

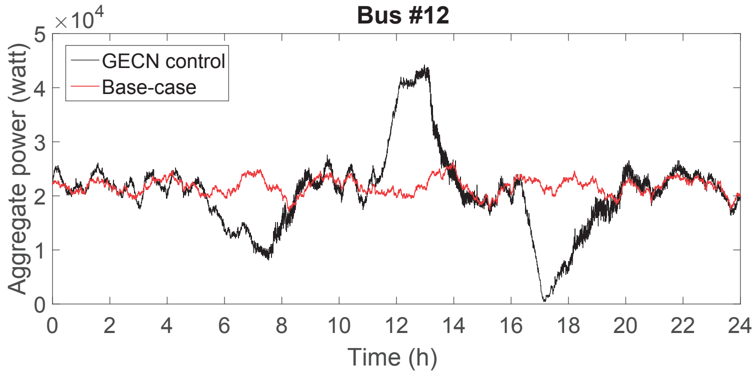
Figure 5.25 – Voltage profile, GECN signal and aggregate TCL power of bus #3.



(a) 24 h voltage profile of bus #12 before (black dashed line) and after (black continuous line) the GECN control.



(b) 24 h GECN signal sent to bus #12.



(c) 24 h aggregate power consumption of the TCLs connected to bus #12 before (red curve) and after (black curve) the GECN control.

Figure 5.26 – Voltage profile, GECN signal and aggregate TCL power of bus #12.

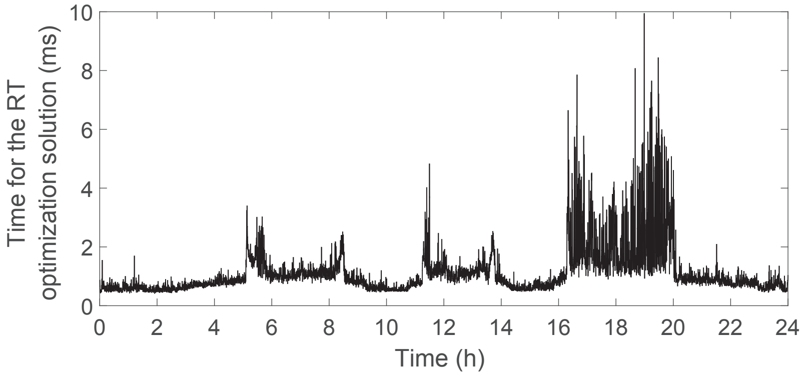


Figure 5.27 – Time required for the solution of the optimization problem.

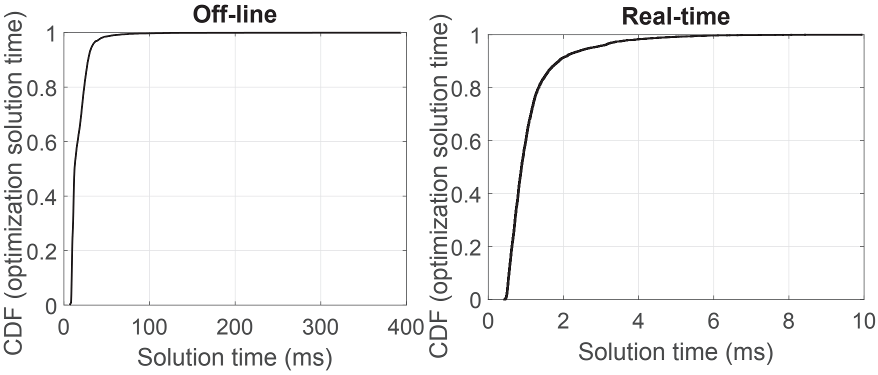


Figure 5.28 – CDF of the time required to solve the optimal control problem, comparison between off-line and RT implementations.

1.12 ms in RT with a corresponding 95-th percentile of 2.70 ms, where as off-line these values are 17.37 ms and 32.82 ms respectively. The latency from the moment the data enters the PDC until the state is available from the RTSE is assessed in [165] to be in the order of 20 ms for the Alliander distribution feeder. Therefore, taking into account the time latencies shown in Fig 5.27, within roughly 35 ms from the moment the data is available to the PDC we are able to solve the centralized optimization problem and compute the GECN signals. Overall, the timing performance shown here confirms the adequateness of GECN as a primary controller.

5.5.4 Conclusions

In this section we have experimentally validated the operation of GECN, a soft real-time, primary voltage control mechanism. This application represents a second example on how, a timely and accurate knowledge of the system state can support network operators in manage their electrical grids. We have designed a specific HIL setup to evaluate voltage optimality and time latency of the control process. The real-time validation on a real medium voltage feeder has shown that GECN can successfully maintain the network voltage profile within the acceptable limits for safe operation (typically $\pm 5\%$ of the network rated value). Furthermore, we have computed the time required for the centralized GECN network controller to solve the optimal control problem and we have shown that it is in the order of few ms. Such time requirements indicate the adequateness of GECN as a primary voltage control scheme. Finally, the RT implementation of the GECN network controller, as well as TCL controllers into dedicated equipment can, in principle, facilitate the actual deployment of the control process in the real field.

Conclusions

This thesis focused on the design and validation of resilient synchrophasor networks for the real-time monitoring, protection and control of power grids. Since synchrophasor networks are identified as enablers of transmission and distribution systems of the future, the thesis provided an overview on the state-of-the-art and insights on the status of the current research and operational practices, always keeping the focus on the challenges that have still to be addressed. Additionally, we produced major efforts to design and validate synchronized measurement technology in distribution networks.

A modern synchrophasor networks is a complex and multi-function infrastructure. For this reason, we presented its architectural layers together with their key-components. As the time synchronization of PMUs is identified as one of the major challenges for the reliable operation of synchrophasor networks, particular focus is given to this topic. Time dissemination techniques suitable for synchrophasor networks are introduced, together with advantages and drawbacks when adopted in power systems. Always in the context of reliable operation of synchrophasor networks, we defined a novel algorithm for the pre-estimation filtering of bad data in PMU-based power system linear state estimators, able to deal with intentional or unintentional tampering of synchrophasor measurements. The algorithm is proven to be computationally efficient and robust against multiple bad data of different nature and magnitudes. Additionally, it is able to distinguish between actual bad data and unexpected operating conditions and thus it is suitable for being adopted in real PMU-based state estimators.

Again, in the context of reliable operation of synchrophasor network, we focused on cyber-attacks on the time-reference of synchrophasor networks. We showed that it is possible to forge delay attacks undetectable by state-of-the-art bad-data detection algorithms used in conjunction with state estimation processes. We gave a closed form for an undetectable attack that imposes two phase offset to two or more PMUs. We also proposed different methods for combining two-delays attacks to produce a larger impact. We proved that the attacks are successful and can lead to physical grid damage. Among the countermeasures proposed, we validated the novel pre-estimation filtering of bad data as an effective way of neutralizing the attack.

In the context of real-time monitoring of an electrical network by means of synchrophasor technology, we designed a phasor data concentrator that, in addition to the data-pushing logics suggested by the reference standard, implements a logic to minimize the latency introduced in the concentration point without increasing the data incompleteness. The performance of the data-pushing logics has been assessed in terms of reliability, determinism and reduction of the overall latency in three real synchrophasor networks adopting different telecom infrastructures (i.e., 4G-LTE, optical fiber links and twisted pairs). The experimental results showed that the proposed data-pushing logic is indeed characterized by the lowest latency contribution.

