Microgrid real-time active power diagnostic against cyber-physical attacks using recurrent neural networks

Bushra Canaan

Année 2023 N◦ d'ordre :

Université de Haute Alsace
Université de Freiburg (Albert-Ludwigs-Universität Freiburg)

Thèse
Présentée pour obtenir le grade de
DOCTEUR DE L'UNIVERSITÉ DE HAUTE-ALSACE
Discipline : Électronique, Électrotechnique et Automatique
par
Bushra CANAAN

Microgrid real-time active power diagnostic against cyber-physical attacks using recurrent neural networks

(Arrêté Ministériel du 30 mars 1992)
Soutenue publiquement le 06 /Juin/2023 devant le jury composé de :

Prof. Dr. rer. nat. Michael SCHMIDT (Rapporteur)

Prof. Dr. Mauro CARPITA (Rapporteur)

Prof. Dr. Marie-Cécile PERA (Présidente du jury)

Prof. Dr. Barbara KOCH (Directrice de Thèse)

Prof. Dr. Djaffar OULD ABDESLAM (Directeur de Thèse)

Dr. Bruno COLICCHIO (Encadrant)

Thèse préparée au sein de l'Institut de Recherche en Informatique,
Mathématiques, Automatique et Signal (IRIMAS)
à l'Université de Haute-Alsace sous la direction de

Prof. Dr. Djaffar OULD ABDESLAM
Dr. Bruno Colicchio

et au sein de la « Chair of Remote Sensing and Landscape Information Systems (FeLis) » de l'Université de Freiburg

Prof. Dr. Barbara Koch

Microgrid real-time active power diagnostic against cyber-physical attacks using Recurrent Neural Networks

Thesis submitted in partial fulfilment of the requirements
of the degree Doctor rer.nat of the
Faculty of Environment and Natural Resources,
Albert-Luwdwing-Universiät
Freiburg im Breisgau, Germany

By

Bushra CANAAN

Freiburg im Breisgau, Germany

Name of Dean: Prof. Dr. Heiner Schanz

Name of the 1st Supervisor: Prof. Dr. Barbara Koch

Name of the 2nd Supervisor: Prof. Dr. Djaffar Ould Abdeslam

Name of 1st Reviewer: Prof. Dr. Michael Schmidt

Name of 2nd Reviewer: Prof. Dr. Carpita Mauro

Date of the thesis defence: 06 June 2023

Contents

List of Figures

List of Tables

Abbreviations

Advanced metering infrastructure (AMI)

Advanced Persistent Threats (APT)

Artificial Intelligence (AI)

Artificial Neural networks (ANNs)

Battery output (B)

Communication and Information Technologies (ICT)

Controller-In-the-Loop Simulation (CIL)

Convolutional Neural Networks (CNNs)

Cooperative Vulnerability Factor (CVF)

Cyber-Physical System (CPS)

Demand Response (DR)

Denial of service attacks (DoS)

Devices Under Test (DUT)

Distributed Energy Resources (DERs)

Distributed Generation units (DGs)

Distributed-Denial-of-Service (DDoS)

Distribution System Operators (DSOs)

Electric Vehicle behaviour (EV)

Electricity Information Sharing and the Analysis Centre (E-ISAC)

Electronically Interfaced Distributed Generation (EI-DG)

Energy Management Strategy (EMS)

Energy Storage Systems (ESSs)

European Union Agency for Cybersecurity (ENISA)

False Data Injection (FDI)

Feeder Remote Terminal Units (FRTUs)

Field-Programmable Gate Array (FPGA)

Graphical User Interface (GUI)

Hardware-In-the-Loop (HIL)

Human–Machine Interface (HMI)

Incremental Input-to-State Stability (δISS)

Industrial Control Systems (ICS)

Industrial Control Systems Computer Emergency Response Team (ICS-CERT)

Input-Output (I/Os)

Input-to-State Stability (ISS)

Integrated Development Environment (IDE)

Intelligent Detecting System (IDS)

Intelligent Electronic Devices (IED)

International Energy Agency (IEA)

Load Frequency Control (LFC)

Load value (L)

Machine learning (ML)

Machine-to-Machine (M2M)

Maximum Power Point Tracker (MPPT)

Mean Squared Error (MSE)

MicroController Unit (MCU)

Microgrid (MG)

Model in the loop (MIL)

Multi-Class Support Vector Machines (MSVM)

National Institute of Standards and Technology (NIST)

Nonlinear Auto-Regressive eXogenous (NARX)

Operational Technology (OT)

Over-The-Air (OTA)

Parallel (P)

Phase-Locked-Loop (PLL)

Phasor Data Concentrators (PDCs)

Phasor Measurement Units (PMUs)

Point of Common Coupling (PCC)

Power Management System (PMS)

Processor in the Loop simulation (PIL)

Proportional–Integral (PI)

PV production output (PV)

Rapid Control Prototyping (RCP)

Recurrent Neural Networks (RNNs)

Recursive Systematic Convolutional (RSC)

Regression (R)

Replicating the Electromagnetic Transient (EMT)

Series-Parallel (SP)

Smart Meters (SM)

Software-in-the-Loop (SIL)

State-Space-Nodal (SSN)

Static State Estimator (SSE)

Supervisory Control And Data Acquisition (SCADA)

The Long Short Term memory (LSTM)

Transmission control Protocol (TCP)

Unknown Input Observer (UIO)

Voltage Source Converter (VSC)

Weighted Least Squared (WLS)

Acknowledgment

This work was supported by the European INTERREG-V program RES_TMO (Project No. 6.3). We thank the project lead of RES_TMO and Upper Rhine Cluster for Sustainability Research.

To Djaffar, and Bruno first and foremost, Thank you from the bottom of my heart!

I always used to think of myself as an unlucky person until life gave me the chance to work with these incredible and unbelievably kind people. You both are every PhD dream crew, and I extremely appreciate everything that you have done for me throughout these years.

You have proven, against all stereotypes, that a person doesn't need to be distant, cold or uncaring to be successful. Undoubtedly, I am very grateful for all the guidance and support that you have provided me with, but above all, thank you for being the source of relief instead of being another stress generator.

On the other hand, and apart from being my supervisor, I gained myself now a new family member and a dearest friend. I would always say if everyone had a Djaffar in their lives, the world would be a much nicer place. Thank you for giving me an example of how I want to exist in this life.

I would also like to express my sincere gratitude to Dr Barbara Koch for accepting to be a part of this work and simply for being the inspiring woman that she is for me and for a lot of young women that struggle to find their place in this life.

Additionally, many thanks to the reviewers and examiners of this work, your time and effort that you consecrated are much appreciated.

Finally, I should also like to thank my dad for providing me with every single quality that made me the person I am today and for always encouraging me to never settle for anything less than my best. My one and only support system Karam and Baraa, my sisters, blood-related or not Hala and Asha, the dearest friends who always embraced the nerd in me Ghifar, Ammar, Karin, Hanna and Sarah, and last but not least my emotional punching bag and the person who had no other choice than to put up with my multiple breakdowns, panic attacks and episodes of depression Ahmad.

Abstract:

This research provides a comprehensive analysis of cyber-attacks on cyber-physical systems (CPSs) and proposes an Intelligent Detecting System (IDS) based on Recurrent Neural Networks (RNNs) to identify cyber-physical anomalies in AC-connected microgrids. The study examines various forms of attacks, including False Data Injection (FDI) and Denial of Service (DoS), and their potential impacts on microgrid data integrity and system disturbances. The research addresses attacks not only at the communication level but also at the physical layer, where control settings of controllable units can be manipulated. The thesis is structured into chapters that cover the research background, theoretical frameworks, testbed configuration, proof of concept, and hardware-in-the-loop testing. The work concludes with insights into unresolved challenges, realistic recommendations, and discussions on future exploration tracks.

General Introduction

The sustainable flow of energy, or in other words, energy security, in the field of electrical supply systems, does not only rely on the physical availability of resources. Today's technical challenges are extended to include highly complexed demand response (DR) mechanism in the presence of greater share renewables, and to intricate market dynamics and cyber security.

The bidirectional flow of power and information generated and monitored by highly advanced equipment/mechanisms signifies the new face of the energy networks. Smart grids are expected to deliver tangible progress to the conventional power systems on both aspects of efficiency and reliability, all together with guaranteeing a maximum renewable penetration reinforced by distributed intelligent and demand-side management techniques [1] [2].

Changes will give the consumers and prosumers a wider range of choices and accord them with the possibility to actively participate in the optimizing operation of the system, by means of providing them with detailed instructions on how to better use their supply and act as authorized partners.

Smart grid benefits can also be extended to enrich the coupled economic sector through reducing operational costs and losses, generating new job opportunities, and revolutionizing the energy market with time-based pricing and a more accurate speculation of demand and response profiles. This comes in a time where electricity price forecasts have become a fundamental input and an important tool for decision-making mechanisms of the energy service provider companies [3].

But yet, the complexity level of the actual power networks and the critical role that it plays in every domain form a double-edged challenge, especially when the introduced technologies might itself be the source of threat.

Upgrading the electrical network has not been as expeditious as it should be. With technology being implemented in almost every area of our modern life and smart applications growing in scope and complexity, the power sector makes its steps towards the smart grid at a pace of an extreme cautiousness.

New types of communication and data-management systems must handle not just the different emerging media trends and smart equipment (e.g., computer-based or microprocessor-based), it also needs to cope with existing legacy systems in a manner that is adjustable to scalability and above all, resistant to cyber intrusion [4][5]. To this end, smart grids must come as a complementary solution and not an eliminating or excluding one. These technical uncertainties, plus the additional investment costs, have evoked the political reluctance practiced by energy operators against this shift.

Europe has been working on energy transition and smart grids since 2005, starting by creating the smart grid technology platform which has set the year 2020 as a horizon to complete the process [3]. There

were also several initiatives that carried out the development of experimental testbeds for smart grids solutions which aimed to highlight the most critical challenges and potentials accompanied by this evolution and their influence on the European power systems. Nevertheless, a further and more holistic analysis that is based on a profound technical understanding of each individual system architecture and basically includes the impact of both social and economic aspects on such heterogeneous systems, is yet to be accomplished in order to be able to trade-off between the existing approaches and pilot experiences, choosing a unique and valid experience that is suitable to be scaled up and replicated [6].

On the other hand, a very promising approach to overcome the majority of previous issues appears through energy communities, in which current grid problems are managed in a coordinated way such that avoiding costly network reinforcement along with maintaining aspired values of the smart grid. That is why we might be able to envisage the future smart grid as a sort of aggregation of multiple integrated entities or microgrids (MGs) supervised, monitored, and controlled via a reliable communication-based layer. Accordingly, the increasing interest in microgrid development as the core of the smart grid systems is completely justified [7].

Although this increasing interdependency between physical and nonphysical power system components, which forms the so-called cyber-physical systems, raises a whole new level of complications even on the scale of microgrids.

This work provides a comprehensive analysis of the matter of cyber-attacks on cyber-physical systems (CPSs). It conceptualizes a method to represent and diagnose the existence of cyber-physical anomalies in CPSs represented by AC-connected microgrids. A selection of tools from different domains and backgrounds have been incorporated throughout this research in an attempt to create a testing environment that reflects the complex nature of the studied system.

An Intelligent Detecting System (IDS) based on Recurrent Neural Networks (RNNs) has been proposed to learn the normal behaviour of the Power Management System (PMS) that governs the flow of active power sharing between the MG and the main grid.

We examine different forms of False Data Injection (FDI) attacks including Replay attacks, in addition to the well-known Denial of service attacks (DoS). These attacks tamper the microgrid data integrity and availability by maliciously altering the measurements sent or the commands received by the Distributed Energy Resources (DERs) to or from the microgrid controller. Which in turn could result in large disturbances in the system, especially in low inertia microgrids with extensively deployed static power electronic interfaced Distributed Generation units (DGs). Admittedly, a key highlight in this context was to represent and deal with attacks that happen not just on the communication level but also on the real physical layer. With attackers being able to locally manipulate the control setting of the available controllable units (battery storage systems), this research doubles the challenge for detection

mechanisms and proves, at the same time, the reliability of the proposed IDS to successfully detect both types of attacks.

The structure of this thesis is organised as follows:

In Chapter 1 we set the basic elements of the research background. The gradient evolution of the concept of the cyber threat, starting from the attacks targeting industrial control down to the electrical grid is presented in the first part of the chapter. While the next part elaborates on standardized definitions and terminology choices for the contemporary problematic challenges. The last part concludes this chapter with discussions on why adopting the microgrid paradigm for investigating security aspects in the widespread grid cyber-physical systems.

The recently proposed approaches from different domains to confront cyber-physical attacks are reviewed in chapter 2. A comprehensive theoretical framework has been provided to classify the contributions from different standpoints to help the reader distinguish common points and build an easier decision on which area is more convenient to start from.

The third chapter paves the way for the other two last practical chapters by laying out the needed justification behind the choices made in this work concerning the testbed configuration. It starts by introducing the concept of real-time simulation highlighting the need for this tool to be exploited in the context of cyber-physical system modelling. Then it goes through explaining the advantages of Artificial Intelligence (AI) models, more particularly, Machine learning algorithms (ML) in anomaly detection mechanisms. All along with extracting the research hypothesis upon which the results are proceeded.

Chapter 4 carries out the proof of concept of the proposed IDS. The chapter begins with a description of the adopted methodology moving on to stating the contributions of this work. Furthermore, it puts forwards the technical characterization of the used microgrid model and the used artificial neural network Nonlinear Auto-Regressive eXogenous (NARX). Correspondingly, it presents the modelling and testing in the real-time environment of the used methodology over two groups of attacks: the cybernetic induced attacks over the communication channels and the local physical manipulation of the battery control system.

The investigation of the compatibility of this detection technique to work within real-time constraints continues in Chapter 5 with the hardware-in-the-loop testing. The testbed setup that encompasses the real-time simulator from Opal RT with NARX network on the Arduino microcontroller is demonstrated in the first part of this chapter. While the second part is dedicated to the principle of the analysis of embedded recurrent neural networks and more specifically the NARX model. Additionally, this section had also succeeded into setting the limits of the NARX model in this particular application. Afterwards, The Long Short Term memory (LSTM) model has also been introduced in a successful attempt to overcome these limits in the last section.

Finally, we conclude the work in by providing some insights about the unsettled challenges in addition to realistic recommendations in light of the presented arguments. The perspectives and possible exploration tracks were also discussed in detail as well.

Chapter 1: Securing Cyber-Physical Systems CPSs

This chapter provides an explanatory review of the research context. After a brief description of the smart grid evolution with a link to the introduction of cybernetic-induced industrial attacks, the definitions of the most used concepts are then presented in section 1.2. At last, section 1.3 sets the ground for selecting the targeted system, offering arguments about the interest gained in adopting the microgrid diagram and corresponding challenges, in particular, those related to cyber intrusions.

1.1 Smart grids

1.1.1 The digitalization of the energy sector

Meeting the increased demand rates for electrical energy is getting progressively challenging for grid operators. These difficulties stem not only from the perspective of providing new resources but also from distributing, managing, and securing these newly introduced capacities. Which comes with a growing expectation for a greater reliability, efficiency, safety, and observance of environmental and energy sustainability goals.

The electricity grid in its actual condition with the rather elevated transmission losses, substandard power quality and possible brownouts and blackouts is not in a position that enables it to receive all the emerging aspects of the network evolution.

A smarter grid with real-time observability, intelligent control functionalities and forecasting applications will better handle the transition towards more decentralised, optimised, and greener grids.

Modern aspect of smart grids also includes supporting accurate and advanced communication, energy storage either by classic storage units like batteries or flexible storage such as the vehicle-to-grid models and automated decision-making mechanisms according to a given situation.

The moment where this transformation has started or when it will be completed is still not scientifically calibrated [8]. However, the massive integration of distributed renewable generation into the conventional grid has already started changing the dynamics of the power system from how we know it. Cutting edge devices with smart connected features such as intelligent inverters, meters and controllers effectively regulate the intermittent behaviour of these resources and orchestrate their functioning when transitioning between connected or islanded modes. On the other hand, it also compromises the grid security by introducing additional access points through the cyber layer [9][10][11][12].

Another dimension that smart grids need to accommodate is the exploding diversity of the energy market trends which is also being empowered by the Communication and Information Technologies (ICT) and

digital interactions [13]. This adds another layer of entangled complexity that gets in the way of transparent observability, accurate tracing of reliability analysis and anomaly detection. Especially when breaches into the system could happen at any given stage of its operation process starting from data collection to data transmission, processing and storage [14].

1.1.2 Industrial cybersecurity incidents emergence

The 21st century witnessed the initiation of various cyber incidents affecting sensitive infrastructures. The discovered complexity of cyber-attacks on Industrial Control Systems (ICS) revealed the dexterity level of the attackers in Industrial Con [15].

The smart grid internet interconnection subjects the grid to different forms of hazards, particularly with regard to Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets, and zero-days. Stuxnet, Duqu, Red October, or Black Energy are only a few examples of the advent mayhems touching industrial security since 2010 [3].

Stuxnet, the worm that caused the first reported cyber-physical incident, was discovered by a senior researcher at Kaspersky Lab, Roel Schouwenberg, in June 2010. With a purpose that was beyond stealing, erasing, or modifying data, Stuxnet endeavoured to cause material sabotage in the Supervisory Control And Data Acquisition (SCADA) system as a physical industrial control system. It was regarded as the first cyber-warfare weapon to encompass a complex piece of malware that has infected an estimated 50,000 to 100,000 computers mostly found in Iran, Indonesia, India, and Azerbaijan [16].

Duqu and Flame, another two worms intended towards industrial control systems, were observed more than a year after Stuxnet. Despite the similarities in code source with Stuxnet, they had different objectives. Duqu was designed to track and gather useful information that would help to compromise the opted industrial control set. Flame (or Flamer) was a more sophisticated malware, especially developed for cyber espionage on these networks. Spotted cases were mainly located in Iran and other countries of the Middle East [17].

In December 2015, a cyber-attack on Ukraine’s power system has procured a wide-area outage, affecting around 225,000 customers. The attack was associated with a new variant of Black Energy Trojan named Disakil [3]. According to reports issued by power companies, the SANS institute and Electricity Information Sharing and the Analysis Centre (E-ISAC), the problem started several months before the actual attack by installing the malware through phishing emails. At this period, the hackers only monitored and collected valuable information about the system operation during what is usually called the reconnaissance phase [18]. On the day of the incident, the attackers took control over the Human–Machine Interface (HMI) and cut the power by opening a certain number of breakers. They were capable of disturbing the infrastructure of the Operational Technology (OT) that deploys communication protocols such IEC 60870-5-104 and IEC 61850 [19].

In order to intercept the service restoration, a denial of service (DoS) attack on the communication network, additionally to the classic telephone lines, was employed to prevent the clients from reporting the problem. Even applications that determined the outage extent were blocked by the malware that was able to recognize the system software [20] [21].

This was the first publicly acknowledged incident to have been induced by cyber intrusion which powerfully demonstrates the vulnerability of highly automated cyber information-based smart grid environments to coordinated cyber-attacks.

One year earlier, the same threat agents were identified by the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) during an attempt to penetrate the U.S. electric sector. Despite the fact that the attack, in this case, never happened, it definitely attracted attention on the future potentials of the cyber threats on a sector of utmost vitality [16].

1.2 Definitions

1.2.1 Energy security and Cyber physical systems (CPSs)

The International Energy Agency (IEA) defines energy security as “the uninterrupted availability of energy sources at an affordable price”. Traditionally, security used to be achieved on two fundamental levels; short-term security, which deals with the stability of the demand-supply procurers, and the flexibility that enables the energy system to adapt as quickly as possible to sudden changes in the grid loads. Whereas long-term security focuses on investments that support economic and sustainable development requirements.

Recently, with the arrival of smart grids which are essentially defined according to IEEE 2030-2011 standard, as a composition of three interoperable infrastructures, as set forth in Figure 1. This suggested interdependency that primarily focused on boosting the performance, has led the security problem to grow in complex imposing supplementary challenges threatening to introduce easier ways of causing damage to the fundamental security concerns, all along with creating new ones [14]. Especially in the case of large scale, cyber-physical systems spread over wide geographic areas that generally gather enormous amounts of data.

Consequently, recent security assessment has focused on identifying the potential vulnerabilities introduced by the cyber layer and analyses the possible impacts on energy systems, which has given birth to a brand-new research area called cyber-physical security. A cyber-physical system is co-engineered collaborating domains of physical and computational counterparts, in which the crucial system tasks are basically handled with its physical part, while informatically enhanced processes normally referred to as cyber are responsible for maximizing the exploration of intelligent devices and application [22].

The reason why academia recently chosen to add the term “physical” to the equation is to shed light over the emerging threats imposed by connecting these three fundamentally different infrastructures together, which practically may lead to problems that do not particularly belong to a failure of either systems [23]. In light of these assumptions, further investigations are still needed to either confirm or deny the putative relationships [24].

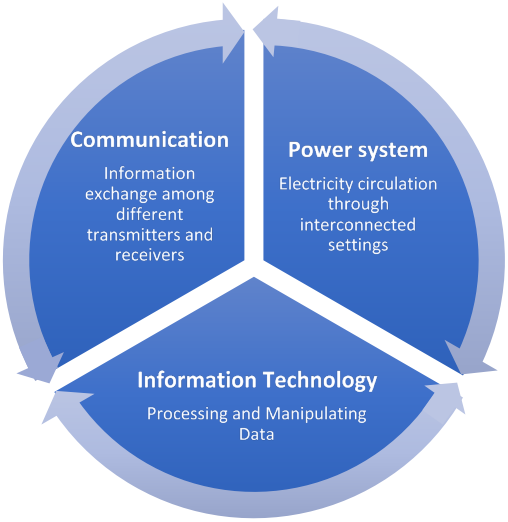


Figure.1 Smart grid architecture in compliance with IEEE 2030.

1.2.2 Security criteria in the energy sector

The most indispensable objectives of security requirements considerations of any data transferring communication in the IT network security are known as CIA-triad, which stands for Confidentiality, Integrity, and Availability, respectively. According to the National Institute of Standards and Technology (NIST)’s guide on cybersecurity strategy, architecture, and high-level requirements. Confidentiality refers to “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” [44, U.S.C., Sec. 3542], and a loss of confidentiality results in unauthorized disclosure of information. Whereas Integrity is “Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity” [44, U.S.C., Sec. 3542]. In other words, attacking integrity is the unauthorized modification or destruction of transferred information. Availability, on the other hand, means “Ensuring timely and reliable access to and use of information” [44, U.S.C., Sec. 3542] as if altering availability will lead to the disruption of the access to or the use of the information system [25][26][27][28].

Smart grid security is also built upon the previous pillars, but with a difference in priority order, where the highest priority objective depends on the industry specific applications. For instance, availability and integrity are the most important critters in the generation and transmission systems, while in advanced metering infrastructure, customer’s confidentiality of personal data is the most critical aspect

[13]. Other references emphasizes the accountability as additional security criteria [29]. The previous sequence of importance goes back to the severity of impacts resulting from tampering with these criteria.

Consequently, supporting reliability and resilience in the events of cyber-attacks is the focus of cyber security strategies in the energy sector. Contrary to the IT systems, when under attack, a control system in the energy sector cannot be simply disconnected from the network as this may trigger safety issues, brownouts or even blackouts. That is why securing the energy sector necessitate a sector-specific approach that cope with the following consideration:

- Real-time requirements: Some energy systems must react so quickly that typical security procedures, such as command authentication or digital signature verification, are simply not feasible due to the time required to implement them.
- Cascading effects: Across Europe the energy trading infrastructure as in electricity grid and gas pipelines are deeply interconnected, so an outage happening in one country could be transmitted triggering blackouts or shortages of supply in other areas and countries. The European Union Agency for Cybersecurity (ENISA) has emphasised the significance of mapping the reciprocal dependencies of crucial sectors. This is critical for determining the extent of an incident's potential spread and ensuring well-coordinated responses.
- Combined legacy systems with new technologies: Many aspects of the energy system were conceived and constructed long before cybersecurity was a factor. These existing assets must now interact with cutting-edge automation and control equipment, such as smart metres and connected appliances, as well as gadgets from the 'Internet of Things,' without being vulnerable to cyber-threats [30].

1.2.3 Attacks terminology (Attacks classification)

Despite the fact that cyber intrusions on cyber-physical systems (CPSs) can be found under different terms depending on the research background, such as bias injection attack, zero dynamics attack, denial of service (DoS) attacks, eavesdropping attack, replay attack, stealthy attack, covert attack, and dynamic false data injection attacks [31]. These attacks can still be classified according to the one or multiple security criteria they are jeopardizing, as set forth in Figure.2.

Intentionally introduced faults or malicious attacks triggered by the cyber layer leaving serious impacts on not only the technical aspects, but also on economic and social correlations in the power network operations, are the focus of this research.

One must admit that even though the attack is generated and injected through the application or communication layer, for the physical part of the system, a cyber-attack is still simply an undetected anomaly that drives the systems to exceed its limits.

Effects range from causing a minor degradation of the services by reducing the efficiency of the attacked systems, to paralysing or stopping critical operations, and could reach up to destroying certain equipment and causing physical damages [32].

However, achieving such results is never an easy task. Physical prerequisites and the current state of the power system architecture with contemporary defence mechanisms, such as controllers prepared to re-examine each input parameter against a selection of acceptable values preventing possible physical damages [20]. This burden the attacker with the mandatory acquisition of a customized knowledge about the physical nature of the system added to the already required computer-related competencies. But then again, this does not mean that the conventional ways of protection, such as the ones adopted to restrain the spread of fault effects by isolating of a malfunctioning entity, are enough to prevent an attacker from achieving an unacceptable condition in the grid [33].

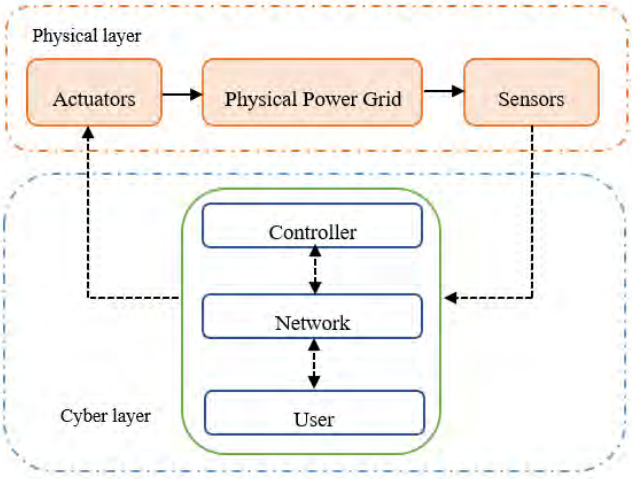


Figure.2 The three types of cyber-attacks.

In that vein, reasonable strategies to fend off such incidence fall into two complementary categories. The first one is about developing measures that tend to detect malicious attacks and tackle down the cause of infection in the system in order to deal with either the compromised unit or entity through isolation or the direct cause from wherein the adversary could have accessed the network. The second important aspect is cyber resiliency, in which we anticipate the behaviour of our system under attack and elaborate on what could be done to expeditiously recover from these attacks in a passive protection fashion.

At any rate, we must keep in mind that keeping the system utterly safe, over and above maintaining a level of simplicity allowing the intuitive understanding of the entangled operation, is a paradox that preoccupies the power system researchers and engineers.

1.3 Motivation for going down scale to microgrids:

1.3.1Modern distribution network vulnerabilities

Distribution systems play a major role in the electricity sector value chain linking transmission to consumption and providing direct contact with consumers [6]. In the transition towards smarter and more decentralized grids, distribution systems are the tip of the spear facing emerging challenges. Knowing that their systems were originally designed for passive energy delivery (unidirectional flows), Distribution System Operators (DSOs) find themselves nowadays forced to cope up with the tremendous changes pertaining to the electrical networks, especially on the medium to low voltage scale.

Accommodating the expansion of variable renewable generation, the growing adoption of prosumer and active consumer roles, and the electrification of the heat and transport sectors are leading to an increased complexity of planning and operation of these networks, which calls for more sophisticated and comprehensive network optimisation tools.

Unlike transmission systems that have adopted the Energy Management Strategy (EMS) early in the 1970s, the application of proper EMS at the distribution level was not put into action until recently [34]. This is due to the fact that distribution networks were traditionally designed to be almost invariably radial and tapered in nature. Generally, they use to be passively operated and need minor supervision or metering which it could be called fit-and-forget networks. It rarely relied on any support generation or other connected resource for security purposes. With low utilisation rates and the use of fixed-tap or off-load tap changing facilities for voltage control, resulting in constraints on the voltage level prevent the access to the full available thermal capacity [35].

The introduction of dispatchable generation units owned by the DSO is a very useful avenue that has been widely exploited over the years. These dispatchable units can be turned on and off by the energy operator to match a scheduled output meeting the network requirements for peak shaving and declining stress over the network components at times of high demand. Nevertheless, the surplus of the distributed generation (DG), especially the non-dispatchable (renewable) type, can adversely affect the performance of the distribution systems causing power quality issues, augmented fault levels, voltage violation, protection issues, in addition to line overloading or congestion [34].

These added distributed units will reflect an ongoing transfer of generation capacity from the transmission to the distribution networks. As it is very important for a cost-effective transition of the distribution systems to drop the fit-and-forget culture and become dependent on these resources for supply security and quality, energy balancing and resilience similar to what is found in transmission systems. Otherwise, alternatives would be economically exorbitant to an extent where it becomes an obstacle in the face of the energy transition.

While following the foregoing tendency, measures continue to offer incentives that consolidate the integration of all flexible distributed resources into the market, side by side, with new demand–response technologies on the demand side [5]. Consumers and community energy are becoming more and more active in developing local, versus national markets embracing the latest technological trends. Self-consumption behaviour where users adjust their demand via storage or other means in response to dynamic pricing signals or other incentives is an example on how deeply interconnected the evolution of the distribution networks is.

The different classes and modalities of prosumers and active customers that the DSO have to coordinate outstand the number of customers that TSOs conventionally serve. This entails the need for even more powerful supervisory control with data acquisition network management facilities to support the real-time functionalities including monitoring and controlling of the network assets in addition to assisting the procurement process.

3.1.1 The role of smart metering

Advanced metering infrastructure (AMI) is one major transformation aspect that allow DSO to better managing their utilities along with providing a superior customer service. Smart metering deployment as a key element in the AMI is expected to generate the necessary data for regulating the consumer's impact on the network and allocate recovery costs in a fair manner amongst newly formed customer categories.

Smart Meters (SM) at the endpoint of distribution networks liaise with consumers and lend them an open window to interact with the utility. In an ideal scenario, smart appliances must effectively communicate throughout AMI to optimize its operation scheduling, as set forth in Figure 3.

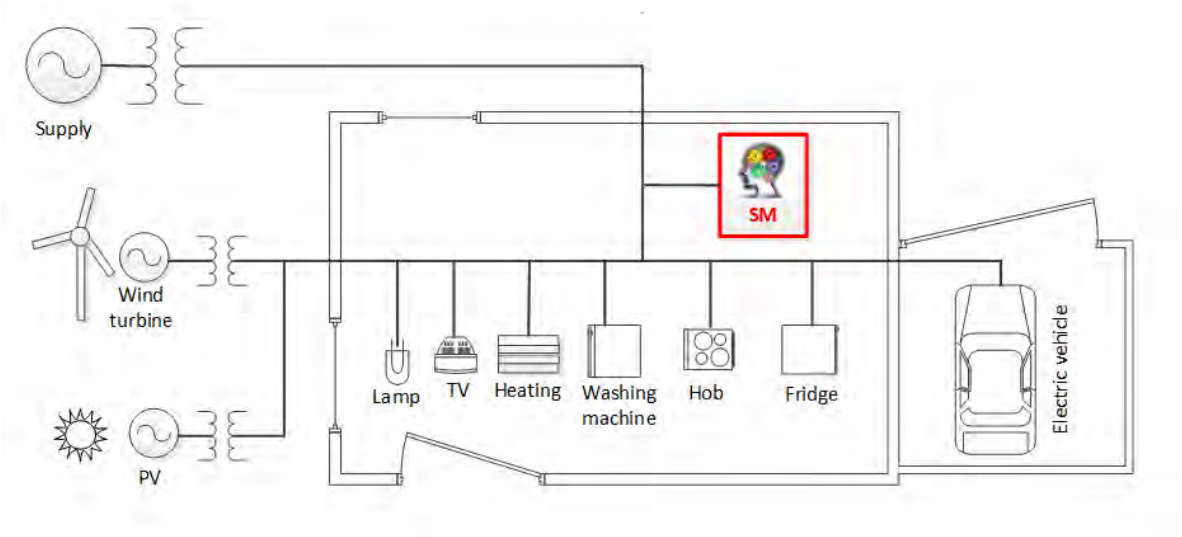


Figure.3 Smart meter connection.

Since its first appearance in 1872 [36], the concept of electricity meter has drastically evolved. Conventionally, electricity meters used to provide information only about electricity consumption in terms of total current amplitude, while intelligent meters are supposed to support a wide range of applications rather than just metering [37]. Providing measurement, control, communication, power display, and synchronization capabilities shall be no easy task to be handled by smart meters alone.

For the time being SMs are installed and deployed by the utility inside of consumer's facilities. They communicate with data concentrators and control centres which monitors and partially control the meters. Machine-to-Machine (M2M) communications among appliances in accordance with information provided by service providers enhance demand response functionality, leading to a win–win situation [38]. Besides the aforementioned control and management advantages, collected data can also help the grid operators in applications such load forecasting.

