Security Assessment and Protection of Cyber-Physical Energy Systems

Rasmussen, Theis Bo

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Center for Electric Power and Energy

Theis Bo Rasmussen

Security Assessment and Protection of Cyber-Physical Energy Systems

PhD Thesis, May 2019
Kongens Lyngby, Denmark

DANMARKS TEKNISKE UNIVERSITET
Center for Electric Power and Energy (CEE)
DTU Electrical Engineering

Security Assessment and Protection of Cyber-Physical Energy Systems

Sikkerhedsvurdering og Beskyttelse af Cyber-fysiske Energisystemer

Dissertation, by Theis Bo Rasmussen

Supervisors:
Associate Professor Guangya Yang, Technical University of Denmark
Associate Professor Arne Hejde Nielsen, Technical University of Denmark
Professor Zhao Yang (Joe) Dong, University of New South Wales, Australia

DTU - Technical University of Denmark, Kgs. Lyngby - May 2019

Security Assessment and Protection of Cyber-Physical Energy Systems

This thesis was prepared by:
Theis Bo Rasmussen

Supervisors:
Associate Professor Guangya Yang, Technical University of Denmark
Associate Professor Arne Hejde Nielsen, Technical University of Denmark
Professor Zhao Yang (Joe) Dong, University of New South Wales, Australia

Dissertation Examination Committee:
Associate Professor Chresten Trœholt (Chairman)
Department of Electrical Engineering, Technical University of Denmark, Denmark

Senior Research Scientist Marija D. Ilić
Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, MA, USA

Professor Yusheng Xue
State Grid Electric Power Research Institute, China

Center for Electric Power and Energy (CEE)
DTU Electrical Engineering
Elektrovej, Building 325
DK-2800 Kgs. Lyngby
Denmark

http://www.cee.elektro.dtu.dk

Release date: May 1st, 2019

Edition: 1st

Class: Public

Field: Electrical Engineering, Electric Power System

Remarks: The dissertation is presented to the Department of Electrical Engineering of the Technical University of Denmark in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Til Line

Preface

This thesis is prepared at the Department of Electrical Engineering of the Technical University of Denmark in partial fulfillment of the requirements for acquiring the degree of Doctor of Philosophy in Engineering. The Ph.D. project was funded by internal DTU Elektro funding.

This dissertation summarizes the work carried out by the author during his Ph.D. project. It started on 1st April 2016, and it was completed on 1st May 2019. During this period, he was hired by the Technical University of Denmark as a Ph.D. student at the Center for Electric Power and Energy (CEE).

The thesis is composed of 7 chapters and is based on 6 scientific papers where one describes an invention that is described in a patent application submitted to the European Patent Office on the 24th of June 2019. Until the day of submitting the patent application, this thesis was kept confidential. Five of the scientific papers have been peer-reviewed and published, whereas the one is to be submitted to a relevant journal.

May 1st 2019

Acknowledgements

I want to express my gratitude to my two supervisors at DTU, Guangya and Arne, who gave me the opportunity to pursue a PhD degree. During the three years of my studies, I have been fortunate to work in close collaboration with these passionate and experienced researchers. In particular, I would like to thank my principle supervisor, Guangya for never restricting the direction of my work and for our numerous discussion that have helped shaping the research contribution presented in this thesis.

In my three years as a PhD student at DTU, I have been fortunate to travel for external courses, meetings, conferences and an external stay. For these opportunities, I'm grateful for the funding that I've received, both from DTU Elektro through my internal scholarship, and from external funding sources. I therefore thank National Instruments for awarding me a travel grant, as well as Otto Mønsted Foundation and the Idella Foundation for helping me fund my external research stay.

A special appreciation goes to my external supervisor, Professor Joe Dong at University of New South Wales, Sydney, Australia, for hosting and welcoming me on my external research stay from November 2017 to February 2018. I enjoyed my time at UNSW and my discussions with Professor Dong and his research group. In particular I found the external research stay a great opportunity to experience a change of scenery which helped my focus my work for the last part of my PhD project.

I have enjoyed my time at DTU, especially in the presence of my talented colleagues with whom I have shared an office space. Therefore I want to express a very special thanks to Can, Jakob, Christina, Jundi and Ha, for being great colleagues and friends. Last but not least, I feel lucky to have such a great family and group of friends, who have always been there for my during the ups and downs of my journey in academia. Especially, I would like to thank my father Lars and uncles Anders and Finn, for their feedback on my written work including this thesis. The greatest thanks however, goes to my loving fiancée, Line, for your amazing and endless support!

Theis Bo Rasmussen

Kongens Lyngby, Denmark, May 2019

Table of Contents

List of Figures

List of Tables

Abstract

The quest of a decarbonized modern society has increased the integration of small Distributed Generation (DG) units that are based on renewable sources of energy in the electric power system, and has entailed a decentralization of power generation. In parallel with a decommissioning of central fossil-fueled power plants, this development has gradually decentralized active and reactive power flow management from the transmission to the distribution network. Moreover, the increased focus on investment and utilization of the Information and Communication Technology (ICT) infrastructure has caused a transition of the power system into a Cyber-Physical Energy System (CPES). From a distribution network perspective limited attention has been paid to assess the security and protect the CPES operation, therefore new methods are needed to 1) enable the monitoring of Low Voltage (LV) network operational conditions using the existing ICT infrastructure, and 2) protect the DG controls against cyber-physical interdependencies.

The work presented in this thesis focuses on distribution network security assessment and protection in a CPES perspective considering 1) the entailed information security challenges in terms of confidentiality, integrity, and availability, and 2) the limited performance of the existing ICT infrastructure deployed in distribution networks in terms of metering, communicating, and processing equipment. Acknowledging these challenges and limitations, this thesis proposes two LV network monitoring approaches, a demonstration of a bottom-up approach to DG unit cyber error detection, and an investigation of the impact from cyber-physical conditions on the coordination of DG controls in a LV network.

From the activation of the General Data Protection Regulation (GDPR) by the European Commission, the information about consumption from residential load points can be restricted for LV network monitoring. Therefore, only shared network quantities can be used estimate network conditions. The first LV network monitoring method proposed in this work addresses this challenge. While acknowledging the risk of asynchronous measurement acquisition from smart meters, it estimates the interval of voltage magnitude conditions of an entire radial LV feeder through processing the measurements from network nodes one by one.

If information confidentiality concerns are less stringent, individual household consumption can be applied in monitoring of the LV network. However, existing Distribution System State Estimation (DSSE) methods ignore the time requirements of three phase state estimation for LV network application, which combined with the volatile LV network operation scenarios from demand side management and operation of DG units, can diminish DSSE results. Therefore, the second proposed LV network monitoring approach considers these challenges, and applies DSSE through a bi-level processing platform. This platform is developed to utilize both periodic and event-driven measurements and can return network conditions during and between DSSE execution.

With the decentralization of generation and control from an increased integration of DG units, it is increasingly important to protect the DG controls against hazardous commands. Their protection

is however challenged since both cyber and physical system operational conditions affect the reliability of DG controls. Such challenge is considered in this work through demonstration and investigation of DG control protection against cyber system integrity disturbances, and physical system perturbations. In particular, a physical system analysis based approach for cyber error detection, is demonstrated through establishment and implementation of state estimation and bad data detection techniques in a distributed processor. This represents a bottom-up approach to DG control protection against unintended and intended information integrity disturbances from ICT infrastructure deficits and cyber-attacks, respectively. In the end, a cyber-physical simulation platform is established to investigate and coordinate DG control strategies in cyber-physical conditions.

Resumé

Målet om udfasning af fossile brændstoffer i det moderne samfund har øget integrationen af små el-producerende enheder, drevet af vedvarende energikilder, i elnettet og har medført en decentralisering af hele elproduktionen. Kombineret med en udfasning af centralt placeret fossile kraftværker har denne udvikling gradvist decentraliseret aktive og reaktive strømstyringsfunktioner fra transmissionen til distributionsnetværket. Desuden har investeringer og udnyttelse af informations- og kommunikationsteknologi (IKT) forårsaget, at elnettet udvikler sig til et cyber-fysisk energisystem. På distributionsnetværks niveau er der begrænset opmærksomhed på at vurdere sikkerheden og beskytte driften af det cyber-fysiske energisystem. Derfor er der brug for nye metoder til at 1) muliggøre overvågning af lavspændingsnettet igennem anvendelse af eksisterende IKT-infrastruktur og 2) beskytte kontrollen af de distribuerede el-producerende enheder imod indbyrdes cyber-fysiske afhængigheder.

Denne afhandling fokuserer på vurdering og beskyttelse af distributionsnetværkets sikkerhed i et cyber-fysisk energisystem, mens der tages højde for 1) udfordringer omkring informationssikkerheden med hensyn til fortrolighed, integritet og tilgængelighed og 2) den begrænsede ydeevne for eksisterende IKT-infrastruktur, implementeret i distributionsnet med henblik på måle-, kommunikations- og databehandlingsteknologier. Gennem en anerkendelse af disse udfordringer og begrænsninger bidrager denne afhandling med en udvikling af to netværksovervågningsmetoder til vurdering af driften i lavspændingsnetværket, en demonstration af et cyber-fejls detektionssystem til anvendelse i distribuerede el-producerende enheder gennem en nedefra og op tilgang, samt en undersøgelse af hvordan kontrollen af lavspændingsnetværks forbundne el-producerende enheder påvirkes af cyber-fysiske tilstande.

Siden aktiveringen af persondataforordningen fra Europa-Kommissionen kan udnyttelsen af forbrugsprofiler være begrænseset i forhold til lavspændingsnetværks overvågning. Dette efterlader kun delte netværksobservationer til vurdering af lavspændingsnettet. Den første af de to forslåede metoder til overvågning af lavspændingsnettet løser denne udfordring, mens risikoen for asynkron måleindsamling fra smart målere anerkendes. Således opnås en estimering af mulige spændingsbetingelser som intervaller for en hel lavspændingsradial, mens målinger fra netværksknudepunkters behandles individuelt.

Et mere afslappet forhold til forbrugsmønstres fortrolighed betyder, at forbrugsprofiler kan inddrages i en estimering af lavspændingsnettets drift. Eksisterende programmer, der benytter distributionsnetværks tilstandsestimering, ignorerer dog problemet med begrænset databehandlingskapacitet samt den stigende variation af driftstilstande i lavspændingsnettet pga. elektrificering af tjenester og integration af små el-producerende enheder. Kombinationen af disse udeladelser kan forælde resultaterne af tilstandsestimeringen, hvilket begrænser værdien af disse fremgangsmåder. Derfor berører den anden af de to foreslåede lavspændingsnetværks overvågningsmetoder disse udfordringer ved anvendelse af tilstandsestimering i en todelt behandlingsplatform. Denne platform er udviklet til at udnytte både periodisk og eventdrevet

måleindsamling og kan derved estimere og returnere netværksforholdene under og mellem udførelsen af tilstandsestimering.

Vigtigheden af at beskytte små el-producerende enheder mod uhensigtsmæssig adfærd stiger med decentraliseringen af elproduktion og -kontrolfunktioner. Beskyttelsen er imidlertid udfordrende, da både de cyber- og de fysiske systemer påvirker pålideligheden af kontrollen af de distribuerede el-producerende enheder. Denne udfordring betragtes i denne afhandling gennem en demonstration og undersøgelse af beskyttelse af distribuerede el-producerende enheder imod cyber systems integritetsforstyrrelser og fysiske systemforstyrrelser. Konkret set demonstreres en tilgang til cyberfejl detektering gennem analyse af det fysiske system, der udgør de distribuerede el-producerende enheder. Dette detekteringssystem er formet af en etablering og implementering af tilstandsestimering og dårlige data detektionsteknikker i en distribueret databehandlingsteknologi. Dette repræsenterer en nedefra og op tilgang til kontrolbeskyttelse af de distribuerede el-producerende enheder mod informationsintegritetsforstyrrelser. Derudover er en simpel cyber-fysisk simuleringsplatform etableret til simulering af en lavspændingsradial med forbundne el-producerende enheder og brugt til at undersøge og koordinere kontrolstrategier for distribuerede el-producerende enheder under cyber-fysiske betingelser.

Acronyms

The acronyms in this thesis are sorted in an alphabetic order

AC Alternating Current

AEE Average Euclidean Error

BDD Bad Data Detection

CENELEC European Committee for Electrotechnical Standardization

CER Commission for Energy Regulation

CFS Control Flow Structure

CIP Critical Infrastructure Protection

COSEM Companion Specification for Energy Metering

CPES Cyber-Physical Energy System

CPH Copenhagen

CPS Cyber-Physical System

cRIO compact-RIO

CVR Conservative Voltage Reduction

DC Direct Current

DER Distributed Energy Resource

DFIG Doubly Fed Induction Generator

DG Distributed Generation

DLMS Device Language Message Specification

DNO Distribution Network Operator

DNP3 Distribution Network Protocol

DoS Denial of Service

DSSE Distribution System State Estimation

E-ISAC Electricity Information Sharing and Analysis Center

EFS Energy Flow Structure

EU European Union

EV Electric Vehicle

FACTS Flexible Alternating Current Transmission System

FASE Forecast Aided State Estimator

FDIR Fault Detection, Isolation and Service Restoration

FPGA Field Programmable Gate Array

GDPR General Data Protection Regulation

GPRS General Packet Radio Service

GPS Global Positioning System

GSM Global System for Mobile Communications

ICT Information and Communication Technology

IDE4L Ideal Grid for All

IDS Intrusion Detection System

IEA International Energy Agency

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

LV Low Voltage

MFM Multilevel Flow Modeling

MFS Mass Flow Structure

MPC Model Predictive Control

MV Medium Voltage

NAN Neighborhood Area Network

NERC North American Electric Reliability Corporation

NI National Instruments

NTP Network Time Protocol

OBIS Object Identification System

OFGEM Office of Gas and Electricity Markets

OPC Open Platform Communications

OPF Optimal Power Flow

OS Operating System

PDF Probability Density Function

PLC Power Line Communication

PMU Phasor Measurement Unit

PV Photovoltaic

RES Renewable Energy Source

RF Radio Frequency

RTDS Real Time Digital Simulator

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

TSO Transmission System Operator

UCTE Union for the Coordination of the Transmission of Electricity

VI Virtual Instrument

VUF Voltage Unbalance Factor

WAN Wide Area Network

WAMS Wide Area Monitoring System

WLS Weighted Least-Squares

WPP Wind Power Plant

WTCP Wind Turbine Control Panel

Part I

Introduction

CHAPTER 1

Introduction

1.1 Background

Since the origin of the electric power system in the late 19th century, where Thomas A. Edison, Charles Steinmetz, William Stanley, Nikola Tesla among others, performed pioneering work that enabled supply of electricity to consumers, remote monitoring and control have played a vital role in maintaining a reliable supply [1]. The concept of Supervisory Control and Data Acquisition (SCADA) systems origins from the telecommunication industry in the beginning of the 20th century, and its modern architecture is typically composed of a central unit, multiple Remote Terminal Units (RTUs), and a network of communication technology that connects the assets. As power systems grew in size and complexity, the communication infrastructure became more of an essential for supervision of remote assets rather than an accessory [2].

The RTUs were traditionally seen as the sensing and actuating part of the SCADA system, but from the 1980s, the development and integration of Intelligent Electronic Devices (IEDs), capable of monitoring, processing and controlling substation equipment and information, the RTU role in modern SCADA systems has changed, and it now act as a gateway for protocol compliant data routing [3, 4].

Over time, Information and Communication Technology (ICT) development and implementation has increased the amount and diversity of power system related information that can be measured, communicated and processed in modern SCADA systems [5, 6]. Such development improve the foundation for supervision and control of the power system and simultaneously entails interdependencies between the operation of the physical system and the cyber system, transitioning the power system into one of the most complex Cyber-Physical Systems (CPS's) created by mankind. During the last few decades, evidences of this transition and the interdependencies between domains in the Cyber-Physical Energy System (CPES) have been revealed by catastrophic events. In 2003 alone, four unwanted events occurred due to CPES issues as listed in Table 1.1.

Table 1.1: Evidences of cyber-physical interdependencies in the power system during 2003

Location	Date	Cause
North America	14 Aug	Lack of real-time measurements at the control center prevented network monitoring applications and eventually caused line tripping and cascading events [7].
London (UK) West Midlands (UK)	28 Aug 5 Sept	For both events, malfunction of substation protection equipment caused breaker openings and cascading failures [8].
Italy	28 Sept	A large angle difference across a tripped line violated the threshold settings of the automatic re-closer, which eventually caused cascading failures [9].

While the listed events were caused by ICT failures triggering CPES interdependencies, recently there have been reports of intentional exploitation of ICT vulnerabilities, of which the consequences can be substantial. In December 2015, the Ukrainian power system was subject to a cyber-attack where adversaries gained access to the SCADA system of a utility company and managed to remotely open substation breakers, causing an interruption of the power supply to approximately 225,000 customers for a duration of 6 hours [10]. The Ukrainian power outage was caused by exploitation of CPES interdependencies, and represent an extreme examples of the potential impact of cyber-attacks. Such consequences has attracted considerable attention from the research community in recent years [11–32]. This effort and the cyber-physical events show that the CPES is a reality, and that assessment and protection of the energy system security requires careful consideration of both cyber and physical domain. The CPES transition is emphasized by one of the key trends of our modern society, i.e. the global concerns of climate changes. This concern entails a decentralization of generation from a few centralized power plants to numerous Distributed Generation (DG) units, which increase the necessary reach of supervision and control systems.

The desire for sustainability has entailed ambitious targets for decarbonisation of the energy system, including the electricity infrastructure. In 2014, the European Council reached an agreement to reduce the greenhouse gas emissions by 2030 to a targeted value 40 % lower than that of 1990 [33]. Recently, the *Clean energy for all Europeans* package, from the European Union (EU), seeks to upgrade this target to 45% lower than that of 1990 [34]. In this context, the targeted share of energy consumption from Renewable Energy Sources (RES's) is set to be 32% by 2030. The decarbonisation of the electricity generation is visible from the annual global electricity generation from RES's, such as wind and solar. Wind power has almost ten-doubled from 104 TWh in 2005 to 958 TWh in 2016, while annual electricity production from solar Photovoltaic (PV) has increased from virtually nothing in 2005 to more than 300 TWh in 2016, which is more than the combined annual electricity consumption of Denmark, Norway and Sweden [35]. Due to the low energy density of the RES-based power generation compared to the conventional fossil fuel power plants, these DG units have much lower power capacity. Combined with their dependency on fluctuating RES's, a vast quantity and distribution of units is necessary to fulfill the CPES electricity demand.

With relatively small individual generating units, their connection to the power system is typically seen as either an aggregation of multiple units that reach a considerable power capacity and connects to the transmission or Medium Voltage (MV) distribution network, or as stand alone systems that connect to the MV or Low Voltage (LV) network. As a greater share of the generating capacity is implemented in the MV and LV distribution network, where SCADA systems are less comprehensive and the ICT infrastructure less reliable [36], the importance of assessment and protection of this part of the CPES increases.

As conventional power plants are decommissioned, the characteristics of CPES control capability[1] and thereby the means of performing protective changes in the power flow, changes from being centralized at a few large generating plants connected to the transmission system, to being distributed in numerous small DG units largely connected to the distribution network. In addition, control capabilities of such DG units are directly limited by their dependency on fluctuating RES's. With the distribution of control capabilities away from the SCADA system due to its limited reach within the distribution network, these DG units will operate autonomously [37, 38]. Such autonomous behaviour, however, does not contribute to overall coordination of DG controls which

[1] Referring to active and reactive power control during quasi-steady state operation.

is useful to obtain higher sustainability and for achieving a response to network wide control objectives. Enabling such behaviour requires bi-directional flow of information between the DG unit and a control center processor that handles control coordination based on the conditions in the physical system, meaning the quality of controls depend on the operation of the supporting ICT infrastructure.

The pursuit of a RES-based power generation and the interdependencies between cyber and physical infrastructures therefore entail research challenges in distribution network security assessment and protection of CPES. Firstly, at the LV level, networks are designed for uni-directional power flow without the need of monitoring due to over-dimensioned infrastructure. The implementation of DG, and electrification and possible control of residential services, such as heating and transportation, entails the possibility of greater and bi-directional power flows within the distribution network, thereby increasing the need for monitoring at the last mile of the electricity supply. Secondly, the decentralization of power system control capabilities means operation of the CPES depends on the reliability of DG controls. Such can be coordinated from an estimation of physical conditions based on acquired information about system conditions, with the risk of potential distortion through measurement noise or the interference from adversaries. This increase the importance of protecting DG controls against hazardous conditions of the cyber-physical operating environment. To protect and assess security of CPES, monitoring of LV networks and protection of DG controls thereby represent a considerable research challenge with multiple open questions.

1.2 State of the art

Understanding the existing efforts in monitoring LV networks and protection of DG controls requires an overview of ICT infrastructure differences at the two levels of the power system, transmission and distribution. With this overview, current state of the art within security assessment and protection is evaluated and discussed from a distribution network perspective, leading to the identification of research questions within LV network monitoring and protection of DG controls, that are addressed as the contribution of this thesis.

1.2.1 Information and communication technology development

The development of ICT equipment is analyzed at transmission and distribution network levels and based on a separation of equipment domains in metering, communicating, and processing. For each ICT domain, representative technology categories are presented as the current state of the art in the cyber systems.

Metering

Two major ICT developments capture the evolution of metering at different levels of the power system. Worldwide increase in smart meter deployments has increased the number of measurement points in distribution networks, while synchrophasors improves metering at transmission level through capturing a high level of details of the power system operational conditions.

The objective of synchrophasor measurements is to enable a measurement of power system phase angle at distant locations. For such ability, a global reference must allow a coupling between measurement equipment. With Phasor Measurement Unit (PMU) technology utilizing Global Positioning System (GPS) satellites, the phase angle measurement of power system voltages and

currents can be measured [39]. According to the IEC/IEEE International standard 60255-118-1 in [40], PMU must be able to report the acquired data as sub-multiples or multiples of the nominal system frequency, which for 50 Hz system must be within 10 to 100 reports per second. Furthermore, the requirements for measurement error are specified through the total vector error, which must be below 1%. This corresponds to a magnitude error of $\pm 1\%$ of rated voltage with zero angle error, and an angle error of ± 0.01 rad with zero magnitude error.

Smart meters are electricity meters with bi-directional communication capabilities. Electricity consumption information is measured periodically with time intervals shorter than one hour, and collected daily by the grid company. These meters can be configured by adjusting the Object Identification System (OBIS) codes using the Companion Specification for Energy Metering (COSEM) protocol, to broadcast a variety of measured data periodically [41]. The accuracy requirements of smart meters are defined in international standards, such as EN 50470-3 [42], and depends on the phase connection and the accuracy class. Most polyphase meters are of class B, which allows an error of $\pm 1.5\%$ and $\pm 1\%$ compared to rated characteristics for low and high load conditions, respectively.

The current deployment status of PMUs worldwide is driven by a desire for better estimation capabilities through Wide Area Monitoring System (WAMS). The deployment is ongoing and typically seen through integrated devices in transmission system substations [43, 44]. In distribution networks, the integration of PMUs is impeded by the high expenses associated with integrating the necessary communication infrastructure and ensuring compliance with cyber-security protocols, meaning only around 5% of the total cost, reportedly around $40,000 to $180,000, is for the PMU technology [45].

In comparison, the deployment of smart meters is supported by governmental initiatives and desire for a more efficient electricity delivery. This means the expected quantity of smart meters in 2022 is around 1 billion devices worldwide [46]. An observation through trials of managing numerous devices is that the reliability of acquisition has been challenging [47, 48]. Furthermore, the handling and processing of smart meter data is affected by the EU General Data Protection Regulation (GDPR), which increase the consumer rights in deciding on the use of their data, including electricity meter readings [49]. While the deployment of smart meters is much further than that of PMUs, effectively providing a better spatial metering resolution, the PMUs offer a more reliable stream of data with a higher time resolution.

Communicating

Communicating capabilities are key to enable control and metering of IEDs, PMUs, smart meters, etc. Two key characteristics that differentiate the transmission and distribution requirement of the communication capabilities, are the distance and data rate at which information is transferred. Two terms are formed to represent this differentiation, Wide Area Networks (WANs) and Neighborhood Area Networks (NANs) for transmission and distribution system data communication, respectively. Current literature has defined distance coverage as 10 - 100 km for WAN and 0.1 - 10 km for NAN, which are based on the distribution of units within each network. The data rate requirements of communicating media are identified through an analysis of the applications that require a transfer of information. These requirements can be based on the urgency of the data acquisition or control activation, or from the sampling frequencies of the connected devices [50, 51].

In [50], a possible applications in a WAN and in a NAN are listed. This list show that NANs applications, such as smart meter reading, electricity price broadcasting and demand response signaling, have latency requirements in the range of seconds to hours, and reliability performance requirements above 98%. For WANs, latency in the order of milliseconds to minutes and a reliability larger than 99.9% is desired for applications such as PMU data acquisition, Flexible Alternating Current Transmission System (FACTS) device control, and under-frequency load shedding.

The higher requirements on the WAN, means suitable communication media must be able to handle environmental impact such as structural blockage and electromagnetic interference, and congestion due to shared media utilization along other applications, such as television, telephone calls and internet traffic. For such abilities, optic fiber technology has proven an ideal media as it simultaneously allows communication across long distances. The more relaxed requirements on the NAN communication infrastructure, enables the use of lower cost technologies, such as Radio Frequency (RF) mesh, Power Line Communication (PLC) and older generation cellular including Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS) [50, 52].

Processing

Prior to the implementation of IEDs SCADA systems were predominantly centralized in the sense that all information from RTUs was transmitted to a control center for processing. With the integration of multiple IEDs from the 1980s, processing capabilities were to a greater extend decentralized closer to the point of metering and control, thereby slowly changing the architecture of power system processing from a centralized to a decentralized topology. With the decentralized processing architecture, the information flow within the CPES is processed in multiple subsystems by their respective processing unit, meaning the flow of information is decreased and the computational requirement of each processor is lowered compared to a centralized topology.

In recent years, the changes in power system composition through integration of numerous RES-based DG units and the increasing information flow from investments in ICT infrastructure, challenges the processing of information in the CPES [53]. Such a challenge is addressed through technological advances in both centralized and decentralized processing.

Firstly, the centralized processing topology is gaining attention due to the technology development of high performance computation techniques, allowing faster processing of a greater information flow [53–55]. Within high performance computing, the use of cloud servers offers a processing solution which can be utilized on a subscription basis, this diminish the need for utility investment in processing infrastructure and takes advantage of economics of scale [52]. The use of cloud computing, however, is not considered for handling real-time data acquisition, due to the expected latency of internet traffic, and removes the utility control of data handling as hardware assets are owned by tertiary entities [56]. These security concerns are avoided if the utility owned SCADA system is supported by high performance computational resources, such as numerous graphical processing units that provide an infrastructure for parallel processing. Parallel computing in large centralized units can satisfy the execution time and has been a known field of research in recent years [54, 55].

Secondly, the decentralization of CPES processing is becoming increasingly feasible with the implementation of additional IEDs within the power system, also at the distribution level through digitization of substations according to IEC 61850 and implementation of smart meters and Distributed Energy Resources (DERs) that have inherent computational capabilities. This

integration of computational resources increases the level of decentralization, in which the subsystem domain of individual processors can be all the way down to a single component level, e.g. a household or a PV plant, through the smart meter and PV inverter, respectively. Decentralizing processing closer to the boundary between the cyber and physical systems is sometimes referred to as distributed processing or edge computing[2] [57]. Such processing at the peripheral of the cyber system, entails a possibility for autonomous and closed loop behaviour of CPES components without the dependency on flow of information to and from other devices.

From a power system architecture perspective, the distribution network contains a greater number of nodes than the transmission network, but is usually separated in geographically smaller areas that only connects through the transmission system allowing a division into processable sub-systems. Additionally, distribution networks are usually divided at different voltage levels, where the higher voltage network connection is represented as an infinite bus, and lower voltage networks are aggregated at the point of connection, which allows a further decomposition of the network into smaller processable sub-systems. This makes decentralized processing suitable for hierarchical processing of data within the CPES, through which large data quantities can be handled locally across multiple computing devices [58, 59]. In comparison, the transmission network is usually represented as a whole and covers a large geographical area. Considering the information flow at the transmission level of the CPES, the implementation of metering devices with high temporal resolution e.g. PMUs, and the reliable and fast communicating infrastructure e.g. optic fibres, entails steady flow of information from distant locations available for processing in a centralized processing topology.

Advances in both centralized and decentralized processing technology can therefore improve the ICT infrastructure at transmission and distribution network levels of the CPES. With the high performance computation technology of the centralized processing topology, the performance of evaluating a large scale transmission network with frequent updates can be improved [55]. In addition, the separation of the distribution network into sub-system is well suited for the decentralized processing. Furthermore, the lower temporal resolution of the metering infrastructure in the distribution network entails the possibility of utilizing low-cost IEDs, that have considerable lower computational performance and quality of components than high performance computing infrastructure [13].

1.2.2 Security assessment and monitoring

One of the key processing tasks in power system supervision is static security assessment, where the operational security of the power system is evaluated before and after possible disturbance scenarios. The assessment process consists of a monitoring phase where network conditions are compared against physical and regulatory limitations. Here, especially the nodal voltages and equipment current ratings are considered. Following the evaluation of observed network conditions, an analysis of possible contingencies is performed using simulation tools according to a pool of possible contingencies. The considered contingencies typically include $N-1$ conditions, representing situations where the most critical power system component in each category, e.g. transmission line, power generator, transformer, etc. is subject to an error and stops functioning correctly. In the case that any network constraints are violated either prior to or after any of

[2]Referred to as distributed processing in this thesis

the disturbance scenarios analyzed, possible protective measures are identified and activated accordingly [60, 61].

However, the security assessment is vulnerable to entailed measurement error and un-measured network quantities, e.g. the current flow in lines not covered by the metering infrastructure. Such error can cause un-favorable operating conditions and potentially inflict hazardous control actions. Therefore, the security assessment is supported by processing the acquired measurements through state estimation. This process inputs a set of measurements that contains an unknown error, and returns an estimation of the network conditions at all nodes in the network that in combination with information about the physical system can estimate all static operating conditions. The process of state estimation can exploit a difference between the number of measurements and states to be estimated, defined as the degree of freedom expressing the observability of a system. With an observable system, where the number of measurements is greater than the number of states to be estimated, theoretical network relations are expressed to filter measurement noise and estimate network state variables, typically the nodal voltage magnitudes and angles [62].

Security assessment for transmission network application is well-known and supported by the characteristics of the cyber and the physical systems. For the former, the metering infrastructure has a broad coverage and is improving with the implementation of PMUs and the communicating infrastructure is reliable and dedicated. For the latter, a lower resistance over reactance (R/X) ratio of the transmission lines enables the simplification of calculations to Direct Current (DC) power flows where conductor resistance is neglected. Furthermore, a typically meshed network topology allows redirecting the current path in case of identified vulnerability from different investigated contingencies, and large generating units provides different control capabilities for adjusting power flows within the transmission network.

Distribution network security assessment

From a CPES perspective, however, the assessment of security in distribution network is challenged by the characteristics of both the cyber and the physical systems. Here, the inferior ICT infrastructure discussed in subsection 1.2.1 limits the information flow, and physical network topology and the conductor parameters increase the evaluation complexity. Specifically, the conductors in lower voltage networks generally have higher R/X ratios entailing the necessity to consider the conductor resistance and calculate the Alternating Current (AC) power flows rather than DC. Similarly, the radial topology at lower voltage levels of the distribution network means the failure of transmission lines or transformers will cause an interruption of the power supply in a part of the network [63].

As such, both the monitoring and contingency analysis phase of security assessment in distribution networks are challenging. For the contingency analysis challenge, distribution network vulnerability has entailed a research interest in resiliency, which is the system ability to restore operation following a disturbance that interrupt the supply of electricity. In [64], locating faults from multiple IEDs is studied for both transmission and distribution networks. Later, the concept of self-healing methods through Fault Detection, Isolation and Service Restoration (FDIR) methods was proposed for power system application in numerous ways as described by the comprehensive review in [65]. To utilize resiliency approaches however, it is necessary to observe network conditions through monitoring. Therefore, security assessment of distribution network relies on the monitoring ability, and due to the inferior ICT infrastructure of distribution networks, monitoring network conditions has proven a challenge, especially at the LV level. Current literature in distribution network

monitoring is in general split in two directions, planning ICT upgrades and the application of Distribution System State Estimation (DSSE).

Information and communication technology upgrades

The current deployment of smart meters is analyzed as an approach to improve distribution network monitoring through direct analysis of raw information in [66]. The results showed promising in monitoring the network conditions, but an analysis based on raw measurements neglects the inclusion of measurement and communication noise that implicates the information flow. Furthermore, such analysis does not allow representation of network conditions at nodes without metering equipment, and it ignores the possibility that GDPR can limit the knowledge about load point consumption from consumers who decide to restrict the utilization of consumption information due to data privacy concerns.

Besides direct utilization of smart meter deployment, current literature presents metering placement strategies that can upgrade distribution network ICT infrastructure [67, 68]. In [67], the authors propose a distribution of meters in secondary substations to monitor both sides of the MV /LV transformer, and the report in [68] describes the status of the Distribution Monitoring and Control (DM&C) program in Australia. Here 1090 distribution substations were fitted with sensors. While 19 of these substations had problems with insufficient data sets, the program enabled real-time monitoring of LV network feeder quantities, such as peak consumption and asset utilization. These approaches to improving distribution network monitoring, however, requires a considerable investment in ICT infrastructure when desiring an evaluation of all network operational conditions.

Current literature in ICT upgrades is mainly focused on supporting the implementation of DSSE improving observability and lowering uncertainty. A rule-based meter placement method is proposed in [69], which determines the suitable distribution of meters that can improve DSSE accuracy by supporting load forecasting. A probabilistic approach is proposed in [70], which consists of an iterative assessment of meter placements that can lower the DSSE estimation error. Also the implementation of synchrophasor metering technology in the distribution network is investigated for improving DSSE performance in [71]. While these methods can improve the observability of the DSSE state estimation model, the implementation and execution of DSSE is challenged by the characteristics of the CPES, especially at the LV network.

Distribution system state estimation

There exists numerous research efforts in DSSE including methods that handle the higher computational requirement compared to transmission level state estimation, by formulating the problem through current flows rather than power flows [72] and by using branch currents as state variables [73]. The branch current representation of state variables in DSSE is found superior in execution time when handling inclusion of PMU readings compared to the nodal voltage representation [74]. But so far, the deployment of PMUs in the distribution networks is very limited due to the relatively high costs. Instead, the inclusion of smart meter readings entails an equal number of nodal voltage and current readings. Such measurement distribution is studied in [75] comparing branch current and nodal voltages as state variables, and the results show similar execution times. Furthermore, the transforming power and voltage measurements into current equivalents, require careful evaluation of the transformation of the measurement variance.

According to recent work within the field, monitoring LV conditions has gained limited attention [76–79]. The distinction between MV and LV networks entail challenges since the LV network level has relatively higher R/X ratio, more severe and likely unbalanced conditions, and is less predictable load point interactions. With an increased focus on activating the distribution network through coordination of flexible resources that can alleviate congestion, increase the potential DER capacity, decrease power losses, etc., and on providing ancillary services for higher voltage level networks, entails a necessity of monitoring network conditions at LV networks in order to avoid hazardous control actions [80].

The advanced deployment of smart meters has been considered in proposing DSSE for LV networks. In [81], the authors propose an approach considering measurements from both smart meters and installed household PV systems. The study includes a demonstration using metering data from a small German LV feeder with PV integrated, and shows how the accuracy of the approach depends on the reliability of data acquisition. As part of the German smartSCADA project, the work in [82] presents a linearized DSSE approach using smart meter and PV information from a real LV feeder, and focus on the integration of a Bad Data Detection (BDD) method that detects, identifies and eliminates data with large measurement errors using the χ^2 test. The EU seventh framework program funded INTEGRIS project propose a decentralized monitoring, congestion management and fault management framework for distribution network integration [83]. The monitoring was tested through field trials of implementing a branch-current-based DSSE developed in [84]. The field results evaluates the ability to monitor power quality of the network with the support of DSSE [85]. True for all these studies, is that they were made in an offline environment through processing stored information and therefore does not consider the consequences of ICT infrastructure inadequacies.

The state estimator in the INTEGRIS project was, however, tested with an Real Time Digital Simulator (RTDS) using different measurement configurations in terms of reading frequencies and averaging times [86]. This study showed that reading frequencies and averaging times have a considerable impact on the estimation accuracy, especially when considering the integration of DG and the electrification of residential services such as transportation and heating. The use of a real-time simulation platform is likewise presented in [87], and used to investigate a platform for integrating DSSE in a LV network. Here the smart meter data is generated by an RTDS, gathered by a data concentrator, communicated and stored in a cloud storage, and used in a state estimator covering multiple LV feeders and executed on a control center computer connected to the cloud server. In addition, the data concentrators are assumed fitted with computational resources and execute DSSE for their respective domains. Although communication limitations between the data concentrators and the cloud server are investigated, the study neglects latency and reliability limitations in communication between smart meters and data concentrator.

There have been different demonstrations of integrating LV network monitoring through DSSE in an online environment where effects of ICT limitations are visible. The EU funded Ideal Grid for All (IDE4L) project implemented a smart metering infrastructure for LV monitoring and other applications, using a sampling window of 200 ms and 1 min broadcasting intervals. These settings were based on lessons learned from the INTEGRIS project, which shared multiple partners [78]. The key findings from the IDE4L project are presented in [47] and describe the revealed benefits from the secondary controller for congestion management and the fault location isolation separation and restoration technique capabilities, but also reports frequent monitoring problems due to unreliable

data acquisition as input to the state estimator. Similar experience were uncovered during the EU funded evolvDSO project that integrated a neural network based LV network DSSE algorithm [88]. The main issues with this approach were the limited and varying availability of information. This limited availability made training the artificial neural network complicated as it could potentially result in hazardous ignorance of changing conditions when trained with a biased, incomplete or erroneous set of input information.

The problem with information availability in distribution networks entails a need to utilize pseudo-measurements to obtain an observable system required for executing the DSSE. Definition of such pseudo-measurements has been proposed through artificial neural network establishment [89] and stochastic variables [90]. However, the use of pseudo-measurements is challenged by the complexity of determining appropriate weights in the state estimation [91]. With limited ICT communicating performance, some work try to adjust the weighting factor of measurements and pseudo-measurements to the time delay [92]. Here the weighting factor of smart meter readings is stated to depreciate with time in an attempt to account for the asynchronous acquisition of data collection in distribution network. The weight of the out-dated measurement is represented by the measurement device error and the short term load variation, the latter of which is expressed through an analysis of historical data to follow a normally distributed pattern at MV level. However, at the LV network, the irrational behaviour of consumers heavily affects the accuracy of such analysis.

The uncertainties entailed by inclusion of pseudo-measurements complicate the utilization of deterministic DSSE results as the integrity of these is difficult to determine. Alternative ways of presenting DSSE results, which include information on the expected uncertainty, are probabilistic and interval-based. In [93], a data driven forecasting of network conditions is proposed to feed pseudo-measurements to a DSSE algorithm. The forecasts are based on historic smart meter data and the DSSE results are given as a probabilistic range based on historic error distribution of forecast node contribution. While the proposed forecasting technique is tested using a simulation of a LV network, it is only investigated with balanced load conditions. An interval-based estimation is proposed in [94] for MV network DSSE considering uncertainty in network equipment parameters and measurements, where results are given as interval ranges of possible conditions.

With the activation of the distribution networks, management of DG controls is enabled, and increased volatility of network operation is expected. Such conditions entails possible network changes during DSSE execution, especially when considering the relative low processing performance of decentralized processing units. While the work presented in [95] propose an event-driven execution of DSSE through adapting the reporting rate of PMUs for more frequent estimation during operation close to security margins, it does not consider the computational burden of converging the DSSE algorithm.

In the CPES, the existing ICT infrastructure impedes the implementation of LV distribution network monitoring techniques, especially when considering the diversity of feeder cyber-physical characteristics. For LV network monitoring, it is necessary to consider the ICT infrastructure capabilities and performance, and to provide an estimation of network conditions during processing of network conditions. Approaches that acknowledge ICT limitations and consider the inherent challenges of CPES operation in terms of the quality and availability of information is missing for LV networks in existing literature, thereby limiting the capability to assess distribution network security.

1.2.3 Cyber-physical protection of DG controls

In the transmission network, active and reactive power controls are mainly shared by a few large centralized power plants, that are controlled by power plant SCADA systems and receives commands from the transmission network SCADA system. These control capabilities are characterized by their controllable energy sources and only depend on the physical restriction of the plant. Such capabilities of controlling active and reactive power injection at transmission system nodes are well suited for remedial actions identified from the transmission system security assessment process described in subsection 1.2.2, and therefore provides considerable protection against disturbances in the physical system. For distribution networks, the implementation of DG entails increasing active and reactive power control capabilities. These are, however, dependent on the operating conditions of both the cyber and the physical system.

Physical system impact on DG controls

The physical system characteristics of the distribution network, e.g. the topology as well as the size of DG units, limit the possible control actions that can change the operational conditions. In addition, the dependency of fluctuating RES's affects the active power control activation from DG within the distribution network. Besides the control restrictions, the integration of DG entails new challenges in operational security of the physical system, such as bi-directional power flows and voltage rise at feeder end-nodes [96]. These conditions means control of DG units must be carefully considered in order to avoid hazardous control actions that potentially violate physical system security constraints. As a consequence, grid codes require protection of DG controls through enabling autonomous behaviour designed to protect against voltage rise issues in radial distribution feeders, referred to as a local control strategy [97, 98].

As introduced in subsection 1.2.1, local control of DG units is enabled through the decentralization of processing capabilities, including the inherent processing capability of individual DG units referred to as distributed processing. The impact of such autonomous behaviour of DG units in distribution networks is investigated in prior work by [96, 99], and through a survey of German Distribution Network Operators (DNOs) in [100]. Such default control behaviour however, does not enable the DG units to participate in achieving optimal operating conditions, e.g. minimized active power losses. As a consequence, optimal setting of local control has been investigated in different works [101–103], where improvement of the network conditions during autonomous control is presented. The identification of such settings, however, requires supervision on a network level where an optimization of individual DG settings is coordinated to achieve an optimal objective of the entire feeder. The update of local control patterns is required when there are changes in the network operation, e.g. due to load changes and implementation of additional DG units. Furthermore, the local control strategy makes DG units unable to respond to system wide requests for specific control actions, such as those traditionally supplied by the central power plants.

Enabling optimal control of DG active and reactive power injection and the possibility to respond to system wide commands, require an acquisition and evaluation of network operating conditions, network specific processing of suitable controls of connected DG units, and a distribution and activation of control commands through active and reactive power set-points. Such DG controls is typically decentralized as its processing usually covers a sub-system and not the entire power system due to the amount of installed DG units. Therefore, such a control strategy is referred to as

decentralized, which is widely proposed in current literature [104–106]. The increasing share of renewable integration in the distribution network is considered by the authors in [104] that propose an optimization based regulation of the PV plant reactive power control for minimization of network losses and to minimize energy consumption through application of Conservative Voltage Reduction (CVR). A combined optimal dispatch of DG real and reactive power control is proposed in [106], and the work in [105] propose a multi-step optimization based on Model Predictive Control (MPC), where the targeted voltage profile is calculated based on network objectives. Here, the method assigns limits around the target values, outside which the MPC algorithm perform minimal corrective controls to push the voltage within the targeted operation region.

However, the decentralized DG control process entails a dependency on the performance and operation of the cyber system infrastructure due to the bi-directional flow, and necessary processing of information [107]. For network operators, the activation of the local or decentralized control strategies for DG active and reactive power injection, must therefore be done carefully to protect the network against harmful control actions and simultaneously ensure a secure supply of electricity. Coordinating between the local and decentralized control strategies has previously gained little attention in [108], where PV inverters are instructed with an optimal reactive power set point every 15 minute, within which they operate according to a local control strategy for voltage deviation reduction. While this methodology enables robust operation during physical system uncertainties, the impact of ICT infrastructure performance is not considered.

Cyber system impact on DG controls

Enabling decentralized controls must consider ICT performance and security impact as a mean of protection against cyber system disturbances that can cause harmful control activation. As a consequence of the increased interdependencies within the CPES, and following the events in Ukraine as well as recorded cyber-attacks in other sectors, a considerable interest in cyber-security for power systems has emerged. The vulnerabilities implied by concerns of cyber-security in the CPES have been investigated by several prior works, notably with the proposal of a layered vulnerability assessment of the SCADA systems infrastructure in [16], an investigation of cyber-security concerns in power system communication infrastructure in [17], and an extensive survey of cyber-security requirements and possible communication vulnerabilities in [18]. Furthermore, the standard Critical Infrastructure Protection (CIP) issues presented by North American Electric Reliability Corporation (NERC) describe the requirements for assessment of vulnerabilities of both cyber and physical domains of the power system infrastructure [109].

Such vulnerabilities are analyzed theoretically and empirically through the development of CPES testbeds as described with an extensive survey in [19]. With such testbeds, researchers can investigate the impact from different cyber-attacks as they can represent the interdependencies within the CPES. Till now, there has been a major effort within the research community to formulate attack models that represent the behaviour of possible adversaries and their ability to compromise information security [20, 21]. In [20], the authors model integrity and availability attacks and apply them to a chemical reactor system. The integrity attack models include scaling and min/max attacks, and these are tested on an automatic generation controller for power systems in [21] together with ramp, pulse and random attacks models. Modeling the impact of cyber-attacks is likewise explored for DG units that hold control capabilities. With the work in [22], the cyber security of a Wind Power Plant (WPP) SCADA system is investigated with inclusion of power system dynamics,

leading to an identification of its vulnerabilities. These vulnerabilities are tested by simulating cyber-attacks, which shows these can have major impact on power system operation. Inspired by this study, the authors in [23] performs a quantitative evaluation of a WPP SCADA system during cyber-attacks. The evaluation is based on an assessment of the mean time to compromise and repair, which are used to estimate the probabilities of successful cyber-attacks.

Illustrating the impact of cyber-attacks on DG unit controls reveals a need for detection of unauthorized access. The detection of intrusion can be done from an analysis of the ICT network performance and through observing the physical system operation. The former entails an investigation of known virus signatures, and monitoring system access attempts and data traffic statistics within the information flow to observe abnormalities, and the latter includes an analysis of the transferred information. Such data analysis based cyber error detection methods are proposed for distribution network equipment. The work in [24] propose a set of expert rules for defining normal operation, which are intended for protecting transformer tap controller. An approach for detecting abnormal conditions of PV plants is proposed in [25] through training and utilizing an artificial neural network. In addition, the application of state estimators with BDD to detect large data error has been proposed extensively in power system literature, including the application within wind turbine generators using detailed differential equations in [110], Kalman filtering in [111, 112], and an artificial neural network in [113].

Artificial intelligence based methods are inherently dependent on the quality of the training set, which entails a risk of biased response during unknown conditions. The implementation of Kalman filters for nonlinear systems is reported particularly challenging due to the requirement of detailed system and noise models [114, 115]. Finally, the integration of state estimators based on detailed differential equations describing the physical relations of a system entails substantial parameterization and computational requirements. Due to the diversity of DG and scale of the distribution network, such approaches are challenging using the existing ICT infrastructure.

With the decentralization of generation from implementation of DG units within the distribution network, and the entailed decentralization of control capabilities, CPES control depends in greater terms on the quality of DG controls at all levels of the distribution network. With both physical and cyber system affecting DG control performance, through changing power system composition, irrational household load profiles, and reliability and cyber-security concerns of the ICT infrastructure, it is necessary to protect the DG controls against CPES operational conditions. However, existing methods for DG unit cyber error detection are challenged by their complexity relative to the implementation in the limited ICT infrastructure. Furthermore, a study of the performance of DG control strategies in a CPES is necessary for the careful coordination between local and decentralized control strategies in network operator decision making.

1.3 Motivation

The tightening interdependencies between the cyber and physical domains of the power system reveals a transition towards a CPES where both domains must be considered for secure operation as introduced in section 1.1. Such transition entails handling information flow within the ICT infrastructure of both transmission and distribution networks, which increase the impact from information security concerns as acknowledged for CPS in [14] and for CPES in [15]. Such information security is defined by international standard *ISO/IEC 17799:2000* as *"... the preservation of information confidentiality, integrity and availability."* [116, p. 61], where each of the three components can be described as:

Confidentiality is the ability to keep the information secret from unauthorized persons and depends on the infrastructure ability to restrict the visibility of information to only authorized actors.

Integrity is the level of trust in the information transferred through the ICT infrastructure and is affected by the level of artifacts in the information flow from different sources, including background noise and manipulation from adversaries.

Availability is the ability to acquire and access information when demanded, such as the infrastructure capability of transferring information from one point to an other within the requested timing requirements.

Comparing the ICT categories in transmission and distribution described in subsection 1.2.1, from an information security perspective, reveals immediate differences. In terms of confidentiality, the GDPR limitations on smart meter data can label network operators as unauthorized, restricting the use of information. Since the Transmission System Operator (TSO) owns the PMUs and other metering devices integrated in the transmission system, they are able to govern the authorization of data handling. The communication media of transmission systems likewise offers a better data confidentiality due to the higher security of optic fibers and other dedicated wired media than wireless communication, which means it is less susceptible to unauthorized access.

The communication media used in distribution networks is in general less robust against noise than the transmission system counterpart meaning the information integrity is harder to maintain in distribution networks than in transmission networks. From an information availability perspective, the major difference in reporting rates of distribution and transmission metering devices, as well as the stricter reliability and latency requirements of the transmission system communicating infrastructure, leads to higher information availability in transmission networks.

While the transmission network ICT infrastructure has a larger potential impact in case of a hazardous event, due to the larger connected components and thereby a higher security risk [13], this comparison shows how the distribution network ICT infrastructure is far from the transmission network counterpart. Therefore, the information security challenges in distribution networks from the inferior ICT infrastructure entails challenges for distribution network monitoring, specifically for LV network monitoring and protection of DG controls in the CPES.

1.3.1 Focus of research

While existing literature discussed in section 1.2 has resulted in different research efforts within distribution network monitoring and DG control protection, there are open questions considering information security challenges for distribution networks. From these challenges, open research questions are identified and addressed as the contribution of this thesis, where the overall focus on distribution networks is used to scope the work as illustrated by the overview of the present thesis in Figure 1.1.

This thesis investigates CPES conditions and propose solutions that address information security related challenges to overcome in the area of LV network monitoring and protection of DG controls. These challenges are addressed while considering the limited metering, communicating and processing capabilities of the deployed ICT infrastructure of the distribution network. Four central research questions are hence formulated, which scope the general focus of the entire thesis as illustrated in Figure 1.1.

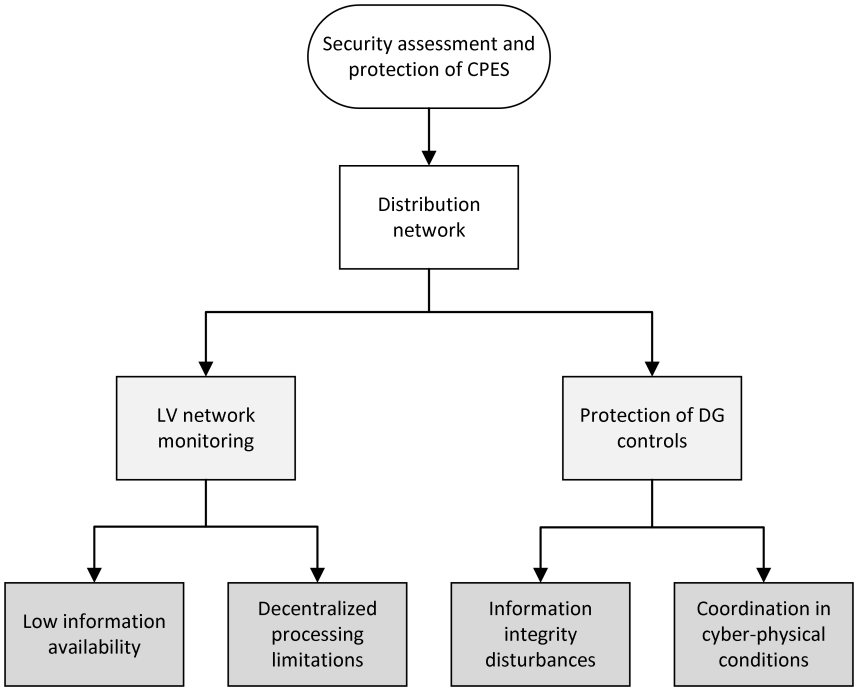


Figure 1.1: Overview of research focus

1.3.2 Central Research questions

The research work is as presented in Figure 1.1 separated in two parts, one for LV network monitoring, and one for protection of DG controls.