The same IEEE C37.118 Class-P Std compliant synchrophasor extraction algorithm adopted in the real-fields is implemented and validated in a GPS-synchronized real-time simulator. The simulated PMUs are used to validate two applications for the real-time protection and control of electrical networks by means of synchrophasor technology. The first one is a protection mechanism for fault detection and faulted line identification that relies on PMU-based real-time state estimation processes. The aim was to make the validation as realistic as possible, and thus we modeled in the real-time simulator a real distribution network, we adopted a real synchrophasor extraction algorithm and we inferred the measurement noise from real measurements. We showed that, in terms of latency and accuracy, the proposed process is suitable for both transmission or distribution networks (active or passive), with solid-earthed and unearthed neutral, for low- and high-impedance faults of any kind (symmetric and asymmetric) occurring at different locations. As a second example of synchrophasor network application able to enhance the distribution network operations, we chose to validate in a real-time HIL setup the GECN voltage control mechanisms. We modeled a distribution network, the measurement devices, the data concentration, the real-time state-estimation and the control mechanism. We showed that by leveraging on the accurate and frequent knowledge of the system state, GECN is able to control the state of the system in time-scales of seconds, in order to maintain its voltage level within predefined limits.

In the coming years, the advancement of PMU and telecommunication technologies are likely to facilitate the real deployment and field testing of the functionalities and applications proposed in this thesis. However, several aspects are left for future research. For instance:

- An optimal delay attack could be formulated to take into account (i) the maximum step and derivative of the reference time to avoid alarms in the clock-servo and (ii) the actual response of the clock-servo to a variation of its reference time input. In this case, research has to propose effective countermeasures.
- The adoption of the proposed protection scheme in real installations, might be preceded by the deployment of a robust and possibly redundant communication

layer. An evaluation of the impact of line-parameter errors on the fault-location accuracy is needed. Another important aspect may be the development of a method that relaxes the assumption of having a PMU at every bus.

Although further research is still needed , this thesis has shown that, by leveraging on the proposed synchrophasor networks, system operators might already acknowledge the benefits delivered by PMUs and therefore adopt such technology for the monitoring, protection and control of their assets.

Appendix

Table 28 – SiL field trial, line parameters: length L in km, resistance R in Ω/km, reactance X in Ω/km, and susceptance B in S/km. The subscripts 0 and 1 stand for zero and positive sequence, respectively.

	L	R_0	X_0	B_0	R_1	X_1	B_1
Line 1	4.682	0.217	0.756	14.3e-6	0.112	0.372	15.1e-6
Line 2	1.625	0.168	0.093	63.2e-6	0.051	0.205	63.2e-6
Line 3	1.916	0.168	0.093	63.2e-6	0.051	0.205	63.2e-6
Line 4	1.849	0.185	0.102	60.4e-6	0.051	0.210	60.4e-6
Line 5	4.249	0.177	0.498	57.2e-6	0.061	0.201	57.2e-6
Line 6	4.291	0.168	0.093	63.2e-6	0.051	0.205	63.2e-6
Line 7	2.841	0.226	0.611	57.4e-6	0.064	0.210	57.4e-6
Line 8	3.800	0.420	1.272	1.8e-6	0.159	0.410	2.8e-6
Line 9	4.682	0.217	0.756	14.3e-6	0.112	0.372	15.1e-6
Line 10	3.800	0.420	1.272	1.8e-6	0.159	0.410	2.8e-6

Table 29 – SiL field trial, accuracy classes of PTs and CTs.

	PT sending	CT sending	PT receiving	CT receiving
Line 1	0.2	0.2	0.2	0.2
Line 2	0.2	0.5	0.5	0.5
Line 3	0.5	0.5	0.2	0.5
Line 4	0.2	0.5	0.2	0.5
Line 5	0.2	0.2	0.5	0.5
Line 6	0.2	0.5	0.2	0.5
Line 7	0.2	0.2	0.5	0.5
Line 8	0.2	0.2	0.2	0.2
Line 9	0.2	0.2	0.2	0.2
Line 10	0.2	0.2	0.2	0.2

Table 30 – EPFL field trial, line parameters: length L in km, resistance R in Ω/km, reactance X in Ω/km, and susceptance B in S/km. The subscripts 0 and 1 stand for zero and positive sequence, respectively.

	L	R_0	X_0	B_0	R_1	X_1	B_1
Line 1	0.46032	0.159	0.113	130e-6	0.159	0.113	130e-6
Line 2	0.0728	0.159	0.113	130e-6	0.159	0.113	130e-6
Line 3	0.07168	0.159	0.113	130e-6	0.159	0.113	130e-6
Line 4	0.03472	0.159	0.113	130e-6	0.159	0.113	130e-6

Table 31 – BML field trial, line parameters: length L in km, resistance R in Ω/km, reactance X in Ω/km, and susceptance B in S/km. The subscripts 0 and 1 stand for zero and positive sequence, respectively.

	L	R_0	X_0	B_0	R_1	X_1	B_1
Line$_{1,2}$	0.74464	1.0571	0.9104	7.3390e-5	0.1393	0.0752	1.4794e-4
Line$_{2,3}$	0.92883	1.0568	0.9095	7.6043e-5	0.1393	0.0752	1.4718e-4
Line$_{3,4}$	1.43843	0.8439	0.1967	1.1959e-5	0.1593	0.0874	1.4495e-4
Line$_{4,5}$	1.81345	1.0405	0.8551	7.1209e-5	0.1408	0.0761	1.4942e-4
Line$_{5,6}$	0.7059	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{6,7}$	0.31992	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{7,8}$	0.4312	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{8,9}$	0.5916	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{9,10}$	0.56363	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{10,11}$	0.45427	0.8150	0.1000	1.4137e-5	0.1620	0.0890	1.4137e-4
Line$_{11,12}$	0.42235	1.2369	1.3535	5.5964e-5	0.3571	0.0824	1.0621e-4
Line$_{5,13}$	0.51052	1.0600	0.9200	7.3828e-5	0.1390	0.0750	1.4765e-4
Line$_{13,14}$	0.457	1.0600	0.9200	7.3828e-5	0.1390	0.0750	1.4765e-4
Line$_{14,15}$	0.47166	1.0600	0.9200	7.3828e-5	0.1390	0.0750	1.4765e-4
Line$_{13,16}$	0.22738	1.2400	1.3800	5.3407e-5	0.3560	0.0820	1.0681e-4
Line$_{16,17}$	0.21808	1.2400	1.3800	5.3407e-5	0.3560	0.0820	1.0681e-4
Line$_{17,18}$	0.41697	1.1922	0.9745	8.7439e-5	0.3734	0.0883	1.0003e-4

Table 32 – BML field trial, power of the transformers.

	Rated Power (kVA)
Bus 2	160
Bus 3	250
Bus 4	400
Bus 5	200
Bus 6	250
Bus 7	1000
Bus 8	400
Bus 9	400
Bus 10	400
Bus 11	400
Bus 12	400
Bus 13	400
Bus 14	250
Bus 15	250
Bus 16	250
Bus 17	250
Bus 18	400

Table 33 – BML field trial, accuracy of the combination of measurement sensors and PMUs, adopted for the validation of the fault detection and faulted line-identification method.