The absence of human interventions as a key feature of advanced metering plug and play mode, is very desirable but unfortunately, at its earliest phases, comes with relatively high expenses. The exposure to a different kinds of communication systems, including internet, in addition to the needed adaptability to work with different billing applications, that are probably open sourced not to mention the double ownership making smart meters the most vulnerable component of the distribution systems. On the other hand, and in the process of pursuing autonomy, future meters are being tested to enlarge their authority margin so the amount of transferred data to and from control centres can be reduced [39].

This intensive dependency on the information and communication technology (ICT) in performing market-based solutions in one hand and managing constraints while maintaining network security on the other hand, calls for additional packages of competencies that DSO needs to acquire. Especially regarding data processing, application design, support or virtually managing energy producers through the cloud, and all of which a cyber intrusion might seize to breach these networks and tamper with its essential operation conditions.

Addressing these challenges without derailing the energy transition or compromising security requirements will not be fulfilled only by enthusiastically receiving innovation and novel working approaches. Significant structural changes are also needed, as investment in modernizing the distribution network should not only be meant for the containment of the newly introduced elements, but it should also cover the costs of replacing ageing network component. Not to forget that deciding on the scale, the time and the proper pace that this investment should take is a central challenge on its own in the presence of all related uncertainties.

All that and more has raised the need to integrate unconventional approaches to alleviate the burden on the distribution networks. Here where microgrids (MGs) are perceived as one of the ways that DSO challenges are managed locally. It also plays a pivotal role in accounting for cascading failure events either induced by natural causes or as a result of intended sabotaging intrusion attempts.

1.3.2 Microgrids as a Cyber-Physical System (CPS)

Despite the tendency to associate the term microgrid with the power sector, we find that the concept represents itself in a larger context related to the energy community with different means of energy production, transition, and storage, all along with achieving the mutual goals of boosting technical and economic resilience [40].
Through the years, different definitions have been placed in the technical literature to describe the concept of a microgrid. The first one was proposed in [41] imagining the microgrid as the ultimate solution for the reliable integration and control of the ensemble of Distributed Energy Resources (DERs), including Energy Storage Systems (ESSs) and controllable loads [42].

Similarly, in [43][44], microgrid paradigm is foreseen as a very appealing strategy to overcome challenges in integrating the massive renewable resources resulting from summing up all community-scale capacities, which is still being kept on hold due to the inflexibility of the current networks. Furthermore, these individual DERs are often too small to enter the electricity market, which is another problem that has been solved thanks to this new topology.

This goes in line perfectly with what is stated by the US Department of Energy, with only one difference stressing the clear barriers with respect to the distribution network, in the way that it permits the microgrid to have the ability to operate not only within grid-connected mode but also in autonomous island mode [45]. Which in turn was found, in numerous studies, to be considered as a prerequisite to denote a microgrid [16].

With microgrid pushing the power system over the edges of decentralization, a geographically localized distributed power model makes more sense regarding risk-management in terms of regional resilience and preventing cascading failure in the event of extreme weather conditions, cyber-attacks, etc. [44]. Knowing that the electricity supply for small urban or industrial communities (isolated microgrid) where the main grid connection is inaccessible was never a novel trend in the world of electrical alimentation [43]

There were numerous attempts to create a standardized configuration of the smart grid's building block, namely microgrid. However, its structure is yet considered to be arbitrary and any technically well-functioning connection is valid [22] [43]. It is important to notice that the microgrid's ability to fit in different configurations and to be customized as a function of the present requirements and constraints is the exact same reason why it is utterly difficult to classify it in a fixed frame.

However, from an operational perspective, there are only two types of microgrids (MGs): A grid-connected MG, which is built to operate in either islanded or connected mode, might have one or several connection points with the grid. A single point of connection is very common though [15]. Whereas, an

isolated or stand-alone microgrids does not even have a Point of Common Coupling (PCC) with the main grid [32].

In grid-connected mode, for example, frequency and voltage values are regulated by the host grid at the point of common coupling. Whereas tasks like the DER's active and reactive power accommodation, energy management and load sharing, in addition to a safe transition between connected–islanded modes are still elaborated by the microgrid's control systems. During islanded mode or in remote conditions that are completely isolated from the grid, the microgrid's local controllers take full responsibility for all stability measures which also vary depending on the microgrid type (Islanded AC, synchronized islanded AC, naturally islanded DC) [43]. Typically, having one of the DERs operating as the isochronous generator forming the microgrid voltage and frequency is quite common in islanded microgrids. In this case, the rest of the DERs could participate in supporting voltage and frequency if needed [16], whilst the complete absence of a dominant source of energy generation during the autonomous mode of operation adversely amplifies the complexity of the assigned task list.

Microgrids' implementation into utility does not always have to follow the classical case where a single MG is connected directly. Other alternatives can still exist, such as multiple tie line-based interconnected microgrids and small MGs within larger ones, so as the biggest takes the role of the governor large areas electrical power system [44].

Being highly dependent on multi-layered functionalities starting with data acquisition mechanisms usually performed by cyber sensors and intelligent measurement devices. These transmit critical data through a communication layer that in turn includes a vast range of wired/wireless technologies and network devices. The information then are finally being delivered to the energy management system (EMS) on the application layers that optimizes, monitors, and sends control signals back to the actuators on the physical layer. That's why microgrids are a real representation of cyber-physical entities that inherits both advantages and disadvantages of the aforementioned interconnected infrastructures.

3.2.1 Microgrid control

The majority of prior research pictures the microgrid's control paradigm in a hierarchical manner, following the successfully adopted structure in the legacy grid [40]. Hierarchical control levels of microgrids are usually anticipated in three layers: primary, secondary, and tertiary. There are no definite technical boundaries between strategies of each level rather than a sort of indication based on relevant considerations, such as response rapidity interval, purpose-oriented control, and central-distributed control.

However, without losing generality, we can say that primary and secondary control strategies are practically associated with operational stability and accordance between microgrid's components, while harmonization with the host grid is applied by tertiary control [43].

Primary control features the fastest response with the smallest decision time step, voltage, and frequency regulation, as well as protection executed on this level, which is entirely based on local measurements and droop mechanism with no communication needed [43]. That is why operations on this level are conserved away from cyber incidents.

On the contrary, secondary control operates on a slower time scale, often with a reduced communication bandwidth by using sampled measurements. It collaborates consistently with the other two levels to satisfy the requirements set by the tertiary control. The secondary control measures values across the microgrid, and accordingly, updates the desired setpoints for the primary controllers [46].

Tertiary control on the highest hierarchy collects state information of the energy system through the communication infrastructure and makes decisions to optimize the overall performances of microgrid with the longer decision time step. It may also be responsible on the economic dispatch of controllable resources and coordination with the distribution system operator with Energy Management System (EMS) ensuring power balance, security, and operational constraints [40]. Figure.4 illustrates a generalized structure for modern microgrids.

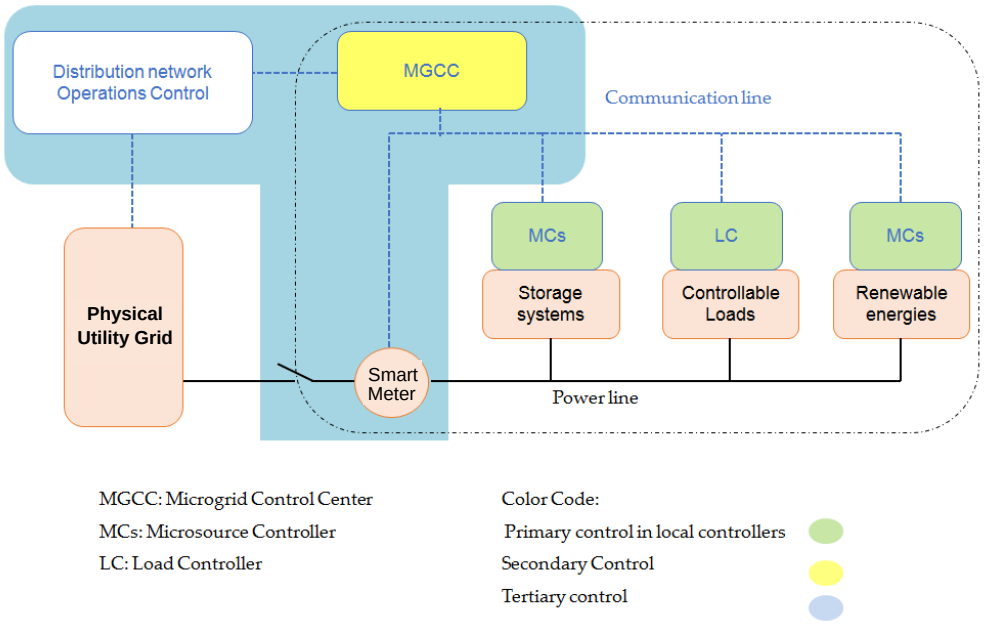


Figure.4 Modern basic structure of a microgrid.

Previous control functions can be achieved through either centralized or distributed implementation of the control architecture.

Distributed control was originally proposed as a solution to boost scalability in modern networks by means of facilitating the introduction of supplementary DERs. It splits control tasks between units instead of the substantive upgrading of single excessive computational capacities. Moreover, the sparsity

of communication networks utilized in distributed control schemes reduces the infrastructure cost [47]. Not to mention, that is also considered to be more resilient as single-point failure does not lead to cascading event, unlike centralized or what might be called hierarchical control, in which messages that carry out measurements and instructions from and to all system components should pass by a dedicated central controller. Correspondingly, centralized control schemes have a better understanding of the microgrid functions since it has an embedded version of the system model in the central controller which in turn will trigger an optimal application of EMS objectives including the economic performance simultaneously with satisfying real-time operational constraints.

Among distributed optimization methods, consensus control has gained more attention in the microgrid control community recently. The initial notion was inspired by biological phenomena that revolve around providing each unit of vision on the overall objective to a limit where different DERs converge to a single value. Here, decisions are built upon local measurements and peer-to-peer communication, offering this model extra flexibility, adding to the already well-established feature in the distributed structure. Cooperative control is also a very feasible solution for stability control in terms of voltage and frequency equilibration and economic control with cost consensus for generation units across the network [40].

The discussion on privileging one control method over the other is still questioned by several papers focusing on different aspects [7][40][47]. Regarding the scope of this work, the authors in [7] review basic branches of distributed control optimization and their application with a brief reflection on the cybersecurity consideration, promoting distributed control on the bases of mitigation obstacles relevant to communication risks and stakeholders' resistance to sharing critical data. While others in [48][49], highlight that a distortion effect of anomalies produced in a single DG unit might trigger a cascading propagation in other units under a cooperative control protocol.

3.2.2 Potential risks form attacks (Attack vectors).

Despite its substantial advantages in regard to simplifying the management of small to medium-scale generation capacities, MGs are still considered as non-intuitive or even quite complex systems with a high degree of parametric uncertainties resulting in high failure rates. Especially with the absence of governing norms that provide reference identifications of acceptable participating gadgets which might include wide range power electronic devices or incompatible micro-sources. In addition, to the lack of inertia that is hardly being compensated by expensive emerging storage capacities. Not to mention, the increased dependency on intelligent features. All that and more, has rendered microgrids extremely vulnerable cyber-physical systems.

Therefore, Smart microgrids are exposed to the risks of cyber intrusions and they represent a fairly tempting target, depending on the attacker incentives which may include energy theft, data leaking, or even damaging physical infrastructures. Of course, the success yardstick is highly correlated with the

presence of security gaps and the attacker's level of competences that would enable him to penetrate the system and perform the task without triggering any defence mechanisms.

Additionally, microgrids are prone to the same types of attacks found in the utility grid. However, the sound operation of power management strategy (PMS) is more critical in microgrids. Reasons narrow down to the imperative adjustment of multiple interconnected DG units with significant differences in power capacities and generation system characteristics that become more and more Electronically Interfaced (EI-DG), requiring a faster and more customized response to keep dynamically changing characteristics (voltage/angle) within the appropriate margins [42][31]. This introduces practical limitations that distinguish MGs' fault detection, classification, and coordination from approaches adopted in legacy protection systems [50].

A microgrid’s control systems are a typical target for attackers. voltage and frequency regulation appear as a trivial subject for attackers that focus on deteriorating the technical functioning of a smart microgrid. FDI targeting voltage control could modify sensor measured voltage and/or reactive power data and control parameters [51][52][53]. It is even possible to break into the microgrid's multi-layer control system and tamper with control signals among layers inducing errors in DGs reference power signals and transformer tap changer signal [54][55][56].

Similarly, for attacks on transient stability in AC microgrids that Jeopardize the frequency control. Active power and frequency measurements, in addition to reference signals, are susceptible to being maliciously intercepted and manipulated. Resulting in changing the behaviour of the physical equipment responsible for active power regulation such as rotating machines and energy storage systems. As it may change rotor speed or angle measurements [57][58][59], as well as commands that actuate the storage systems to absorb and/or inject active power from the microgrid [60][61][62].

More information on cyber-attacks on load frequency regulation can be found in the following articles [63][64][65][66].

One of the most important aspects that need to be seriously taken care of in the context of cyber-attacks is the MG ability to connect or disconnect from the grid. Especially when disconnecting a malfunctioning MG that is suspected of being under attack is an indispensable safety measure that enables the grid to reserve itself from attacks. Simultaneously, unintentional or unplanned islanding also has a severe impact on the MG stability [67]. In a best-case scenario, triggering this effect by attackers without instantaneous detection or mitigation would drive the protection schemes to initiate nuisance load shedding and generation curtailment that might result in a complete shutoff of the MG (microgrid blackout) [16].

Knowing that, the phenomenon when parts of the power system get separated from the rest of the network was a prior concern according to IEEE Std. 1547 [68].

Smart households resemble more and more to microgrids. Where different generating units, storage and connected appliances are being remotely managed through a centralized controllers that handles the consumption scheduling based on telemetry data and price indications provided by utilities' service providers.

In this sense, pricing cyberattacks on the guideline of the electricity price information is another way of disturbing consumption mode scheduling. This would induce a negative economic impact on each individual attacked entity, but most importantly when applied to a larger context with multiple affected MG. It could create a peak energy load leading to an overexertion of generation capabilities of the grid [69]. On the contrary, Attacks could also be designed to manipulate the smart metering transferred data indicating lower consumption rates for a reduced billing in an attempt for energy theft.

Figure.5 shows an example on the types and location of attacks that could affect the MG security internally or potentially get exported to the distribution system.

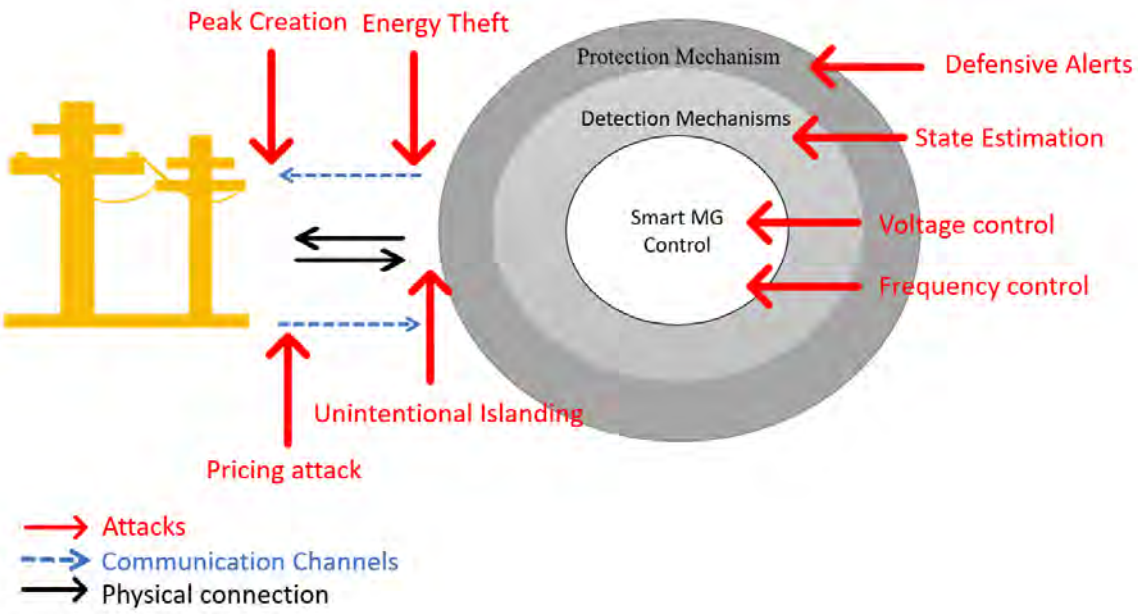


Figure.5 Cyber-attacks on smart microgrids.

Smart devices included in the MG topology could be breached like any other connected device through six approaches as follows: Breakthroughs could occur either by attacking the device during the boot process when high-level protection mechanisms are non-executable or, through hardware exploitation, due to the fact that the majority of security implementations and protection measures are found at the software or firmware layer. This last one involves searching for windows left from manufacturers as debugging ports and uses it to perform tasks like flashing external memory, timing attacks, etc. Hardware exploitation could also be utilised to repeal authenticating process in order to gain access to

the device's cloud services , like what happened with the Itron Centron smart meter case whereby attackers were able to manipulate the ID information [70].

Another type of exploitation could happen on Chip-level of integrated circuit for the purpose of retrieving sensitive information stored in hardware modules along with bypassing hardware protection mechanisms.

Passwords and other sensitive information are normally securitized using encryption and hash functions that take a crucial part in device communication and authentication, are known to be mathematically reliable and robust on their own. Yet, their integrity is susceptible to side-channel attacks and information-based cryptanalysis methods Especially when their implementations are done improperly deploying cryptographically weak encryption algorithms.

Backdoor access channels used in remote debugging and Over-The-Air (OTA) firmware upgrades could also be one of the possibilities that enable the attacker to obtain the status of a given device or even control it.

This leaves us with the last approach that takes advantage of software-level vulnerabilities typically found in standard embedded systems and computing systems.

Most of these gaps have been addressed by cyber security specialists in different fields, But what makes this problem more critical in smart grid applications is that most of the mitigation solutions may not fit in the smart devices by reason of computational and resource constraints [70].

In conclusion, microgrids are a highly sensitive cyber-physical systems [22], in which the physical part is strongly influenced by the integrity of the cyber part, due to more entry points, very low required latency and the absence of multi-stage security detection. Consequently, attackers have more of a chance to cause serious problems in microgrids, leading to overall catastrophic consequences [71].

That is why we decided to work on the level of microgrid security in this research. Throughout the next chapters, we will explore the state of the art of recent papers that discussed the cyber-physical security of smart microgrids, to finally develop our own proposed strategy employing our own selection of tools and techniques.

Chapter 2: Relevant works: overview and state of the art on conventional attack detection mitigation

This chapter introduces the concept of cyber-physical security from a cross-layer perspective. It addresses the existing approaches attending to cyber-physical security in power systems from a microgrid-oriented viewpoint.

2.1 Perspective-based interventions addressing cyber attacks

In contending counteracting measures against cyber-attacks there is no unique and only way to proceed. That is why everyone would have the chance to contribute from their own perspective and domain of speciality in a multidisciplinary manner.

The following subsections will dive into the actual issues and case studies that occupy the researchers' attention from different viewpoints. We tried to classify the contributions to the microgrid security against cyber-attacks into 3 main categories.

2.1.1 Microgrid communication

Being a cyber-physical system, microgrids inherent equally advantages and disadvantages of the combined systems. Communication network is essential to effectively incorporate many of desired features of the smart grid, such as the distributed automated systems, distributed energy resource protection, islanding, and the display of network state and performance.

Standard communication problems also appear in microgrids, as it suffers from incompatibility between different types of heterogeneous communication technologies [22]. Besides the increasing reliance on Wi-Fi and internet-based communications, which are more susceptible to cyber interference but still essential for ancillary services related to microgrids, such as weather forecast data, electricity prices, peak hours, etc. [22]. Taking into consideration the expanding amount of data transferred between microgrid's components, different connected microgrids, or with an external centralized control and monitoring point, upon the design of the control structure. Satellite data (GPS) might also be a sort of communicated signals under danger in synchronous microgrid with Phasor Measurement Units (PMUs).

On the other side, intrusion detection, firewall, and other selected solutions from the traditional security measures against rudimentary attacks targeting conventional data networks can also be included in smart microgrid applications as mentioned earlier [72].

While some prefer to leave the power generation control network isolated from the public network as a countermeasure against cyber contingencies, the leverage of open transmission protocols and computers

with common operating systems that performed as Intelligent Electronic Devices (IED) cannot be neglected nor eliminated today. Especially with essential improvements on automation efficiency and control system costs [29].

As an attempt to study and simulate the influence of an attacked communication network on electric power systems, earlier efforts went to model the attacks as a time delay to be accounted within the control loop, a subject that has been widely explored even outside the scope of cyber-attacks. For example, in an islanded microgrid, the authors in [73] have examined the communication delay limits beyond which we might risk having instability issues. They proposed an impact mitigation approach that revolves around gain scheduling for Proportional–Integral (PI) controller used in the secondary frequency that can be adopted in other microgrids as long as they can be modelled in the same small-signal model.

However, these assumptions on the nature of attack impacts are oversimplified and do not fully cover the new debouching aspect of joint cyber-physical models [74][57]. Others argue on the matter of communication latency's impact on microgrid control on the first place, building on an example that puts out shreds of evidence on having an inconspicuous and highly nonlinear relationship of delay rates between the source causing the delay and the resulting delays in the networks [75]. They also state the fact that, except for the simplest of cases, deriving tight bounds between delays, or other relevant metrics such as loss rates, is nearly impossible, especially when the models' analytical accuracy declines as the network size grows from single-hop settings to relay networks.

Taking the communication problem to a larger extent, a Cyber-Physical Power System (CPPS), authors in [76] dig into what might be a better communication configuration in terms of preventing a cascading failure, and in a comparison, based on transmission efficiency threshold values, they find that double-star communication networks perform better than the mesh communication networks.

Preventing cascading failure in cyber-physical power systems (CPPS) through a comprehensive analysis of the mechanisms and dynamical characteristics of interdependent networks was also the focus of the research presented in [24]. The writers have reviewed the different existing approaches and methods of power and communication systems coupling and interconnection and then proposed a novel interdependent model with the "degree–electrical degree" assortative link pattern that has proved its effectiveness in reducing the probability of large-scale blackouts caused by random attacks. Whereas, in the case of malicious attacks, simulation outputs have demonstrated the superiority of the random link model. Results also highlight in a more general manner the importance of coupling strength between the two layers over the choice of the interdependent model. Clearly, the more dependent the power system is on the communication system, the more fragile it becomes.

Among a very diverse variety of problems discussed in the Information and Communication Technology (ICT) field, the particularity of synchrophasor systems vulnerabilities against cyber-attacks was highlighted due to the growing interest in synchrophasor technology applications [77].

Notably, the absence of built-in security structures in the widely adopted IEEE C37.118 communication framework that sets up the standards for PMUs and Phasor Data Concentrators (PDCs) is making it highly exposed to cyber threats [78].

Experiments involved resiliency examination of the communication system structure based on IEEE C37.118 under different attack scenarios, accompanied by estimation of possible impacts on synchrophasor application that uses this standard [78].

In [79], vulnerability analysis went deeper into the IEEE C37.118 framework structure to its weakest components, which the transport protocol layer, as they discuss the susceptibility of two commonly used protocols in transport layers (i.e., Transmission control Protocol (TCP) and User Datagram Protocol UDP) against DoS and FDI attacks summarizing the requirements to be used for creating a successful cyber intrusion as well as to prevent it.

A comprehensive comparison with IEC 61850 that took into consideration the security implication of both standards stressing the advantages and disadvantages that encounter the synchrophasor application developers was also performed in [80].

Figure 6 summarizes the proposed approaches explaining the main mechanisms and pathways considered in acting against cyber intervention in the communication domain.

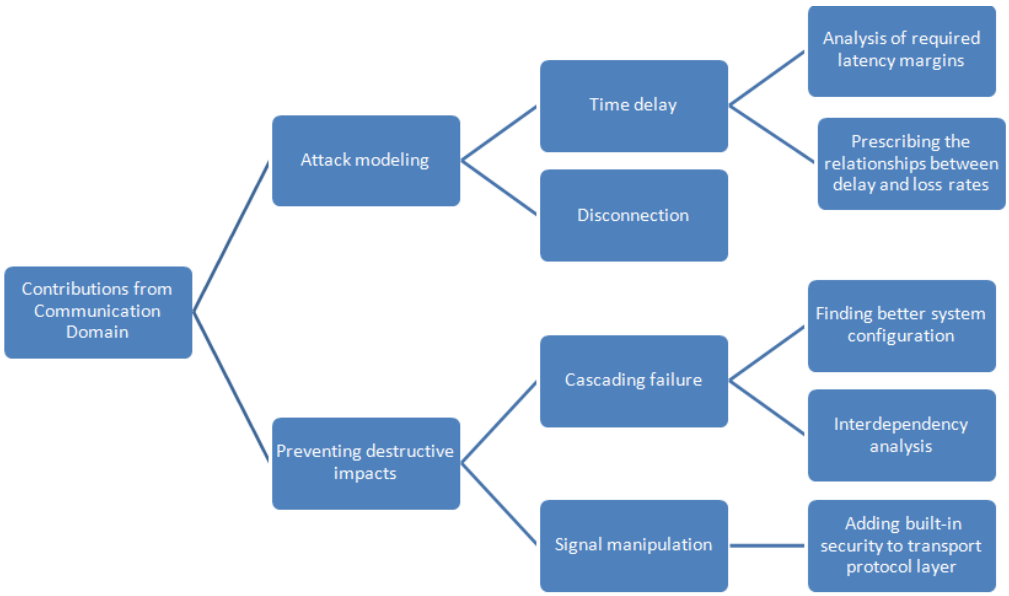


Figure.6 Contributions against cyber intervention from the communication domain.

2.1.2 Conventional control-based strategies against cyber-attacks

Since control systems were conventionally developed to detect, process, and mitigate systematic and unpredicted errors, there is no wonder it has been the focus of numerous research cases in the field of attack predictability, detection, and protection.

Broadly, detection and mitigation of conventional attacks are already well explored in the literature. FDI that succeeds in penetrating the network while maintaining discretion without altering the system observability disturbance alarms, also known as stealth attacks [81], are able to cause unpredictable stability issues and the worse is that they are practically impossible to detect [82].

From a defender perspective, recent research attainable choices are perceived into either addressing the fault detection and isolation in control loops (detection based) [83] or working on precaution measures based on threat modelling and security analysis (protection based) [84].

The popular method used to detect bad measurement data in power transmission systems is the Static State Estimator (SSE). It is generally based on a Weighted Least Squared (WLS) solution and it is not immune against attacks itself [85][86].

State estimation is also important to microgrid control functionality and it is usually found in traditional energy management systems derived from steady-state models [31]. However, static state models were no longer able to capture the systems' dynamics accurately with the exacerbated numbers of DERs on the generation side and the debuting retrofits on the demand side.

The research presented in [31] emphasizes the importance of deploying a secure dynamic state estimation on the side of AC-connected microgrids as a portion of the distribution network. Similar to [87] they proposed an estimator algorithm for a standard structure-preserving model that incorporates system dynamics. Method validation illustrates the estimator's ability to give a secure dynamic state estimation when supplied with inaccurate measurements caused by either an attack that manipulates communication between transceivers and the microgrid operator, or attacks that manipulate measurement units themselves, even without considering an attack scenario.

Traces left on the operation of observers turn into an efficient key to be used in attack detection. Distributed state estimation method is used as a way of detecting cyber-attacks of the FDI type. In [88], a consensus-based controlled DC microgrid was investigated where each distributed generation unit had employed the Unknown Input Observer (UIO) to estimate the state of its neighbouring units and isolating the fault source consequently.

Another control approach using UIO was proposed in [83]. Where a fully decentralized load frequency controller was developed and tested with a perspective to be applied to multi-AC and DC microgrids.

Given that the relative simplicity of the cyber-attack detection of the FDI type in distributed control schemes, authors in [82] have decided to raise the bar by firstly introducing a stealth attack that is able to deceive the conventional distributed voltage observer without triggering the detection mechanism. After that, they proposed a general algorithmic-based detection framework for DC microgrids where they added a Cooperative Vulnerability Factor (CVF) to the voltage PI controller. Finally, and under worst-case scenarios, artificial disturbances were added to by coupling the CVF with the secondary current sublayer in order to enhance the chance of capturing the attacks.

Later, the same DC microgrid model was used in another experiment using artificial intelligence in [89]. A Nonlinear Auto-Regressive eXogenous (NARX) neural network was trained over the previously mentioned control method during offline operation, capturing and storing its behaviour, only to be used then as an online estimator for DC voltages and output currents of each unit. The FDI attacks detectability of this method was built on the estimation errors making it suitable for a larger spectrum of DC microgrid, in contradiction to the cases presented in [82], [90] that only suits those functioning with cooperative consensus-based algorithms.

The FDI problem shaping in terms of determining the aspects that could be altered by such an attack was the subject of [91], in which a detection method was built on the assumption of the attack capability to modify the invariant values required in the secondary distributed control layer.

A new technique for optimal dynamic state estimation, based on a distributed algorithm for multiple connected DC microgrids under FDI attack, was proposed and tested over malicious and normal load disturbance in [92], proving its capability of distinguishing between the two cases. Unlike previous literature that dealt with DC microgrids as quasi-static models, this work employed a dynamic microgrid paradigm where the three DC connected microgrids employed in the study collaborated under a control configuration, that enabled each of them to verify the security status of the other two, making it possible to isolate the potentially infected entity.

2.1.3 Impact analysis to enhance protective control

Another way of proving that cyber-physical solutions for the power sector are not just a solution waiting for a problem, remarkable efforts in the field of impact estimation and threat modelling were made to dispel the doubts on the capability of cyber-attacks to cause actual physical damage.

That is instead of delving into the communication protocol and current computer network security measures, data integrity attack investigations, for example, often focus on the outcome of accepting false hostile data into the system controls. This gives the research problems more leeway in their design and

allows them to investigate the potential consequences of a successful false data attack on the system [93].

The research presented in [33] demonstrates the possibility of authentic corruption caused by two types of cyber-attacks (availability and integrity attacks) jeopardizing the ICT and the GPS systems required for the sane functioning of a microgrid in three different operating modes (connected, islanded and sync-islanded). The severity of the physical impact, which may vary between local blackout, the main instability violation of power quality equipment damage and human danger witnessed in the example microgrid is strongly related to its own architecture.

Other researchers were more interested in exploring the effects on a specific area in the microgrid systems, such as secondary frequency control function in [47] and distributed load sharing [94]. But since these studies are limited by the chosen system, more efforts had to go further into developing threat modelling methodology that fits into the purpose of risk characterization in different systems architectures.

As an attempt to fill the gap, authors in [77] explore the possible arising genres of threat in the components of different systems predicted on missing security properties, and how powerful this could be on the system security entirely.

Without continuing further into the investigation on the nature of the imperilling data or the way that the attackers may use in order to achieve instability in the system, other research simply focused on adding redundancy security to the existing used control methods. Authors in [71] have proposed increasing the security by coding the signals that carry the information about the state's measurements, with an error-correcting code Recursive Systematic Convolutional (RSC) code, and then decoding it to enhance the performance of the proposed semidefinite programming based on optimal feedback controller, coupled with Kalman filter estimator by elimination of a portion of noise on an IEEE 4-bus distribution feeder considered as four grid-connected microgrids.

Reachability analyses were frequently employed to determine if an unstable state could be reached due to certain changes in the monitored variable. This was elaborated in [44] by designing a stability monitoring and control comprehensive framework, that guarantees resiliency against attacks through isolating the problematic bus, while covering critical loads compensated from neighbouring microgrids.

Ultimately, we are still far from finding the optimal mix of competencies that will help researchers to resolve all the nascent problems pertaining to smart microgrid cyber-physical security. Holistic solutions should be based on the multidisciplinary intersections between different domains. It should also come as a result of the concerted efforts of researchers within their fields of interest. Thus, deciding on the angle that a group of researchers would choose to attack this subject is vital. This often requires the

extraction of the set of approaches that match the basket of skills and tools they master, which happen to be the goal of the third chapter of this work.

Chapter 3: Aspects for Modelling and simulation of CPSs for investigating cyber-physical security

Security analysis that covers fault detection methods may be conceived through three groups, that is either model based [95], signal-processing based [96] or data-driven methods [97].

Our testing methodology for detecting cyber physical attacks in microgrids (explained later in Chapter 4) and validation tests (Chapter 5) involve both aspects of real-time simulation used in modelling and proof of concept purposes, as well as the deployment of Artificial Intelligence (AI) applications for anomaly detection and security assessment.

This chapter justifies the choice of these techniques from a theoretical point of view and extracts hypotheses upon which this test selection is based. It starts with expounding the problematic of providing an acceptable testbed that is able to represent all aspects of CPSs along with exploring different approaches to co-simulate or represent needed environments. The concept of real-time simulation with relative advantages and defiance cases is also introduced in detail, as an indispensable approach, to emulate the systems under test in an adequate accuracy. All in keeping the real dimensions of the studied phenomena as close as possible to reality.

The second part introduces the application of Artificial Intelligence (AI) models, more particularly, Machine learning algorithms (ML) in the context of data-driven system identification and anomaly detection and hence Cyber-physical intrusions.

3.1 The need of Real time simulation in investigating MG security (accuracy- online detection- and HIL Application)

Practical experimentation on security vulnerability of CPS necessitates an accurate representation of these systems. Experimental studies are still dangerous and economically unfeasible for microgrids, as it is for large-scale smart grids. That is where simulation platforms come to provide an effective way to test and validate the future aspects of the power system in a low-risk environment while offering the most time and cost-efficient solutions.