Low voltage network monitoring

Monitoring the LV network becomes increasingly importance as the number of DG units entails an increased risk of reverse power flow, and the electrification of services through DERs increase the potential peak loading. Furthermore without appropriate monitoring techniques, coordinating the control of these units is similar to driving while blind-folded.

- *Low information availability* is entailed by limited ICT infrastructure performance and data privacy restrictions. It impedes the LV network implementation of DSSE solutions from existing literature for condition monitoring:

  How can the operating conditions of LV network with low measurement availability be estimated while considering the limited performance of the ICT infrastructure?

- *Distributed processing limitations* can diminish the accuracy of estimated state variables due to the inherent volatility of DER operation and direct consumer behavioural impact on LV network conditions:

  With the existing ICT infrastructure, how can information availability and integrity issues be addressed while considering network monitoring during and in-between DSSE periodic execution?

Protection of DG controls

With the distribution of control capabilities, the reliability of DG control commands is increasingly important, and due to the CPES transition, the DG controls depend on the operating conditions of both the cyber and physical systems.

- *Information integrity disturbances* can be intended as cyber-attacks or unintended as deficits in the ICT infrastructure. Both types of disturbances have a potentially high impact on CPES operation with the decentralization of network control capabilities. Protecting DG against cyber errors, issues must consider the limitations of ICT infrastructure through appropriate representation of the physical system:

  How can information integrity of power plants composed of renewable DG be evaluated with existing limitations of ICT computational resources, and how can it be used to protect the DG controls from cyber system disturbances?

- *Control coordination in cyber-physical conditions* challenges network operator decision making to consider both domains while protection against hazardous control actions while harvesting benefits from network constrained optimization:

  How does CPES operation impact optimization of DG controls, and what CPES operational factors must be considered in control strategy decision making of a LV feeder?

1.4 Contribution

The contribution of this thesis to the literature on distribution network security assessment and protection in a CPES is presented through addressing the research questions identified in section 1.3 and illustrated in the bottom layer of the research overview in Figure 1.1. The contribution is separated between the four research questions as follows.

Enabling LV network monitoring of a feeder with low information availability is proposed through:

- *Development of a voltage interval estimation method considering low information availability:* The proposed method utilize feeder information and acquisition of three-phase voltage measurements from distributed meters within the feeder. Together with an estimation of worst-case branch currents, the range of possible node voltages are estimated using interval arithmetic.

Providing a means for LV network monitoring through DSSE application while acknowledging the limited processing power is proposed through:

- *Development of a bi-level estimation platform for periodic and event-driven execution:* The platform distinguish between periodic and event-driven measurement acquisition, performs DSSE in accordance to the periodic acquisition interval, and updates network condition intervals during and in-between DSSE execution through evaluating the impact of reported conditional changes.

Investigating the impact of and protection against information integrity disturbances on DG is considered by:

- *Applying functional modeling for wind turbine generator monitoring:* A functional model is established to represent a DG unit, in this work a wind turbine generator. From this model, key physical relations within the energy conversion process are identified.
- *Demonstration of cyber error detection system for DG control protection:* Identified key relations from the functional model of a wind turbine are used to establish a state estimation model, enabling the detection of cyber errors through physical system properties and relational equations. Through implementing the proposed error detection system in a distributed processing topology representing appropriate ICT infrastructure, it is evaluated as a bottom-up approach to protect the DG controls against information integrity issues in terms of computational speed and performance.

The performance and coordination of DG control in cyber-physical conditions is considered by:

- *Investigating DG control strategies in cyber-physical operating conditions:* The local and decentralized strategies used for DG controls are evaluated in different CPES operating conditions using a real-time power system simulation platform that includes an emulation of the metering, communicating, processing and controlling infrastructure and capabilities. Finally, simple guidelines are proposed for coordination between the local and decentralized strategies of a benchmark European Cigré LV network.

1.5 Thesis structure

This thesis is structured in four parts, 1) introduction, 2) low voltage network monitoring, 3) protection of DG controls, and 4) conclusion. The first part is used to introduce the content of the thesis and existing literature on LV network monitoring and protection of DG controls, the second and third part describes the methodology proposed in this thesis to extend state of the art in LV network monitoring and protection of DG controls, respectively, and the final part concludes. The four parts are composed of 7 chapters that have the following outline:

Chapter 1: Introduce the motivation and overall problem topic of this dissertation, leading to a discussion-based presentation of state of the art literature on security assessment and protection of CPES. From this discussion, the motivation behind the thesis work in LV network monitoring, as a key part of distribution network security assessment, and protection of DG control is emphasized through the formulation of four key research questions. The chapter ends with a presentation of the thesis contribution, structure and the list of publications prepared throughout the study.

Chapter 2: Presents an elaboration of the entailed information security challenges separated in terms of confidentiality, integrity and availability, followed by a description of existing methodology that address these security challenges in the context of LV network monitoring and protection of DG controls. The chapter ends with a formulation of high level research approaches for each of the four research questions considered in this thesis.

Chapter 3: Develops an approach to LV network monitoring through consideration of low measurement availability. Firstly, the CPES related shortcomings of the existing DSSE based approaches are discussed, followed by a detailed description of the proposed interval based voltage magnitude assessment method. The method is demonstrated and tested through simulation case studies of a Cigré LV benchmark feeder.

Chapter 4: Describes an innovative application of the well-known DSSE methodology as part of a bi-level processing platform for LV network monitoring. The details of both processors and their handling of event-driven and periodic measurements are then described, and finally the method is demonstrated using a LV feeder from the Bornholm distribution network, and its performance is evaluated for different degrees of information availability.

Chapter 5: Formulates a functional model of a wind turbine as a representation of the physical system and its internal relations, which serves as a basis for establishing a state estimation model that can be utilized on a distributed processing topology. This represents a bottom-up approach to cyber error detection of DG units in an effort to protect the DG controls. The cyber error detection system and its implementation on a distributed processor is described and evaluated in a stand-alone situation and as part of a WPP through simulation case studies.

Chapter 6: Investigates the CPES interdependencies impact on the performance of local and decentralized control strategies in a LV network case study with reactive power control of distributed PV plants. The chapter describes the layout, set-up and execution of a simple cyber-physical simulation platform which is used extensively in the evaluation of the two control strategies during perturbations in the physical system and disturbances in the cyber system. Finally, simple guidelines for control strategy coordination of a Cigré LV benchmark feeder are presented.

Chapter 7: Concludes the work conducted in this dissertation by addressing the formulated key research questions and discussing possible directions of further work building on the contribution from this thesis.

1.6 List of publications

The relevant publications formulated during the PhD project are the core of this thesis. In the following, they are separated in peer-reviewed journal articles in [**Pub. A**] to [**Pub. D**] and conference articles in [**Pub. E**] to [**Pub. F**]. The work in [**Pub. D**] describes an invention that is undergoing a patent application process. The invention has been presented to the patent and commercialization offices at DTU and has been through a novelty search conducted by external patent agents. The invention is given the internal DTU reference: 96276. At the time of writing, the invention is being evaluated internally for progressing the patent application process.

Journal articles

[**Pub. A**] **T.B. Rasmussen**, G. Yang, A.H. Nielsen, and Z.Y. Dong. Application of functional modeling for monitoring of WTG in cyber-physical environment. *IET Cyber-physical Systems: Theory and Applications*, 4(1):79-87, Mar 2019. DOI: 10.1049/iet-cps.2017.0109.

[**Pub. B**] **T.B. Rasmussen**, G. Yang, A.H. Nielsen, and Z.Y. Dong. Effects of centralized and local PV plant control for voltage regulation in LV feeder based on cyber-physical simulations. *Journal of Modern Power System and Clean Energy*, 6(5):979-991, Sept 2018. DOI: 10.1007/s40565-018-0445-x.

[**Pub. C**] **T.B. Rasmussen**, G. Yang, and A.H. Nielsen. Interval estimation of voltage magnitude in radial distribution feeder with minimal data acquisition requirements. *International Journal of Electric Power and Energy Systems*, 113:281-287, Dec 2019. DOI: .

[**Pub. D**] **T.B. Rasmussen**, and G. Yang. Distribution feeder bi-level interval estimation platform with periodic and event-driven data acquisition. (To be submitted).

Conference articles

[**Pub. E**] **T.B. Rasmussen**, G. Yang, A.H. Nielsen, and Z.Y. Dong. A review of cyber-physical energy system security assessment. In *IEEE Power and Energy Society PowerTech Conference*, Manchester, UK, June 2017. DOI: 10.1109/PTC.2017.7980942.

[**Pub. F**] **T.B. Rasmussen**, G. Yang, A.H. Nielsen, and Z.Y. Dong. Implementation of a simplified state estimator for wind turbine monitoring on an embedded system. In *Federated Conference on Computer Science and Information Systems*, Prague, Czech Republic, Sept 2017.

CHAPTER 2

Distribution network monitoring and DG control protection in CPES

This chapter elaborates the challenges identified in chapter 1 within security assessment and protection of CPES with focus on monitoring the LV level of the distribution network, and protection of DG controls. The elaboration is initiated with a description of the information security terminology introduced in section 1.3, i.e. confidentiality, integrity and availability. Next, considerations of information security issues in existing methodology on LV network monitoring and protection of DG control is described. This forms a base for formulating high level research approaches for each of the four considered research questions defined in subsection 1.3.2, scoping the necessary considerations for addressing each question from a CPES perspective. The chapter is based on content of the work described in **[Pub. A]**, **[Pub. B]**, **[Pub. C]**, **[Pub. D]**, **[Pub. E]**, and **[Pub. F]**.

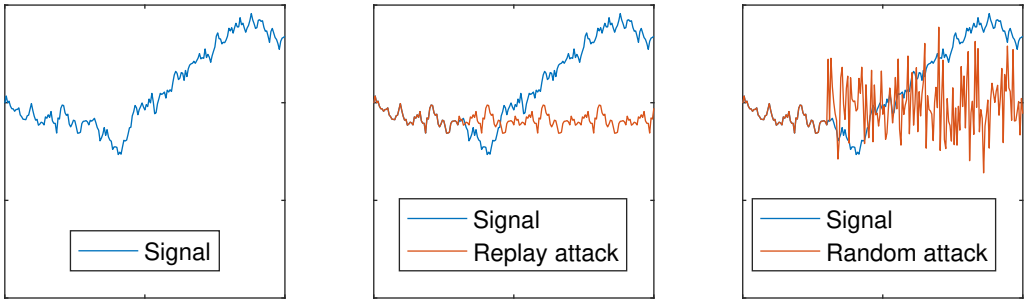
2.1 Information security challenges

In the distribution network, the tight interdependency between the cyber and physical systems, the ICT resource limitations, and the growing data privacy concerns, entail different challenges for monitoring the network conditions and for protecting DG controls. One of the key threats to information security is the distortion of information flow due to manipulation from adversaries. An illustration of such cyber attacks is presented in Figure 2.1, where the measured signal in Figure 2.1a is subject to different attack patterns in Figure 2.1b to Figure 2.1f, compromising confidentiality, integrity and availability.

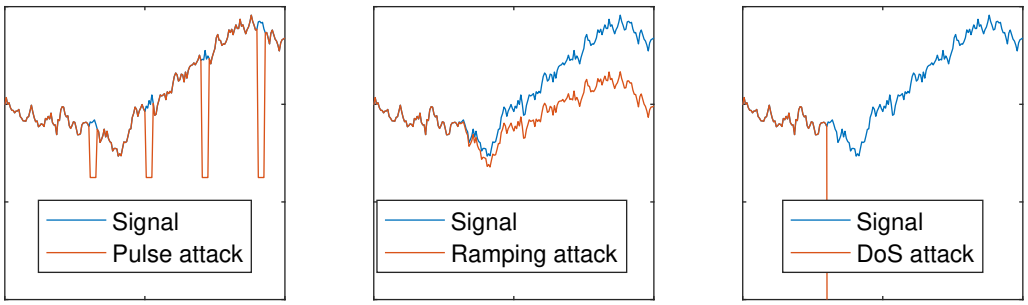
2.1.1 Confidentiality concerns

As a result of growing data privacy concerns, the EU introduced the GDPR on the 27th of April 2016 which was activated on the 25th of May 2018. The data protection regulation was formulated to harmonize the data handling and thereby give more rights of consent to the data owners and better transparency in data utilization [49]. In the context of power systems, this regulation potentially limits the use of residential electricity consumption data for network operators, which is assumed available in a wide variety of existing work for approaches in; network monitoring [81–83, 87, 88, 92], forecasting [117–119], demand-side management [120], and appliance recognition [121, 122].

Additional concerns of information confidentiality in distribution networks are observed in the communicating infrastructure. Here there are concerns of adversaries being able to eavesdrop on the information flow [12, 22, 123]. While the impact of such eavesdropping attacks is not immediate,



(a) Arbitrary measurement signal (b) Signal subject to replay attack (c) Signal subject to random attack



(d) Signal subject to pulse attack (e) Signal subject to ramping attack (f) Signal subject to DoS attack

Figure 2.1: Arbitrary measurement signal subject to confidentiality, integrity and availability attacks

the attackers breach data privacy rules and can potentially utilize the collected information to learn about the physical system characteristics. Such knowledge can be used to perform replay attacks, where the information flow from a sensor is replaced by a previously recorded sequence [26] as illustrated in Figure 2.1b.

Besides replay attacks, a knowledgeable attacker can bypass security measures through exploiting their limitations as in [27], where a power system state estimator is compromised by an attacker who knows the system configuration and have the ability to manipulate a portion of the metering infrastructure. Additionally, the work in [28] investigates the ability of an adversary to corrupt the CPES without being detected through utilizing different degrees of network knowledge.

2.1.2 Integrity issues

Cyber-attacks that manipulate the information from sensors are considered as one of the major integrity issues of the CPES. Such attacks are studied in numerous existing works with focus on control systems [20, 21], SCADA systems [29] and electricity markets [30] among others, from which specific false data injection strategies are revealed as shown in Figure 2.1c to Figure 2.1e. In addition to the false data injection risk, the ICT infrastructure deficits pose a challenge for network operators. Here, accuracy limitations of metering devices, and potential noise in communication from physical obstacles and electromagnetic interference can entail integrity issues. Such limitations

can distort the information flow through single or consecutive occurrences of measurement error with different amplitudes.

Whether from manipulation of adversaries or due to ICT infrastructure performance, the information integrity issues can cause problems for network operators in both monitoring and control of the power system assets. Artifacts in measurements can, if not being treated properly, cause a distorted image of network operation. Furthermore, the utilization of physical system observations in control strategies can cause harmful operation if the interpreted network conditions are different from reality.

2.1.3 Availability limitations

Information availability is primarily offered through the deployment and connection of sensors, but their distribution entails limitations that must be considered. Implementing sensors in diverse environments may lead to failure of a portion of these, simultaneously, the information flow from the sensors to an acquisition unit can be impeded by the reliability of communication infrastructure. Such communication channel congestion can happen in media that is improperly designed and therefore is unable to handle the requested data rates, or if the media is used for other types of data communication. Exploitation of the latter through so-called Denial of Service (DoS) attacks can limit the availability of measurement acquisition [31, 124], as illustrated in Figure 2.1f.

Besides the risk of failure, the configuration and confidentiality of metering resources can affect the availability of measurements. The internal clock of low-cost sensors is calibrated during installation or continuously through connection to a Network Time Protocol (NTP) server, but infrequent calibration could potentially cause time displacement in measurement acquisition [125]. The availability of information from meters is further limited by their configured measurement and broadcast time resolutions. Such configuration is based on the utilization of the readings and limitations of the communicating and processing infrastructure. Furthermore, for smart meters and other sensors that register information about the behaviour of people, restrictions from data privacy legislation through GDPR can limit availability. This can restrict utilization of information to quantities that are shared by multiple actors and therefore prevails anonymity of the individuals. For monitoring of network conditions through information processing, all these availability limitations pose a challenge since existing methodology to a large extend requires complete data sets in order to converge.

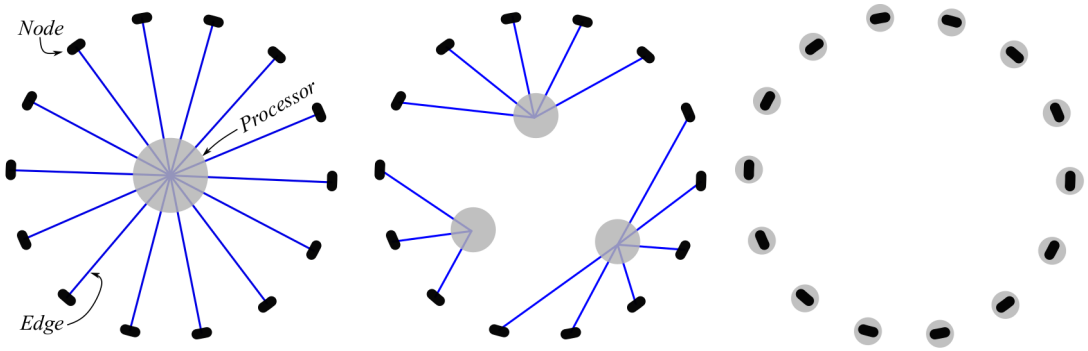
2.2 Information security in existing theory on LV network monitoring and protection of DG controls

With the importance of information security in ensuring the operation of the CPES, existing work for detecting and solving issues with confidentiality, integrity and availability is proposed through analysis of the cyber system. Such analysis is proposed through the development and implementation of Intrusion Detection Systems (IDS's), which are characterized by their detection technique being signature, anomaly, or specification-based [32].

The signature-based IDS is instructed to evaluate the flow of information for comparison to predefined behaviour patterns that have previously been identified as harmful, this could be a specific sequence of bytes or a sequence of specific commands. Such detection techniques relies on frequent updates of the signature database, but since it only react to the recognition of suspicious patterns, it infrequently reports false alarms of intrusion.

Both anomaly and specification-based IDS's are in contrast implemented with the aim of detecting unknown attacks. These techniques are performed through analysis of the information flow and an evaluation of whether it is normal. The distinction between anomaly and specification-based IDS's is in the perception of normal, where the former pattern recognition is based on historical data, through machine-learning or similar algorithms, and the latter is from specified healthy conditions based on an analysis of the system by an expert in the field.

An alternative to cyber network IDS's for addressing information security challenges is by processing the acquired information. Such analysis enables utilization of physical system domain knowledge to detect cyber system error, and can be done through centralized, decentralized, and distributed processing techniques as illustrated in Figure 2.2, where the ring of nodes in each sub figure, represent an entire system.



(a) Centralized (b) Decentralized (c) Distributed

Figure 2.2: Centralized, decentralized, and distributed processing topology

In the processing topology illustrations in Figure 2.2, the blue edges are used to represent communicating infrastructure, the black nodes illustrate metering infrastructure, and the grey circles represents processing resources. The centralized processing network topology in Figure 2.2a is typically used for transmission system analysis. Here a central processing unit is utilized to evaluate the information being transferred from all network sensors as illustrated by the central processor in Figure 2.2a. For processing the information flow for an entire distribution network, a

centralized topology is considered infeasible due to its scale and number of components, hence, the processing requirements are too extensive for such techniques [58].

More suitable processing for distribution networks is the decentralized topology in Figure 2.2b and the distributed topology in Figure 2.2c. The former topology is used to separate the widespread distribution network into smaller sub-systems in which information from sensors is acquired by the area specific processing unit performing the necessary calculations with its individual objective. This way, each of the areas operate independently and due to the network decomposition, the entailed computational requirements are lowered. The latter topology, distributed processing, serves a desire for distributed information acquisition and processing made in accordance to predefined objectives, meaning the multiple processing units are able to perform individual computational tasks locally.

The independence from communicating infrastructure performance and the low computational requirements entailed by the narrow area of responsibility of the distributed topology, are key advantages for this solution, however, their coordination is limited since the processing infrastructure is used to analyze primarily local information flows. Therefore, the distributed processing topology entails limited overview a system as a whole. Such an overview picture is obtainable through the centralized and decentralized processing topology, which improves the possible coordinated activation of network assets.

From a practical perspective, the distribution of processing in the CPES offers a strength in numbers compared to the decentralized processing topology. This is obvious as the failure of the single decentralized processor will have a larger impact than failure of a single distributed processor, as its area of responsibility is larger by definition. Furthermore, the changing CPES composition, whether through addition or removal of appliances, maintenance of physical and cyber assets, or equipment failure, can impact the accuracy of the decentralized processor as its system representation diverges from reality in such conditions [126].

2.2.1 Low voltage network monitoring

The utilization of decentralized processing shown in Figure 2.2b for information security in LV network is proposed through application of DSSE. Such application is intended for handling information integrity issues through exploiting known physical relations of quantities in a system. This is possible when the network is considered observable, which is when the number of measurements N_m is larger than the number of states N_x. Besides the ability to reduce measurement error, the state estimation process enables an estimation of unmeasured quantities.

The process of state estimation is built around the nonlinear measurement model in (2.1), where the set of measurements $\mathbf{z}$, is defined as a sum of nonlinear state equations $\mathbf{h}(\mathbf{x})$ that are expressions of the state variables in $\mathbf{x}$, and the relative measurement error set $\mathbf{e}$.

$$\mathbf{z} = \mathbf{h}\left(\mathbf{x}\right) + \mathbf{e} \tag{2.1}$$

For distribution network application the state variables $\mathbf{x}$ are typically expressed by either complex node voltages V or complex branch currents I of a network. Considering the node voltage representation, the state variable vector $\mathbf{x}$ contains the voltage angle δ_n and magnitude $|V_n|$ for each node n. Usually, the voltage angle of one of the network nodes is assumed equal to $0°$

as a reference for the rest of the network. In transmission and distribution networks, common measured quantities include voltage magnitudes as well as active and reactive power readings. To remove measurement noise from these, state equations $h_m(\mathbf{x})$ are formulated based on the physical relations between measurement m and state variables $\mathbf{x}$. For voltage magnitude readings, the specific measurement is simply set equal to the corresponding state variable. For active and reactive power readings, the expression is more complicated as it is based on the power injection of the measured power system node n and the flow of power between it and other network nodes [see Appendix A].

With the higher R/X ratio in distribution networks compared to the transmission level due to smaller conductor cross sectional area, both the resistance and reactance have considerable impact on the power flow calculation representing the active and reactive power measurements in the state estimation model. In addition, the operation of the distribution network, especially at the LV network, is likely to operate with unbalanced phases. This means that a single line representation of the network conductors can be inaccurate for LV networks.

Three-phase DSSE model

A three-phase state estimation model is described in work presented in the late 20$^{\text{th}}$ century in [72, 127, 128]. Here the starting point is to convert the state variables to a three-phase representation. Such representation triples the number of state variables and thereby increases the computational requirements. To align power injection measurements in the three-phase DSSE, the active and reactive power flow equations must be converted to a three-phase representation as well. This conversion requires an expansion of the admittance matrix Y through definition of the self and mutual admittance of each line segment.

To accommodate the likelihood of unbalanced load points in the LV network, the three-phase line segments are installed with a parallel neutral wire. With relatively low neutral wire impedance, the potential of the neutral point is kept close to zero as it is grounded at different distribution network nodes. Due to a non-zero current flow in the neutral wire during unbalanced load connections, the neutral wire is usually relevant in LV network analysis and most work considers the neutral wire through a three-phase presentation of the four wire system. Such consideration is enabled through different methodologies, including the Kron reduction method that assumes zero potential at both ends of the line segment [see Appendix A.1]. While such assumption distort the neutral wire contribution it has been used extensively as a simplification of the power flow calculation in existing literature [72, 127–129].

The Kron reduction method represents the admittance $\mathbf{Y}_l$ of each line l as a three by three matrix. A polar decomposition of each element in $\mathbf{Y}_l$ can then be utilized to express the three phase active and reactive power injection P_n^p and Q_n^p per node n and phase p as shown in (2.2) and (2.3), respectively.

$$P_n^p = |V_n^p| \sum_{k=1}^{N_n} \sum_{j=1}^{3} |Y_{nk}^{pj}||V_k^j| cos\left(\delta_n^p - \delta_k^j - \gamma_{nk}^{pj}\right) \tag{2.2}$$

$$Q_n^p = |V_n^p| \sum_{k=1}^{N_n} \sum_{j=1}^{3} |Y_{nk}^{pj}||V_k^j| sin\left(\delta_n^p - \delta_k^j - \gamma_{nk}^{pj}\right) \tag{2.3}$$

where the nested summation from $j = 1$ to $j = 3$ represents the consideration of each of the three power system phases one by one, and N_n is the number of nodes within a network. With

the defined state variables through complex node voltages, description of typical power system measurements i.e. voltage magnitudes, and active and reactive power injection, and a formulation of expressions relating the state variables to the state equations, the DSSE model can be solved through estimation of the state variables.

State variable estimation

The process of state estimation considers the error in measurements and network observability through application of a statistical criterion that returns the optimal state variable values in accordance to the criterion objective. One of the most frequently utilized criteria is the Weighted Least-Squares (WLS), where the state variables are estimated through minimization of the sum of weighted square residuals between the measured quantities $\mathbf{z}$ and the corresponding estimated value $\mathbf{h}(\mathbf{x})$. Through assumed normal distribution of measurement error for all measurements $m \in N_m$ with zero mean μ_m and standard deviation σ_m, the best estimates of the states can be found through solving (2.4).

$$\min_{\mathbf{x}} J_{sum} = \sum_{m=1}^{N_m} \frac{\left[z_m - h_m\left(\mathbf{x}\right)\right]^2}{\sigma_m^2} \tag{2.4}$$

where J_{sum} represent the objective value, i.e. the sum of weighted square residuals $J\left(\mathbf{x}\right)$. The non-linearity of the state equations in (2.2) and (2.3) means the WLS criterion in (2.4) cannot be solved directly, hence an iterative algorithm is necessary. Fortunately, existing literature propose different approaches for calculating the sum of residual and making it converge below a threshold, through multiple iterations, where one of the common methods for solving non-linear problems is the Newton method [see Appendix B.1].

To estimate the state variables in the DSSE for removing measurement error and thereby ensuring the information integrity, the DSSE input measurement set must represent an observable system. With the information confidentiality and availability concerns discussed in section 2.1, such representation is challenged.

Distribution network measurement availability

Availability limitations are typically handled in DSSE through integration of pseudo measurement. These measurements can represent known quantities, such as zero injection nodes, and estimated operation of equipment connected throughout the network, such as wind farm production based on forecasts of wind speeds, or load point estimation from historic data.

At the LV level of the distribution network, the accuracy of estimated non-zero power injections is limited due to the information confidentiality concerns and irrational user behaviour. In existing work, there have been different attempts to forecast individual load point power injection based on historical data analysis [118, 130, 131]. These works however assume availability of historical data of household consumption, which might violate the information confidentiality concerns, especially with the introduction of the GDPR. Furthermore, the accuracy of these estimates relies on unchanged residential equipment and cannot be used for transparency between diverse residential load points.

While shared parameters, such as solar irradiance, wind speed, temperature, and network voltage, could potentially be utilized to estimate the operation of network equipment that depend on these

quantities, such as PV plants and other DERs, the information availability limitations heavily impede the implementation of existing techniques for improving the LV distribution network monitoring capabilities.

2.2.2 Protection of the DG controls

Utilization of DG control is based on an assessment of appropriate control actions through processing information flow. Such information can include both power system specific quantities, such as voltage and current magnitudes, and parameters from neighbouring energy systems that affect the DG unit, such as how the weather conditions affect the operation PV plants and wind turbines. This information can be processed through a centralized, decentralized, or distributed computing topology, illustrated in Figure 2.2, but with the increasing integration of DG, the application of a fully centralized processing of information from all such units illustrated in Figure 2.2a, would require substantial computational resources.

Through the application of distributed information processing highlighted in Figure 2.2c however, the DG units can be specified to autonomously follow certain instructions. Such control settings are defined in various grid codes [98] and referred to as local control strategies because the metering, processing and controlling activities are all executed at the DG unit without utilization of the information communicating infrastructure. Two power system related properties that are considered when discussing DG controls are the active and reactive power interaction with the electricity infrastructure. In distribution networks, due to the higher R/X ratio than in transmission systems, the effects of both control parameters have an effect on the voltage magnitude across conductors. This principle can be derived from studying a simple two bus system with an external grid connected to one end, and a load connected to the opposite end as in [96] where the direction of the current I is from the external grid to the load. The drop in voltage magnitude $|\Delta V|$ across a line with impedance $Z = R + jX$, is expressed in (2.5) to (2.7) by the voltage at the load connection node V_L, and the active and reactive power consumption at that node P_L and Q_L, respectively.

$$\Delta V = I\left(R + jX\right) \tag{2.5}$$

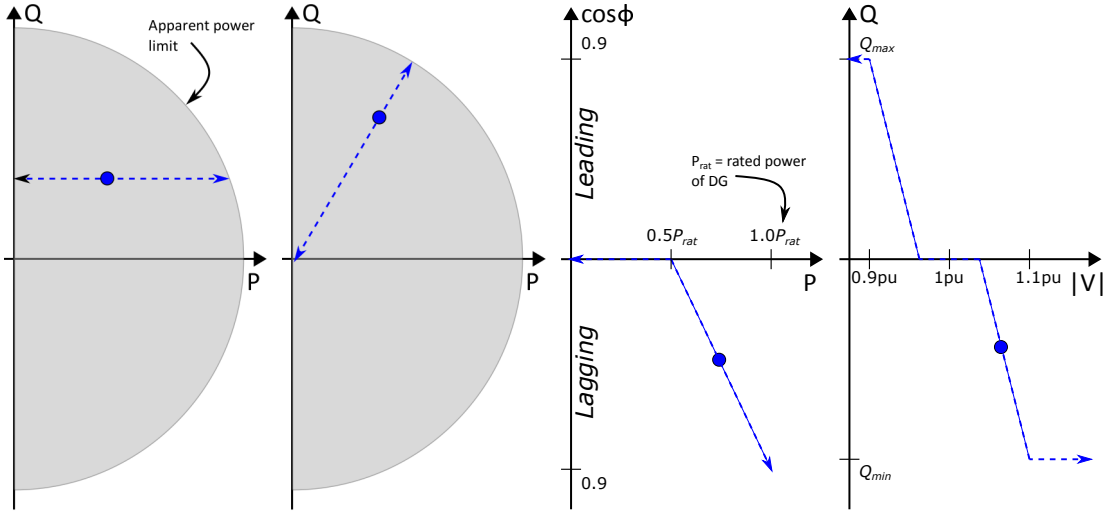
$$= \left(\frac{P_L + jQ_L}{V_L}\right)^* \left(R + jX\right) \tag{2.6}$$

$$= \frac{P_L R + Q_L X}{V_L} + j\frac{P_L X - Q_L R}{V_L} \tag{2.7}$$

With DG integrated at the load point, the active power consumption P_L can be either positive or negative since the flow of generated power is in the opposite direction of the network convention. While the only form of active power control of DG units is curtailment of generation due to the dependency on an uncontrollable RES, the reactive power Q_L can be configured to inject or absorb reactive current and thereby control the voltage drop ΔV. This is of particular importance when considering the risk of over-voltage due to the reverse power flow as can be seen if the reactive power is kept zero in (2.7).

Local control strategies of DG units

For local control of reactive power through distributed processing as illustrated in Figure 2.2c, there are four major control strategies; 1) constant Q, 2) constant power factor, $cos\phi$, 3) power factor as a function of active power generation, $cos\phi(P)$, and 4) reactive power as a function of terminal voltage magnitude, $Q(|V|)$. These four typical control options are illustrated in Figure 2.3 from a generator perspective meaning a positive value represents power generation and lagging power factor means inductive behaviour.



(a) Constant Q (b) Constant $cos\phi$ (c) $cos\phi(P)$ (d) $Q(|V|)$

Figure 2.3: Local reactive power control strategies with distributed processing illustrated with a blue dot, as an arbitrary operating point, and a blue line on which the operating point can move

The four control strategies in Figure 2.3 can be separated in two that only require operational set point instructions, i.e. constant Q and constant $cos\phi$ controls in Figure 2.3a and Figure 2.3b, respectively, and two which requires operational pattern instructions, i.e. $cos\phi(P)$ and $Q(|V|)$ in Figure 2.3c and Figure 2.3d, respectively. From a CPES protection perspective, the limited flow of information in these local control strategies means information security challenges in the metering, and processing is limited to the individual units. Furthermore, the presence of measurement error has limited impact as the local controls are based on a consecutive distributed processing of information and update of control actions. However, the limitations of distributed processing equipment and its fit-and-forget implementation entail a necessity for robust computation of control actions, especially when considering the limited performance of metering and communicating infrastructure. If not considered, the depending equipment can, as a result, receive hazardous commands or ignore changing network conditions. Although errors in the set point and pattern instructions could have substantial hazardous impact, the distributed processing topology in Figure 2.2c only considers initial compliance and therefore performs no coordination during operation.

While the local control strategies in Figure 2.3 entail built-in CPES protection, the non-coordinated control actions limit the ability to achieve a common operational objective, e.g. minimizing the power transfer losses or the amount of reactive power through the secondary transformer. As an alternative, optimization based strategies for coordinating control actions of multiple DG units through a decentralized processing topology as shown in Figure 2.2b can be applied, where

optimal power injection set points are estimated and communicated to each participating DG unit on a periodic basis. For DG control coordination, information about network configuration and operation is utilized to formulate a mathematical model. This model is composed of an objective function representing the common goal to achieve, and a set of constraints representing the physical network limitations.

Decentralized control strategy for DG units

Typical objectives of decentralized control strategies for DG units within a sub-system include; 1) minimization of active power losses within the network as a mean of reducing operational costs, and 2) minimization of voltage magnitude deviation from reference values as a way of limiting the impact of DG volatility in cases where the control set points are updated with low frequency. For both objectives, the considered control variables are limited to the active and reactive power interaction of DG units when assuming no ability to reconfigure the network topology or switching operation of equipment such as tap-changing transformers and FACTS devices. Therefore, the objective function of the former and latter objectives can be described through typical expressions in (2.8) and (2.9), respectively.

$$\min_{(P_n^{gen},Q_n^{gen})\forall n\in N_n} f_{obj} = \sum_{n=1}^{N_n} P_n^{gen} - P_n^{load} \tag{2.8}$$

$$\min_{(P_n^{gen},Q_n^{gen})\forall n\in N_n} f_{obj} = \sum_{n=1}^{N_n} \|V_n^{ref} - |V_n|\|_2 \tag{2.9}$$

where the objective value f_{obj} in (2.8) is based on a minimization of the imbalance between active power generated or imported from external sources, and the power consumed within the network, which evidently results in a active power loss minimization. The alternative objective in (2.9) of minimizing voltage deviation from its reference value V_n^{ref}, is based on a minimization of the Euclidean norm of that deviation. To ensure load demand is satisfied and the supply of electricity satisfy equipment limitations and comply with operational standards, the objective function is subject to a set of constraints in (2.10) to (2.15).

$$P_n^{gen} - P_n^{load} = |V_n| \sum_{k=1}^{N_n} |Y_n k||V_k| cos\left(\delta_n - \delta_k - \gamma_{nk}\right) \quad \forall_{n\in N_n} \tag{2.10}$$

$$Q_n^{gen} - Q_n^{load} = |V_n| \sum_{k=1}^{N_n} |Y_n k||V_k| sin\left(\delta_n - \delta_k - \gamma_{nk}\right) \quad \forall_{n\in N_n} \tag{2.11}$$

$$\left|\frac{V_k - V_n}{Z_{nk}}\right| \leq I_{nk}^{max} \quad \forall_{n\in N_n \wedge k\in N_n} \tag{2.12}$$

$$P_n^{min} \leq P_n^{gen} \leq P_n^{max} \quad \forall_{n\in N_n} \tag{2.13}$$

$$Q_n^{min} \leq Q_n^{gen} \leq Q_n^{max} \quad \forall_{n\in N_n} \tag{2.14}$$

$$V^{min} \leq |V_n| \leq V^{max} \quad \forall_{n\in N_n} \tag{2.15}$$

where the first two constraints (2.10) and (2.11) ensures correct power flow calculation and supply of demanded consumption. In distribution network the conductor current limit I^{max} is restricted

by the thermal limitation as represented in (2.12). For this constraint, only nodes n and k connected by a line with impedance Z_{nk} are considered. As control variables, some studies considers the possibility of active power curtailment while others restrict the control to the reactive power interaction. Either study can be applied using the boundary constraints in (2.13) and (2.14). Here the maximum and minimum limits follow the operational conditions and can be adjusted to ensure compliance with study specific restrictions. The last constraint is to ensure voltage magnitude compliance for all node points, in most cases considered as the rated voltage $\pm 10\%$. The accuracy of the resulting optimal solution can be enhanced by further inclusion of additional constraints such as short circuit current requirements, transformer reactive power flow limits, etc.

Solving the mathematical model presented above returns the optimal solution of DG active and reactive power injection according to the chosen objective function. Such set of DG control actions must be communicated from the decentralized processor to the DG units as illustrated in Figure 2.2b. Therefore, the performance of the decentralized control strategy depends on the ICT infrastructure ability to ensure the information security of the bi-directional flow of information. From a security perspectives, the decentralization of processing task already offer some protection since a compromise will not affect the entire distribution network but only the area of the compromised processor as illustrated in Figure 2.2b [132]. Furthermore, the ability to switch the operation of DG units to follow local control strategies offers additional protection against cyber related disturbances. Therefore, careful considerations of CPES operation must be taken when deciding the coordination between local or decentralized control strategies.

Cyber error detection

Beside the protection against cyber errors in the ICT infrastructure offered through choosing a local control of DG active and reactive power injection, more active measures of protecting against cyber error through detection can be helpful as introduced in the beginning of section 2.2. Such detection is especially valuable when considering the active participation of DG units in providing control actions for the entire CPES through centralized or decentralized control commands. The impact of hazardous control actions of DG due to cyber errors can be relatively high, especially when considering an aggregation of multiple DG units connected to the distribution network as part of a WPP or a large scale PV plant. While the latter can be connected through a common inverter at the point of connection, wind turbines in a WPP are distributed across a geographical area and connected to the power system through a collector system. The higher capacity and thereby higher control capabilities, means the information security challenges can have substantial impact on the CPES operation.

The control of wind turbines in a WPP can be handled by a plant controller to ensure higher level commands are satisfied at the point of connection to the power system. Such control requires decentralized processing of information from within the collector grid as shown in Figure 2.2b, hence the information security conditions must be considered. In particular, the integrity of information is important as a distorted overview of operational conditions can cause unintended control actions.

Addressing the integrity issue is proposed through establishing state estimation models for application in distribution network monitoring [58, 113]. The formulation of such models are based on an analysis of the system under investigation and can correlate different power system and neighbouring energy system related measurements with defined state variables, and thereby

limit the impact of small measurement error in the accuracy of estimated states. The occurrence of bad data in monitoring systems can be because of malfunctioning metering infrastructure, faulty communicating infrastructure, or as discussed in section 2.1 from the hazardous actions of adversaries.

Information error is categorized in three groups by the work in [133], based on the error magnitude compared to the data sheet specific standard deviation σ of the metering device as illustrated with the Probability Density Function (PDF) in Figure 2.4. Normal measurement error is expected to have a magnitude of up to 5σ, gross measurement error is between 5 to 20 times the standard deviation, and extreme measurement error is described to be above 20σ.

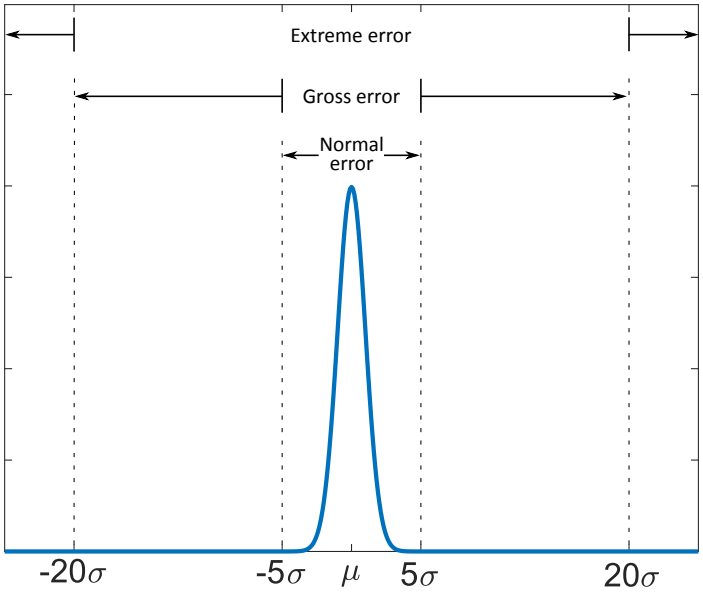


Figure 2.4: Illustrated PDF with mean μ and standard deviation σ representing a metering device accuracy and characterize normal, gross, and extreme error

The existence of normal, gross and extreme measurement error can be devastating for coordinating DG controls that rely on the cyber system information security. Hence, techniques for bad data detection, identification and elimination exists. Mili, Van Cutsem and Ribbens-Pavella defined the task of BDD, in the context of state estimation, as *"... to guarantee the reliability of the data base generated through the estimator."* [134, p. 3037]. In existing literature, multiple approaches were proposed [134–137] in the second half of the 20$^{\text{th}}$ century, with the J_{sum} test proposed in [135] still considered a useful method [62].

The J_{sum} method is based on an assumption that the weighted sum of square residuals, presented as J_{sum} in (2.4), follow a chi-square distribution, χ^2 as shown in Figure 2.5, with four examples of degree of freedom, ν, equal to the number of measurements N_m minus the number of state variables N_x.

The J_{sum} test is done through evaluating whether the residual J_{sum} follow a χ^2 distribution or not. Such evaluation is performed through determination of a threshold value K that indicates the presence of bad data if the residual value is larger than the $(1-\alpha)$-quantile of the χ^2 distribution, as illustrated by the colored area beneath the PDF curves in Figure 2.5. The quantity α indicates the trade-off between false positives and negatives in BDD and is usually chosen between 1 and 10%, and is used together with the degree of freedom in calculating the threshold K through (2.16).

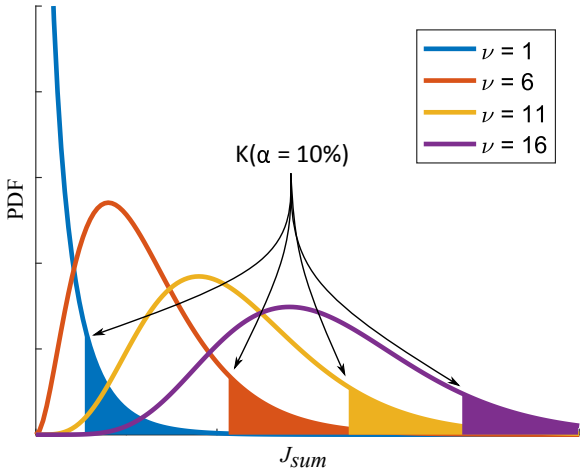


Figure 2.5: Probability density function of χ^2 distribution for four different degree of freedom settings ν, with the colored area beneath each curve representing the area in which the J_{sum} test detects bad data as configured by the false positive and negative trade-off coefficient $\alpha = 10\%$

$$K = \chi^2_{\nu,1-\alpha} \tag{2.16}$$

With the presented J_{sum} test, the results of the state estimation process are scanned for bad data. If such occurrences are detected, the specific measurement containing bad data is identified. Such process could be done through sorting each measurement residual with respect to the estimated quantity, in a descending order and assuming the measurement with highest residual is the bad data. Following such process, the bad data is eliminated through complete removal of the measurement point in the next estimator iteration, or through replacing the identified bad data with historical information, the estimated result or alternative options. Considering the technique of bad data detection, identification and elimination, such effort relies on the quality of the state estimation model of the physical system.

2.3 Research approach formulation

As described in the literature review and motivation behind the research focus on security assessment and protection of CPES for distribution networks in chapter 1, available methodology for LV network monitoring and protection of DG controls do not fully recognize information confidentiality, integrity, and availability concerns. Such challenge is emphasized by the elaborate description of information security and its impact in the distribution network in section 2.1, and through the discussion of existing methodology in section 2.2 around the identified research areas considered in this work, i.e. LV network monitoring and protection of DG control in the CPES. From the presentation on existing theory in DSSE, DG control strategies, and cyber error detection approaches in section 2.2, high level research approaches are formulated for each of the identified research questions of this dissertation presented in Figure 1.1. These approaches form a base for the studies conducted and methods proposed in the remainder of the thesis.

2.3.1 Low voltage network monitoring with low information availability

In the CPES, where consumers with data privacy concerns can limit the availability of measurements, and limited metering and communicating infrastructure performance entails information integrity issues as described in section 2.1, LV network monitoring solutions must consider several factors:

- If all consumers in a LV network decide to make consumption data unavailable for the utility company, the network monitoring methodology must consider only shared measurements in the input data set as these do not reveal individual user behaviour.
- Chances of asynchronous smart meter data acquisition, due to drifting of the internal clock, communication congestion or other circumstances, means the assessment of operational network conditions should be executable with limited information availability.
- The limited measurement availability, in terms of timing and processable quantities, affects the utilization of exiting DSSE based methods for LV network monitoring, alternative approaches should acknowledge and overcome such challenges.
- The information about topology, connected consumers, and other grid parameters, available to the network operator, could be utilized to gain a feeder wide overview of network conditions from individual node measurements.
- Since the integrity of the distributed meters is affected by communication noise and meter inaccuracy, a proposed solution must be able to report the expected uncertainty of resulting quantities.

2.3.2 Low voltage network monitoring with decentralized processing limitations

If only a portion of the LV feeder connected consumers restrict the utilization of consumption measurements for the network operator, compared to the assumed conditions in subsection 2.3.1, these can be included in the DSSE data set, increasing the information availability. The inherent volatility of neighbouring energy systems affecting the operation of DG units however, calls for network monitoring between periodic DSSE executions. Combined with the limited processing capacity of decentralized processors, DSSE results can potentially be diminished during its execution. Addressing the integrity of the LV network monitoring through DSSE should consider these challenges to enable implementation in existing networks. Therefore, an alternative to existing DSSE application techniques must consider multiple aspects:

- With the challenge of accurately formulating pseudo measurements for LV network load points due to the dependency on irrational user behaviour that not necessarily follow historic patterns, missing elements in DSSE input data set, from GDPR or other availability limitations, must be replaced by quantities that represent the network conditions.
- An acknowledgement of the limited processing requires that a solution must be able to represent network conditions during and in-between DSSE execution.
- The uncertainty of results from a proposed solution must be reported to give network operators a better indication of the network operating conditions.

2.3.3 Protection of DG control during information integrity disturbances

In the distribution network layer, connection of small and medium sized power plants composed of multiple DG units, and their decentralized control coordination for power system connection, requires protection against information integrity disturbances that could lead to harmful control actions. Such protection is possible through state estimation model establishment and BDD implementation in a distributed processing topology as illustrated in Figure 2.2c, where each DG unit has its individual cyber error detection system that offers a bottom-up approach to information integrity protection. Such approach must satisfy different properties:

- With the limited performance of distributed processing equipment, representation of the system and the CPES interdependencies in state estimation model must be carefully considered to achieve a trade-off between level of detail and entailed computational burden.
- A distributed processing based approach to cyber error detection must consider robustness of execution and avoid infinite loops that lead to unavailable or incorrect set of filtered measurements.
- Different categories of cyber errors must be detectable, including ICT inflicted measurement error of different categories, and information integrity attacks from adversaries.

2.3.4 Protection of DG control through coordination in cyber-physical conditions

The CPES environment affects DG controls from both cyber and physical domains. With the ability to perform DG controls in LV networks based on a distributed or decentralized processing topology as illustrated in Figure 2.2c and Figure 2.2b, respectively, network operators must carefully consider when to apply local and decentralized control strategies. Such decision making requires coordination and study of the impact from volatile neighboring energy systems, and information security challenges from limited ICT infrastructure by addressing a number of concerns:

- With the possibility of information integrity issues in acquisition, processing, and distributing DG control commands, the relationship between decentralized a DG control strategy and information security challenges must be investigated while considering the optimization process of these strategies.
- Considering a volatile physical operating environment due to DG operation and consumer interactions, the effects of perturbations in the physical system caused by neighboring energy systems interacting with the power system must be evaluated for the DG control strategy coordination.
- Studying the impact of CPES conditions on DG control strategy coordination requires tools for simulating the physical system, CPES interdependencies, and decentralized processing ability to optimize DG operation.

Part II

Low voltage network monitoring

CHAPTER 3

Voltage interval estimation considering information availability limitation

This chapter describes the development and evaluation of a voltage interval estimation method that considers the limited information availability in LV networks for monitoring application. From a CPES perspective, the shortcomings of existing methods introduced in subsection 2.2.1 for LV network monitoring with respect to the formulated high-level research approach in subsection 2.3.1 are summarized. The key characteristics of the proposed monitoring methodology are presented with a focus on the low information availability research question identified in section 1.3.

The details of the proposed methodology are described in terms of the necessary formulation of the physical network information, and formulation of the voltage interval estimation algorithm. The methodology is validated through a sensitivity analysis of assumptions, a demonstration of the resulting estimation granularity, and a probabilistic based analysis of the method performance in different ICT infrastructure scenarios. The entire validation is performed using a Cigré benchmark representation of a European LV feeder as described in [138], and the results show the value of the proposed methodology while considering the ICT infrastructure and information security limitations of such distribution networks in the CPES. In the end of the chapter, the work is summarized and its application is analyzed from a network operator perspective. The majority of this chapter is based on the prepared manuscript in [**Pub. C**], with minor changes to coherently fit into the framework of this thesis.

3.1 Shortcomings of existing DSSE approaches

As introduced in chapter 1, the increased complexity of electric distribution networks from implementation of DG units and electrification of services, entails a need for better monitoring of distribution networks down to the LV level as part of assessing the operational security and for enabling a firm foundation for coordinated control of DERs.

For an assessment of network operation, DSSE methods are proposed as introduced in subsection 1.2.2 and described in subsection 2.2.1. In comparison to state estimation at transmission level, the application of DSSE is more complicated due to the physical characteristics and the inferior performance and reliability of the ICT infrastructure in distribution networks [77, 139]. Existing works in DSSE utilize the improved spacial resolution from deployment of smart meters, but are generally based on an assumption of time synchronized measurement acquisition [92, 140]. Such assumption can be valid at transmission network level as the communicating infrastructure, the WAN has higher requirements for latency and reliability as discussed in subsection 1.2.1,

and the more relaxed NAN communication infrastructure requirements of distribution networks can, as discussed in section 2.1, entail less reliable operation and higher vulnerability to noise and congestion [141, 142]. Therefore, the implementation of DSSE is challenged by the ICT infrastructure ability to ensure information availability, as revealed in different demonstration studies [47, 48].

As described in subsection 2.2.1, support of existing DSSE methods in conditions of low information availability, can be considered through the generation of pseudo-measurement. Such techniques are proposed to give an idea of the load point interactions and thereby estimate load point behaviour in distribution networks [143]. While achieving high accuracy at MV level by aggregating lower level load points at MV connection points, the LV load points are directly dependent on irrational consumer behaviour, challenging load modelling and impeding the implementation of DSSE in the existing ICT infrastructure.

The application of existing DSSE solutions is further complicated when considering the impact of emerging data privacy concerns that can prevent utilization of household consumption data as discussed for information confidentiality concerns in subsection 2.1.1. Due to the GDPR activation, consumers have more control over the utilization of personal data, including the consumption data from residential smart meters [144], which means a complete set of smart meter data is not guaranteed for the execution of existing DSSE methods.