Noise level 1	$\sigma_{V_{mag}} = 1.6 \cdot 10^{-3}$ % $\sigma_{I_{mag}} = 4.0 \cdot 10^{-1}$ %	$\sigma_{V_{ph}} = 5.1 \cdot 10^{-5}$ [rad] $\sigma_{I_{ph}} = 5.8 \cdot 10^{-3}$ [rad]
Noise level 10	$\sigma_{V_{mag}} = 1.6 \cdot 10^{-2}$ % $\sigma_{I_{mag}} = 4.0$ %	$\sigma_{V_{ph}} = 5.1 \cdot 10^{-4}$ [rad] $\sigma_{I_{ph}} = 5.8 \cdot 10^{-2}$ [rad]

Table 34 – BML field trial, accuracy of the combination of current protection sensors and PMUs, adopted for the validation of the fault detection and faulted-line identification method.

Noise level 1	$\sigma_{I_{mag}} = 4.0$ %	$\sigma_{I_{ph}} = 5.8 \cdot 10^{-2}$ [rad]
Noise level 10	$\sigma_{I_{mag}} = 12.0$ %	$\sigma_{I_{ph}} = 1.7 \cdot 10^{-1}$ [rad]

List of acronyms

ADN	Active Distribution Network
AOA	Angle Of Arrival
BD	Bad Data
BDD	Bad Data Detection
cRIO	Compact Reconfigurable I/O (compactRIO)
CT	Current Transformer
DER	Distributed Energy Resource
DFT	Discrete Fourier Transform
DG	Distributed Generation
DKF	Discrete Kalman Filter
DMS	Distribution Management System
DN	Distribution Network
DNO	Distribution Network Operator
DOS	Denial Of Service
DSO	Distribution System Operator
DSSE	Distribution System State Estimation
e-IpMSDFT	Enhanced Interpolated Modulated Sliding DFT
EMS	Energy Management System
FDI	False Data Injection
FFT	Fast Fourier Transform
FIFO	First In First Out
FPGA	Field Programmable Gate Array
GECN	Grid Explicit Congestion Notification
GLONASS	GLObal NAvigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICT	Information and Communications Technology
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IpDFT	Interpolated Discrete Fourier Transform
IRIG	Inter-Range Instrumentation Group
IT	Information Technology

KF	Kalman Filter
LAV	Least Absolute Value
MITM	Man In The Middle
MV	Medium Voltage
NASPI	North American Synchrophasor Initiative
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PBTSP	Packet-Based Time-Synchronization Protocol
PDC	Phasor Data Concentrator
PE	Phase Error
PMU	Phasor Measurement Unit
PPS	Pulse Per Second
PTP	Precision Time Protocol
RAM	Random Access Memory
RER	Renewable Energy Resource
RFE	Rate of change of Frequency Error
RFI	Radio Frequency Interference
RMS	Root Mean Square
ROCOF	Rate Of Change Of Frequency
RTOS	Real-time Operating System
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDFT	Sliding Discrete Fourier Transform
SE	State Estimation
SNR	Signal to Noise Ratio
TAI	International Atomic Time
TCP	Transmission Control Protocol
TCL	Thermostatically Controlled Load
TNO	Transmission Network Operator
TSO	Transmission System Operator
TVE	Total Vector Error
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VT	Voltage Transformer
WAMS	Wide Area Monitoring System
WAMPAC	Wide Area Monitoring Protection and Control
WLS	Weighted Least Square

Bibliography

[1] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, “Wide-area monitoring, protection, and control of future electric power networks,” *Proceedings of the IEEE*, vol. 99, pp. 80–93, Jan 2011.

[2] F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, and M. Shahidehpour, “Synchrophasor measurement technology in power systems: Panorama and state-of-the-art,” *IEEE Access*, vol. 2, pp. 1607–1628, 2014.

[3] NASPI, “NASPI 2014 survey of synchrophasor system networks - results and findings,” tech. rep., NASPI Data and Network Management Task Team, Network Systems Group, July 2015.

[4] NIST, “Timing challenges in the smart grid,” tech. rep., NIST, January 2017.

[5] NIST, “Time synchronization in the electric power sytem,” tech. rep., NASPI, March 2017.

[6] M. Chenine and L. Nordstrom, “Modeling and simulation of wide-area communication for centralized PMU-based applications,” *IEEE Transactions on Power Delivery*, vol. 26, pp. 1372–1380, July 2011.

[7] K. Zhu, M. Chenine, and L. Nordstrom, “ICT architecture impact on wide area monitoring and control systems’ reliability,” *IEEE Transactions on Power Delivery*, vol. 26, pp. 2801–2808, Oct 2011.

[8] C. H. Lo and N. Ansari, “The progressive smart grid system from both power and communications aspects,” *IEEE Communications Surveys Tutorials*, vol. 14, pp. 799–821, Third 2012.

[9] T. Yang, H. Sun, and A. Bose, “Transition to a two-level linear state estimator - part I: Architecture,” *IEEE Transactions on Power Systems*, vol. 26, pp. 46–53, Feb 2011.

[10] T. Yang, H. Sun, and A. Bose, "Transition to a two-level linear state estimator - part II: Algorithm," *IEEE Transactions on Power Systems*, vol. 26, pp. 54–62, Feb 2011.

[11] M. Göl and A. Abur, "A hybrid state estimator for systems with limited number of PMUs," *IEEE Transactions on Power Systems*, vol. 30, pp. 1511–1517, May 2015.

[12] K. D. Jones, J. S. Thorp, and R. Gardner, "Three-phase linear state estimation using phasor measurements," in *IEEE Power and Energy Society General Meeting (PES), 2013*, pp. 1–5, 2013.

[13] J. Yang, W. Li, T. Chen, W. Xu, and M. Wu, "Online estimation and application of power grid impedance matrices based on synchronised phasor measurements," *IET Generation, Transmission Distribution*, vol. 4, pp. 1052–1059, September 2010.

[14] S. M. Abdelkader and D. J. Morrow, "Online tracking of Thevenin equivalent parameters using PMU measurements," *IEEE Transactions on Power Systems*, vol. 27, pp. 975–983, May 2012.

[15] P. Overholt, K. Uhlen, B. Marchionini, and O. Valentine, "Synchrophasor applications for wide area monitoring and control," tech. rep., ISGAN, 2016.

[16] A. G. Phadke, "The wide world of wide-area measurement," *IEEE Power and Energy Magazine*, vol. 6, pp. 52–65, September 2008.

[17] J. R. Garcia, M. A. Young, D. T. Rizy, L. C. Markel, and J. Blackburn, "Advancement of synchrophasor technology in projects funded by the american recovery and reinvestment act of 2009," tech. rep., U.S. Department of Energy, March 2016.

[18] W. G. B5.14, "Wide area protection and control technologies," tech. rep., CIGRE, September 2016.

[19] NASPI, "Model validation using synchrophasor," tech. rep., NASPI, October 2013.

[20] D. Novosel, V. Madani, B. Bhargave, K. Vu, and J. Cole, "Dawn of the grid synchronization," *IEEE Power and Energy Magazine*, vol. 6, pp. 49–60, January 2008.

[21] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proceedings of the IEEE*, vol. 93, pp. 1890–1908, Nov 2005.

[22] J. H. Eto, E. M. Stewart, T. Smith, M. Buckner, H. Kirkham, F. Tuffner, and D. Schoenwald, "Scoping study on research and priorities for distribution-system phasor measurement units," tech. rep., Lawrence Berkeley National Laboratory, December 2015.

[23] R. A. Walling, R. Saint, R. C. Dugan, J. Burke, and L. A. Kojovic, “Summary of distributed resources impact on power delivery systems,” *IEEE Transactions on Power Delivery*, vol. 23, pp. 1636–1644, July 2008.

[24] W. G. B5/C6.26/CIRED, “Protection of distribution systems with distributed energy resources,” tech. rep., CIGRE/CIRED, September 2014.