Simulations in general, allow clear and multiple options of trade-offs that could be tested parallelly and iteratively without experiencing any degradation of the system qualities or parameters changing over time. Initial conditions restauration is an advantage in attack testing scenarios to eliminate any suspicion of cascading events.

However, capturing all aspect of the large number of components, modules, and buses of the distribution network and consequently microgrids especially with the tendency of using an increasing switching frequency needs an extremely powerful computational resources and a suitable simulation technique.

Based on the synchronization of the required time step with the real-time clock, one can distinguish two basic sorts of simulation: offline simulation and real-time simulation.

3.1.1 Offline simulation environments

Some simulation environments like PSCAD/EMTDC, NETOMAC, Spice, Power System Blockset, and other offline digital simulators are designed to run on a conventional multitasking CPU. These types of simulators solve mathematical equations that represent the dynamics of the modelled system for a given sampling step, where each variable/state of the system is solved successively according to the variables/states at the end of the previous sampling step. Upon that, the actual time required to calculate all the equations representing a system in a given time step may be either shorter than the sampling step of the simulation, in which we call an accelerated simulation Figure.7(a), or even longer as demonstrated in Figure.7(b). Considering that offline simulation objectives are to obtain the results in the shortest period of time possible. One should keep in mind that the system solving speed relies principally on two factors: the computation capacity of the simulator and the level of complexity that defines the given mathematical model [98].

However, In both cases of an offline simulation, the computational time of an event does not reflect the event's real-time which impedes offline simulator from being implemented in interaction testing of different physical control and protection equipment [99].

3.1.2 Real-time simulation environments

Real-time simulation on the other hand, refers to a computer model of a physical system that can execute at the same rate of time of as its physical counterpart (i.e., If a bucket takes 2 minutes to fill in the real world, then the simulation will take exact 2 mins as well). To be more precise, the required time interval for computing and producing results at each time-step must not exceed the wall clock time-step see Figure.7(c). Unlike accelerated simulation mode where the execution time step is also less than the physical one. The real time simulator will delay the beginning of another operation until the start of the next sampling step leaving an interval of an idle time (dead time).

This will allow the simulator to complete all processes needed in order to achieve a relevant real-time simulation that is able to drive inputs and outputs (I/O) to and from externally connected devices [98].

It is essential for inputs and outputs in a real-time simulator model to be synchronized to a real-time clock at any given point of time during the simulation, which may be considered as the main difference with "time-scaled" offline simulation [99].

Real-time simulations are performed in discrete time with a fixed time step that moves forward in an equal duration of time contrary to other approaches that use variable step sizes to achieve a higher level of precision in applications that encounter high-frequency transients and nonlinearity [100][101].

Real-time simulation was firstly introduced in computer gaming, but it was able to find its way into the industry in many applications as operator training and off-line controller tuning [102]. LabVIEW, VisSim, Simulink and some other advanced computer languages feature a great ability to create such simulations in a very efficient rate of time.

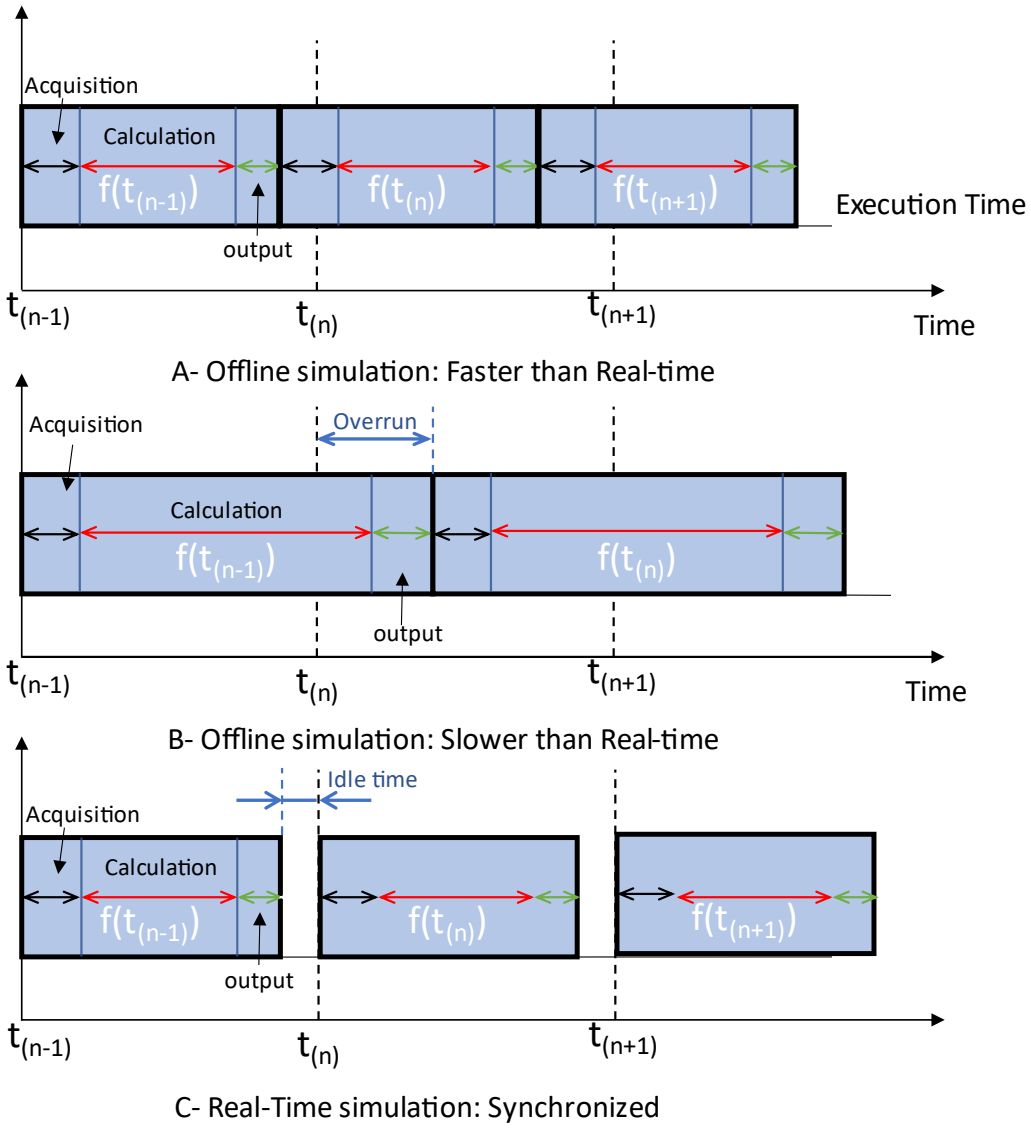


Figure.7 Different types of simulations.

With only a few reliable platforms around the world capable of performing highly complicated tests, real-time simulation is a powerful alternative solution in this area of research [75].

In smart grid in general and particularly, in microgrids, there is a growing interest in the real-time applications for heuristic optimization algorithms, control and energy management purposes. System diagnosis and fault detection are also attracting attention for putting self-healing perspectives into operation especially in adaptive readjustment after a contingency. For instance, in the cases when a quick or immediate reconfiguration process is needed after a microgrid is islanded from the grid, real time detection of faulted areas is essential both for the MG and the distribution network stability [103].

With only few deployed efforts in this area, real-time experimentation still has plenty of potentials to offer. Real time testing could be used in different configurations serving various objectives as explained in the next section.

3.2 Real-time simulation categories

RT simulation types can be classified as depicted in Figure.8. The adopted classification here focuses on the purposes of consulting real-time simulations in different steps of development and testing. It boils down to two main categories that either incorporate an external hardware or not. Most of the terms used in this paragraph can be found in different contexts that do not necessarily stipulate the implementation in a real-time environment notably the full software branch. This made it indispensable to provide categorization that prevents the overlapping of the introduced aspects.

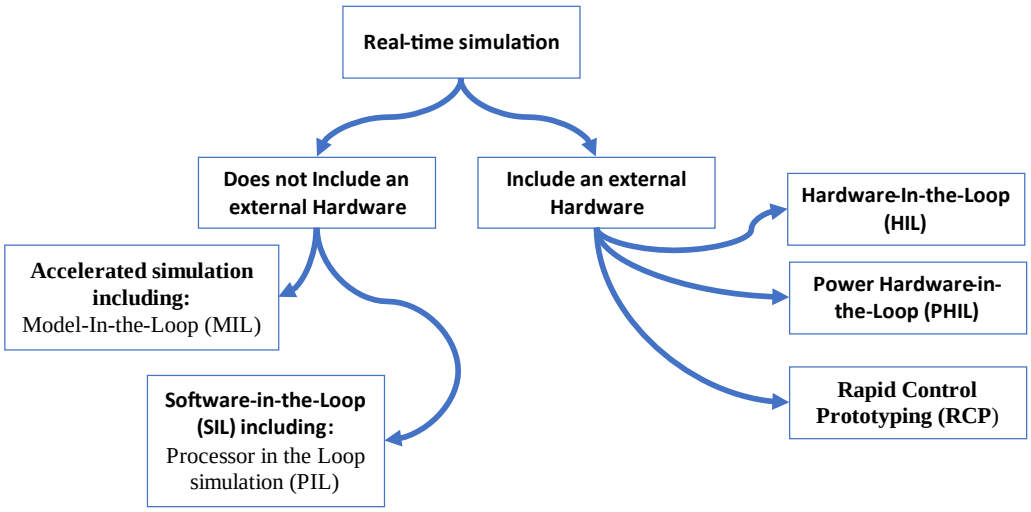


Figure.8 Real-Time simulation branches.

3.2.1 Full software simulation (no external connected hardware)

Even though the primary purpose of developing the concept of real-time simulation is to interface the simulated part with actual physical equipment, Real-time simulators can also operate offline to perform accelerated simulations or Software-in-the-Loop (SIL) testing.

3.2.1.1 Accelerated simulation (Model in the loop)

The importance of this simulation mode derives from the fact that significant improvements in processor technology throughout the last years were not enough to drag out the conventional performance of simulation from being a laborious exercise. Simulation on traditional CPUs/GPUs often involves a considerable waiting time for a few seconds of simulation. Simulation Acceleration makes the most of computational power to drastically cut down on the amount of time needed to process model results.

With a sufficiently powerful simulator, the controller and the installation (power part) can be run in real time in the same real-time environment.

This configuration is used to boost the conventional Model in the loop (MIL) simulation, which evaluates the algorithms in the simulation environment at the initial stages of the development cycle. It is usually very popular for verifying the controller logic validity on the simulated model of the plant.

Our laboratory simulator from OPAL-RT provides flexible Simulation Acceleration solutions, running on the latest generation of Intel Xeon simulators or a PC workstation.

3.2.1.2 Software-in-the-Loop (SIL) Fastest Production Source Code Validation

In the software-in-the-loop (SIL) simulation, the system model and the control are also studied in the same simulation environment. It stipulates of compiling the generated source code of the one of the subsystems (generally the control algorithm) and executing it as a separate process on the host computer or simulator. In other words, it represents the integration of compiled production source code into a mathematical model simulation.

When performed on the real time target (as in the case presented in this work) this category will naturally include the Processor in the Loop simulation (PIL) step that is found on model-based development and testing guide [104][105].

By doing so, the numerical equivalence of the intended model and the generated code can be tested simply through comparing the results of the normal and SIL simulation. Under this configuration, code coverage and execution-time metrics for the generated code could be accessed and gathered if necessary. It is usually used for the development and testing of detailed control strategies for large and complex systems.

Researchers usually resort to this method when the real-time simulator reaches its limits with certain systems, as it enables them to still benefit from the computation capacity of the real-time simulator, which generally found to be more powerful than regular computers.

SIL allow developers to test and modify their source code using their PCs directly and repeatedly by means of linking the software to a digital plant model that substitutes the highly expensive systems, prototypes, or test benches as set forth in Figure.9. This makes it possible to test software before initiating the hardware prototyping phase for earliest detection of system-level defects or bugs, which in turn considerably accelerates the development cycle and reduces the later stage troubleshooting time and costs prior to the expansion of the number and complexity of component interactions.

One can consider the absence of using the IOs as an advantage in preserving the signal integrity. Furthermore, as both the controller and the simulated model are running on the same simulator, synchronization with real time is no longer mandatory, it can be slower or faster than real time without impacting on the validity of the results, making this configuration ideal for accelerated simulation.

Overall, SIL comes as an excellent complementary tool to traditional HIL simulation, ensuring faster time-to-market and more effective software development.

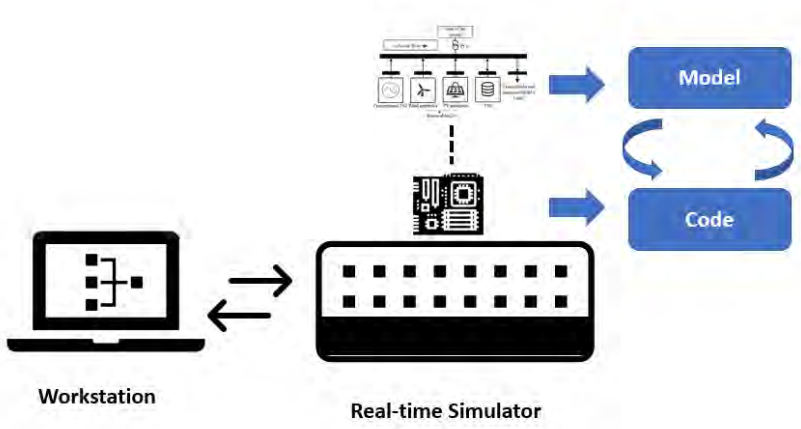


Figure.9 Simulation-In-the-Loop (SIL) configuration.

3.2.2 Including a hardware (the real-time target is connected to a hardware)

3.2.2.1 Hardware-In-the-Loop (HIL)

Hardware-In-the-Loop (HIL) simulation has become a standard for the development, testing and validation of the most complex control, protection and monitoring systems. It offers a great alternative to standard expensive testing methods, where the physical part of the tested system (physical plant) is replaced by a highly accurate simulation model executed on a real-time target that is able to accurately

reproduce the plant and its dynamics. This, in turn, makes it possible to communicate with real-world hardware such as controllers in the Controller-In-the-Loop Simulation (CIL), Intelligent Electronic Devices (IEDs), or any other intended equipment through the Input-Output (I/Os) interface as seen in Figure.10.

HIL's rise is the result of two major factors currently affecting product development across all industries: time-to-market and system complexity.

Researchers opt for this type of simulation when the physical test benches are not available, extremely expensive or as a final validation step prior to the real product testing. The attention at this phase is on identifying issues related to the communication channels and I/O interface, for example, attenuation and delay, which are introduced by an analogue channel and can make the controller unstable.

On the other hand, HIL also allow to expose the system limits that only appears under extreme testing conditions. By doing so, It helps avoiding potential damages when experiencing with CPSs in real hardware testing as suggested in [106].

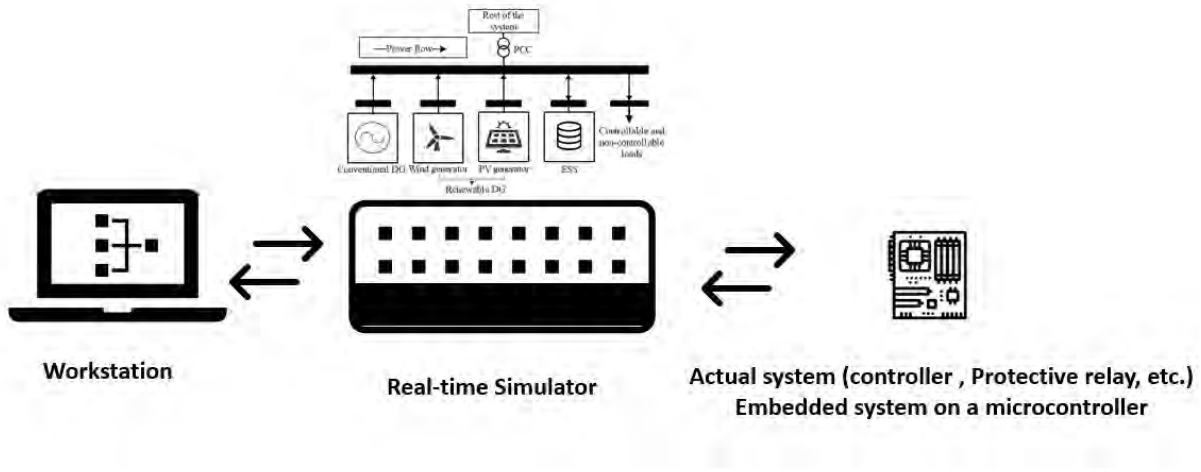


Figure.10 Hardware-In-the-Loop (HIL) configuration.

3.2.2.2 Power Hardware-in-the-Loop (PHIL)

This type of simulation can be considered as an extension of HIL, in which the power needed for the Devices Under Test (DUT) is provided also through the real-time simulation environment passing through a power amplifier (Figure.11). That, in turn, bridges the gap between DUTs rated for higher power and the low-level simulator I/Os. The selection of these amplifiers depends on the intended application, the matching closed-loop performance (as it is also important to properly close the loop by providing the necessary feedback) in addition to ability to generate and absorb power.

Engineers use this type of simulation to test systems that would not simply function only on low-voltage, low-current signals exchanged in the HIL simulation. This includes power converters, generators, PVs, motors and other loads. By doing that, they still have access to the advantages of high-fidelity simulation with greater flexibility and safety that outstands typical analogue.

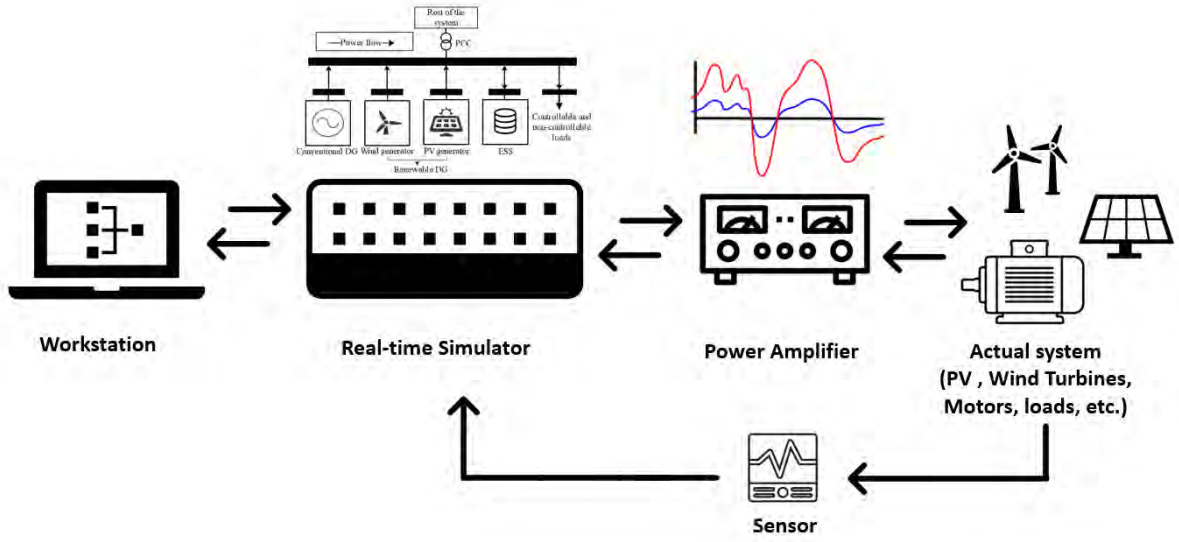


Figure.11 Power Hardware-in-the-Loop (PHIL) configuration.

3.2.2.3 Rapid Control Prototyping (RCP)

In rapid control prototyping applications (Figure.12), the controller model runs on the real-time simulator via the CPU cores while the real tested plant or the actual drive is connected physically to the real-time target with input/output (I/Os) interfaces.

It is basically used when developing control strategies as it gives the researchers the flexibility to refine the parameters and modify the implemented algorithms rapidly with a few mouse clicks.

With RCP, mathematical models are automatically imported from the design software on the host computer into a real-time simulator before being connected to real-world systems. Controller functionality can then be tuned avoiding all encountered errors and undesirable bugs to ensure smooth and rapid operation throughout the project. As a result, it reduces costly rework delays and improve overall product quality allowing the technology demonstrations earlier in the project stages, while avoiding the integration of complex coding.

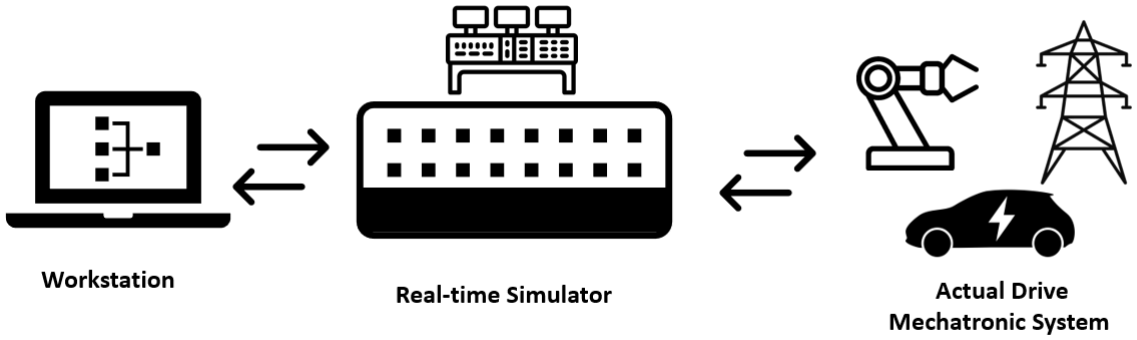


Figure.12 Rapid Control Prototyping (RCP) configuration.

3.3 Real-time and co-simulation challenges

3.3.1 Real-time timing constraints

The basic major challenges facing the real-time simulation especially in regard to the simulation of microgrids, and distribution systems can be summarized in two key points: The resolution level outlined by the selection of the solver sampling step and the difficulty of distributing large models over several processors/cores [103][107].

Models running on this mode of simulation adhere to a very small step size in order to achieve an accurate result. Bypassing the right step size to a larger value produces an erroneous simulation while smaller values do not fit into the simulator constraints. This, in turn, creates a challenge, especially with models with high-speed switching devices [75].

In Replicating the Electromagnetic Transient (EMT) behaviour of the complex power systems, the recommended step size is normally chosen in the range of 20-100 µs. However, with the connected power electronics required equally for the renewable generation resources and active loads, the switching frequency of convertors and the need to investigate harmonics frequencies would drag the step size toward smaller values as low as 1 µs or even below [108]. In this case, computing models with frequencies in range of (1to 100 kHz) will need to be achieved with the help of on a dedicated Field-Programmable Gate Array (FPGA) chips.

It is also possible for a circuit that contains both a ‘slow’ part (power grid), and a ‘fast’ part such as PV conversion system, drives, etc. to share the execution of these parts. Where the power grid runs on a multi-core processor at a typical 25-50 microseconds and the converters are simulated on the FPGA at a sub-microsecond step. The FPGA ,in this case, takes the responsibility of exchanging the data with the distribution network that runs on the CPUs through the simulator PCI express link [107].

On the other hand, handling a large number of switching devices in bulky model requires the computation of large matrices. While the real-time simulators' only way of solving these last ones within the finite simulation cycle is to divide the model and dispatch it to multiple cores [107]. The separation of the grid models on several processors is still a tricky task. This is mainly due to the inherent added delay resulting from communication and sending/ receiving overheads among the processing units [109]. This becomes even more challenging in the case of decoupling the distribution network into subsystems. Contrary to the propagation delay in the Bergeron-type line models adopted in the transmission lines which serves to split the model at different locations [110], the short lines (1-10 km) in the distribution systems do not tolerate the Bergeron's line-type logic for model decoupling. This implies the engaging of another decoupling mean such as adding artificial delays or a short transmission line with one-time-step delay typically referred to as stub-lines. As a consequence, a delay of one-step and an artificial capacitor will be added to the original system. Eventually, intensive deployment of these delay-based strategies of approximations can adversely affect the accuracy and numerical stability in a significant way [107].

State-Space-Nodal (SSN) solver developed by OPAL-RT Technologies propose a solution for this problem. Broadly, there are two main methods for solving the equations describing power grids, the state space and the nodal method. What the SNN algorithm does is that it creates virtual state-space partitions which is solved at the same time using a nodal method at the partition points of connection[109]. In addition, the SNN give the user the ability to choose where to place the nodes which permits the optimization of the needed number of nodes that will be later computed parallelly with the different processors with no added delays [107]. This method has enabled the real-time simulator from Opal to simulate large distribution networks with up to 750 single-phase nodes with the absence of any approximation delay.

3.3.2 Co-simulation complexity

Additional complications come to the surface concerning the representation of the cyber-physical components in the same computational environment. The inhomogeneous nature of both power and communication systems plus the obvious differences in components, transmission content, and working mechanisms make it very challenging to accommodate the desired realistic features in one frame. For instance, the time-varying or continuous solvers suit the power systems while communication networks' simulation necessitate a discrete or event-dependent simulation [111]. In other words, the behaviour of the grid control is mainly well defined using mathematical formulations, which is not exactly the case in the nearly stochastic, unpredictable data transmission protocol layer that belongs to the accompanying ICT system [112].

Even when ending up finding the perfect tool to simulate each structure separately, interfacing the two simulators in a way that guarantees the integration of the distinct characteristics for both, without restraining the core to either of each is not always evident and often stipulates grappling with synchronization and data exchange.

With all these obstacles, it seemed just right that some works had chosen to probe the different types of taxonomies of the existing testbeds since that discovering the various tools and techniques implemented in the current testbeds, counting also the strong and weak points for each one, is crucial to build and develop new experimental platforms.

In this context, the term “co-simulation” refers to the practical and realistic co-existence of the examined subsystems whereupon they operate hand by hand to reflect smart grid interactions [113].

The co-simulation development can take two directions; the first one primarily focuses on a specific tool that has been familiarly dealt with, in the course of studying individual subsystems. Researchers who seek this approach are usually more concerned in deepening their understanding of the interaction control between the intended subsystems. The second approach is a platform-based one, which implies fixing the attention on the development of a comprehensive framework with a standardized interface capable of embracing different tools. This attracts researchers who deal with utterly complicated simulation environments, especially when flexibility in connecting the subsystem is inevitably expected, without intervening in neither layouts [112].

At the end, no matter how much the method that relay on the physical representation of smart power system (of which microgrids are part of) is accurate, detailed or elaborated. There would still be aspects of these systems that would not be captured, reflect the real interactions, or even completely missed. This is practically due to the model simplification of each participating component and underlying layers.

Deciding on the approach to use for recreating or representing a system always depends on how much we know about the system. That is why white box approaches using first principles and physical modelling, is suitable to the situation when a full access of all essential features is guaranteed with an understanding of how these features contribute to its dynamic behaviour. Which is not nearly the case in the modern smart microgrids.

With the explosion of the amount of data and algorithms in machine learning, data science and regression techniques that uses applied math and statistics optimization, the discover (identify, characterize), control and modelling complex dynamical systems using data driven approaches are busting every door.

3.4 Anomaly detection using Machine Learning for cyber-physical security aspects

In this section, we review academic papers that address ML-based methods for detecting cyber-physical systems vulnerabilities. This genre of research is based on finding a tool that enables us to deeply characterize these complex systems in a way that allows us to put our hands on the undetected anomalies (cyber-attacks). The results devise a new hierarchical cascading conceptual framework for analysing the evolution of ML applications in this field. The presented structure also helps in underpinning the choice made in this research to work with Recurrent Neural Networks (RNNs).

3.4.1 Dynamic system identification using data driven models

Data-driven system identification is the process of using data instead of physics to develop a model of a dynamic system. In which we try to reproduce the system behaviour that mimics the essential features of the system in question concerning the observed problem dynamics leaving out every other unnecessary detail.

All data-driven methods start with a proper preparation of the needed data. The principle is to excite the system with input signals that generate the outputs in a way that assumes triggering all the essential dynamics of this system. These collected dualities of the input and the response output are then fitted to a model structure that has a good chance of representing the intended aspect of the given system and discover the relationship that governs the behaviour of the examined feature.

The used models could be based on the numerical estimation techniques, which is a counterpart to deriving models through first principles. However, it could eventually be a combination of both methods to afford more flexibility in picking some model parameters and the power to learn the others.

Machine learning (ML), on the other hand, exploits the gathered observation data from a given experiment on a system and automatically builds the models that predict or explain the behaviour of the system [114].

Largely based on statistical principles, ML algorithms outperform the standardized data-driven methods in performing predictions using fewer assumptions that result from understanding the underlying mechanisms. While both methods from statistics and ML may be consulted for creating Inference models and predictions in principle. It is known that statistical methods tend to focus more on inference utilizing a project-specific probability model, whereas ML uses general-purpose learning algorithms to find patterns in an often what seems to be a more rich and unwieldy data[115].

The influence of the physical model when deploying conventional ML techniques does not proceed beyond the data-generation stage. This goes for both cases where data are generated from the actual

physical model, or using a computer simulation based on the first principles to reproduce the physical process. The reason is that it will always be perceived by means of the ML techniques in a discrete form made out of data points and not equations [116].

The terms AI and ML are often used interchangeably even if they do not refer to the same thing. In this work, we refer to ML as an application of AI in general.

3.4.2 Detection and classification of anomalies on power systems using ML for cyber security purposes

ML had become a hot topic in the power engineering research world in the early 90s with clear promising avenues in applications such as power quality, security assessment, fault diagnosis, and load forecasting [117].

The complex nature of highly nonlinear systems in addition to the model uncertainties and external disturbances makes it intractable for traditional modelling techniques. On the other side, the plethora of the generated measurements accompanying the rise of the intelligent revolution in the modern grid has opened the possibility for data-driven system identification techniques to understand, model and predict the dynamics of these systems without the need for a full visibility of the governing principles beneath it.

However, the progress of these applications through time was not as significant as what other communities have witnessed. Research areas such as computer vision and mathematical programming, for example, have been making remarkable breakthroughs on both the theoretical and practical levels.

The main explanation for this lies in the very same reason that makes these techniques attractive in the first place. Being a black box, raise numerous concerns in the power industry on the need and the cost of replacing already existing solutions with ML based ones. Notably for critical assignment when the risk associated with a task is catastrophic, such as avoiding blackouts or finding optimal operating points without violating line limits [116].

Nevertheless, with the shortfall of conventional decision-making mechanisms to keep up with the real-time grid operational requirements under the ongoing shift to smarter grids, Al based methods are finding their own place in the new configuration due to their ability to be easily adapted to their environments and high-speed computing which make them more suitable to online applications [97] [116]. The ability of ML algorithms to process thousands of scenarios at the same time comparing to conventional tools that only can assess a limited number, makes it very feasible for rapid security assessment [116]. Correspondingly, applications such as neural network can be much more effective avoiding neglected or overlooked indications of critical incidents.

In fact, practices of low-risk nature such as predictive maintenance for transmission lines and transformers or smart scheduling for charging and discharging patterns of the vehicle to grid are already penetrating the market. Which highlight the fact that ML based tools are only acceptable in the first phase of power systems transition as decision-support tools that assists or enhance the performance of established procedures leaving final decision in the hands of operators [116].

Anomaly detection, classification and localization in complex CPPSs is another promising utilization of data driven artificial intelligence methods. Especially in the absence of any existing approaches that are able to address unconventional anomalies in the case of cybernetic-induced faults. In addition to the existing evidence where data driven deep learning algorithms were able to spot unusual activities that normally go undetected with conventional bad data detection [118][119].

Over the last years, this direction has been getting very popular which has led to a wide exploration in the literature.

Binary classification that classes the measurements of the electrical systems as sane (secure) or infected (attacked) data within its two sub-genres those being supervised, and unsupervised learning were heavily employed in detecting cyber intrusions.

The ambiguity that comes along with the characterization of cyber-physical attacks in the power system, the low number of reported attack cases and the unwillingness of operators to share sensitive data that details previous incidents, result in a lack of open-source information. This eliminates the access of the needed material upon which machines can learn to identify attacks in supervised methods.

That's why researchers such in [120] and [121] tend to design aspects of the attack that they want to detect. This enables them to simulate scenarios where they introduce the attack, collect its effect on the systems in the form of labelled data base and perform supervised or semi-supervised approaches.

Multi class classification was also deployed. Statistical features extracted from time-series for voltage and current are used in [121] for developing an intelligent anomaly identification technique based on Multi-Class Support Vector Machines (MSVM). The method was tested and validated under cyber anomalies induced by attacks such as False Data Injection (FDI), Denial of Service (DoS) in addition to the presence of power system faults.

Outside the scope of attacks supervised learning could be applied to perform security assessment in the sense of evaluating the system stability after the occurrence of a disturbance [122].

3.4.2.1 Regression models

On the other hand, deviations between the estimated and the observed state was one of the priorly adopted techniques to encounter data manipulation inducted by False Data Injection attacks (FDI) in the power systems [123][85][124]. Starting with static state estimation [125], to more recent and adjusted

forms of dynamic estimators [31], a proper estimation always entails an adequate description of systems dynamics.

Broadly, ML-based models that estimate system's future states or desired parameters are very useful in surveillance control and operation optimization in industrial systems in particular. These models gained a special interest in the case of renewable generation production forecasting owing to the role of its implications in power balance effectiveness and stability [126][127][128].

ML algorithms that perform regression almost employ more or less the same training process found in the classification task. Although, the output is presented differently. Instead of a "yes" or "no" response in the classification networks. A continuous function value is yielded in the regression mode. This provides another way of determining whether the system functions as it should or not, through estimating how a certain supervised feature should vary based on an accurate modelling of the dynamics that directly produce or contributes to the predicted feature.