Considering a desirable representation of both active and reactive power for each load point [141], the assumption of fairly synchronized measurements, and the low accuracy in compensating missing quantities with pseudo-measurements in exiting DSSE approaches, their implementation is impeded by the existing ICT infrastructure and its entailed information security challenges discussed in section 2.1. Therefore, network operators might seek alternatives to existing DSSE-based solutions for monitoring the LV network operational conditions.

3.2 Voltage interval estimation method

The proposed method in this chapter can be seen as an alternative to existing LV network monitoring approaches as it does not apply DSSE within its estimation of network conditions. The proposed method takes advantage of network operator available knowledge of the load point distribution and their extreme operating boundaries defined by the implementation of DG units, electrified services, and the electrical installation fuse ratings. Through this information, the proposed method can provide an estimation of the voltage interval of a radial feeder bounded by the worst case voltage magnitude upper and lower profiles whenever it receives voltage magnitude measurements from a single point in the feeder.

As distribution networks have high R/X ratios, the complex current has an impact on the worst case voltage magnitudes in the network as described in subsection 2.2.2. Therefore, the proposed method includes an estimation of worst case line current magnitude and angle in each line segment of the LV feeder, where the worst case conditions are defined as those that cause the largest deviation in voltage magnitude across a line segment. Utilizing the worst case current interval, the methodology estimates an interval around all possible voltage magnitudes for all nodes and phases of the feeder.

The proposed methodology is intended for application in radial distribution networks. In such networks, especially at a LV level, unbalanced operation is a possible and likely scenario. Therefore, the proposed method considers all three phases. An illustration of the method initialization and execution phases is shown in Figure 3.1.

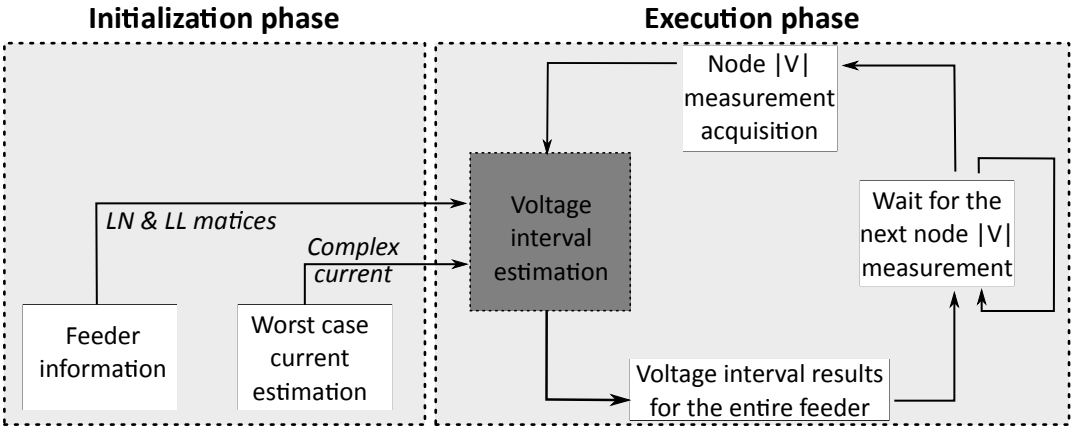


Figure 3.1: Flowchart describing the initialization and execution of the voltage interval estimation method. Source: [**Pub. C**]

3.2.1 Network information processing in the initialization phase

As illustrated in Figure 3.1, the proposed method is divided in an initialization and an execution phase. To initialize the method, the feeder information must be represented with a specific syntax formulated by two matrices LN and LL.

Feeder information

For convenience, the feeder information is represented using matrix notation. The first matrix is a bus incidence matrix and it contains information about the connection between lines and nodes in the LV network feeder. Each row in the LN-matrix represents a line in the feeder, and each column in the matrix represents a node. LN is therefore a $N_l \times N_n$ $(0, 1)$-matrix, where N_l is the number of lines in the feeder and N_n is the number of nodes. An element (r, c), in the LN matrix, is equal to 1 when representing a connection between the r'th line and c'th node.

The second matrix of a particular feeder is defined as the LL-matrix. This matrix is a $N_l \times N_n$ $(0, 1)$-matrix, where each row represents each line and each column represents each node. This matrix describes the shortest path of lines connecting a node to the root-node. In this way, if the c'th node connects to the root-node through lines 1, 2 and 3, the three first rows in column c are equal to 1 while all other elements in the column are equal to 0.

In addition to the specific feeder information, the proposed method requires an estimation of the worst case current interval of each conductor as illustrated in Figure 3.1. In this work, the worst case current is that which causes the most severe change in voltage magnitude across the conductor considering the effects from both the current magnitude and the angle. This is illustrated in Figure 3.1 through the included complex current from the worst case current estimation.

Worst case current interval estimation

With the interval arithmetic approach utilized for power flow calculation in [145], the line current intervals are expressed through a minimum, $Imin_l^p$, and a maximum, $Imax_l^p$, for each line segment $l \in N_l$ and each phase p. As a result of the initialization phase of the proposed method a worst case current interval matrix Iwc^{3p} is expressed with the interval of each line segment l and phase p as shown in (3.1).

$$Iwc^{3p} = \begin{bmatrix} Imin_1^a & Imin_1^b & Imin_1^c & \cdots & Imin_{N_l}^a & Imin_{N_l}^b & Imin_{N_l}^c \\ Imax_1^a & Imax_1^b & Imax_1^c & \cdots & Imax_{N_l}^a & Imax_{N_l}^b & Imax_{N_l}^c \end{bmatrix}^T \tag{3.1}$$

Estimating the magnitude of the line current intervals in (3.1) utilizes prior knowledge of network and load point information. Considering the network in Figure 3.2 with an external grid connection at node $R1$, and consuming units connected to nodes $R2$ to $R7$, and conductors connecting the nodes.

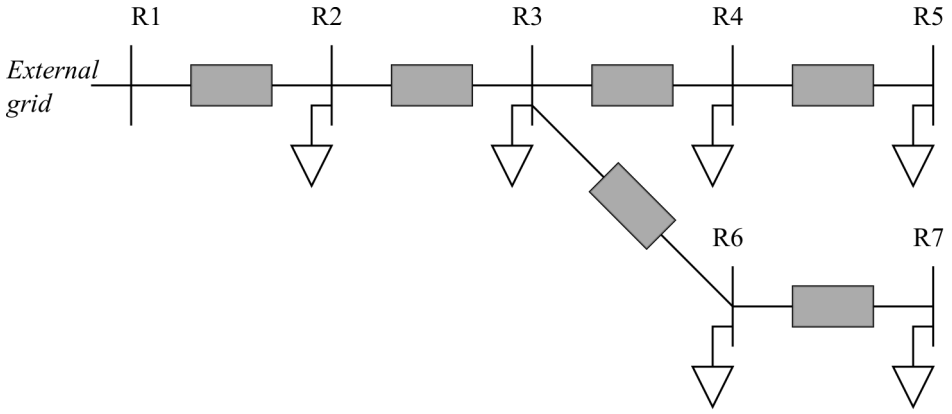


Figure 3.2: One line diagram of simple network demonstrating line current magnitude estimation procedure. Source: **[Pub. C]**

The maximum line current to be expected in the line segment between nodes $R1$ and $R2$ is estimated as the sum of maximum phase currents in each of the consumers connected to the nodes downwards from node $R1$ excluding $R1$. That is, the combined maximum current from loads at nodes $R2$ to $R7$. This estimation can be done for all the conductors in the radial feeder using the LL-matrix, and the feeder load point current magnitude limits.

The load point information is assumed known through an overview of large consuming equipment, e.g. Electric Vehicles (EVs) and heat pumps, and general residential consumption limited by fuses. Therefore, a matrix, $|Imax_n^{3p}|$, containing the maximum load limit of current draw per phase and node can be constructed as in (3.2).

$$|Imax_n^{3p}| = \begin{bmatrix} |Imax_1^a| & \cdots & |Imax_{N_n}^a| \\ |Imax_1^b| & \cdots & |Imax_{N_n}^b| \\ |Imax_1^c| & \cdots & |Imax_{N_n}^c| \end{bmatrix} \tag{3.2}$$

The expected maximum current in each line l and phase p, represented by $|Imax_l^p|$ in (3.1) can then be calculated by transforming the results of (3.3) into a column vector of length $3 \cdot N_l$.

$$|Imax_l^{3p}| = |Imax_n^{3p}| \cdot LL^T \tag{3.3}$$

The minimum line current magnitude is found in a similar way as for the maximum, and $|Imin_n^p| = 0$ if the considered load point n and phase p is composed by consuming equipment. However, modern distribution networks can be bidirectional, meaning $|Imin_n^p| > 0$, with a negative current direction, if a generating unit is connected to node n and phase p. As for the estimation of maximum line current, it is assumed that the network operator knows about connected units capable of injecting current into the LV network, e.g. PV plants and batteries, and their characteristics.

Estimating the current angle intervals for each phase and each line segment is more complicated than for the magnitude as it depends on the specific line impedance matrix Z_l . This is further complicated by the inclusion of a neutral conductor and the geometry of LV network cables and overhead lines, making the impedance matrix non-bisymmetrical as described by the Kron reduction method [see Appendix A.1]. The three-phase conductors will therefore experience different voltage drops at balanced current angles. Furthermore, the worst case current angle combination depends on the balance of current magnitudes in the phases of the line segment.

Therefore, estimation of the current angle interval, resulting in the most severe voltage drop across a line segment, is done through solving a non-linear optimization problem considering the current magnitude intervals estimated using (3.3). Solving this optimization problem, gives the most severe voltage drop across Z_l averaged across the three phases, and therefore returns the optimal combination of current angles of a line segment.

To simplify the estimation of the current angle interval, the minimum and maximum voltage drop optimization problems are combined as a single minimization problem. This is possible since the current direction simply changes the sign of the voltage change at the receiving end. Therefore, an overall objective function f, expressing the receiving end average voltage magnitude for the three phases, can be formulated for each line l and extreme e (minimum or maximum), using Ohm's law as shown in (3.4), subject to the constraints described in (3.5) ensuring a single solution to the non-linear programming problem.

$$\min_{\beta e_l^a, \beta e_l^b, \beta e_l^c} f = \left\langle \left| \begin{bmatrix} |V^a| \underline{/\delta^a} \\ |V^b| \underline{/\delta^b} \\ |V^c| \underline{/\delta^c} \end{bmatrix} - Z_l \begin{bmatrix} |Ie_l^a| \underline{/\delta^a + \beta e_l^a} \\ |Ie_l^b| \underline{/\delta^b + \beta e_l^b} \\ |Ie_l^c| \underline{/\delta^c + \beta e_l^c} \end{bmatrix} \right| \right\rangle \tag{3.4}$$

Subject to

$$-\frac{\pi}{2} \leq \beta e_l^p \leq \frac{\pi}{2} \quad \forall_{p \in \{a,b,c\}, l \in N_l} \tag{3.5}$$

where $|Ie_l^p|$ and βe_l^p are the line l, extreme e, phase p current magnitude and angle, respectively, and $|V^p|$ and δ^p are the sending end, phase p voltage magnitude and angle, respectively. At the sending end phase a complex voltage, $|V^a| \underline{/\delta^a}$ is assumed as $1 \underline{/0°} pu$ and the two other phases are assumed evenly phase shifted $120°$. For convenience in calculating the resulting current angles, the voltage phase angles are added in the phase current angles in (3.4). A magnitude imbalance at

the sending end has no impact on the optimal solution, only on the objective value in (3.4), The three phases are therefore assumed to have balanced voltage magnitudes.

An imbalance in the sending end voltage angle, however, will affect the optimal solution. This effect is limited while considering a maximum allowed Voltage Unbalance Factor (VUF) of 2% according to EN 50160 [146]. The sending end voltage angle is therefore assumed balanced in the proposed method, and the impact of this assumption is evaluated in subsection 3.3.1 through a probabilistic sensitivity analysis. The VUF can be calculated from the negative sequence voltage magnitude over the positive sequence voltage magnitude. However, this work uses the equivalent calculation method described in the IEC 61400-4-30 [147]. With this approach, the VUF can be calculated through the phase to phase voltage magnitude of all three phases by the expression given in (3.6), where the term M is given in (3.7).

$$VUF = 100\% \cdot \sqrt{\frac{1 - \sqrt{3 - 6 \cdot M}}{1 + \sqrt{3 - 6 \cdot M}}} \tag{3.6}$$

$$M = \frac{|V_{ab}|^4 + |V_{bc}|^4 + |V_{ca}|^4}{\left(|V_{ab}|^2 + |V_{bc}|^2 + |V_{ca}|^2\right)^2} \tag{3.7}$$

The optimization problem expressed in (3.4) and (3.5) is solved twice for each line segment, once for each interval extreme, minimum and maximum. This gives the needed quantities in the phasor representation of the line current interval matrix in (3.1). Since the interval matrix only change due to changes in the load composition and long term degradation of feeder infrastructure, from partial discharges and other phenomenons, the initialization phase of the methodology only requires long-term updating.

3.2.2 Measurement acquisition and processing in execution phase

The execution phase in Figure 3.1 of the proposed method is initiated with the acquisition of a voltage magnitude measurements from an arbitrary node and metering device within the feeder as shown in Figure 3.1. With the existing deployment of smart meters, forecasted to reach 1 billion devices globally in 2022 [46], and their configuration capabilities through compliance with international standards, these devices are considered suitable as data sources for the proposed method.

Smart meter configuration

One of the overall benefits of a wide deployment of smart meters, from a consumer perspective, is the enabling of variable energy prices. To obtain this capability, all smart meters must have the ability to accurately measure the household consumption at a high sampling frequency. Smart meters can sample the power consumption at a high frequency through an analog to digital converter, and broadcast the recorded data through inherent communicating capabilities according to the smart meter configuration. The utilization of smart meters allows further acquisition of additional physical properties such as reactive power, voltage profiles and power quality quantities.

Configuration and operation of smart meters is performed according to international standards. In Europe, the International Electrotechnical Commission (IEC) 62056 standard, which represent the Device Language Message Specification (DLMS)/COSEM protocol is most commonly used [148]. The DLMS/COSEM application layer protocol provides a variety of services for interfacing with the

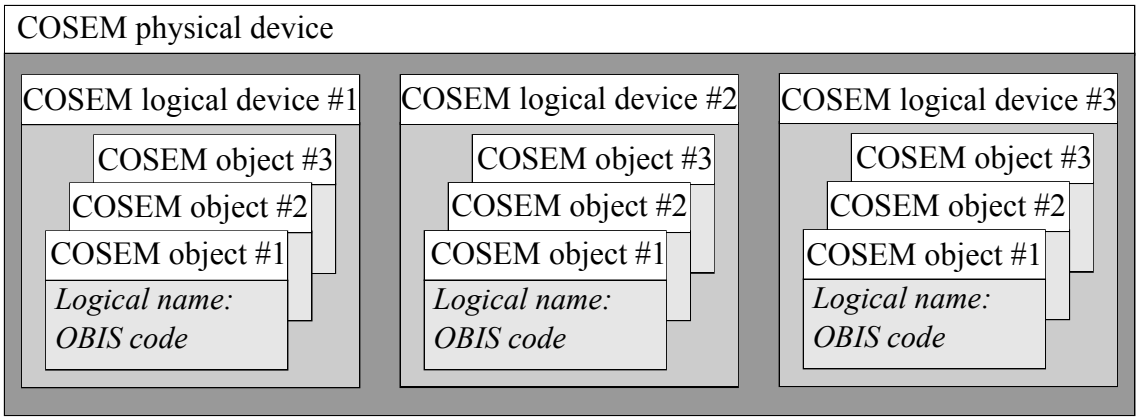


Figure 3.3: Structure of COSEM interface model with physical and logical devices, and COSEM objects defined by the OBIS code specific logical name

COSEM interface model, including; the possibility of initiating a connection between a client and the smart meter, the request for specific data from the client, setting attributes in the smart meter, and pushing data from the smart meter to subscribing clients. For periodic reporting the smart meter data, the latter of the services, called *DataNotification*, can be configured to push messages defined by a list of objects. Such push is initiated when the internal timer reaches a defined time period specific value, thereby enabling a periodic transmission of network information, for example every 10^{th} minute.

Physical devices, such as smart meters, can in the DLMS/COSEM protocol consist of multiple logical devices which are used to differentiate between metering of different energy systems, i.e. gas, water and electricity as illustrated in Figure 3.3.

Within each logical device, COSEM objects are defined through declaring protocol specific OBIS codes as the logical name as illustrated in Figure 3.3. Such codes contains information about:

- The type of logical device, which further specifies the different possible quantities to measure, e.g. voltage magnitude in electricity meters and water flow in water meters.
- The indexation of COSEM objects according to the measurement or communication channel of each object.
- The logical device specific code corresponding to different physical quantities measured.

Configuration of smart meters that follow the DLMS/COSEM protocol allows multiple configuration possibilities that can be exploited. In the proposed voltage interval estimation method, it is assumed that all smart meters are configured to send voltage magnitude for all three connected phases as periodic readings, to a decentralized processor as illustrated with Figure 2.2b that executes the proposed method for a sub-system of the distribution network, e.g. a LV feeder.

Voltage interval estimation algorithm

With an overview of the worst case current interval in polar form for each feeder line segment in (3.1), the feeder voltage magnitude intervals can be estimated as smart meter measurements containing voltage magnitude readings are received. The proposed calculation method, shown in the dark grey box in Figure 3.1, executes based on the received reading and rated accuracy of the meters.

The voltage magnitude interval describes the estimated extremes $|Vmin_n^p|$ and $|Vmax_n^p|$ for each node n and phase p. These results are the output of the proposed method and are structured as in (3.8).

$$|Vwc^{3p}| = \begin{bmatrix} |Vmin_1^a| & |Vmin_1^b| & |Vmin_1^c| & \cdots & |Vmin_{N_n}^a| & |Vmin_{N_n}^b| & |Vmin_{N_n}^c| \\ |Vmax_1^a| & |Vmax_1^b| & |Vmax_1^c| & \cdots & |Vmax_{N_n}^a| & |Vmax_{N_n}^b| & |Vmax_{N_n}^c| \end{bmatrix}^T \tag{3.8}$$

The two matrices LN, and LL described in subsection 3.2.1, are central in the proposed algorithm and only depend on the feeder information. After acquiring a measurement package from an arbitrary node, the proposed method requires one additional vector N and one additional matrix CL.

The vector N is constructed and used to index the location of the received measurement. Therefore, this vector is of size $N_n \times 1$ and contains $N_n - 1$ zeros and a single 1 element. The non-zero element represents the node under consideration, which changes as the algorithm advances.

With the vector N, a diagonal matrix CL can be formed, which defines the lines connected to that node. The matrix CL is calculated using (3.9).

$$CL = diag(LN \cdot N) \tag{3.9}$$

The proposed algorithm is developed for execution every time an arbitrary node voltage magnitude reading is acquired by the decentralized processor from node n_{acq}. For the acquired measurement, the sensor accuracy classification is given by datasheets according to standards such as EN 50470-3 [42], and such accuracy is usually given as two boundaries $\pm\varepsilon_m$ of the possible error of measurement m as introduced in subsection 1.2.1. This error classification is used to form an interval by adding and subtracting the indicated measurement error $\varepsilon_{n_{acq}}$ to the acquired voltage magnitude reading. This gives the initial interval at the node n_{acq} with the boundaries $|Vmin_{n_{acq}}^{3p}|$ and $|Vmax_{n_{acq}}^{3p}|$ in (3.8). It is assumed that the voltage angles $\delta_{n_{acq}}^{3p}$ of the three phases are balanced $120°$ phase-shifted and are considered as the reference angles for all other nodes.

The acquisition initiates the algorithm described in algorithm 1, by increasing the size of the indexation vector N_{idx} to one, with the element being equal to the n_{acq} node number. The role of the indexation vector is to control the sequence of node voltage estimations from the measurement node n_{acq} and ensure that all nodes are estimated when the algorithm finishes.

The idea behind the algorithm is to start from the node of the acquired measurement n_{acq} and identify the lines connected to this node. This process is described in lines 2 to 4 in algorithm 1. For each line under consideration l_{uc}, the two nodes connected to that line are identified in line 7 of algorithm 1. The node corresponding to $N_{idx}\,(1)$ is then removed from the line under consideration, enabling an identification of the neighbouring node n_{nbn}, described in lines 8 and

Algorithm 1: Estimate feeder voltage magnitude interval matrix from single node reading

```
1  while N_idx contains at least 1 element do
2      Initialize the N-vector of zeros;
3      N(N_idx(1)) ← 1;
4      Calculate CL using (3.9);
5      forall Rows cl ∈ CL do
6          if ||cl||_2 > 0 then
7              l_uc ← cl · LN;
8              l_uc(N_idx(1)) ← 0;
9              n_nbn ← index of non-zero element ∈ l_uc;
10             if n_nbn has not yet been estimated then
11                 Concatenate N_idx and n_nbn;
12                 if n_nbn < N_idx(1) then
13                     Vmax^3p_{n_nbn} ← Vmax^3p_{N_idx(1)} + Z_l · Imax^3p_l;
14                     Vmin^3p_{n_nbn} ← Vmin^3p_{N_idx(1)} + Z_l · Imin^3p_l;
15                 else
16                     Vmax^3p_{n_nbn} ← Vmax^3p_{N_idx(1)} − Z_l · Imin^3p_l;
17                     Vmin^3p_{n_nbn} ← Vmin^3p_{N_idx(1)} − Z_l · Imax^3p_l;
18                 end
19                 Insert the estimated boundaries for n_nbn in (3.8)
20             end
21         end
22     end
23     Mark N_idx(1) as estimated, and remove it from N_idx;
24 end
```

9 of algorithm 1. In line 10 and 11, the identified neighboring node n_{nbn} is added to the N_{idx} vector to make sure it will be used as the starting point for one of the consecutive executions of the algorithm, but only if it has not yet been estimated. This way the voltage magnitude interval of every node in the LV network under consideration, is estimated exactly once for each received smart meter reading.

The if-statement in line 12 is used to determine whether the n_{nbn}-node is closer to the root-node than the $N_{idx}(1)$-node, through examining the indexation. This entails that the indexation of all nodes in the network must increase away from the root node while assuming a radial feeder topology. After inserting the estimated boundaries of the neighboring node n_{nbn} in (3.8), the next node in N_{idx} is used as the starting point for executing the algorithm once again, as described by the removal of the node corresponding to the first index in the N_{idx} vector shown in line 23 of the algorithm in algorithm 1. The algorithm then estimates the voltage interval boundaries for each of the nodes in the LV network until the vector N_{idx} is empty meaning the $|Vwc^{3p}|$ matrix in (3.8) is complete.

3.3 Demonstration and performance evaluation

Considering the limitations in existing LV network monitoring solutions and the importance of assessing distribution network security, the proposed method can estimate network voltage conditions without complete data sets and without utilizing consumer consumption data. This is true since: 1) The minimum amount of data required by the proposed algorithm is only the three-phase voltage magnitude measurements from one arbitrary node in the feeder, and 2) because the proposed method only considers the per phase voltage magnitude as input, which is a shared network quantity that does not directly reveal the consumption pattern of the individual load points.

The proposed method is tested using a modified version of an European LV feeder benchmark feeder shown in Figure 3.4 [138]. An apparent power base per phase of $S_{base} = 166.67$ kVA and a line to neutral voltage base of $V_{baseLN} = 230.94$ V is used.

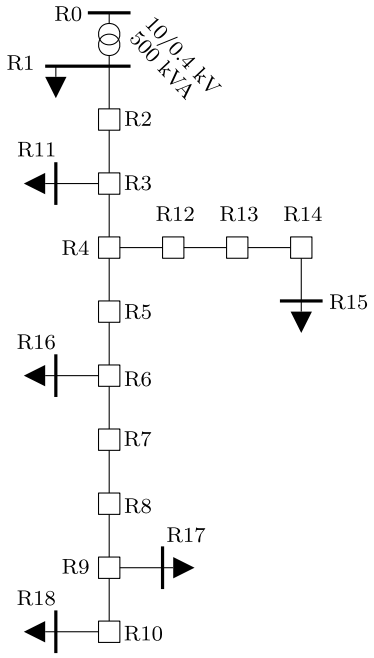


Figure 3.4: Cigré European LV benchmark network. Source: [**Pub. C**]

All load points in Figure 3.4 are residential. In this work fuse ratings are assumed 13 A per phase, meaning each household will have an absolute max current draw of 39 A equal to approximately 9 kW. The apparent power and power factor rating of the original and modified LV feeders are given in Table 3.1. The modifications of the Cigré feeder are based on the distribution of the node $R1$ consumption to the remaining load points. This modification distributes the branch current loading within the network and thereby entails a distribution of the feeder voltage drop. It is important to emphasize that the modifications are only made to enhance the visibility of the proposed method and that the method could be executed on the original feeder as well. This would only entail narrower ranges of the estimated voltage intervals due to the strength of the original grid. For each of the load points in the modified feeder, except for $R1$, the original number of houses are estimated using the prior assumed maximum residential consumption of 9 kW, and four additional houses at each load point are implemented. This means the total consumption in the modified network correspond to 96% of the original network as described in Table 3.1.

Table 3.1: Original and modified load points in Cigré network

Node		$R1$	$R11$	$R15$	$R16$	$R17$	$R18$	All
$\|S\|$ [kVA]	Original	200	15	52	55	35	47	404
	Modified	0	54	90	90	72	81	387
$cos\phi$		0.95	0.95	0.95	0.95	0.95	0.95	
Houses	Original	22.2	1.7	5.8	6.1	3.9	5.2	44.9
	Modified	0	6	10	10	8	9	43

Besides the load point configuration, the LV grid in Figure 3.4 contains two different conductors. The lines connecting nodes $R1$ to $R10$ are all referred to as type 1, while the remaining lines are of type 2. The main difference between these conductors is apparent from [138], where the cross sectional area of the two conductors is 240 and 50 mm^2, respectively. The LV feeder is used to execute three case studies, each with specific objectives. Firstly, a sensitivity analysis of how different parameters affect the worst case line current angles estimate is conducted from a voltage deviation perspective. Secondly, a demonstration of the voltage magnitude interval estimation from single node measurements is presented and extended with an evaluation of the granularity expected from the proposed methodology when acquiring using multiple measurements within a short time period during which the network is in a quasi steady state. Finally, an evaluation of the proposed method application is performed using Monte Carlo simulations while considering different meter distribution and meter accuracy scenarios.

3.3.1 Current angle sensitivity analysis

For the first case study, the proposed worst case complex current matrix in (3.1) is identified for the Cigré feeder using the optimization problem in (3.4) subject to (3.5) and the genetic algorithm solver. The resulting phasor diagram is given in Figure 3.5.

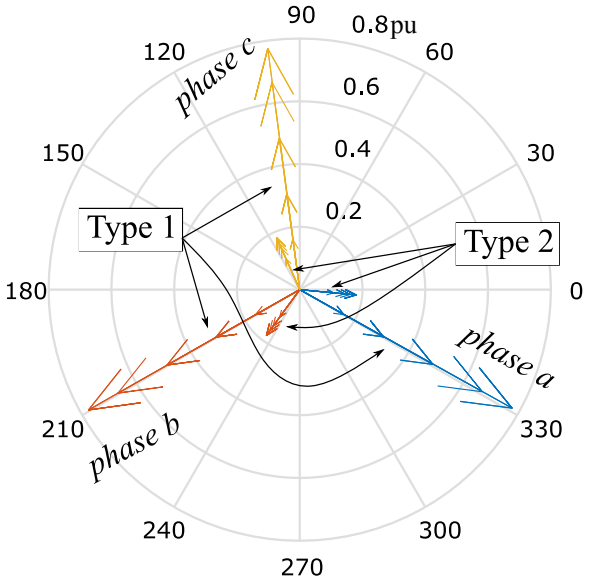


Figure 3.5: Phasor diagram of worst case line currents of all line segments in Cigré LV feeder. Source [**Pub. C**]

From Figure 3.5 the dominating parameter in determining the worst case current angle is the line impedance matrix while the current magnitude has only a limited effect. The limited effect of the current magnitude is because the estimated worst case conditions are balanced as none of the load points in the considered LV network have additional single phase connected equipment, e.g. a heat pump. With the limited impact due to balanced worst case current magnitudes, the worst case current interval estimation part of the proposed method can be further simplified through only estimating the current angles for the different line types in the network.

In the proposed method, the voltage angles at the sending end are assumed balanced in (3.4). To analyze this assumption, Monte Carlo simulations are conducted where the sending end voltage angles in (3.4) are randomized and unbalanced, leading to different estimated worst case current angles. Both the voltage and current magnitudes are kept constant during this analysis. The outcome of the probabilistic analysis is then the correlation between sending end voltage angle imbalance expressed by the voltage imbalance factor according to [146], and the average receiving end voltage drop. The Monte Carlo simulations are conducted for a representation of each of the conductor types in the network and the results are shown in Figure 3.6.

Included in Figure 3.6 is a representation of the voltage magnitude drop in a simplified estimate of the worst case current interval, where the current angle phase shift is assumed $\beta = 0°$ for all phases. Comparing the two worst case current angle considerations in Figure 3.6, show the importance of considering the worst case current angle in the conductors for the proposed method. This is visible from the difference in voltage magnitude deviation ΔV between the two current angle scenarios for both conductor types in Figure 3.6. For type 1 conductor, the estimated worst case current

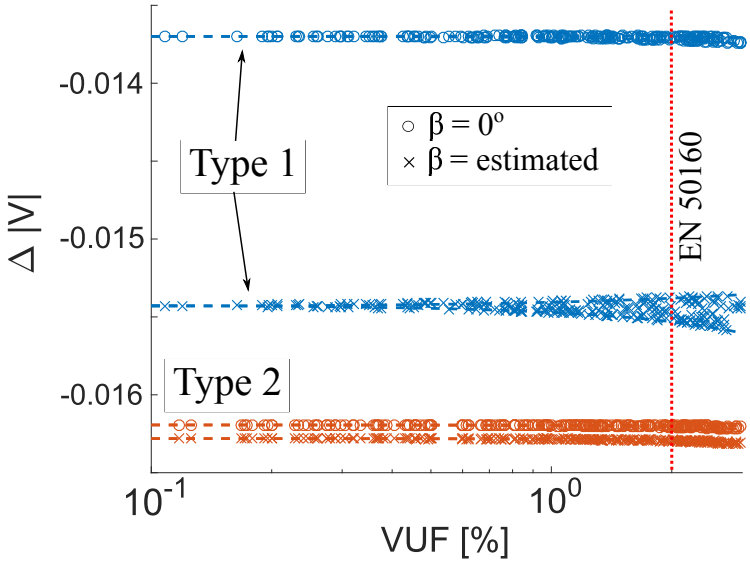


Figure 3.6: Voltage unbalance factor impact on angle estimation and consequently voltage drop. Source [**Pub. C**]

angle is found approximately equal to $-30°$ for each of the three phases, while the conductor of type 2, is around $-5°$ for each of the phases. The difference in estimated worst case current angles is reflected by their distance to the simplified representation of $\beta = 0°$, which is considerably larger for type 1 than type 2. For both however, it is seen that with the estimated worst case current angle, the voltage drop across the conductor is more severe.

From Figure 3.6, the two conductors are seen to react differently to unbalanced sending end voltage angles, shown by the increasing spread of voltage magnitude drop with increasing VUF percentage calculated using (3.6). For both conductors in the LV network, the maximum allowed VUF of 2% according to the EN 50160 standard [146] only express a small difference from the voltage magnitude drop seen at a VUF equal to 0%, limiting the impact of the assumed balance between sending end voltage angles.

3.3.2 Demonstration of estimated interval granularity

The benefits of the proposed method can be evaluated by estimating the voltage intervals based on a measurement acquisition from one smart meter at each of the load points in Figure 3.4 $R11$, $R15$, $R16$, $R17$, and $R18$, assuming each smart meter measures and reports the voltage magnitude for each of the three phases of the LV feeder and that all the reporting smart meters have equal measurement accuracy. The evaluation is demonstrated using randomized operating conditions with the apparent power and inductive power factor of each load point and phase in Table 3.2.

With the load properties in Table 3.2, a power flow calculation is executed to retrieve the voltage magnitude at each node and phase using the DistFlow method described in [149], which is used as a representation of the actual voltage profile of the feeder during the loading described in Table 3.2. For each LV feeder load point in Figure 3.4, the voltage magnitude measurements of all phases are distorted by adding a normal distribution random error with zero mean and standard deviation, $\sigma = 0.01/3$. The standard deviation of the measurement error is based on an assumed meter

Table 3.2: Load point phase parameter during voltage assessment evaluation

Node		$R11$	$R15$	$R16$	$R17$	$R18$
$\|S\|$ [kVA]	phase a	17.4	29.0	50.5	21.0	70.8
	phase b	16.8	28.0	85.8	43.8	64.0
	phase c	12.2	20.3	64.3	52.6	6.1
$cos\phi$	phase a	0.94	0.99	1.00	0.95	0.96
	phase b	0.92	0.97	0.92	0.94	0.90
	phase c	0.95	0.98	0.99	0.96	0.96

accuracy of $\pm 1\%$ relative to rated conditions, and that $3 \cdot \sigma$ encapsulates 99.7% of the normal distribution probability density function.

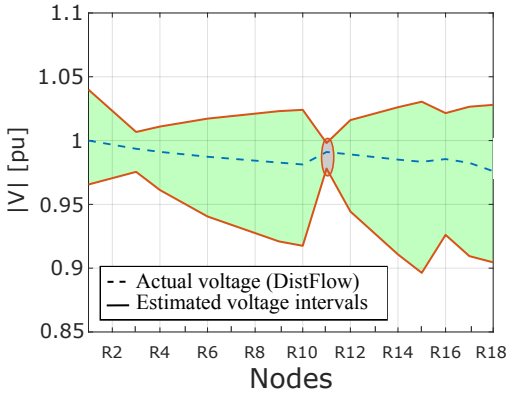
The distorted values from each load point are used in the execution of algorithm 1 one by one, starting from node $R11$. The resulting voltage assessment for phase a is presented in Figure 3.7a.

From Figure 3.7a, a wide interval range of the phase a voltage magnitude profile is estimated. With this estimate, the network operator would read a risk of under-voltage conditions at node $R15$, since the lower boundary of the interval at this node is lower than the 0.9 pu limit set by EN 50160 [146]. If it is assumed that a package of voltage magnitude measurements from node $R15$ is acquired shortly after the $R11$ measurements and that the LV network has been in a quasi steady state, the proposed estimation method can be used to narrow the potential voltage magnitude interval as seen by the results in Figure 3.7b.

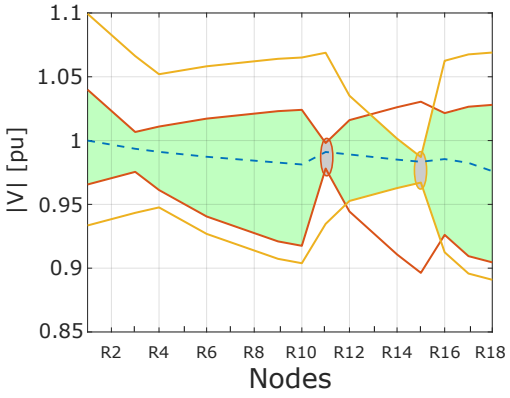
After processing the node $R15$ measurements, the estimated interval no longer considers a risk of under-voltage on phase a. Furthermore, from the results in Figure 3.7b, the interval estimate is narrower at nodes $R12$, $R13$, $R14$, and $R15$ compared to the estimate from processing $R11$ measurements alone in Figure 3.7a. Such improvement from processing multiple measurements acquired with short time delays is further visible when considering the results in Figure 3.7c to Figure 3.7e, where measurements from nodes $R16$ to $R18$ are processed by the proposed method, one by one.

For each received measurement package from smart meters assumed at each load point in Figure 3.4, a maximum and minimum voltage profile is estimated and shown in Figure 3.7. This way, Figure 3.7 shows how a single measurement point gives a rough estimate of the voltage profile across the entire feeder, where it is narrowest at the point of measurement shown by the grey ellipses. Highlighting the region within the interval boundaries of all estimated profiles in green in Figure 3.7 shows how it encapsulates the DistFlow resulting voltage magnitude profile. Such voltage interval estimation enables the operator to easily and quickly assess the security of the LV network, simultaneously, it gives an input to the decision making for different control capabilities within the network.

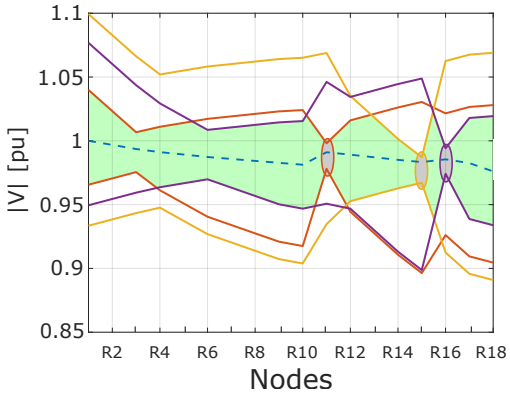
The results in Figure 3.7 also show the strength of the proposed method in conditions where the ICT infrastructure is unable to ensure reliable information availability. Such ability is visible by considering each of the colored interval estimations in Figure 3.7 individually. If only a single measurement is received due to limited information availability, an interval of the feeder voltage profile will still be estimated and transmitted to the operator. This way, the proposed method can utilize minimal measurement acquisition and still inform the network operator on the operational conditions within the feeder.



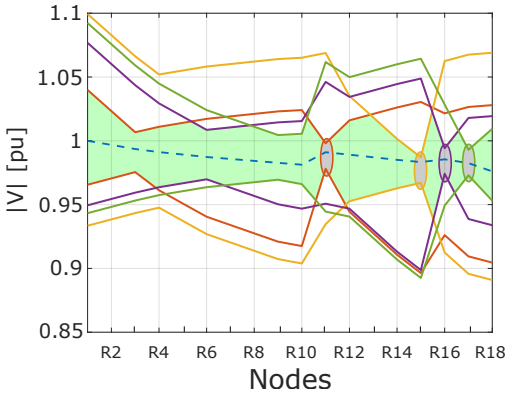
(a) Interval estimated from $R11$ measurement, red



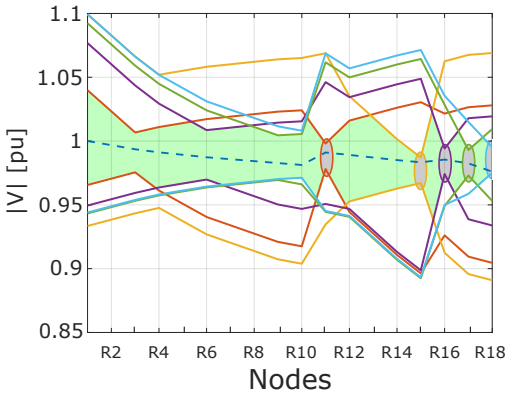
(b) Interval estimated from $R15$ measurement, yellow



(c) Interval estimated from $R16$ measurement, purple



(d) Interval estimated from $R17$ measurement, green



(e) Interval estimated from $R18$ measurement, light blue

Figure 3.7: Phase a voltage magnitude assessment with load configuration in Table 3.2. Source: **[Pub. C]**

3.3.3 Performance in different metering scenarios

Evaluating the performance of the proposed method is done through a probabilistic analysis of the method's ability to capture the voltage profile from DistFlow results within the estimated interval. To perform this analysis, Monte Carlo simulations with a population of 100,000 are performed, where the power flow is calculated using the DistFlow method described in [149], and the voltage intervals are estimated using the proposed LV network monitoring method of this chapter. For

this analysis the voltage interval estimation is performed through assuming an acquisition of measurements from multiple meters within a short time period during which the network operates in a quasi steady state. The number of measurement locations is based on scenario specific meter distributions. Furthermore, the assumed meter accuracy is varied for evaluating the method's dependency on the meter quality.

For the distribution of meters, three scenarios are considered; one where meters are placed only at the nodes furthest away from the root node, i.e at $R15$ and $R18$, one where meters are placed at all load points $R11$, $R15$, $R16$, $R17$, and $R18$ in Figure 3.4, and one where meters placed at all nodes in the network from $R1$ to $R18$. For the second and third meter acquisition scenarios, DSSE could theoretically be implemented, however this requires handling power consumption or node voltage angle information which is considered unavailable for the proposed methodology due to the assumed information availability restrictions from GDPR. Furthermore, three different meter accuracy conditions are assumed, where all meters have an accuracy of $\pm 1\%$, $\pm 0.1\%$, and $\pm 0.01\%$, respectively.

To execute the probabilistic analysis, the apparent power of the feeder load points is randomized within the rated apparent power given in Table 3.1, and through an assumption that all residential load points have integrated DG units through rooftop PV equivalent to 30% of their rated consumption. Additionally, the power factor is randomized between 0.9 lagging and 0.9 leading. The results are analyzed by looking at instances where the voltage profile from the DistFlow results is outside the narrowest estimated voltage interval considering an estimation using measurements from multiple meters according to the meter distribution scenario. Hence, for the first meter distribution scenario, the estimated voltage intervals are the combination of estimated intervals at nodes $R15$ and $R18$, for the second meter distribution scenario, the aggregated intervals are based on estimated intervals from all load points in the LV feeder, and the combined intervals for the third meter distribution scenario are based on intervals estimated from measurements at all the nodes in the LV feeder. The violation of the assessed boundaries are registered per phase and node, meaning the total count of evaluations is $3 \cdot 18 \cdot 100,000 = 5,400,000$. The results of the probabilistic analysis are given in Table 3.3.

Table 3.3: Probabilistic analysis of voltage estimation violations in different meter distribution and accuracy scenarios

Meters at	$R15$ & $R18$			$R11$, $R15$, $R16$, $R17$ & $R18$			$R1$ to $R18$		
Meter accuracy	$\pm 1\%$	$\pm 0.1\%$	$\pm 0.01\%$	$\pm 1\%$	$\pm 0.1\%$	$\pm 0.01\%$	$\pm 1\%$	$\pm 0.1\%$	$\pm 0.01\%$
Count	1617 (0.03%)	1650 (0.03%)	1637 (0.03%)	4044 (0.07%)	4041 (0.07%)	3984 (0.07%)	14560 (0.27%)	14719 (0.27%)	15485 (0.29%)
Median error [V]	0.152	0.016	0.002	0.155	0.016	0.002	0.156	0.016	0.002
Max error [V]	1.446	0.127	0.038	1.553	0.155	0.042	1.788	0.177	0.325

The results in Table 3.3 show that there is a small risk of violating the assessed voltage boundaries, meaning the proposed method is able to fully encapsulate the voltage profile of the feeder in most cases. This risk of wrongful estimation is evaluated to depend on the number of measurement points collected, but is below 1% for all the different distribution scenarios. The inability to encapsulate the voltage profile is partly due to the conversion of the sensor classified measurement error into an interval, which not encapsulates 100% of the possible error. Furthermore, the assumed

balanced sending end voltage when estimating the current angle entails a minor error as illustrated in Figure 3.6. Finally, the non-linearity of the optimization problem, the objective of finding the worst current angle based on an average voltage deviation for all three phases, and the accuracy of the genetic algorithm all contribute to the risk of wrong estimates.

Looking at the violation statistics of Table 3.3, it is seen that having highly accurate sensors and a high performance of the data communication infrastructure supports the proposed method by limiting the median and maximum violations. The highest violation is seen when measurements are acquired from all load points and all sensors have high rated measurement error. Here however, the violation is a most 1.8 V which is less than 0.01 per unit. This extreme case is not common as can be seen by the median which is around a tenth of the maximum observed violation.

3.4 Conclusion

This chapter describes the development of a voltage interval estimation method that offers an alternative to existing DSSE approaches that are impeded by the limited performance of the existing ICT infrastructure. The objective of the proposed method is to enable estimation using the existing ICT infrastructure, which is considered through development based on the high-level research approach described in subsection 2.3.1.

The proposed method satisfies the identified ICT infrastructure related information security challenges, as it is able to estimate the LV network conditions through processing only shared information, here in the form of voltage magnitude measurements from the smart meter connection terminals. Such utilization satisfy the information confidentiality concerns as it does not reveal individual user behavior. Furthermore, with the proposed method, the operator available network knowledge is utilized to estimate the conditions of the entire feeder through processing measurements from individual nodes and is shown able to improve the estimation through processing multiple measurements that are acquired within a short time period. This processing approach therefore acknowledges the risk of asynchronous measurement acquisition.

The estimation of worst case line current interval is evaluated through a sensitivity analysis, where the impedance matrix of the conductor is found to have a greater impact on the worst case current estimation than the current magnitude through the conductor. Such evaluation is especially true when the worst case current magnitudes are estimated to be balanced, which is the case when the implementation of single phase connected DERs is limited. Furthermore, an assumption of balanced sending-end voltage used in the optimization is evaluated and the results show that only a minor impact is expected while considering the EN 50160 standard requirements to the voltage unbalance factor.

A randomized load profile configuration and the corresponding power flow results show the value of the proposed method. From this analysis, the proposed method is shown to give the operator a means of evaluating the voltage magnitude profile of a feeder through acquisition from a single measurement point. Furthermore, the results indicate the benefits of performing the proposed voltage assessment on multiple measurements acquired with short time delays. This utilization narrows the voltage magnitude boundaries giving the operator a more detailed view of the operation during quasi steady state operation.

In the end the proposed method is evaluated using Monte Carlo simulations with randomized load point operational conditions. This evaluation is based on an analysis of the number of simulation

conditions where the estimated boundaries where unable to encapsulate the network conditions, and the severity of which the estimated intervals excluded the network conditions. Although the proposed method is unable to perform perfectly in any of the three considered meter distributions and rated error scenarios, the method encapsulates the voltage magnitude profile in more than 99% of the simulated conditions.

From a network operator perspective, the proposed voltage magnitude estimation method brings value through enabling an assessment of LV network operational conditions. As such the proposed method is comparable to the utilization of state estimation in transmission networks. The proposed monitoring approach gives an overview of an entire LV feeder through the acquisition of per phase voltage magnitude readings from a single node. For each phase and node, the method returns an interval representation of the estimated voltage profiles, which gives the network operators an indication of the information integrity. Form the analysis of limited estimation error in terms of magnitude and occurrence, the proposed method offers a reliable overview of network voltage conditions.

With implementation of the proposed method, the network operator could provides an important input to DG control strategies and further network analysis, every time the decentralized processor receives and treats a measurement package from a smart meter within the network. Such further analysis include planning of investment in power system and equipment through identification of critical equipment, and phase coordination of new single-phased DERs equipment through identfication of severe unbalance. Finally, the proposed voltage interval estimation method for monitoring LV feeders enables identification of critical feeders within the distribution network, which can support network operator in prioritizing the investment in ICT infrastructure and implementation of more advanced monitoring approaches.

CHAPTER 4

Bi-level estimation platform considering limited processing capacity

This chapter presents the development of a bi-level processing platform for estimation of distribution network condition through application of DSSE. With information security challenges and limited performance of the existing ICT infrastructure, the application of existing DSSE applications is impeded as highlighted in the presentation of current literature state of the art in section 1.2, and the elaborate discussion on their shortcomings in section 3.1. The bi-level estimation platform proposed in this chapter is focused around the identified research question about limited processing capabilities impact on DSSE application utilized in the formulation of the high level research approach in subsection 2.3.2. The developed platform can be considered as a more advanced approach to LV network monitoring compared to the interval estimation method presented in chapter 3 as it enables estimation of network conditions between periodic acquisition of smart meter data.

The developed platform for distribution network monitoring is based on a careful processing of measurements through distinguishing between data sources with different transmission settings, which are presented in the beginning of this chapter. The details of the bi-level estimation platform are described in terms of its execution, intended implementation and overall architecture. Afterwards, the platform is demonstrated and verified through processing power flow simulation results from a LV feeder model. The performance evaluation is done with different degrees of data loss, that represents both the limited ICT performance and the availability restrictions from GDPR. The development and evaluation of the bi-level monitoring platform is summarized and considered from a network operator perspective. The majority of this chapter is based on prepared manuscript in [**Pub. D**], with minor changes to coherently fit into the framework of this thesis.

4.1 Metering transmission settings

The deployment of smart meters and the installation of numerous DERs with inherent measurement and communication capabilities have increased the number of observation points that can be utilized in distribution network monitoring. Most European smart meters form data packages according to the DLMS/COSEM protocol [150] as introduced in subsection 3.2.2, and are primarily used for electrical billing purposes. Adjusting the DLMS/COSEM settings through the OBIS codes allow customizing the data package content and the communication settings, meaning the smart meters can be adjusted to fit additional applications.

While the installation of DERs stretches across multiple technologies and numerous manufacturers, international efforts are made to ensure technology and manufacturer neutral standards. The IEEE 1547 aims to standardize interconnection and interoperability requirements of DER capabilities and the IEC 61850 aims to standardize the communication between distributed IEDs and digital substations [151–153]. Open source protocols that align information models and communication between DERs and servers are also proposed, such as the SunSpec protocol, which focus on, but is not limited to, solar PV integration [154].

These efforts in standardization enable utilization of different data sources in the proposed distribution network monitoring platform. Each data source can be characterized by its transmission setting, of which there are three available options as illustrated with the examples in Figure 4.1.

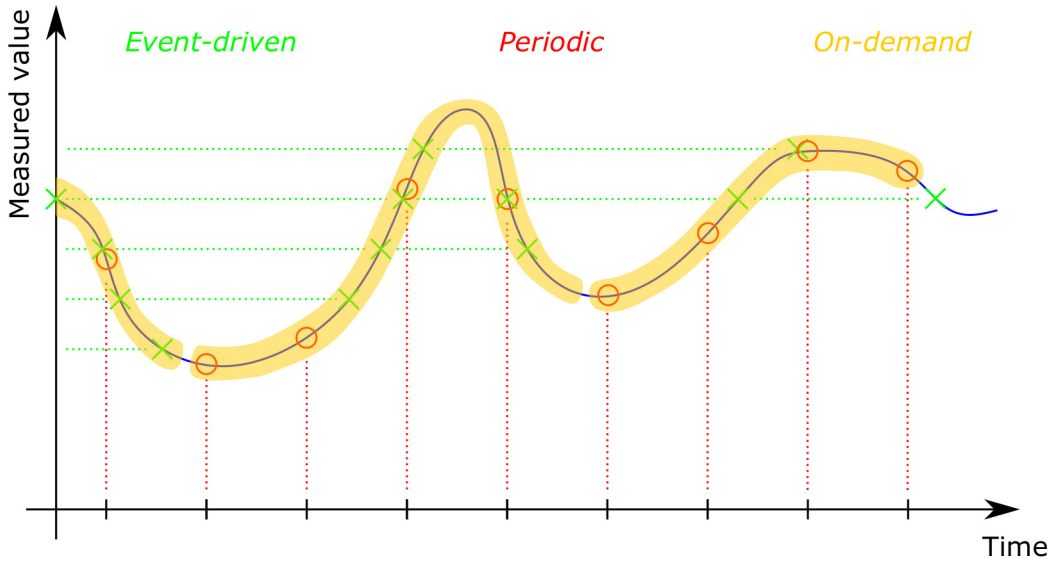


Figure 4.1: Measurement transmission setting options

The three options for measurement transmission illustrated in Figure 4.1 consists of event-driven, periodic, and on-demand acquisition. The first option configures the data source to initiate a transmission of information when a measured quantity changes substantially. The necessary change, that causes a new transmission is predefined by a threshold value that can be different for different measured quantities. In Figure 4.1, the event-driven option is illustrated with green crosses and is seen able to capture the dynamics of the signal while limiting the transmission frequency. Considering the case of multiple distributed meters that transmit information according to the event-driven option, there is a high chance that these meters will transmit the gathered information in an asynchronous fashion. Such asynchronous acquisition is considered undesirable for measurement processing, as it entails the need for measurement alignment or inclusion of measurement estimates, such as pseudo values as discussed in subsection 2.2.1.

