Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers

By Martine Chlela

Department of Electrical & Computer Engineering

McGill University

Montréal, Canada

May 2017

A thesis submitted to McGill University in partial fulfillment of the requirements for the degree of Doctorate of Philosophy in Electrical Engineering

Abstract

Microgrids are constantly evolving to integrate more renewable generation, operate autonomously, provide continuous power supply to critical and high-value loads and offer advanced control capabilities necessitating the deployment of a communication infrastructure vulnerable to cyber intrusions. This thesis provides a cyber security analysis of microgrid systems and proposes novel cyber resilient control strategies to mitigate cyber-attacks. Benchmark systems are first developed to provide a basis for the cyber security analysis of diverse microgrid configurations operating based on different control strategies. Interest is attributed to cyber-attacks compromising the microgrid data integrity and availability, namely FDI and DoS/DDoS cyber-attacks. Mathematical models for the attacks are developed and performance indices are rigorously defined to provide a mean for cyber-attack physical impact quantification. The impact assessment results are then used to facilitate the proposition of novel mitigation strategies, to test their performance and evaluate their effectiveness in enhancing the resiliency and robustness of the microgrid control infrastructure to resist cyber intrusions. Enhanced supplementary control loops added at the primary and secondary control levels are proposed to provide attack compensation and post-attack recovery in the event of FDI cyber-attacks. A novel rule-based fallback control strategy is proposed to mitigate DoS/DDoS cyber-attacks and provide coordination amongst DERs in a partially or fully-decentralized manner. A multi-stage cyber resilient control infrastructure is then developed to embed cyber security into the microgrid's design to ensure resiliency, robustness and reliability in the event of cyber-attacks. A real-time HIL co-simulation platform modeling and interfacing the microgrid power system, information and communication network layers is presented and used to analyze the impact of cyber-attacks and to test and validate the effectiveness of the proposed cyber resilient mitigation strategies. Recommendations and best cyber security practices concluded from this work are also presented.

Résumé

Les microréseaux sont en constante évolution pour intégrer plus de production renouvelable, fonctionner de façon autonome, fournir une alimentation continue à des charges critiques et offrir des capacités de contrôle avancées nécessitant le déploiement d'une infrastructure de communication vulnérable aux intrusions cybernétiques. Cette thèse fournit une analyse complète de cybersécurité des systèmes de microréseau et propose de nouvelles stratégies de contrôle cyber-résilients pour mitiger les cyber-attaques. Des systèmes de référence sont d'abord développés pour fournir une base pour l'analyse de la cybersécurité de différentes configurations de microréseaux fonctionnant selon des stratégies de contrôle divers. L'intérêt est attribué aux cyber-attaques compromettant l'intégrité des données et la disponibilité du microréseau, à savoir les cyber-attaques FDI et DoS/DDoS. Des modèles mathématiques pour les attaques sont développés et les indicateurs de performance sont rigoureusement définies pour fournir un moyen de quantification de l'impact physique. Les résultats de l'analyse d'impact sont ensuite utilisés afin de faciliter la proposition de nouvelles stratégies de mitigation, tester leurs performances et évaluer leur efficacité pour améliorer la résilience et la robustesse de l'infrastructure de contrôle des microréseaux pour résister aux intrusions cybernétiques. Des boucles de contrôle supplémentaires ajoutées aux niveaux primaire et secondaire sont proposées pour fournir une compensation d'attaque et une récupération après attaque dans le cas de cyber-attaques FDI. Une nouvelle stratégie de contrôle de repli est proposée pour atténuer les attaques DoS/DDoS et assurer la coordination entre les ressources énergétiques distribuées de manière partiellement ou entièrement décentralisée. Une infrastructure de contrôle cyber résiliante à plusieurs étapes est ensuite développée pour intégrer la cyber sécurité dans la conception du microréseau afin d'assurer la résilience, la robustesse et la fiabilité en cas de cyber-attaques. Une plateforme de co-simulation HIL en temps réel, modélisant et interfaçant les couches du réseau électrique, des réseaux d'information et de communication du microréseau, est présentée et utilisée pour analyser l'impact des cyberattaques et tester et valider l'efficacité des stratégies de mitigation cyber-résilientes proposées. Les recommandations et les meilleures pratiques de cybersécurité découlant de cette recherche sont également présentées.

Acknowledgments

First and foremost, I would like to express my special appreciation to my supervisor Professor Geza Joos who has taught me a lot on both the personal and the professional levels. I will always be indebted to him for all the advice and opportunities he has offered me throughout my graduate studies. His guidance and criticism encouraged me to overcome all the challenges of a Ph.D.