When time is the main factor that we trace the system behaviour in relationship to, sequential analysis could be quite beneficial.

Time series regression or forecasting determines the dependencies and trends found in the time series data and estimates the future steps accordingly [129][130].

In the case of microgrid diagnosis using ML, one must keep in mind that understanding the behaviour of such an entity that does not have a generalizable structure must not demand very dedicated efforts. Learning how different components of the highly customisable MGs could be done in an extremely sophisticated manner those results in a very specific approach designed to fit each unique system. This may include learning patterns and classes that do not necessarily exist in other MGs. There is no doubt that using ML techniques implies learning from a specific case, and while the result (the trained algorithm) cannot be replicated for multiple MGs the adopted approach on which we decide which feature to be learned should be reproducible expecting a relatively similar outcome.

With only a limited amount of resources to be attributed to accomplish the task of identifying any deviations from the normal functioning behaviour, time series regression can hold a very intuitive visual representation of the indicated problem. In addition to arguments that sequential ensemble learning based detection offers the most stable detection performance [131].

3.4.2.2 Recurrent neural networks

Artificial Neural networks (ANNs) belong to the most promising group of ML tools, due to their ability to extract nonlinear features or relationships and to approximate any function (universal approximation) [132]. They adopt expressive architectures that learn, store and retrieve information through passing

batches of data several times from arbitrary input-output data [133]. Its iterative optimization algorithms imitate the way that human brains perceive and trace the connections between variables [134][116].

Recurrent Neural Networks (RNNs) in general have a good reputation for dealing with problems that include signals varying in time due to its advanced capability of learning complex temporal sequence. That is why RNNs have been very popular in many tasks such as audio signals in text generation and speech recognition [135].

As the name may suggest, RNNs are not just feed-forward networks as the case of most common Convolutional Neural Networks (CNNs) used in image processing, for example, which are governed by a static IO relationship. The output in RNNs is calculated with the aid of both inputs and outputs historical value by dint of feedback flows across the neuron itself or even between the network underlying layers [136].

Due to the inclusion of feedback loops that improves its learning capability, RNNs excel other types of neural networks when it comes to time series prediction [137]. That is what makes them suitable for studying phenomena pertaining to electrical signals in the time domain.

In this work, we have selected 2 models of the RNNs world: the Nonlinear Auto-Regressive Exogenous (NARX) and the Long-Short Term Memory (LSTM). Both networks have been successfully explored in anomaly detection applications, and more importantly, both had a good performance in real time applications.

NARX model has been used in real-time simulation and eventually Hardware-In-the-Loop framework in [138] for their high accuracy and short execution time. That is why they have been quite popular in renewable forecasting applications [127][139][140][141].

In [142] an LSTM based fluctuation identification tool was also operated in real-time to provide an enhanced control reference for the load frequency control after being trained in an offline mode to distinguish the real-time power fluctuations based on the measured frequency.

Detecting attacks in real-time commonly encompasses an offline training phase where the pre-processing of the historical sensor data take place. Which in turn is followed by using the trained model in the online mode that receives the new data with multivariate data streams [112] [120].

An real-time attack detection mechanism for DC microgrids using NARX network has been developed in [89]. The network is first trained and fine-tuned to estimate the output DC voltages and currents of MG units, which helped to determine the existence of cyber-attacks such as FDI attacks by calculating the estimation error.

Based on the deviation of the predicted normal behaviour of the substation, the anomaly detection approach adopted in [19] determines whether a new reading of the management information bases MIB

object is attacked through the GOOSE messages or not. Using a two-step deep learning framework that includes LSTM, RNN, and GRU combined with an auto-encoder and enhanced by the ensemble learning model.

Cyber intrusion was investigated in another critical cyber-physical system such as water treatment plants or distribution systems, Time-series anomaly detection was also a success. LSTM-RNN was employed by [135] as a predictor to model the normal behaviour and detect intrusions using the cumulative sum (CUSUM) method to identify anomalies. In a similar way, authors in [143] and [144] has used NARX network to design an early-alarm system that recognizes patterns corresponding to abnormal working conditions producing unexpected states in the system.

3.5 Hypothesis

In this work, we present the deployment of system identification using machine learning as an approach to detect the cyber intrusion on the level of active power sharing in AC connected microgrid based on the following assumptions:

- Attacks are considered as an unobservable error (fault or errors caused by unknown system nonlinearities).
- The adoption of real time simulation concept is based on two propositions:
    a. The real-time execution of a system helps to approximate the model of the real functioning of the studied system (the microgrid). This in turn will help us prepare the needed database that describes the system dynamics which will be used later to train the adopted ANN.
    b. Selected Ml based detection methods is assumed to comply with the real time constrains in terms of computational resources needed to deliver the desired output. This in turn permits to explore the limitation of these tools in the context of attack detection in a faster and more practical way.
- The importance of the time factor in choosing the ANN type and the compatibility of time series sequences neural networks with the problem of attack detection in the time domain. This is based on fragments of discussions presented in the relevant studies addressing criteria of adopting Ml techniques energy systems reliability assessment and control, and they are;
    a) The designed approach should remain as simple as possible without compromising the robustness of the operation.
    b) The output of the detection algorithm should be of high interpretability, as it is meant to help human experts to understand the main features of the problem at hand.
- Modern smart microgrids follow very complicated modes of functioning. These modalities are usually customized based on one of the following prerequisites:
    a) Either set on the customer's preferences in the residential types.

b) Or to inject all the produced energy directly in the grid in the cases of advantageous purchasing prices
c) Or even to prioritize self-consumption in the cases where local policies provide subsidies concerning the capital cost of renewable generation without necessarily having a competitive purchasing tariff.
d) Or in the most complex scenario to change as a function of the electricity dynamic pricing.

- Attacks targeting energy management systems are scantly addressed in the literatures, and analysing the power and sharing dynamics in the scope of attacks has been never evoked to the best of the authors' knowledge.
- Adopting attack detection on the level of microgrids is of an extreme importance. In view of the immense technological trends that advent the distribution network through the concept of local private networks or microgrids. It is a way to combine micro and macro concerns in the same frame. It allows to address the malicious intrusions in way that reflects on socio-economic analysis while remaining feasible and socially accepted.

Chapter 4: Methodology Testbed Description

In this chapter, we dive into the technical specification of the adopted platform (designed workstation). The remainder is organized as follows: First, the adopted methodology is presented with a brief reflection on the incentives behind the choice of the proposed reasoning. Next, the contributions of this work were highlighted in a separate section. In the following segments, the simulation model of the AC-connected microgrid is detailed, followed by a descriptive introduction of the selected ANN type (The NARX) with the governing equations. Afterwards, attack modelling for both addressed scenarios (cybernetic-induced attacks and physical attacks) was laid out describing how vulnerabilities can be exploited to create undesirable situations. Several realistic case studies that represent commonly known attacks were developed and tested in a real-time environment, side by side with experiment results that affirm the effectiveness of the used strategy. Finally, we conclude this chapter with a discussion on the method's attributes, possible research tracks and reencountered constraints.

4.1 Methodology

The rising expectations for system safety have drawn the attention towards online fault detection in the world of automation. Active power estimation is necessary for frequency control at the distribution level and Load Frequency Control (LFC). The increased complexity in distribution level due to the lack of inertia resulting from the integration of a greater share of renewable production, and the non-observability droved by the heavy deployment of controllable storage and loads in addition to the market-driven dynamics, has made the work on power balancing severely demanding [145] [142]. Traditional LFC will soon be unable to adapt to these challenges without even broaching the scope of this research, which covers maliciously introduced faults and errors (cyber-physical attacks).

As mentioned earlier when building the hypothesis of this thesis, the more locally based a given solution starts to diagnose disturbances and errors in the complex CPPs, the more effective it is.

This work deploys the AutoRegressive eXogenous Neural Network (NARX) model as an Intelligent Detection System (IDS), to detect cyber-physical anomalies in the behaviour of exchanged active power in a connected AC microgrid configuration (see Figure.13).

The exploited NARX estimates the active power that enters or leaves the microgrid at the Point of Common Coupling (PCC) through estimating the convening battery dynamic behaviour. Similar to the methodology proposed in [89], we are using the NARX model for detecting cyber-attacks by estimating the normal behaviour of one of the components in reference to the other components. Based on these

predictions, we then calculate the difference between the estimated outputs denoting the theoretical sensor value under normal conditions and the actual sensor data.

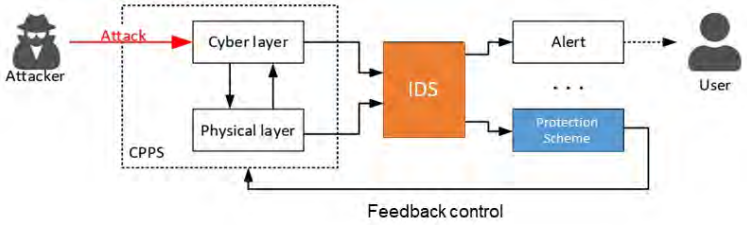


Figure.13 Intelligent Detection System (IDS) for Cyber-physical Security.

A series of experimental assessments took place before deciding on the right component or the correct function to predict. In conclusion, results have prioritized working with the active power level based on various grounds. First, it is more informative and could clearly reflect the occurring events and variations of the whole microgrid, forming a suitable instrument for system monitoring. Furthermore, power consumption in electronic based systems is an essential feature for the management of energy autonomy, performance analysis, and the ageing monitoring of components [146]. Additionally, it is also because that we think that microgrids are largely equipped with voltage and current regulators that could detect the source of anticipated deficiencies and deal with it either by tackling the spotted problem or completely disconnecting the malfunctioning unit.

More importantly, integrating a battery storage system within the microgrid configuration, especially the residential type, generates an unpredictable influence of the adjustable battery control system. This could reach a limit where studies such as [147] propose the implementation of a rechargeable battery as a potential countermeasure to the privacy leakage problem in smart grids. These batteries can be used as a relay to store the electrical energy before reporting the energy usage rates to help prevent the exposure of the consumption signature of each home appliance.

The model uses a time-series database collected from a simulation model presented later in (section 4.3) to learn the normal behaviour of the system concerning the relationship between the different units. This includes model limits, self-consumption behaviour, load sharing, battery charging program and the system set of priorities. For example, in reference to other units functioning it could indicate when it is normal to charge the electric vehicle or to start a diesel unit in systems that include it. Hence, it can clearly indicate the occurrence of unplanned events.

In an ideal scenario, any identified variation will indicate anomalies of some sort. Nevertheless, in reality, the model estimation accuracy is limited, and transient events could cause temporary fluctuations. Deriving from the fact that the NARX training was carried out completely using an ordinary functioning dataset (without attacks), a remarkable visible divergence between the network output and the target

indicates a constant inconsistency with normal behaviour which cannot be attributed to an arbitrary incident [143].

For extreme simple flows, of which the architecture of a microgrid encompasses only one type of production or consumption means. Reading the parameters at the PCC could be done in an intuitive way. However, with customizable Energy Management Systems (EMSs) and more complex configurations including a variety of different heterogeneous DG units connected in all sorts of commercial schemes propositions, and which at some point of its life cycle may be expanded or edited by adding or replacing other resources or loads changing the originally adopted structure in an unideal fashion. These cases are hard to diagnose, and operators most likely will not tell when the system is operating properly or experiencing unanticipated scenarios.

Detecting attacks by comparison covered the malicious transmission of information in studied such as [14] to detect energy theft cyberattacks with the help of inserting Feeder Remote Terminal Units (FRTUs) that compares the measurements from smart meters with the measurements of energy flow taken from the distribution sub-network.

These units are still relatively expensive which led others to design techniques to optimize their numbers in a way that does not deteriorate the performance in [148]. Most importantly, these types of detectors would not detect an intentional physical manipulation of the battery systems that would change the actual flow of power rather than just transmitted signals.

Furthermore, most of the papers that probed the world of attack using ML algorithms have been realised in DC power systems/microgrids [149][150] [151][152]. Contrasting with the fact that real-world utilities still favour AC power system models over DCs. This assumption is quite misleading in the sense that it neglects the level of complexity and sophistication needed for bad-data detection in AC systems [153].

4.2 Contributions:

The previous discussion highlights the originality of our approach compared to the literature, and the following key points outline the main contributions:

- It provides a large and multi-disciplinary exploration of the state of the art, which has resulted in a non-bias research direction that draws attention towards the emerging risks in the progressively increasing adoption of microgrid structure.
- It clearly identifies potential attack surfaces and probes the active power management and the role of battery, which have not been addressed in the context of Cyber-physical security to the best of the authors knowledge.

- It investigates attacks in the AC environment in contrary to most of the established work in the microgrid domain.
- It elaborates on attack modelling and building a testbed that could represent physical and cyber intrusions.
- It designs a detection mechanism based on artificial intelligence (artificial neural networks) that is capable to reproduce the studied microgrid dynamics and hence predict normal operation as a function of the system limits and variables.
- It tests the compatibility of the proposed network (NARX) to work on real-timeconstrains and validates results using Hardware-In-the Loop (HIL) simulation.
- It sets the limits of the NARX neural networks and conducts a performance comparison with Long Short-Term Memory (LSTM) neural networks.

4.3 The plant (Simulink model)

In order to validate the proposed methodology and generate the database needed for the tests, supposing that such data are mostly hard to get in the aspired accuracy, consistency and flexibility due to confidentiality demands.

We have selected an already built simulation prototype by the Snohomish County Public Utility District (Snohomish PUD) in Arlington, Washington State [154], which was intended to be carried into the field later in 2021. The model is created using the Simscape Power systems library from Matlab, and it is available online as an open-access Simulink file through the Mathworks platform. The model was already customized to be executed in the Real-time environment using the RT-lab software that supports transferring the simulation on Opal- RT simulator.

The model contains all essential elements found in a typical microgrid, i.e., Photovoltaic (PV), Battery storage system, connected load, Vehicle to grid unit in addition to an emergency generation that has been withdrawn in the connected mode.

The project file contains three cases in which the microgrid's configuration changes between the case (A) that correspond to a Grid-connected operation phase with a slight fluctuation in the renewable generation profile, load, and Battery control program. The case (B) where the battery switches to the grid-forming mode as the microgrid steps to the islanded mode after 10 seconds of the simulation time determined at 98 seconds, and the last one case (C) where the emergency generator starts compensating the power in the islanded mode once the battery gets discharged simultaneously with an insufficient PV production.

The microgrid components in the case A are illustrated in (Figure.14) It also offers the possibility to change PV generation, load and battery control system using different scenario profiles, which helped us creating the dataset used in the offline training of our artificial neural network.

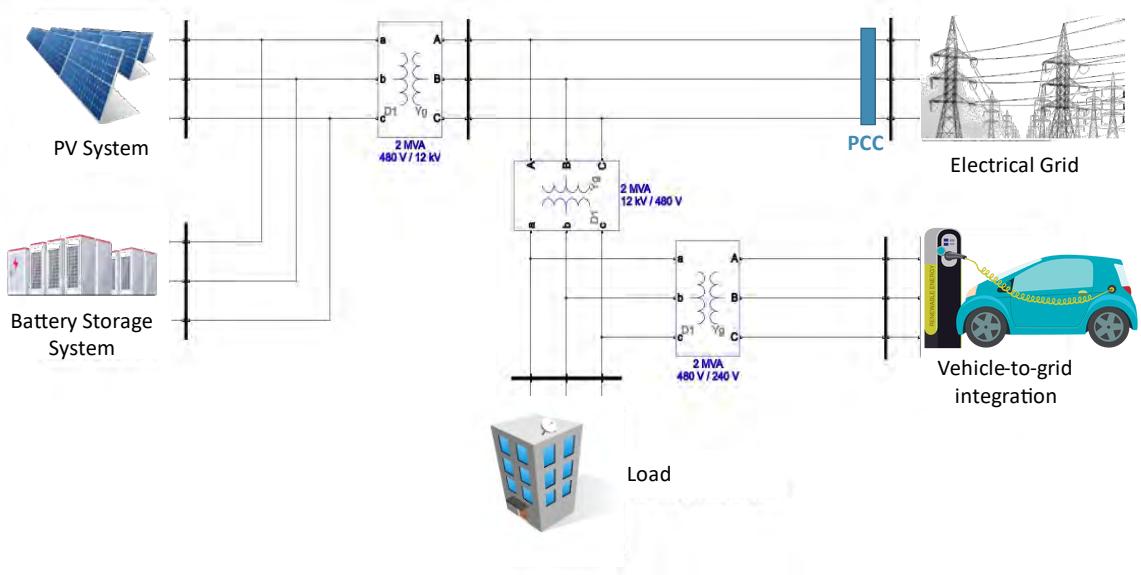


Figure.14 The used microgrid components: Case (A).

In this work, we have decided to choose the case (A) as a starting point to conduct the tests for several reasons. First, we believe that the paradigm of the connected microgrid is the most common and promising choice in recent applications where the completely islanded mode is unfavourable by the energy companies at this stage and comes only as a redundant security extra in the hypothetical cases of widespread blackouts. Second of all, the fear of triggering a cascading failure generated by the violated AC microgrid occupies the biggest part of power operators concerns since it still communicates with the grid on both the physical and cyber levels. Finally, solving the problem for a connected microgrid is based on the same hypothesis of using the completely isolated types. Therefore, if we end up finding a form of artificial intelligence that could understand and interpret the normal functioning of connected microgrid, replicating the process towards other types of microgrids would not involve but minor adjustments in the overall application of this methodology.

Keeping in mind that, ideally, a perfect attack detector mechanism should be able to work also for microgrids that transition between connected and disconnected operations. Which is a scenario that is envisaged in the future proceedings of this research.

The renewable generation in this model is represented by a set of PV arrays with a total rated capacity of 615 kWp DC. Each array is equipped with Maximum Power Point Tracker (MPPT) and an inverter. Every array comprises a number of PV modules (1640) of the type (REC TWINPEAK 2S MONO 72 SERIES 375 Wp) split into 4 sub-arrays. Table.1 presents the full specification of these modules.

Parameters	Values
Maximum Power	375 Wp
Open Circuit voltage (Voc)	48 V
Rated Voltage (Vr)	40.1 V
Short circuit current (Isc)	9.96 A
Rated current (Ir) 9.36 A	9.36 A
Temperature coefficient of Voc	-0.28%/C
Temperature coefficient of Isc	0.04%/C
Number of cells per module 144	144

Table.1 specification of PV modules.

These PV modules are connected in both series and parallel combinations to achieve the desired voltage and current (Figure.15) shows the (current-voltage) and (power-voltage) graphs that describes the sub-array characteristics for different solar irradiation and temperature values.

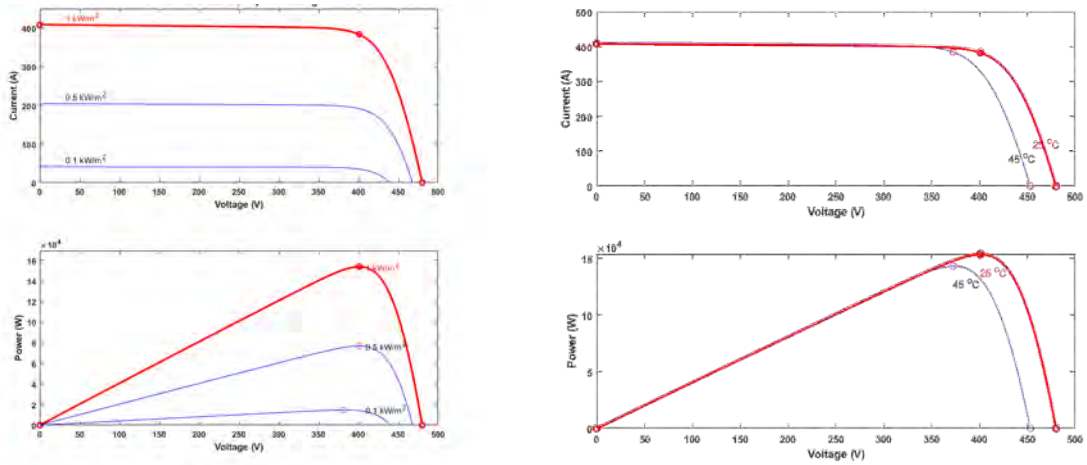


Figure.15 PV sub-array (I_V) and (P_V) for solar irradiances (0.1 kW/m^2,0.5 kW/m^2, 1 kW/m^2) and temperatures (25°C, 45°C).

The MPPT tries to keep the voltage at the maximum power point with changing solar irradiation and temperature with the help of a two-stage topology DC-DC converter that uses the perturb and observe algorithm. This explains the differences in the voltage values measured on the output of the PV array and the output of the DC link.

Regarding the used inverter, the model deploys a two-level three-bridge Voltage Source Converter (VSC) set to operate on a grid-following mode. A Phase-Locked-Loop (PLL) and a measurements block transform the reference frame by calculating the angle synchronized on the rising zero-crossing of the fundamental received reference voltage and current signals from the output of the inverter as summarized in Figure.16.

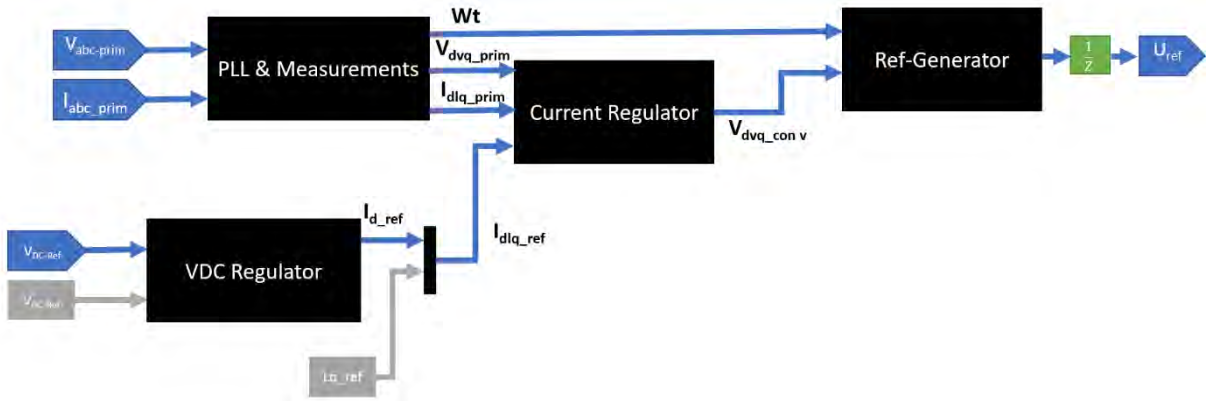


Figure.16 Control algorithm of the PV inverter.

The mismatch between the power obtained from the array and the power delivered to the grid makes the voltage regulator function changes the active power reference current (Id) that comes from the current regulator. This continues until the power values on both sides are matched [155].

On its turn, the current regulator calculates the inverter's voltage reference using Id and the reactive current reference (Iq) which is set to zero in this model. This means that the microgrid does not inject reactive power into the grid and it only supplies it with active power. A single inductor (L) filter is used to eliminate the resulting harmonics caused by the inverter [156].

The second component of the microgrid is the energy storage system. It includes a Li-ion battery, a bi-directional DC-DC converter that controls the battery charge and discharge rates and an inverter that is able to switch between grid-forming and grid-following modes. The battery inverter performs a similar control method for a grid-connected mode, while it operates as a voltage regulator in islanded mode. The full specification of the battery is given in Table.2.

The vehicle-to-grid (EV) integration on the other hand is modelled using also a battery model and an average model of an DC-AC inverter to regulate the bidirectional flow rates of charging and discharging [157][158]. Table.3 provides the technical description of the EV battery.

Simulation time is set to be 100 seconds for each iteration. During this period, the model in the default scenario experiences the following operation phases:

In the first 60 seconds, the battery compensates the degradation in the PV production and then continue to charge and discharge independently. Variation of the active load happens between t = 50 seconds to t = 90. While the EV model chargers for the first 40 seconds, discharges in the next 40 and then gets disconnected for the rest of the experiment.

Parameters	Values
Nominal voltage	800 V
Rated capacity	1250 Ah
Fully charged voltage	931.2V
Maximum capacity	1320 Ah
Capacity at the nominal voltage	1250 Ah
Nominal discharge current	1250 A
Exponential zone voltage	860 V
Exponential zone capacity	60 Ah
Internal resistance	0.0064

Table.2 Battery specification.

Parameters	Values
Nominal voltage	200 V
Rated capacity	500 Ah
Fully charged voltage	232.8 V
Maximum capacity	500 Ah
Capacity at the nominal voltage	452.2 Ah
Nominal discharge current	217.4 A
Exponential zone voltage	216.1 V
Exponential zone capacity	24.6 Ah
Internal resistance	0.004

Table.3 EV specification.

Modification on the functioning of the case (A) model has also been carried out on our part with the objective of constructing an operating mode as close as it could be to reality. Considering that in the default case above, variations in active power levels in all units are only a function of time. In other words, there is no interdependency or correlation between the different units, except the part where the battery acts in solar smoothing mode. Randomness is typically normal in the case of Load value (L), PV production output (PV) and Electric Vehicle behaviour (EV) which are considered as unpredictable or uncontrollable units. Of course, there exist cases where some of these variables depend on other factors such as dynamic pricing, weather, and patterns of prosumer habits. These mechanisms necessitate severely elaborated models which are, at the same time, not mature enough or even underspecified in real-world standards, and hence there are out of the scope of this research. On the other hand, battery storage systems are usually deployed to boost the economic efficiency of the microgrid based on different factors. The power output of the Battery (B) primarily takes into account available production-consumption capacities and acts in favour of a self-consumption behaviour in most cases.

Thus, changes were made in the control system of the battery to correspond to a self-consumption scenario. In case (B) here, compensate any degradation in the PV output also covering the increase in the consumption to assure that the microgrid output is stable on 500 kw injected in the grid. The battery in this case only charges when the available overall power exceeds 500 kw.

Various scenarios were applied using different irradiation profiles, consumption demands and electric vehicle charging-discharging routines. Resulting time-series sequences were gathered and stored in .mat file using a 5ms sampling time.

4.4 The Neural Network model (NARX)

Selecting the right type of neural network that suits the nature of the implicated system and provides a better correspondence to the input/output (IO) relationship, is a fundamental step to begin with [89].

Recurrent Neural networks RNNs were widely exploited in time series analysis and sequential fitting. Due to their ability to take into account the variables' lagged values using feedback flows between its layers and neurons.

NARX model is a variant of RNNs that is considered an important class that - unlike other time-series methods- has proven to be effective in discrete-time nonlinear and non-stationary modelling [159]. Despite the limited feedback which comes only from the output neuron rather than from hidden states, NARX can replace conventional RNNs without any computational loss [160]. Moreover, with the additional inputs, it could overcome the traditional recurrent networks in important criteria such as speed of convergence, better generalization, precision, and overall performance [161].

Besides, NARX structure is also considered user-friendly given the fact that its relatively simpler and provide easily comprehensible application [140]. However, since the training in this work is done offline, the speed of convergence is not relevant, as it does not influence the network performance.

According to [162], the NARX models does enjoy a certain Input-to-State Stability (ISS) and Incremental Input-to-State Stability (δISS) with a limited perceived performance degradation in comparison with more complex neural networks.

A three-input one-output NARX model was employed in this work. with a setup of one hidden layer comprising 10 neurons and 2-time delays. The configuration of the constructed NARX is illustrated in Figure.17 and Figure.18 The mathematical input-output representation is governed by the equation (1) below:

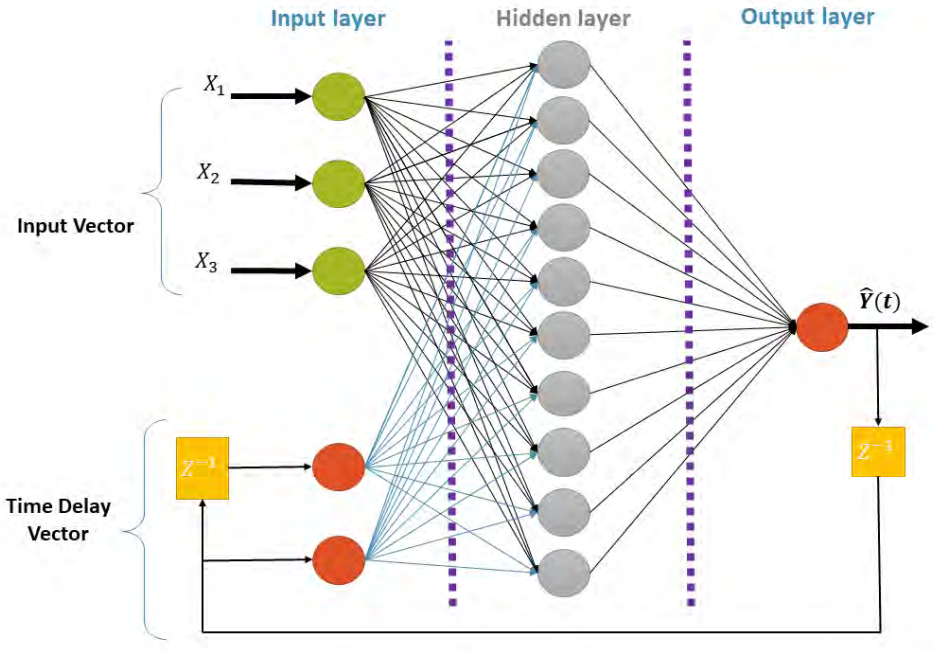


Figure.17 General structure of the used NARX.

$$Y(t) = f(x(t-1), \dots, x(t-d), y(t-1), \dots, y(t-d)) \quad (1)$$

Where $Y(t), x(t), f(), d$ denotes the output, the input, the nonlinear regression function that defines the IO relationship and time delay respectively. The next value of the $Y(t)$ dependent output signal is regressed on previous values of the output signal and previous values of an independent (exogenous) input signal.

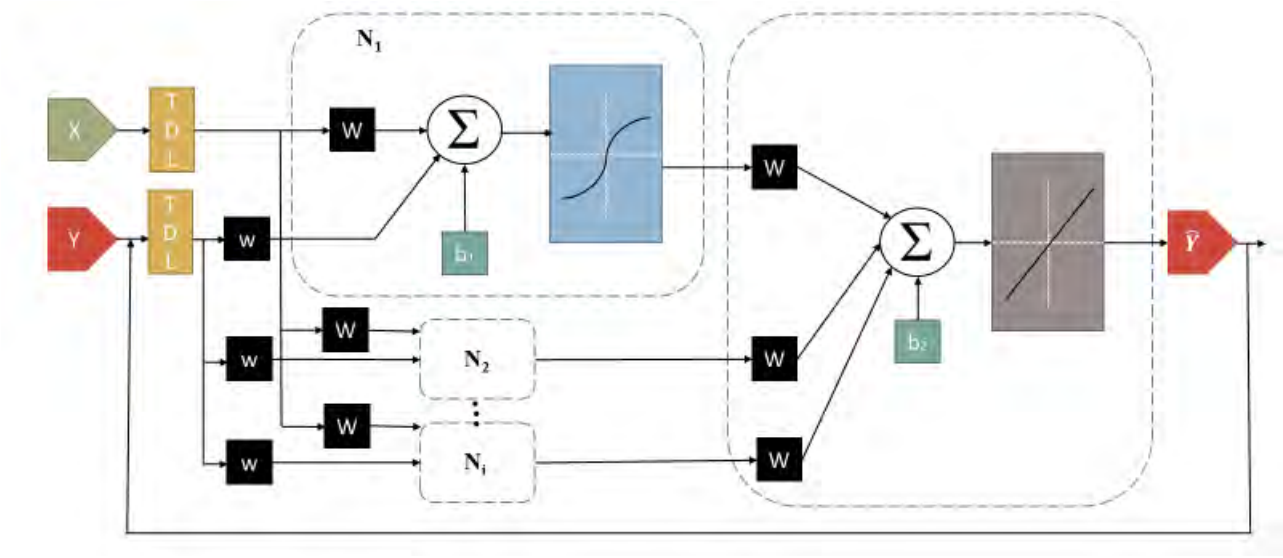


Figure.18 Detailed cross-section structure of the used NARX.

The hyperparameter tuning of the ANN, which usually includes setting the number of the hidden layers and the number of neurons within each layer for trying to obtain a superior performance has been performed through a series of experiments and tests in this study. Accordingly, and as in all studies that use the applications of this emerging field, the resulting setup of hyperparameters is not generalizable and highly dependent on the properties of the used database [163].

The next chart (Figure.19) schematizes the process of obtaining the best-trained network and puts forward the workflow step-by-step.

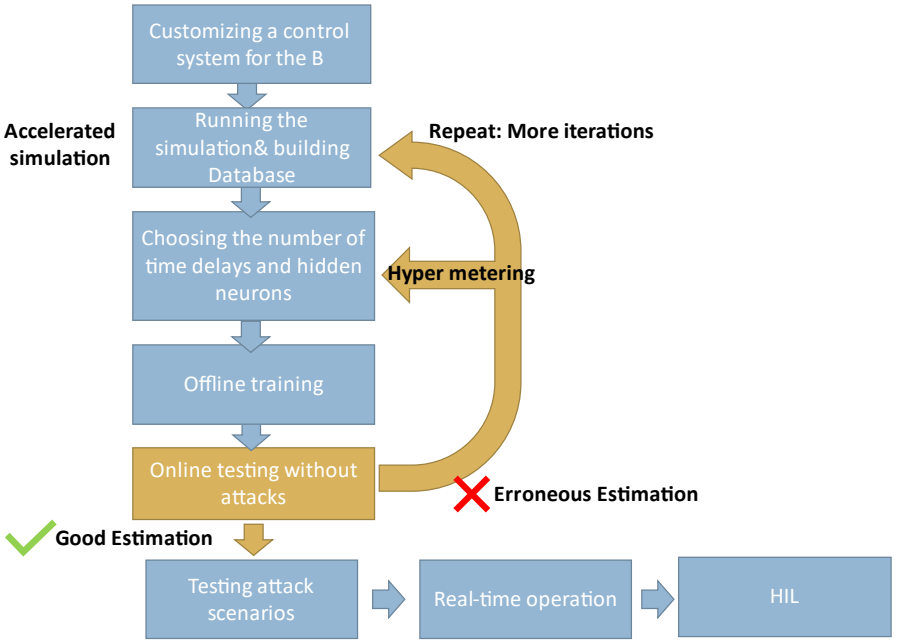


Figure.19 Work flowchart.