In comparison, a periodic transmission option enables synchronous data acquisition if the effects of ICT infrastructure limitations are ignored. The synchronous acquisition is valuable in processing data as complete data sets are updated in a periodic fashion, which alleviates the need for aligning the information and simplifies the evaluation of historic data. Such option is initiated by the periodic triggering of a timer inside the meter with a custom time-interval as illustrated in Figure 4.1

as red circles. Here, the periodic transmission of measurements is seen unable to completely capture the dynamics with the frequency of information transmission used in the example. To capture more dynamics, this frequency must be increased which entails higher requirements on the ICT infrastructure. Besides higher communicating requirements, a smaller time-interval between periodic transmissions increases the likelihood of unnecessary transmissions of unchanged quantities as illustrated by the last two periodic acquisitions in Figure 4.1.

The last transmission setting is used to transmit data on-demand. Such option is initiated by a request from a data client, which ask the data source to transmit the desired information when needed. This option is currently used for the application of electricity billing, where the retailer can ask smart meters to send daily load profiles once a day. In Figure 4.1, this setting is illustrated as yellow areas in which the sampling frequency is configurable but depends on the local data storage of the metering device. With limited data storage capacity, the on-demand transmission option risks loosing stored information if the storage is overflown between data requests. Furthermore, this option is not intended for operational processing as it requires a longer initiation of transmission through the request and respond characteristics, and since the potentially large data set can be subject to large communication delays.

4.1.1 Existing event-driven network monitoring methods

The advantages and shortcomings of the three introduced transmission setting makes them feasible for different applications. In existing literature on distribution level monitoring, either the periodic or the event-driven options are utilized for estimating the network conditions. The periodic acquisition is the main option in DSSE applications as introduced in section 2.2, since provision of complete data sets is of high importance for the DSSE execution.

An alternative to DSSE methods are Forecast Aided State Estimator (FASE) approaches. These utilize a state space model of the network and its dynamics to describe the slow time evolution of the network based on multiple acquired measurements within the network [155]. The FASE methods have the added advantage of being able to estimate the network conditions with incomplete data sets since they have an inherent state forecasting step integrated in the algorithm, and can therefore utilize the event-driven transmission setting. This however relies on correct knowledge of future behaviour of loads and generators which can be complex at LV level due to the tight link to irrational consumer behaviour. Furthermore, the replacement by forecast values is only possible when there are no major changes in the operating conditions of all other quantities than the measured value. This is due to the estimation through fine-tuned Kalman filters, and the risk of filtering these changes as if they were errors.

The use of FASE techniques is historically challenged by the complexity of implementation and parameterization, and it is shown unreliable for systems that are not close to being linear between updates [114]. These issues are proposed handled by the unscented transformation that improves the approximation of the linearized model through considering additional input points based on the input statistics. From a distribution network perspective, the quantity and diversity of feeder networks complicate the deployment of FASE-based monitoring systems. Considering the application of unscented transformation to ease implementation is affected by likely changes in consumer connected devices and user irrational behaviour that can change the input statistics. These conditions inherently entail a risk that the FASE-based methods diverge.

4.2 Bi-level interval estimation platform

The novelty of the developed bi-level approach to distribution network monitoring introduced in this chapter is the utilization of both periodic and event-driven information acquisition through a two-layered data processing strategy. On one level, a three-phase DSSE algorithm, as introduced in subsection 2.2.1, is executed using acquisition of periodic smart meter readings. This execution is possible when assuming that not all consumers restrict the data utilization through GDPR as considered in chapter 3. In the second processing layer, event-driven measurements from DERs are processed after acquisition. This event-driven update of network conditions gives a potentially near real-time monitoring and captures system dynamics, which can be used by the operator for LV network security assessment and as input to control decision making. The second layer processing is handled by an interval-arithmetic consideration of measurement inaccuracy and a calculation of the impact on branch currents and node voltages from a recorded change in DER operation. With the interval-arithmetic approach, the network conditions are given as a range rather than a specific value. This has the benefit of giving an indication of uncertainty not provided by DSSE itself, which provides deterministic results. Furthermore, the combination of two processing layers is useful since the second layer provides updated results that can replace missing entities in the periodic DSSE data set.

4.2.1 Platform and processor execution overview

The developed distribution network monitoring platform is intended for implementation at secondary substations where LV radial feeders are connected to the higher voltage level distribution network. It requires a configuration of the data source transmission settings and a routing of the information flow towards a decentralized IED illustrated in Figure 2.2b, and has the developed bi-level processing approach integrated. From a cyber-physical perspective, the load points connected to a specific LV feeder transmit their reading towards the utility company. This transmission can be routed to go through a data concentrator which bundles the data from multiple sources. Such data concentrator can be configured to collect data from other IEDs, such as those controlling and metering DERs. By connecting a data concentrator to the proposed platform, all information is routed to the monitoring platform. This shortens the distance and limits the cumulative communication network utilization compared to a centralized implementation of the proposed platform as illustrated by the processing topology in Figure 2.2a. An overview of the implementation of the platform presented in this work, and a flowchart of its execution is shown in Figure 4.2.

The platform initiates its execution after the connected data concentrator receives new measurements, as shown in Figure 4.2. As shown in the flowchart of Figure 4.2, the information is initially sorted as periodic and event-driven acquisitions and used in the execution of the two processing units. The routing of data within the proposed platform is shown in Figure 4.2, where the periodically acquired information is send to the data set formulation process before being used in the DSSE execution. The necessity of the data set formulation process comes from the risk of limited information availability as discussed in subsection 2.1.3. In addition, the confidentiality concerns and entailed GDPR discussed in subsection 2.1.1, enables consumers to limit the use of their data, which can cause missing data set elements as considered in great extend in chapter 3. Furthermore, the robustness of communication network used for distribution network data transmission, either PLC, cellular, or others is affected by a harsher environment compared to the use of optic fibres

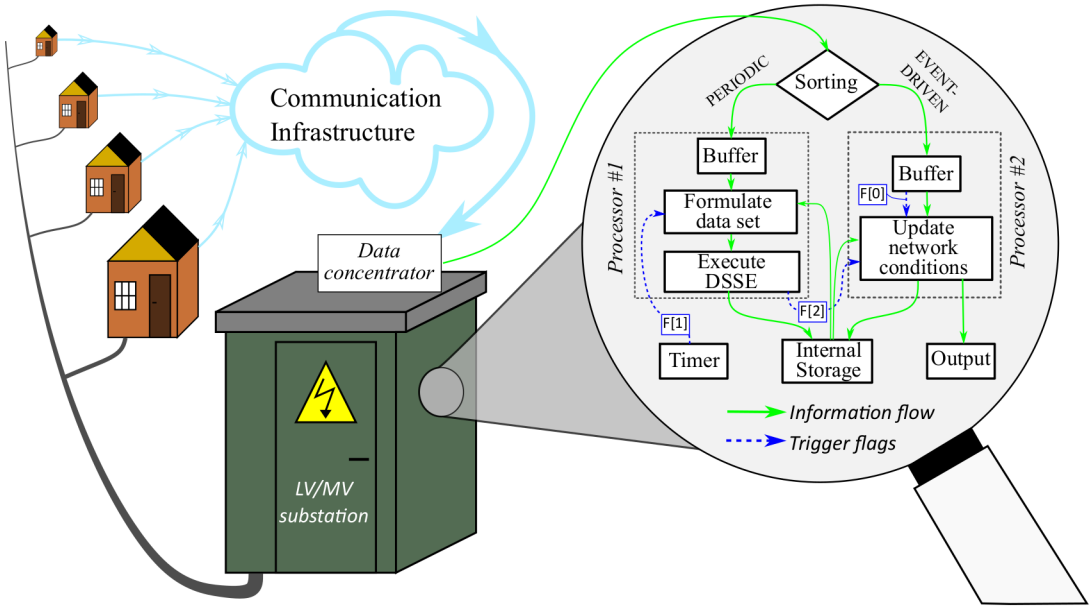


Figure 4.2: Overview of the bi-level LV network monitoring platform and its implementation in a secondary substation cabinet

in transmission level SCADA systems. This lower robustness can cause direct data loss due to congestion or large errors from noise and thereby limit the availability of information.

Besides the periodic readings that do arrive at the platform, the data set is formulated through the inclusion of network condition information that is updated when event-driven measurements are routed through processor 2 in Figure 4.2. With the acquisition of event-driven measurements, the changed physical conditions are evaluated through estimating the resulting change in network branch currents. These are analyzed to update the voltage magnitude interval of all phases and nodes within the network. The replacement of missing measurements in the data set formulation and ensures that the DSSE is given a complete data set every time it executes. The utilization of such regularly updated pseudo measurements, that do not depend on the integrity and availability of historic information, entails a consideration of network operation compared to using forecasts or historic data directly. When the DSSE execution finishes, event-driven updates performed during the DSSE execution are re-evaluated by processor 2 with the new DSSE results.

The consideration of both periodic and event-based data acquisition, thereby, enables formulation of data sets for DSSE execution in the first processor, and allows an update of LV network conditions in the second processor when changes in the physical system cause new data transmissions. For this purpose, the proposed platform considers smart meters as periodic measurements, and suggests configuring DERs to follow the event-driven transmission setting. It is assumed in this work, that all DERs are connected through bi-meters and their network interactions are not included in the smart meter measurements. Additional sensor readings of systems that affect the network conditions can be included. These sensors include IoT sensors of traffic and residential activities, as well as weather sensors and forecasts. With the addition of more sensors, the event-driven updates of network conditions are more frequent, meaning the network conditions can be monitored with higher granularity.

The execution of the proposed platform depends on the activation of triggers as shown in the

flowchart of Figure 4.2 by the 3-bit flag indicator F. The least significant bit in F indicates the acquisition of new event-driven measurements, the next bit controls the periodic execution of the DSSE algorithm, and the most significant bit is used to notify processor 2 when processor 1 has finished the estimation of the state variables. The different trigger flags initiate the two processing units according to the state machine diagrams in Figure 4.3 and Figure 4.4, which are explained in details in subsection 4.2.2 and subsection 4.2.3, respectively.

4.2.2 Execution of processor 1: DSSE

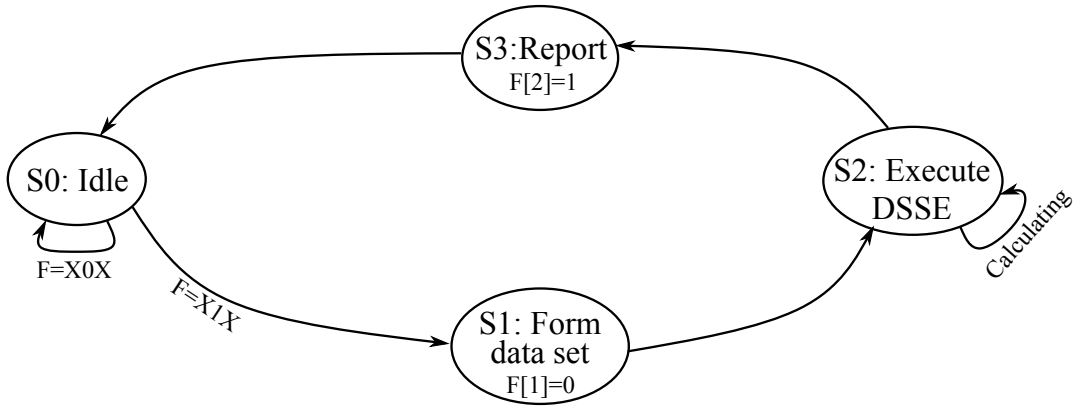


Figure 4.3: State machine representation of processor 1 execution. Source: [**Pub. D**]

Processor 1 executes in accordance to the state machine diagram in Figure 4.3, where it by default enters an idle state S0, until the timer flag is triggered. This triggers in alignment to the smart meter periodic transmission setting, which limits the amount of missing elements in the data set and ensures timeliness of the DSSE execution. In state S1, the missing elements are identified and substituted with information loaded from the internal storage of network conditions that are updated by processor 2. For each node in a radial feeder, it is assumed that the DSSE data set includes three measurements for each of the three phases, that is active and reactive power injection, and the voltage magnitude.

After ensuring a complete data set through substituting missing smart meter readings, a state estimation algorithm is executed to find the optimal solution. Due to the high R/X ratio of distribution networks in general, the DSSE algorithm chosen must consider the AC power flow mismatch functions, and due to the likelihood of unbalanced operation in the LV network, it is based on a three-phase representation of the feeder in question. Such DSSE algorithms are used in numerous studies in current literature as discussed in section 1.2 and introduced in subsection 2.2.1.

The estimation techniques used in the DSSE execution in state S2 is based on the WLS algorithm that finds a solution to the minimization problem in (2.4), through application of the Newton method [see Appendix B.1]. All measurements are here assumed to have equal weights in the covariance matrix $[R]^{-1}$, except the power injections measurements at the root node, which are considered un-measured in the current formulation due to a lack of metering equipment at secondary substations. Instead, these are based on an estimate of the branch currents and node voltages from the network condition updates and Kirchhoff's current law, and are therefore given a lower weight than the remaining measurements.

Although the platform is proposed to utilize this specific DSSE algorithm and data representation, other methods can be used instead as long as they return the three-phase conditions of the network. For simplicity, the state variables are chosen to be node voltage angle and magnitude as shown in (4.1), where the node 1 voltage angles are assumed balanced, with $\delta_{1a} = 0°$ for reference.

$$\mathbf{x} = [\delta_{2a}, ...\delta_{Nc}, |V_{1a}|, ..., |V_{Nc}|]^T \tag{4.1}$$

Following the nonlinear measurement model in (2.1), the state equations are formulated in accordance to the three identified measurement types, that is active and reactive power injection, and voltage magnitude. The set of state equations $\mathbf{h}(\mathbf{x})$ therefore consists of the power balance equations in (2.2) and (2.3), as well as an equality between the voltage magnitude measurements and the respective state variable.

The DSSE approach requires a considerable amount of computational resources, and if implemented on low cost IED technology feasible for broad network distribution, this entails a significant time difference between starting the DSSE execution when entering state S2, and finishing the estimation process when leaving state S2. After convergence of the Newton method in accordance to the stopping criteria, processor 1 enters state S3. In this state the optimal set of state variables are saved in the internal storage of the proposed platform in Figure 4.2 and the trigger flag for completed DSSE is activated.

4.2.3 Execution of processor 2: Event-driven updates

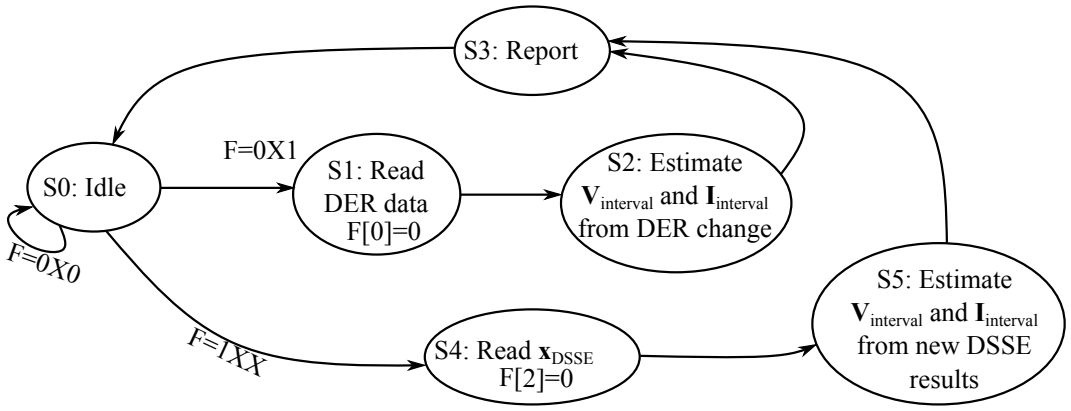


Figure 4.4: State machine representation of processor 2 execution. Source: **[Pub. D]**

The execution of processor 2 in the proposed platform flowchart shown in Figure 4.2 is per default in the idle state S0 in Figure 4.4. The transition from state S0 to any of the states S1 or S4 is activated by the least and most significant bits of the trigger flag, F[0] and F[2], as shown in Figure 4.4. To enable an event-driven update of network conditions, the platform has an internal storage as shown in Figure 4.2 where key parameters are saved and updated. These key parameters consists of:

- The network information such as line segment impedance matrices Z_l for all lines $l \in N_l$, and the location and accuracy of both periodic and event-driven metering units.
- The most recent results from DSSE execution by processor 1.

- A list of event-driven metering units sorted by the update sequence together with their recorded changes.
- Estimated branch current intervals $\mathbf{I}_{interval}$.

The latter two of these stored quantities are updated every time event-driven measurements are acquired and are used to correlate the registered network changes and their impact on the voltage magnitude conditions of the entire LV feeder. Such processing is done in the state S2 shown in Figure 4.4 and described in the following. Firstly, in the event that the flag F[0] is triggered by the arrival of a new DER reading, processor 2 shifts from the idle state S0 into S1. Here the acquired measurement is read and used to estimate the voltage interval $\mathbf{V}_{interval}$ and branch current interval $\mathbf{I}_{interval}$ updated by the reported change in DER operational conditions.

New event-driven measurement acquisition

Initially, the node n_{acq} which connect the event-driven measurement unit u to the LV network is identified through consulting the internal storage of the platform in Figure 4.2. For all data acquisitions, a full package delivery is assumed when successful. This means, the received measurement package contains active and reactive power, and voltage magnitude for all connected phases. These measurements are used to form intervals together with the respective voltage magnitude $\pm\varepsilon_u^V$, active power $\pm\varepsilon_u^P$, and reactive power $\pm\varepsilon_u^Q$ meter accuracies. These characteristics are assumed known and the intervals for voltage magnitude $V_{n_{acq}}$, active power P_u, and reactive power Q_u, are formulated as shown in (4.2) to (4.4), respectively.

$$V_{n_{acq}} = \begin{bmatrix} V^a_{n_{acq}} \pm \varepsilon_u^V \\ V^c_{n_{acq}} \pm \varepsilon_u^V \\ V^b_{n_{acq}} \pm \varepsilon_u^V \end{bmatrix} = \begin{bmatrix} Vmin^a_{n_{acq}} & Vmax^a_{n_{acq}} \\ Vmin^b_{n_{acq}} & Vmax^b_{n_{acq}} \\ Vmin^c_{n_{acq}} & Vmax^c_{n_{acq}} \end{bmatrix} \tag{4.2}$$

$$P_u = \begin{bmatrix} P^a_u \pm \varepsilon_u^P \\ P^b_u \pm \varepsilon_u^P \\ P^c_u \pm \varepsilon_u^P \end{bmatrix} = \begin{bmatrix} Pmin^a_u & Pmax^a_u \\ Pmin^b_u & Pmax^b_u \\ Pmin^c_u & Pmax^c_u \end{bmatrix} \tag{4.3}$$

$$Q_u = \begin{bmatrix} Q^a_u \pm \varepsilon_u^Q \\ Q^b_u \pm \varepsilon_u^Q \\ Q^c_u \pm \varepsilon_u^Q \end{bmatrix} = \begin{bmatrix} Qmin^a_u & Qmax^a_u \\ Qmin^b_u & Qmax^b_u \\ Qmin^c_u & Qmax^c_u \end{bmatrix} \tag{4.4}$$

For the voltage interval in (4.2), the angle of both extremes are assumed equal to the respective node voltage angles from the most recent DSSE results that are loaded from the internal storage. The established interval in (4.2) is initially used as input to the voltage interval estimate $\mathbf{V}_{interval}$ for the node n_{acq}. Afterwards, the objective of processor 2 is to evaluate the corresponding change in branch current interval of the entire feeder $\mathbf{I}_{interval}$ from the reported DER change and eventually estimate the voltage magnitude interval $\mathbf{V}_{interval}$ of the entire feeder. This is done by calculating the change in current injection interval $\Delta I_{n_{acq}}$ due to the changing physical conditions that triggered the transmission of new information from unit u at node n_{acq} through (4.5).

$$\Delta I_{n_{acq}} = I_u^{new} - I_u^{old} + \Delta I_{n_{acq}}^{load} \tag{4.5}$$

where I_u^{old} represents the current injection interval of unit u most recently reported change prior to the newly received update at I_u^{new}, and ΔI^{load} is used to consider a possible change behind the smart meters, which are only considered visible on a periodic basis. The I_u^{old} can be loaded from historic data in the internal storage of the platform and ΔI^{load} is assumed as $\pm 1A$ in this work, but is completely configurable.

In (4.5), changes in other DERs connected to n_{acq} are not considered in the estimation of the $\Delta I_{n_{acq}}$ interval. This is because all other DERs connected to n_{acq} are assumed to operate in quasi steady state conditions since no new reports of conditional changes have been reported. As such, there is a risk of error in the estimated change in current injection that depends on the defined threshold within which the DERs are able to operate without reporting a change. Furthermore, there is a risk that DERs reports are lost in transmission, which increase the possible error. To convert the received power injection measurements intervals in (4.3) and (4.4) to I_u^{new}, the voltage measurement intervals in (4.2) are utilized in the execution of (4.6).

$$I_u^{new} = \left(\frac{P_u + jQ_u}{V_{n_{acq}}} \right)^* \tag{4.6}$$

With all three quantities on the right hand side of (4.6) representing intervals, the equation must be solved $2^3 = 8$ times in order to find the minimum and maximum of I_u^{new}. Such combinations are evaluated through comparing the average voltage drop of all three phases across an arbitrary three-phase line segment, from which the combinations causing the largest and smallest voltage magnitude changes are identified.

After calculating the interval changes in the current injection at node n_{acq}, the path L_{path} consisting of all the lines connecting the node n_{acq} to the root node are identified from network topology information. With this information, the branch current interval boundaries $Imin_l^{new}$ and $Imax_l^{new}$ in $\mathbf{I}_{interval}$ of all lines l within the identified path are estimated using (4.7) and (4.8).

$$Imin_l^{new} = Imin_l^{old} + \Delta Imin_{n_{acq}} \quad \forall_{l \in L_{path}} \tag{4.7}$$

$$Imax_l^{new} = Imax_l^{old} + \Delta Imax_{n_{acq}} \quad \forall_{l \in L_{path}} \tag{4.8}$$

where the boundaries $\Delta Imin_{n_{acq}}$ and $\Delta Imax_{n_{acq}}$ are from the estimated change in current injection due to the reported change of unit u operational conditions $\Delta I_{n_{acq}}$ in (4.5).

With the updated branch currents, voltage profile boundaries $Vmin^{new}$ and $Vmax^{new}$ in the estimated voltage estimate $\mathbf{V}_{interval}$ can be estimated for all nodes n in the entire feeder and for each of the three phases. The voltage estimation is split in two steps, considering both the upwards and the downwards propagation of unit u inflicted changes in current flows. First, the upwards propagation of changes in the voltage can be calculated for all nodes $N_{upwards}$ in the path connecting the node n_{acq} to the root node. To perform this calculation, processor 2 must know the three-phase impedance matrices of the conductors in the feeder. The minimum and maximum voltages are estimated for each node in the path $N_{upwards}$, using (4.9) and (4.10) in an iterative

manner. Initially n_{acq} is represented by $n-1$ and n represents the node one step closer to the root node. The line l represents the line that connects n and $n-1$.

$$Vmin_{n}^{new} = Vmin_{n-1}^{new} + Z_l \cdot Imin_{l}^{new} \tag{4.9}$$

$$Vmax_{n}^{new} = Vmax_{n-1}^{new} + Z_l \cdot Imax_{l}^{new} \tag{4.10}$$

Following the first execution of (4.9) and (4.10), the nodes n and $n-1$ are updated to represent all nodes in $N_{upwards}$ and all lines in L_{path}, in an iterative way by moving one step closer to the root node after each estimation using (4.9) and (4.10).

Now that all node voltages in $N_{upwards}$ are estimated, the downwards propagation of change is estimated. Here the minimum and maximum of the voltage of all nodes not included in the upwards propagation path, i.e. $N_{downwards}$, is estimated using (4.11) and (4.12). This estimation process starts with the node with smallest index numbering, as the node indexation is assumed to increase with the distance from the root node. This node is represented by n and the node on the opposite end of the line l connecting n in the direction towards the root node, is represented by $n-1$.

$$Vmin_{n}^{new} = Vmin_{n-1}^{new} + Z_l \cdot Imax_{l}^{new} \tag{4.11}$$

$$Vmax_{n}^{new} = Vmax_{n-1}^{new} + Z_l \cdot Imin_{l}^{new} \tag{4.12}$$

where the nodes n and $n-1$ are updated to represent all nodes in $N_{downwards}$ and all lines not included in L_{path}, through removing the newly estimated node from $N_{downwards}$ and defining the new smallest indexed node in $N_{downwards}$ as the node n in (4.9) and (4.10).

Following the estimation of the node voltage of the entire feeder, the processor transits from state S2 to S3. Here the results are saved in the internal storage and made available for utilization by the network operator. In the event that new DSSE results are estimated, thereby activating the flag F[2] in Figure 4.3, processor 2 can re-evaluate the network conditions that have been estimated during the DSSE execution, and thereby aligning the internal storage to the newly estimated state variables. From Figure 4.4, it is apparent that the processor prioritize transition to state S4 rather than to S1, since the opposite would entail an unnecessary redundant processing of the new event-driven measurements if these concise with processor 1 finishing the DSSE execution.

New DSSE results

The new DSSE results are read from the optimal solution vector $\mathbf{x}_{DSSE}$ as illustrated in state S4 of Figure 4.4. After transitioning to state S5, processor 2 updates the estimated branch current interval of all lines stored in the internal database. This update is conducted through application of Ohms' law and affects the network condition monitoring in (4.7) and (4.8). Besides an update of the database, the new DSSE results affects the monitoring of changes from receiving new event-driven measurements. This means that all recorded changes between the time that the DSSE was initiated $t_{DSSE,start}$ and the time it finished $t_{DSSE,finish}$ must be re-evaluated to update the network conditions appropriately.

The re-evaluation is enabled by assuming that all equipment connected to event-driven metering devices have constant impedance and that the characteristics of the recorded changes are saved in the internal storage of the proposed platform. With this assumption, each recorded change is processed in the same way as in state S3 described above, with an impact from the updated DSSE results in two ways. Firstly, the initial estimation of changes in the current contribution from unit u is affected by new DSSE results because of the assumed voltage angles equal to those of the DSSE results described in (4.2). Secondly, the branch current interval updates in (4.7) and (4.8) utilize the most recent estimated branch currents, which can be derived from DSSE results from the estimation of voltage magnitude and angle for all LV network load points and knowledge about network impedance matrices. This way, the DSSE execution in processor 1 supports the interval estimation of processor 2 by aligning the estimation foundation to converged DSSE estimates. After recalculating all effects of recorded changes, the processor returns to the idle state S0 through state S3, where the results are updated and made available for the network operator.

4.3 Demonstration and performance evaluation

The proposed platform is implemented in MATLAB and tested with a simulation of a LV distribution feeder from the Bornholm Island shown in Figure 4.5. For the load points in the LV network, residential consumption and DERs are distributed with the quantities shown in Table 4.1. The distribution of DERs represents a future scenario where 100% of the households have installed energy systems consisting of a PV plant and a battery storage unit. The batteries are assumed to store excess PV production and discharges when household consumption exceeds the local production. Furthermore, approximately 68% of the residential load points are assumed to have EVs connected.

All loads are considered three phase and operate in unbalanced conditions. Each EV is considered to charge through three-phase chargers with rated currents of either 16 or 32 A. All PV plants and batteries are rated at 5 kVA and are set to operate with $cos\phi(P)$ reactive power control as illustrated in Figure 2.3c following a linear relationship from unity power factor at 50% rated active power to 0.9 lagging power factor, from a generator perspective, at 100% rated active power. Furthermore, the event-based DER readings are send every time the active power operating point changes with more than predefined thresholds. These thresholds are assumed ± 50 W for PV plants and batteries, and ± 100 W for the EV chargers. For the latter DER type, the threshold is chosen arbitrarily as the EV chargers are modelled to either charge at 0 or 100% of the rated charging current. For both PV and battery inverters, the sensitivity threshold is chosen equal to the assumed metering accuracy of $\pm 1\%$ of the rated power.

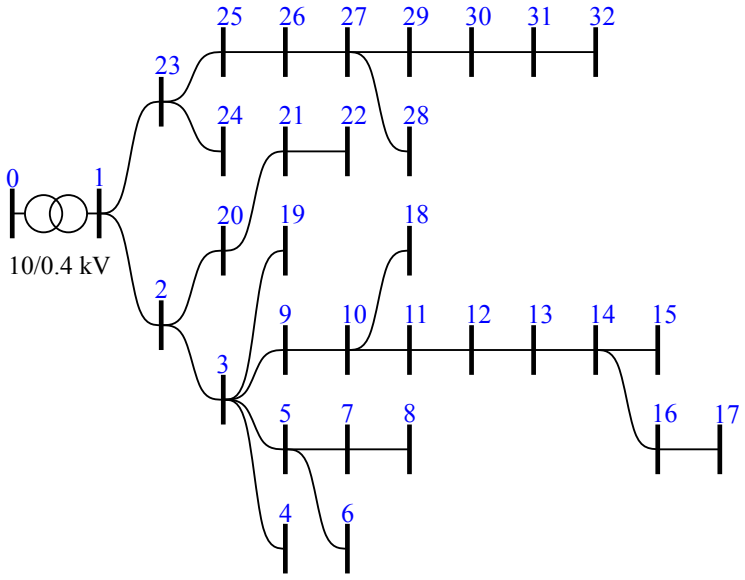


Figure 4.5: Low voltage feeder on Bornholm Island used as a test case

Table 4.1: Load and DER distribution among nodes in the Bornholm LV feeder

Node	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Loads	0	2	2	1	3	2	4	2	3	1	3	1	2	5	2	4
EV	0	1	0	1	2	2	2	2	3	1	2	1	2	0	1	2
PV	0	2	2	1	3	2	4	2	3	1	3	1	2	5	2	4
Battery	0	2	2	1	3	2	4	2	3	1	3	1	2	5	2	4

Node	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Loads	4	2	6	1	1	1	0	3	2	4	1	1	1	2	2	3
EV	3	2	4	0	1	1	0	3	1	4	1	1	1	2	0	2
PV	4	2	6	1	1	1	0	3	2	4	1	1	1	2	2	3
Battery	4	2	6	1	1	1	0	3	2	4	1	1	1	2	2	3

In the following simulation based scenarios, all load points and DERs are assumed to follow generic load and generation curves that are randomized for the different distributed units. With the LV network in Figure 4.5, the distribution of DERs presented in Table 4.1, and the considered thresholds defining the sensitivity of the event-driven transmission setting, the number of registered changes during a single day is found as 16,061. This high number of changes is only used for demonstrating the capability of the proposed platform and does not represent a requirement of necessary changes throughout a day for the approach to work. The temporal distribution of these changes are shown in Figure 4.6.

In Figure 4.6 the registered changes are aggregated on a 1-minute time resolution and the maximum number of changes within a single 1-minute period is equal to 34, which is equivalent to 18% of the total number of DERs in the considered LV feeder case study. This relatively high percentage of registered changes occurs 4 times between hours 14 and 16. The component type representation of changes is also visible in Figure 4.6. Here it can be observed that the PV inverters register and transmit information due to changes in the physical conditions, i.e. solar irradiance and

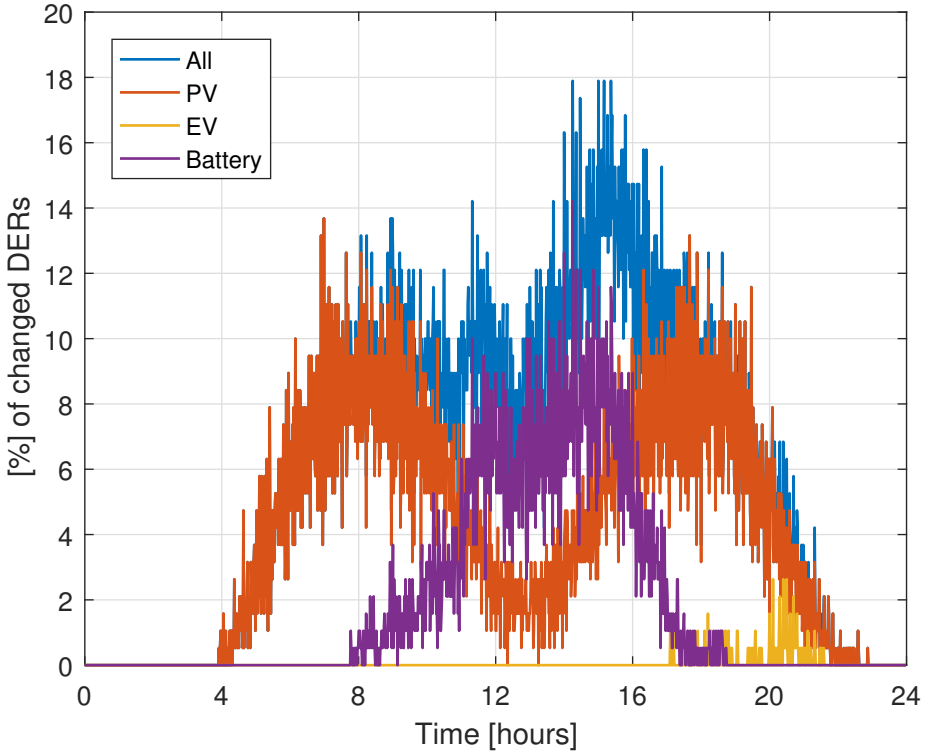
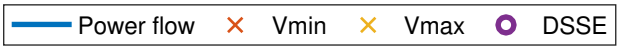


Figure 4.6: Temporal and type distribution of registered changes in simulating the Bornholm LV feeder

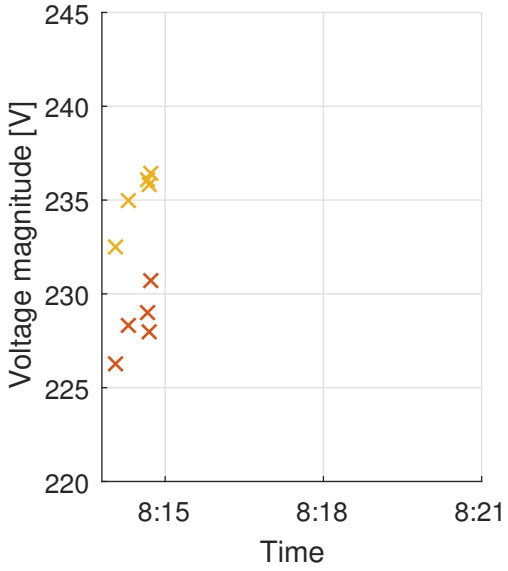
temperature, in particular during the morning and the afternoon, while less changes happen during midday. When the PV generation exceeds the local consumption, the battery starts storing the excess energy production as visible from the number of battery condition changes from hours 8 to 19. Finally, the EVs are modelled to return home and connect to the residential feeder in Figure 4.5 from around hour 17.

4.3.1 Demonstration of platform interval estimation

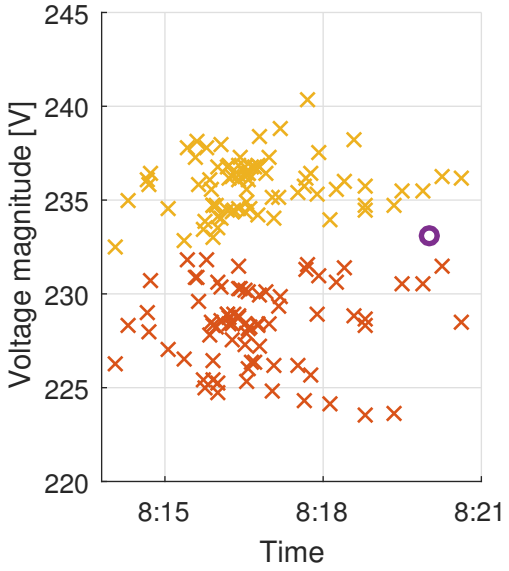
The demonstration of the proposed platform implemented for monitoring the LV feeder in Figure 4.5 is performed at a time interval between 8:14 and 8:36 of the described simulation study. As the DSSE is considered executed periodically every 15^{th} minute, this demonstration contains two execution of processor 1. Furthermore, a 1% probability of data loss is assumed meaning there is a 1% risk of loosing the periodic and event-driven measurements as these are send through the ICT infrastructure. The objective of this demonstration is to illustrate how the bi-level configuration of the proposed platform enables LV network monitoring with limited processing capabilities. This is highlighted by showing the estimated conditions in a time series plots at time instances where the DSSE algorithm on processor 1 is initiated and when it has finished its execution. To demonstrate this capability, an observation of the node 6 phase a voltage magnitude is shown in Figure 4.7.



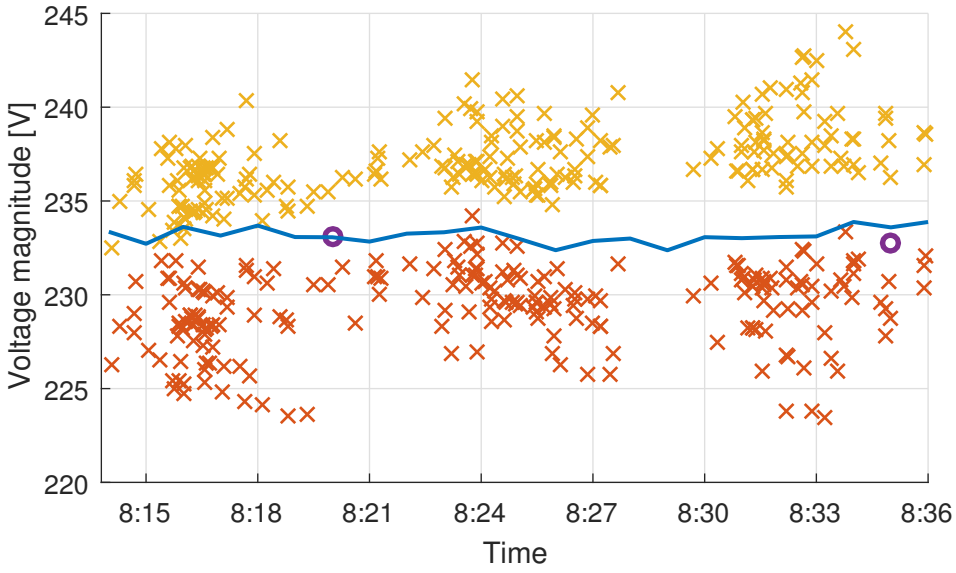
(a) Plot legend of bi-level platform demonstration



(b) Zoomed view of estimated intervals from acquired measurements at nodes 14, 26, 21, 2 and 31



(c) Zoomed view of estimation with DSSE execution and DSSE deterministic results



(d) Full time series illustrating two DSSE executions and the power flow results

Figure 4.7: Demonstration of voltage magnitude interval estimation of phase a at node 6 using the bi-level LV network monitoring platform in time interval 8:15 to 8:36. Source: **[Pub. D]**

The illustrations in Figure 4.7b and Figure 4.7c are zoomed to the time interval between 8:14 and 8:21, and Figure 4.7b show the first 5 estimated intervals between 8:14 and 8:15. These are calculated from the reporting of updated conditions of 5 PV plants at nodes 14, 26, 21, 2, and 31, meaning their active power generation has changed relative to the previously reported conditions by a quantity larger than the predefined threshold as explained with the event-driven transmission setting in Figure 4.1. At 8:15, the platform timer triggers processor 1 to start executing the DSSE algorithm by changing its state from S0 to S1 in Figure 4.3.

With limited processing power, the DSSE execution takes a considerable amount of time as seen by the time difference between the DSSE start time 8:15 and the return of the deterministic voltage magnitude estimate represented by the purple circle in Figure 4.7c at approximate 8:20. It is worth remembering that the deterministic DSSE results represent the estimated network conditions at 8:15 because the input data set is based on periodic metering acquisition at 8:15. In addition, Figure 4.7c show how the proposed platform is capable of estimating voltage magnitude intervals during the DSSE execution because of the bi-level processing architecture.

The complete time series from 8:14 to 8:36 used in this demonstration is shown in Figure 4.7d together with the power flow voltage profile results in blue. Here the power flow results are calculated every minute, between which the conditions are assumed to follow a linear relationship. In the illustrated time period, two DSSE executions are initiated at 8:15 and 8:30, and finishes approximately 6 minutes after. For the first DSSE result representation, the power flow voltage profile at 8:20 looks accurately estimated. However, the DSSE estimation results represent the 8:15 power flow conditions and a careful investigation shows a small estimation error is visible. The same conditions apply for the evaluation of the second DSSE execution. For the demonstrated time series, the network conditions are not severely volatile. But in modern distribution networks, with many DG and electrified services, the changes can be severe as seen in the illustration of node 6, phase a time series between 19:40 and 20:40 shown in Figure 4.8.

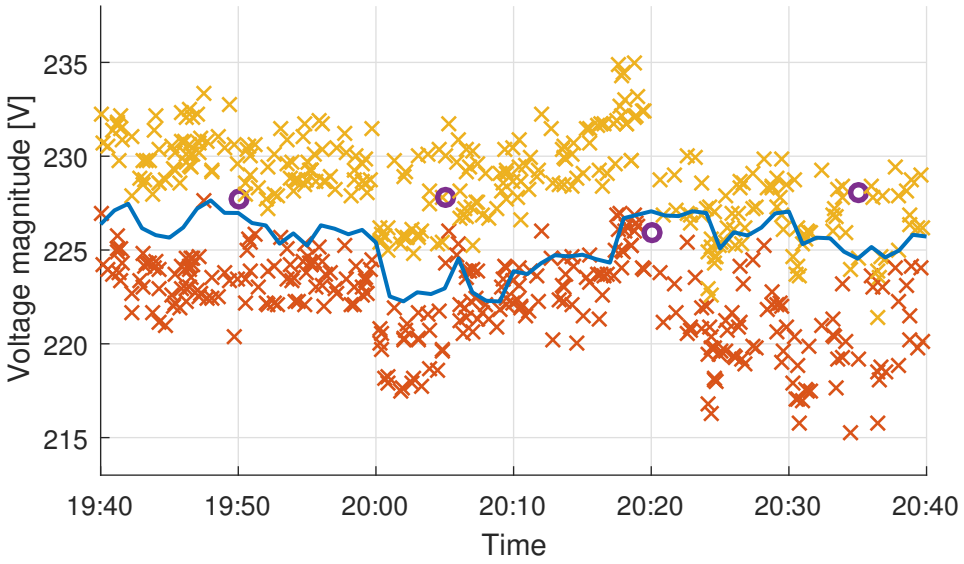


Figure 4.8: Bi-level platform demonstration in volatile conditions between 19:40 and 20:40 with legend in Figure 4.7a

The demonstration of volatile network conditions in Figure 4.8 reveals how the DSSE estimation results can be diminished due to the changing conditions. Such effects are especially true for the DSSE results at 20:05 which represent the conditions at 20:00, where the DSSE execution was initiated. During the 5 minutes of execution, the power flow voltage profile has changed considerably. These changes are captured by the event-driven measurements as seen by the estimated intervals between 20:00 and 20:05.

While it is apparent that the proposed platform gives a more frequent overview of network conditions than the DSSE execution alone, the proposed platform is not completely accurate in its attempt to encapsulate the power flow voltage magnitude profile. In Figure 4.7d, there are 5 occasions between 8:15 and 8:18 where the maximum voltage interval boundary is smaller than the power flow profile, and a single occasion at approximately 8:25 where the minimum boundary is estimated higher than the power flow results. Furthermore, in more volatile operating conditions, as shown in Figure 4.8, the estimated intervals are more likely to exclude the power flow voltage profile due to the greater DSSE accuracy error.

4.3.2 Performance evaluation in different conditions

Evaluating the performance of the developed bi-level processing platform for LV network monitoring is done through analyzing its ability to contain the voltage magnitude at all nodes and phases during a single day of operation. The performance is therefore evaluated through the statistics of the estimated range at all nodes and phases in the network. Furthermore, the information availability limitations are considered through analyzing the platform performance with different scenarios of data loss probability.

First of all, a statistical overview of the platform performance compared to that of the processor 1 DSSE algorithm itself is given in Table 4.2. The results are found by simulating the LV feeder in Figure 4.5 for an entire day with the mentioned operating conditions, and only changing the data loss probability to values of 0%, 1%, 5%, 10% and 25% as seen in the first column of Table 4.2.

Table 4.2: Interval estimation error statistics at different loss of data probability scenarios

Data loss Probability	Registered DER changes (Intervals)	Interval errors	Bi-level platform $\|V\|$ error $< 1\%$	Bi-level platform $\|V\|$ error $\geq 1\%$	Bi-level platform Max error	Processor 1 DSSE $\|V\|$ error $< 1\%$	Processor 1 DSSE $\|V\|$ error $\geq 1\%$	Processor 1 DSSE Max error
0%	16,061 (1,541,856)	18,503 (1.20%)	18,089 (97.76%)	414 (2.24%)	5.73 V (2.48%)	90.87%	9.13%	12.48 V (5.40%)
1%	15,890 (1,525,440)	20,716 (1.36%)	20,272 (97.86%)	444 (2.14%)	5.08 V (2.20%)	90.52%	9.48%	12.39 V (5.37%)
5%	15,254 (1,464,384)	28,229 (1.93%)	27,312 (96.75%)	917 (3.25%)	5.85 V (2.53%)	89.01%	10.99%	12.59 V (5.45%)
10%	14.482 (1,390,272)	31.438 (2.26%)	29.887 (95.07%)	1.551 (4.93%)	5.75 V (2.49%)	88.04%	11.96%	12.75 V (5.52%)
25%	12,014 (1,153,344)	72,433 (6.28%)	63,465 (87.62%)	8,968 (12.38%)	9.78 V (4.23%)	78.79%	21.21%	14.91 V (6.46%)

In the second column of Table 4.2, the number of registered DER changes are summarized. Here it can be seen that with 0% probability of data loss, the number of registered changes is aligned with the temporal distribution shown in Figure 4.6. The numbers within the parentheses are the quantity of voltage magnitude intervals that are estimated based on the number of registered changes. For 16,061 DER changes, 32 LV network nodes in Figure 4.5, and three phases means that the total number of intervals that are estimated by processor 2 during the 24 hour simulation case is 1,541,856. Comparing the number of registered changes for the remaining data loss probability scenarios, reveals that the probability of loosing event-driven transmissions is aligned with the considered scenarios.

In the third column of Table 4.2, the total number, and percentage, of estimated intervals that do not contain the power flow voltage profile is shown. Such error can be because of the assumed residential load change ΔI^{load}, a large deviation in initial DSSE estimation accuracy, or unregistered changes in other DERs within the network, either due to data loss or due to small changes within the threshold boundaries. From comparison between the different data loss probabilities, it is apparent that with lower information availability, the accuracy of the proposed platform decreases. At a information availability corresponding to less than 10% data loss probability, however, the platform is able to contain the power flow voltage magnitude profiles in about 98% of the estimated intervals.

Columns 4 to 6 in Table 4.2 presents how far the power flow voltage magnitude profiles are outside the processor 2 estimated intervals. For all data loss probability scenarios, it is apparent that the majority of the errors are relatively small, less than 1 % of rated voltage magnitude equal to 230.94 V. Furthermore, while the occurrence of larger errors increases with higher data loss probabilities, the maximum error between the estimated intervals and the power flow resulting profiles is relatively similar for the data loss probabilities between 0 and 10%.

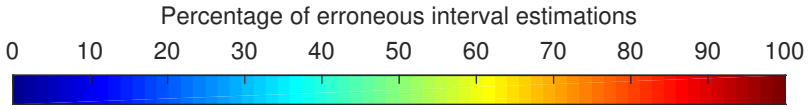
In comparison, columns 7 to 9 in Table 4.2 shown the accuracy of the deterministic voltage magnitude estimation done by the processor 1 DSSE algorithm. The difference between the column 4 and 7 clearly shows the strength of the interval representation of results compared to the deterministic representation. With the interval representation of estimated network conditions, a measure of the information integrity is entailed, and as the intervals consider multiple possible operating conditions, the maximum error between the estimation error and the actual network conditions is smaller compared to the deterministic DSSE results. Furthermore, the comparison in Table 4.2 show that with the DSSE alone, it is expected that the estimated results will container a greater error, and that a greater number of relatively large estimation errors is expected compared to the combined bi-level platform.

Correlation between measurement nodes and nodes with estimation errors

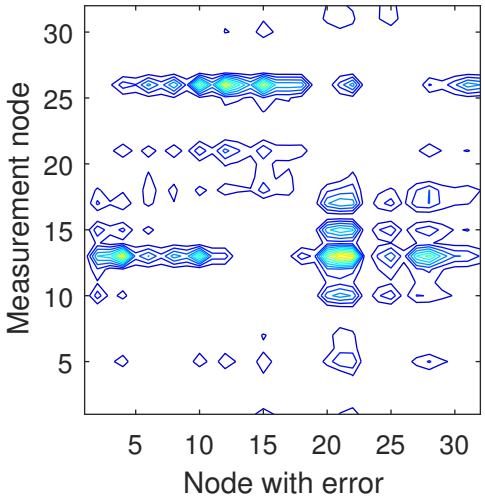
A deeper analysis of the estimated intervals for which the power flow voltage magnitude profiles is excluded, reveals certain LV network characteristic vulnerabilities of the proposed platform. In Figure 4.9, three contour plots are used to illustrate the number of times an interval estimation based on a certain measurement node on the y-axis, causes an error in the estimated interval in LV network node in the x-axis. The intensity of the combination is based on the percentage of the estimations that are erroneous based on the different measurement nodes as shown in Figure 4.9a.

Evaluating the combinations between nodes with error and measurement nodes during a 0% data loss probability scenario in Figure 4.9b show that in particular when measurements from nodes 13 and 26 are acquired, the proposed platform struggles with containing the voltage magnitude profile within the interval boundaries. The largest percentage of erroneous intervals is for nodes 4, 20, 21 and 22 when measurements are acquired from node 13, and at nodes 10, 12 and 15 when estimated based on measurements from node 26. For such combinations, an investigation of the relative node locations in Figure 4.5 and the distribution of load points described in Table 4.1 show how the electrical distance between nodes affect the estimation accuracy.

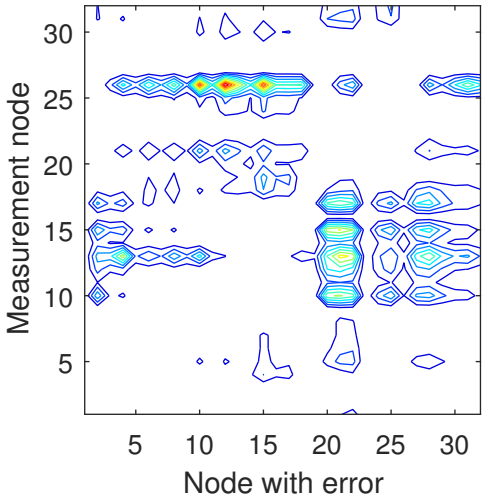
True for all the nodes experiencing erroneous interval estimates is that only a small amount of resources are connected at these points. This means that the physical conditions at these points are updated less frequently, limiting the platforms ability to correctly estimated the conditions when processing acquired measurements from distant network nodes. These two factors are seen more visible in Figure 4.9c and Figure 4.9d, where the limited information availability worsens the platform ability to estimate correctly. Comparing the error distribution in the three different data loss probability scenarios shows how the problematic areas remain largely the same and only the intensity changes. A way of avoiding such errors could therefore be to split the network in different sections used to limit the distance between measurement node and nodes with estimated conditions.