[25] D. Haughton and G. Heydt, “A linear state estimation formulation for smart distribution systems,” *Power Systems, IEEE Transactions on*, vol. 28, pp. 1187–1195, May 2013.

[26] S. Sarri, L. Zanni, M. Popovic, J. Y. L. Boudec, and M. Paolone, “Performance assessment of linear state estimators using synchrophasor measurements,” *IEEE Transactions on Instrumentation and Measurement*, vol. 65, pp. 535–548, March 2016.

[27] M. Pau, P. A. Pegoraro, and S. Sulis, “Performance of three-phase WLS distribution system state estimation approaches,” in *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*, pp. 138–143, Sept 2015.

[28] J. Liu, J. Tang, F. Ponci, A. Monti, C. Muscas, and P. Pegoraro, “Trade-offs in PMU deployment for state estimation in active distribution grids,” *Smart Grid, IEEE Transactions on*, vol. 3, no. 2, pp. 915–924, 2012.

[29] J. Liu, F. Ponci, A. Monti, C. Muscas, P. A. Pegoraro, and S. Sulis, “Optimal meter placement for robust measurement systems in active distribution grids,” *IEEE Transactions on Instrumentation and Measurement*, vol. 63, pp. 1096–1105, May 2014.

[30] “Microgrid at Illinois Institute of Technology.” http://www.iitmicrogrid.net/. Accessed: 2016-07-22.

[31] A. von Meier, D. Culler, A. McEachern, and R. Arghandeh, “Micro-synchrophasors for distribution systems,” in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, pp. 1–5, Feb 2014.

[32] M. Pignati, M. Popovic, S. Barreto, R. Cherkaoui, G. Dario Flores, J.-Y. Le Boudec, M. Mohiuddin, M. Paolone, P. Romano, S. Sarri, T. Tesfay, D.-C. Tomozei, and L. Zanni, “Real-time state estimation of the EPFL-campus medium-voltage grid by using PMUs,” in *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power Energy Society*, pp. 1–5, Feb 2015.

[33] “Cyber-secure data and control cloud for power grids (c-dax) fp-7 project.” http://www.cdax.eu. Accessed: 2016-07-22.

[34] A. Borghetti, C. A. Nucci, M. Paolone, G. Ciappi, and A. Solari, “Synchronized phasors monitoring during the islanding maneuver of an active distribution network,” *IEEE Transactions on Smart Grid*, vol. 2, pp. 82–91, March 2011.

[35] P. Romano, *DFT-based Synchrophasor Estimation Algorithms and their Integration in Advanced Phasor Measurement Units for the Real-time Monitoring of Active Distribution Networks.* PhD thesis, STI, Lausanne, 2016.

[36] *Instrument transformers - Part 2: Additional Requirements for current transformers*, 2012. IEC Standard 61869-2.

[37] *Instrument transformers - Part 3: Additional Requirements for inductive voltage transformers*, 2011. IEC Standard 61869-3.

[38] *IEEE Standard for Synchrophasor Measurements for Power Systems*, Dec 2011. IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005).

[39] P. Romano and M. Paolone, "Enhanced interpolated-DFT for synchrophasor estimation in FPGAs: Theory, implementation, and validation of a PMU prototype," *Instrumentation and Measurement, IEEE Transactions on*, vol. 63, pp. 2824–2836, Dec 2014.

[40] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, Dec 2011. IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005).

[41] *IEC/IEEE International Standard - Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*, May 2012. IEC/TR 61850-90-5:2012.

[42] A. Ikbal, A. Mohd Asim, and H. S M Suhail, "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 (Springer)*, vol. 4, no. 3, pp. 487–495, 2016.

[43] P. Kansal and A. Bose, "Bandwidth and latency requirements for smart transmission grid applications," *IEEE Transactions on Smart Grid*, vol. 3, pp. 1344–1352, Sept 2012.

[44] M. Popovic, M. Mohiuddin, D. C. Tomozei, and J. Y. L. Boudec, "iPRP - the parallel redundancy protocol for IP networks: Protocol design and operation," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2016.

[45] *IEEE Guide for Synchronization, Calibration, Testing, and Installation of Phasor Measurement Units (PMUs) for Power System Protection and Control*, March 2013. IEEE Std C37.242-2013.

[46] *IEEE Guide for Phasor Data Concentrator Requirements for Power System Protection, Control, and Monitoring*, May 2013. IEEE Std C37.244-2013.

[47] W. K. Chai, N. Wang, K. V. Katsaros, G. Kamel, G. Pavlou, S. Melis, M. Hoefling, B. Vieira, P. Romano, S. Sarri, T. T. Tesfay, B. Yang, F. Heimgaertner, M. Pignati, M. Paolone, M. Menth, E. Poll, M. Mampaey, H. H. I. Bontius, and C. Develder,

"An information-centric communication infrastructure for real-time state estimation of active distribution networks," *IEEE Transactions on Smart Grid*, vol. 6, pp. 2134–2146, July 2015.

[48] K. V. Katsaros, W. K. Chai, N. Wang, G. Pavlou, H. Bontius, and M. Paolone, "Information-centric networking for machine-to-machine data delivery: a case study in smart grid applications," *IEEE Network*, vol. 28, pp. 58–64, May 2014.

[49] M. Hoefling, F. Heimgaertner, M. Menth, K. V. Katsaros, P. Romano, L. Zanni, and G. Kamel, "Enabling resilient smart grid communication over the information-centric C-DAX middleware," in *Networked Systems (NetSys), 2015 International Conference and Workshops on*, pp. 1–8, March 2015.

[50] M. Chenine, K. Zhu, and L. Nordstrom, "Survey on priorities and communication requirements for PMU-based applications in the nordic region," in *PowerTech, 2009 IEEE Bucharest*, pp. 1–8, June 2009.

[51] A. Phadke and J. Thorp, "Communication needs for wide area measurement applications," in *5th International Conference on Critical Infrastructure (CRIS), 2010*, pp. 1–7, Sept 2010.

[52] T. Van Cutsem and C. Vournas, *Voltage stability of electric power systems*, vol. 441. Springer Science & Business Media, 1998.

[53] A. Lombardi, "Fundamentals of time and frequency," in *The Mechatronics Handbook, Second Edition - 2 Volume Set* (R. Bishop, ed.), CRC Press, 2004.

[54] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, pp. 1258–1270, June 2016.

[55] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, pp. 87–98, March 2013.

[56] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, pp. 3253–3262, Aug 2013.

[57] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to {GPS} spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3–4, pp. 146 – 153, 2012.

[58] A. Siverstein, "Leap second effects on synchrophasor systems - recent leap second experiences," Tech. Rep. NASPI-2016-TR-008, North American SynchroPhasor Initiative (NASPI), November 2016.

[59] A. Mujunen, J. Aatrokoski, M. Tornikoski, and J. Tammi, "GPS time disruptions on 26-jan-2016," tech. rep., Aalto University, February 2016.

[60] *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, July 2008. IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002).

[61] "White rabbit – overview – open hardware repository." http://www.ohwr.org/projects/white-rabbit/. Accessed: 2016-11-25.

[62] *IRIG serial time code formats*, Sept 2004. IRIG Std 200-04 (Revision of IRIG Standard 200-98).

[63] *IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications*, July 2011. IEEE Std C37.238-2011.

[64] J. Serrano, M. Lipinski, T. Wlostowski, E. Gousiou, E. van der Bij, M. Cattin, and G. Daniluk, "The white rabbit project," in *2013 International Beam Instrumentation Conference (IBIC)*, 2013.