Besides my supervisor, I am hugely appreciative to Yves Brissette for sharing his technical expertise so willingly and for being so dedicated to his role as my mentor during my internship at the Hydro-Québec Research Institute. With the same level of gratitude, I would like to thank Dr. Marthe Kassouf for her help. I would also like to recognize the help and information that Dr. Mathieu Lambert, Dr. Chad Abbey and Sylvain Morin provided me.

I would also like to thank my supervisory committee, Professor François Bouffard and Professor Ioannis Psaromiligkos, for their insightful comments and the challenging questions which incented me to widen my research from various perspectives.

I would also like to express my gratitude to all my friends and colleagues in the Electric Energy Systems Laboratory, with whom I have had numerous stimulating discussions. Thanks to Carlos Mauricio Rangel for helping me prepare the setups and to Diego Mascarella with whom I have collaborated on different projects and papers.

I gratefully acknowledge the financial support granted to me by McGill University through the McGill Engineering Doctoral Award. I was very honored to receive such a prestigious award. I also acknowledge the financial support from Pervasive and Smart Wireless Applications for the Digital Economy and the Natural Sciences and Engineering Research Council of Canada and Hydro-Québec to the NSERC/Hydro-Québec Industrial Research Chair.

A thank you from the heart goes to my friends Pia and Maria for the support and encouragement they provided from overseas. I would also like to extend my special thanks to my best friend Hassana who accompanied me throughout this journey, making it easier, pleasurable and definitely memorable.

Last but not least, no words could express the level of gratitude I extend to my parents, Michel and Marie, and my sister, Myriam. Your never-ending support and encouragement are the main reasons behind my success and your prayers for me were what sustained me thus far. I will always be indebted to you for all the sacrifices you made and for continuously believing in me. The least I could do to thank you is dedicate this thesis to you.

Contents

List of Figures

List of Tables

List of Acronyms

AC	Alternating Current
AES	Advanced Encryption Standard
AGC	Automatic Generation Control
CMAC	Cipher-based Message Authentication Code
CSIS	Canadian Security Intelligence Service
DC	Direct Current
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DFIG	Doubly-Fed Induction Generator
DNP	Distributed Network Protocol
DOE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic-Curve Digital Signature Algorithm
EMS	Energy Management System
EPS	Electric Power System
ESS	Energy Storage System
FDI	False Data Injection
GCM	Galois/Counter Mode
GOOSE	Generic Object-Oriented Substation Events
HIL	Hardware-In-the-Loop
HMAC	Hash Message Authentication Code
HMI	Human Machine Interface
I/O	Inputs/Outputs

IAP	Interoperability Architecture Perspectives
ICD	Intelligent Electronic Device Capability Description
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IESO	Independent Electricity System Operator
IP	Internet Protocol
LAN	Local Area Network
LR	Load Redistribution
MIMO	Multiple-Input Multiple-Output
MITM	Man-in-the-Middle
MMS	Manufacturer Message Specification
MPPT	Maximum Power Point Tracking
NERC	North American Electric Reliability Corporation
NI	National Instruments
NIST	National Institute of Standard and Technology
OPM	Office of Personnel Management
PCC	Point of Common Coupling
PI	Proportional Integral
PLL	Phase-Locked-Loop
PV	Photovoltaic
RSA	Rivest-Shamir-Adleman
SCL	Substation Configuration Language
SITL	System-in-the-Loop
SM	Synchronous Machine
SMV	Sampled Measured Values
SOC	State-of-Charge
TCP	Transmission Control Protocol

TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
U.S.	United States
UFLS	Under Frequency Load Shedding
UVLS	Under Voltage Load Shedding
VLAN	Virtual Local Area Network
VSI	Voltage Source Inverter
WTG	Wind Turbine Generator

List of Symbols

Indices, subscripts and superscripts

0	Current index
dDER	Dispatchable DER
droop	Droop control
isochronous	Isochronous DER
lb	Lower bound
MPPT	Maximum power point tracking
R	Renewable DER
RDER	Renewable DER
shed	Energy shed
ub	Upper bound
VI	Virtual inertial response
L	Load
d	Diesel generator
$forecast$	Energy forecasted
i	Index for repetitive FDI cyber-attacks
j	Index for renewable DERs
l	Index for Dispatchable DERs
max	Maximum value
$meas$	Measured value
min	Minimum value
$nadir$	Lowest possible frequency value
nom	Nominal value
ref	Reference value
res	Residual