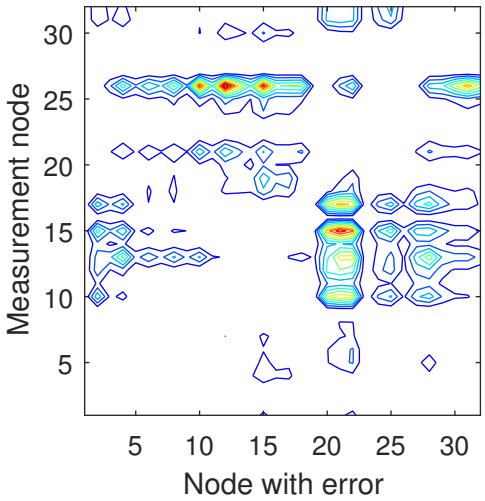
(a) Intensity representation of combinations between measurement nodes and nodes with error



(b) 0% data loss probability



(c) 5% data loss probability



(d) 10% data loss probability

Figure 4.9: Network distribution of erroneous estimated intervals, with data loss probability of 0%, 5% and 10 %. Source: **[Pub. D]**

Interval range in different time scales

The added value of the event-driven interval estimates for network operators is seen in Figure 4.7 through the increased temporal overview of network conditions compared to relying solely on the DSSE estimates, and compared to the voltage interval estimation method proposed in chapter 3. The utilization of the frequent estimates from the proposed platform could be challenging if a centralized processing topology shown in Figure 2.2a is assumed responsible for assessing the operational security of numerous LV networks because of the asynchronous acquisition. Furthermore, as seen by the previous work in chapter 3 it is beneficial to aggregate intervals that are estimated within relatively short time periods. Such aggregation can narrow the estimated range and give a more detailed overview of network conditions. For the proposed platform and the utilized simulation case study with assumed 1% probability of data loss, the statistics of estimated interval ranges are summarize for two representation cases in Figure 4.10. Firstly, considering individual estimated intervals in Figure 4.10b, and secondly, considering a narrower estimate through aggregation of estimates within 1-minute time periods in Figure 4.10c.

A direct comparison between the stand-alone estimated intervals in Figure 4.10b and those aggregated across a 1-minute resolution in Figure 4.10c, reveals several characteristics. First of all, more than 95% of all estimated intervals have a voltage magnitude range narrower than 10% of rated LV network voltage magnitude, equal to 23.1 V. Secondly the narrowest possible range of estimated intervals at any node in the network is approximately 2% of the rated voltage i.e. 5 V corresponding to the metering infrastructure accuracy of $\pm 1\%$ of rated voltage. Thirdly, the aggregated intervals have much narrower voltage magnitude range, and finally, in less than 5% of the aggregated intervals the minimum boundary is lower than the maximum boundary seen as negative interval ranges in Figure 4.10c.

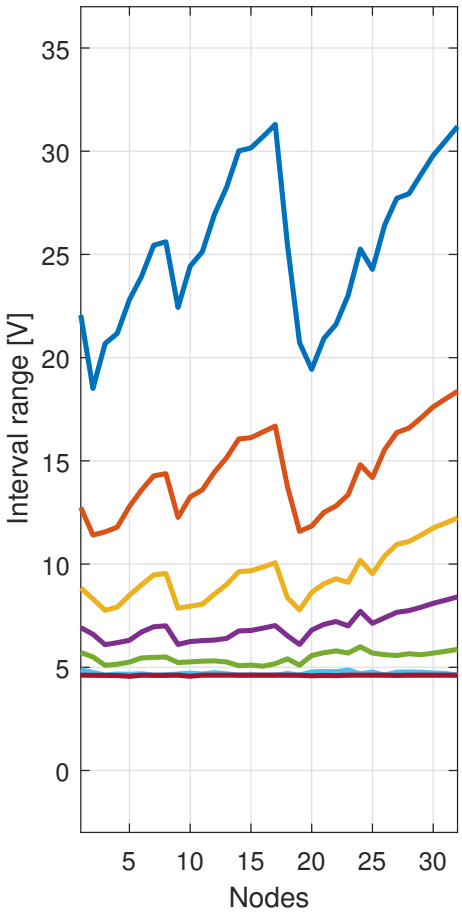
While the narrower interval ranges provide better details of network conditions, it is important to review the statistics of how many of these aggregated intervals that encapsulate the power flow voltage magnitude profiles. Such statistics are represented in Table 4.3 where only 1-minute periods with estimations are considered, i.e. periods where a least 1 event-driven measurement is received and processed by processor 2 in the proposed platform, which depend on the information availability and changes in the neighbouring energy systems.

Table 4.3: Statistics of interval estimation error for 1-minute aggregated intervals at different loss of data probability scenarios

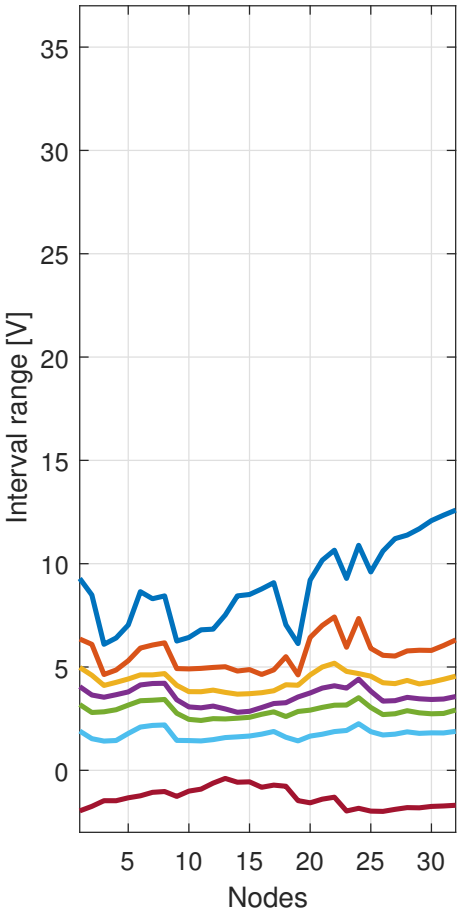
Data loss probability	0%	1%	5%	10%	25%
Erroneous intervals (percentage)	5,325 (5.13%)	5,689 (5.48%)	7,018 (6.79%)	8,455 (8.15%)	18,567 (18.14%)
$\|V\|$ error $< 1\%$ (percentage)	5,179 (97.26%)	5,535 (97.29%)	6,705 (95.54%)	8,083 (95.60%)	16,052 (86.45%)
$\|V\|$ error $\geq 1\%$ (percentage)	146 (2.74%)	154 (2.71%)	313 (4.46%)	372 (4.40%)	2,515 (13.55%)
Max error	5.73 V	5.08 V	5.85 V	5.56 V	9.78 V

From Table 4.3, it is clear that the aggregated intervals, with narrow range encapsulates the power flow voltage magnitude profile in 95% to about 80% of the 1-minute periods with registered and

(a) Plot legend of different statistics quantities, where Q abbreviates *Quantile*



(b) All estimated intervals



(c) Narrowest estimate in 1-minute periods

Figure 4.10: Statistics of the interval range for phase a at all nodes considering a 1% chance of data loss. Source: **[Pub. D]**

processed changes, depending on the data loss probability. Furthermore, the maximum difference between the interval boundary and the outside power flow results is less than 6 V for information availability conditions corresponding to 10% data loss, and the vast majority of the errors is less that 2.3 V. The benefits of aggregating the estimated intervals in short time-periods and their relative performance in encapsulating the actual voltage magnitude, provide useful tools for network operators in gaining an overview of the network conditions with a higher time resolutions than the 15-minute periodic execution of DSSE.

4.4 Conclusion

This chapter presents the developed bi-level interval estimation platform for periodic and event-driven execution as a novel alternative to existing DSSE application approaches for monitoring of LV network conditions. The proposed platform consists of two processor with divided responsibility of processing information gathered through periodic and event-driven transmission settings, respectively. One processor handles the periodically acquired measurements through an execution of a DSSE model and algorithm, and the second processor handles the event-driven measurements. The event-driven measurements are processed to estimate the impact of changes on the entire LV feeder as intervals.

The proposed bi-level processing architecture satisfies the high level research approach formulated in subsection 2.3.2, and entails useful synergies between the two processors. The periodically executed processor provides estimated foundation for the processor handling event-driven measurements on a regular basis. Furthermore, with frequently estimated interval conditions used to replace missing entities in the DSSE input data set, the DSSE algorithm is guaranteed a high quality data set. Such synergy allows network condition estimation in situations where information availability is limited due to ICT infrastructure performance and information confidentiality restrictions.

With a simulation model of a LV feeder with high integration of DG units and other DERs that operate according to randomized generic profiles, the proposed approach is demonstrated and its performance is evaluated through a statistical analysis. The demonstration reveals how the bi-level architecture of the platform enables frequent interval estimates, and shows its ability to provide such estimates during the execution of the DSSE algorithm. Furthermore, a demonstration of volatile network conditions shows how the DSSE results can be diminished due to the long processing time required. One key observation from the demonstration was how, in some cases, the proposed platform was unable to estimate intervals that encapsulate the real voltage profile of the network.

The performance of the bi-level interval estimation platform was evaluated with different information availability conditions, represented through scenarios with different data loss probabilities. Such scenarios revealed that only 2% of all estimated intervals excluded the voltage profile during a data loss probability greater than 5%, and that the error between the interval boundaries and the power flow voltage magnitude was less than 1% of rated voltage magnitude for about 90% of the erroneous intervals. The distribution of erroneous intervals in terms of nodes with interval estimation errors and nodes from which the event-driven measurement was sent, revealed performance dependencies on the distance between nodes and the number of node connected reporting devices.

In the end the benefit and accuracy of aggregating estimated intervals in short time-periods with the objective of narrowing the estimated interval were demonstrated. With a 1-minute time resolution of the interval aggregation, the resulting magnitude range reduces greatly. One disadvantage however, was that the aggregation entailed a risk of negative interval range, meaning the minimum boundary was larger than the maximum boundary. Such conditions were rare but should be handled before real life implementation of the proposed platform. In terms of estimation accuracy, the aggregated intervals were analyzed through statistics of interval estimation errors. These showed that less than 10 % of the aggregated intervals were erroneous with a information availability corresponding to 10% data loss probability.

With the proposed LV network monitoring platform, network operators can gain an overview of the operational conditions at the end of the electricity supply. Such monitoring is seen as a prerequisite for implementing different smart grid approaches in such networks. In particular, the developed monitoring platform allows an assessment of network conditions during and in-between DSSE execution through the utilization of two independently executing processors. With a higher temporal granularity of monitoring the network conditions, compared to periodic execution of DSSE, the network operator can identify possible problems within the LV network, e.g. voltage magnitude or unbalance issued. As such, the output of the proposed platform can be used as input to network operator decision making on when and where to make protective actions that can secure the network against hazardous operation conditions. Compared to the proposed network monitoring approach in chapter 3, the developed platform offers both a narrower range and more frequent estimate of network conditions. Such advantages are achieved through handling the assumed greater availability of information in terms of data sources and attributes. As such, the developed LV monitoring platform can be viewed as an enabling technology for smart control of distribution network assets.

Part III

Protection of DG controls

CHAPTER 5

Cyber error detection with distributed processing

This chapter presents the formulation and application of functional modeling for wind turbine generator representation and the demonstration of a cyber error detection system integrated in a distributed processing topology. As emphasized by the research motivation in section 1.3, the protection of DG controls against cyber-physical disturbances is increasingly important as more of the power system control capabilities are shifted from large centralized generators. The distributed cyber error detection system presented here utilize known information integrity protection techniques discussed in subsection 2.2.2 while following the high level research approach introduced in subsection 2.3.3.

Firstly, different approaches to modeling physical systems are discussed from an application perspective, leading to the formulation of a functional model of a wind turbine generator. Secondly, the requirements and strategy of implementing a cyber error detection system using a distributed processing topology illustrated in Figure 2.2c are presented. Based on the functional model representation of a wind turbine generator, the establishment of a state estimation model is introduced as a central part of the cyber error detection system. Afterwards, a description of how the cyber error detection system is implemented on a commercially available distributed processing device using a robust estimation algorithm is presented. The distributed cyber error detection system is tested in stand-alone scenario for different measurement error characteristics shown in Figure 2.4. Afterwards, the performance of the distributed cyber error detection system is evaluated in a simulation environment of a WPP, where its ability to protect the DG control against integrity attacks as illustrated in Figure 2.1 is investigated during active power curtailment. Finally, the demonstrated cyber error detection system is summarized and reviewed from system and DG owner perspectives. The majority of this chapter is based on published material in [**Pub. F**] and [**Pub. A**], with minor changes to coherently fit into the framework of this thesis.

5.1 Physical system modeling

Modeling physical systems, such as wind turbine generators and other DG units, enables a study and representation of their behavior in different environments. With the integration of numerous and vastly diverse DERs, exact representation of each type becomes unfeasible due to the required effort. Instead, different modeling approaches have been proposed and investigated; empirical, physical, and functional.

The three modeling approaches are compared in [156], and from a DER representation perspective, each have advantages and disadvantages. The empirical approach is based on pattern recognition from previous observations, i.e. historic data, and is sometimes referred to as a black-box approach.

This modeling approach requires only limited domain knowledge but a considerable amount of historic information about the system behaviour. An example of this approach is the use of artificial neural networks, which has been proposed for different power system applications as presented in [157]. However, the efficiency of the empirical models depends strongly on the quality of the training data set, and its ability to represent all likely operating conditions, as it restricts the model representation to specific operational conditions [158]. Therefore, the black-box approach may fail to accurately identify and represent the performance of the system, and possibly react arbitrarily to unrecognized patterns [159].

Opposite empirical modeling, the physical modeling approach requires extensive domain knowledge and some benchmark representation of operational performance as it is based on first principles, i.e. differential equations. This approach is used in different dynamic power system modeling applications [160], and can be highly detailed and even compensates for unobserved quantities. However, the low abstraction level entails high computational requirements, and parametrization challenges at different operation situations.

As an alternative, the functional modeling approach is based on an analysis of physical phenomenons and cause-effect relations within the system and therefore requires domain knowledge on a high level of abstraction. So far, functional modeling has experienced limited application within power system modeling, as its main application has been within process control and fault diagnosis [161, 162]. One of the few applications of functional modeling in power systems is found in [163], where the modeling approach is used to explain how functions within power system frequency control are related in the complex control system.

To summarize, the empirical modeling approach has the ability to indicate the system operation but its dependency on quality of historic data and limited inclusion of domain knowledge entails risks if implemented as part of operation and control applications. In comparison, the highly detailed representation of physical modeling makes it feasible for such applications and it is traditionally for control design and transient performance studies. With an objective of detecting cyber errors by analysis of information from physical system relations and thereby provide an accurate indication of the wind turbine operational conditions, the high abstraction level of functional modeling gives a suitable foundation from which a state estimation model can be established. Furthermore, the functional modeling approach is previously shown able to represent implicit control knowledge that could be missed by the limited reasoning offered by empirical modeling and the low abstraction level of physical modeling. Therefore, the approach offers a qualitative interpretation of the physical processes, while maintaining an overview of the system.

5.1.1 Functional model of wind turbine generator

The concept of functional modeling originates from software development, with the purpose of generalizing a software application to enable implementation in different programming languages. The functional model of software development describes the desired functions of the application and explains what happens to objects within the application. It can be understood as a representation of pseudo-code using flow charts and other graphical tools [164]. The functional modeling approach was later applied to fault diagnosis where it has been used to capture the key physical relations within a specific system. Examples include a simple water mill in [165] and a nuclear power plant in [156, 161].

In order to establish a functional model of a system, knowledge about its entirety is required, which includes, but is not limited to, the overall function of the system and internal sub-processes, performance standards, and the relations among sub-processes. The model is formulated based on a high level abstraction of an object that helps operators in handling the complex dynamics and relations without loss of details [165].

The representation of a physical system through functional modeling is initiated through a method called functional decomposition. As the name suggests, the principle is to consider the overall system and decompose its function into sub-functions in an iterative way [164]. In [166], the functional decomposition process is demonstrated for a power system. When decomposing the functions of a system, relations between the different functions are revealed. There are different methods for graphical representing of these relations and functions of a specific system, the methodology used in this paper is Multilevel Flow Modeling (MFM), which relates the goals, functions and relations of a system [165].

The MFM methodology forms a visual representation of the dependencies between the different functions of a process through utilizing different graphical components shown in Figure 5.1. What characterizes the MFM methodology is how it separates the functions of a physical system in terms of mass or energy handling functions, and enables a meaningful way of representing advanced control processes. The functions handing mass are collected in Mass Flow Structures (MFS's) and can represent a physical transportation, separation, storage, etc. within the process. Similarly, the Energy Flow Structure (EFS) characterize functions that transports, transforms, converts, etc. energy. The separation helps improve the reasoning of the process functions, and relations.

In fault diagnosis, MFM is used to monitor an industrial process by representing each function by a signal value and to evaluate its operation according to predefined limits. If a process is equipped with control capabilities, through one or more actuators, a violation of an operational limit can be handled through appropriate actions. In MFM, controls are represented in Control Flow Structures (CFS's), which evaluate the status of a function and performs the appropriate actuation on a function to change the process operation.

Multilevel flow modeling representation of wind turbine generator

The functional model formulation of a wind turbine generator through MFM graphical representation is done through analysis of the a Doubly Fed Induction Generator (DFIG) wind turbine. An overview of the wind turbine energy conversion process is shown in Figure 5.2a, where each of the conversion steps are separated to improve readability. One of the central functions within the wind turbine, is the balancing between the electric power output and the mechanical power input.

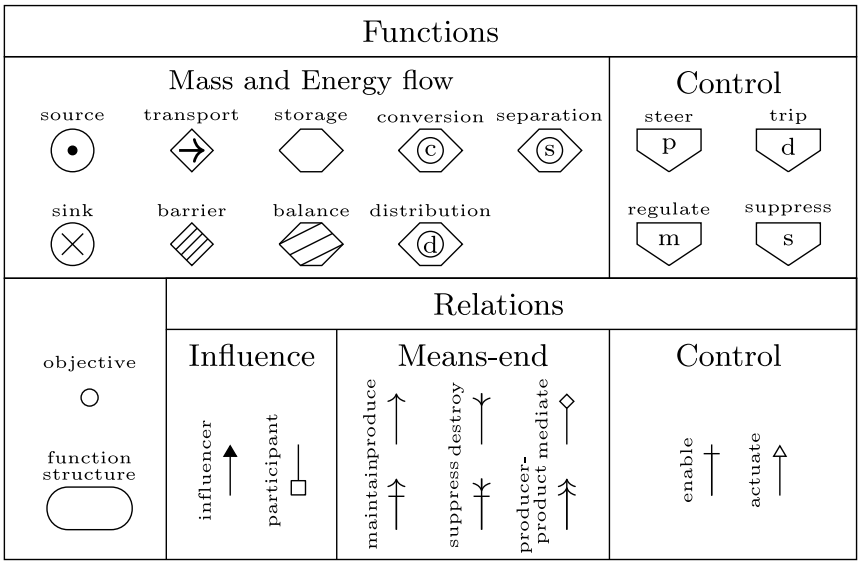


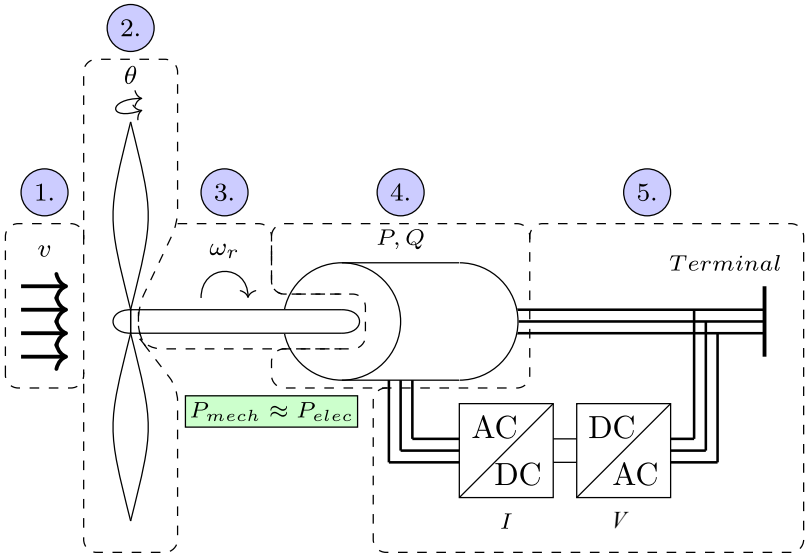
Figure 5.1: Multilevel flow modeling graphical representation of functional modeling. Source: [**Pub. A**]

This behavior is indicated in Figure 5.2a by the approximate equation to represent its interaction with the entire conversion process.

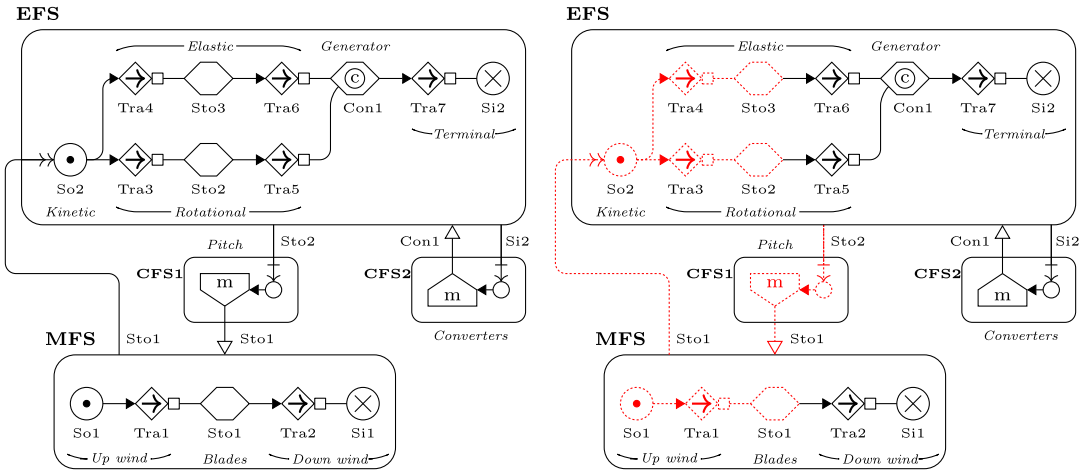
In the first step of Figure 5.2a, the wind intercepted by the turbine blades, is characterized by its speed, v measured in meters per second. In MFM, the flow of wind is modelled as the mass flow shown in the MFS in Figure 5.2b using the graphical representation tools in Figure 5.1. The upstream and downstream wind is modelled as a source, *So1* and a sink, *Si1*, respectively. The wind is transported towards and away from the turbine blades through the transport functions *Tra1* and *Tra2*, respectively. As the wind is intercepted by the wind turbine blades in the second step of the process in Figure 5.2a, the mass of air is momentarily stored at the point of interception. Therefore, the blades are characterized in the MFM model through the storage function, *Sto1* in Figure 5.2b.

Here, a means-end relation represents how the stored wind at the blades can be interpreted as a source of kinetic energy, *So2*, as shown in the EFS. The kinetic energy is transformed into rotational and elastic energy through the connection between the turbine hub and the shaft as indicated by the third step in Figure 5.2a. In the MFM model in Figure 5.2b, the energy transformation from kinetic to rotational and elastic energy is represented by *Tra3* and *Tra4*, respectively. Afterwards the rotational energy is stored in the rotational mass, *Sto2* and the elastic energy is stored in the twisted shaft, *Sto3*.

In Figure 5.2a, the rotational energy is represented by the rotational speed, ω_r measured in radians per second, while the elastic energy is included in the balancing between mechanical power, P_{mech}, and electrical power, P_{elec} both with the unit of kW. The rotational and elastic energy is transported towards the induction generator through *Tra5* and *Tra6*, respectively, followed by the conversion into electric energy modelled by *Con1* in Figure 5.2b. In the fourth step of Figure 5.2a, the conversion to electric energy is described by the active and reactive power P and Q, measured in MW and Mvar, respectively.



(a) Overview of wind turbine generator energy conversion



(b) Multilevel flow modeling representation of wind turbine generator functional model

(c) Multilevel flow modeling representation during high wind speeds

Figure 5.2: Formulation of functional model of wind turbine generator. Source: [**Pub. A**]

The electric energy is transported towards the grid connected terminals, represented by the sink *Si2*, through the transport function *Tra7*. In Figure 5.2a, the grid connection is indicated by the fifth step of the conversion process, where the stator and grid side converters of the DFIG have different responsibilities. The stator side converter is responsible for controlling the current from the wind turbine generator to the grid, and the grid side converter controls the voltage to a certain degree. These control responsibilities are indicated in Figure 5.2a by V and I and assumed measured by metering devices at the terminal connection to the grid indicated in Figure 5.2a.

The blade pitch angle, θ measured in degrees, in the second step of Figure 5.2a can control the kinetic energy harvested by the blades. In MFM, this ability is modelled by the first CFS, *CFS1*, which has the objective of maintaining the rotational speed within its operational limits. This is achieved by adjusting the mass storage of wind at the turbine blades. The second CFS in Figure 5.2b, *CFS2*, is used to represent how the back-to-back converters in the DFIG are responsible for maintaining

appropriate interaction between the wind turbine generator and the grid. This is done through controlling the conversion of rotational energy into electric energy as represented by *Con1*.

The MFM model in Figure 5.2b allows a rule based analysis of the cause-effect relations. As an example, consider a scenario where the wind speed is increasing from normal to high, which causes a large flow of mass through *So1*. The cause-effect relations can be evaluated through Figure 5.2c, where the affected functions are marked in red. Initially, the wind speed in the MFS is indicated high by the red source function *So1* in Figure 5.2c, which subsequently increases the mass flow from the up wind stream and past the wind turbine, indicated by the red transport and storage functions in Figure 5.2c. In theory, the mass of wind could potentially also change in the down stream sink *Si1*, although the scale of this increase depends on the aerodynamic efficiency of the blades and their capability of absorbing the increased mass flow.

Following the increased wind mass passing the blades as a result of the increased wind speed, the kinetic energy, *So2* in the EFS of Figure 5.2c increases as indicated by the red marking. With a higher kinetic energy, the rotation of the wind turbine generator shaft increases, and this acceleration twists the shaft, resulting in an increase in both elastic and rotational energy as indicated in red in Figure 5.2c. As *Sto2* increases, the pitch angle control in *CFS1* evaluates the rotational speed, and if the rotational speed exceeds a predefined control limit, the pitch angle is increased to lower the wind mass stored in *Sto1*. This control completes the loop indicated in red in Figure 5.2c and the example demonstrates how the functional model can be used to analyze wind turbine generator behaviour due to its intuitive representation of cause-effect relations.

5.2 Distributed processing requirements and implementation

The formulated functional model in subsection 5.1.1 is analyzed with the objective of establishing a state estimation model that can be solved using the WLS minimization approach described in subsection 2.2.1 and used as a foundation for detecting, identifying and eliminating bad data using the $J(\mathbf{x})$ method introduced in subsection 2.2.2 which represents a way of protecting DG controls against information integrity disturbances such as gross and extreme measurement noise described in Figure 2.4.

The implementation of a cyber error detection system with a distributed processing topology in Figure 2.2c entails certain requirements on the model characteristics and the algorithm chosen to solve the WLS problem. The chosen approach has to be numerically robust, as rounding errors are more likely in a distributed processor compared to a SCADA system computer due to the limited bit number of the embedded Operating System (OS) compared to general purpose OS. Furthermore, the distributed processor has to ensure a fast and accurate convergence within a timing requirement set by the time period between availability of new information, that alleviates the risk of processor overflow.

The applied bottom-up approach to protect the DG controls therefore entails a necessary trade-off between level of details that can be included in the state estimation model and computational requirements for ensuring robust convergence of the WLS solution. Compliance with these requirements are considered in this work through choosing orthogonal factorization as the estimation algorithm due to its robustness described in [167]. This decision however, entails a computational disadvantage due to the inherently required QR factorization of the Jacobian matrix. Furthermore, the distributed processor robustness and timing requirements are considered through

limiting the number of state variables and equations included in the nonlinear measurement model in (2.1) that represent the wind turbine generator. Therefore, the state estimation model is established through the functional model of the wind turbine, which limits the number of measurements, equations and variables included in the state estimation model because of the high level of abstraction.

5.2.1 Establishing, solving and utilizing the wind turbine state estimation model

As introduced in subsection 2.2.1, a state estimation model can be established around the nonlinear measurement model in (2.1). Such estimation model therefore consists of a set of measurements $\mathbf{z}$, a set of state variables $\mathbf{x}$, and a set of state equations $\mathbf{h}(\mathbf{x})$ representing the relationship between the measurements and state variables through the nonlinear measurement model in (2.1).

Using the functional model in Figure 5.2b as a representation of the physical relations within the wind turbine generator energy conversion gives a high level overview of the system. While a deeper decomposition of the different functions and sub-process could reveal additional functions and relations, such as more in-depth representation of the mechanisms within the two converters or for the elasticity of the turbine shaft, this would entail additional complexity and computational requirements for solving the WLS problem. Considering the ability of the formulated functional model to describe the operational status of the DG unit illustrated by the high wind speed example in Figure 5.2c, ten key quantities characterizing the mechanical and electrical systems are identified. Together these quantities can describe the conditions of the energy conversion process at the considered level of decomposition in Figure 5.2b, and form a set of measurements $\mathbf{z}$ shown in (5.1).

$$\mathbf{z} = [v, \theta, \omega_r, P, Q, V_{rms}, I_{rms}, V, I, \Delta\omega_r] \tag{5.1}$$

where V_{rms} and I_{rms} are the root mean square line to ground voltage in volts and line current in ampere, respectively, V and I are the instantaneous phase sine wave voltage in volts and current in ampere, and $\Delta\omega_r$ is a pseudo measurement of the change in rotational speed in radians per seconds squared between two time instances. In this work the time period between measurement acquisition is assumed equal to a time resolution of 1 s.

The set of measurements identified from the MFM model in Figure 5.2b captures the key steps in the energy conversion process starting from the effects of the free wind speed and finishing at the delivery of current at the grid terminals. A direct relation between each of the identified quantities in (5.1) and the MFM function representation in Figure 5.2b can be seen in Table 5.1.

Table 5.1: Set of measurements derived from functional model

z	v	θ	ω_r	P	Q	V_{rms}	I_{rms}	V	I	$\Delta\omega_r$
Functions	*Sto1*	*CFS1*	*Sto2*	*Con1*	*Con1*	*Si2*	*Si2*	*CFS2*	*CFS2*	*So2/Con1*

From the derived measurement and MFM functions in Table 5.1, it is noticeable how the established state estimation model contains quantities in both the MFS, EFS, and both CFS of Figure 5.2b. From the functional relations identified in Table 5.1, the pseudo measurement $\Delta\omega_r$ can be related through the power balancing function in the shaft. The acceleration of the rotating shaft is defined by the difference mechanical and electrical torque as shown in (5.2).

$$\Delta\omega_r = \frac{1}{2H}\left(T_{mech} - T_{elec}\right) \tag{5.2}$$

where H is the moment of inertia of the wind turbine generator, and T_{mech} and T_{elec} are the mechanical and electric torque, respectively. The right hand side of (5.2) can be expanded further in (5.3)-(5.5) through applying physical relations.

$$\Delta\omega_r = \frac{1}{2H}\left(\frac{P_{mech}}{\omega_r} - \frac{P_{elec}}{\omega_r}\right) \tag{5.3}$$

$$= \frac{1}{2H}\left(\frac{P_{wind}\left(v\right)C_p\left(\lambda,\theta\right)}{\omega_r} - \frac{3V_{rms}I_{rms}cos\phi}{\omega_r}\right) \tag{5.4}$$

$$= \frac{1}{2H}\left(\frac{P_{wind}\left(v\right)C_p\left(\omega_r,v\right)}{\omega_r} - \frac{3V_{rms}I_{rms}cos\phi}{\omega_r}\right) \tag{5.5}$$

where $P_{wind}\left(v\right)$ is and expression of the power in the wind specific kinetic energy, $cos\phi$ is the power factor, and $C_p\left(\lambda,\theta\right)$ is the power coefficient as a function of the tip speed ratio, λ and the blade pitch angle, θ, respectively.

From (5.4) to (5.5), the power coefficient dependency is changed by utilizing that λ is defined by the dimensions of the wind turbine blade radius R, ω_r and v through (5.6), and finding an expression of the blade pitch angle and the tip speed ratio θ as a function of ω_r and v.

$$\lambda = \frac{\omega_r R}{v} \tag{5.6}$$

The second expression linking θ to ω_r and v can be derived by assuming optimal pitch controller operation and performing a study of a specific wind turbine during different wind speeds. With a suitable simulation model or a set of historic data representing a wind turbine during steady state operation and with implemented pitch angle controller, different wind speed scenarios can be investigated. At steady state, the λ and θ can be registered and since the pitch controller is designed to keep ω_r at optimal conditions at different wind speeds, the magnitude of the wind speed will have the greatest impact on λ. Therefore, a relationship between θ and λ can be formulated, and with (5.6), this relationship can be converted from $\theta(\lambda)$ to $\theta(v,\omega_r)$.

The expression in (5.5) only depend on four of the parameters in Table 5.1. With this observation and an assessment of the set of measurements in (5.1), it is determined that all measurement quantities can be estimated from a set of independent variables $\mathbf{x}$ in (5.7), and a set of state equations $\mathbf{h}(\mathbf{x})$.

$$\mathbf{x} = [v, \omega_r, V_{rms}, I_{rms}] \tag{5.7}$$

With the set of variables in (5.7) of size $n = 4$, and the set of measurements in (5.1) of size $m = 10$, the redundancies used for estimating the state variables in the model, are calculated as the degree of freedom $\nu = m - n = 6$. The objective of the state estimation process is to exploit such an over-determined non-linear system through an iterative process of estimating independent state variables based on equations and measurements. This way, the knowledge about the physical system can help reduce the inclusion of measurement error in the estimated

wind turbine operational conditions, providing a better information integrity for further data analysis and utilization by wind turbine owners.

The state equations can be identified to finalize the establishment of the state estimation model, and these are found through the consideration of the defined set of independent variables in (5.7) and the physical relations within the wind turbine generator represented by the functional model in Figure 5.2b. The set of state equations $\mathbf{h}(\mathbf{x})$ is defined based on the identified state variables in (5.7). With the four state variables being included in the set of measurements, these equations can be easily identified as in (5.8), (5.10), (5.13), and (5.14). As discussed above, a study of the aerodynamic characteristics and pitch controller settings of specific wind turbine models can reveal relationships between the pitch angle θ and v and ω_r in ideal operating conditions. Therefore, this expression is used as a state equation in (5.9), and similarly used in the $C_p(v, \omega_r)$ representation used to describe the mechanical power impact on the shaft acceleration, shown in the state equation (5.17). The last four remaining state equations in (5.11), (5.12), (5.15) and (5.16) are identified through power system theory.

$$v = v \tag{5.8}$$
$$\theta = \theta\left(v, \omega_r\right) \tag{5.9}$$
$$\omega_r = \omega_r \tag{5.10}$$
$$P = 3V_{rms}I_{rms}cos\phi \tag{5.11}$$
$$Q = 3V_{rms}I_{rms}sin\phi \tag{5.12}$$
$$V_{rms} = V_{rms} \tag{5.13}$$
$$I_{rms} = I_{rms} \tag{5.14}$$
$$V = V_{rms}\sqrt{2}sin\left(2\pi ft + \delta\right) \tag{5.15}$$
$$I = I_{rms}\sqrt{2}sin\left(2\pi ft + \beta\right) \tag{5.16}$$
$$\Delta\omega_r = \frac{1}{2H}\left(\frac{P_{wind}\left(v\right)C_p\left(\omega_r, v\right)}{\omega_r} - \frac{V_{rms}I_{rms}cos\phi}{\omega_r}\right) \tag{5.17}$$

The 10 state equations in (5.8) to (5.17) collectively represent $\mathbf{h}(\mathbf{x})$ for the set of measurements in (5.1). Equations (5.15) and (5.16) include the voltage and current angles, δ and β, respectively. These angles are assumed accurately acquired through the use of synchrophasor measurement units at the wind turbine terminals. Since the voltage and current angles are assumed accurately acquired the maximum total vector error of PMU defined by international standards [40], means the voltage magnitude measurement accuracy is within $\pm 1\%$. This simplification is used as an assumption that allows the inclusion of the instantaneous voltage and current. Furthermore, the assumption enables the calculation of the power factor angle ϕ used in (5.11) and (5.12) through (5.18).

$$\phi = \delta - \beta \tag{5.18}$$

Solving the state estimation model

Finding a solution to the WLS problem that returns the optimal combination of the state variables in (5.7) requires, as mentioned, a robust estimation algorithm when implemented on a distributed processor. With the Newton method [see Appendix B.1], the formulation of the gains matrix can

causes ill-conditioning when considering different weighting factors, a large set of measurements, or the relative characteristics of the state equations. To ensure a robust execution, different methods are proposed where the gain matrix is not formulated. One such alternative estimation algorithm is the orthogonal factorization in which the inverse of the diagonal weight matrix, i.e. R^{-1} is separated in two identical terms $R^{(-1/2)}$. The product of the Jacobian and the separated inverse diagonal weight matrix then forms a new expression $\tilde{\mathbf{H}} = \mathbf{R}^{(-1/2)}\mathbf{H}$, which is factorized through an orthogonal matrix Q and an upper triangular matrix U [see Appendix B.2].

Bad data detection, identification and elimination

After each iteration of the state estimation through orthogonal factorization, it is desirable that the cyber error detection system detects, identifies and eliminates occasions of bad data. There are multiple analytic and data driven approaches to the identification of gross or extreme measurement error as introduced in subsection 2.2.2. In the distributed cyber error detection system demonstrated in this chapter, the J_{sum} method presented in (2.16) is applied after each state estimation iteration because of its simplicity and its alignment with the state estimation execution.

In the case of bad data being detected, the process of bad data identification is initiated. A widely used identification method of sorting the weighted residuals in J_{sum} in a descending order and assuming the measurement with the largest weighted residual as the bad measurement b as introduced in [136], is implemented in the bad data detector implemented in this work.

After detecting and identifying the bad data, the bad measurement must be eliminated to make sure the state estimator will converge towards an accurate solution. There exists multiple different techniques in eliminating bad data, with different computational requirements [134, 137]. As DG units are operating in a volatile environment, the process of replacing the bad data by the measurement from the last period is unreliable. Instead a similar approach as the one used in [137] is utilized, where the bad measurement is replaced by a pseudo measurement based on the estimated value and the gains matrix. In the simplified state estimator, the gains matrix is avoided, therefore the identified bad measurement is calculated using (5.19).

$$z_b^{new} = z_b^{old} - \text{sign}\left(z_b^{old} - h_b(\mathbf{x})\right) \cdot |a| \tag{5.19}$$

where $|a|$ represents the absolute value of a normal distribution random number with zero mean and a standard deviation of $\sigma = 0.01$. The idea behind the value subtracted from the bad data to form the new data in (5.19), is that the sign of difference between the bad data and the estimated value is assumed to represent the sign of the difference between the bad data and the correct data. By simply pushing the bad data in the direction of the estimated value, the new data should be closer to the correct data, assuming the estimated value is closer to the correct data.

After eliminating the identified bad data, the state estimator initiates its next iteration or execution and the process of bad data detection, identification and elimination is repeated. It might be necessary to execute the bad data detector several times until the hypothesis of bad data being present is thrown and in this work, it is assumed that only one measurement can be identified as bad for each iteration of the state estimation model.

5.2.2 LabVIEW implementation

Representing a distributed processing topology illustrated in Figure 2.2c, the cyber error detection system is implemented on a National Instruments (NI) compact-RIO (cRIO). Such a device enables highly reliable operation in a considerable time frame and consists of a real-time processing target, which is a small processor with no general purpose OS meaning it allows deterministic execution. Furtermore, the cRIO is equipped with an Field Programmable Gate Array (FPGA) target that is a configurable micro chip with a limited number of logical gates. The FPGA target is capable of executing multiple simple calculations simultaneously with very high speed, and the real-time target offers execution of more complex calculations with lower computational speed.

The implementation of the cyber error detection system in NI LabVIEW can be done through separating its processes in; 1) acquisition of measurements from wind turbine sensors, 2) execution of state estimation iterations, 3) execution of bad data detection, and 4) a communication of the processed information to an external client. Such processes can be represented by LabVIEW Virtual Instrument (VI), where the implementation targets and the inter-communication on the cRIO device can be illustrated through the system diagram in Figure 5.3.

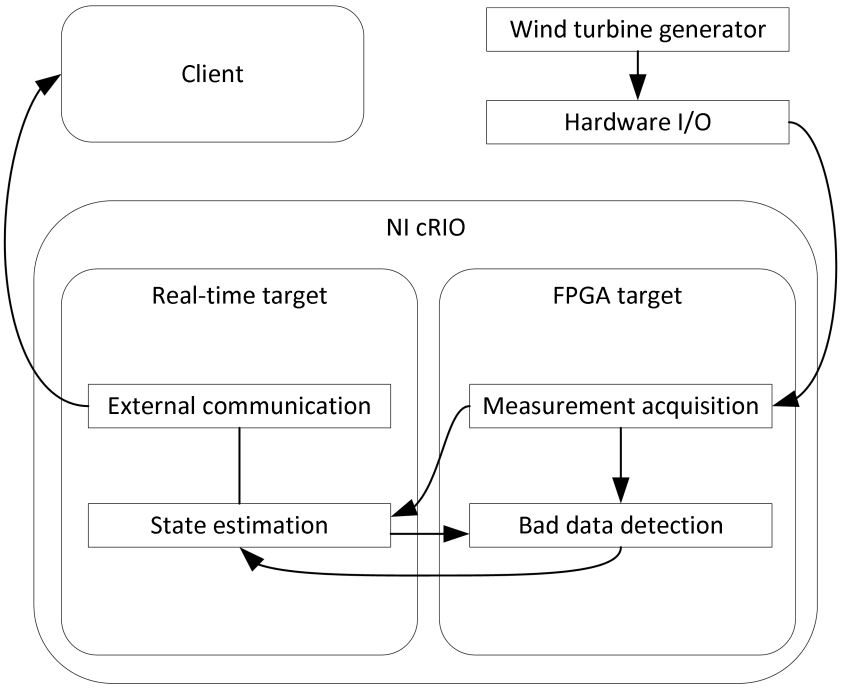


Figure 5.3: LabVIEW system diagram implementation of cyber error detection system

With an operating wind turbine, the metering equipment collects information about the physical conditions corresponding to the set of measurements in (5.1). These measurements can be collected by the NI hardware input/output modules that are communicating directly to the FPGA target through the process bus as illustrated in Figure 5.3. After acquiring the measurement set, this is forwarded to the state estimator VI executing the orthogonal factorization algorithm on the set of state equations in (5.8) to (5.17) as an iterative effort to estimate the state variables in (5.7). The set of measurements are likewise transferred to the bad data detection VI where it is used in collection with the state estimation results after each iteration in an effort to detect and identify any bad data.

When the bad data detection VI is executed, it returns the detection and identification results to the state estimator VI, which is responsible for eliminating any identified bad data. After converged execution of the state estimator, the estimated states and representative measurement values are made available for client acquisition illustrated by the external communication VI in Figure 5.3. With the overview in Figure 5.3, the cyber error detection system is intended for execution between data acquisition from wind turbine sensors, and the communication of information to different subscribers. This means the system offers a means of investigating the integrity of wind turbine information before it is utilized for further analysis by subscribers such as the wind farm owners or network operators. Instead of applying the cyber error detection system directly on a real wind turbine generator, a simulation model is utilized for demonstrating the system performance.

Simulink wind turbine model

Simulation of generic wind turbine operation is proposed in [168], where a DFIG turbine model is separated into a generator and converter model, a turbine and turbine control model, and an electrical control model. Such model has been implemented in MATLAB Simulink with the aim of using the simulation in relation to the LabVIEW implementation of the cyber error detection system. Through the NI Veristand software add-on to MATLAB, the Simulink model is converted into C code and later implemented on the cRIO together with a controllable wind speed generator and the remaining VIs in Figure 5.3.

In [168], different parameters of the generic 1.5 MW DFIG wind turbine are given, including generic aerodynamic characteristics of the wind turbine blades and their geometry. With such characteristics, the functional expression of pitch angle based on ω_r and v in (5.9) can be derived through simulating the Simulink model in different wind speed conditions as described earlier. These simulation results are shown in Figure 5.4 together with a four term Gaussian curve fitted using the MATLAB curve fitting toolbox. The functional expression of the curve fitting results are presented in (5.20).

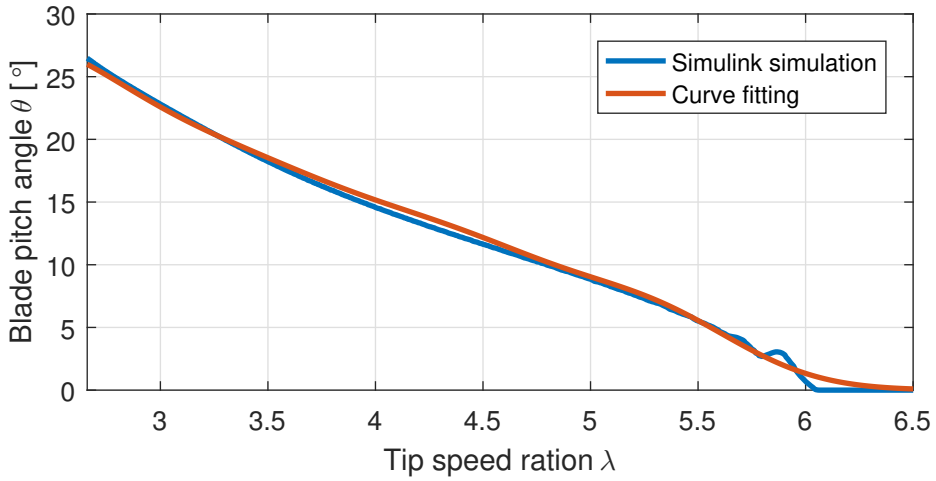


Figure 5.4: Relationship between blade pitch angle and tip speed ratio for a generic 1.5 MW DFIG wind turbine

$$\theta(\lambda) = 743.1 \cdot exp\left(-\left(\frac{\lambda - 3.237}{1.095}\right)^2\right) - 800.2 \cdot exp\left(-\left(\frac{\lambda - 3.258}{1.048}\right)^2\right) + 78.48 \cdot exp\left(-\left(\frac{\lambda - 3.341}{0.8431}\right)^2\right) + 3.516 \cdot exp\left(-\left(\frac{\lambda - 5.361}{0.5485}\right)^2\right) \quad (5.20)$$

With the expression in (5.20) and knowledge about the blade geometry, the expression can be converted to a $\theta(v, \omega_r)$ instead, and inserted into (5.9) and (5.17). In [168], the radius of the wind turbine blades is, however, given as part of a parameter K_b that also contains the per unit base value of the rotational speed because the DFIG turbine model represents the rotational speed of the generator shaft in per units. To ensure smaller differences between the different measurement values processed by the state estimator, all other quantities of the wind turbine model are converted to per unit, starting from a definition of the apparent power base $S^{base} = 1.5$MVA according to the wind turbine characteristics. The per unit base of the free wind speed v is assumed as 12 m/s from an identification of the minimum wind speed that cause rated power generation by the wind turbine generator. The V_{rms} per unit base is assumed as 690 V according to the terminal voltage of the wind turbine. With the per unit base of apparent power and voltage, the current per unit base can be found in (5.21).

$$I_{rms}^{base} = \frac{S^{base}}{\sqrt{3} \cdot V_{rms}^{base}} = 1255,1A \quad (5.21)$$

Replacing the blade radius in (5.6) with the K_b parameter from [168] equal to 56.6 for the 1.5 MW DFIG turbine, the per unit base of the tip speed ratio λ^{base} is calculated through the modified (5.6) and v^{base} as shown in (5.22).

$$\lambda^{base} = \frac{K_b \cdot \omega_r}{v^{base}} = \frac{56.6 \cdot 1pu}{12m/s} = 4.72 \quad (5.22)$$

Relating the tip speed ratio per unit base to the pitch angle through Figure 5.4, reveals $\theta^{base} = 10.4°$. Assuming the active and reactive power measurements have the same per unit base as the apparent power, and that the instantaneous voltage and currents share per unit base with their respective rms quantities, finalize the per unit conversion. With this conversion, the standard deviation of all measurements is assumed equal to 1% of the per unit base values as represented in Table 5.2.

Table 5.2: Assumed measurement standard deviation σ for the set of measurements **z**

z	v	θ	ω_r	P	Q
σ_z	$0.12m/s$	$0.104°$	$0.01pu$	$0.015MW$	$0.015Mvar$

z	V_{rms}	I_{rms}	V	I	$\Delta\omega_r$
σ_z	$6.9V$	$12.551A$	$6.9V$	$12.551A$	$0.01pu$

5.2.3 Performance evaluation

The cRIO implementation of the Simulink wind turbine simulation model and the cyber error detection system are executed and the performance of the bottom up approach to DG control protection is evaluated by considering; 1) its ability to solve the WLS problem within a short time sequence, 2) its accuracy in estimating the solution to the state estimation model compared to raw measurements subject to normal measurement error, and 3) its performance in terms of detecting, identifying and eliminating gross measurement error. The three evaluation parameters are evaluated through conducting three test cases, where the state estimator is executed once every second and the Simulink model is simulated in discrete time with a fixed time resolution of 40 ms.

Execution time

The purpose of the first test is to evaluate how fast the simplified state estimator with integrated bad data detector can solve the WLS problem of the state estimation model established in subsection 5.2.1. This objective is reached by implementing tick counts in the LabVIEW system diagram before and after the state estimation and the bad data detector process execution in Figure 5.3.

Under low measurement error conditions, where the standard deviation of the signal noise is equal to the assumed measurement device accuracy shown in Table 5.2, the QR factorization algorithm only requires a single or two iterations to solve the WLS problem. To evaluate the execution time of the distributed cyber error detection system at a different number of iterations, the standard deviation of the measurement noise is doubled for all measurements. This results in a higher chance of the measurement error causing a detection of bad data, while using a detection probability of $\alpha = 5\%$ in the J_{sum} test in (2.16) illustrated in Figure 2.5.

The cRIO is executed for a time series where the state estimator executes in total 162 times. The resulting execution time data is separated based on the number of iterations needed to find a solution to the WLS problem, reached after the Euclidean norm of the change in state variable value between two iterations is below the convergence threshold chosen as $\varepsilon = 0.01$.

The number of iterations ranges from 1 to 14. In the case where 1 iteration is needed, the first solution of the state estimation is close enough to the final solution of the previous execution, used as the starting point for the following execution. The minimum, average and maximum execution time is calculated and presented in Figure 5.5 as a function of the required number of iterations before converging.

A linear relationship between the number of iterations and the average execution time is observed in Figure 5.5. For the executions with 2 to 4 iterations, the maximum observed execution is around 5 ms slower than the average execution time. At the same time, the average value is observed closer to the minimum execution time, which indicates that the occurrence of large execution times is rather limited.

From Figure 5.5 the execution time of the distributed cyber error detection system can be evaluated. As previously mentioned, the system is intended to run between the acquisition and the communication of data, and the added timing requirements of validating the data must be low enough to allow further data handling. For an iteration count between 1 and 14, the execution time varies from around 5 ms to 45 ms. Considering the case of three iterations, the average execution time is calculated in Figure 5.5 as approximately 10 ms, this corresponds to an execution frequency of 100 Hz and with a state estimator execution frequency of 1 Hz, the risk of overflowing the distributed processor is relatively low.