[65] J. L. Gutiérrez-Rivas, C. Prados, and J. Díaz, "Sub-nanosecond synchronization accuracy for time-sensitive applications on industrial networks," in *2016 European Frequency and Time Forum (EFTF)*, pp. 1–4, April 2016.

[66] R. Razzaghi, A. Derviskadic, and M. Paolone, "A white rabbit synchronized PMU," in *Submitted to Innovative Smart Grid Technologies Conference (ISGT), 2017 IEEE Power Energy Society*, Sept 2017.

[67] A. Derviskadic, P. Romano, M. Pignati, and M. Paolone, "Architecture and experimental validation of a low-latency phasor data concentrator," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[68] M. Adamiak, M. Kanabar, J. Rodriquez, and M. Zadeh, "Design and implementation of a synchrophasor data concentrator," in *IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East), 2011*, pp. 1–5, Dec 2011.

[69] M. Kanabar, M. Adamiak, and J. Rodrigues, "Optimizing wide area measurement system architectures with advancements in phasor data concentrators (PDCs)," in *IEEE Power and Energy Society General Meeting (PES), 2013*, pp. 1–5, July 2013.

[70] Y. Guan, M. Kezunovic, A. Sprintson, and M. Yan, "Verifying interoperability and application performance of PDCs in synchrophasor system solution," in *North American Power Symposium (NAPS), 2012*, pp. 1–6, Sept 2012.

[71] H. Retty, J. Delport, and V. Centeno, "Development of tests and procedures for evaluating phasor data concentrators," in *IEEE Grenoble PowerTech (POWERTECH), 2013*, pp. 1–5, June 2013.

[72] A. Armenia and J. H. Chow, "A flexible phasor data concentrator design leveraging existing software technologies," *IEEE Transactions on Smart Grid*, vol. 1, pp. 73–81, June 2010.

[73] M. He and J. Zhang, "Deadline-aware concentration of synchrophasor data: An optimal stopping approach," in *IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014*, pp. 296–301, Nov 2014.

[74] K. Zhu, M. Chenine, L. Nordström, S. Holmström, and G. Ericsson, "Design requirements of wide-area damping systems - using empirical data from a utility IP network," *IEEE Transactions on Smart Grid*, vol. 5, pp. 829–838, March 2014.

[75] K. Zhu, S. Rahimi, L. Nordström, and B. Zhang, "Design phasor data concentrator as adaptive delay buffer for wide-area damping control," *Electric Power Systems Research*, vol. 127, pp. 22 – 31, 2015.

[76] M. Chenine and L. Nordström, "Investigation of communication delays and data incompleteness in multi-PMU wide area monitoring and control systems," in *International Conference on Electric Power and Energy Conversion Systems, 2009. EPECS '09.*, pp. 1–6, Nov 2009.

[77] W. G. C4.34, "To appear: Application of phasor measurement units for monitoring power system dynamic performance," tech. rep., CIGRE, 2017.

[78] L. Georgiadis, R. Guerin, V. Peris, and K. N. Sivarajan, "Efficient network QoS provisioning based on per node traffic shaping," *IEEE/ACM Transactions on Networking*, vol. 4, pp. 482–501, Aug 1996.

[79] M. Pignati, L. Zanni, S. Sarri, R. Cherkaoui, J. Y. L. Boudec, and M. Paolone, "A pre-estimation filtering process of bad data for linear power systems state estimators using PMUs," in *2014 Power Systems Computation Conference*, pp. 1–8, Aug 2014.

[80] K. D. Jones, A. Pal, and J. S. Thorp, "Methodology for performing synchrophasor data conditioning and validation," *IEEE Transactions on Power Systems*, vol. 30, pp. 1121–1130, May 2015.

[81] F. C. Schweppe, "Power system static-state estimation, part III: Implementation," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 130–135, Jan 1970.

[82] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part I: Exact model," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 120–125, Jan 1970.

[83] F. C. Schweppe and D. B. Rom, "Power system static-state estimation, part II: Approximate model," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 125–130, Jan 1970.

[84] J. Grainger and W. Stevenson, *Power System Analysis.* Electrical engineering series, McGraw-Hill, 1994.

[85] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach.* Power Electronics and Power Systems, Springer US, 2012.

[86] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation.* Power Engineering (Willis), CRC Press, 2004.

[87] M. Paolone, A. Borghetti, and C. A. Nucci, "A synchrophasor estimation algorithm for the monitoring of active distribution networks in steady state and transient conditions," in *Proc. of the 17th Power Systems Computation Conference (PSCC 2011), Stockholm, Sweden*, 2011.

[88] C. Muscas, M. Pau, P. A. Pegoraro, and S. Sulis, "Effects of measurements and pseudomeasurements correlation in distribution system state estimation," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, pp. 2813–2823, Dec 2014.

[89] E. Caro, A. J. Conejo, and R. Mínguez, "Power system state estimation considering measurement dependencies," *IEEE Transactions on Power Systems*, vol. 24, pp. 1875–1885, Nov 2009.

[90] F. Milano, ed., *Advances in Power System Modelling, Control and Stability Analysis.* Energy Engineering, Institution of Engineering and Technology, 2016.

[91] G. Welch and G. Bishop, "An introduction to the kalman filter," Tech. Rep. TR 95-041, Dep. of Computer Science, University of North Carolina, July 2006.

[92] A. M. L. da Silva, M. B. D. C. Filho, and J. F. de Queiroz, "State forecasting in electric power systems," *IEE Proceedings C - Generation, Transmission and Distribution*, vol. 130, pp. 237–244, September 1983.

[93] M. Hassanzadeh and C. Y. Evrenosoğlu, "Power system state forecasting using regression analysis," in *2012 IEEE Power and Energy Society General Meeting*, pp. 1–6, July 2012.

[94] A. S. Debs and R. E. Larson, "A dynamic estimator for tracking the state of a power system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 1670–1678, Sept 1970.

[95] L. Zanni, S. Sarri, M. Pignati, R. Cherkaoui, and M. Paolone, "Probabilistic assessment of the process-noise covariance matrix of discrete Kalman filter state estimation of active distribution networks," in *Probabilistic Methods Applied to Power Systems (PMAPS), 2014 International Conference on*, pp. 1–6, July 2014.

[96] M. Pignati, L. Zanni, P. Romano, R. Cherkaoui, and M. Paolone, “Fault detection and faulted line identification in active distribution networks using synchrophasors-based real-time state estimation,” *IEEE Transactions on Power Delivery*, vol. 32, pp. 381–392, Feb 2017.

[97] S. Horowitz, A. Phadke, and J. Niemira, *Power System Relaying*. Wiley, 2013.

[98] W. G. C-14, “Use of synchrophasor measurements in protecting relaying applications,” tech. rep., CIGRE, August 2013.

[99] S. Das, S. Santoso, A. Gaikwad, and M. Patel, “Impedance-based fault location in transmission networks: theory and application,” *IEEE Access*, vol. 2, pp. 537–557, 2014.

[100] F. H. Magnago and A. Abur, “Fault location using wavelets,” *IEEE Transactions on Power Delivery*, vol. 13, pp. 1475–1480, Oct 1998.

[101] R. Razzaghi, M. Paolone, F. Rachidi, J. Descloux, B. Raison, and N. Retière, “Fault location in multi-terminal HVDC networks based on electromagnetic time reversal with limited time reversal window,” in *Power Systems Computation Conference (PSCC), 2014*, pp. 1–7, Aug 2014.