4.4.1 The training phase:

As mentioned before, the access to real data that captures the parameters of the required system was out of reach as is the case in most research [164]. However, the alternative was to create the required data by using the possible profile input option for several units in the model, like the ability to change the solar irradiation for the PV system, load and electric vehicle profiles.

We might even argue also that it is even better to use artificially generated data for the training phase to make sure that we have included all the possible scenarios in an optimized way since that the time that separates events is not a criterion here.

Since we are working on the active power level, conducted events do not require high precision sampling. We found that deployed simulation sampling time (ts=50e-6) which is usually consulted when investigating events such as harmonics, is exaggerated. Hence, we decided to downward it in the training phase to (ts=50e-4) with a decimation factor of 100. This downsampling was proved not to have any effects on the representation of the signals used in the training. It would rather lessen the time needed to train the network over a larger number of samples with the exact amount of information.

Knowing that once the training phase is done, the NARX could successfully operate online using a shorter sampling time, which has been demonstrated in the real-time testing of this method.

The training database is divided randomly at a percentage of 70% for the training phase and 15% for each of the validation and testing steps, and results are carried out using the Levenberg-Marquardt

algorithm. Notwithstanding the numerous trials to determine the optimum values of the aforementioned choices, it had not happened to witness any significant enhancement in the training results.

The offline training and the creation of Simulink block are done automatically using the MATLAB application toolbox. This has facilitated the implementation of the NARX in the Simulink environment for prior testing and validation of the method. Given the fact that an access to the real measured values during the training operation was imperative. A Series-Parallel (SP) mode or open-loop (single-step) form, illustrated in Figure.20, was a better fit in the training phase while a Parallel mode in the operation phase was needed in this practice.

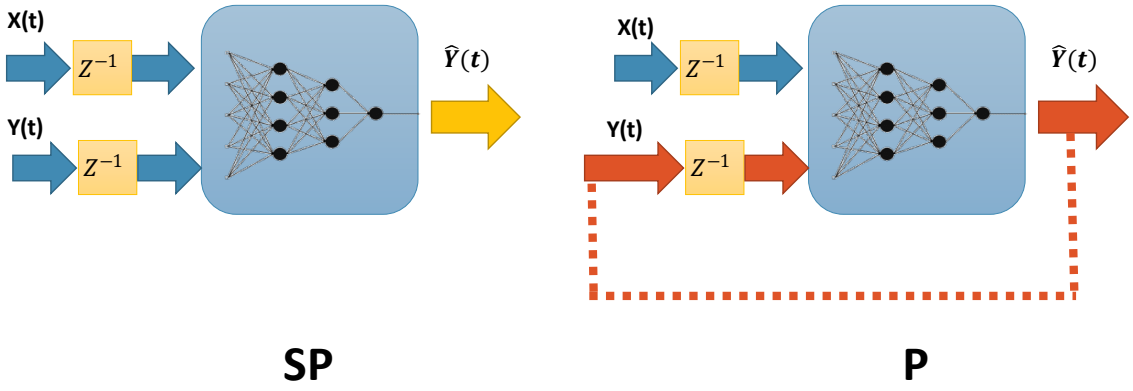


Figure.20 Series-Parallel (SP) and Parallel (P) modes of NARX.

This is due to the fact that feeding the NARX the true values of the power-sharing curve between the microgrid and the main grid during the online phase will affect or cover the estimated dynamics that are being reproduced using only the communicated values of the different components of the microgrid. Given that, the main purpose of the NARX to recreate how the system should exchange active power based on the communicated measures of the instantaneous and historical values of production and consumption of the MG components. All along while keeping the ground truth value of the measured active power at the PCC isolated for further use as a reference to detect the presence of incoherent behaviour.

We started by preparing the input-target matrices. For this stage, the input matrix X consists of the power values of all the microgrid components, while the target matrix Y contains the battery output power as illustrated in Figure.21.

Correspondingly, the estimated output of the NARX system could be written as follows:

$$B(t) = f(L(t-1), L(t-2), PV(t-1), PV(t-2), EV(t-1), EV(t-2), y(t-1), y(t-2)) \quad (2)$$

The next step was to run the simulation several times using different profiles and store the results into time-seriesMAT-files. The data contained in these files were then used to construct extended X, Y

matrices which, in turn, were fed to the NARX during the offline training phase in order to learn the relationship that governs the flow of active power between the units.

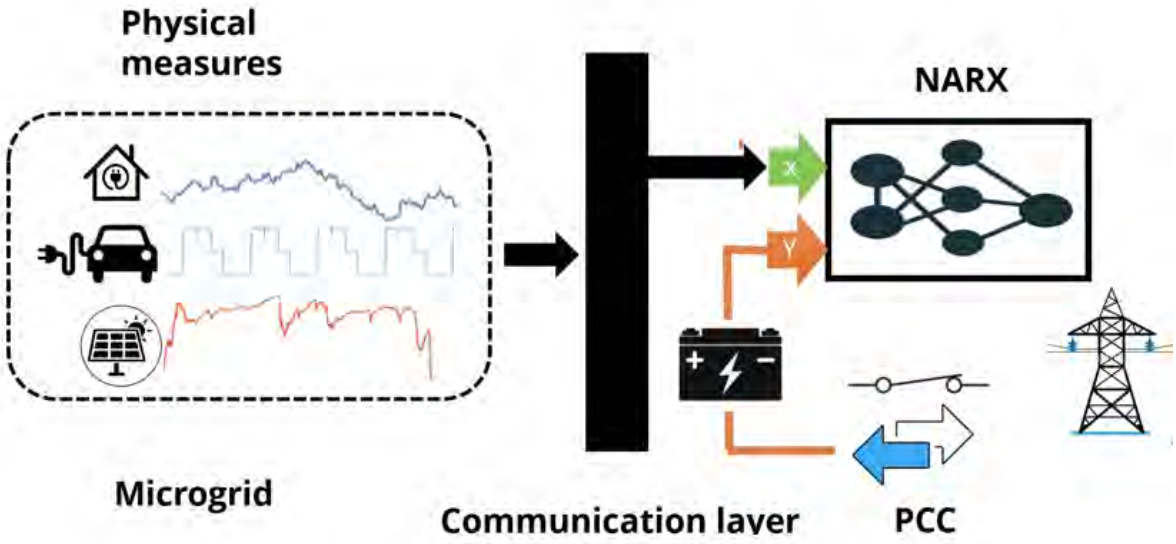


Figure.21 The NARX Input and target in the training phase.

The scenarios were created randomly, with an attempt to include the maximum rate of change possible ignoring the fact that these shifts maybe illogical in the propped time interval. Which in turn, was also what exposes us to encountering problems with the model limits. However, this is a valid case study because what we are trying to capture is the mathematical relationship between the power variations of the different units, which is not dependent on the time interval between these events. Therein, we must point out the fact that the only difference between the real data and the generated one is that we are erasing the time gaps between events and not by any mean, the time needed for an event to be reproduced.

Since there is no way to predict the number of scenarios needed to have a fully trained network, our approach was to train and test a new NARX after adding each scenario.

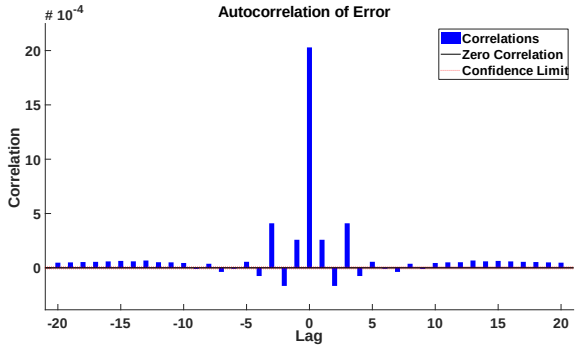
The offline training is performed on a computer with an Intel(R) Core (TM) i7-8650U CPU @ 1.90GHz 2.11 GHz processor and 16.0 GB of RAM memory.

Results show that, the best performance was obtained within 10 scenarios database, which corresponds to around 196000 (2000000) values for each measured parameter. We started with a minimum number of 3 scenarios and kept on adding and testing, until we remarked that adding more data is offering no progress or leading to a counterproductive situation after the 10^{th} scenario.

With an extended training database that only incorporated 10 scenarios (100 seconds for each one) we had obtained a fully trained NARX that succeeded in the estimating test conducted by using completely new generation-consumption profiles. Training results of the network that has the best performance are shown in the Table.4 and Figures (22,23,24)

Results	**Table Column Head estimation and real**		
	Target values	***MSE***	***R***
Training	139860	2.03626e-3	9.99999e-1
Validation	29970	2.23058e-3	9.99999e-1
Testing	29970	1.79436e-3	9.99999e-1

Table.4 Training results.



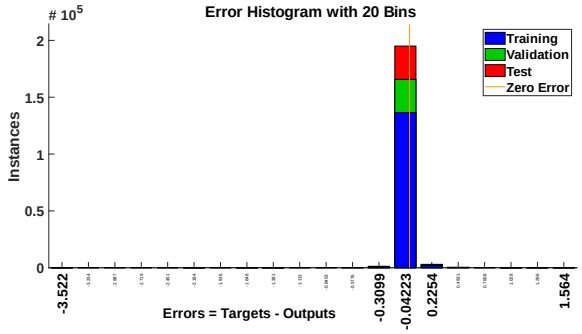


Figure.22 Autocorrelation of the Error.

Figure.23 Error Histogram.

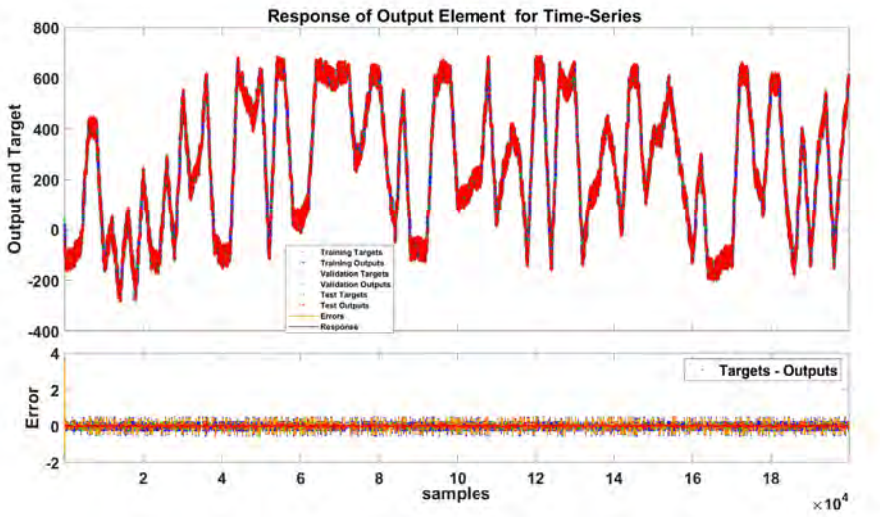


Figure.24 Response of Output Element for Time-series.

4.4.2 The online phase:

The trained network could be extracted and deployed using several forms (Matlab function, Simulink Diagram, simple or advanced script). The Simulink diagram is implemented in the model to test the online performance. Testing scenarios were created with the help of Python scripts in the RT-lab environment using random combinations of generation-consumption profiles.

The comparison between the estimated signal $\hat{y}(t)$ and the measured one y(t) in the normal functioning (without attacks) and the error signal calculated by equation (3) is shown in Figure.25 and Figure.26.

$$y(t)-\hat{y}(t) = \varepsilon \qquad (3)$$

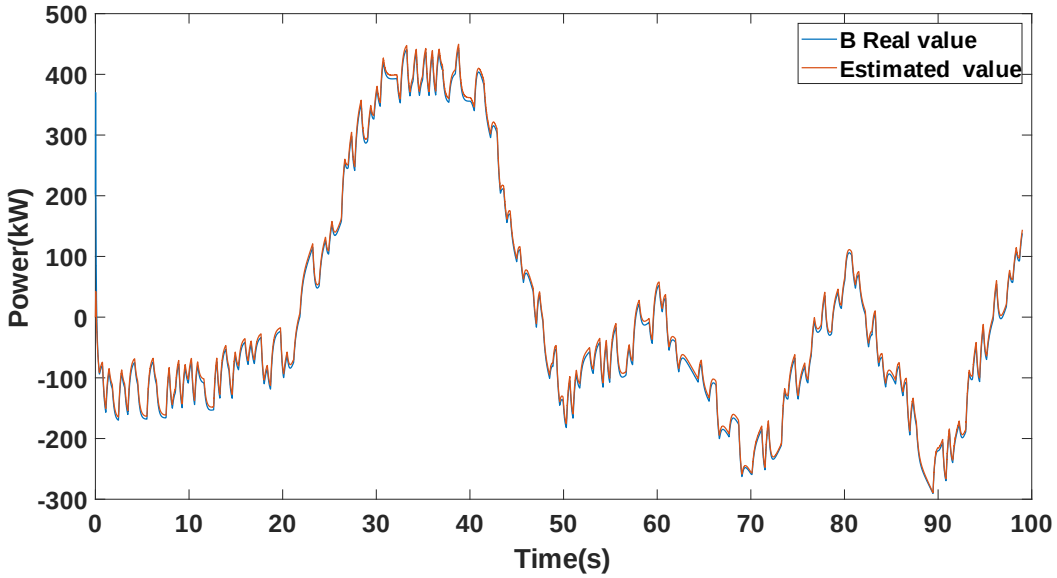


Figure.25 Comparison between NARX estimation of the Battery active power(B) and the real measured value.

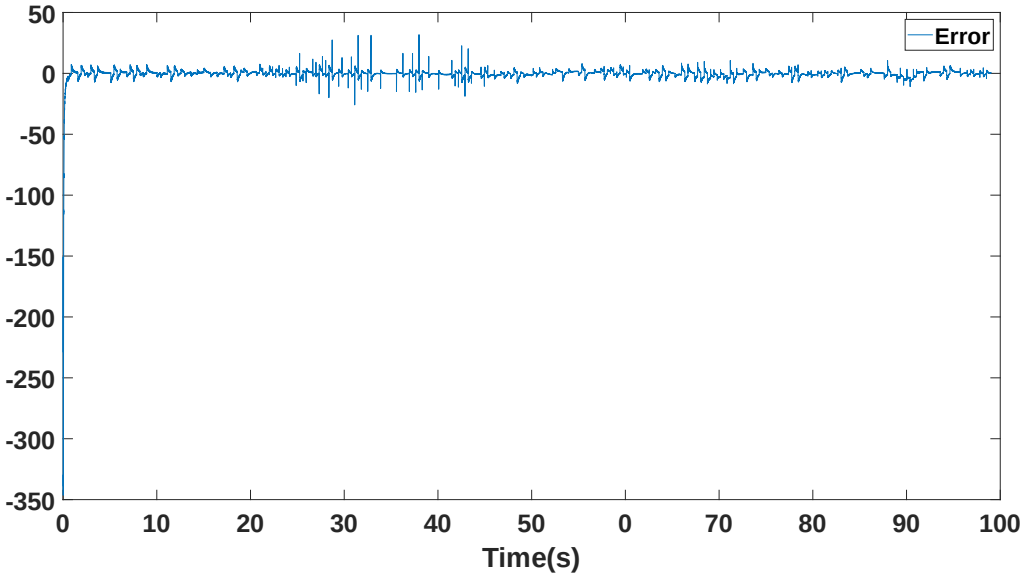


Figure.26 Error value from Equation.3.

4.5 Attack modelling and testing

We focus on two different aspects of attacks that together will cover the cyber and physical intrusion possibilities on the microgrid system.

The first type is cyber-attacks that target the communicated measurements from the physical layer through the communication layer to the detection mechanism (NARX) depicted in Figure.27 These attacks will include different forms of FDI attacks counting Replay attacks, which could be categorized as a sort of FDI as they share most of their characteristics. FDIs are the most commonly reported type of cyberattacks and the most severe ones given that attacks such as DoS attacks are easily detected. They compromise the integrity of the information flow between the communicating parts of a system and can impede control applications such as voltage control or active power control in microgrids. However, both FDI and DoS are tested in the following section.

Attack scenarios were designed based on the assumption that an attacker has already breached the communication network and was able to access and modify any desired parameter that is being transmitted to the control point placed at the point of common coupling PCC.

Any supervisory mechanism at the PCC would then receive the corrupted information keeping in mind that it has only access to what is physically placed at the PCC that is the parameters of the injected power in and out of the MG as the ground truth value.

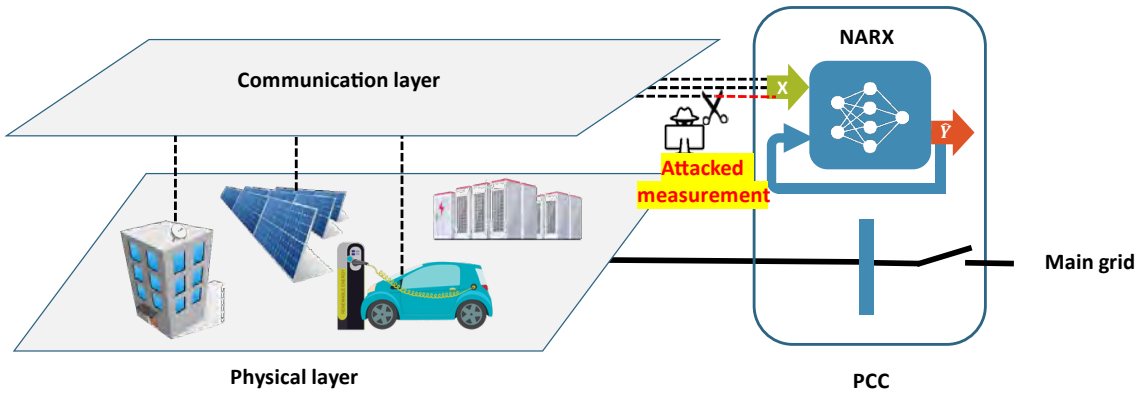


Figure.27 Cyber-attack on the transmitted measurements.

The second type is physical attacks, in which the attacker has physical access to the battery control system and is able to maliciously adjust the Energy management program to induce an undesired effect (Figure.28) this type of attack is harder to spot for the distribution system operators, as they have no access to battery information.

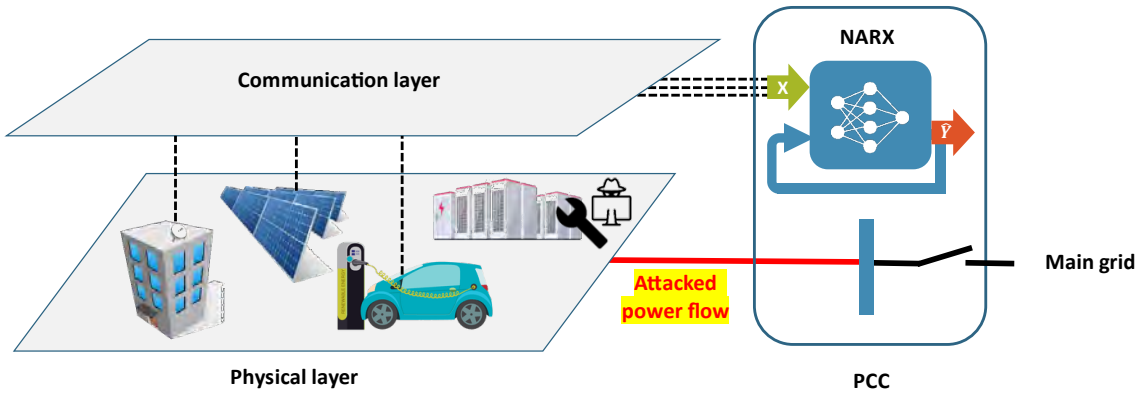


Figure.28 Physical attack on the BMS.

4.5.1 Cyber-attacks scenarios:

The attacks were generated as follows:

A number of different types of FDI attacks were considered. Under the assumption that the attacker could tamper one unit at a time by manipulating the transmitted data between the jeopardized unit sensors and the attack detector represented by the online NARX.

To create this effect, one of the NARX's input signal components was replaced by another without affecting the other signals by means of tampering with the signal source. In doing that, we keep the measured reference signal of the power at the PCC untouched while altering the relationship between the components entering the NARX, which in turn will result in an erroneous estimation indicating the presence of the attack.

In the following, a sample of attack cases was built to approximate a genuine interest in injecting an attack and cover widely discussed attack introduction means.

4.5.1.1 FDI attack on the PV production (PV overproduction):

An overproduction of PV panels is a way of cheating subsidy programs that reward high-penetration PV rates in cases where smart meters collect these types of information. The attack can be modelled according to one of the equations (4,5) below:

$$PV_{attacked} = PV_{real} + \alpha \qquad (4)$$

$$PV_{attacked} = \alpha \qquad (5)$$

Where $PV_{attacked}$ is the reported value of PV production to the NARX after the injection of the FDI attack, while PV_{real} is the actual measured value (the un-attacked value) and α is the false injected measurements.

The following figures illustrate the results of injecting an FDI attack according to equation (4) at the 30th second of the test. Figure.29 demonstrates the resulting divergence between the physically measured Ppcc and the estimated values right after the injection of the attack. While Figure.30 displays the simple subtraction error (ε) denoted by equation (3).

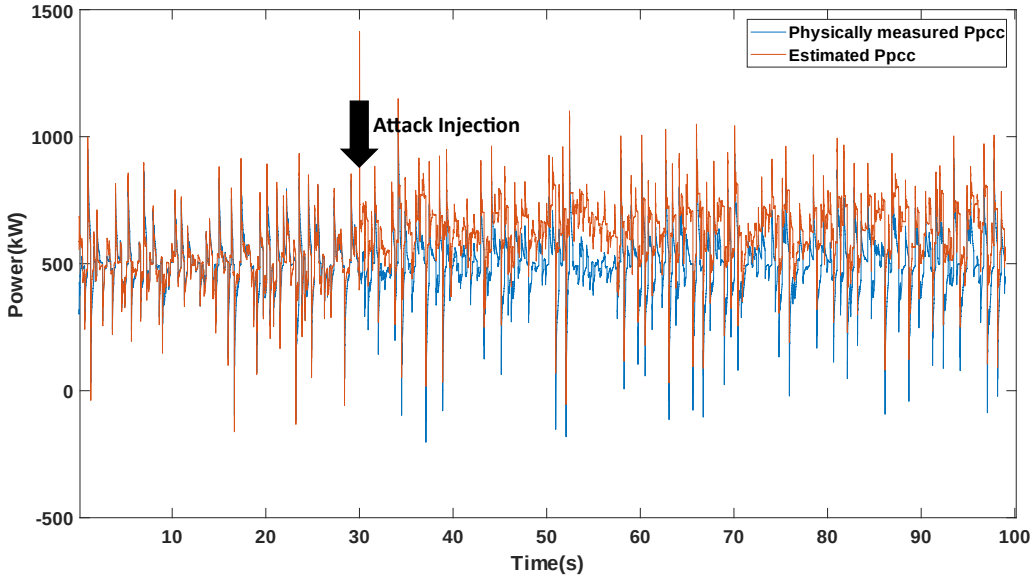
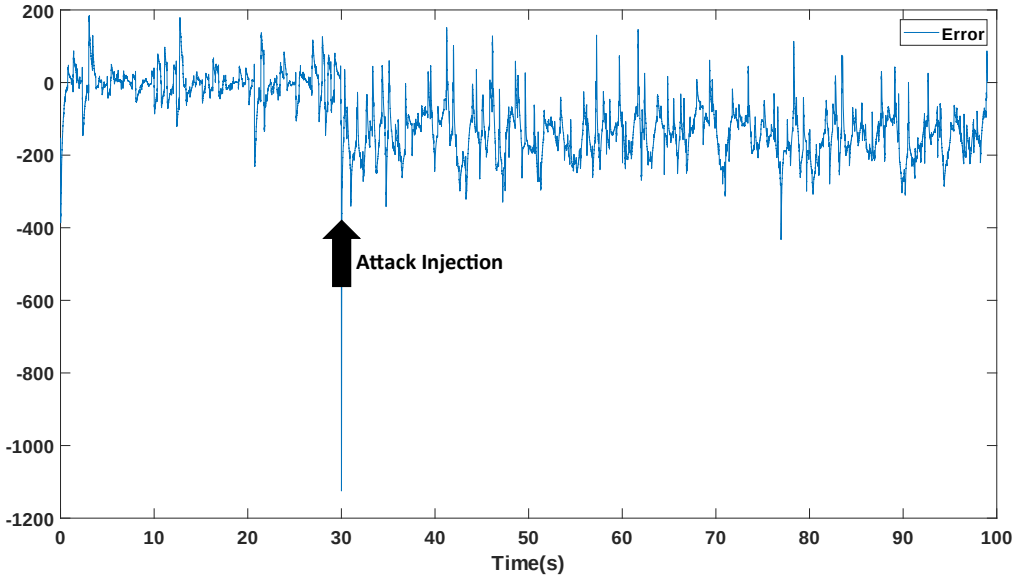


Figure.29 FDI attack: injection of higher production PV profile.



Figre.30 Error signal.

4.5.1.2 Replay attack (Replayed PV profile):

A replay attack happens when the attacker records the intendent signal (measurement/s) for a period of time in which the conditions are favourable to yield better economic profit or to induce an undesirable reaction of the battery control system.

The reason why these types of attacks might interest a cyber adversary is that the injected false or bad measurements in this case follows an absolutely normal distribution since that it was originally generated from the same system. This will block the intervention of ordinary fault detection mechanisms and hides the attack from the operator's viewpoint.

The attack is modelled based on the equation (6) below:

$$PV_{attacked} = PV_{replayed} \qquad (6)$$

A replayed PV profile is injected at 50th second of the test as seen in Figure.31 and even more clearly in the error graph in Figure.32.

One must notice that the clarity of the visual detection of the attack represented by the mismatch between the two signals (the estimated and the measured) in the two previous cases is much simpler in tests with less event density. Considering that the variation frequency of the events is an optional variable that doesn't reflect on the performance of the adopted detection method. The results in the third and last case (the delay attack) are presented in a lower event change rate for demonstration purposes as seen in the next section.

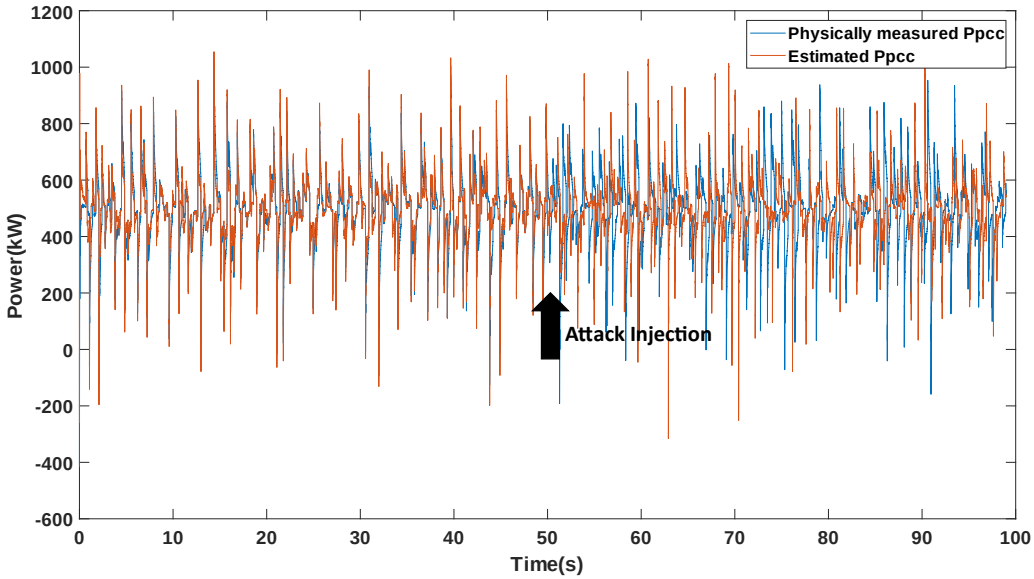


Figure.31 FDI attack: injection of replayed (repeated) PV profile.

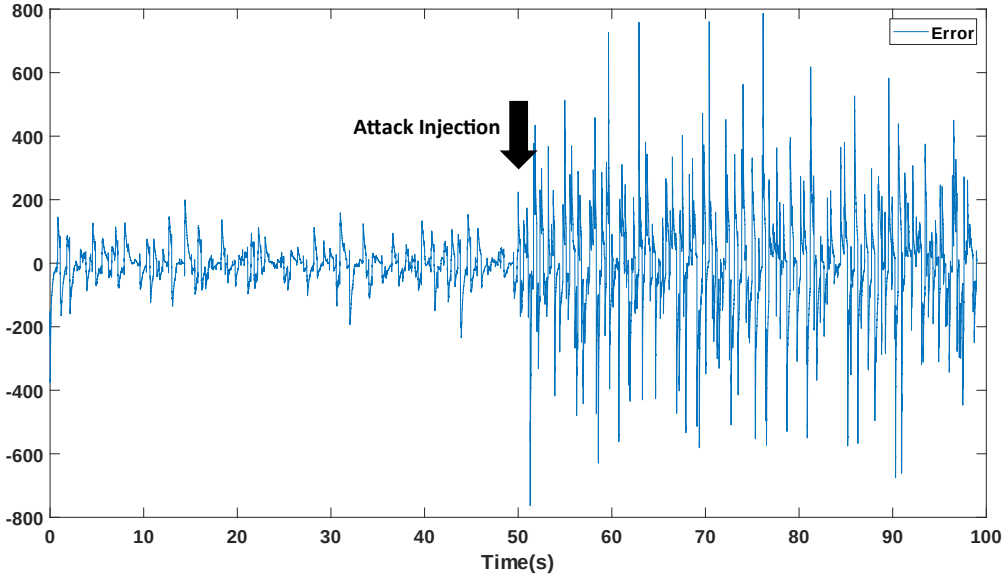


Figure.32 Error signal.

4.5.1.3 DoS Attack (Delay attack)

Delayed measurements in systems that necessitate extremely rapid responses could lead to catastrophic events as previously mentioned in this work. This type of DoS attacks could be established when the real measurements are delayed due to congestion attacks that slow down the communication system and create a transport delay.

The $Ppcc_{real(t)}$is the reference value that the BMS receives in order to adjust the B output at time (t). Altering this signal by retarding it, will set back the proper action to be taken from the Battery storage side either to interfere with compensating for a lack of production or to seize the chance to charge from an over-production low-consumption scenario. In both cases, the damage on the economic scale, at least, is guaranteed.

The attack model is given by equation (7).

$$Ppcc_{attacked} = Ppcc_{real(t-d)} \qquad (7)$$

Where the $Ppcc_{attacked}$ is the delayed signal by the attacker, d is the introduced time delay. A suggested d of 5 seconds is introduced in the following Figures (Figure.33, Figure.34).

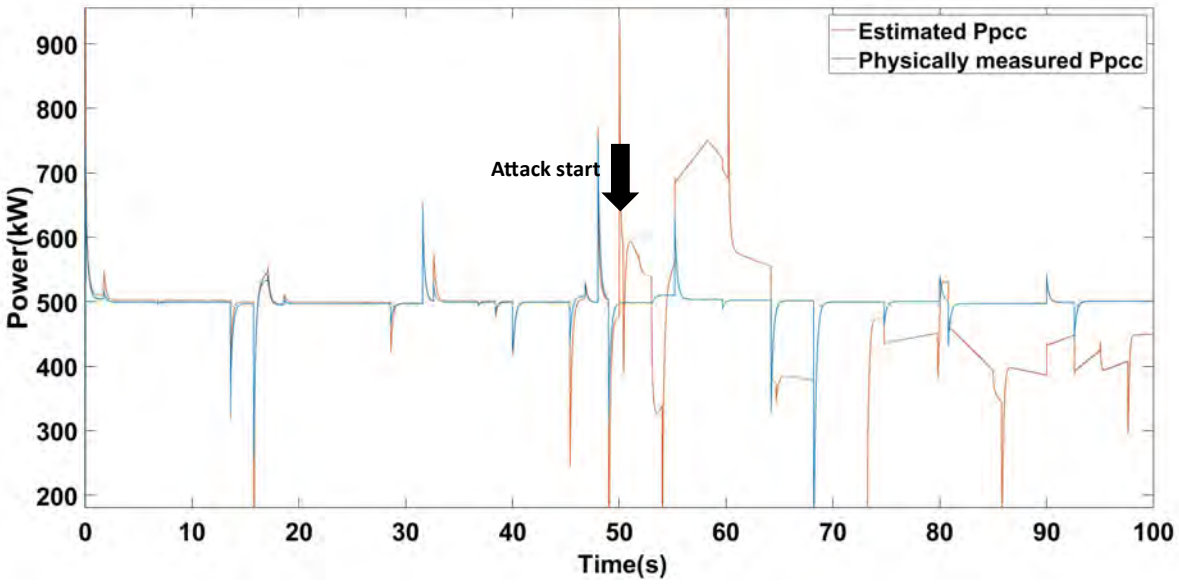


Figure.33 Dos attack: Delayed BMS reference signal.