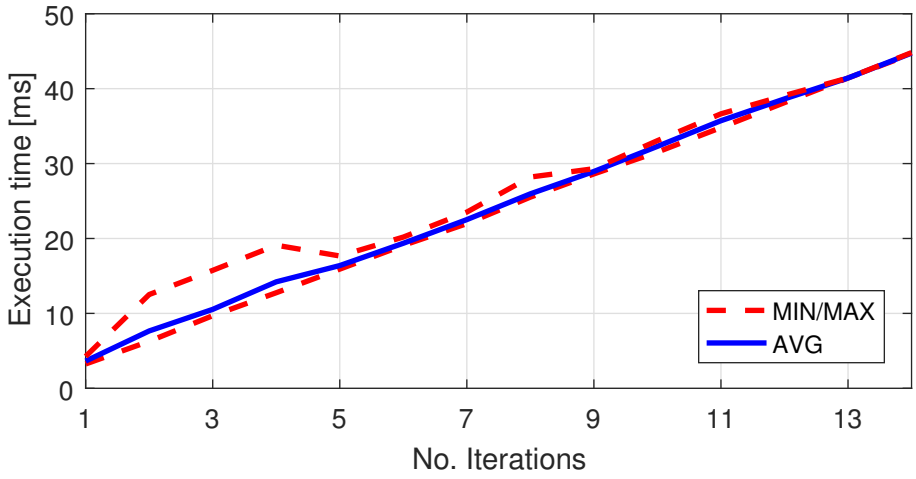


Figure 5.5: Minimum, maximum and average execution time of distributed cyber error detection system at different number of iterations before convergence. Source: **[Pub. F]** © 2017

Estimation accuracy

In the second test of the cRIO implemented cyber error detection system, the objective is to compare the accuracy of the estimated and the disturbed signals to the correct signals from the Simulink model simulation. In this test case, all measurements are disturbed with normal measurement noise, described in Figure 2.4, and assumed to follow a Gaussian distribution with zero mean and the standard deviation shown in Table 5.2.

The cRIO is executed and the accuracy of the solution to the established state estimation model is analyzed by comparing the estimated signals $\mathbf{h}(\mathbf{x})$ to the correct simulated signals $\mathbf{z}_{real}$ and the distorted signals $\mathbf{z}$. These three results are found for each measurement in (5.1) except for the change in rotational speed which is only obtained as a pseudo measurement. A numerical comparison on a per unit base of the accuracy results is performed by calculating the Average Euclidean Error (AEE) over the executed time period τ, using (5.23), as introduced in [169].

$$AEE(d_i) = \frac{1}{\tau}\sum_{t=1}^{\tau} ||d_{t,i}||_2 \tag{5.23}$$

where $\mathbf{d}$ is the difference between $\mathbf{z}_{real}$, and $\mathbf{z}$ or $\mathbf{h}(\mathbf{x})$, and i is the index of the measurements in (5.1). The AEE is calculated for both $\mathbf{z}$ and $\mathbf{h}(\mathbf{x})$ and is shown in Table 5.3.

Table 5.3: Average euclidean error of distorted measurements and estimation results compared to the real physical conditions

$\mathbf{d}$	v	θ	ω_r	P	Q	V_{rms}	I_{rms}	V	I
$\mathbf{z}_{real} - \mathbf{z}$	0.0067	0.0067	0.0095	0.0074	0.0070	0.0061	0.0090	0.0084	0.0085
$\mathbf{z}_{real} - \mathbf{h}(\mathbf{x})$	0.0085	0.0064	0.0074	0.0055	0.0004	0.0057	0.0052	0.0056	0.0053

The small values of all the AEE results in Table 5.3 show a similarity in the average error of $\mathbf{z}$ and $\mathbf{h}(\mathbf{x})$. Evaluating the accuracy of the convergence of the established state estimation model based on these results therefore gives an indication that $\mathbf{h}(\mathbf{x})$ offers similar accuracy in situations with normal

measurement noise as the raw measurements. The state estimator could be improved by utilizing a more detailed set of state equations as in [112] or [111], however this would simultaneously change the execution time as the detailed model requires an increased number of calculations in finding the solution to the WLS problem.

Gross and extreme error detection

After testing the accuracy of the cyber error detection system when measurements are subject to normal measurement noise, the third test case evaluates the performance of the distributed cyber error detection system when gross and extreme measurement errors, as defined in Figure 2.4, are injected into a set of target measurements. Evaluating the ability to detect gross and extreme measurement errors is done through choosing three different measurements and exposing them to injections of measurement error at the time instances and with the comparable error magnitude presented in Table 5.4.

Table 5.4: Gross and extreme measurement error injection to measurements in the established state estimation model

Time	8 s	13 s	18 s	28 s	33 s	38 s
z	v	P	I_{rms}	v	P	I_{rms}
Error	1 m/s (8σ)	0.1 MW (7σ)	0.15 kA (12σ)	1.6 m/s (13σ)	0.35 MW (23σ)	0.35 kA (28σ)

From Table 5.4 the magnitude of the measurement error injected is arbitrarily chosen between 7 and 28 times the standard deviation of the measurements shown in Table 5.2. The schedule is used while running the cRIO, giving the results illustrated in Figure 5.6.

In Figure 5.6, the left hand side shows the wind speed, the active power and the rms current during the time period of execution. From these plots, $\mathbf{z}$ is clearly affected by the gross measurement error injected two times for each measurement. In comparison, the estimated results in $\mathbf{h}(\mathbf{x})$ are closer to the correct measurements $\mathbf{z}_{real}$ for each injection of measurement error according to Table 5.4.

In the right hand side plot of Figure 5.6, the absolute error between $\mathbf{z}_{real}$, and $\mathbf{z}$ and $\mathbf{h}(\mathbf{x})$, is shown for each of the three measurements. Here the performance of the distributed cyber error detection system, in handling gross and extreme measurement errors is easily visible, as it is able to detect, identify and eliminate the error and estimate a better signal value than the raw measurements $\mathbf{z}$.

The error in I_{rms} after 33 s visible in the right hand side of Figure 5.6, equal to approximately 0.1 kA indicates room for further improvements of the error detection system. The cause of the large error is that the bad data detection part of the distributed system first correctly identifies the active power as the bad measurement, and after eliminating the error, it wrongly identifies a bad data at the rms current as well. This increases the difference between the pseudo measurement value and the correct value. This could possibly be avoided by finding the optimal trade-off between false positives and negatives, through fine tuning the detection threshold K, or refining the methods used in the bad data detector.

Besides the false identification of the rms current as containing bad data, the results confirm the added accuracy of using the distributed cyber error detection system compared to using raw measurements when monitoring the performance of DG units. This accuracy could be valuable when considering the utilization of measurements in determining control actions within the CPES.

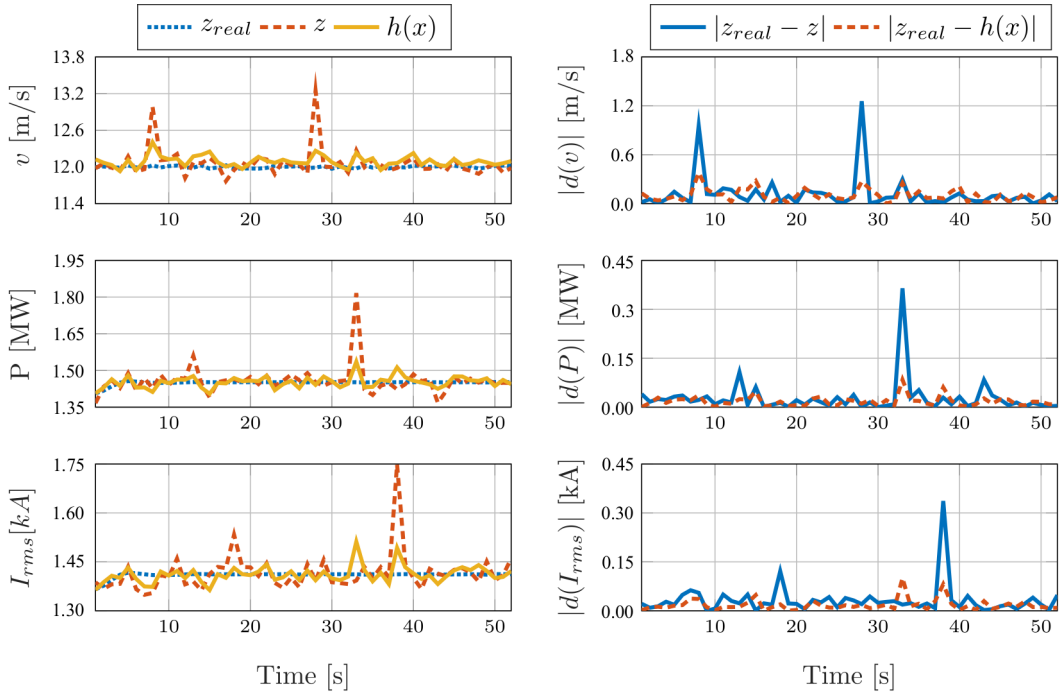


Figure 5.6: Left: The wind speed, active power and rms current when subject to gross measurement error. Right: The absolute error between the true simulated signal and the distorted signal (blue line) and the estimated signal (red line), for the three measurements subject to gross and extreme error. Source: **[Pub. F]** © 2017

5.3 Cyber-physical emulation of WPP operation

The current practice of monitoring operation of individual wind turbines in a WPP through standard SCADA systems is to average the incoming measurements across 10 minutes of operation [170]. This approach efficiently removes gross measurement error, but limits the visibility of the dynamics in the system. With implementation of the distributed cyber error detection system described in section 5.2, the monitoring of a individual wind turbines can be improved by actively removing gross measurement errors before broadcasting measurement at normal SCADA resolution of 1 Hz.

The cyber error detection system is intended for implementation on a distributed processing topology as illustrated in Figure 2.2c, and is located between the acquisition and the communication of data between the individual wind turbines and a WPP control center. The purpose of the test scenario investigated in this section is to indicate how the implementation of the established state estimation model at the individual wind turbines in a small WPP improves the monitoring through higher time resolution data acquisition as well as limiting the impact of cyber vulnerability exploitation through active removal of gross measurement errors.

The removal of gross measurement errors becomes important when utilizing the measurements of individual wind turbines in performing WPP controls. In the recent decades, DG has been required to actively participate in the grid operation through active and reactive power controls [171]. One of these control strategies commands the WPP to limit its active power output to a portion of its rated capacity thereby curtailing the generation from the wind turbines [172].

Such a control command can be handled in different ways. One option is stopping the current injection of wind turbines one by one until the active power limit is satisfied, however, due to the

fluctuations of the wind, this crude method is not desirable. Instead, each turbine can be controlled to lower their power production to a value coordinated by the WPP controller dispatch function. The dispatch function of the controller is supported by a feedback loop that evaluates whether the WPP satisfies its desirable set point P_{set}^{WPP} [171].

The active power set point of each wind turbine generator, P_{set}^{WTG}, can be equal for all wind turbine generators. However, P_{set}^{WTG} usually varies according to the available power of each individual wind turbine. Calculating the available power of each wind turbine, P_{avail}^{WTG} can be done through different techniques, as described in [173]. Most of the methods rely on observations from the physical system to estimate the available power for each wind turbine, making them vulnerable to gross measurement error and data integrity attacks. In this work, the adjusted power curve distribution function is considered, where the power is estimated through the power curve of the wind turbine and the free wind speed [173]. The individual wind turbine generator power set point is then calculated by a percentage of the available power, making it capable of delivering the WPP power set point during wind fluctuations.

With the active participation of the wind turbine in the WPP active power control, the expressions in (5.9) and (5.17) need to consider the possibility of sub-optimal blade pitch angle due to control signals from the main controller. The sub-optimal position of θ is defined by the WPP main controller active power set point P_{set}^{WTG} communicated to each wind turbine within its control area [171]. Using the active power set point as input, the correctional coefficients K_θ and K_{Cp} are defined by fine tuning (5.9) and (5.17), respectively. To include the correction coefficients the state equations in (5.9) and (5.17) changes to (5.24) and (5.25), respectively.

$$\theta = f\left(v, \omega_r\right) K_\theta \tag{5.24}$$

$$\Delta\omega_r = \frac{1}{2H}\left(\frac{P_{wind}\left(v\right)\frac{C_p(\omega_r,v)}{K_{C_p}}}{\omega_r} - \frac{V_{rms}I_{rms}cos\phi}{\omega_r}\right) \tag{5.25}$$

Wind power plant simulation model

The established state estimation model based on the functional model in Figure 5.2b, is evaluated through implementation in a numerical WPP simulation model, defined by the single line diagram in the *Physical system* part of Figure 5.7.

The WPP, composed of 6 DFIG wind turbines each with a rated power of 1.5 MW, is assumed located perpendicular to the wind direction to neglect wake effects. Each wind turbine is experiencing a wind speed with equal average value with different local fluctuations to represent turbulence. These assumptions are included to emphasize the effects of gross measurement error and are not limiting the independence of the cyber error detection system in practice. The wind turbines are modeled using the parameters given in [168], and the WPP collector system is modeled by assuming an onshore radial topology with the grid equipment parameters shown in Table 5.5 [168, 174, 175] and a system frequency of 60 Hz.

The *cyber system* of the WPP illustrated in Figure 5.7 includes the Wind Turbine Control Panel (WTCP), from where measurements and control signals are communicated. The WTCP is located at the bottom of the wind turbine tower, and can be used by maintenance crews to acquire data and control the wind turbine [22]. To emulate measurement noise in the simulation of the WPP, a

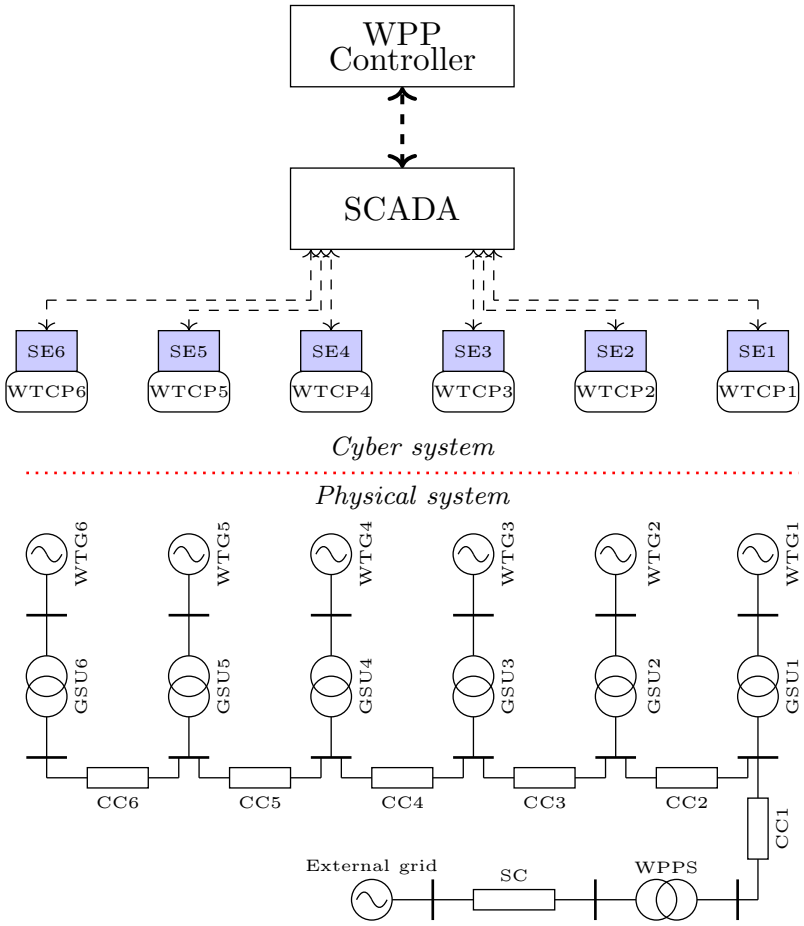


Figure 5.7: Wind power plant cyber and physical system, represented by the ICT infrastructure and a single line diagram, respectively. Source: **[Pub. A]**

normal distributed random noise with zero mean and standard deviation according to Table 5.2 is added to each measurement before it is acquired. Before communicating the individual wind turbine measurements with the SCADA system of the WPP the distributed cyber error detection system evaluates the information as illustrated by the SE1 to SE6 in Figure 5.7, where SE is used to represent the state estimation characteristics of the bottom-up approach to protection of DG controls.

5.3.1 Integrity attack detection

The application of the distributed cyber error detection system is investigated in a scenario where the distributed processor is connected directly to the WTCP as shown in Figure 5.7 and evaluated in a DG control application through test cases with large disturbances on the free wind speed signal. The disturbances are assumed added to the free wind speed signal at the WTCP of one of the wind turbines. The WPP controller will be evaluated based on its reaction when raw measurements are received directly through the SCADA system, and when measurements have been through the distributed cyber error detection system before being broadcasted. Four different disturbances are investigated based on current literature in false data injection attacks shown in Figure 2.1 and their impact on power system controls described in [21]. The four disturbances considered in our work are similarly based on attack templates from [20] as follows:

Table 5.5: Collector system parameters

Equipment	Abbreviation	Parameter	Value
Substation cable	SC	Length	20 km
		Resistance	77.8 mΩ/km
		Inductance	10 μH/km
		Capacitance	0.14 μF/km
Wind power plant substation transformer	WPPS	Primary voltage	230 kV
		Secondary voltage	34.5 kV
		Rated power	10 MVA
Collector cable	CC1-6	Length	10 km
		Resistance	268 mΩ/km
		Inductance	482 μH/km
		Capacitance	0.16 μF/km
Generator step-up transformer	GSU1-6	Primary voltage	34.5 kV
		Secondary voltage	0.6 kV
		Rated power	2 MVA

1. Gross measurement error.
2. Random data injection attack as illustrated in Figure 2.1c.
3. Pulse data injection attack as illustrated in Figure 2.1d.
4. Ramping data injection attack as illustrated in Figure 2.1e.

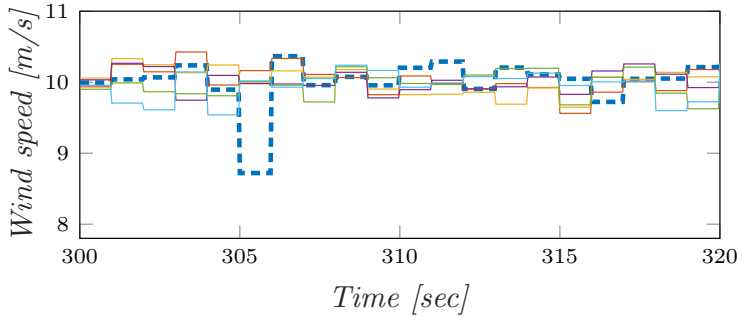
For each of the test scenarios, the average wind speed will be 10 m/s for all wind turbines and the WPP controller is commanded by the transmission system operator to curtail 60% of its active power generation. Such a scenario emulates a situation where the power system has over-production and requires a down-regulation of the DG units.

The test cases simulate situations where the cyber system of one wind turbine experience errors or attacks by adversaries with the objective to disturb the operation of the wind turbine. In test case 2, the adversaries acquire the free wind speed, adds a normal distributed random number of zero mean and standard deviation of $\sigma = 1.2m/s$ equal to ten times the normal standard deviation of the free wind speed measurement in Table 5.2. In the third test case, the adversaries add an impulse of, $a_{pulse} = -1.2m/s$ on the free wind speed every 5^{th} second. The last data injection attack simulates a scenario where the adversaries distort the free wind speed signal through ramping with a slope equal to $a_{ramp} = -0.012m/s$.

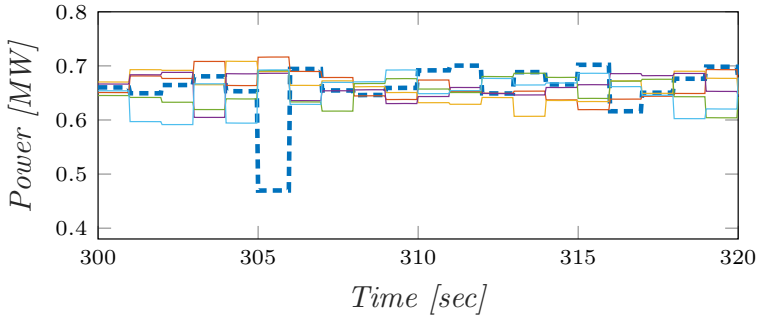
Gross measurement error for wind turbine 1 in the WPP test system

In the first test case, a single occasion of gross measurement error, equal to $\varepsilon = -1.2\sigma$, on the free wind speed signal for WTG1 in Figure 5.7 is simulated and investigated in a situation where the cyber error detection system is deactivated. The reason for deactivating the detection system is to illustrate how harmful gross measurement error can be to the plant controller.

The plots in Figure 5.8 and Figure 5.9 represent the results of simulating the system during steady state operation while being subject to an injection of gross measurement error. For each plot, the signals from all six wind turbines in the WPP are included, were WTG2 to WTG6 are represented with solid lines, and as WTG1 is the one being subject to gross measurement error its response to error in the free wind speed is highlighted by the dashed line in Figure 5.8a. The consequence of gross measurement error is seen directly in the WPP controller calculated active power set points in Figure 5.8b where WTG1 is highlighted by the dashed line.



(a) Wind speed measurement of all wind turbines



(b) Power set point control signal for all wind turbines

Figure 5.8: Wind speeds and active power set points of the WPP during single occurrence of gross measurement error on the free wind speed of WTG1, where its signals are highlighted with dashed lines, and the remaining wind turbines are represented in solid lines for the scenario where the detection system is inactive. Source: **[Pub. A]**

The occurrence of gross measurement error is clearly visible in Figure 5.8a, where the free wind speed signal of WTG1 is around 1 m/s lower than the other wind turbines. In both Figure 5.8a and Figure 5.8b, the value of the signal changes once every second due to the assumption of 1 Hz SCADA data acquisition frequency.

In Figure 5.8b, the active power set point decided by the WPP controller is shown for each wind turbine, where WTG1 has a considerably lower set point than the rest of the turbines. This happens

as the WPP calculates the expected available power for each wind turbine using the power curve characteristics and the received free wind speed measurements, the results of which are presented in the fourth column of Table 5.6. Here the available power calculated for WTG1 is estimated 0.25 MW less than for the other wind turbines in the WPP due to the lower free wind speed observation received by the WPP controller.

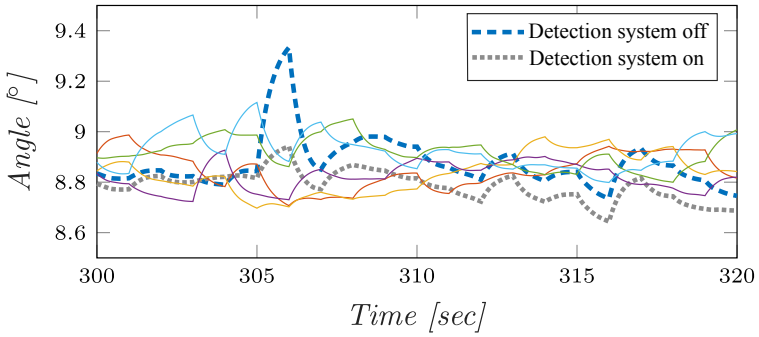
Table 5.6: Comparison of WPP controller signals with and without cyber error detection system

		$v[m/s]$	$P_{avail}^{WTG}[MW]$	$P_{avail}^{\%WPP}$	$P_{set}^{WTG}[MW]$
SE1 deactivated	WTG1	8.72	0.512	11.9%	0.516
	WTG2	10.20	0.781	18.2%	0.787
	WTG3	10.00	0.752	17.5%	0.759
	WTG4	9.98	0.748	17.4%	0.754
	WTG5	10.00	0.754	17.5%	0.761
	WTG6	10.00	0.755	17.6%	0.762
SE1 activated	WTG1	9.68	0.693	15.5%	0.672
	WTG2	10.16	0.781	17.4%	0.756
	WTG3	10.00	0.752	16.8%	0.728
	WTG4	9.98	0.748	16.7%	0.724
	WTG5	10.01	0.754	16.8%	0.729
	WTG6	10.02	0.755	16.8%	0.731

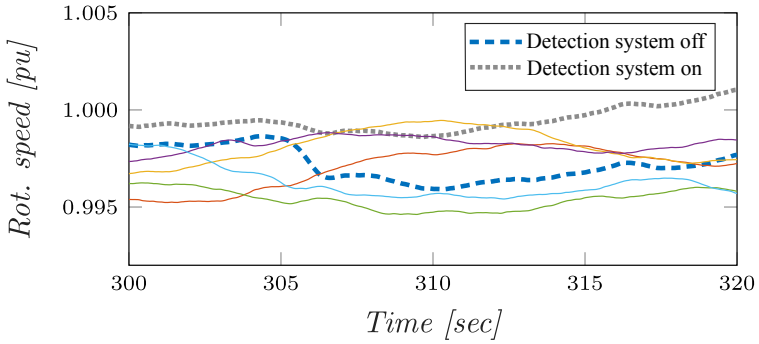
In Table 5.6, a comparison is made between two scenarios, where the cyber error detection system of WTG1 is deactivated and activated. From the P_{avail}^{WTG} in the fourth column in Table 5.6, the available active power for all wind turbines, except the first, in both scenarios are equal, clearly indicating that the only difference between the two scenarios is the status of the cyber error detection system. From the v signal received by the controller, it is apparent that when the cyber error detection system is active, the free wind speed is closer to the average speed of 10 m/s. The difference is due to the system having removed a part of the gross measurement error and estimated the signal value with higher accuracy than using the raw measurement directly. This result in a more equal distribution of available power between wind turbines in the WPP as described by the fifth and sixth columns of Table 5.6.

Furthermore, Table 5.6 indicates the capability of limiting measurement error through utilizing the cyber error detection system developed in subsection 5.2.1. The motivation behind removing the error is clearly visible when observing the blade pitch angle and rotational speed signals taken directly from the simulation model and presented in Figure 5.9a and Figure 5.9b, respectively. In both figures, the dotted line is the results of WTG1 from simulating the system with the distributed cyber error detection system activated.

The results in Figure 5.9a show how the change in the active power set point forces the blade pitch angle of WTG1 to increase rapidly. This is mainly due to the mismatch between the wind speed measurement received by the WPP controller and the actual wind speed experienced by WTG1. This mismatch is a result of the added gross measurement error and assumed noise in the communication channel. The distribution function in the WPP controller believes the first wind turbine is experiencing lower wind speeds than the other wind turbines and as a result asks WTG1 to decrease its active power generation seen in Figure 5.8b. As WTG1 experience higher wind speeds than believed by the WPP controller, it has to rapidly increase the blade pitch angle,



(a) Simulated blade pitch angle signal of all wind turbines



(b) Simulated rotational speed signal of all wind turbines

Figure 5.9: Blade pitch angle and turbine rotational speed from simulating the WPP during single occurrence of gross measurement error on the free wind speed of WTG1, where its signals are highlighted with dashed and dotted lines, and the remaining wind turbines are represented in solid lines for the scenario where the detection system is inactive. Source: **[Pub. A]**

shown in Figure 5.9a, to meet the active power set point set by the WPP controller. As the pitch angle increases from 8.8°to 9.5°, the aerodynamic efficiency of the blades decreases which slow down the rotational speed of the shaft, as shown in Figure 5.9b. In comparison, with the cyber error detection system activated the changes in blade pitch angle and rotational speed of WTG1 are similar to those observed for the remaining five wind turbines. This is because the detection system improves the accuracy of the physical system observability by reducing the mismatch between the wind speed perceived by the plant controller and experienced by WTG1.

From a mechanical and maintenance perspective, the gross measurement errors cause additional stress on the rotating parts. In this test case, only a single instance of gross measurement error is investigated. In the two following tests, the mechanical system is stressed further through injection of higher than normal measurement error and pulse injection of gross measurement error, respectively.

Random and pulse integrity attacks

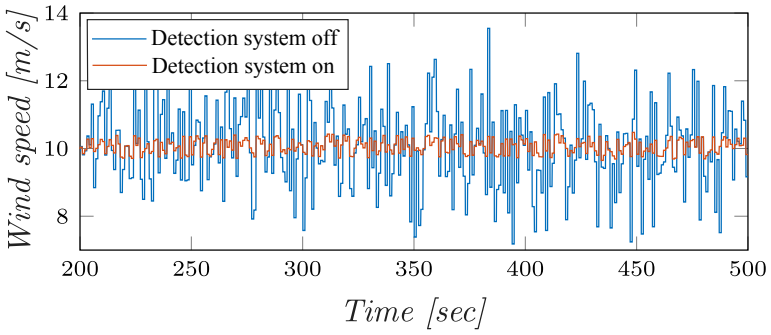
The analysis of the test cases with the injection of gross measurement errors through random and pulse data injection, starts by observing how the free wind speed signal received by the plant controller propagates with the distributed cyber error detection system deactivated and activated. The wind speed signals of the two test cases are shown in Figure 5.10a and Figure 5.10b.

From the free wind speed signal in Figure 5.10a, the measurement error is rather large compared to the average wind speed of 10 m/s, if the raw measurement is used to calculate the available active power in the WPP controller, it will affect the active power set point of WTG1, as observed in the gross measurement test case.

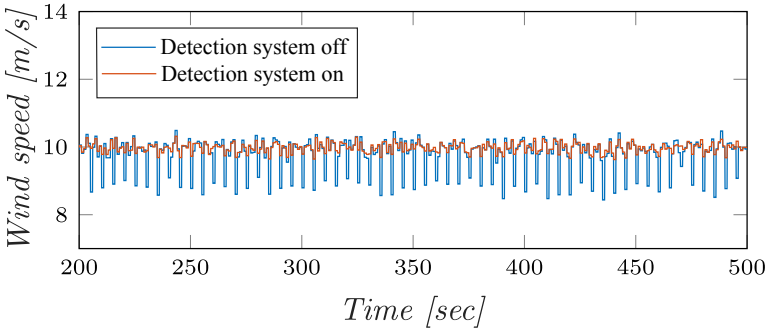
The large deviations in active power set point affects how the rotational speed of WTG1 changes. In Figure 5.10c the rotational acceleration between each second of operation is calculated through the time derivative and is shown for the two scenarios of random false data injection where the distributed cyber error detection system is either activated or deactivated. The results clearly show how the large measurement error cause more violent changes in rotational speed, which ultimately affects the lifetime of the rotating shaft.

For the third test case, the free wind speed signal is subject to a 0.2 Hz pulsating measurement error as seen in Figure 5.10b. The pulsating injection of bad data is included in the WPP calculations of the active power set point of WTG1, and can be observed affecting the acceleration of the rotating shaft in Figure 5.10d. For both these test cases, utilizing the distributed cyber error detection system can limit the higher mechanical stress entailed by data integrity attacks.

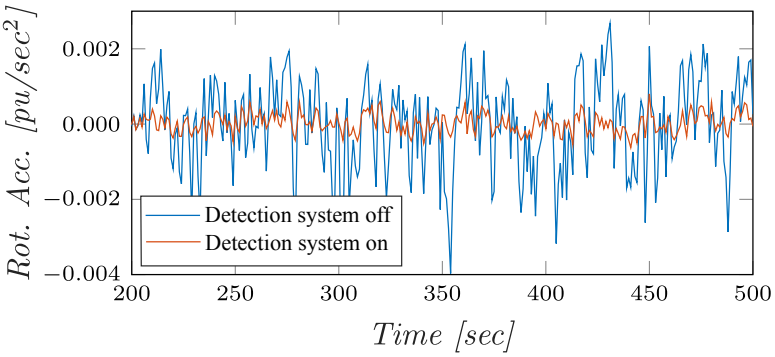
Lowering the lifetime and increasing maintenance cost is one way of attacking wind turbine generators, which was previously used in the famous Stuxnet attack on the Iranian nuclear program where centrifuges were controlled to run faster than rated speed causing their lifetime to decrease. A more direct approach would be to try to stall the turbine by ramping down the free wind speed signal until the rotational speed decreases beyond its tripping limit.



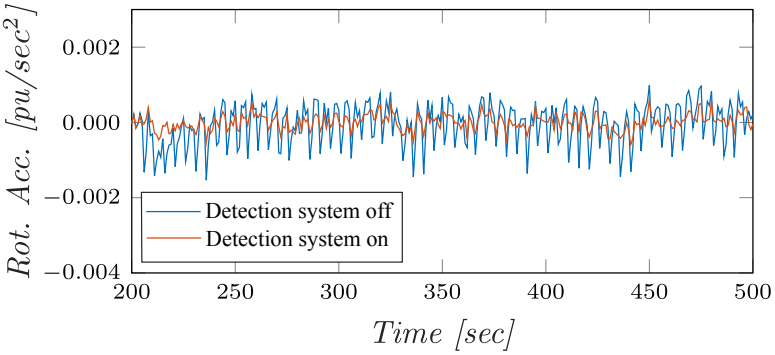
(a) Wind speed measurement of WTG1 during random integrity attack



(b) Wind speed measurement of WTG1 during pulse integrity attack



(c) Shaft acceleration signal of WTG1 during random integrity attack

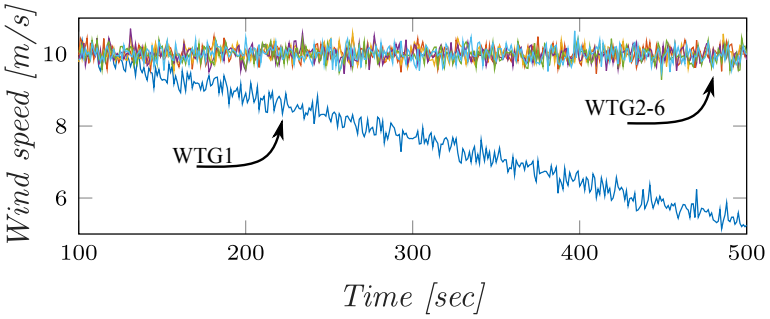


(d) Shaft acceleration signal of WTG1 during pulse integrity attack

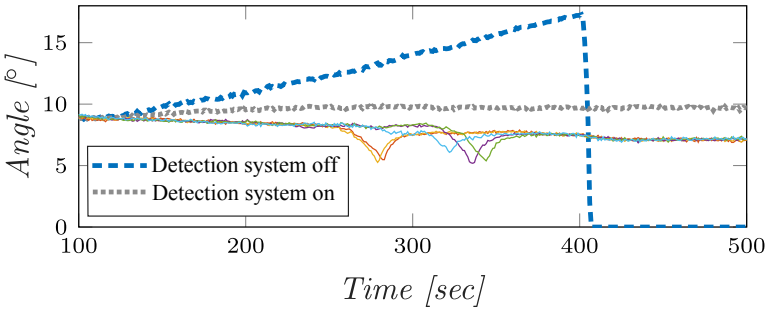
Figure 5.10: Simulation results for random and pulse injections of gross measurement error on the free wind speed signal. Source: **[Pub. A]**

Ramping integrity attack

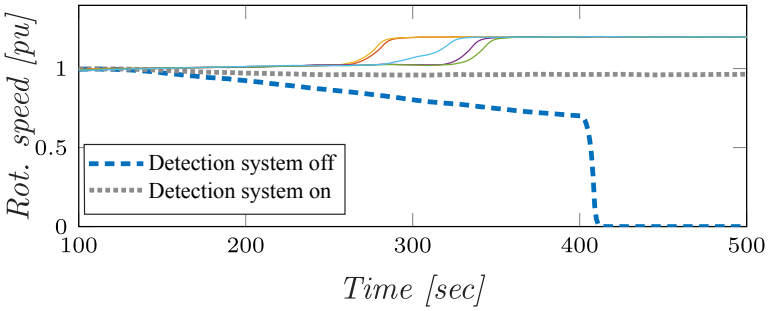
This test case is used to demonstrate whether the distributed cyber error detection system is able to prevent WTG1 from tripping during a ramping attack. First of all, the severity of ramping attacks is evaluated by observing the free wind speed measurement for all wind turbines in the WPP as shown in Figure 5.11a.



(a) Wind speed measurement of all wind turbines during ramping integrity attack



(b) Blade pitch angle signal of all wind turbines during ramping integrity attack



(c) rotational speed signal of all wind turbines during ramping integrity attack

Figure 5.11: Simulation results for ramping integrity attack on the free wind speed signal, where its signal are highlighted in dashed and dotted, and WTG2 to WTG6 are represented with solid lines for the case where the detection system deactivated. Source: **[Pub. A]**

Comparing the measurements of the different wind turbines in Figure 5.11a, a clear difference is visible between the wind speed of WTG1 and the remaining five turbines. This is due to the information integrity attack that tries to mimic a situation where the wind speed is slowly decreasing. The consequence of the decreasing wind speed is visible in Figure 5.11b, where the blade pitch angle of WTG1, highlighted by the dashed blue line, is slowly increasing compared to the other wind turbines. The pitch angle increases due to the mismatch between observed

free wind speed from the wind turbine and the WPP controller perspectives. As the central plant controller receives information of lower than actual free wind speed, it calculates a lower than actual P_{avail}^{WTG1}. And as the WPP controller uses a dispatch function for curtailment operation, P_{set}^{WTG1} is lower than necessary.

Therefore, the local controls of WTG1 needs to increase the pitch blade angle considerably more than the other wind turbines in the WPP. Around the 400th second of simulation time, the pitch angle starts decreasing drastically. The reason can be observed in Figure 5.11c, where the rotational speed of WTG1, highlighted by the dashed line, slowly decreases proportionally to the free wind speed signal. After approximately 400 seconds, the rotational speed exceeds the lower tripping limit, assumed equal to 0.7 pu. From the results in Figure 5.11c, a visible difference is also observed in the rotational speed of the 5 other wind turbines in the WPP around the 300th second of simulation. As the power production of WTG1 decreases, the other wind turbines needs to compensate for the missing active power causing them to increase their rotational speed. The effects of the ramping attack means one of the wind turbines shut down, increasing the share of generation responsibility for the remaining generators. This affects the plant owner as fluctuations in the wind can cause dips in production and thereby decrease the economic benefits of the WPP and the reliability of the DG controls offered to the network operator.

The system is simulated once again, now with the cyber error detection system activated. In Figure 5.11b and Figure 5.11c, the blade pitch angle and rotational speed, of WTG1 in this scenario, is illustrated by the dotted line. Clearly, the detection system improves the operational situation of the WPP as it helps avoiding a tripping of WTG1. In Figure 5.11b, the blade pitch angle of WTG1, in this scenario, is observed slightly higher than the other wind turbines, consequently, the rotational speed is slightly lower for WTG1 in Figure 5.11c. The reason for these differences is the limited accuracy of the state estimation model based on the functional modeling approach. If substituted by a cyber error detection system based on physical modeling, it could be more accurate, however, it would entail a higher computational requirement as well as necessary detailed parameterization for different models.

5.4 Conclusion

From a CPES perspective, the importance of reliable DG control increase with the decentralization of generation, especially with the decommissioning of large fossil fuel power plants. With numerous distributed units, the coordination of resources challenges network operators as the optimal control actions are calculated based on network observation. Therefore, the protection of the DG control resources against cyber system errors is important. This chapter presents the process of applying functional modeling for the representation of a wind turbine generator, and how the representation is used to establish a state estimation model that can be implemented on a distributed processor topology as illustrated with Figure 2.2c as part of a distributed cyber error detection system that serves as a bottom-up approach to CPES protection of DG controls.

As requested in the formulated high level research approach in subsection 2.3.3, the functional model representation of a wind turbine generator and its functional relations is presented graphically through MFM. From this model, the key functions and relations were identified to form a state estimation model as a trade-off between level of details and computational burden. Furthermore, the estimation model was solved through orthogonal factorization, which is a more robust state estimation algorithm than the Newton method and therefore supports the execution on a distributed

processing topology concept shown in Figure 2.2c. Choosing a NI cRIO platform as a distributed processor, the state estimator was implemented together with a bad data detection, identification and elimination process that is based on the J_{sum}-test. This chapter therefore presents an approach to evaluate and support information integrity in DG based power plants, and a demonstration of its value in protecting DG control assets from adversaries.

Executing the cRIO in connection to a simulation model of a generic wind turbine generator was done to illustrate the time requirements for converging the established state estimation model and its ability to remove gross and extreme measurement error in a stand-alone operation scenario. Simulation results show that the simplified state estimator has a fast execution time which offers utilization in current and future measurement systems. Compared to utilizing raw measurement data, the simplified state estimator has similar average Euclidean error as normal measurement error and can remove gross measurements, which shows its application potential in the cyber-physical energy system. The system, however, did not perform perfectly as the bad data detection algorithm misidentified the location of bad data in the case study with extreme measurement error on the active power signal. Such erroneous identification could lead to decreased integrity of the processed information, and should therefore be avoided.

Implementing the distributed cyber error detection system as part of a WPP simulation test case was done to evaluate its performance in different information integrity attack scenarios. From these studies, the system was shown capable of limiting the effects of attacks on the lifetime and maintenance of the mechanical assets in a wind turbine. Furthermore, it has been demonstrated how the state estimator prevents wind turbine tripping while subject to a ramping attack. In this demonstration it was, however, shown that with the simple state estimation model, the cyber error detection system was delayed in detecting the ramping attack, meaning the affected wind turbine caused an imbalance in the distribution of power curtailments.

Integrating the developed cyber error detection system into the DG units in a RES-based power plant would benefit the plant owner in different perspectives. As shown in the analysis of the wind turbine during different integrity attacks, a control of the DG assets based on information about operational conditions can cause unnecessary control actions. With these controls potentially changing the mechanical system, its components are subject to excessive wear. Stressing mechanical systems usually entail an increase in maintenance costs and reduction of component life time. In addition, maintenance issues could be falsely reported if there are errors in the acquired information. With the proposed cyber error detection system, individual DG units would be protected against unnecessary maintenance and additional stress of the mechanical system components from cyber-physical interactions. Furthermore, with RES-based power plants being subject to grid integration requirements, such as provision of different controls of the active and reactive power injection into the power system, the power plant owner must ensure compliance. This requires a high integrity of the information about the interconnection between power plant and the remaining power system, as a misalignment between observed and actual power flows can affect the power system operation. With integration of the cyber error detection system, a validation of the information from the DG units would be enabled to increase the integrity of the information acquired within the RES-based power plant.

CHAPTER 6

Investigation of control strategy coordination in cyber-physical environment

This chapter investigates how operational conditions in a cyber-physical environment affect the performance of DG controls during local and optimization-based decentralized control strategies. As described in chapter 1, with their dependency on both cyber and physical operation conditions, DG controls risk execution of hazardous control actions if not both CPES domains are considered. The coordination between local and decentralized control strategies hence follows the formulated high level research approach in subsection 2.3.4 considering representations of both control strategies presented in existing literature and introduced in subsection 2.2.2.

Firstly, a simple cyber-physical simulation platform is established that satisfies identified requirements in terms of power system and DG control simulation, simple communication network representation with an assumption of full observability of physical conditions, and an emulation of a decentralized processor topology as shown in Figure 2.2b, with optimization capabilities. Next, the cyber-physical simulation platform is used to investigate the operation of the Cigré LV network feeder in Figure 3.4 during physical perturbations and cyber disturbances. Afterwards, the observations from simulating the LV feeder in different cyber-physical conditions are evaluated to formulate a set of guidelines for network operator control strategy decision making. Finally, the performed investigation is summarized and evaluated from a network operator perspective. The majority of this chapter is based on published material in [**Pub. B**], with minor changes to coherently fit into the framework of this thesis.

6.1 Real-time cyber-physical simulation platform

When evaluating the performance of control strategies of DG units introduced in subsection 2.2.2, it is important to consider the effects of environmental changes in both the physical domain and the cyber domain of the CPES. In particular, the use of optimization-based control strategies are critical as they tend to push the operation of the physical system towards vulnerable regions [24, 176, 177]. The investigation of cyber disturbances on such decentralized control strategies can be done using a cyber-physical simulation platform [19, 58]. Such a platform can model and simulate the cyber and physical systems to show the relations between the two domains at different levels of complexity. For the evaluation of decentralized control of PV plants in LV networks, the simulation platform must support optimization and real-time control, emulating the processes in a decentralized and distributed processing topology described in Figure 2.2b and Figure 2.2c, respectively. With a simulation platform capable of emulating a distribution network, both local and decentralized

control strategies can be simulated and compared during different cyber-physical operational situations.

Numerous cyber-physical simulation platforms are proposed in current literature, with different focus and levels of complexity [19, 178]. The diversity of simulation platforms is due to the specific focus of different studies, which affects the requirements of the established platforms. Furthermore, while real-time power system simulators can be purchased and installed directly from manufacturers, current cyber-physical simulators are usually a combination of different software and hardware components. These components are connected to enable specific studies in different areas of power system research, e.g. transmission, distribution, and microgrids. To establish a cyber-physical simulation platform, it is therefore important to define the study specific requirements and identify appropriate software and hardware components. In this work, there are five main requirements:

1. The platform should be capable of solving the optimization problem defined by an objective function in (2.8), (2.9), or similar, subject to a set of constraints as those defined in (2.10) to (2.15).
2. The platform must allow simulation of a LV distribution network with high penetration of PV-based power generation.
3. The platform should enable implementation of local control strategies for the PV plants in the simulated LV network, such as those illustrated with the four different strategies in Figure 2.3.
4. The platform must enable switching between different DG control strategies, both decentralized and local.
5. The platform must represent a completely controllable ICT infrastructure.

With the list of requirements, an appropriate power system simulator would be the RTDS, as it can simulate a LV distribution network and allows implementation of local control strategies. The RTDS is a combination of hardware and modeling software that has been used extensively in the formulation of cyber-physical simulation platforms [19, 178–180]. The RTDS allows real-time external communication of simulated values through so called GTNETx2 cards. These cards are installed with firmware that correspond to different communication protocols, such as PMU, Distribution Network Protocol (DNP3) and IEC 61850 sampled values.

The RTDS is not capable of performing the needed optimization of the decentralized PV control strategy, meaning it must be connected to additional software components. The MATLAB software can provide the needed optimization capabilities, and allow customization of the mathematical problem and the use of different solvers. Communication of simulation results and control signals between RTDS and MATLAB is possible by running the RTDS simulation software, called Runtime, as a TCP server [181]. The Runtime software is used to control and monitor the simulations conducted by the RTDS and contains different meters and actuators. When running the Runtime software as a TCP server, its meters and actuators are visible from the MATLAB environment, which enables direct control of the RTDS simulation through MATLAB [181]. However, the acquisition of data is more complicated as MATLAB must encode the Runtime meter data to a

specific syntax, and afterwards decode the value to enable processing. Therefore, an alternative way of data acquisition from RTDS to MATLAB is considered.

From current literature on cyber-physical simulation platforms, the acquisition of data from RTDS can be done through an Open Platform Communications (OPC) server [179, 180]. These servers are commonly used in industrial sites to manage the translation of data from different meters to a common protocol [182]. An OPC server can therefore directly communicate with the GTNETx2 card of the RTDS. Furthermore, MATLAB provides an OPC toolbox, making communication between the two components simple to establish. The main argument against using the OPC communication channel for control signals is a combination of limited computational resources of the RTDS, and because control actions communicated through the OPC server require utilization of the RTDS resources.

The last requirement for the simulation platform involves the representation of the ICT infrastructure and control of its performance. In different simulation platforms, communication system simulators, e.g. OPNET and NS-3, or hardware is used [19, 178–180]. While these give a realistic representation of the cyber-system and the specific protocols, they offer limited control capabilities. For the current study focus, the platform should allow full observability of the network, and a representation of cyber disturbances, e.g. communication noise. Therefore, the cyber-system is emulated in the MATLAB software through the control of noise added after the acquisition of simulation results and before sending control signals to RTDS. Compared to current literature, the established platform is similar to the platforms proposed in [179] and [180], although with a simplified ICT infrastructure emulation and the use of MATLAB instead of a hardware representation of the decentralized processor. An overview of the established cyber-physical simulation platform is presented in Figure 6.1.

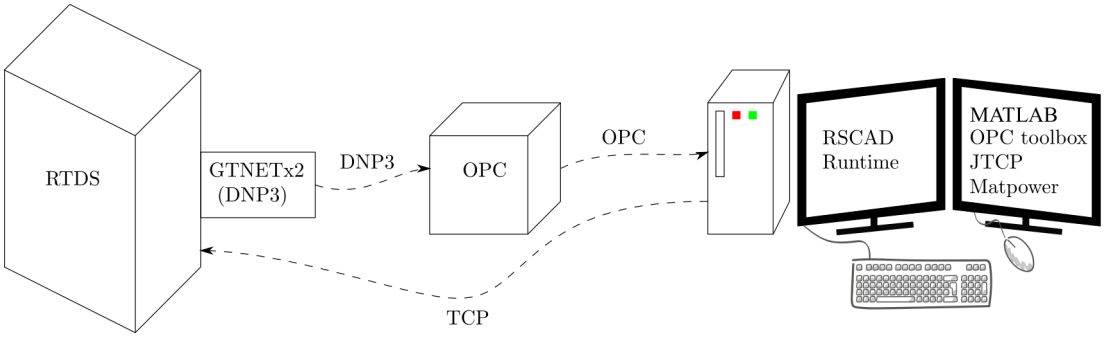
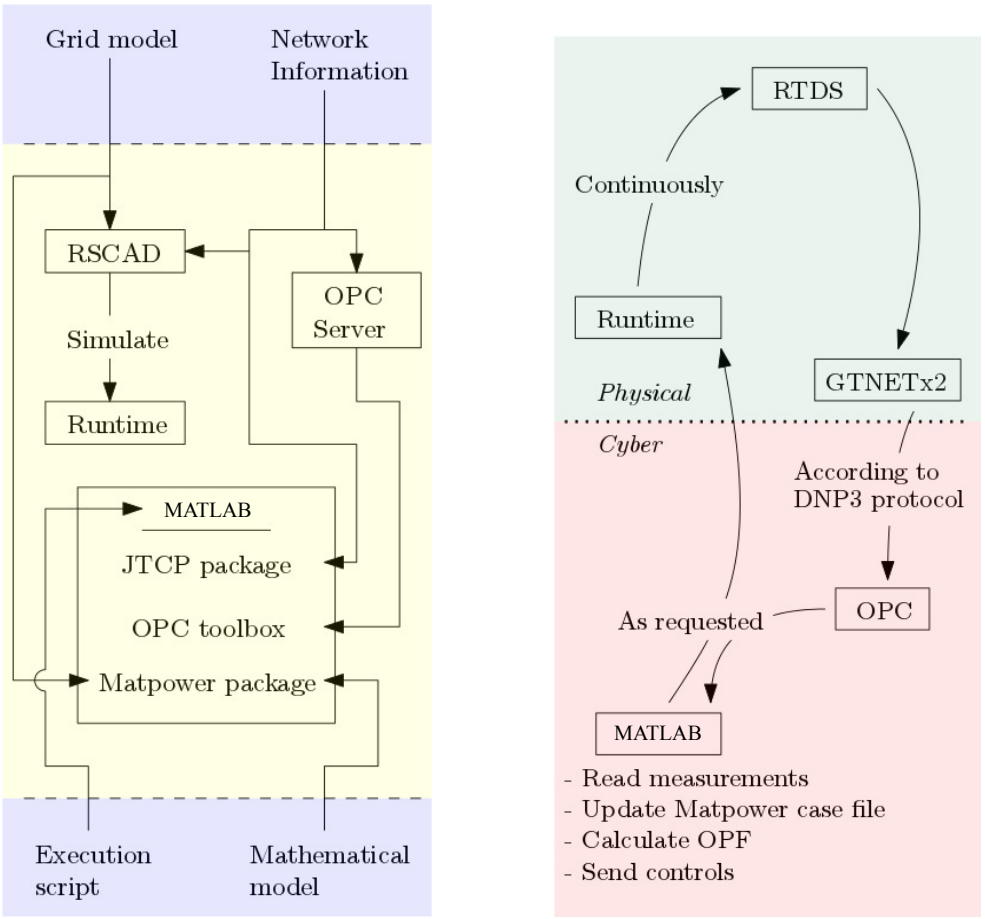


Figure 6.1: Overview of cyber-physical simulation platform composed of RTDS, OPC server and a decentralized processor emulation

The simulation platform in Figure 6.1 is configured by first defining four input sets, represented in the blue areas of Figure 6.2a. The "Grid model" contains information about the power system infrastructure of the LV feeder under investigation. The "Network information" input defines the cyber network in which the simulation platform is installed and contains information such as IP addresses, protocol information and port numbers of the RTDS. The "Execution script" input is used to control the cyber system representation in MATLAB, and describes how and when the computation software must execute as well as the operational characteristics of the cyber system. In this work, the "Execution script" input depends on the scenario being investigated and is changed accordingly.