[102] M. Korkali, H. Lev-Ari, and A. Abur, “Traveling-wave-based fault-location technique for transmission grids via wide-area synchronized voltage measurements,” *IEEE Transactions on Power Systems*, vol. 27, pp. 1003–1011, May 2012.

[103] K.-P. Lien, C.-W. Liu, C.-S. Yu, and J. A. Jiang, “Transmission network fault location observability with minimal PMU placement,” *IEEE Transactions on Power Delivery*, vol. 21, pp. 1128–1136, July 2006.

[104] Q. Jiang, X. Li, B. Wang, and H. Wang, “PMU-based fault location using voltage measurements in large transmission networks,” *IEEE Transactions on Power Delivery*, vol. 27, pp. 1644–1652, July 2012.

[105] J. Mora-Flòrez, J. Melèndez, and G. Carrillo-Caicedo, “Comparison of impedance based fault location methods for power distribution systems,” *Electric Power Systems Research*, vol. 78, no. 4, pp. 657 – 666, 2008.

[106] A. Borghetti, M. Bosetti, C. Nucci, M. Paolone, and A. Abur, “Integrated use of time-frequency wavelet decompositions for fault location in distribution networks: Theory and experimental validation,” *Power Delivery, IEEE Trans. on*, vol. 25, pp. 3139–3146, Oct 2010.

[107] J. Ren, S. Venkata, and E. Sortomme, “An accurate synchrophasor based fault location method for emerging distribution systems,” *Power Delivery, IEEE Transactions on*, vol. 29, pp. 297–298, Feb 2014.

[108] M. Shiroei, S. Daniar, and M. Akhbari, "A new algorithm for fault location on transmission lines," in *Power Energy Society General Meeting, 2009. PES '09. IEEE*, pp. 1–5, July 2009.

[109] A. Öner and M. Göl, "Fault location based on state estimation in PMU observable systems," in *Innovative Smart Grid Technologies Conference (ISGT), 2016 IEEE Power Energy Society*, pp. 1–5, Sept 2016.

[110] A. Abur, H. Kim, and M. Celik, "Identifying the unknown circuit breaker statuses in power networks," *Power Systems, IEEE Transactions on*, vol. 10, pp. 2029–2037, Nov 1995.

[111] F. Wu and W.-H. Liu, "Detection of topology errors by state estimation [power systems]," *Power Systems, IEEE Transactions on*, vol. 4, pp. 176–183, Feb 1989.

[112] V. Freitas and A. Simoes Costa, "Integrated state & topology estimation based on a priori topology information," in *PowerTech, 2015 IEEE Eindhoven*, pp. 1–6, June 2015.

[113] K. Christakou, D. C. Tomozei, J. Y. L. Boudec, and M. Paolone, "GECN: Primary voltage control for active distribution networks via real-time demand-response," *IEEE Transactions on Smart Grid*, vol. 5, pp. 622–631, March 2014.

[114] A. Borghetti, M. Bosetti, S. Grillo, S. Massucco, C. A. Nucci, M. Paolone, and F. Silvestro, "Short-term scheduling and control of active distribution systems with high penetration of renewable resources," *IEEE Systems Journal*, vol. 4, pp. 313–322, Sept 2010.

[115] D. Torregrossa, J.-Y. L. Boudec, and M. Paolone, "Model-free computation of ultra-short-term prediction intervals of solar irradiance," *Solar Energy*, vol. 124, pp. 57 – 67, 2016.

[116] E. Scolari, F. Sossan, and M. Paolone, "Irradiance prediction intervals for {PV} stochastic generation in microgrid applications," *Solar Energy*, vol. 139, pp. 116 – 129, 2016.

[117] G. Valverde and T. V. Cutsem, "Model predictive control of voltages in active distribution networks," *IEEE Transactions on Smart Grid*, vol. 4, pp. 2152–2161, Dec 2013.

[118] K. Christakou, *Real-Time Optimal Controls for Active Distribution Networks.* PhD thesis, IC, Lausanne, 2015.

[119] F. Sossan, E. Namor, R. Cherkaoui, and M. Paolone, "Achieving the dispatchability of distribution feeders through prosumers data driven forecasting and model predictive control of electrochemical storage," *IEEE Transactions on Sustainable Energy*, vol. 7, pp. 1762–1777, Oct 2016.

[120] K. Christakou, J. LeBoudec, M. Paolone, and D.-C. Tomozei, "Efficient computation of sensitivity coefficients of node voltages and line currents in unbalanced radial electrical distribution networks," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 741–750, 2013.

[121] D. Bertsekas, *Nonlinear Programming.* Athena Scientific, 1995.

[122] P. Constantopoulos, F. Schweppe, and R. Larson, "ESTIA: A real-time consumer control scheme for space conditioning usage under spot electricity pricing," *Computers & operations research*, vol. 18, no. 8, pp. 751–765, 1991.

[123] K. Christakou, M. Pignati, R. Rudnik, S. Sarri, J. Y. L. Boudec, and M. Paolone, "Hardware-in-the-loop validation of the grid explicit congestion notification mechanism for primary voltage control in active distribution networks," in *2016 Power Systems Computation Conference (PSCC)*, pp. 1–7, June 2016.

[124] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[125] A. Monticelli and A. Garcia, "Reliable bad data processing for real-time state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102, pp. 1126–1139, May 1983.

[126] T. V. Cutsem, M. Ribbens-Pavella, and L. Mili, "Hypothesis testing identification: A new method for bad data analysis in power system state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-103, pp. 3239–3252, Nov 1984.

[127] L. Mili and T. V. Cutsem, "Implementation of the hypothesis testing identification in power system state estimation," *IEEE Transactions on Power Systems*, vol. 3, pp. 887–893, Aug 1988.

[128] J. Zhu, *Detection and identification of network parameters errors using conventional and synchronized phasor measurements.* PhD thesis, Northeastern University, 2008.

[129] Y. Lin and A. Abur, "Strategic use of PMUs to improve network parameter error detection," in *2016 North American Power Symposium (NAPS)*, pp. 1–6, Sept 2016.

[130] A. M. L. da Silva, M. B. D. C. Filho, and J. M. C. Cantera, "An efficient dynamic state estimation algorithm including bad data processing," *IEEE Transactions on Power Systems*, vol. 2, pp. 1050–1058, Nov 1987.

[131] K. Nishiya, J. Hasegawa, and T. Koike, "Dynamic state estimation including anomaly detection and identification for power systems," *IEE Proceedings C - Generation, Transmission and Distribution*, vol. 129, pp. 192–198, September 1982.

[132] A. Leite da Silva, M. Do Coutto Filho, and J. F. De Queiroz, "State forecasting in electric power systems," *IEE Proceedings on Generation, Transmission and Distribution*, vol. 130, no. 5, pp. 237–244, 1983.

[133] J. Zhang, G. Welch, G. Bishop, and Z. Huang, "A two-stage Kalman filter approach for robust and real-time power system state estimation," *IEEE Transactions on Sustainable Energy*, vol. 5, pp. 629–636, April 2014.

[134] L. Zanni, J. Y. L. Boudec, R. Cherkaoui, and M. Paolone, "A prediction-error covariance estimator for adaptive Kalman filtering in step-varying processes: Application to power-system state estimation," *IEEE Transactions on Control Systems Technology*, vol. PP, no. 99, pp. 1–15, 2016.