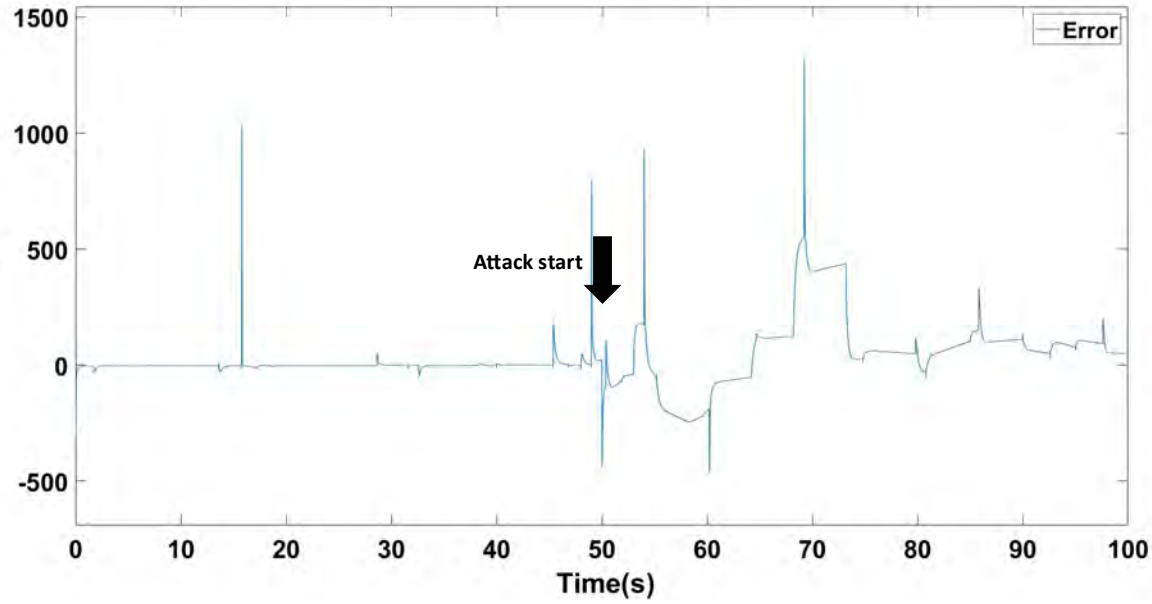


Figure.34 Error signal.

4.5.2 Physical attacks scenarios

What distinguishes the approach delivered by this study from other attack detection mechanisms is the ability of this unique tool to identify anomalies on both cyber and physical layers. An undetected malfunctioning of the BMS could easily result in destroying the storage unit if not extra equipment connecting to it as explained later in the two discussed attacks underneath.

4.5.2.1 Forced charging

In this attack scenario, the attacker forces the Battery to charge when conditions for charging from the microgrid set by the BMS are not met. Depending on the microgrid set of priorities, forced charging may put the MG's distributed generation under pressure or causes the battery to draw from the grid in peak hours.

A force charging command is launched at the 60th second of the test scenario as observed in Figures (Figure.35, Figure.36) below causing the estimated signal to derail from the real measured curve indicating the presence of the attack.

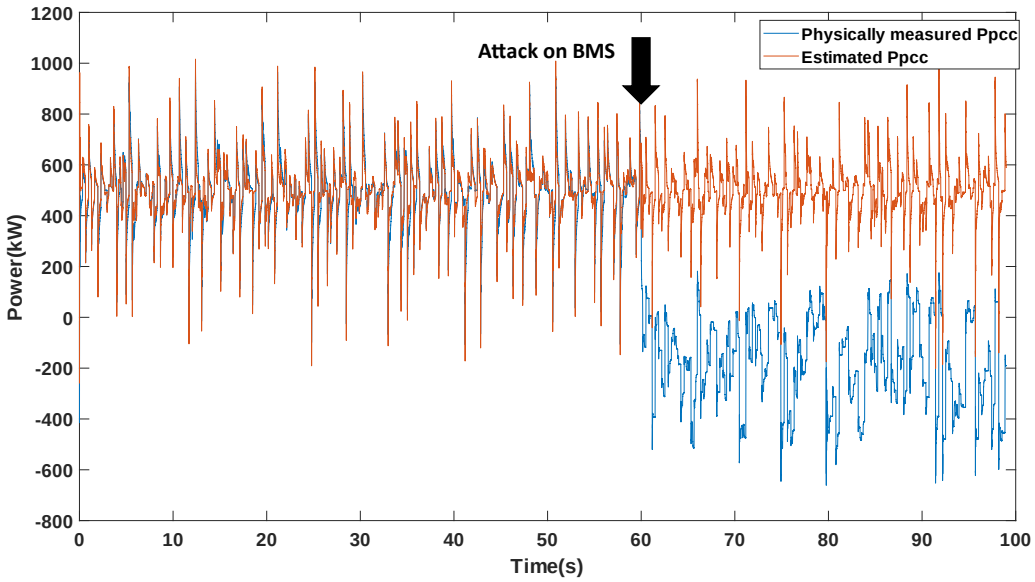


Figure.35 Forced charging attack on the battery at ts=60 s.

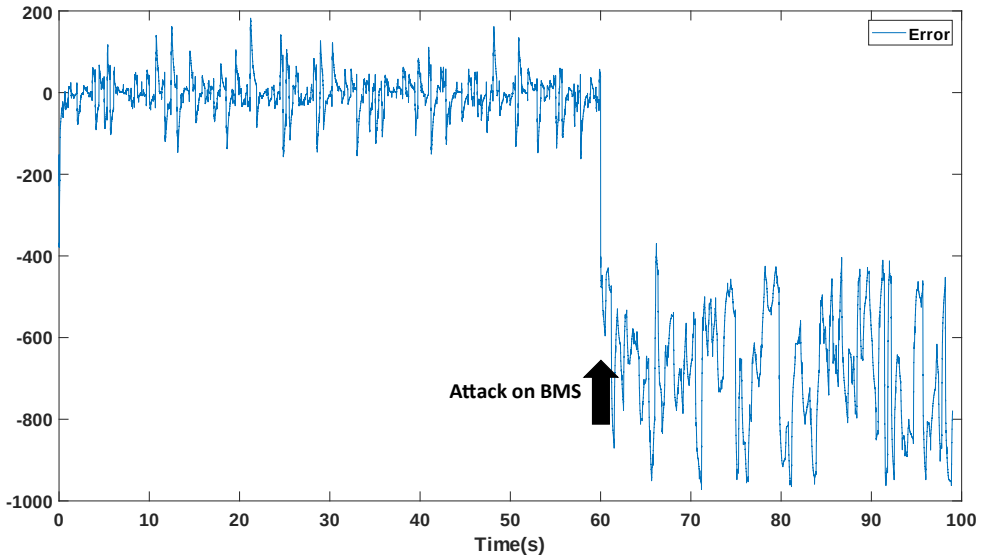


Figure.36 Error signal.

4.5.2.2 Forced discharging

A slightly more severe physical attack on the BMS could be initiated by forcing the battery system to discharge when there is no need for battery support. This action could easily damage the battery structure when it is forced to continue to discharge dropping under the advised limits, especially when injecting this non-absorbed power from the battery output can be injected into the grid. Figure.37 and Figure.38 show the effect of this attack on the estimation of the NARX at (ts=80s).

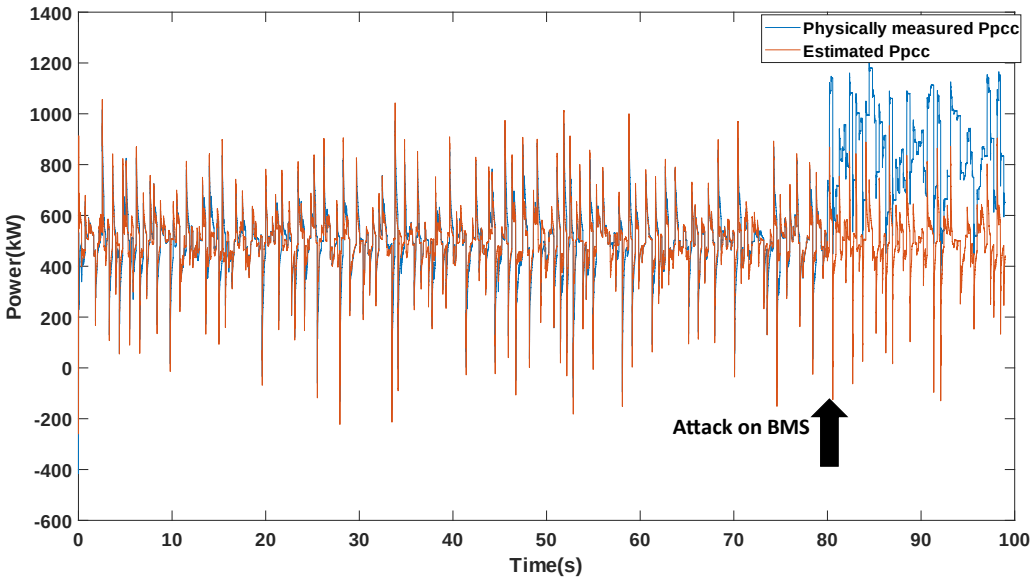


Figure.37 Forced discharging attack on the battery at ts=80 s.

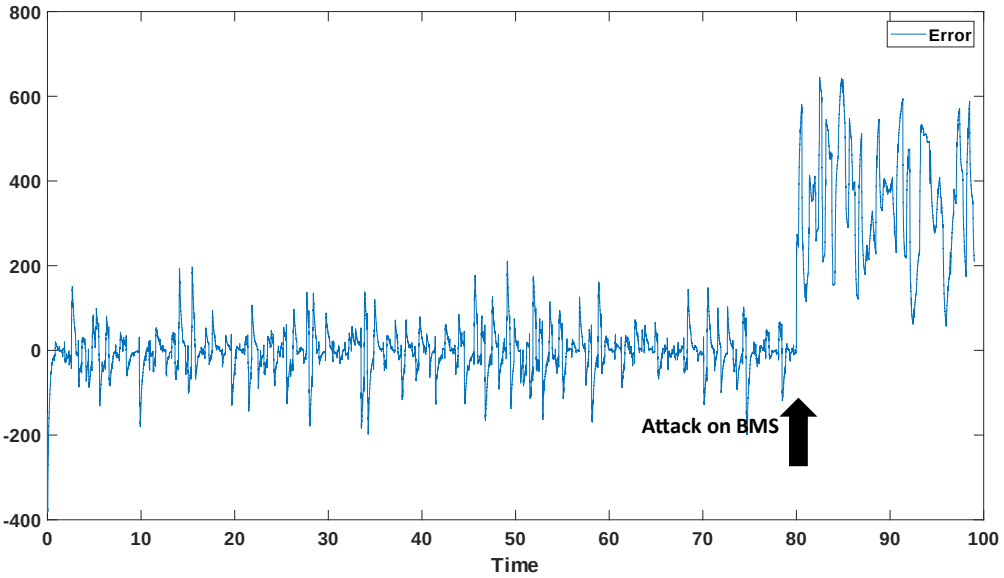


Figure.38 Error signal.

4.6 Discussion and conclusion

The proposed strategy has been proven effective in detecting all kinds of considered attacks. Simulation results show that after only one sampling time after injection we could start noticing the estimated signal veering off the target indicating occurring anomalies. Which will be confirmed as a possible cyberattack when the calculated error does not eventually converge to zero.

It should be noted that the data used in network training has not been subjected to any external of Input optimization (normalization or standardization). The same thing goes for the error signal.

In this work, the generated error was perceived intuitively, and it was not processed by any statistical technique to detect the attack. Developing an indication factor, upon which an automatic detection of the attacks could be performed, is still an indecisive problematic not least because of the following arguments.

The effects generated from all the possible attack types targeting different points of a certain MG cannot be confined. In addition to the fact that the microgrid paradigm is not generalizable and the effects of the same type of attacks change dramatically by changing the size, the number, the type, and the connection between of the MG units. Besides, each deployed NARX should first learn the normal behaviour of the MG in question and then be subjected to each and every one of these attack scenarios in order to record its response to these different attacks. Therefore, building a database that encompasses these information is quite impracticable.

That's why the focus of this method was to prioritize offering a detection mechanism that alert the operators for all kinds of anomalies (the known and the unknown ones).

In a related vein, we could have easily duplicated the experiment and estimate the power outcome of each component as a function of the remaining others which will provide extra information about the infected unit as suggested in [89]. But once again, the focus was on minimizing the supervised variable in a way that makes it extremely simple built demanding a computation resources as low as possible.

This has resulted in a trained NARX that was also proven to work in a real-time environment, meaning that, all needed computations for delivering each step of the output fit inside the intervals for real-time simulation constraints.

It is important to note that training the network multiple times will result in different values for Mean Squared Error (MSE) and Regression (R), due to the different initial conditions and sampling. Taking MSE and R as the only criteria to judge the best network performance as in most of the studies that use neural networks was not satisfying in this case, and actual testing of each trained network was imperative.

However, even when ending up settling for a trained network that provides satisfactory results, it is always important to investigate the limits of this network in the desired application. As a result, this will be the subject of practical experimentation found in the final following chapter.

Chapter 5: Practical validation and limitation

In this Chapter, we continue to explore the practical dimension of the proposed cyber intrusion detection mechanism. First, the ability of the NARX-based real-time detection tool to work as a stand-alone device is tested in section 5.1. A Hardware-in The loop simulation using the Opal RT real-time simulator and an external microcontroller board (Arduino) for Embedding the used Artificial Neural Network (ANN) was employed. Then in section 5.2, the limitation of the NARX model in this particular application is defined (traced). Finally, the LSTM model is introduced, tested, and validated over several battery management systems in section 5.3.

5.1 Hardware In the Loop setup

As mentioned earlier in chapter 3, Hardware-in-the-loop (HIL) simulation is a technique for the development and testing of complex real-time embedded systems. It provides an effective testing platform by means of combining the plant's process-actuator mathematical representation with the embedded system to be tested. There are plenty of reasons upon which this configuration is usually consulted to further verify the effectiveness of the proposed solution. However, in this study, the interest was to investigate the method's practicality in terms of the implementation conditions.

The testbed used in this work consists of a host computer, a real-time simulator, and a microcontroller. The AC microgrid model is running on the real-time target from Opal-RT technologies and connected with the proposed ANN-based detection mechanism embedded on a microprocessor, in our case the Arduino MEGA 2560 board as shown in Figure.39.

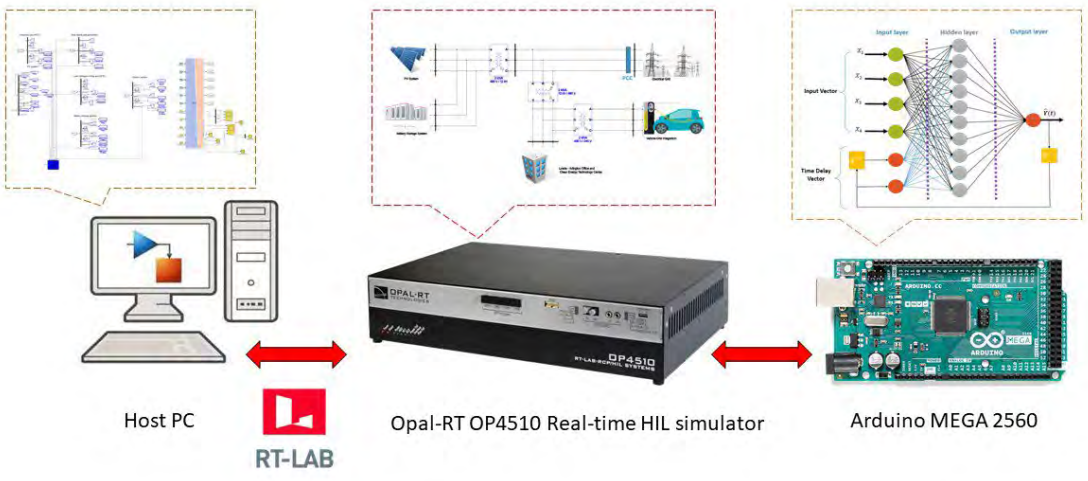


Figure.39 The Hardwar-In-th-Loop configuration.

5.1.1 The plant on real time simulation

As illustrated in Figure.40, the top level of Simulink model must at least be divided into two functional subsystems to be compatible with the real-time simulation environment. This process in RT-LAB follows the objective of distinguishing the computational subsystems (SM, SS) from Graphical User Interface (GUI) subsystems (SC). While the Computational subsystems include all of the model's elements that need to be calculated such as mathematical operations, I/O blocks, signal generation, physical models, etc. Each computational subsystem is executed in real-time (or accelerated simulation mode) on one CPU core of the real-time target. Communication between computational subsystems is synchronous while it is asynchronous between SC and (SM, SS). On the other hand, GUI subsystems are considered a tool that allows monitoring and interaction with the system's outputs. It is displayed on the Host PC.

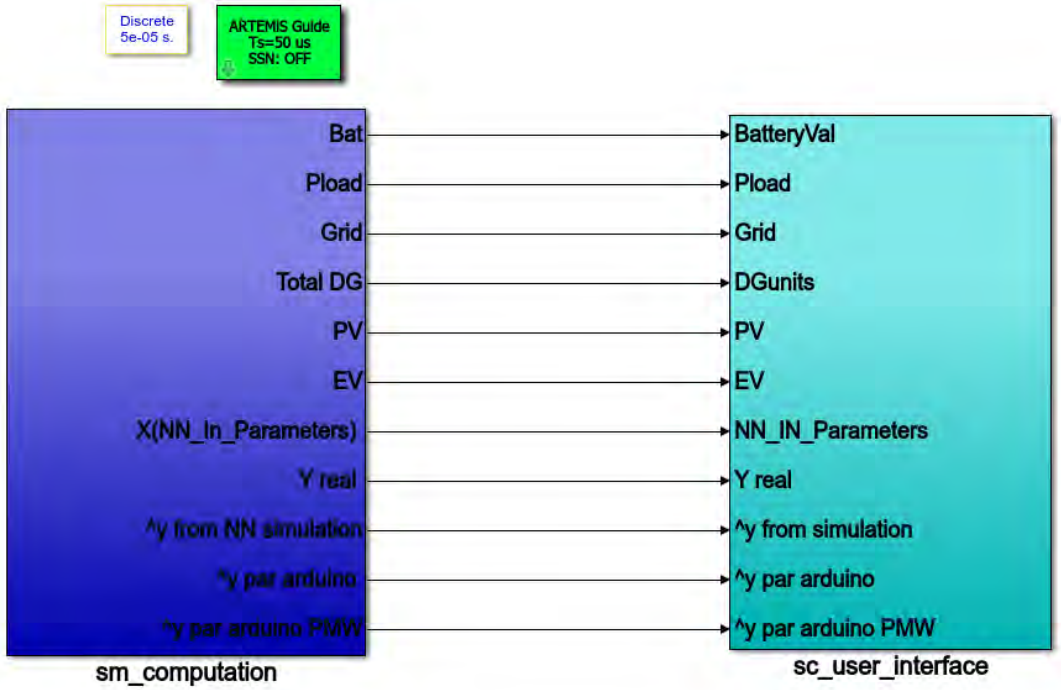


Figure.40 The Computational (SM) and Graphical User Interface (GUI) subsystems.

The experiment is performed using the same AC connected microgrid mentioned in the previous chapter. It is the most common yet the most vulnerable type, given the fact that it still exchanges both communication data and physical power with the grid.

The model runs on the real-time target (OP 4510) from Opal RT with the technical specifications found in Table.5.

Processor	CPU	Intel Xeon E3 4-core 3.5 GHz
FPGA	Kintex™-7 K325T standard (K410T optional)	
Performance	CPU	Min. time step model execution of 7 microseconds
	FPGA	Timer resolution of 10ns and minimum time steps of 250 ns
I/O cassettes (max. 4 per system)	Analog	16 channels (max. of 64 per system)
	Digital	32 channels (max. of 128 per system)
Dimensions	W x D x H	2U, 17” x 10.8” x 3.5”

Table.5 OPAL-RT (OP 4510) technical specifications.

Analogue output signals that represent the Input of the NARX, being the PV production, load consumption and the electric vehicle charging-discharging profiles were outputted from the simulator to be later inserted into the embedded ANN model on the microcontroller.

5.2 Embedded RNN

Recurrent neural networks in general are increasingly used in the analysis of time-dependent signals as discussed in chapter 3. The diagnostic of power management behaviour in the context of this work is dealt with as a sequence of events that is a function of time.

Despite the relatively high computational and memory resources required in executing RNNs on embedded devices, there has been strong interest in their implementation. This interest has originally derived from the objectives that could be reduced to pursuing better efficiency and flexibility. Implementations for efficiency objectives will seek high throughput, low energy consumption, and real-time compatibility. While flexibility objectives would require the implementation to support the diversity in the RNN models, online training, and satisfy different domains application requirements [165].

The challenges specific to the implementation of the recurrent structure include factors such as the matrix vector multiplications, especially for LSTM layers. In addition to the temporal dependency that results from waiting for the previous time-step computation to complete, in order for the output to be refed back as an input. Which in turn, makes it very difficult to perform parallelized computing over time-steps.

In most cases, it is difficult to run RNN models in their original form efficiently on embedded platforms. Especially when these platforms often suffer from limited memory and power capacities. The thing that led researchers to opt for optimization measures on both levels of the RNN models (algorithmic optimizations) and target platforms (platform-specific optimizations) [165].

However, during the implementation of the NARX proposed in this research, none of the previous limitations was encountered. The next section will put forward the technical specification of executing our neural network on the selected microprocessor.

5.2.1 NARX on Arduino

Following the objectives of efficient implementation, no online training or adaptive learning functionalities was involved in testing the used NARX performance. Interestingly, the choice of using a statically fully trained network was built on a deeper reflection on the nature of the attack detection problematic and not just as an attempt to boost efficiency. A network that continues to learn during the online phase will fit every anomaly that faces it into the normal functioning characteristics. As a consequence, recognizing the attack based on differences between the estimated and real behaviour is simply not possible.

This has inevitably affected the choice of the used edge device driving us towards less exigency for sophisticated options as explained in the following.

The microcontroller board used in this test is an Arduino Mega 2560 which is based on ATmega2560 and contains 54 digital input/output pins and 16 analogue inputs. The total flash memory for code storage is 256 KB (8 KB of it is for the bootloader), 8 KB of SRAM and 4 KB of EEPROM. It is also equipped with, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, an ICSP header.

Normally, the Integrated Development Environment (IDE) is used to program the Arduino board as the ATmega2560 on the Mega 2560 offers a bootloader that permits updating the code without any external hardware programmer. The established communication through the original STK500 protocol, which is a starter kit for Atmel AVR Flash microcontrollers, interfaces Atmel's studio IDE for code writing and debugging offering developers a quick start.

However, for this experiment, the deployment of the C code of the trained NARX is done automatically using Simulink embedded coder application directly, skipping the reconfiguration of the code.

The Arduino board receives the analogue signals from a real-time target after adapting all signals to the acceptable voltage limits [0-5] volts using a simple gain and an offset effect for the representation of negative values. Needless to say, these changes need to be reversed to their original values before using them as the NN input.

The Arduino board used in this test does not have an analogue out pin. Instead, a PWM output signal was employed to extract the estimated Ppcc at the output of the embedded NARX, which is returned to the simulator as an input signal. Thereafter, the comparison between the real measured Ppcc and the estimated one coming from the Arduino for attack detection is observed in real-time on RT-lab's Graphic User Interface (GUI).

Figure.41 shows the used workstation integration with the Arduino board connected to the real-time simulator with the help of input-output extensions. While the connection of the Arduino with the digital inputs and analogue output (A: DB37 connectors for digital or analogue inputs and outputs) appears in Figure.42.

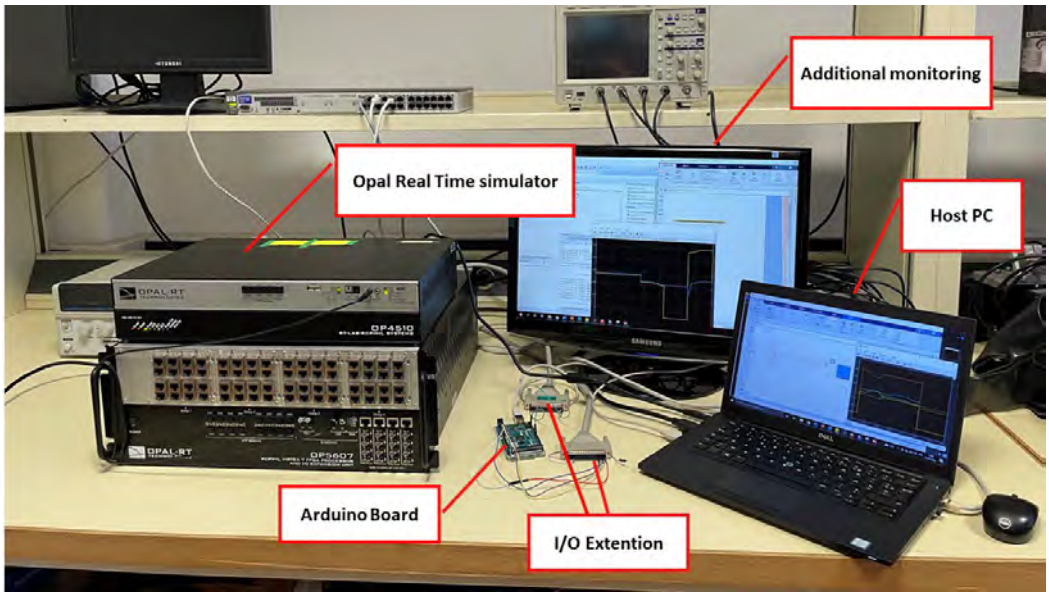


Figure.41 The experimental workstation.

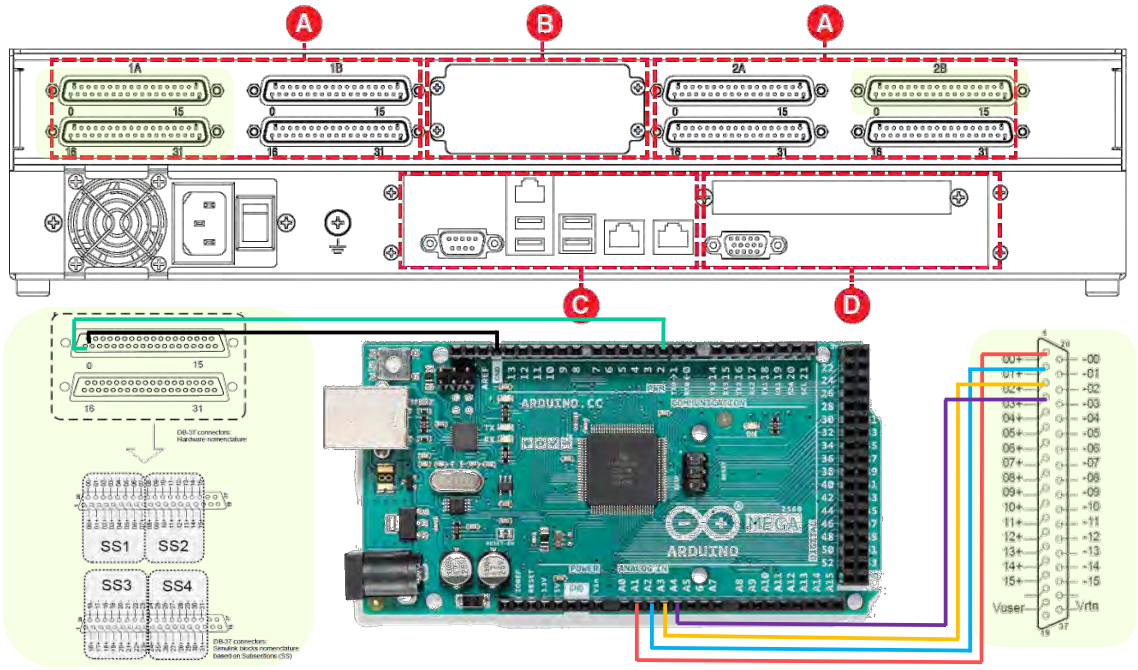


Figure.42 Connections between the Arduino board and IO opal interface.

5.3 Case study validation

In this section, we discuss the results of applying the different attack scenarios presented earlier in chapter 4 to demonstrate the effectiveness and potential drawbacks of the propped implementation.

To start with, there were no signal deformation problems related to mis-sampling and hence no declination in signal representation accuracy. Given the fact that the used MicroController Unit (MCU), has a sampling rate of around 150K samples per second as digital pin write takes about 6.50 Microseconds while digital pin read takes about 6.35 Microseconds and analogue pin read takes about 112.01 Microseconds [166]. Keeping in mind that the model's smallest time step is 50 Microseconds and NARX can still catch all intended dynamics that enable it to function correctly on lower resolution signals of 5 Millisecond sampling time.

Concerning attack detection performance, results show an immediate reaction to the attack denoted by visual divergences of the estimated Ppcc from the real measured value as observed in Figure.43, which represents a screenshot of the real-time scopes. While a more accurate graph is provided from the files generated using OpWrite file at the end of the simulation Figure.44 These figures are from a case study that has been selected as an example to demonstrate the absence of any performance degradation in term of detection efficacity.

The introduced attack here is a BMS attack that changes the default battery response at the 60th second of the test. It is important to note that both figures represent the exact same test with a difference in the time scale of which the graph is consulted. In real time supervision provided by RT-LAB's GUI, results only appear at the end of each frame (set as 1 second) regardless of the selected simulation time step. This in turn explained the appearance of the very low starting point with the initial values at the start of the simulation in Figure.44 that is completely missed in Figure.43.

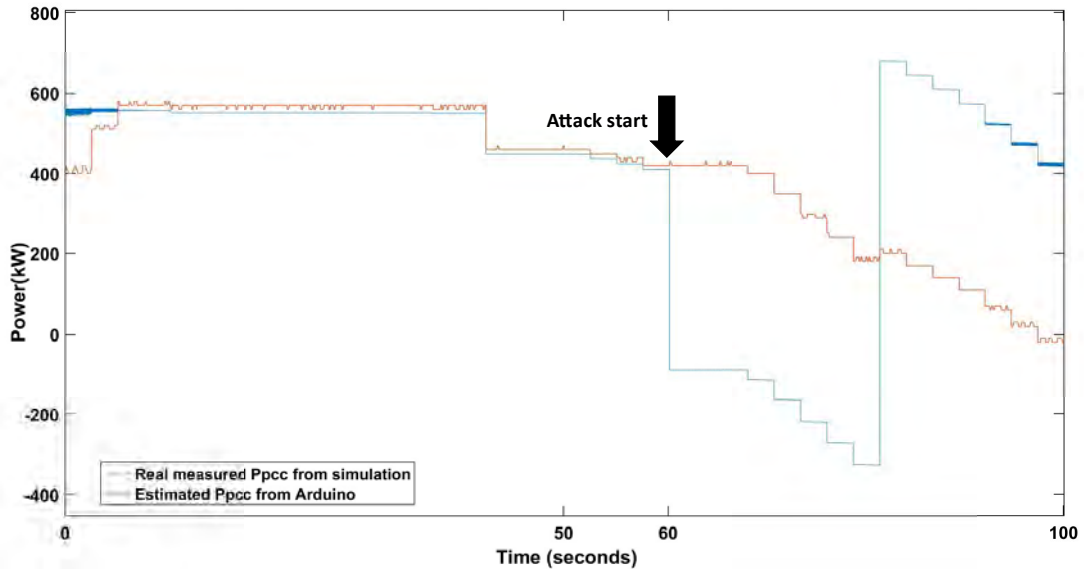


Figure.43 Screenshot form the real-time execution.

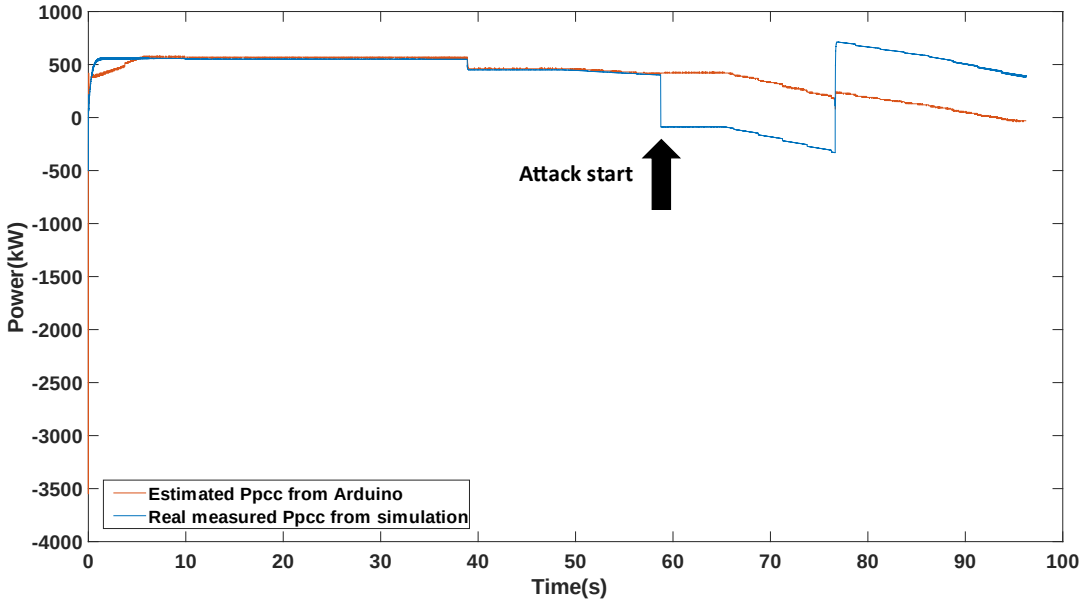


Figure.44 Results from OpWrite file at the end of the execution.