(a) Platform configuration

(b) Platform execution. Source: **[Pub. B]**

Figure 6.2: Cyber-physical simulation platform set up and execution flowcharts

The simulation platform is here created for reactive power control of PV plants implemented in the simulated LV network, but by changing the "Mathematical model" input, it could be used for other studies, such as battery charging or demand response investigations. The yellow part of Figure 6.2a shows how the different parts of the simulation platform are connected and fed with the four defined input sets. First a representation of the grid model is implemented into the RTDS modeling software called RSCAD, together with utilization of the GTNETx2 card and definition of the measurement points being send through the OPC based communication channel. The grid model can then be compiled and simulated using Runtime. Next, the OPC server is configured to connect to the GTNETx2 card on the RTDS rack and to use the appropriate port number according to the protocol installed as firmware. Now, the MATLAB software can connect to the OPC server using the OPC toolbox. Besides connecting to the OPC server, MATLAB connects to Runtime using the JTCP package, this enables control of the Runtime components from MATLAB. Finally, the Matpower package requires information about the grid for which it is calculating the Optimal Power Flow (OPF) while considering reactive power control of DG units within the simulated LV feeder.

When running, the cyber-physical simulation platform executes as illustrated by the flowchart in Figure 6.2b. The flowchart is split in a physical part, representing how performed control

actuation conducted in the Runtime environment are continuously recognized by the representation of the physical system in the RTDS. Furthermore, Figure 6.2b shows how the RTDS enables the external communication of measurements through the GTNETx2 card. The cyber system is then executed according to the DNP3 protocol and the user-defined execution. With the DNP3 protocol, values are only updated when their change is larger than a predefined threshold value as described with the event-driven transmission setting in section 4.1. MATLAB can read measurements from the OPC server, update the parameter in the optimization problem constraints in (2.10) to (2.14), find the optimal solution through OPF, and send new control commands to the PV plants in the test grid.

6.2 Cyber-physical environment condition impact on DG control strategies

To evaluate the cyber-physical nature of the power system, and how it affects the usage of both local and decentralized DG reactive power control, different physical perturbations and cyber disturbances are considered. In a LV feeder, physical faults on equipment most likely interrupts services as controls are limited. Instead, perturbations in the physical system considered in this work are based on the impact from neighboring systems, such as the weather system and residential consumer behaviour.

The interdependencies of the cyber-physical system indicates the necessity for analyzing not only how perturbations in the physical system affect the physical system, but also how cyber disturbances affect the physical system. Additionally, one could investigate how cyber disturbances and physical perturbations affect the cyber system, however, this requires a more detailed and realistic representation of the ICT infrastructure, which is outside the scope for the current study. While perturbations in the physical system affect the LV feeder when utilizing local and decentralized control of DG units, cyber disturbances will have a smaller impact on local control since it is a continuous process. A single occurrence of error will therefore quickly be erased compared to the decentralized control, where the control is only executed in a discrete fashion.

Cyber disturbances that can affect the physical system during decentralized control, can be split into three areas. Errors occurring 1) in the process of acquiring measurements from the sensor and sending them to the decentralized processor, 2) within the calculation of control commands in the decentralized processor, and 3) in the process of communicating and performing the commands send by the decentralized processor. The analysis of the perturbations in the physical system and cyber disturbances is hence conducted by running the cyber-physical simulation platform while activating different scenarios, one at a time. The impact of these scenarios is evaluated through an analysis of the effects in voltage magnitude and active power losses. The power losses are considered as a performance indicator as they are minimized in the decentralized control strategy objective function presented in (2.8), and the voltage magnitude is evaluated for assessing the network operational security. The scale of impact from the scenarios depends on the power system feeder and the operational conditions considered.

6.2.1 Case study: Cigré LV feeder in Copenhagen, Denmark

To scope the investigation, a Cigré European LV feeder model is chosen and modified to represent a future scenario, furthermore, a set of operational test scenarios has been formulated for the city of Copenhagen in terms of neighboring energy system operation. The original Cigré LV feeder is presented in [138] and illustrated in Figure 3.4.

The original Cigré feeder has been modified in four ways and integrated in the established cyber-physical simulation platform. Firstly, the load connected to node $R1$ in Figure 3.4 is removed and its demand is distributed among the rest of the loads, similar to the modification performed in section 3.3. This gives a higher requirements of power transfer within the LV feeder and represents a feeder in an urban area of a large city with large building blocks connected to each load-point. The peak consumption of each load in the modified grid is given in Table 6.1.

Table 6.1: Rated power consumption and generation of load points in modified Cigré network in Figure 6.3

Node	$R1$	$R11$	$R15$	$R16$	$R17$	$R18$	All
Load [kVA]	0	55	92	92	75	87	404
PV [kVA]	0	15	42	42	21	42	162

Secondly, PV plants have been implemented at each of the load points, as shown in Table 6.1 and the single line diagram of the modified LV feeder in Figure 6.3, representing a scenario where each building block has invested in DG. Thirdly, due to the computational resource limitations of the RTDS with PV plant representations, the cables in the original grid are aggregated to remove the nodes with zero current injection as shown in Figure 6.3 using the Kron reduction method [see Appendix A.1]. Finally, the cables connecting $R1$ to $R3$ and $R4$ to $R6$ have been reinforced by implementing parallel lines to allow the higher transport of power in the distribution network. All other grid details are as described for the original Cigré European LV residential feeder described in [138].

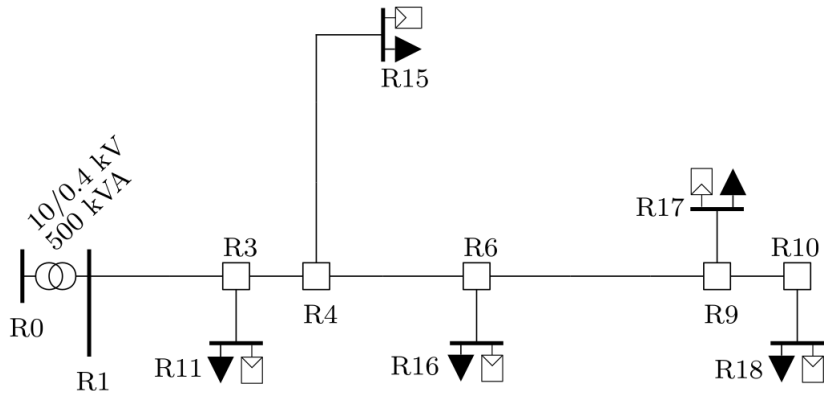


Figure 6.3: Modified Cigré European LV benchmark network. Source: **[Pub. B]**

Reactive power control strategies

Since the focus of the current study is to evaluate the performance of both local and decentralized control of DG in a cyber-physical environment, grid code specified implementation of $cos\phi(P)$ is

considered as shown in Figure 2.3c. Where the specific strategy considered for all the PV plants in this work is equal to the one introduced in section 4.3 where unity power factor is maintained for an active power generation between 0 and 50% of rated characteristics as described in Table 6.1. Above half the active power generation, the $cos\phi$ follows a linear curve towards 0.9 lagging at 100% of rated operation.

For the decentralized control strategy an objective of minimizing the active power losses within the network is considered by solving the optimization problem composed of the objective function presented in (2.8) subject to the constraints in (2.10) to (2.15). The active power generation of the PV plants is assumed uncontrollable to avoid differentiation between the different residential load points, meaning both P_n^{min} and P_n^{max} in (2.13) are set equal to P_n^{gen} for all nodes n in the LV network. The reactive power capabilities of the PV plants are assumed limited in (2.14), by a power factor between 0.9 lagging and 0.9 leading and therefore depend on the operational conditions of the PV plant.

Physical operating conditions in Copenhagen

To choose the operational conditions of the power system environment, hourly data of irradiance for Copenhagen (CPH), Denmark of the year 2005 [183], and hourly consumption data from apartments in Denmark in 2012 [184] are found. To give an indication of the combinations of load and irradiance levels in CPH, the gathered irradiance data have been rounded to nearest 10 W/m^2, and the gathered consumption data has been normalized to the largest consumption in the data set for the whole year and rounded to nearest 1% loading level. A heat map has been created as shown in Figure 6.4 by finding the corresponding point in the irradiance-consumption plane for each hour in a year.

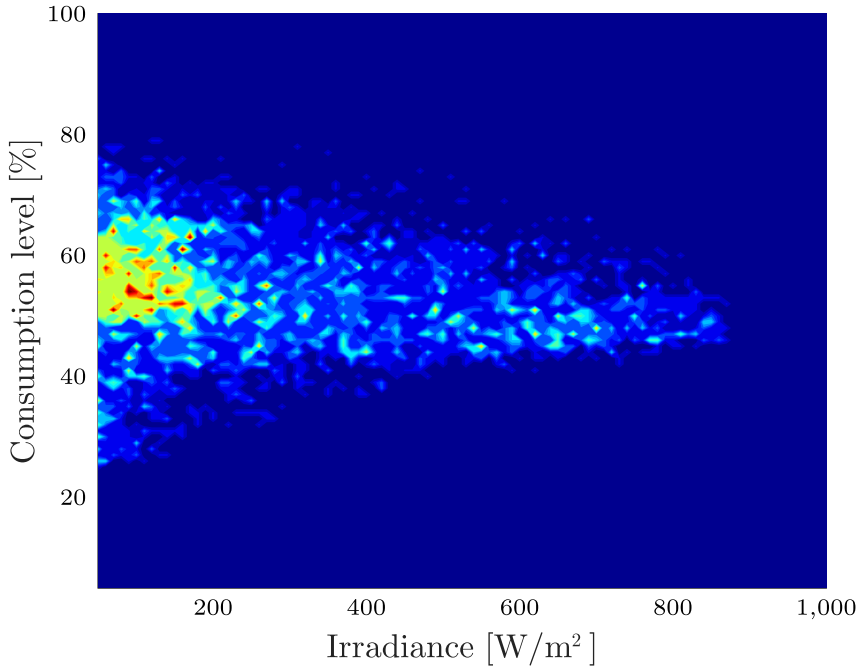


Figure 6.4: Heatmap of irradiance and consumption data in Copenhagen based on hourly data. Source: **[Pub. B]**

The intensity of the representation in Figure 6.4 reveals that the most likely combination is an irradiance around 100 W/m^2 at a consumption level of around 55%. With the Cigré feeder and the CPH configuration, the cyber-physical simulation platform is utilized in five different test scenarios.

6.2.2 Cyber-physical environment test scenarios

The first test scenario compares the two DG reactive power control strategies while the system is not exposed to any CPES disturbances. The LV feeder is simulated in every possible operating situation in the irradiance-consumption plane and the PV plant reactive power control strategies are evaluated from a voltage magnitude and network loss perspective.

In the second test scenario, the system is exposed to perturbations in the physical system, specifically as changes in consumption and irradiance level at the load points connected to node R15 in the Cigré feeder in Figure 6.3. Again, the voltage magnitude and network loss results are used to evaluate the effects of both reactive power control strategies.

The third, fourth, and fifth test scenarios investigate the impact of cyber system disturbances on the decentralized control strategy. The LV feeder is simulated in three different operating situations and exposed to noise in the data acquisition and command signal communication channels. The results of the simulations are evaluated, based on the effects on the optimizer performance, the network losses, and the voltage magnitude of the most vulnerable node.

Control strategy comparison in ideal conditions

Simulations of the modified feeder in all possible combinations of the irradiance-consumption plane shown in the heatmap of Figure 6.4, are performed using the cyber-physical simulation platform established in this work as described in section 6.1. Specifically, the grid is simulated with a consumption level of 5% to 100% of the maximum consumption from the profiles in [184], in steps of 5%. The irradiance is changed from 50 W/m^2 to 1000 W/m^2 in steps of 50 W/m^2. The resulting loss comparison is shown in Figure 6.5 where the network losses as a function of irradiance level is plotted for four different consumption levels during decentralized control D_C, solid lines, and local control D_L, dashed lines.

Comparing the effect of the control strategies on network losses within the feeder, clearly shows a large difference as the irradiance increases from 50 W/m^2 to 1000 W/m^2, corresponding to rated PV plant operation. This is due to the inductive nature of the chosen reactive power control plan used in the local control strategy and shown in Figure 2.3c. In Figure 6.5 the crosses represent the smallest irradiance level at which decentralized control gives 1 kW less losses than local control for the four represented consumption levels. An interesting observation in Figure 6.5, is that there appears to be an optimal PV generation for each consumption level where the losses are minimal. This corresponds to the situation where the consumption is mainly supplied by local PV, which minimize the amount of power flow in the grid and thereby the active power losses.

The results from the simulations are further used to compare how the voltage magnitude is affected by local and decentralized DG reactive power control strategies. Theoretically from (2.7), the highest voltage magnitude at any of the nodes in the modified feeder would happen in the bottom right corner of the irradiance-consumption plane in Figure 6.4, where consumption is low, and irradiance is high as discussed in subsection 2.2.2. The node in the modified Cigré LV feeder

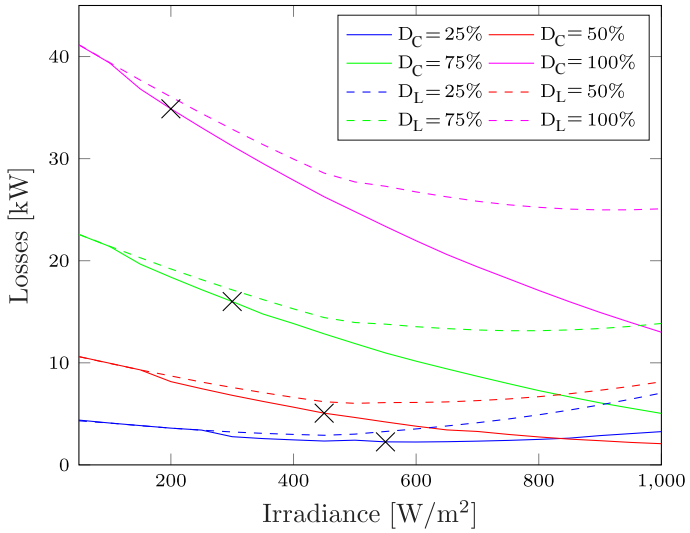


Figure 6.5: Active power losses in the modified LV feeder using decentralized D_C, solid lines, and local D_L, dashed lines, control, for different consumption and irradiance levels. The crosses show irradiance level where decentralized control result in 1 kW less losses than local control. Source: **[Pub. B]**

experiencing the highest voltage magnitude during low consumption and high irradiance, is found to be $R15$.

To investigate the voltage vulnerability of the system during normal operational situations, the heatmap of irradiance and consumption in Figure 6.4 is layered with contour lines representing the node $R15$ voltage magnitude for each operational scenario. Two sets of contour lines are included in Figure 6.6, the solid lines showing the results during decentralized control, and dashed lines showing the results during local control.

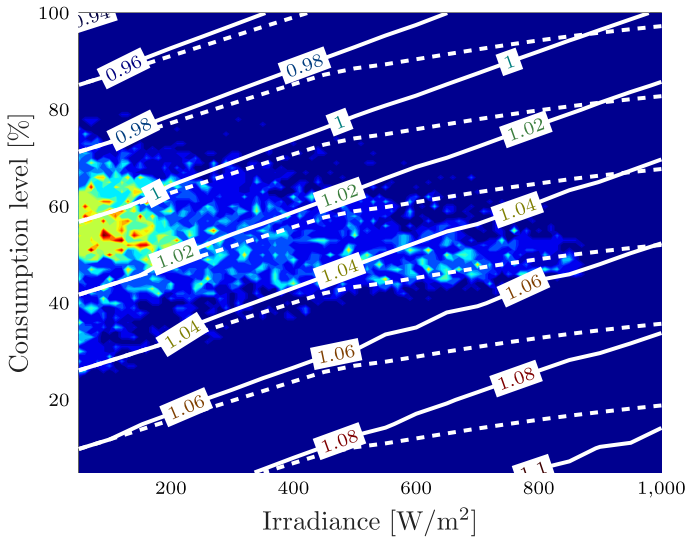


Figure 6.6: Irradiance and consumption heatmap for normal operation in Copenhagen, with contour lines representing the voltage magnitude of node $R15$ during decentralized control, solid line, and local control, dashed line. Source: **[Pub. B]**

From Figure 6.6 clearly the voltage magnitude is most vulnerable during high irradiance and low consumption, in fact the voltage limit of 1.1 pu with a rated voltage magnitude of 400 V line to line, is exceeded during this operation with decentralized control. Furthermore, the dashed contour lines show that during local reactive power control, the node $R15$ voltage magnitude will not exceed 1.1 pu. This clearly emphasizes the necessary trade-off between voltage vulnerability and loss minimization when deciding on appropriate control strategies.

Based on the heatmap for irradiance and consumption for CPH included in Figure 6.6, the local control strategy will at most result in 1.04 pu at node $R15$, while the decentralized control can reach 1.06 pu. This is not exceeding the voltage magnitude limit of 1.1 pu. But as discussed, with the electrification of services through installation of large consuming units e.g. heat pumps and EV, the heatmap in Figure 6.4 showing the normal combinations of irradiance and consumption can be affected. The maximum consumption representing 100% in Figure 6.4 will increase due to the implementation of large consuming units and push the current peak of irradiance-consumption combinations in Figure 6.4 towards 0%, thus creating two peak irradiance and consumption combinations at low and high consumption levels. Furthermore, a greater energy efficiency of household electrical appliances will lower the peak of irradiance-consumption combinations closest to 0%. For a future feeder scenario the changes in load point composition can potentially push the operating area towards the vulnerable region with high irradiance and low consumption.

Control strategy comparison during physical system perturbations

Besides the long-term changes affecting the operational situation, the occurrence of perturbations in the physical system can be interpreted as shifting the operational point of the irradiance-consumption plane. This interpretation is valid under the assumption that the effects are only analyzed during static operation.

From the results in the first test scenario, the feeder can experience over-voltage during high irradiance and low consumption when being centrally controlled. Therefore, the effect of physical perturbations is studied in two conditions. Firstly during present normal operation of CPH, which is found in Figure 6.4 and highlighted in the blue area of Figure 6.7. Secondly during more vulnerable operation of the LV feeder, highlighted by in the yellow area of Figure 6.7. In both studies, the possible situations due to exposure of physical perturbations are included.

For each operational scenario, the blue and the yellow regions of Figure 6.7, changes in consumption of 5%, 10% and 20%, negative and positive, and changes in irradiance of 50 W/m^2, 100 W/m^2 and 200 W/m^2, negative and positive, are considered. The changes in the operational situation caused by the physical perturbations are represented in Figure 6.7 in the green and the red areas for normal and vulnerable operation conditions, respectively.

The physical perturbations are simulated in the cyber-physical simulation platform while controlling the PV plants through the local and decentralized control strategies. During local control, the system is simulated for a couple of seconds in each of the situations in the blue and yellow areas of Figure 6.7 and exposed to each of the physical perturbations returning results representing the system operation in the blue, green, yellow and red areas of Figure 6.7 as illustrated in the top half og Figure 6.8. For the decentralized control strategy, the reactive power is optimized at the situations in the blue and yellow areas of Figure 6.7. After one second of simulation and after the decentralized processor has estimated and distribution optimal PV control set points within the LV network, the system is exposed to a perturbation in the physical system and simulated for

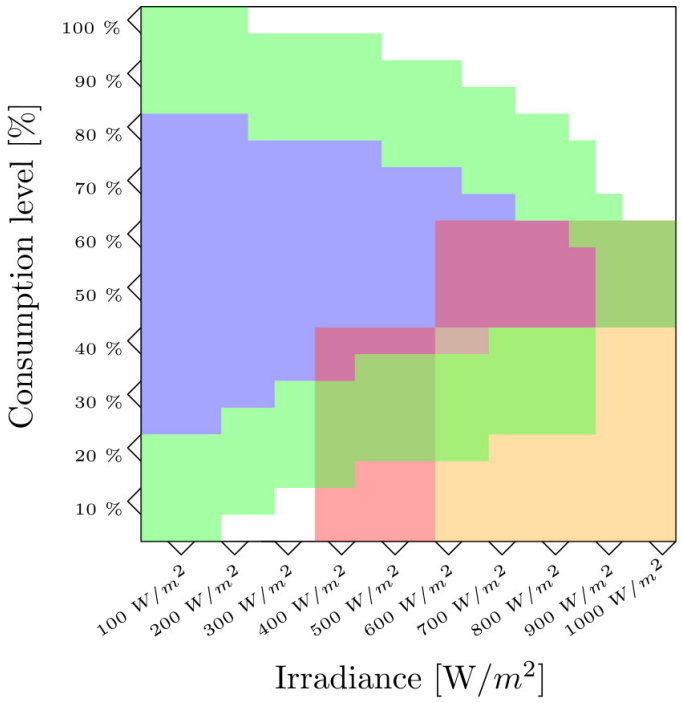


Figure 6.7: Irradiance-consumption plane with the normal operation of Copenhagen in blue, including the area of operation during physical perturbations, in green, and a vulnerable operating area, in yellow, with matching physical perturbation area, in red. Source: **[Pub. B]**

seconds. Then the reactive power is optimized again, and the system is simulated for an additional five seconds. This gives an opportunity to analyze the impact of physical perturbations pre- and post-optimization as shown in the bottom half of Figure 6.8.

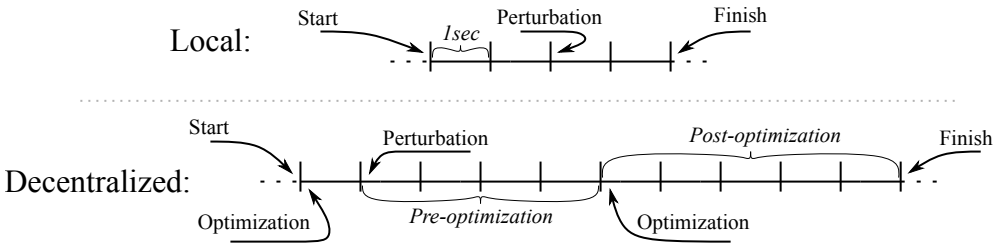
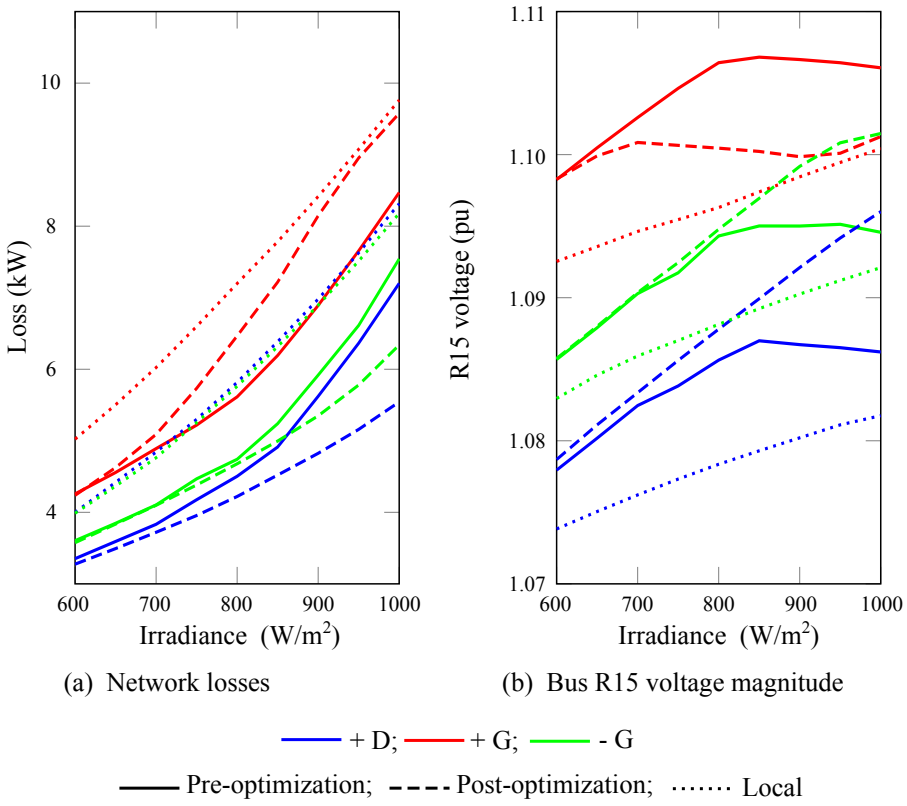


Figure 6.8: Physical perturbations simulation sequence for the two control strategies

The simulation results of all the irradiance and consumption level combinations in the normal CPH operating conditions highlighted in blue in Figure 6.7, showed that in all of the simulated conditions, the system survived the perturbations in the physical system considered, which is visible since the none of the operating conditions in the green areas of Figure 6.7 cause over-voltages according to Figure 6.6.

For the vulnerable operating situations highlighted in yellow in Figure 6.7, however, the most severe operating conditions were substantially impacted by the physical perturbations. This impact is illustrated by the simulation results for 5% consumption level and exposure to a 20% consumption increase, and a 200 W/m^2 irradiance increase and decrease, are shown in Figure 6.9.

In both plots of Figure 6.9 the solid lines represent the simulation results during decentralized



(a) Network losses (b) Bus R15 voltage magnitude

Figure 6.9: Results from simulating physical perturbations during low consumption high irradiance, represented by the network losses and the node $R15$ voltage magnitude. Source: **[Pub. B]**

control after a perturbation and before the optimizer has reacted to the new operational situation, described as the pre-optimization conditions in Figure 6.8. The dashed lines represent the post-optimization results, and the dotted lines represent local control.

The system losses in Figure 6.9a as a function of irradiance show that at high irradiance and low consumption, a consumption increase, +D, and irradiance decrease, -G, will increase the losses until the reactive power has been optimized according to the new operational situation. At 1000 W/m^2, the pre-optimization losses nearly reach the local control system losses.

An irradiance increase, +G, will have the opposite effect as the pre-optimization losses are lower than the post-optimization losses. The reason is clearly visible in Figure 6.9b where the irradiance increase causes the pre-optimization node $R15$ voltage magnitude to violate the 1.1 pu voltage limit. The optimizer then lowers the voltage as seen by the post-optimization voltage magnitude, which increase the system losses. This observation shows the importance of caution when choosing an appropriate periodic execution of the decentralized optimization control strategy for DG protection against hazardous actions.

Decentralized controls strategy during small cyber error in information acquisition

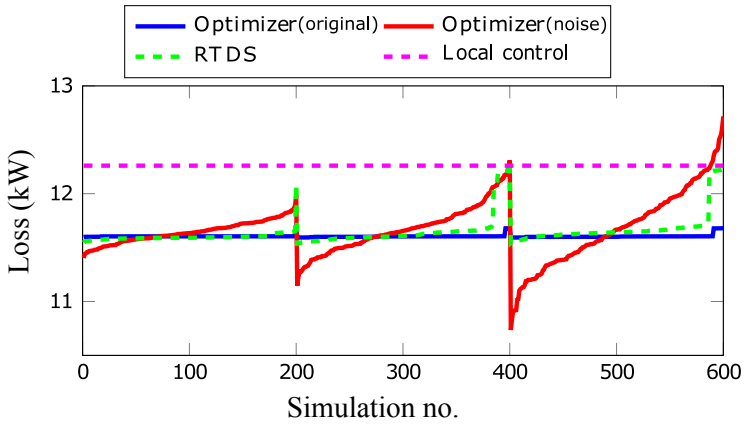
With the distributed cyber error detection system developed and demonstrated in chapter 5, gross and extreme measurements according to the definition in Figure 2.4 can be detected, identified, and eliminated. But due to its simplicity, the cyber error detection system did struggle with eliminating lower degrees of information integrity disturbance. In this case study, the impact of these small errors and other information integrity disturbances in the flow of information, is considered from a decentralized control strategy perspective.

Through utilizing the cyber-physical simulation platform established in this work, the effects of three different cyber disturbances are investigated and analyzed. Firstly, the occurrence of noise in the acquisition and communication of observations in the physical system is investigated, where the noise is assumed to have zero mean and standard deviation of 0.005, 0.01 and 0.02 relative to the rated network line to line voltage of 400 V and the respective maximum power consumption and generation at each load point. Secondly, the substitution of one or two of the acquired measurements by zeros is investigate. This scenario represents an extreme case where zero-readings are input to the decentralized processor. Finally, the occurrence of noise in the communication and interpretation of command signals by the PV plants, of zero mean and standard deviation of 0.005, 0.01 and 0.02 is evaluated.

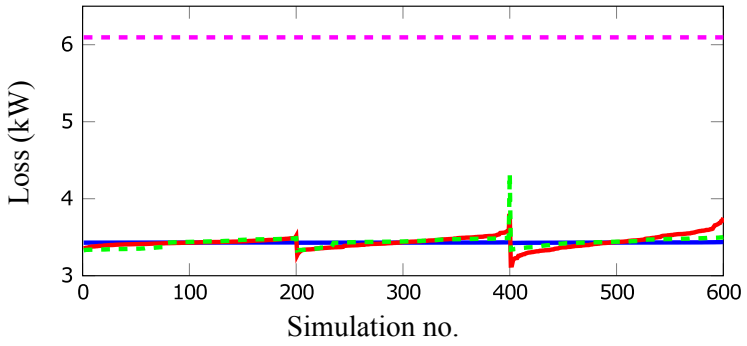
For each of the cyber disturbances, the LV feeder is simulated with decentralized control in three different operating situations, representing three characteristic conditions. Situation 1 represents normal CPH conditions with 60% consumption and irradiance of 200 W/m^2 according to Figure 6.4. Situation 2 represents a future scenario with low consumption of 20% and high irradiance of 900 W/m^2, and situation 3 represents another future scenario with high consumption of 70% and high irradiance of 800 W/m^2.

When noise is introduced in the measurement acquisition part of the ICT infrastructure either in the metering or communication of information, the immediate effect will be on the performance of the optimizer. The investigation of the effects of the first cyber disturbance for each of the three operating situations is therefore done by comparison of the network losses calculated by the optimizer using original and correct measurements, those calculated by the optimizer using measurements subject noise with the three different magnitudes of standard deviation, losses calculated by the RTDS in the cyber-physical simulation platform, and finally, the network losses corresponding to the first test scenario in Figure 6.5 during local reactive power control of the PV plants.

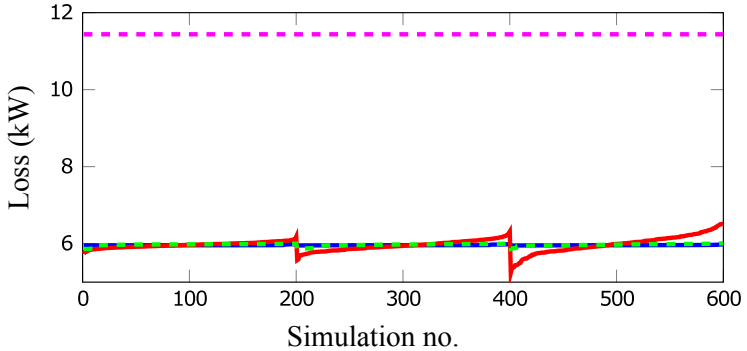
The network losses from the four different calculations are shown in Figure 6.10 sorted in an ascending order, for each of the three operating situations from minimum to maximum, where a standard deviation of 0.005, 0.01 and 0.02 is assumed in simulations 1 to 200, 201 to 400 and 401 to 600, respectively.



(a) Situation 1: 60% consumption and 200 W/m^2 irradiance



(b) Situation 2: 20% consumption and 900 W/m^2 irradiance



(c) Situation 3: 70% consumption and 800 W/m^2 irradiance

Figure 6.10: Effects of small noise in the measurement acquisition channel during three different operating situations with decentralized reactive power control. Source: [**Pub. B**]

The effects of measurement noise are clearly visible in Figure 6.10a, where the network losses calculated by the optimizer using the original measurements is constant, and the losses calculated using noisy measurements deviates substantially as a function of the magnitude of the noise standard deviation. The noise therefore affects the optimizer to believe that it either can operate with lower network losses, or must operate at higher network losses.

The difference between the optimizer calculated network losses and the actual losses observed in the RTDS is due to the noise in the measurements which distorts the integrity of the information about the physical system conditions. The severity of the impact from noise in measurements, from a network loss minimization perspective, can be analyzed by comparison of the RTDS observed losses and the previously calculated network losses during local control for the first operating situation. At a low noise magnitude, only a single simulation caused network losses close to the expected losses from local control at the first operating situation. However, at standard deviation of 0.01 and 0.02, more than 10 of the simulations, equal to 5% of the number of simulations, caused network losses only marginally different from what was found during local control in Figure 6.5.

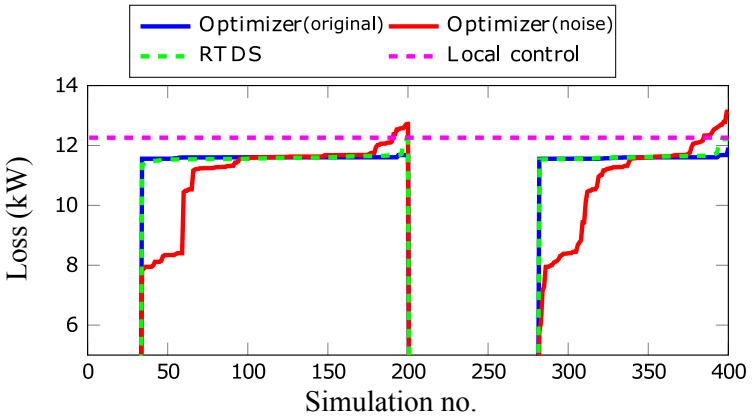
By comparison of the effects from measurement noise in the three different operating situations, all three situations are affected, where the effect is based on the influence and reactive power control capability of the PV plants in the system and the gradient in the network losses caused by changing the $cos\phi$ set points. As the nonlinear optimization problem is solved using the FMINCON algorithm, the optimal solution is found by initializing the algorithm with the noisy measurements and move in the direction of the largest negative gradient of the network losses. During high irradiance and low noise levels, the algorithm will therefore be more robust in terms of finding the correct optimal solution than during low irradiance as visible in the first 200 simulations of situation 2 and 3 in Figure 6.10b and Figure 6.10c, respectively. To have an impact during higher irradiance, the cyber disturbances must be more significant, which is studied in with the second cyber disturbance, where one or two of the measurements have been substituted by zeros.

Decentralized controls strategy during large cyber error in information acquisition

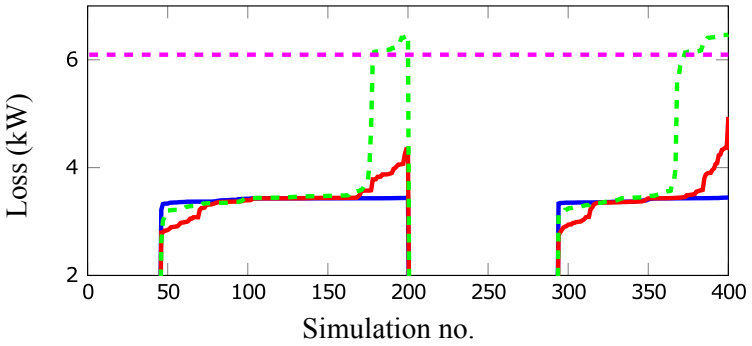
Substituting measurements by zeros can be interpreted as severe noise in the cyber system. This has been tested by randomly selecting one or two of the measurements used in the optimization algorithm and substituting its value by zero and maintaining original values for all other measurements. As with the previous cyber disturbance under investigation, the system is simulated during the three different operating situations using the established cyber-physical simulation platform, and the effects on each situation are evaluated from a network loss perspective, shown in Figure 6.11.

The x-axis of Figure 6.11 represents the simulation number. From simulation 1 to 200 one of the measurements has been substituted by zero, and from simulation 201 to 400 two measurements have been substituted with zeros. For each of the three operating situations, the cyber disturbances cause the optimizer to not converge in at least one of the simulations, which is shown as 0 in the sorted list of ascending losses in Figure 6.11. In reality, the losses will in such conditions depend on the backup strategy chosen in case the optimizer does not converge.

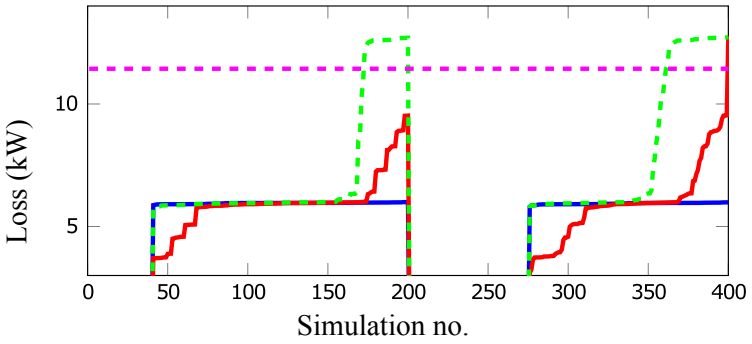
Comparing the losses calculated by the optimizer using original and noisy measurements in Figure 6.11, clearly the substitution of zeros for measurement values affect the optimizer calculation results. The impact difference is more severe than in Figure 6.10 due to the chance of one or two of the load point consumption levels being observed as zero, thereby lowering the required power



(a) Situation 1: 60% consumption and 200 W/m^2 irradiance



(b) Situation 2: 20% consumption and 900 W/m^2 irradiance



(c) Situation 3: 70% consumption and 800 W/m^2 irradiance

Figure 6.11: Decentralized control strategy efficiency with measurements substituted by zeros during three different operating situations. Source [**Pub. B**]

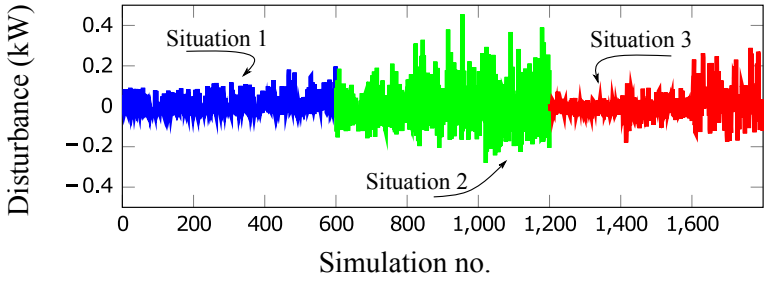
flow. This show the importance of protecting the DG decentralized control strategy against gross and extreme measurement errors.

Comparing the results for each of the three operating situations in Figure 6.11, the cyber disturbance has larger impact during the second and third operating situations, because the disturbances in some occasions are large enough to divert the optimizer from the global minimum and instead command more inductive power factor set points from the PV plants according to a local minimum. As the irradiance is high during these operating situations, the sub-optimal control of the power factor will have a large effect on the system losses, visible from the RTDS acquired losses in Figure 6.11b and Figure 6.11c. Besides noise in the measurement acquisition channel, the

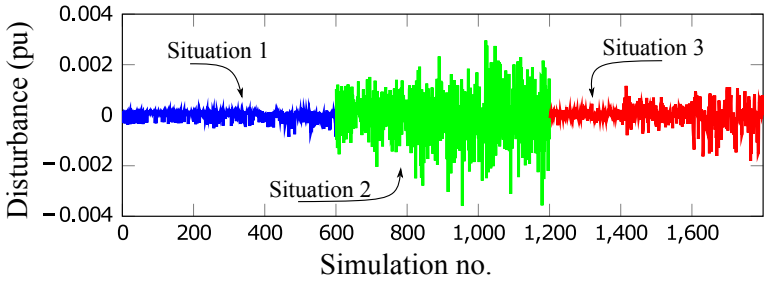
effect on the decentralized control strategy is evaluated by exposing the distribution of command signals, i.e. power factor set points, to noise of varying degrees of standard deviation.

Decentralized controls strategy during cyber error in command distribution

The system is simulated for each of the three operating situations, represented by the blue, green and red parts of the lines in Figure 6.12. A noise standard deviation of 0.005 is assumed in the simulations 1 to 200, 601 to 800 and 1201 to 1400. For simulations from 201 to 400, 801 to 1000 and 1401 to 1600, the standard deviation of the noise is assumed 0.01 and for the rest of the simulation results, the noise standard deviation is assumed 0.02.



(a) Network loss disturbance



(b) Bus R18 voltage disturbance

Figure 6.12: Results from simulating cyber disturbance between optimizer and PV plants for three situations. Source: **[Pub. B]**

From the network losses, in Figure 6.12a, the cyber disturbance on the power factor set points clearly has an impact, which is seen most severe for the second operating situation. This is due to the high percentage of PV plant generation compared to load consumption in this scenario, which increases the influence of the reactive power control of the PV systems in the network. The effects of the set point noise also affects the voltage magnitude of the nodes in the system, mostly for the node furthest away from the feeder, i.e. node $R18$ in Figure 6.3, as its voltage is affected by the error from all the prior feeders.

The voltage magnitude disturbance of node $R18$ is visible in Figure 6.12b for all the three operating situations, from which the impact can be considered only marginal. However, as the noise magnitude increases, so does the disturbance. The vulnerability of the voltage in the considered operating situations is not close enough to the upper limit of 1.1 pu to experience over-voltage, as the maximum voltage is experienced in the second operating situation equal to 1.09 pu and the observed voltage magnitude disturbance is less than $\pm 0.004pu$.

In this work full observability of the network conditions is assumed, which means there are sufficient measurements from the system to execute the optimization algorithm, and perhaps the

effects of cyber disturbances are not pronounced due to this assumption, or due to the simplicity of the algorithm for decentralized control itself. This study however, shows that the cyber system can affect the operation of DG controls within a LV feeder, specifically as disturbances in the system losses and the node voltage magnitudes. Furthermore, the cyber system disturbance simulation test cases show the importance of considering a backup strategy for the decentralized control in case the optimizer does not converge.

6.3 Control strategy decision making guidelines

Coordination between the decentralized and local control strategies of reactive power for LV network integrated PV plants must enable the exploitation of the voltage rise alleviation capabilities from local control visible in Figure 6.6. Furthermore, the coordination should support network conditions by gaining optimal benefits from decentralized control illustrated in Figure 6.5. Based on the cyber-physical environment impact scenarios considered in subsection 6.2.2, guidelines for when to use local and decentralized control for the Cigré European LV feeder are formulated as identified boundaries in the irradiance-consumption plane. The intention with this coordination is to assist the network operator in the decision-making and thereby ensure secure operation of LV networks in the CPES, without the shortcomings of each individual control strategy.

Results from the cyber-physical simulator show two zones for coordinating reactive power control, one area where the decentralized control improves the operation of the network without jeopardizing the security of supply, and one region where local control is suggested. Furthermore, the simulations with cyber disturbances during decentralized control show how artifacts in the communication channels can have a considerable impact of the performance of the control strategy. The guidelines for coordinating the two control strategies are represented in Figure 6.13, where the blue color represents areas to use local control and the orange color shows areas to use decentralized control. In addition, the numbers within the irradiance-consumption plane represents the operating situations evaluated during the cyber error disturbance simulation studies.

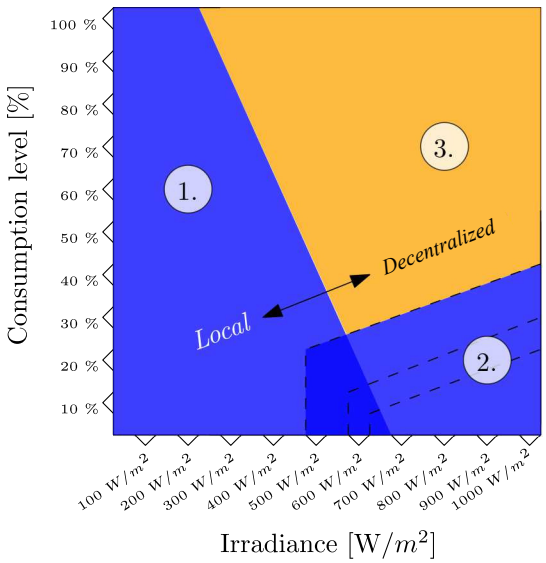


Figure 6.13: Guidelines for operating the PV systems with local, blue area, and decentralized, orange area, reactive power control strategies. Source: **[Pub. B]**

The first observation, marked in Figure 6.13, is made from the direct comparison between the two strategies during no perturbations in the physical system. Such comparison is investigated in Figure 6.5, where the active power losses of both control strategies were presented for four different consumption levels. The significant benefits from utilizing a decentralized control strategy with an objective of minimizing active power are highlighted with crosses in Figure 6.5 for each consumption level. Here a loss reduction of 1 kW compared to local control is chosen to represent a significant benefit, and the crosses in Figure 6.5 show how the active power loss reduction depends on both the consumption and irradiance level. From this analysis, the first part of the guidelines in Figure 6.13 are defined by the boundary from a point with 100% consumption and 200 W/m^2 to a point of 5% consumption and 650 W/m^2, and represent the boundary of when a significant active power loss can be achieved from using the decentralized control strategy compared to the local control strategy considered in this work.

The second observation is based on the analysis of the impact from changes in consumption and irradiance level within the vulnerable operating area highlighted in yellow in Figure 6.7. Here the perturbations could cause over-voltage in node R15. Therefore, the over-voltage vulnerability area in the bottom right corner of the irradiance-consumption plane is marked in blue in Figure 6.13. Here three dashed lines represent the severity of physical perturbations the system should be able to resist, with the largest to smallest areas representing a consumption change of 20%, 10% and 5% combined with an irradiance change of 200, 100 and 50 W/m^2, respectively.

While the local control strategy offers security against over-voltage and decrease the utilization of communication, decentralized control is recommended in the orange area of Figure 6.13, as it can substantially decrease network losses without jeopardizing the voltage magnitudes during perturbations in the physical system. Utilizing decentralized control however, entails a vulnerability towards disturbances in the cyber system.

As shown in Figure 6.10, the occurrence of small measurement error in the acquisition of measurements has very limited impact on the active power losses during the third operation situation considered, which lies within the decentralized control strategy beneficial region of the coordination guidelines in Figure 6.13. While small errors in the distribution of optimized set point commands also has limited impact during the situation 3 operational conditions as shown in Figure 6.12, the possibility of large measurement errors represented by the replacement of measurements with zeros in Figure 6.11 has a substantial effect on the resulting active power losses during these operating conditions, but not severe enough impact on voltage magnitude conditions to violate security limits as shown by Figure 6.6 although this might change in future composition of the LV network.

6.4 Conclusion

This chapter investigates the cyber-physical environment impact on the performance of DG controls during local and optimization-based decentralized control strategies using a simple cyber-physical simulation platform. The established simulation platform consists of an RTDS, an OPC server and a MATLAB client. Furthermore, the simulation platform contains a controlled emulation of the ICT infrastructure and representation of a decentralized processor that can acquire real-time simulated information and execute an optimization algorithm. Utilizing the established simulation environment for satisfying the high level research approach formulated in subsection 2.3.4, shows

how the CPES interdependencies affect PV plant controls in a LV feeder during both considered control strategies.

The simulation of a Cigré European benchmark LV feeder shows how minor and major measurement errors in information flow from the metering devices to the decentralized processor have different degrees of impact on the performance of optimization algorithm to reach its objective of minimizing the operational active power losses. An evaluation of cyber disturbances in the information flow between the decentralized processor and the DG units shows a small impact on the coordination of DG units in the LV network. Here, the received control commands are distorted and are therefore different from the optimized set points. This means the PV plants in the network are unable to fully achieve the minimized active power losses. In general, the cyber vulnerability is highest during low consumption and high irradiance, in which the LV network is simultaneously more likely to experience voltage security issues. In such conditions, caution should therefore be taken when utilizing a decentralized control strategy. As an alternative, the local control strategy can be considered as it is independent from the communication channel performance that, however, entails limited possibility of coordination between DG units.

From a network operator perspective, the cyber-physical simulation of a LV network reveals the importance of coordinating between local and decentralized control strategies. In particular, the results show how the physical steady state and the possible changes in neighboring energy systems must be considered when coordinating between the two control strategies. Furthermore, the cyber disturbance investigations reveals the importance of removing gross measurement error from the acquired network information, and to have a back-up strategy for decentralized control in the case of divergence. These results are evaluated and utilized to form a set of guidelines that support the reactive power control strategy decision making process for the LV feeder under investigation. With these simple guidelines, the network operator can protect the DG units against hazardous control actions through changing the control strategy of all units within a feeder.

Part IV

Conclusion

CHAPTER 7

Conclusion and future work

The interdependencies between the electric power system and its supervision and control infrastructure have tightened with the increasing deployment and utilization of metering, communicating, and processing technologies. The power system thereby transits into a CPES as revealed by recent power system disturbances caused by hazardous ICT infrastructure operation. Moreover, the decentralization of generation through integration of RES-based DG and the decommissioning of central fossil fuel power plants, has shifted the active and reactive power control capabilities from the transmission to the distribution network, increasing the importance of ensuring operational security at this part of the electric power system. With existing security assessment and protection approaches focused on the transmission network, this thesis explores the possibility of assessing and protecting operational security in the distribution network. In this part of the CPES however, assessment is impeded by limited ICT infrastructure performance and concerns of information security that challenge existing approaches for distribution network monitoring, especially at the LV network level where residential load points are connected. Furthermore, the protection of distribution network secure operation relies on the performance of DG controls, which depends on the operational conditions of both the cyber and the physical system environment.

7.1 Conclusion

This thesis investigates the consequences of the CPES transition from a distribution network perspective, with a particular focus on LV network monitoring and protection of DG controls. The concerns related to information confidentiality, integrity, and availability, and to limited ICT infrastructure performance are considered for both studied research areas. With these concerns, firstly, two approaches for monitoring LV networks are proposed, secondly, the protection of DG control is studied through the application of a DG cyber error detection system, and through an investigation of the impact from cyber system disturbances and physical system perturbations on the coordination of DG control strategies.

7.1.1 Low voltage network monitoring

With LV network monitoring as a vital part of distribution network security assessment, two challenges are considered from a CPES perspective, i.e. low measurement availability and decentralized processing limitations. Considering these challenges, the proposed LV network monitoring solutions enable an estimation of network conditions based on existing metering infrastructure, and can be viewed as intermediary steps towards more advanced security assessment of distribution networks. With assessment of network security at the LV level, operators can identify critical feeders and are given an input to estimate appropriate control actions for DERs.

Low information availability

Consumer information confidentiality concerns and limited distribution network ICT infrastructure affect the availability and integrity of the information used for estimation of LV network operational conditions. The limited availability in terms of information quantity and content impedes application of existing DSSE approaches.

Therefore, this work proposes a solution that offers an alternative estimation approach and enables monitoring of LV networks with smart meters deployed, during low measurement availability. The proposed methodology considers acquired voltage magnitude measurements from individual smart meters one by one, and returns estimated network conditions as intervals that gives network operators an overview of the LV feeder operating conditions. As such the proposed method is based on an acknowledgement of information confidentiality concerns, integrity issues, and availability limitations.

The developed method estimates the LV network operating conditions through utilizing available information about the network topology, conductor impedance, and number, type, and topology specific distribution of connected load points. It adopts an assumption that the operator is restricted to only utilize the shared network information, i.e. voltage, due to consumer privacy concerns. The limitations of available information mean the proposed approach is based on an estimation of the worst case current intervals for each of the LV network conductors, resulting in the greatest voltage magnitude deviation across the conductors. While the current magnitude interval can be obtained directly from aggregating the expected maximum and minimum current in each line segment from the load type and distribution within a radial feeder, the current angle in each interval boundary is identified through solving an optimization problem for each line segment.

With the estimated worst case current intervals, the received voltage magnitude readings can be processed individually through establishing an interval based on the meter accuracy rating, and by assuming worst case current in line segments connected to the measured node. This gives the voltage magnitude intervals at the neighbouring nodes, and the process of considering worst case current in the adjacent line segments can be continued until the complete feeder is estimated. With a simulation study of the proposed LV network monitoring approach, assumed simplifications in estimating the worst case current angle through optimization are analyzed, and the method is shown reliable in encapsulating the voltage profile within the estimated intervals.

Decentralized processing limitations

Integrating DG in LV networks means the operational conditions can be affected by the volatility of neighbouring energy systems. This challenges existing DSSE approaches due to their periodic and time consuming execution, meaning the estimation results can be diminished. Furthermore, limited metering and communicating performance at the LV network entails a risk of missing elements in the DSSE data set. Due to the tight coupling with individual consumer behavior, filling these empty data set elements is challenged by the limited accuracy of estimating consumption profiles.