[135] W. Kersting, "Radial distribution test feeders," in *IEEE Power Engineering Society Winter Meeting, 2001*, vol. 2, pp. 908–912 vol.2, 2001.

[136] M. Shahidehpour and M. Khodayar, "Cutting campus energy costs with hierarchical control: The economical and reliable operation of a microgrid," *IEEE Electrification Magazine*, vol. 1, pp. 40–56, Sept 2013.

[137] S. Barreto, M. Pignati, G. Dan, M. Paolone, and J. Y. L. Boudec, "Undetectable PMU timing-attack on linear state-estimation by using rank-1 approximation," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[138] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *2013 IEEE Energytech*, pp. 1–5, May 2013.

[139] N. Freris, S. Graham, and P. Kumar, "Fundamental limits on synchronizing clocks over networks," *IEEE Transactions on Automatic Control*, vol. 56, pp. 1352–1364, June 2011.

[140] S. Barreto, A. Suresh, and J. Y. L. Boudec, "Cyber-attack on packet-based time synchronization protocols: The undetectable delay box," in *2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, pp. 1–6, May 2016.

[141] *IEC/IEEE International Standard - Wide area network engineering guidelines*, July 2015. IEC/TR 61850-90-12:2015.

[142] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, pp. 87–98, March 2013.

[143] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, p. 56, 2008.

[144] G. Dán and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010*, pp. 214–219, Oct 2010.

[145] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, “Network-aware mitigation of data integrity attacks on power system state estimation,” *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1108–1118, July 2012.

[146] A. Pai, *Energy function analysis for power system stability*. Springer Science & Business Media, 2012.

[147] S. Sarri, *Methods and Performance Assessment of PMU-based Real-Time State Estimation of Active Distribution Networks*. PhD thesis, STI, Lausanne, 2016.

[148] J. Zhang and A. D. Domínguez-García, “On the failure of power system automatic generation control due to measurement noise,” in *2014 IEEE PES General Meeting & Conference Exposition*, pp. 1–5, July 2014.

[149] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle., “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, no. 127072, 2012.

[150] D. L. Mills and P.-H. Kamp, “The nanokernel,” in *Proceedings of the Precision Time and Time Interval (PTTI) Applications and Planning Meeting*, 2000.

[151] P. Romano, M. Pignati, and M. Paolone, “Integration of an IEEE Std. C37.118 compliant PMU into a real-time simulator,” in *2015 IEEE Eindhoven PowerTech*, pp. 1–6, June 2015.

[152] D. Ouellette, M. Desjardine, R. Kuffel, Y. Zhang, and E. Xu, “Using a real time digital simulator with phasor measurement unit technology,” in *Advanced Power System Automation and Protection (APAP), 2011 International Conference on*, vol. 3, pp. 2472–2476, Oct 2011.

[153] A. T. Al-Hammouri, L. Nordström, M. Chenine, L. Vanfretti, N. Honeth, and R. Leelaruji, “Virtualization of synchronized phasor measurement units within real-time simulators for smart grid applications,” in *2012 IEEE Power and Energy Society General Meeting*, pp. 1–7, July 2012.

[154] K. Zhu, S. Deo, A. T. Al-Hammouri, N. Honeth, M. Chenine, D. Babazadeh, and L. Nordström, “Test platform for synchrophasor based wide-area monitoring and control applications,” in *2013 IEEE Power Energy Society General Meeting*, pp. 1–5, July 2013.

[155] D. C. Ramirez, G. Gutiérrez-Alcaraz, A. Esparza-Gurrola, and J. Segundo-Ramírez, “Implementation of nonrecursive algorithm in RTDS for phasor estimation,” in *2016 North American Power Symposium (NAPS)*, pp. 1–5, Sept 2016.

[156] P. Romano and M. Paolone, "An enhanced interpolated-modulated sliding DFT for high reporting rate PMUs," in *Applied Measurements for Power Systems Proceedings (AMPS), 2014 IEEE International Workshop on*, pp. 1–6, Sept 2014.

[157] "Opal-RT eMEGAsim powergrid real-time digital hardware in the loop simulator." http://www.opal-rt.com/system-emegasim/. Accessed: 2017-02-24.

[158] "Spectracom PCI express slot cards." https://spectracom.com/products-services/precision-timing/tsync-timecode-processors. Accessed: 2017-02-24.

[159] "Current and voltage sensors - altea solutions." http://www.alteasolutions.com/new/. Accessed: 2017-01-07.

[160] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, "Cyber-secure communication architecture for active power distribution networks," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, SAC '14, (New York, NY, USA), ACM, 2014.

[161] C. M. Roberts, C. M. Shand, K. W. Brady, E. M. Stewart, A. W. McMorran, and G. A. Taylor, "Improving distribution network model accuracy using impedance estimation from micro-synchrophasor data," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2016.

[162] M. Brown, M. Biswal, S. Brahma, S. J. Ranade, and H. Cao, "Characterizing and quantifying noise in PMU data," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2016.

[163] F. Li and R. Bo, "Small test systems for power system economic studies," in *IEEE PES General Meeting*, pp. 1–4, July 2010.

[164] P. Janssen, *Monitoring, protection and fault location in power distribution networks using system-wide measurements*. PhD thesis, Ecole Polytechnique de Bruxelles, 2013-2014.

[165] S. Sarri, M. Pignati, P. Romano, L. Zanni, and M. Paolone, "A hardware-in-the-loop test platform for the performance assessment of a PMU-based real-time state estimator for active distribution networks," in *the 2015 IEEE PowerTech Conference*, 2015.

MARCO PIGNATI

Rue du Maupas 16 ⋄ 1004 Lausanne, Switzerland
+41 (0)78 673 74 18 ⋄ marco.pignati@gmail.com

RESEARCH INTERESTS

- Smart grids
- Phasor Measurement Units and their synchronization
- Real-time monitoring, protection and control of electrical grids

EDUCATION

EPFL – École Polytechnique Fédérale de Lausanne April 2013 - Present
PhD in Energy, Distributed Electrical System Laboratory (DESL) *Lausanne, Switzerland*

- Thesis title: "Resilient Synchrophasor Networks for the Real-Time Monitoring, Protection and Control of Power Grids: from Theory to Validation" (supervisor: Prof. Mario Paolone).

NEU – Northeastern University October 2015 - December 2015
Visiting researcher, Prof. Ali Abur's Power Systems Group *Boston, USA*

- Research related to the PhD thesis.

UNIBO – University of Bologna September 2010 - February 2013
M.Sc. in Electric Engineering *Bologna, Italy*

- Thesis title: "Integration of Phasor Measurement Units in Active Distribution Networks: Real-Time Synchronization and Data Collection" (supervisor: Prof. Carlo Alberto Nucci).
- Final mark: 110/110 with honors.

UNIBO – University of Bologna September 2007 - December 2010
B.S. in Electric Engineering *Bologna, Italy*

- Thesis title: "Automatic System for the Fault Location in Urban Medium Voltage Distribution Feeders" (supervisor: Prof. Mario Paolone)
- Final mark: 110/110 with honors.

SCIENTIFIC PUBLICATIONS

Journal papers[1]

1. Barreto, S.; Pignati, M.; Dan, G.; Paolone, M.; Le Boudec, J.-Y, "Undetectable PMU timing-attack on linear state-estimation by using rank-1 approximation," IEEE Transactions on Smart Grid, vol. PP, no. 99, pp. 11, 2016.
2. Derviskadic, A.; Romano, P.; Pignati, M.; Paolone, M., "Architecture and experimental validation of a low-latency phasor data concentrator," in IEEE Transactions on Smart Grid, vol. PP, no. 99, pp. 1-1.
3. Pignati, M; Zanni, L.; Romano, P; Cherkaoui, R.; Paolone, M., "Fault detection and faulted line identification in active distribution networks using synchrophasors-based real-time state estimation", in IEEE Transactions on Power Delivery, vol. 32, pp. 381-392, Feb 2017.