5.4 NARX limits:

When testing the NARX configuration on a more elaborated control system, the results weren't as satisfactory as in the previous case.

A multi-condition BMS that controls the transition of the battery system between the different modes of functioning has been constructed with the help of a python script. This new control system was set to include forced charging or discharging possibilities under a preselected set of conditions as seen in Figure.45

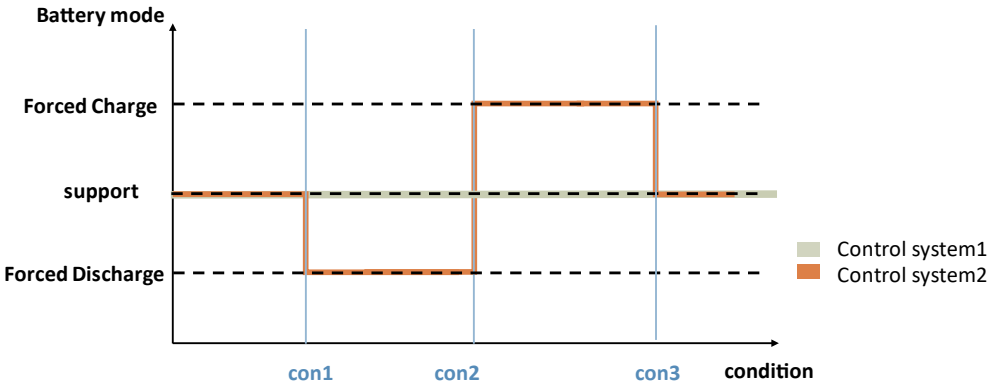


Figure.45 Different Battery control systems.

Building the training dataset, the offline training and testing has been carried out in a similar fashion. The following Figure.46 presents the best performance obtained from a NARX trained on the new control system.

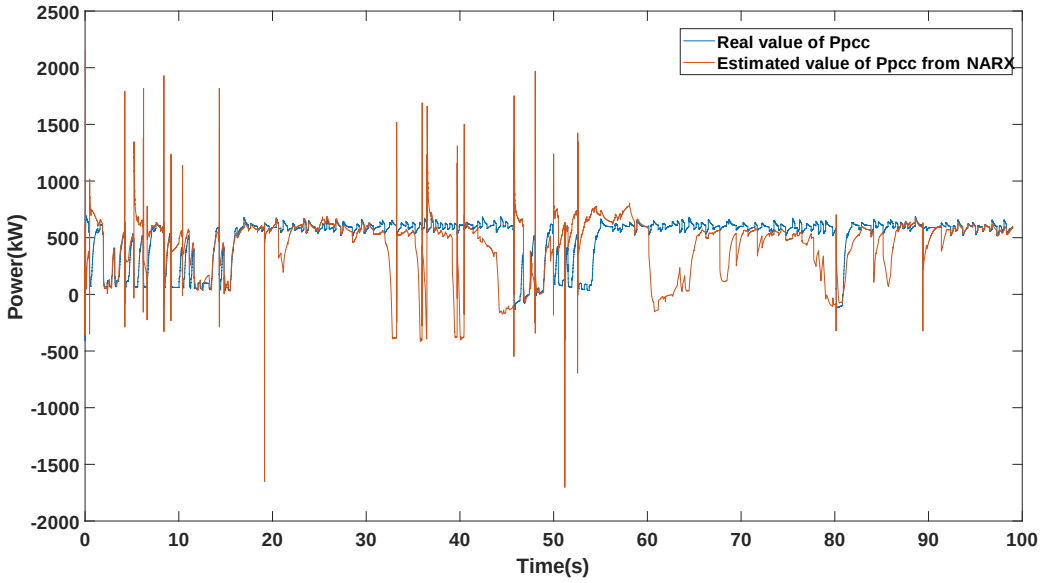


Figure.46 NARX output when estimating battery control system2.

In theory NARX should be able to react to conditions that only appear in the time delay window set by the equation (1) That's what made it miss conditions that develop on different time scales. Especially with a script that is not executed in real-time. The Figure.47 below illustrate the different time scales upon which an event is produced. Where T_{C1} is the control time step needed for constants that control the PV production, the load and the electrical vehicle behaviour set by the script to change these profiles. T_{script} is the time needed for the script to run the conditions on which the battery system is defined including the time needed to set the battery control constant (B-const) on the decided value. Finally, T_{C2} is the control time step needed for the battery system to act based on B-const.

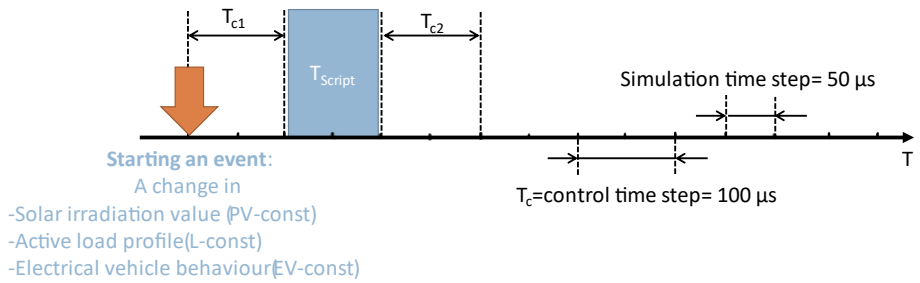


Figure.47 The different time scales for an event to be produced in the model.

It is essential to mention that different configurations of the NARX networks were tested by modifying the number of time-delay steps, the number of neurons in the hidden layer (Figure.48), or even the number of hidden layers itself without any perceived amelioration.

This test sets the limits of the NARX capability to dynamically identify the battery control system. hence, it clearly draws the line under which case studies the implementation of the NARX model is expected to deliver accurate estimations.

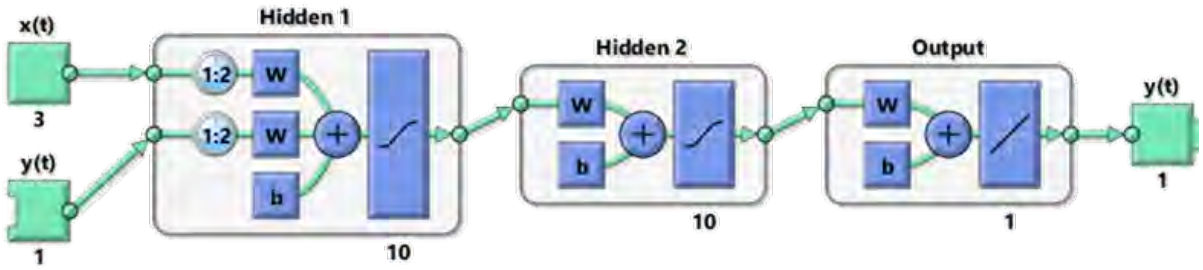


Figure.48 Two hidden layers NARX.

5.5 LSTM to upgrade the RNN model for better results

In pursuit of better results, the model of LSTM recurrent neural network has been consulted. Driven by the outweighed performance and promising avenues of the LSTM model that appears side by side with every study that uses RNNs, more particularly, in studies that compares it with NARX performance on an identical research problem [167] [162].

As discussed in [168] , this superiority in performance of the LSTM is not only due to their complicated structure but also to the necessity for state observers to run these RNNs models in a closed-loop mode, using the previous input and output data to estimate the current states and enhance the predictions of the future outputs.

Moreover, The LSTM network has initially been introduced to solve the problem of the vanishing gradient [169]. Whereas NARX NN is still limited, to a certain degree, by this issue which makes it stop the learning process after a specific number of outputs. This influences the memory function as in classic RNNs the gradient descent shrinks in long-range dependencies causing the memory to fade out [161].

The ability of the LSTM model to fully exploit the long dependencies comes from the implementation of the several gates that enables it to only store relevant pieces of information and ignore irrelevant ones.

The LSTM cell is featured in the Figure.49: where I_t is the input gate, f_t the forget gate and O_t the output gate. These gates are selected according to the hyperbolic tangent function (tanh), the Sigmoid function or matrix multiplication as described in the following set of equations (8):

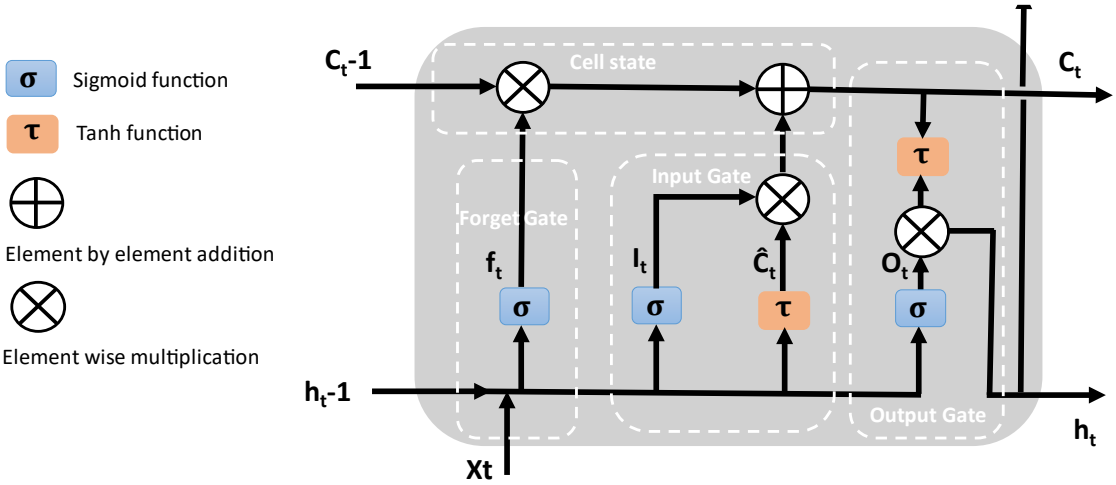


Figure.49 LSTM Cell.

$$
\begin{aligned}
I_t &= \sigma(W_I x_t + U_I h_{t-1} + b_I) \\
f_t &= \sigma(W_f x_t + U_f h_{t-1} + b_f) \\
O_t &= \sigma(W_O x_t + U_O h_{t-1} + b_O) \\
\hat{C}_t &= tanh(W_C x_t + U_C h_{t-1} + b_C) \\
C_t &= f_t . C_{t-1} + I_t . \hat{C} \\
h_t &= O_t . C_t . tanh(C_t)
\end{aligned}
\qquad (8)
$$

Additionally, $\hat{C}_t$, C_t are the candidate for cell state and the updated cell state value that helps determining the new hidden state h_t. x_t is the input sample at time t, correspondingly (W_I, W_f, W_O, W_C), (U_I, U_f, U_O, U_C), (b_I, b_f, b_O, b_C) represents the recurrent and input weights also the biases respectively for each given gate.

LSTM model was trained to directly predict the Ppcc without passing through the step of estimating the Battery first. It has circumvented the problem of recognizing multiple operation conditions and hence can be used to detect attacks that target more complicated BMS.

A network with one LSTM layer with 200 hidden units and a fully connected layer trained on a database collected over 1000 seconds has already provided good results with minor disturbances as seen in Figure.50 (lstm1).

These occasional misestimations have been overcome when extending the training database to 4000 seconds in (lstm2). However, the optimal estimation was obtained from a network than encompasses 2 LSTM layers (lstm3).

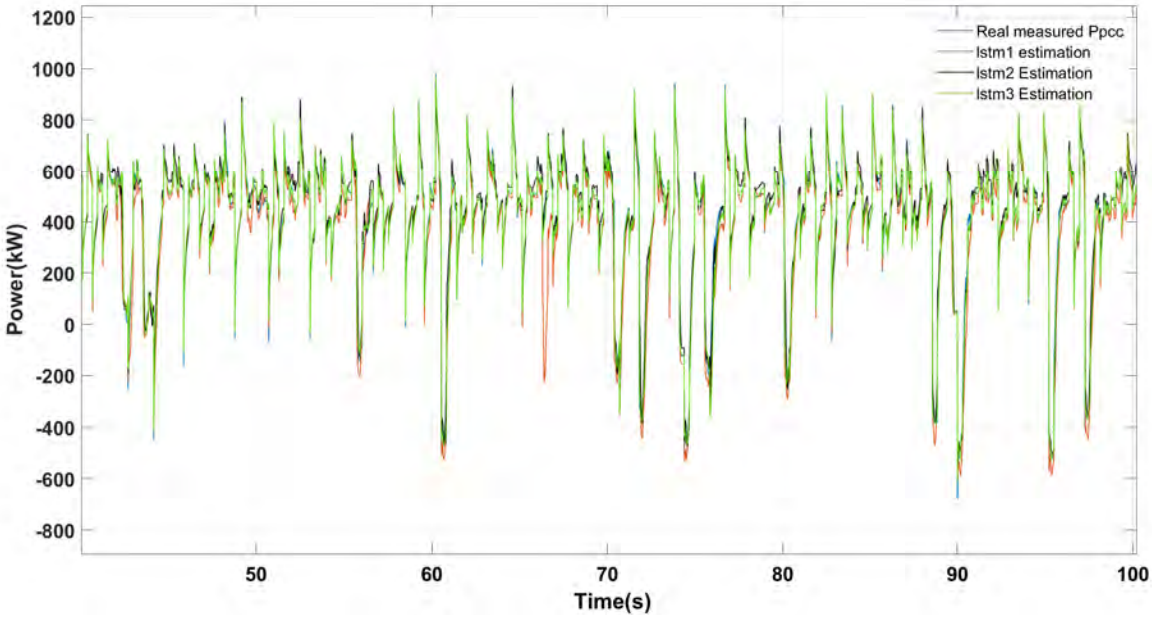


Figure.50 Estimating normal behaviour of muli-conditions BMs.

The training results of the lstm3 is shown in Figure.51

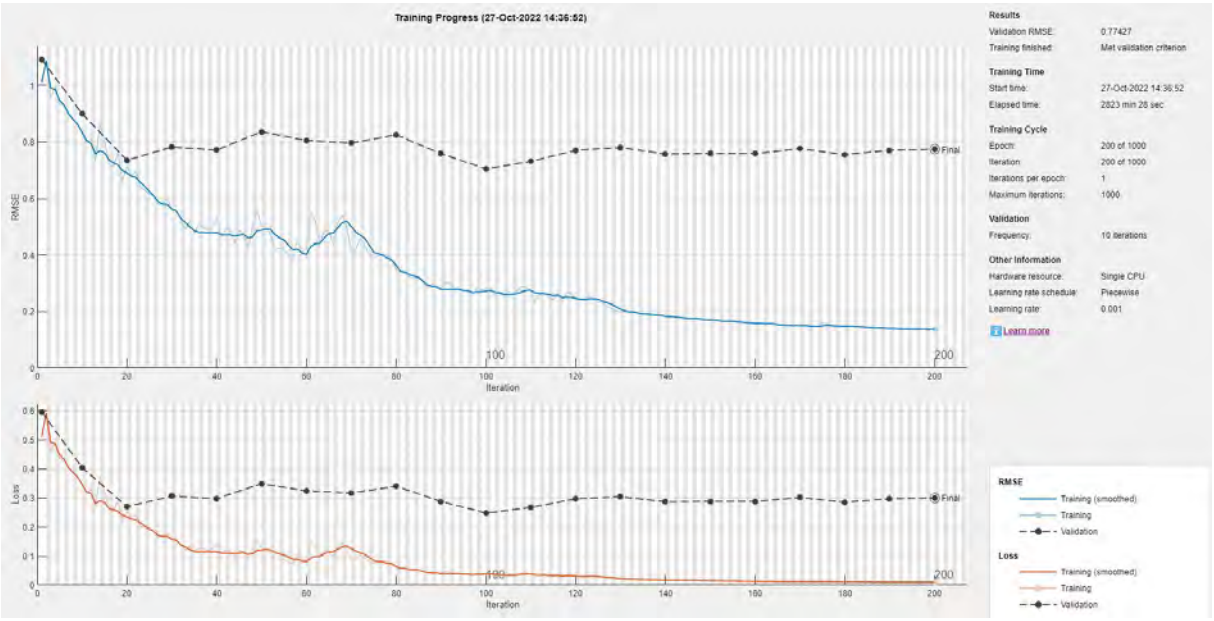


Figure.51 training results of LSTM3.

We believe that NARX models in general faces difficulties dealing with multi dynamical systems. In studies such as [170][171], the NARX model, on its own, was not enough in systems that change its dynamics and it was employed in a hybrid manner. A possible hypothesis that might describe this underperformance of the NARX is linked to the absence of hidden states or any mean that enables the networks to extract the effect of a triggering factor that sets the boundaries between different dynamics. In addition to the fact that unmodified NARX models tend to fit the whole database into a single nonlinear relationship that describes the output.

5.5.1 HIL limitation

Hardware in loop testing for the LSTM has not been proceeded in this research. The protocols of implementing the LSTM model in the Simulink environment is still in its infancy. The only way to execute it within the MG same model environment is to use the stateful predict block that supports LSTM only in a mat file version. Storing the time series object in mat file make it impossible for code generators to extract the function of the network and generate the C code needed for running the LSTM on the real-time target or external micro controller.

Other alternatives to construct an LSTM network exist of course. Popular cases use python scripts for example. However, and at any rate, the exploration of the best tool to write the LSTM script for this specific application in addition to investigating the network performance on embedded system and the compatibility for real time applications were out of the scope of this work in the current phase. Inevitably, these research orientations will be added to the perspectives of the following projects.

5.6 Discussion and Conclusions

The experimental results of this work suggest that trained NARX models do not experience performance degradation when embedded in microcontrollers. On the other hand, it is very important to note that the network in question was of small size and the implementation on the microcontroller did not include offline training or any tuning or adjusting of weights and biases of any sort.

Adaptive methods through which the ANN continue learning during the online execution are not suited for attack detection application. A continuous learning will make the network assume that all encountered scenarios are normal and subsequently not distinguishing anomalies.

The simplicity of the exploited ANN architecture in terms of computing resources, deployment and training objectives had made the development of the detection method feasible for Real-time implementation and hence, practical application. Especially when a criterion such as speed of convergence in extremely small step sized simulations was not regarded in the online phase.

However, the NARX models have encountered their limits when testing on control systems that employ different modalities for battery behaviour. These limitations have been alleviated using another type of RNNs, those being, LSTM models.

Signals in the frequency domain representation may indeed contain more information about the events and the signature of the different load appliances and generation sources [172]. That in turn, would help to provide an enhanced version of the detection mechanism. However, applying frequency domain transformations (such as Short Time Fourier Transform) in real-time constraints, in addition to the probable need to use 2-D signal filtering techniques (i.e., image processing) and to add convolutional layers to the employed ANN, would require a bigger computational capacity and hence higher expenses. Not to mention conservations about the exposure of personal user data that many consider as a confidentiality boundary not to be violated.

General conclusions and perspectives

As a result of the increasing reliance on Renewable Energy Sources (RES) in the power supply chain, smart grids will have to be at the top of their performance to optimize the grid capacity. Intelligent features provided by these new grids will have to adapt to the rising challenges enabling an intelligent management of real-time coordination among producers, consumers and storage facilities [9][10][11].

The fusion of the communication and information technology with legacy systems is introducing a new range of challenges that grid operators need to deal with. Cyber-physical attacks that come as an attribute of upgrading the grid with an intensive deployment of intelligent mechanisms would require additional consideration, especially on the scale of distributed resources that penetrate the grid with physically accessible production meters [173].

However, research that deals with a critical issue such as the electrical power data system security enhancement is still quite scant and produces rather primitive results, in comparison with the outcome and resources that have been dedicated to robust the security of the traditional power system [174].

Particularly, with hardware not having the flexibility found in software/firmware when updating patches, the choice of upgrading the entire hardware components of the grid to a more ‘secured’ version is simply not feasible. This procedure will include higher costs for labour and martial replacement, not to mention the difficulty to deal with different parts of the systems assets that were added to the Cyber physical structure in an ad-hoc way [14].

Cybersecurity measures for energy systems still come as accessory and not as a built-in function. For most of its parts, the electricity-related equipment that evolved at an exponential rate makes it extremely difficult for cyber defences’ mechanisms to keep pace with this development in the absence of up-to-date standards and common market trends. Securing the smart grid requires a multidisciplinary approach, and economic and social development are usually forgotten or neglected aspects in this process. Even the most remarkable technology inventions are useless without being approved by clients.

When the security aspect of the smart grid components is overlooked, the risk of unintentional faults or malicious attacks that could trigger undesired events is multiplied. Especially at the early stages of design and deployment before the problem gets more challenging when billions of devices with security vulnerabilities are added at once. leading us to the conclusion that working locally addressing smart grid building blocks is way more viable than bolting solutions that handle the whole system altogether.

One way to manage the lack of approach intersections, that faces researchers who addresses the security of smart grids from separate domains is through adopting the microgrid model. Microgrids play an important role in paving the way towards smart grids. To start with, microgrids are seen as collective nodes within the modern smart grid’s architecture. It is a network of small distributed electrical power

generators and local loads that operates under both local and central control. They support the tendency towards more decentralised energy systems and help with the integration of small to medium scale renewable generation.

By guaranteeing an ongoing real-time coordination between producers, consumers, and storage systems, microgrids enable intelligent energy management algorithms to be more efficient. The microgrid model is also a very convenient alternative to be consulted in research that tackles cyber-physical security owing to the relative simplicity in capturing and recording interventions, either as an injected attack or control modification. Above all, microgrids represent an attractive structure to be targeted by adversary attackers which might aim to perform malicious actions that lead to energy theft, data leaking, or even damaging physical infrastructures.

On the other hand, the full characterization of a widely adjustable microgrid in a way that enables the system operators to diagnose anomalies or eventually cyber-attacks is a complicated assignment. System identification for modern electrical or energy assemblies is a veritable challenge. However, security assessment of dynamic systems with highly non-linear characteristics that might even be difficult to access, or measure is a must. That classically included the ability to come up with mathematical models that define normal functioning behaviour. In which, these models were built on the basis of implementing statistical and stochastic approaches and then fine-tuned with the observable data from the real system [175].

There is no as simple recipe to follow for nonlinear system identification, with all available choices of model structure, model order, optimization algorithm and parameters. However, Artificial intelligence applications are a very effective tool when dealing with data-driven dynamics. They represent a valid substitute for using physical or mathematical models. And it is widely used in pattern recognition for a vast spectrum of fields including dynamic identification [143].

This work has introduced a real-time cyber-physical attack detection method for AC connected microgrids based on active power consumption. Where, we estimate the power exchanged between the microgrid and the utility grid in the normal functioning conditions using a special type of recurrent neural networks (the NARX model). The estimation is built on real values of active kilowatts produced or consumed by the microgrid components. In this sense, expanding deviations between predicted and real signal refers to the presence of an attack. The developed method can detect different types of attacks including False Data Injection FDI and replay attacks. The performance of the proposed approach was evaluated, and the advantages and drawbacks were highlighted.

For that to be done, we closely examined the existing approaches to address the cyber-physical security in power systems with focusing on microgrids.

Recent papers have gone through securing the cyber-physical structure of the microgrid from different standpoints. Preliminary efforts probing cyber-attacks against the power systems would usually treat these attacks as a sort of noise or disturbance. So, they tried their best to eliminate these disturbances using filtration techniques [74][75].

After that, researchers started dealing with what seems to be the most encountered types of attacks. Those were: attacks that jeopardize the system availability (denial of service attacks DoS) and those which target the system integrity (False data Injection FDI attacks).

DoS events provoke multiple issues without a doubt, but at the same time, they are easily detected by the system operator, which will probably recognize in an adequate rapidity that it is under attack. Similarly, the superior severity of the FDI attacks is largely attributed to the detection method's complexity and variability upon the adopted control structure [73].

Attack modelling in this work have taken into consideration both types of attacks in addition to developing the tests in a way that include the two dimensions of introducing an attack of the cyber and physical levels.

A Hardware-In-the Loop (HIL) validation of the cyber-physical attack detection method based on Real time simulation was also deployed in this work. The performance of the embedded AutoRegressive eXogenous Neural Network NARX on the microcontroller board was investigated and results that demonstrate the effectiveness of the proposed method were presented and compared with previous simulation outcomes.

Results of this phase came to confirm that the performance of the online trained NARX embedded on the microcontroller (Arduino Mega 2560) has not declined. However, these conclusions had been made under the condition that the resulted network happens to be of a small size and more significantly, no online training or network adjustment on the microcontroller board was involved.

This corresponds to the fact that methods that apply adaptive learning throughout the online execution are unsuitable for use in an attack detection application. since that continuous learning causes the network to assume that all encountered scenarios are normal, making it incapable of distinguishing anomalies.

In contrast to most Data-driven methods that use recorded measured process data, the training signals in this work was not subjected to any external or preliminary processing. At the same time, the events were planned and generated manually for the purpose of capturing all possible operational cases in an optimized database.

The simplicity of the exploited ANN architecture in terms of computing resources, deployment and training objectives had made the development of the detection method feasible for Real-time

implementation and hence, practical application. Especially when a criterion such as speed of convergence in extremely small step sized simulations was not regarded in the online phase.

However, certain limitations were encountered during this research, starting with the nature of neural networks in general. Being a black-box, NARX models do not necessarily interpret correctly the real dynamics of the given system [12] [13].

Moreover, choosing the best network is not done automatically as there is no reliable indicator that could suggest the required training repetition. Ameliorating training results, which are the most commonly adopted criteria among researchers dealing with neural networks do not always, correspond to better estimation. Multiple training will produce different results due to different initial conditions and sampling which are set randomly making it nearly impossible to reproduce the desired network at the same accuracy. Not to mention that networks with better or even identical MSE, R-values are never guaranteed to deliver an enhanced or matching performance. The thing that could be associated with problems that are hard to diagnose like overfitting for example.

Moving on to more method-related limitations, when investigating more elaborated control systems with different modalities for battery behaviour, the NARX model has met its limits. This in turn has motivated us to go after a more elaborated model of the recurrent neural network (the Long Short Term Memory LSTM model). These new structures were used to prob the aforementioned limits with the ability to capture events that develop on a multi-time scale, which eventually proved its effectiveness in this particular case.

Working on synthetic simulation data might give an indication on how adequate a given method can be for the desired application. However, interference from the external environment, such as the existence of normal system faults and noise will make the pilot phase of any simulated product suffers from a lack of integrability into the actual working condition.

That’s why perspectives of this work include the utilization of a more realistic database collected from the Lab microgrid installation for a double validation. Consequently, continue exploring the LSTM model in HIL tests using adapted microcontrollers. It is also envisaged to use the Multi Support Vector Machine MSVM to detect the compromised unit based on the error signal calculated between the real and the estimated output of the ANN (Estimated Ppcc).

More sophisticated case studies will also be probed in the perspectives of this work. This will include cases were the control system of the microgrid is a function of more diverse factors such as dynamic pricing indexes, curtailment situations when microgrids are required to switch to islanded modes, in addition to the possibility of introducing a more complex mixture of distributed generation and load units.

Theoretical exploration of the reasons behind the drawback of the NARX model under certain case studies could also be seen as a possible direction to resume this work. This comes from the observation of a trivial number of resources found that explains the limitation of these neural networks when dealing with multi dynamical systems.

In the last chapter (chapter 5), we shortly went through the preference of using the time over frequency domain. Claiming that the more details offered by the frequency transformations would come at the expense of needing more computational capacity which will reflect adversely on the real-time implementation of the method. Not to mention the additional concerns in relation to the problem of personal data infiltration, and confidentiality requirements that users of smart metering infrastructure are highly vigilant about these days.

The non-intrusive load monitoring techniques that are coupled with smart meters to boost their capabilities to analyse the contributions of each home appliance of the total energy load based on their energy consumption signatures, is another project proposal from our team. This newly explored functionality also offers a pathway to link both approaches to work together. Where the detection of the attacks might come as a second phase after the classification of the activities inside a microgrid.

At the end, it is important to mention that this work paved the way for another Interreg project (CO2Inno : *Laboratoire vivant pour une région d'innovation pilote neutre en CO2 – Développement de solutions énergétiques et de mobilité*). In which we will continue to work on the cyber-physical security aspects in a more multi-sectoral approach side by side with our partners from the University of Khel and Karlsruhe Institute of Technology. Our work package will address the construction of a simulation model of a realistic MG integrating the components of the living laboratory in order to test cyber-attack scenarios in complete security. In addition to gathering detailed information about the security aspects of current smart meters and analysing the market and country trends with respect to the adaptation of different information acquisition policies. Regulatory update on the integration of cyber-physical security in energy systems. Besides offering a regulatory update on the integration of cyber-physical security in energy systems that already have been initiated with the Interreg project that fo<unded this work (RES-TMO). Finally, the Evaluation of the social acceptability of smart infrastructure and the increased use of connected objects will also be provided through the course of this new project.

References

[1] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Comput. Electr. Eng.*, vol. 67, pp. 469–482, 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[2] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” *Comput. Networks*, vol. 57, no. 5, pp. 1344–1371, 2013, doi: 10.1016/j.comnet.2012.12.017.

[3] R. Leszczyna, “Standards on cyber security assessment of smart grid,” *Int. J. Crit. Infrastruct. Prot.*, vol. 22, no. September, pp. 70–89, 2018, doi: 10.1016/j.ijcip.2018.05.006.

[4] E. Hossain, Z. Han, and H. V. Poor, “Communication architectures and models for smart grid,” Cambridge, UK: Cambridge University Press, 2012.

[5] G. Prettico, M. G. Flammini, N. Andreadou, S. Vitiello, G. Fulli, and M. Masera, “Distribution System Operators observatory 2018: Overview of the electricity distribution system in Europe,” 2019.

[6] G. Prettico, G., Gangale, F., Mengolini, A., Lucas, A., & Fulli, “Distribution system operators from European electricity distribution systems to representative distribution networks,” Rep. Luxemb., 2018.

[7] M. Yazdanian and A. Mehrizi-Sani, “Distributed Control Techniques in Microgrids,” *IEEE Trans. Smart Grid*, pp. 1–9, 2014, doi: 10.1016/B978-0-08-101753-1.00002-4.

[8] O. Majeed, M. Zulqarnain, and T. Majeed, “Recent advancement in smart grid technology : Future prospects in the electrical power network,” *Ain Shams Eng. J.*, vol. 12, no. 1, pp. 687–695, 2021, doi: 10.1016/j.asej.2020.05.004.

[9] S. Li, M. Fairbank, C. Johnson, D. C. Wunsch, E. Alonso, and J. L. Proao, “Artificial neural networks for control of a grid-Connected rectifier/inverter under disturbance, dynamic and power converter switching conditions,” *IEEE Trans. Neural Networks Learn. Syst.*, vol. 25, no. 4, pp. 738–750, 2014, doi: 10.1109/TNNLS.2013.2280906.

[10] J. J. Q. Yu, Y. Hou, A. Y. S. Lam, and V. O. K. Li, “Intelligent fault detection scheme for microgrids with wavelet-based deep neural networks,” *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1694–1703, Mar. 2019, doi: 10.1109/TSG.2017.2776310.

[11] P. H. A. Barra, D. V. Coury, and R. A. S. Fernandes, “A survey on adaptive protection of microgrids and distribution systems with distributed generators,” *Renewable and Sustainable Energy Reviews*, vol. 118. Elsevier Ltd, Feb. 01, 2020. doi: 10.1016/j.rser.2019.109524.

[12] L. Marinos, *EU CYBERSECURI TY MARKET ANALYSIS EU CYBERSECURITY IoT in Distribution Grids*, no. April. 2022.

[13] Energy Expert Cyber Security Platform, “Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,” *EECSP Rep.*, no. February, p. 74, 2017.

[14] J. Wurm *et al.*, “Introduction to Cyber-Physical System Security: A Cross-Layer Perspective,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 3, no. 3, pp. 215–227, 2017, doi: 10.1109/TMSCS.2016.2569446.

[15] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014, doi: 10.1109/TSG.2014.2298195.

[16] M. Chlela, “Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers,”

McGill University Montréal, 2017.

[17] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Elsevier Inc., 2013. doi: 10.1016/C2012-0-01113-1.

[18] G. ASSENZA and R. SETOLA, "Operational technology cybersecurity How vulnerable is our critical infrastructure?," *Contemp. Maced. Defense/Sovremena Makedon. Odbrana*, vol. 19, no. 37, 2019, Accessed: Jan. 19, 2022. [Online]. Available: http://www.morm.gov.mk/sovremena-makedonska-odbrana/

[19] A. Albarakati *et al.*, "Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management," *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 1641–1653, Mar. 2022, doi: 10.1109/TII.2021.3082079.

[20] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, no. December 2017, pp. 45–56, 2018, doi: 10.1016/j.ijepes.2017.12.020.

[21] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[22] M. Rekik, Z. Chtourou, C. Gransart, and A. Atieh, "A Cyber-Physical Threat Analysis for Microgrids," in *2018 15th International Multi-Conference on Systems, Signals & Devices (SSD)*, 2018, pp. 731–737.

[23] Y. Cai and T. C. Y. L. Y. Huang, "Cascading Failure Analysis Considering Interaction Between Power Grids and Communication Networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016, doi: 10.1109/TSG.2015.2478888.

[24] X. G. and Y. L. Haiyan Zhang, Minfang Peng , Josep M. Guerrero, "Modelling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Interdependent Networks," 2019.