As an alternative to existing applications of DSSE, a bi-level estimation platform is developed and presented in this PhD project. The platform is based on a bi-level processing architecture where one processor handles periodically acquired network measurements through executing DSSE, and the second processor continuously update network condition intervals through processing

event-driven measurements. This enables the estimation of network conditions during and in-between the periodic DSSE execution. The proposed platform thereby acknowledges the limited ICT infrastructure and information security challenges through considering the challenges of long execution times and replacement of missing DSSE data set elements.

The proposed bi-level estimation platform addresses LV network monitoring through application of DSSE, while estimating network conditions during and in-between periodic DSSE execution through a distinction between periodic and event-driven measurements. This work assume that all smart meters are configured to transfer information periodically, and that the network connected DERs are configured to only share information in the event of a change in their operational conditions. On one processor, a three-phase DSSE is executed in a periodic manner according to the timing of acquiring periodic measurements from network metering infrastructure. In cases where information availability constraints and the performance of the ICT infrastructure cause missing elements in the DSSE input data set of the first processor, these are filled by input from the second processor updated network conditions.

As the second processor runs independently of the DSSE execution, event-driven updates can be processed during the DSSE execution. With event-driven measurements, the processor estimate how the registered change in the physical system affect the current flow within the entire LV feeder by utilizing the identified change to estimate an interval of the branch current in each line segment. From the estimation, the voltage magnitude of all nodes can be estimated as intervals. For the estimated intervals of network conditions to follow the most recent DSSE estimation, periodically estimated DSSE results are utilized to re-evaluate the intervals estimated during DSSE execution. The proposed bi-level estimation is studied through analyzing its performance in different information availability conditions, through evaluating the LV feeder topology and load distribution impact on the accuracy of the estimated intervals, and through considering its accuracy when aggregating the estimated intervals across a 1-minute time duration. These studies show promising application of the proposed application of DSSE for LV network monitoring.

7.1.2 Protection of DG controls

With a focus on the protection of the DG controls, two challenges are considered from a CPES perspective, i.e. information integrity disturbances, and coordination in cyber-physical conditions. With these challenges, investigations are performed and approaches are proposed to improve the reliability of the DG controls within the CPES.

Information integrity disturbance

With the importance of reliable DG controls, especially when aggregated to form a DG-based power plant, information integrity disturbances on DG controls can have substantial impact on network operational security and entail a risk of hazardous control actions. Avoiding such conditions from the application of state estimation and BDD algorithms for individual DG units requires careful system representation that allows a detection of cyber error through evaluation of physical system operation.

This work considers functional modeling as an approach for high level representation of a wind turbine generator and its internal relations. With these key relations, a cyber error detection system is created through implementation of a state estimation and a BDD algorithm. With the functional

modeling representation of the physical system, as a foundation for the established state estimation model, a cyber error detection system is established and demonstrated as a bottom-up approach for protection of DG controls against information integrity disturbances.

The wind turbine cyber error detection system considers the limited processing capability of the distributed processing units through careful representation of the physical system. The wind turbine generator is modeled using functional modeling and is graphically represented through MFM, where the identified key physical relations and quantities are included in the established state estimation model. Furthermore, requirements for distributed processing application are identified and considered. Such requirements are satisfied through establishment of the state estimation model, and through utilizing orthogonal factorization as the state estimation algorithm. With the addition of a BDD, the cyber error detection system can detect, identify and eliminate information integrity issues.

The protection of DG-based power plants is demonstrated through the development of the distributed cyber error detection system. Such system is evaluated in a stand-alone situation and as part of a DG-based power plant. The cyber error detection system is simulated during ICT infrastructure disturbances, and during situations where adversaries exploit the cyber vulnerability of the wind turbine control panel to inject information integrity attacks. For the stand-alone situation, the cyber error detection system is implemented on a NI cRIO processing unit and is capable of identifying gross and extreme measurement error. Furthermore, a simulation study of the cyber and physical infrastructure of a WPP with the cyber error detection system implemented at each DG was conducted. Here the impact from different information integrity attacks by adversaries were considered, and the cyber error detection system demonstrated an ability to improve the security of DG control against cyber system disturbances.

Coordination in cyber-physical conditions

With different opportunities for DG control in the distribution network, e.g. local and decentralized, and control performance impact from both cyber and physical system conditions, careful coordination in decision-making is necessary. In particular information security concerns challenge network operators in determining appropriate control strategies during different cyber-physical conditions.

To assist network operators at LV network in protection of DG controls against hazardous actions in the CPES environment, this work investigates the reliability of DG control strategies in different cyber-physical conditions. In particular, the impact of neighbouring energy system volatility during local and decentralized control is studied through establishment and execution of a real-time cyber-physical system simulation platform that includes an emulation of metering, communicating, processing, and control capabilities.

The real-time simulation platform is composed by an RTDS that performs real-time simulation of the physical system, a MATLAB client that emulates the ICT infrastructure performance, and an OPC server that communicates information from the RTDS to the MATLAB client. The investigation of the DG control performance impact from the cyber-physical operating conditions includes a study of the physical system condition impact on the benefits from utilizing an optimization based decentralized control strategy rather than local controls. Furthermore, a study of how physical system perturbations between periodic estimation and transmission of DG reactive power set points affect the performance of decentralized controls is evaluated. Finally, the effects from

information integrity and availability issues on the decentralized controls during different physical system operating conditions are investigated. From these studies, simplified guidelines for DG control protection from hazardous operating conditions are presented for a Cigré LV benchmark feeder, from considerations of the cyber-physical system operating conditions.

7.2 Future work

To overcome the CPES distribution network security assessment and protection challenges, additional research activities are necessary. Such activities can extend the contribution of this thesis in improving the monitoring of distribution network conditions and the protection of DG control capabilities. The following include suggested directions of further research within the topic of this thesis.

7.2.1 Distribution network monitoring

The proposed voltage interval estimation method that utilizes measurements from a single node to estimate network conditions of the entire feeder should be evaluated with real smart meter measurements. As such, a demonstration of the proposed methodology could reveal critical LV feeders where either ICT or power system investments should be prioritized. Furthermore, the potential of activating flexible resources within different LV feeders could be studied with the use of the estimated intervals as the input to different demand response methods or DG coordination technologies.

For the bi-level estimation platform, multiple directions are suggested for further research activities: 1) The platform could be implemented on a industrial grade single board computer and demonstrated in connection to a real LV feeder. 2) Extending the considered information for estimating the LV feeder conditions through the inclusion of CPES information from internet of things sensors, e.g. weather and traffic information. 3) The possibility of performing a dynamic network monitoring with the limited ICT infrastructure could be investigated. Such investigation could be supported by minimal investment in advanced metering devices, e.g. PMUs or waveform measurement unit, and could reveal additional hazards or possibilities in terms of activating flexible resources. 4) From an application perspective, the added value from gaining network conditions on a sub-15 minute level, when frequent DER events are registered, should be evaluated from both a operational and a planning perspective.

For both proposed LV network monitoring approaches, the level of information that can be transferred to higher voltage levels should be evaluated, e.g. with the estimated conditions at the secondary side of all secondary substations of a particular 10 kV distribution network, the power flow within this network could be estimated. To improve the accuracy of such a bottom-up approach to distribution network monitoring, the information available from metering devices connected to higher voltage levels should be included.

7.2.2 Distribution network protection of DG control

The demonstrated functional modeling extraction of key quantities and relations for wind turbine generators could be applied to other types of DG units, such as PV plants, or even to DERs, such as heat pumps. As such it is suggested to analyze the impact of the bottom-up approach to protection against information integrity issues on a greater scale, where a distribution network with diverse

implementation of utility and residential scale DG and DER units that are all equipped with individual distributed cyber error detection systems. Such analysis should consider multi-point attack vectors and be evaluated in terms of the impact from the cyber-physical environment conditions, and from the reliability of such protected DG controls in different control situations, e.g. optimal power flow and reaction to higher level remedial action support.

For the investigation of DG control strategies in cyber-physical conditions, the coordination between different local and decentralized controls objectives could be studied with the aim of improving the decision making guidelines. With a more elaborate study, a generic formulation of guidelines should be established for diverse LV feeders based on their characteristics.

With means of monitoring LV networks, and protecting DG controls, the application of contingency assessment in distribution networks, considering potential disturbances in both cyber and physical systems, and cascading failures could be an area of further research. In this context, the identification of available remedial control actions for protection of network operation would be an interesting extension and support the application of security assessment and protection in the distribution network domain.

Bibliography

[1] C. Lichtenberg. Supervisory systems for electric power apparatus. *Journal of the A.I.E.E.*, 45(2):116–123, Feb 1926.

[2] R. N. Conwell, G. M. Keenan, C. F. Craig, and E. C. Briggs. Communication plays its part in electric power system operation. *Electrical Engineering*, 50(10):802–802, Oct 1931.

[3] C. G. A. Koreman, S. Lemmer, M. Kezunovic, and A. Newbould. Configuration and integration of substation secondary equipment. In *CIGRé session*, Paris, France, Aug 1996.

[4] M. Kezunovic. Data integration and information exchange for enhanced control and protection of power system. In *36th Annual Hawaii International Conference on system Sciences*, Big Island, HI, USA, Jan 2003.

[5] G. N. Ericsson. Classification of power systems communications needs and requirements: Experiences from case studies at Swedish national grid. *IEEE Transactions on Power Delivery*, 17(2):345–347, Apr 2002.

[6] T. Papallo. Networks in a network, communications in electrical distribution. In *Industry Applications Society 60th Annual Petroleum and Chemical Industry Conference*, Chicago, IL, USA, Sept 2013.

[7] Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. *U.S.- Canada Power System Outage Task Force*, Apr 2004.

[8] Report on support investigations into recent blackouts in London and West Midlands. *Office of Gas and Electricity Markets (OFGEM)*, Feb 2004.

[9] Final report of the investigation committee on the 28 september 2003 blackout in Italy. *Union for the Coordination of the Transmission of Electricity (UCTE)*, Apr 2004.

[10] Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, Mar 2016.

[11] D. Kirschen and F. Bouffard. Keep the lights on and the information flowing. *IEEE Power and Energy Magazine*, 7(1):50–60, January 2009.

[12] J. Liu, Y. Xiao, S. Li, W. Liang, and C.L.P. Chen. Cyber security and privacy issues in smart grids. *IEEE Communications Survey and Tutorials*, 14(4):981–997, Jan 2012.

[13] S. Sridhar, A. Hahn, and M. Govindarasu. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, Jan 2012.

[14] A.A. Cárdenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *The 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, June 2008.

[15] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, Jan 2012.

[16] C. Ten, C. Liu, and G. Manimaran. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4):1836–1846, Nov 2008.

[17] G.N. Ericsson. Cyber security and power system communication - Essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3):1501–1507, July 2010.

[18] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 14(4):998–1010, 2012.

[19] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, 4(2):847–855, June 2013.

[20] Y. Huang, A.A. Cárdenas, S. Amin, Z. Lin, H. Tsai, and S. Sastry. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure protection*, 2(3):73–83, Oct 2009.

[21] S. Sridhar and M. Govindarasu. Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, 5(2):580–591, Mar 2014.

[22] J. Yan, C. Liu, and M. Govindarasu. Cyber intrusion of wind farm SCADA system and its impact analysis. In *IEEE Power Systems Conference and Exposition*, Phoenix, AZ, USA, Mar 2011.

[23] Y. Zhang, Y. Xiang, and L. Wang. Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. *IEEE Transactions on Smart Grid*, 8(5):2343–2357, Sept 2017.

[24] Y. Isozaki, S. Yoshizawa, Y Fujimoto, H. Ishil, I. Ono, T. Onoda, and Y. Hayashi. Detection of cyber attacks against voltage control in distribution power grids with PVs. *IEEE Transactions on Smart Grid*, 7(4):1824–1835, July 2016.

[25] A.M. Kosek. Contextual anomaly detection for cyber-physical security in smart grids based on artificial neural network model. In *Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids*, Vienna, Austria, Apr 2016.

[26] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Conference on Communication, Control, and Computing*, Monticecllo, IL, USA, Oct 2009.

[27] Y. Liu, P. Ning, and M.K. Reiter. False data injection attacks against state estimation in electric power grids. In *ACM Conference on Computer and Communications Security*, Chicago, IL, USA, Nov 2009.

[28] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cyber security analysis of state estimators in electric power systems. In *IEEE Conference on Decision and Control*, Atlanta, GA, USA, Dec 2010.

[29] S. Sridhar and G. Manimaran. Data integrity attacks and their impacts on SCADA control systems. In *IEEE PES General Meeting*, Providence, RI, USA, July 2010.

[30] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, Oct 2010.

[31] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li. A denial of service attack in advanced metering infrastructure network. In *IEEE International Conference on Communications*, Sydney, NSW, Australia, June 2014.

[32] R.R. Mitchell III. *Design and analysis of intrusion detection protocols in cyber physical systems*. PhD thesis, Virginia Polytechnic Institute and State University, 2013.

[33] European Commission. 2030 energy strategy. [Online]. Available: https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/2030-energy-strategy. Accessed: 1 Feb 2019.

[34] European Commission. Clean energy for all Europeans. [Online]. Available: https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans. Accessed: 1 Feb 2019.

[35] Key world energy statistics. *International Energy Agency (IEA)*, Sept 2018.

[36] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Magazine*, 8(1):18–28, Dec 2009.

[37] N. Cohn, S. B. Biddle, R. G. Lex, E. H. Preston, C. W. Ross, and D. R. Whitten. On-line computer applications in the electric power industry. *Proceedings of the IEEE*, 58(1):78–87, Jan 1970.

[38] T. J. Kendrew and J. A. Marks. Automated distribution comes of age. *IEEE Computer Applications in Power*, 2(1):7–10, Jan 1989.

[39] R. E. Wilson. Satellite synchronized measurements confirm power equation. *IEEE Potentials*, 13(2):26–28, April 1994.

[40] IEC/IEEE 60255-118-1. Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements. International standard, IEC, Oct 2014.

[41] Companion Specification for Energy Metering. COSEM interface classes and OBIS object identification system. Excerpt from blue book edition 12.2, DLMS User Association, Jan 2017.

[42] EN 50470-3. Electricity metering equipment (a.c.) part 3: Particular requirements - Static meters for active energy (class indexes a, b and c). European standard, European Committee for Electrotechnical Standardization (CENELEC), Oct 2006.

[43] A. G. Phadke, H. Volskis, R. Menezes de Moraes, T. Bi, R. N. Nayak, Y. K. Sehgal, S. Sen, W. Sattinger, E. Martinez, O. Samuelsson, D. Novosel, V. Madani, and Y. A. Kulikov. The wide world of wide-area measurement. *IEEE Power and Energy Magazine*, 6(5):52–65, Sept 2008.

[44] A. G. Phadke and T. Bi. Phasor measurement units, WAMS, and their applications in protection and control of power systems. *Journal of Modern Power Systems and Clean Energy*, 6(4):619–629, Jul 2018.

[45] Office of Electricity Delivery and Energy Reliability. Factors affecting PMU installation costs. Tech. rep., U.S. Department of Energy, Oct 2014.

[46] N. Strother and B. Lockhart. Smart electric meters, advanced metering infrastructure, and meter communications: Global market analysis and forecasts. *Navigant Research*, 2014.

[47] S. Repo, F. Ponci, D.D. Giustina, A. Alvarez, C.C. Garica, Z. Al-Jassim, H. Amaris, and A. Kulmana. The IDE4L project: Defining, designing, and demonstrating the ideal grid for all. *IEEE Power and Energy Magazine*, 15(3):41–51, Apr 2017.

[48] Commission for Energy Regulation (CER). Electricity smart metering technology trials findings report. Information paper, The Commission for Energy Regulation, May 2011.

[49] Regulation (EU) 2016/679. Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). EU legislation, European Parliament and of the Council, Apr 2016.

[50] M. Kuzlu, M. Pipattanasomporn, and S. Rahman. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, 67:74–88, July 2014.

[51] A. Usman and S.H. Shami. Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*, 19:191–199, Mar 2013.

[52] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - The new and improved power grid: A survey. *IEEE Communications Surveys and Tutorials*, 14(4):944–979, 2012.

[53] F.F. Wu, K. Moslehi, and A. Bose. Power system control centers: Past, present, and future. *Proceedings of the IEEE*, 93(11):1890–1908, Nov 2005.

[54] R.C. Green, L. Wang, and M. Alam. Applications and trends of high performance computing for electric power systems: Focusing on smart grid. *IEEE Transactions on Smart Grid*, 4(2):922–931, June 2013.

[55] Z. Huang and J. Nieplocha. Transforming power grid operation via high performance computing. In *IEEE Power and Energy Society General Meeting*, Pittsburgh, PA, USA, July 2008.

[56] D.S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic. Smart power grid and cloud computing. *Renewable and Sustainable Energy Reviews*, 24:566–577, May 2013.

[57] P.G. Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felberl, and E. Riviere. Edge-centric computing: Vision and challenges. *SIGCOMM Comput. Commun. Rev.*, 45(5):37–42, Sept 2015.

[58] X. Yu and Y. Xue. Smart grids: A cyber-physical systems perspective. *Proceedings of the IEEE*, 104(5):1058–1070, May 2016.

[59] A. Kulmala, M. Alonso, S. Repo, H. Amaris, A. Moreno, J. Mehmedalic, and Z. Al-Jassim. Hierarchical and distributed control concept for distribution network congestion management. *IET Generation, Transmission and distribution*, 11(3):665–675, Aug 2016.

[60] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal. Definition and classification of power system stability. *IEEE Transaction on Power Systems*, 19(2):1387–1401, May 2004.

[61] K. Morison, L. Wang, and P. Kundur. Power system security assessment. *IEEE Power and Energy Magazine*, 2(5):30–39, Oct 2004.

[62] A. Monticelli. Electric power system state estimation. *Proceedings of the IEEE*, 88(2):262–282, Feb 2000.

[63] A. Coelho, A.B. Rodrigues, and M.G. Da Silva. Distribution network reconfiguration with reliability constraints. In *International Conference on Power System Technology*, Singapore, Singapore, Nov 2004.

[64] M. Kezunovic. Smart fault location for smart grids. *IEEE Transactions on Smart Grid*, 2(1):11–22, Mar 201.

[65] A. Zidan, M. Khairalla, A.M. Abdrabou, T. Khalifa, K. Shaban, A. Abdrabou, R. El Shatshat, and A.M. Gaouda. Fault detection, isolation, and service restoration in distribution systems: State-of-the-art and future trends. *IEEE Transactions on Smart Grid*, 8(5):2170–2185, Sept 2017.

[66] A. Dedé, D. Della Giustina, S. Rinaldi, P. Ferrari, A. Flammini, and A. Vezzoli. Smart meters as part of a sensor network for monitoring the low voltage grid. In *IEEE Sensors Applications Symposium*, Zadar, Croatia, Apr 2015.

[67] L. Kumpulainen, S. Pettissalo, P. Trygg, K. Malmberg, M. Loukkalahti, and M. Hyvärinen. Improved monitoring and control of distribution network by smart MV/LV substations. In *IEEE Power and Energy Society International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, UK, Dec 2012.

[68] Ausgrid. Electricity network performance report 2015/16. Technical report, Ausgrid, Nov 2016.

[69] M.E. Baran, J. Zhu, and A.W. Kelley. Meter placement for real-time monitoring of distribution feeders. *IEEE Transactions on Power Systems*, 11(1):332–337, Feb 1996.

[70] R. Singh, B.C. Pal, and R.B. Vinter. Measurement placement in distribution system state estimation. *IEEE Transactions on Power Systems*, 24(2):668–675, May 2009.

[71] J. Liu, J. Tang, F. Ponci, A. Monti, C. Muscas, and P.A. Peforaro. Trade-offs in PMU deployment for state estimation in active distribution grids. *IEEE Transactions on Smart Grid*, 3(2):915–924, June 2012.

[72] C.N. Lu, J.H. Teng, and W.H.E. Liu. Distribution system state estimation. *IEEE Transactions on Power Systems*, 10(1):229–240, Feb 1995.

[73] M.E. Baran and A.W. Kelley. A branch-current-based state estimation method for distribution systems. *IEEE Transactions on Power Systems*, 10(1):483–491, Feb 1995.

[74] M. Pau, P.A. Pegoraro, and S. Sulis. Efficient branch-current-based distribution system state estimation including synchronized measurements. *IEEE Transactions on Instrumentation and Measurement*, 62(9):2419–2429, Sept 2013.

[75] M. Pau, P.A. Pegoraro, and S. Sulis. Performance of three-phase WLS distribution system state estimation approaches. In *IEEE International Workshop on Applied Measurements for Power Systems*, Aachen, Germany, Sept 2015.

[76] S. Lu, S. Repo, D. Della Giustina, F.A. Figuerola, and M. Pikkarainen. Real-time low voltage network monitoring - ICT architecture and field test experience. *IEEE Transactions on Smart Grid*, 6(4):2002–2012, July 2015.

[77] A. Primadianto and C.N. Lu. A review on distribution system state estimation. *IEEE Transactions on Power Systems*, 32(5):3875–3883, Sept 2017.

[78] A. Barbato, A. Dedé, D. Della Giustina, G. Massa, A. Angioni, G. Lipari, F. Ponci, and S. Repo. Lessons learnt from real-time monitoring of the low voltage distribution network. *Sustainable Energy, Grids and Networks*, 15:76–85, Sept 2018.

[79] R. Poudineh, D. Peng, and S.R. Mirnezami. Electricity networks: Technology, future role and economic incentives for innovation. Paper, Oxford Institute of Energy Studies, Dec 2017.

[80] G. Strbac. Impact of dispersed generation on distribution systems: A european perspective. In *IEEE PES Winter Meeting*, New York, NY, USA, Jan 2002.

[81] A. Abdel-Majeed and M. Braun. Low voltage system state estimation using smart meters. In *International Universities Power Engineering Conference*, London, UK, Sept 2012.

[82] D. Waeresch, R. Brandalik, W.H. Wellssow, J. Jordan, R. Bischler, and N. Schneider. Linear state estimation in low voltage grids based on smart meter data. In *IEEE PowerTech*, Eindhoven, Netherlands, June 2015.

[83] S. Repo, D. Della Giustina, G. Ravera, L. Cremaschini, S. Zanini, J.M. Selga, and P. Järventausta. Use case analysis of real-time low voltage network management. In *IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, UK, Dec 2011.

[84] A. Mutanen, A. Koto, A. Kulmala, and P. Järventausta. Development and testing of a branch current based distribution system state estimator. In *International Universities Power Engineering Conference*, Soest, Germany, Sept 2011.

[85] M. Pikkarainen, A. Löf, S. Lu, T. Pöhö, S. Repo, and D. Della Giustina. Power quality monitoring use case in real low voltage network. In *IEEE PES Innovative Smart Grid Technologies*, Lyngby, Denmark, Oct 2013.

[86] A. Mutanen, S. Repo, P. Järventusta, A. Löf, and D. Della Giustina. Testing low voltage network state estimation in RTDS environment. In *IEEE PES Innovative Smart Grid Technologies*, Lyngby, Denmark, Oct 2013.

[87] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons, F. Ponci, and A. Monti. Low voltage system state estimation based on smart metering interface. In *IEEE International Workshop on Applied Measurements for Power Systems*, Aachen, Germany, Sept 2016.

[88] M.V. Sebastian, M. Caujolle, B.G. Maraver, J. Pereira, J. Sumaili, P. Barbeiro, J. Silva, and R. Bessa. LV state estimation and TSO-DSO cooperation tools: Results from the french field tests in the evolvDSO project. *CIRED Open Access Proceedings Journal*, 2017(1):1883–1887, Oct 2017.

[89] A. Bernieri, G. Betta, C. Liguori, and A. Losi. Neural networks and pseudo-measurements for real-time monitoring of distribution systems. *IEEE Transactions on Instrumentation and Measurement*, 45(2):645–650, Apr 1996.

[90] G. Valverde, A.T. Saric, and V. Terzija. Stochastic monitoring of distribution networks including correlated input variables. *IEEE Transactions on Power Systems*, 28(1):246–255, Feb 2013.

[91] D. Atanackovic and V. Dabic. Deployment of real-time state estimator and load flow in BC hydro DMS - Challenges and opportunities. In *IEEE Power and Energy Society General Meeting*, Vancouver, BC, Canada, July 2013.

[92] A. Alimardani, F. Therrien, D. Atanackovic, J. Jatskevich, and E. Vaahedi. Distribution system state estimation based on nonsynchronized smart meters. *IEEE Transactions on Smart Grid*, 6(6):2919–2928, Nov 2015.

[93] B.P. Hayes and M. Prodanovic. State forecasting and operational planning for distribution network energy management systems. *IEEE Transactions on Smart Grid*, 7(2):1002–1011, Mar 2016.

[94] C. Rakpenthai, S. Uatrongjit, and S. Premrudeepreechacharn. State estimation of power system considering network parameter uncertainty based on parametric interval linear systems. *IEEE Transactions on Power Systems*, 27(1):305–313, Feb 2012.

[95] P.A. Pegoraro, A. Meloni, L. Atzori, P. Castello, and S. Sulis. Adaptive PMU-based distribution system state estimation exploiting the cloud-based IoT paradigm. In *IEEE International Instrumentation and Measurement Technology Conference*, Taipei, Taiwan, May 2016.

[96] G. Yang, F. Marra, M. Juamperez, S.B. Kjær, S. Hashemi, J. Østergaard, H.H. Ipsen, and K.H.N. Frederiksen. Voltage rise mitigation for solar PV integration in LV grids. *Journal of Modern Power Systems and Clean Energy*, 3(3):411–421, Sept 2015.

[97] IEC 61400. Wind turbines - part 21: Measurement and assessment of power quality characteristics of grid connected wind turbines. International standard, IEC, 2008.

[98] ENTSO-E. Network code on requirements for grid connection applicable to all generators. European standard, ENTSO-E, Mar 2013.

[99] A. Singhal, V. Ajjarapu, J.C. Fuller, and J. Hansen. Real-time local volt/VAR control under external disturbances with high PV penetration. *IEEE Transactions on Smart Grid*, Early Access.

[100] B. Bayer, P. Matschoss, H. Thomas, and A. Marian. The german experience with integrating photovoltaic systems into the low-voltage grids. *Renewable Energy*, 119:129–141, Apr 2018.

[101] M. Juamperez, G. Yang, and S.B. Kjær. Voltage regulation in LV grids by coordinated volt-var control strategies. *Journal of Modern Power System and Clean Energy*, 2(4):319–328, Dec 2014.

[102] S. Karagiannopoulos, P. Aristidou, and G. Hug. Hybrid approach for planning and operating active distribution grids. *IET Generation, Transmission and Distribution*, 11(3):685–695, Feb 2017.

[103] S. Weckx, C. Gonzalez, and J. Driesen. Combined central and local active and reactive power control of PV inverters. *IEEE Transactions on Sustainable Energy*, 5(3):776–784, July 2014.

[104] M. Farivar, R. Neal, C. Clarke, and S. Low. Optimal inverter VAR control in distribution systems with high PV penetration. In *IEEE PES General Meeting*, San Diego, CA, USA, July 2012.

[105] G. Valverde and T. Van Cutsem. Model predictive control of voltages in active distribution networks. *IEEE Transactions on Smart Grid*, 4(4):2152–2161, Dec 2013.

[106] E. Dall'Anese, S.V. Dhople, and G.B. Giannakis. Optimal dispatch of photovoltaic inverters in residential distribution systems. *IEEE Transactions on Sustainable Energy*, 5(2):487–497, Apr 2014.

[107] G. Mokhtari, G. Nourbakhsh, and A. Ghosh. Smart coordination of energy storage units (ESUs) for voltage and loading management in distribution networks. *IEEE Transactions on Power Systems*, 28(4):4812–4820, Nov 2013.

[108] C. Zhang, Y. Xu, Z. Dong, and J. Ravishankar. Three-stage robust inverter-based voltage/var control for distribution networks with high-level PV. *IEEE Transactions on Smart Grid*, 10(1):782–793, Jan 2019.

[109] North American Electric Reliability Corporation. Critical infrastructure protection standards. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Accessed: 21 Feb 2019.

[110] M. Rana, L. Li, and S.W. Su. Distributed dynamic state estimation considering renewable generation and packet losses. In *International Conference on Control, Automation, Robotics and Vision*, Phuket, Thailand, Nov 2016.

[111] S.A.S. Shahriari, M. Raoofat, M. Dehghani, M. Mohammadi, and M. Saad. Dynamic state estimation of permanent magnet synchronous generator-based wind turbine. *IET Renewable Power Generation*, 10(9):1278–1286, Oct 2016.

[112] S. Yu, K. Emami, T. Fernando, H.H.C. Lu, and K.P. Wong. State estimation of doubly fed induction generator wind turbine in complex power systems. *IEEE Transactions on Power Systems*, 31(6):4935–4944, Nov 2016.

[113] B.N. Miranda-Blanco, E. Díaz-Dorado, C. Carrukki, and J. Cidrás. State estimation for wind farms including the wind turbine generator models. *Renewable Energy*, 71:453–465, 2014.

[114] S.J. Julier and J.K. Uhlmann. Unscented filtering and nonlinear estimation. *Proceedings of the IEEE*, 92(3):401–422, Mar 2004.

[115] D.I. Wilson, M. Agarwal, and D.W.T. Rippin. Experiences implementing the extended Kalman filter on industrial batch reactor. *Computers and Chemical Engineering*, 22(11):1653–1672, Oct 1998.

[116] R. Saint-Germain. Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, 39(4):60–66, July 2005.

[117] F.L. Quilumba, W. Lee, H. Huang, D.Y. Wang, and R.L. Szabados. Using smart meter data to improve the accuracy of intraday load forecasting considering customer behavior similarities. *IEEE Transactions on Smart Grid*, 6(2):911–918, Mar 2015.

[118] M. Ghofrani, M. Hassanzadeh, M. Etezadi-Amoli, and M.S. Fadali. Smart meter based short-term load forecasting for residential customers. In *North American Power Symposium*, Boston, MA, USA, Aug 2011.

[119] B. Hayes, J. Gruber, and M. Prodanovic. Short-term load forecasting at the local level using smart meter data. In *IEEE PowerTech*, Eindhoven, Netherlands, June 2015.

[120] M.E.H. Dyson, S.D. Borgeson, M.D. Tabone, and D.S. Callaway. Using smart meter data to estimate demand response potential with application to solar energy integration. *Energy Policy*, 73:607–619, Oct 2014.

[121] M. Weiss, A. Helfenstein, F. Mattern, and T. Staake. Leveraging smart meter data to recognize home appliances. In *IEEE International Conference on Pervasive Computing and Communications*, Lugano, Switzerland, Mar 2012.

[122] C. Beckel, L. Sadamori, T. Staake, and S. Santini. Revealing household characteristics from smart meter data. *Energy*, 78:397–410, Dec 2014.

[123] J. Kao and R. Marculescu. Eavesdropping minimization via transmission power control in ad-hoc wireless networks. In *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, Reston, VA, USA, Sept 2006.

[124] A.D. Wood and J.A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, Oct 2002.

[125] J. Liu, Y. Xiao, and J. Gao. Achieving accountability in smart grids. *IEEE Systems Journal*, 8(2):493–508, June 2014.

[126] M.J. Daigle, A. Bregon, and I. Roychoudhury. Distributed prognostics based on structural model decomposition. *IEEE Transactions on Reliability*, 63(2):495–510, June 2014.

[127] M.E. Baran and A.W. Kelley. State estimation for real-time monitoring of distribution systems. *IEEE Transactions on Power Systems*, 9(3):1601–1609, Aug 1994.

[128] C.W. Hansen and A.S. Debs. Power system state estimation using three-phase models. *IEEE Transactions on Power Systems*, 10(2):818–824, May 1995.

[129] T.H. Chen, M.S. Chen, K.J. Hwang, P. Kotas, and E.A. Chebli. Distribution system power flow analysis - a rigid approach. *IEEE Transactions on Power Delivery*, 6(3):1146–1152, July 1991.

[130] M. Chaouch. Clustering-based improvement of nonparametric functional time series forecasting: Application to intra-day household-level load curves. *IEEE Transactions on Smart Grid*, 5(1):411–419, Jan 2014.

[131] W. Kong, Z.Y. Dong, D.J. Hill, F. Luo, and Y. Xu. Short-term residential load forecasting based on residential behaviour learning. *IEEE Transactions on Power Systems*, 33(1):1087–1088, Jan 2018.

[132] P. Baran. On distributed communications: I. Introduction to distributed communications networks. Memorandum rm-3420-pr, United States Air Force Project Rand, Aug 1964.

[133] H.J. Koglin, T. Neisius, G. Beißler, and K.D. Schmitt. Bad data detection and identification. *International Journal of Electric Power and Energy Systems*, 12:94–103, Apr 1990.

[134] L. Mili, T. Van Cutsem, and M. Ribbens-Pavella. Bad data identification methods in power system state estimation - A comparative study. *IEEE Transactions on Power Apparatus and Systems*, PAS-104(11):3037–3049, Nov 1985.

[135] F.C. Schweppe, J. Wildes, and D.B. Rom. Power system static-state estimation, parts I, II, III. *IEEE Transactions on Power Apparatus and Systems*, PAS-89(1):120–135, Jan 1970.

[136] E. Handschin, F.C. Schweppe, J. Kohlas, and A. Fiechter. Bad data analysis for power system state estimation. *IEEE Transactions on Power Apparatus and Systems*, 94(2):329–337, Mar 1975.

[137] A. Garcia, A. Monticelli, and P. Abreu. Fast decoupled state estimation and bad data processing. *IEEE Transactions on Power Apparatus and Systems*, PAS-98(5):1645–1652, Sept 1979.

[138] Task Force C6.04. Benchmark systems for network integration of renewable and distributed energy resources. Technical report, Cigré, 2013.

[139] B. Hayes and M. Prodanovic. State estimation techniques for electric power distribution systems. In *European Modelling Symposium*, Pisa, Italy, Oct 2014.

[140] M.M. Albu, M. Sanduleac, and C. Stanescu. Syncretic use of smart meters for power quality monitoring in emerging networks. *IEEE Transactions on Smart Grid*, 8(1):485–492, Jan 2017.

[141] S. Bhela, V. Kekatos, and S. Veeramachaneni. Enhancing observability in distribution grids using smart meter data. *IEEE Transactions on Smart Grid*, 9(6):5953–5961, Nov 2018.

[142] W. Luan, D. Sharp, and S. LaRoy. Data traffic analysis of utility smart metering network. In *IEEE PES General Meeting*, Vancouver, BC, Canada, July 2013.

[143] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu. A survey on state estimation techniques and challenges in smart distribution systems. *IEEE Transactions on Smart Grid*, 10(2):2312–2322, Mar 2019.

[144] A. Albert and R. Rajagopal. Smart meter driven segmentation: What your consumption says about you. *IEEE Transactions on Power Systems*, 28(4):4019–4030, Nov 2013.

[145] B. Das. Consideration of input parameter uncertainties in load flow solution of three-phase unbalanced radial distribution system. *IEEE Transactions on Power Systems*, 21(3):1088–1095, Aug 2006.

[146] European Standard. EN 50160: Voltage characteristics of electricity supplied by public distribution systems. International standard, CENELEC, Sept 2010.

[147] IEC. IEC 61000-4-30:2015 Electromagnetic compatibility (EMC) - Part 4-30: Testing and measurement techniques - Power quality measurement methods. International standard, IEC, February 2015.

[148] S. Erlinghagen, B. Lichtensteiger, and J. Markard. Smart meter communication standards in Europe - A comparison. *Renewable and Sustainable Energy Reviews*, 43:1249–1262, Mar 2015.

[149] C.S. Cheng and D. Shirmohammadi. A three-phase power flow method for real-time distribution system analysis. *IEEE Transactions on Power Systems*, 10(2):671–679, May 1995.

[150] S. Feuerhahn, M. Zillgith, C. Wittwer, and C. Wietfeld. Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. In *IEEE International Conference on Smart Grid Communications*, Brussels, Belgium, Oct 2011.

[151] T.S. Basso and R. DeBlasio. IEEE 1547 series of standards: Interconnection, issues. *IEEE Transaction of Power Electronics*, 19(5):1159–1162, 2004.

[152] F.M. Cleveland. IEC 61850-7-420 communications standard for distributed energy resources (DER). In *IEEE PES General Meeting*, Pittsburgh, PA, July 2008.

[153] N.C. Nair and L. Zhang. Smartgrid: Future networks for New Zealand power systems incorporating distributed generation. *Energy Policy*, 37:3418–3427, 2009.

[154] SunSpec Alliance. Spec alliance interoperability specification. Sunspec technology overview, SunSpec Alliance, Mar 2015.

[155] M.B.D.C Filho and J.C.S. Souza. Forecasting-aided state estimation - Part I: Panorama. *IEEE Transaction of power systems*, 24(4):1667–1677, 2009.

[156] M. Lind and X. Zhang. Functional modelling for fault diagnosis and its application for NPP. *Nuclear Engineering and Technology*, 46(6):753–772, 2014.

[157] R. Aggarwal and Y. Song. Artificial neural networks in power systems. III. Examples of applications in power systems. *Power Engineering Journal*, 12(6):279–287, Dec 1998.

[158] O.Y. Al-Jarrah, P.D. Yoo, S. Muhaidat, G.K. Karagiannidis, and K. Taha. Efficient machine learning for big data: A review. *Big Data Research*, 2(3):87–93, Sept 2015.

[159] R. Aggarwal and Y. Song. Artificial neural networks in power systems. I. General introduction to neural computing. *Power Engineering Journal*, 11(3):129–134, June 1997.

[160] B. Wang and K. Sun. Power system differential-algebraic equations. *CoRR*, abs/1512.05185, 2015.

[161] M. Lind, H. Yoshikawa, S.B. Jørgensen, M. Yang, K. Tamayama, and K. Okusa. Multilevel flow modeling of monju nuclear power plant. *International Journal of Nuclear Safety and Simulation*, 2(3):274–284, 2011.

[162] J.R. Rajan, R.B. Stone, and K.L. Wood. Functional modeling of control systems. In *International Conference on Engineering Design*, Stockholm, Sweden, Aug 2003.

[163] K. Heussen, A. Saleem, and M. Lind. Control architecture of power systems: Modeling of purpose and function. In *IEEE PES General Meeting*, Calgary, Canada, July 2009.

[164] J. Rumbaugh, M. Blaha, and W. Premerlani. *Object-oriented modeling and design*. Prentice Hall, 1st edition edition, Mar 1991.

[165] M. Lind. An introduction to multilevel flow modeling. *International Journal of Nuclear Safety and Simulation*, 2(1):22–32, 2011.

[166] K. Heussen and M. Lind. Decomposing objectives and functions in power system operation and control. In *IEEE Conference on Sustainable Alternative Energy*, Valencia, Spain, Sept 2009.

[167] L. Holten, A. Gjelsvik, S. Aam, F.F. Wu, and W.E. Liu. Comparison of different methods for state estimation. *IEEE Transactions on Power Systems*, 3(4):1798–1806, Nov 1988.

[168] K. Clark, N.W. Miller, and J.J. Sanchez-Gasca. Modeling of GE wind turbine-generators for grid studies. Technical report, General Electric Energy, Apr 2010.

[169] X.R. Li and Z. Zhao. Measures of performance for evaluation of estimators and filters. In *Conference on Signal and Data Processing*, San Diego, CA, USA, July 2001.

[170] J. Tautz-Weinert and S.J. Watson. Using SCADA data for wind turbine condition monitoring - A review. *IET Renewable Power Generation*, 11(4):382–394, Mar 2016.

[171] M. Altin, R. Teodorescu, B. Bak-Jensen, P. Rodriguez, F. Iov, and P.C. Kór. Wind power plant control - An overview. In *International Workshop on Large-Scale Integration of Wind Power into Power Systems*, Aarhus, Denmark, Oct 2010.

[172] M. Tsili and S. Papathanassiou. A review of grid code technical requirements for wind farms. *IET Renewable Power Generation*, 3(3):308–332, Sept 2009.

[173] D. Schneider, K.K Küster, M. Seifert, and M. Speckmann. Available active power estimation for the provision of control reserve by wind turbines. In *European Wind Energy Conference and Exhibition*, Red Hook, NY, USA, Feb 2013.

[174] Nexans. 6-36kv medium voltage underground power cables. [Online]. Available: https://www.nexans.co.uk/UK/files/Underground%20Power%20Cables%20Catalogue%2003-2010.pdf. Accessed: 31 Mar 2019.

[175] Nexans. 60-500kv high voltage underground power cables. [Online]. Available: https://www.nexans.com/Corporate/2013/60-500_kV_High_Voltage_full_BD2.pdf. Accessed: 31 Mar 2019.

[176] P.N. Vovos, A.E. Kiprakis, A.R. Wallace, and G.P. Harrison. Centralized and distributed voltage control: Impact on distributed generation penetration. *IEEE Transactions on Power Systems*, 22(1):476–483, Feb 2007.

[177] K. Turitsyn, P. Sulc, S. Backhaus, and M. Chertkov. Options for control of reactive power by distributed photovoltaic generators. *Proceedings of the IEEE*, 99(6):1063–1073, June 2011.

[178] M.H. Cintuglu, O.A. Mohammed, K. Akkaya, and A.S. Uluagac. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys and Tutorials*, 19(1):446–464, 2017.

[179] V. Venkataramanan, A. Srivastava, and A. Hahn. Real-time co-simulation testbed for microgrid cyber-physical analysis. In *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, Vienna, Austria, Apr 2016.

[180] B. Chen, K.L. Butler-Perry, A. Goulart, and D. Kundur. Implementing a real-time cyber-physical system test bed in RTDS and OPNET. In *North American Power Symposium*, Pullman, WA, USA, Sept 2014.

[181] RTDS. Connecting RTDS/runtime with external application. RSCAD software documentation, RTDS, 2014.

[182] J.R. Moyne and D.M. Tilbury. The emergence of industrial control networks for monitoring control, diagnostics and safety data. *Proceedings of the IEEE*, 95(1):29–47, Jan 2007.

[183] Sophia Antipolis. Helioclim-3 archives solar irradiance data. [Online]. Available: http://www.soda-pro.com/web-services/radiation/helioclim-3-archives-for-free. Accessed: 27 Oct 2017.

[184] Elforbrugs panelerne. [danish] profiler, [english translation] profiles. [Online]. Available: http://www.elforbrugspanel.dk/Pages/Rapportering.aspx#ID18. Accessed: 26 Oct 2017.

[185] G. Kron. *Tensor analysis of networks*. Macdonald and Co., 1965.

A. Power flow equations in state estimation

The apparent power injection at node n, S_n can be expressed using (A.1).

$$S_n = V_n \sum_{k=1}^{N_n} I_{nk}^* \tag{A.1}$$

where I_{nk} is the current that flow between nodes n and k, V_n is the voltage at node n, and N_n is the number of nodes within the system under consideration. Applying Ohms law and using the network admittance matrix $\mathbf{Y}$ converts the apparent power balance in (A.1) to an expression of node voltages and network information as shown in (A.2).

$$S_n = V_n \sum_{k=1}^{N_n} Y_{nk}^* V_k^* \tag{A.2}$$

Separating the apparent power balance in injection of active P_n and reactive power Q_n at node n, and using a polar decomposition representation of the network admittance matrix through its magnitude $|Y_{nk}|$ and angle γ_{nk} for each branch between nodes n and k, result in the power balance equations in (A.3) and (A.4)

$$P_n = |V_n| \sum_{k=1}^{N_n} |Y_{nk}||V_k| cos\left(\delta_n - \delta_k - \gamma_{nk}\right) \tag{A.3}$$

$$Q_n = |V_n| \sum_{k=1}^{N_n} |Y_{nk}||V_k| sin\left(\delta_n - \delta_k - \gamma_{nk}\right) \tag{A.4}$$

A.1. Kron reduction for three phase power flow equations

With the impedance matrix of the four wire system Z_{abcN} where a, b and c are the three phases, and N represents the neutral wire, the voltages V_{abcN} and currents I_{abcN} can be expressed through (A.5).

$$\begin{bmatrix} V_a \\ V_b \\ V_c \\ V_N \end{bmatrix} = \begin{bmatrix} Z_{aa} & Z_{ab} & Z_{ac} & Z_{aN} \\ Z_{ba} & Z_{bb} & Z_{bc} & Z_{bN} \\ Z_{ca} & Z_{cb} & Z_{cc} & Z_{cN} \\ Z_{Na} & Z_{Nb} & Z_{Nc} & Z_{NN} \end{bmatrix} \begin{bmatrix} I_a \\ I_b \\ I_c \\ I_N \end{bmatrix} \tag{A.5}$$

where the impedance indexation represents the mutual and self impedances of the phases and the neutral. Using the Kron reduction method proposed in [185], the neutral potential is assumed

$V_N = 0$ and this assumption is used to find an expression for the neutral current I_N based on the mutual impedance between the neutral and the phases, and the self impedance of the neutral. This expression substitute the neutral current in (A.5) and the reduced impedance matrix Z_{abc} is found as (A.6).

$$Z_{abc} = \begin{bmatrix} Z_{aa} & Z_{ab} & Z_{ac} \\ Z_{ba} & Z_{bb} & Z_{bc} \\ Z_{ca} & Z_{cb} & Z_{cc} \end{bmatrix} - \begin{bmatrix} Z_{aN} \\ Z_{bN} \\ Z_{cN} \end{bmatrix} \begin{bmatrix} Z_{NN} \end{bmatrix}^{-1} \begin{bmatrix} Z_{Na} & Z_{Nb} & Z_{Nc} \end{bmatrix} \tag{A.6}$$

The Kron reduced admittance matrix of a line segment can then be found from the inverse of the impedance matrix Z_{abc} and used in the reformulated power injection balance equations in (A.3) and (A.4) for each node n and phase p, presented in (A.7) and (A.8).

$$P_n^p = |V_n^p| \sum_{k=1}^{N_n} \sum_{j=1}^{3} |Y_{nk}^{pj}||V_k^j| cos\left(\delta_n^p - \delta_k^j - \gamma_{nk}^{pj}\right) \tag{A.7}$$

$$Q_n^p = |V_n^p| \sum_{k=1}^{N_n} \sum_{j=1}^{3} |Y_{nk}^{pj}||V_k^j| sin\left(\delta_n^p - \delta_k^j - \gamma_{nk}^{pj}\right) \tag{A.8}$$

where the nested summation from $j = 1$ to $j = 3$ represents the consideration of each of the three power system phases one by one.

B. State estimation solution methods

B.1. Newton method

The Newton method utilize the gradient of the weighted square residual, $J(\mathbf{x})$ in (2.4) with respect to the state variables in $\mathbf{x}$, as shown in (B.9).

$$\nabla J(\mathbf{x}) = -2 \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_2}{\partial x_1} & \frac{\partial h_3}{\partial x_1} & \cdots \\ \frac{\partial h_1}{\partial x_2} & \frac{\partial h_2}{\partial x_2} & \frac{\partial h_3}{\partial x_2} & \cdots \\ \frac{\partial h_1}{\partial x_3} & \frac{\partial h_2}{\partial x_3} & \frac{\partial h_3}{\partial x_3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} \frac{1}{\sigma_1^2} & & & \\ & \frac{1}{\sigma_2^2} & & \\ & & \frac{1}{\sigma_3^2} & \\ & & & \ddots \end{bmatrix} \begin{bmatrix} z_1 - h_1(\mathbf{x}) \\ z_2 - h_2(\mathbf{x}) \\ z_3 - h_3(\mathbf{x}) \\ \vdots \end{bmatrix} \tag{B.9}$$

From left to right, the first matrix in (B.9) is seen identical to the transpose of the Jacobian matrix, H, of the state equations with respect to the state variables, the second matrix is the inverse of the diagonal weight matrix R containing the variance σ^2 of each measurement m in the diagonal. A simplification of notation hence reduces the expression in (B.9) to (B.10).

$$\nabla J(\mathbf{x}) = -2 \Big[H\Big]^T \Big[R\Big]^{-1} \begin{bmatrix} z_1 - h_1(\mathbf{x}) \\ z_2 - h_2(\mathbf{x}) \\ z_3 - h_3(\mathbf{x}) \\ \vdots \end{bmatrix} \tag{B.10}$$

With the Newton method, the gradient of the residual with respect to the state variables expressed in (B.10) is iterated towards 0 through applying a flat start in the first iteration and updating the state variables through finding the derivative of the gradient with respect to the state variables as expressed in (B.11).

$$\Delta \mathbf{x} = \left[\nabla^2 J(\mathbf{x})\right]^{-1} \left[-\nabla J(\mathbf{x})\right] \tag{B.11}$$

To simplify the calculations in (B.11), the Jacobian matrix H is kept constant which simplifies the state variable update expression to (B.12).

$$\Delta \mathbf{x} = \Big[[H]^T [R]^{-1} [H]\Big]^{-1} [H]^T [R]^{-1} \begin{bmatrix} z_1 - h_1(\mathbf{x}) \\ z_2 - h_2(\mathbf{x}) \\ z_3 - h_3(\mathbf{x}) \\ \vdots \end{bmatrix} \tag{B.12}$$

where $G = [H]^T [R]^{-1} [H]$ is called the gains matrix in the Newton method. With the update expression in (B.12), the state variables for iteration i are calculated through (B.13) for the necessary number of iterations until the stopping criteria in (B.14) is satisfied with g being the threshold of the stopping criteria.

$$\mathbf{x}^i = \mathbf{x}^{i-1} + \Delta\mathbf{x}^{i-1} \tag{B.13}$$

$$\max(|\Delta\mathbf{x}|) \leq g \tag{B.14}$$

B.2. Orthogonal factorization

Orthogonal factorization start with the inverse diagonal weight matrix R^{-1} and by expressing the Jacobian matrix as $\tilde{\mathbf{H}} = \mathbf{R}^{(-1/2)}\mathbf{H}$. Afterwards $\tilde{\mathbf{H}}$ is subject to the decomposition in (B.15).

$$\tilde{\mathbf{H}} = \mathbf{Q}^T\mathbf{U} = \begin{bmatrix}\mathbf{Q}_1^T & \mathbf{Q}_2^T\end{bmatrix}\begin{bmatrix}\mathbf{U}_1 \\ \mathbf{0}\end{bmatrix} \tag{B.15}$$

where $\mathbf{U}_1$ is a upper triangular matrix and $\mathbf{Q}$ is an orthogonal matrix.

Substituting the Jacobian matrix in (B.12) with the decomposed representation of the weighted Jacobian in (B.15) and moving the gains matrix to the left hand side reveals the expression for updating the state variables between iterations in the orthogonal factorized form in (B.16).

$$\mathbf{U}^T\mathbf{Q}\mathbf{Q}^T\mathbf{U}\Delta\mathbf{x} = \mathbf{U}^T\mathbf{Q}\begin{bmatrix}z_1 - h_1(\mathbf{x}) \\ z_2 - h_2(\mathbf{x}) \\ z_3 - h_3(\mathbf{x}) \\ \vdots\end{bmatrix} \tag{B.16}$$

with the upper triangular matrix $\mathbf{U}_1$ having a non-zero determinant for observable systems, it is non-singular and since the orthogonal matrix $\mathbf{Q}$ per definition satisfies $\mathbf{Q}^T\mathbf{Q} = \mathbf{Q}\mathbf{Q}^T = \mathbf{I}$, the expression in (B.16) can be further simplified to (B.17) where only the non-zero rows of $\mathbf{U}$ are considered.

$$\mathbf{U}_1\Delta\mathbf{x} = \mathbf{Q}_1\begin{bmatrix}z_1 - h_1(\mathbf{x}) \\ z_2 - h_2(\mathbf{x}) \\ z_3 - h_3(\mathbf{x}) \\ \vdots\end{bmatrix} \tag{B.17}$$

With the defined state estimation model in, the expression in (B.17) can be solved in an iterative fashion through backwards substitution due to the upper triangular characteristics of $\mathbf{U}_1$.

Department of Electrical Engineering
Center for Electric Power and Energy (CEE)
Technical University of Denmark
Elektrovej, Building 325
DK-2800 Kgs. Lyngby
Denmark

www.elektro.dtu.dk/cee
Tel: (+45) 45 25 35 00
Fax: (+45) 45 88 61 11
E-mail: cee@elektro.dtu.dk