---

[1] Accepted and under review.

4. Wei Koong Chai; Ning Wang; Katsaros, K.V.; Kamel, G.; Pavlou, G.; Melis, S.; Hoefling, M.; Vieira, B.; Romano, P.; Sarri, S.; Tesfay, T.T.; Binxu Yang; Heimgaertner, F.; Pignati, M.; Paolone, M.; Menth, M.; Poll, E.; Mampaey, M.; Bontius, H.H.I.; Develder, C., "An information-centric communication infrastructure for real-time state estimation of active distribution networks," IEEE Transactions on Smart Grid, vol.6, no. 4, pp. 2134-2146, July 2015.
5. Frigo, G.; Colangelo, D.; Derviskadic, A.; Pignati, M.; Narduzzi, C.; Paolone, M., "Definition of accurate reference synchrophasors for static and dynamic characterization of PMUs," submitted to IEEE Transaction on Instrumentation and Measurements.

Conference papers

6. Pignati, M.; Popovic, M.; Barreto, S.; Cherkaoui, R.; Dario Flores, G.; Le Boudec, J.-Y.; Mohiuddin, M.; Paolone, M.; Romano, P.; Sarri, S.; Tesfay, T.; Tomozei, D.-C.; Zanni, L., "Real-time state estimation of the EPFL-campus medium-voltage grid by using PMUs," in Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society, pp. 1-5, 18th-20th Feb. 2015.
7. Pignati, M.; Zanni, L.; Sarri, S.; Cherkaoui, R.; Le Boudec, J.-Y.; Paolone, M., "A pre-estimation filtering process of bad data for linear power system State Estimators using PMUs," in Power System Computational Conference (PSCC), 2014 Wroclaw, August 18th-22nd 2014, pp. 1-8.
8. Christakou, K.; Pignati, M.; Rudnik, R.; Sarri, S.; Le Boudec, J.-Y.; Paolone, M., "Hardware-in-the-loop validation of the Grid Explict Congestion Notification mechanism for primary voltage control in active distribution networks," in Power System Computational Conference (PSCC), 2016 Genoa, Italy, pp. 1-7, 20th-24th June 2016,
9. Romano, P.; Pignati, M.; Paolone, M., "Integration of an IEEE Std. C37.118 compliant PMU into a real-time simulator," in PowerTech, 2015 IEEE Eindhoven, pp. 1-6, June 29th-July 2nd 2015.
10. Paolone, M.; Pignati, M.; Romano, P.; Sarri, S.; Zanni, L.; Cherkaoui, R., "A hardware-in-the-loop test platform for the real-time state estimation of active distribution networks using phasor measurement units," in Proceedings Cigr SC6 Colloquium, Yokohama, Japan, pp. 1-6, 6th-9th October 2013.
11. Zanni, L.; Sarri, S.; Pignati, M.; Cherkaoui, R.; Paolone, M., "Probabilistic assessment of the process-noise covariance matrix of discrete Kalman filter state estimation of active distribution networks," in International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Durham, U.K., pp. 1-6, 7th-10th July 2014.
12. Sarri, S.; Pignati, M.; Romano, P.; Zanni, L.; Paolone, M., "A Hardware-in-the-loop test platform for the performance assessment of a PMU-based real-time state estimator for active distribution networks," in PowerTech, 2015 IEEE Eindhoven, pp. 1-6, June 29th-July 2nd 2015.
13. Colangelo, D.; Zanni, L.; Pignati, M.; Romano, P.; Paolone, M.; Braun, J.-P.; Bernier, L.-G., "Architecture and characterization of a calibrator for PMUs operating in power distribution systems," in PowerTech, 2015 IEEE Eindhoven, pp. 1-6, June 29th-July 2nd 2015
14. Frigo, G.; Narduzzi, C.; Colangelo, D.; Pignati, M.; Paolone, M., "Definition and assessment of reference values for PMU calibration in static and transient conditions," in IEEE International Workshop on applied Measurements for Power Systems (AMPS), Aachen, pp. 1-6, 28th-30th September 2016.

AWARDS

- Best Poster Award at the 2015 SCCER-FURIES Annual Conference, Romano, P.; Derviskadic, A.; Zanni, L.; Pignati, M.; Paolone, M.; Leboudec, J-.Y, "Real-time state estimation of the EPFL-campus medium voltage grid by using PMUs," Lausanne, 25th Nov. 2015.
- Best Paper Award at the 13th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), 2014, Zanni, L.; Sarri, S.; Pignati, M.; Cherkaoui, R. and Paolone, M., "Probabilistic assessment of the process-noise covariance matrix of discrete Kalman filter state estimation of active distribution networks," Durham, U.K., 7-10 Jul. 2014, pp. 1-6.

PATENTS

Pignati M.; Zanni L.; Romano P.; Paolone M., "Method and System for Fault Detection and Faulted Line Identification in Power Systems using Synchrophasor-based Real-Time State Estimation," US Patent App. 15/158,791, June 15th, 2016.

INVITED TALKS

Romano, P.; Pignati, M.; Paolone, M, "Integration of an IEEE Std. C37.118 compliant PMU into the OPAL-RT real-time simulation", RT15 Conference – Opal-RT European User Group Event, Barcelona, Spain, May 27th-28th, 2015.

RESEARCH PROJECTS

NanoTera S^3Grid - SmartGrid April 2013 - April 2017

- Development of new technologies dedicated to the real time monitoring and management of smart grids with validation in the EPFL campus (`smartgrid.epfl.ch`).

ENG52 SmartGrid II September 2014 - May 2017

- Measurement tools for Smart Grid stability and quality (`https://www.euramet.org/`).
- Development of new calibration methods and technologies for Phasor Measurement Unit expected to operate in Distribution Networks.

RT-PMU January 2014 - January 2017

- Installation of 15 Phasor Measurement Units in the sub-transmission network operated by Services industriels de Lausanne (SiL).
- Upgrade of the SCADA system of SiL by integrating a real-time state estimation process based on Phasor Measurement Units.

SUPERVISED STUDENTS

- Bernabeu, J., “Computation of the admittance matrix for fixed or variable network topology”, Semester project, Spring Semester 2013-2014.
- Di Labio, E.,“Integration of an IEEE Std. C37.118 compliant PMU into the OPAL-RT real-time simulation”, M.Sc. Thesis project, Spring Semester 2013-2014.
- Varescon, E., “Latency Optimization on LabVIEW”, Summer project, 2014.
- Cyrille, R., “Modeling and real-time validation of a benchmark test network”, Semester project, Fall Semester 2016-2017.
- Derviskadic, A., “Development of a PMU-based RTSE of subtransmission networks: theory and experimental validation based on the Lausanne 125 kV grid”, M.Sc. Thesis project, Spring Semester 2014-2015.

PEER REVIEWS

- Elsevier Sustainable Energy, Grids and Networks Journal, since 2015
- IET Generation, Transmission & Distribution, since 2016
- IEEE International Energy Conference (EnergyCon), 2016
- 19th Power Systems Computation Conference (PSCC), 2016

LANGUAGE SKILLS

Italian	Mother tongue.
English	Full professional proficiency.
French	Minimum professional proficiency.