[25] A. Calder, *NIST Cybersecurity Framework: A Pocket Guide*. 2018.

[26] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," *Draft Interag. Rep. NISTIR*, vol. 7628, 2009.

[27] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103. 2018. doi: 10.1016/j.compind.2018.09.004.

[28] S. Huang, C. J. Zhou, S. H. Yang, and Y. Q. Qin, "Cyber-physical system security for networked industrial processes," *Int. J. Autom. Comput.*, vol. 12, no. 6, 2015, doi: 10.1007/s11633-015-0923-9.

[29] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 493–508, 2014, doi: 10.1109/JSYST.2013.2260697.

[30] V. Sklyar and V. Kharchenko, "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios," in *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*, 2019, vol. 2. doi: 10.1109/IDAACS.2019.8924452.

[31] D. Fooladivanda, Q. Hu, Y. H. Chang, and P. Sauer, "Secure State Estimation and Control for Cyber Security of AC Microgrids," 2019, [Online]. Available: http://arxiv.org/abs/1908.05843

[32] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–

169, 2013, doi: 10.1109/TSG.2012.2224391.

[33] I. Friedberg, D. Laverty, K. McLaughlin, and P. Smith, “A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation,” pp. 52–62, 2015, doi: 10.14236/ewic/ics2015.6.

[34] B. Hayes, *Distribution Generation Optimization and Energy Management*. Elsevier Inc., 2017. doi: 10.1016/B978-0-12-804208-3.00009-1.

[35] P. Baker, *Challenges facing distribution system operators in a decarbonised power system*. Regulatory Assistance Project (RAP), 2020. [Online]. Available: https://www.raponline.org/wp-content/uploads/2020/05/rap-baker-dso-challenges-june-2020-final.pdf (accessed 30 September 2020)

[36] J. F. Martins, A. G. Pronto, V. Delgado-Gomes, and M. Sanduleac, “Smart Meters and Advanced Metering Infrastructure,” *Pathways to a Smarter Power Syst.*, pp. 89–114, Jan. 2019, doi: 10.1016/B978-0-08-102592-5.00004-1.

[37] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, “State of the Art and Trends Review of Smart Metering in Electricity Grids,” *Appl. Sci.*, vol. 6, no. 3, pp. 1–24, 2016, doi: 10.3390/app6030068.

[38] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, “Energy meters evolution in smart grids: A review,” *J. Clean. Prod.*, vol. 217, pp. 702–715, 2019, doi: 10.1016/j.jclepro.2019.01.229.

[39] N. Efkarpidis, M. Geidl, H. Wache, M. Peter, and M. Adam, “Smart Metering Applications,” in *Lecture Notes in Energy*, vol. 88, Springer Science and Business Media Deutschland GmbH, 2022, pp. 13–124. doi: 10.1007/978-3-031-05737-3_3.

[40] X. Feng, A. Shekhar, F. Yang, R. E. Hebner, and P. Bauer, “Comparison of Hierarchical Control and Distributed Control for Microgrid,” *Electr. Power Components Syst.*, vol. 45, no. 10, pp. 1043–1056, 2017, doi: 10.1080/15325008.2017.1318982.

[41] B. Lasseter, “Microgrids [distributed power generation],” in *2001 IEEE Power Engineering Society Winter Meeting, PES 2001 - Conference Proceedings*, 2001, vol. 1, pp. 146–149. doi: 10.1109/PESW.2001.917020.

[42] F. Katiraei and M. R. Iravani, “Power management strategies for a microgrid with multiple distributed generation units,” *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1821–1831, 2006, doi: 10.1109/TPWRS.2006.879260.

[43] D. E. Olivares *et al.*, “Trends in microgrid control,” *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, 2014, doi: 10.1109/TSG.2013.2295514.

[44] P. Buason, H. Choi, A. Valdes, and H. J. Liu, “Cyber-physical systems of microgrids for electrical grid resiliency,” in *Proceedings - 2019 IEEE International Conference on Industrial Cyber Physical Systems, ICPS 2019*, 2019, pp. 492–497. doi: 10.1109/ICPHYS.2019.8780336.

[45] D. Ton, “DOE Microgrids Program Overview, Power Systems Engineering Research and Development,” 2015. [Online]. Available: http://microgrid-symposiums.org/wp-content/uploads/2015/09/15-Ton-Microgrids-and-Best-Practices-20150813.pdf

[46] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, “Distributed cooperative control of dc microgrids,” *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, 2015, doi: 10.1109/TPEL.2014.2324579.

[47] S. Liu, P. X. Liu, and X. Wang, “Effects of cyber attacks on islanded microgrid frequency control,” *Proc. 2016 IEEE 20th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2016*, pp. 461–464, 2016, doi: 10.1109/CSCWD.2016.7566033.

[48] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, “Synchrony in networked microgrids under attacks,” *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018, doi: 10.1109/TSG.2017.2721382.

[49] Y. Gao and Q. Ai, “A distributed coordinated economic droop control scheme for islanded AC microgrid considering communication system,” *Electr. Power Syst. Res.*, vol. 160, pp. 109–118, Jul. 2018, doi: 10.1016/J.EPSR.2018.02.008.

[50] N. Hussain, M. Nasir, J. C. Vasquez, and J. M. Guerrero, “Recent developments and challenges on AC microgrids fault detection and protection systems-a review,” *Energies*, vol. 13, no. 9. MDPI AG, May 01, 2020. doi: 10.3390/en13092149.

[51] S. Gholami, S. Saha, and M. Aldeen, “A cyber attack resilient control for distributed energy resources,” *2017 IEEE PES Innov. Smart Grid Technol. Conf. Eur. ISGT-Europe 2017 - Proc.*, vol. 2018-Janua, pp. 1–6, 2017, doi: 10.1109/ISGTEurope.2017.8260213.

[52] J. Hao *et al.*, “An Adaptive Markov Strategy for Defending Smart Grid False Data Injection from Malicious Attackers,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2398–2408, 2018, doi: 10.1109/TSG.2016.2610582.

[53] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, “Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017, doi: 10.1109/TSG.2016.2622289.

[54] Y. Isozaki *et al.*, “Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids with PVs,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2016, doi: 10.1109/TSG.2015.2427380.

[55] A. D. Domínguez-Garcia, C. N. Hadjicostis, and N. H. Vaidya, “Resilient networked control of distributed energy resources,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1137–1148, 2012, doi: 10.1109/JSAC.2012.120711.

[56] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, “Cybersecurity for distributed energy resources and smart inverters,” *IET Cyber-Physical Syst. Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016, doi: 10.1049/iet-cps.2016.0018.

[57] A. Farraj, E. Hammad, and D. Kundur, “A systematic approach to delay-Adaptive control design for smart grids,” *2015 IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2015*, pp. 768–773, 2016, doi: 10.1109/SmartGridComm.2015.7436394.

[58] A. Farraj, E. Hammad, and D. Kundur, “A cyber-physical control framework for transient stability in smart grids,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, 2018, doi: 10.1109/TSG.2016.2581588.

[59] A. Farraj, E. Hammad, and D. Kundur, “Enhancing the performance of controlled distributed energy resources in noisy communication environments,” *Can. Conf. Electr. Comput. Eng.*, vol. 2016-Octob, 2016, doi: 10.1109/CCECE.2016.7726806.

[60] P. Mercier, R. Cherkaoui, and A. Oudalov, “Optimizing a battery energy storage system for frequency control application in an isolated power system,” *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1469–1477, 2009, doi: 10.1109/TPWRS.2009.2022997.

[61] A. K. Farraj, E. M. Hammad, and D. Kundur, “A cyber-enabled stabilizing controller for resilient smart grid systems,” *2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2015*, pp. 1–10, 2015, doi: 10.1109/ISGT.2015.7131838.

[62] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, “A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control,” *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, 2014, doi: 10.1109/TSG.2014.2341211.

[63] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, “Novel Detection Scheme Design Considering Cyber Attacks on Load Frequency Control,” *IEEE Trans. Ind. Informatics*, vol. 14, no. 5, pp. 1932–1941, 2018, doi: 10.1109/TII.2017.2765313.

[64] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “A robust policy for automatic generation control cyber attack in two area power network,” *Proc. IEEE Conf. Decis. Control*, pp. 5973–5978, 2010, doi: 10.1109/CDC.2010.5717285.

[65] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “Cyber attack in a two-area power system: Impact identification using reachability,” *Proc. 2010 Am. Control Conf. ACC 2010*, pp. 962–967, 2010, doi: 10.1109/acc.2010.5530460.

[66] A. Sargolzaei, K. Yen, and M. N. Abdelghani, “Delayed inputs attack on load frequency control in smart grid,” *2014 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2014*, 2014, doi: 10.1109/ISGT.2014.6816508.

[67] C. Li, C. Cao, Y. Cao, Y. Kuang, L. Zeng, and B. Fang, “A review of islanding detection methods for microgrid,” *Renewable and Sustainable Energy Reviews*, vol. 35. Elsevier Ltd, pp. 211–220, 2014. doi: 10.1016/j.rser.2014.04.026.

[68] D. M. Tagare, “Interconnecting Distributed Resources with Electric Power Systems,” *Electr. Power Gener.*, pp. 301–313, Jan. 2011, doi: 10.1002/9780470872659.CH15.

[69] Y. Liu, S. Hu, and T. Y. Ho, “Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks,” *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, vol. 2015-January, no. January, pp. 183–190, Jan. 2015, doi: 10.1109/ICCAD.2014.7001350.

[70] O. Arias, J. Wurm, K. Hoang, and Y. Jin, “Privacy and Security in Internet of Things and Wearable Devices,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Jun. 2015, doi: 10.1109/TMSCS.2015.2498605.

[71] M. M. Rana, L. Li, and S. W. Su, “Cyber attack protection and control of microgrids,” *IEEE/CAA J. Autom. Sin.*, vol. 5, no. 2, pp. 602–609, 2018, doi: 10.1109/JAS.2017.7510655.

[72] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, 2014, doi: 10.1109/TCNS.2014.2357531.

[73] S. Liu, X. Wang, and P. X. Liu, “Impact of Communication Delays on Secondary Frequency Control in an Islanded Microgrid,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2021–2031, 2015, doi: 10.1109/TIE.2014.2367456.

[74] E. Hammad, A. Farraj, and D. Kundur, “Fundamental limits on communication latency for distributed control via electromechanical waves,” in *IEEE International Conference on Communications*, 2017, pp. 0–5. doi: 10.1109/ICC.2017.7996942.

[75] F. Guo *et al.*, “Comprehensive real-time simulation of the smart grid,” *IEEE Trans. Ind. Appl.*, vol. 49, no. 2, pp. 899–908, 2013, doi: 10.1109/TIA.2013.2240642.

[76] Y. Cai, Y. Li, Y. Cao, W. Li, and X. Zeng, “Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids,” *Int. J. Electr. Power Energy Syst.*, vol. 89, pp. 106–114, 2017, doi: 10.1016/j.ijepes.2017.01.010.

[77] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “STRIDE-based threat modeling for cyber-physical systems,” in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings*, 2017, vol. 2018-Janua, pp. 1–6. doi: 10.1109/ISGTEurope.2017.8260283.

[78] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “IEEE C37.118-2 synchrophasor

communication framework: Overview, cyber vulnerabilities analysis and performance evaluation," in *ICISSP 2016 - Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2016, pp. 167–176. doi: 10.5220/0005745001670178.

[79] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, 2016, doi: 10.1109/TSG.2015.2499766.

[80] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *IEEE Power and Energy Society General Meeting*, Nov. 2016, vol. 2016-Novem. doi: 10.1109/PESGM.2016.7741343.

[81] J. Zhao, L. Mili, and M. Wang, "A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, 2018, doi: 10.1109/TPWRS.2018.2794468.

[82] S. Sahoo, S. Mishra, J. C. H. Peng, and T. Dragicevic, "A Stealth Cyber-Attack Detection Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, 2019, doi: 10.1109/TPEL.2018.2879886.

[83] H. Haes Alhelou, M. E. Hamedani Golshan, and N. D. Hatziargyriou, "Deterministic Dynamic State Estimation-Based Optimal LFC for Interconnected Power Systems Using Unknown Input Observer," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1582–1592, 2020, doi: 10.1109/TSG.2019.2940199.

[84] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting False Data Injection Attacks in AC State Estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015, doi: 10.1109/TSG.2015.2388545.

[85] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 21–32. doi: 10.1109/TSG.2018.2813280.

[86] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," *2010 1st IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2010*, pp. 1–6, 2010, doi: 10.1109/smartgrid.2010.5622046.

[87] Q. Hu, D. Fooladivanda, Y. H. Chang, and C. J. Tomlin, "Secure State Estimation and Control for Cyber Security of the Nonlinear Power Systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, doi: 10.1109/TCNS.2017.2704434.

[88] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, "Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids," in *2018 European Control Conference, ECC 2018*, Nov. 2018, pp. 344–349. doi: 10.23919/ECC.2018.8550549.

[89] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "Detection of False Data Injection Cyber-Attacks in DC Microgrids based on Recurrent Neural Networks," *IEEE J. Emerg. Sel. Top. Power Electron.*, pp. 1–1, 2020, doi: 10.1109/jestpe.2020.2968243.

[90] S. Sahoo, J. C. H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On Detection of False Data in Cooperative DC Microgrids - A Discordant Element Approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, 2020, doi: 10.1109/TIE.2019.2938497.

[91] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," *IEEE Trans. Ind. Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017, doi: 10.1109/TII.2017.2656905.

[92] T. V. Vu, B. H. L. Nguyen, T. A. Ngo, M. Steurer, K. Schoder, and R. Hovsapian, "Distributed Optimal Dynamic State Estimation for Cyber Intrusion Detection in Networked DC Microgrids," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics*

Society, 2019, pp. 4050–4055. doi: 10.1109/iecon.2019.8927045.

[93] Q. Jiao, H. Modares, F. L. Lewis, S. Xu, and L. Xie, “Distributed ℋ2-gain output-feedback control of homogeneous and heterogeneous systems,” *Automatica*, vol. 71, pp. 361–368, 2016, doi: 10.1016/j.automatica.2016.04.025.

[94] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, “Distributed Load Sharing under False Data Injection Attack in an Inverter-Based Microgrid,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, 2019, doi: 10.1109/TIE.2018.2793241.

[95] S. X. Ding, *Model-based fault diagnosis techniques: Design schemes, algorithms, and tools*. 2008. doi: 10.1007/978-3-540-76304-8.

[96] Z. Gao, C. Cecati, and S. X. Ding, “A survey of fault diagnosis and fault-tolerant techniques-part I: Fault diagnosis with model-based and signal-based approaches,” *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6. 2015. doi: 10.1109/TIE.2015.2417501.

[97] H. Chen, L. Li, C. Shang, and B. Huang, “Fault Detection for Nonlinear Dynamic Systems With Consideration of Modeling Errors: A Data-Driven Approach,” *IEEE Trans. Cybern.*, vol. PP, pp. 1–11, 2022, doi: 10.1109/TCYB.2022.3163301.

[98] J. Bélanger, P. Venne, and S. Member, “The What , Where and Why of Real-Time Simulation,” pp. 37–49.

[99] K. L. Lian, S. Member, and P. W. Lehn, “Real-Time Simulation of Voltage Source Converters Based on Time Average Method,” vol. 20, no. 1, pp. 110–118, 2005.

[100] H. Dommel, “Digital Computer Solution of Electromagnetic Transients in Single-and Multiphase Networks,” *IEEE Trans. Power Appar. Syst.*, vol. PAS-88, no. 4, pp. 388–399, 1969, doi: 10.1109/tpas.1969.292459.

[101] J. J. Sanchez-Gasca, R. D’Aquila, W. W. Price, and J. J. Paserba, “Variable time step, implicit integration for extended-term power system dynamic simulation,” in *IEEE Power Industry Computer Applications Conference*, 1995. doi: 10.1109/pica.1995.515182.

[102] C. D. Bodemann and F. De Rose, “55th International Astronautical Congress 2004 - Vancouver, Canada IAC-04-U.3.B.03 The successful usage of Matlab SIMULINK in the framework of ESA’s ATV project Christian D. Bodemann, Filippo De Rose,” 2004.

[103] R. AhmadiAhangar, A. Rosin, A. N. Niaki, I. Palu, and T. Korõtko, “A review on real-time simulation and analysis methods of microgrids,” *Int. Trans. Electr. Energy Syst.*, vol. 29, no. 11, 2019, doi: 10.1002/2050-7038.12106.

[104] S. R. Mangesh Kale, Narayani Ghatwai, “Processor-In-Loop Simulation: Embedded Software Verification & Validation In Model Based Development.” https://www.design-reuse.com/articles/42548/embedded-software-verification-validation-in-model-based-development.html (accessed Dec. 18, 2022).

[105] “What are MIL, SIL, PIL, and HIL, and how do they integrate with the Model-Based Design approach? - MATLAB Answers - MATLAB Central.” https://fr.mathworks.com/matlabcentral/answers/440277-what-are-mil-sil-pil-and-hil-and-how-do-they-integrate-with-the-model-based-design-approach (accessed Dec. 19, 2022).

[106] S. Y. Shin, K. Chaouch, S. Nejati, M. Sabetzadeh, L. C. Briand, and F. Zimmer, “Uncertainty-aware specification and analysis for hardware-in-the-loop testing of cyber-physical systems,” *J. Syst. Softw.*, vol. 171, 2021, doi: 10.1016/j.jss.2020.110813.

[107] A. Yamane, S. Abourida, Y. Bouzid, and F. Tempez, “Real-Time Simulation of Distributed Energy Systems and Microgrids,” *IFAC-PapersOnLine*, vol. 49, no. 27, pp. 183–187, 2016, doi: 10.1016/j.ifacol.2016.10.680.

[108] W. Li, G. Joós, and J. Bélanger, “Real-time simulation of a wind turbine generator coupled with a battery supercapacitor energy storage system,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 4, pp. 1137–1145, Apr. 2010, doi: 10.1109/TIE.2009.2037103.

[109] C. Dufour, J. Mahseredjian, and J. Bélanger, “A combined state-space nodal method for the simulation of power system transients,” *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 928–935, Apr. 2011, doi: 10.1109/TPWRD.2010.2090364.

[110] J. R. Marti, “Accurate modelling of frequency-dependent transmission lines in electromagnetic transient simulations,” *IEEE Trans. Power Appar. Syst.*, vol. PAS-101, no. 1, pp. 147–157, 1982, doi: 10.1109/TPAS.1982.317332.

[111] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, “Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?,” *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4775–4786, 2018, doi: 10.1109/TPWRS.2018.2818746.

[112] E. Hammad, M. Ezeme, and A. Farraj, “Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification,” *Int. J. Electr. Power Energy Syst.*, vol. 104, no. March 2018, pp. 817–826, 2019, doi: 10.1016/j.ijepes.2018.07.058.

[113] A. M. Kosek, O. Lünsdorf, S. Scherfke, O. Gehrke, and S. Rohjans, “Evaluation of smart grid control strategies in co-simulation - Integration of IPSYS and mosaik,” *Proc. - 2014 Power Syst. Comput. Conf. PSCC 2014*, Feb. 2014, doi: 10.1109/PSCC.2014.7038479.

[114] L. Duchesne, E. Karangelos, and L. Wehenkel, “Recent Developments in Machine Learning for Energy Systems Reliability Management,” *Proc. IEEE*, vol. 108, no. 9, 2020, doi: 10.1109/JPROC.2020.2988715.

[115] D. Bzdok, N. Altman, and M. Krzywinski, “Statistics versus machine learning,” *Nat. Methods*, vol. 15, no. 4, 2018, doi: 10.1038/nmeth.4642.

[116] S. Chatzivasileiadis, A. Venzke, J. Stiasny, and G. Misyris, “Machine Learning in Power Systems: Is It Time to Trust It?,” *IEEE Power Energy Mag.*, vol. 20, no. 3, pp. 32–41, 2022, doi: 10.1109/MPE.2022.3150810.

[117] M. Mohatram and P. Tewari, “Applications of Artificial Neural Networks in Electric Power Industry: A Review,” *Int. J. Electr. Eng.*, vol. 4, no. 2, 2011.

[118] S. Basodi, S. Tan, W. Z. Song, and Y. Pan, “Data integrity attack detection in smart grid: A deep learning approach,” *Int. J. Secur. Networks*, vol. 15, no. 1, 2020, doi: 10.1504/IJSN.2020.106506.

[119] X. Niu, J. Li, J. Sun, and K. Tomsovic, “Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning,” *2019 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2019*, Feb. 2019, doi: 10.1109/ISGT.2019.8791598.

[120] Y. Zhang, J. Wang, and B. Chen, “Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach,” *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021, doi: 10.1109/TSG.2020.3010510.

[121] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, “Intelligent anomaly identification in cyber-physical inverter-based systems,” *Electr. Power Syst. Res.*, vol. 193, no. January, p. 107024, 2021, doi: 10.1016/j.epsr.2021.107024.

[122] B. Wang, B. Fang, Y. Wang, H. Liu, and Y. Liu, “Power System Transient Stability Assessment Based on Big Data and the Core Vector Machine,” *IEEE Trans. Smart Grid*, vol. 7, no. 5, 2016, doi: 10.1109/TSG.2016.2549063.

[123] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, “Sparse attack

construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, 2013, doi: 10.1109/JSAC.2013.130713.

[124] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011, doi: 10.1109/TSG.2011.2163807.

[125] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, 2011, doi: 10.1145/1952982.1952995.

[126] R. Sabzehgar, D. Z. Amirhosseini, and M. Rasouli, "Solar power forecast for a residential smart microgrid based on numerical weather predictions using artificial intelligence methods," *J. Build. Eng.*, vol. 32, no. December 2019, p. 101629, 2020, doi: 10.1016/j.jobe.2020.101629.

[127] S. S. Nuchhi, R. B. Sali, and S. G. Ankaliki, "Effect Of Reactive Power Compensation On Voltage Profile," vol. 2, no. 6, pp. 2627–2634, 2013, Accessed: Nov. 02, 2020. [Online]. Available: https://www.researchgate.net/publication/282003559

[128] S. S. Soman, H. Zareipour, S. Member, O. Malik, and L. Fellow, "A Review of Wind Power and Wind Speed Forecasting Methods With Different Time Horizons," in *North American Power Symposium 2010*, 2010, pp. 1–8. [Online]. Available: papers3://publication/uuid/01A9077B-50C8-47AB-9F17-B4E94F80DFDF

[129] G. Abbas, M. Nawaz, and F. Kamran, "Performance Comparison of NARX & RNN - LSTM Neural Networks for LiFePO4 Battery State of Charge Estimation," *2019 16th Int. Bhurban Conf. Appl. Sci. Technol.*, pp. 463–468.

[130] I. Sutskever, "Training Recurrent Neural Networks," University of Toronto, 2013.

[131] A. Takiddin, M. Ismail, and E. Serpedin, "Detection of Electricity Theft False Data Injection Attacks in Smart Grids," pp. 1541–1545, 2022.

[132] P. L. Lai and C. Fyfe, "A neural implementation of canonical correlation analysis," *Neural Networks*, vol. 12, no. 10, 1999, doi: 10.1016/S0893-6080(99)00075-1.

[133] J. A. Anderson, P. Allopenna, D. Ascher, T. Au, J. Benello, and D. Bennett, "An Introduction to Neural Networks . Acknowledgments," 1995.

[134] A. A. Alsumaiei, "A nonlinear autoregressive modeling approach for forecasting groundwater level fluctuation in urban aquifers," *Water (Switzerland)*, vol. 12, no. 3, pp. 1–16, 2020, doi: 10.3390/w12030820.

[135] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," *Proc. IEEE Int. Symp. High Assur. Syst. Eng.*, pp. 140–145, 2017, doi: 10.1109/HASE.2017.36.

[136] H. I. Fawaz *et al.*, "Deep learning for time series classification : a review To cite this version : HAL Id : hal-02365025 Deep learning for time series classification : a review," 2020.

[137] S. S. Haykin, "Neural networks and learning machines/Simon Haykin." New York: Prentice Hall, 2009.

[138] M. Yu, X. Tang, Y. Lin, and X. Wang, "Diesel engine modeling based on recurrent neural networks for a hardware-in-the-loop simulation system of diesel generator sets," *Neurocomputing*, vol. 283, pp. 9–19, Mar. 2018, doi: 10.1016/j.neucom.2017.12.054.

[139] F. Rodríguez, A. M. Florez-Tapia, L. Fontán, and A. Galarza, "Very short-term wind power density forecasting through artificial neural networks for microgrid control," *Renew. Energy*, vol. 145, pp. 1517–1527, 2020, doi: 10.1016/j.renene.2019.07.067.

[140] N. U. Aningo, A. Hardy, and D. Glew, "Evaluating Solar Prediction Methods to Improve PV

Micro-grid Effectiveness Using Nonlinear Autoregressive Exogenous Neural Network (NARX NN)," in *Sustainable Ecological Engineering Design*, Cham: Springer International Publishing, 2020, pp. 363–376. doi: 10.1007/978-3-030-44381-8_28.

[141] A. G. Casaca de Rocha Vaz, "Photovoltaic Forecasting with Artificial Neural Network," *Fac. CIÊNCIAS\rDEPARTAMENTO Eng. GEOGRÁFICA, GEOFÍSICA E Energ.*, p. 86, 2014, [Online]. Available: http://repositorio.ul.pt/bitstream/10451/11405/1/ulfc107351_tm_Andre_Vaz.pdf

[142] S. Wen, Y. Wang, Y. Tang, Y. Xu, P. Li, and T. Zhao, "Real-Time Identification of Power Fluctuations Based on LSTM Recurrent Neural Network: A Case Study on Singapore Power System," *IEEE Trans. Ind. Informatics*, vol. 15, no. 9, pp. 5266–5275, 2019, doi: 10.1109/tii.2019.2910416.

[143] B. M. Brentan *et al.*, "On-Line Cyber Attack Detection in Water Networks through State Forecasting and Control by Pattern Recognition," *World Environ. Water Resour. Congr. 2017 Hydraul. Waterw. Water Distrib. Syst. Anal. - Sel. Pap. from World Environ. Water Resour. Congr. 2017*, pp. 583–592, 2017, doi: 10.1061/9780784480625.054.

[144] S. A. Taqvi, L. D. Tufa, H. Zabiri, A. S. Maulud, and F. Uddin, "Fault detection in distillation column using NARX neural network," *Neural Comput. Appl.*, vol. 32, no. 8, 2020, doi: 10.1007/s00521-018-3658-z.

[145] T. N. Pham, H. Trinh, and L. Van Hien, "Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 238–252, Jan. 2016, doi: 10.1109/TSG.2015.2449877.

[146] O. Djedidi and M. A. Djeziri, "Power profiling and monitoring in embedded systems: A comparative study and a novel methodology based on NARX neural networks," *J. Syst. Archit.*, vol. 111, no. May, p. 101805, 2020, doi: 10.1016/j.sysarc.2020.101805.

[147] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 415–427, 2012, doi: 10.1145/2382196.2382242.

[148] C. Liao, C. W. Ten, and S. Hu, "Strategic FRTU deployment considering cybersecurity in secondary distribution network," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1264–1274, 2013, doi: 10.1109/TSG.2013.2256939.

[149] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, 2014, doi: 10.1109/TSG.2013.2284438.

[150] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[151] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Physical Syst. Theory Appl.*, vol. 2, no. 4, 2017, doi: 10.1049/iet-cps.2017.0013.

[152] M. O. Faruque *et al.*, "Real-Time Simulation Technologies for Power Systems Design, Testing, and Analysis," *IEEE Power Energy Technol. Syst. J.*, vol. 2, no. 2, pp. 63–73, 2015, doi: 10.1109/JPETS.2015.2427370.

[153] Y. Zhang, J. Wang, and B. Chen, "Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021, doi: 10.1109/TSG.2020.3010510.

[154] C. Keerthisinghe and D. S. Kirschen, "Real-time digital simulation of microgrid control

strategies,” *2020 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2020*, pp. 1–5, 2020, doi: 10.1109/ISGT45199.2020.9087709.

[155] N. M. Mohsin, “Design of a Grid Connected Photovoltaic Power Electronic Converter,” *Uit*, vol. 1, no. 1, pp. 1–90, 2017, [Online]. Available: http://www.bioone.org/doi/abs/10.3159/10-RA-011.1

[156] “250-kW Grid-Connected PV Array - MATLAB & Simulink - MathWorks France.” https://fr.mathworks.com/help/physmod/sps/ug/250-kw-grid-connected-pv-array.html (accessed Sep. 11, 2022).

[157] L. Vanfretti, W. Li, A. Egea-Alvarez, and O. Gomis-Bellmunt, “Generic VSC-based DC Grid EMT modeling, simulation, and validation on a scaled hardware platform,” in *IEEE Power and Energy Society General Meeting*, 2015, vol. 2015-September. doi: 10.1109/PESGM.2015.7285979.

[158] L. Vanfretti, N. A. Khan, W. Li, M. R. Hasan, and A. Haider, “Generic VSC and low level switching control models for offline simulation of VSC-HVDC systems,” in *9th International: 2014 Electric Power Quality and Supply Reliability Conference, PQ 2014 - Proceedings*, 2014. doi: 10.1109/PQ.2014.6866825.

[159] T. Datta Chaudhuri and I. Ghosh, “Artificial Neural Network and Time Series Modeling Based Approach to Forecasting the Exchange Rate in a Multivariate Framework,” *Corresp. Author indranilg@calcuttabusinessschool.org J. Insur. Financ. Manag.*, vol. 1, pp. 92–123, 2016.

[160] H. T. Siegelmann, B. G. Horne, C. Lee Giles, and S. Member, “Computational Capabilities of Recurrent NARX Neural Networks,” 1997.

[161] T. N. Lin, C. Lee Giles, B. G. Home, and S. Y. Kung, “A delay damage model selection algorithm for narx neural networks,” *IEEE Trans. Signal Process.*, vol. 45, no. 11, pp. 2719–2730, 1997, doi: 10.1109/78.650098.

[162] F. Bonassi, M. Farina, and R. Scattolini, “Stability of discrete-time feed-forward neural networks in NARX configuration,” *IFAC-PapersOnLine*, vol. 54, no. 7, pp. 547–552, 2021, doi: 10.1016/j.ifacol.2021.08.417.

[163] T. Hong and P. Wang, “Artificial Intelligence for Load Forecasting: History, Illusions, and Opportunities,” *IEEE Power Energy Mag.*, vol. 20, no. 3, pp. 14–23, May 2022, doi: 10.1109/MPE.2022.3150808.

[164] F. Thams, A. Venzke, R. Eriksson, and S. Chatzivasileiadis, “Efficient Database Generation for Data-Driven Security Assessment of Power Systems,” *IEEE Trans. Power Syst.*, vol. 35, no. 1, 2020, doi: 10.1109/TPWRS.2018.2890769.

[165] N. M. Rezk, M. Purnaprajna, T. Nordstrom, and Z. Ul-Abdin, “Recurrent Neural Networks: An Embedded Computing Perspective,” *IEEE Access*, vol. 8, pp. 57967–57996, 2020, doi: 10.1109/ACCESS.2020.2982416.

[166] “Microcontroller I/O & ADC Benchmarks - Using Arduino / Microcontrollers - Arduino Forum.” https://forum.arduino.cc/t/microcontroller-i-o-adc-benchmarks/315304 (accessed Nov. 25, 2022).

[167] G. Abbas, M. Nawaz, and F. Kamran, “Performance Comparison of NARX RNN-LSTM Neural Networks for LiFePO4 Battery State of Charge Estimation,” in *Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019*, 2019. doi: 10.1109/IBCAST.2019.8667172.

[168] E. Terzi, F. Bonassi, M. Farina, and R. Scattolini, “Learning model predictive control with long short-term memory networks,” *Int. J. Robust Nonlinear Control*, vol. 31, no. 18, 2021, doi: 10.1002/rnc.5519.

[169] Y. Jung, J. Jung, B. Kim, and S. U. Han, “Long short-term memory recurrent neural network for modeling temporal patterns in long-term power forecasting for solar PV facilities: Case study of South Korea,” *J. Clean. Prod.*, vol. 250, 2020, doi: 10.1016/j.jclepro.2019.119476.

[170] M. Massaoudi *et al.*, “An Effective Hybrid NARX-LSTM Model for Point and Interval PV Power Forecasting,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3062776.

[171] B. Bhattacharyya, E. Jacquelin, and D. Brizard, “A Kriging–NARX Model for Uncertainty Quantification of Nonlinear Stochastic Dynamical Systems in Time Domain,” *J. Eng. Mech.*, vol. 146, no. 7, 2020, doi: 10.1061/(asce)em.1943-7889.0001792.

[172] M. Drouaz, B. Colicchio, A. Moukadem, A. Dieterlen, and D. Ould-Abdeslam, “New time-frequency transient features for nonintrusive load monitoring,” *Energies*, vol. 14, no. 5, 2021, doi: 10.3390/en14051437.

[173] H. Riggs, S. Tufail, M. Khan, I. Parvez, and A. I. Sarwat, “Detection of false data injection of PV production,” in *IEEE Green Technologies Conference*, Apr. 2021, vol. 2021-April, pp. 7–12. doi: 10.1109/GreenTech48523.2021.00012.

[174] A. Sanjab and W. Saad, “Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016, doi: 10.1109/TSG.2016.2550218.

[175] M. Gulin, M. Vasak, and T. Pavlovic, “Model identification of a photovoltaic system for a DC microgrid simulation,” in *16th International Power Electronics and Motion Control Conference and Exposition, PEMC 2014*, Dec. 2014, pp. 413–418. doi: 10.1109/EPEPEMC.2014.6980528.