Functions

C_d	Cost function for the diesel generator [$]
C_{ESS}	Cost function for the ESS [$]

Parameters

B_i	Bias used for the ith application of repetitive FDI cyber-attack [kW]
$E_{L\,not\,served}$	Load energy not served [kWh]
E_{shed}	DER energy shed [kWh]
H_{eq}	Equivalent inertia constant
$I^{max}_{grid\,converter}$	Maximum inverter current [A]
K_{SOC}	Gain for supplementary control loops for SOC management
K_{comp}	Gain for supplementary control loop for DERs coordination
K_{droop}	Droop gain
$K_{inertia}$	Inertia gain
$P_{L\,served}$	Load power supplied [kW]
$P_{SOC\,management}$	DER active power for SOC management [kW]
P_{attack}	Modified active power resulting from the application of the FDI attack [kW]
P_{comp}	Active power compensation for long-term excursions and DERs coordination [kW]
P_{droop}	Active power contribution from droop control [kW]
$P_{f\,regulation}$	DER active power for frequency regulation [kW]
$P_{inertia}$	Active power contribution from virtual inertial response [kW]
T_A	Cyber-attack period [s]
c_{ESS}	Levelized cost of ESS energy [$/kWh]
t_A	Time when the cyber-attack is launched [s]
t_{OF}	Period after which over frequency protection schemes initiate [s]
t_{UF}	Period after which under frequency protection schemes initiate [s]
t_d	Time of attack detection [s]
$t_{protection}$	Time of activation of protection scheme [s]
t_{rest}	Frequency and voltage restoration time, in SM and inverter based microgrids [s]
t_s	Simulation time [s]
ΔV_{th}	Minimum permissible voltage deviation [V]
Δt	Simulation time-step [s]
B	Bias used for persistent FDI cyber-attacks [kW]
E	Energy [kWh]

P	Active power [kW]
c	Direct cost of diesel [$/liters]

Variables

i_d	DER inverter current [A]
ΔV_{SOC}	Change in voltage for SOC management [Hz]
Δf_{SOC}	Change in frequency for SOC management [Hz]
Δf_{dec}	Change in frequency for decentralized control[Hz]
η	ESS efficiency [%]
V	Voltage [V]
f	Frequency [Hz]
i	Grid-side currents of DERs [A]
t	Time [s]
α	Quadratic coefficient for the valuation curve of the diesel generator [$/kW^2]
β	Linear coefficient for the valuation curve of the diesel generator [$/kW]
γ	Constant coefficient for the valuation curve of the diesel generator [$]
ω	Speed [rad]

Chapter 1

Introduction

1.1. Background

"The next major war will not be fought with guns, ships and missiles. It will be a cyber war with far more devastation than could possibly be achieved by our combined nuclear arsenals. Or if conventional weapons are used, they are likely to be our own turned against ourselves" said John McAfee, the developer of the first anti-virus program [1]. In fact, numerous cyber events targeting critical infrastructures were launched in the 21st century. Stuxnet was the first cyber-warfare weapon consisting of a complex piece of malware targeting industrial control systems. Its purpose was far more destructive than stealing, erasing or modifying data; instead, the aim of Stuxnet was to cause physical damage to the critical infrastructures [2]. An estimated 50,000 to 100,000 computers located mainly in Iran, Indonesia, India and Azerbaijan have been infected by the Stuxnet [3]. The Canadian government represented a major target to threat agents. As a matter of fact, in 2011, the Canadian government reported a major cyber-attack against its agencies giving hackers access to highly classified federal information and forcing Canada's main economic centers to disconnect from the internet [4]. In 2015, several Denial-of-Service (DoS) cyber-attacks targeted Canadian federal government websites including the Canadian Security Intelligence Service (CSIS) and Service Canada. The United States (U.S.) was also a victim of various cyber-attacks. For instance, coordinated DoS cyber-attacks targeting 46 major financial institutions including the New York Stock Exchange, Bank of America and Capital One have been carried out

in several phases starting in 2012 [5]. One of the cyber-threat agents also gained remote access to the controls of a Dam in New York [6]. Another potential cyber-attack targeted the U.S. Office of Personnel Management (OPM) in 2015 and resulted in the theft of an estimated 21.5 million confidential records [7]. A massive cyber-attack has been launched in May 2017 and has targeted many large international companies resulting in more than 200,000 computers being infected in over 150 countries [8, 9].

The reason behind the numerous cyber events compromising critical infrastructures is the rapid advancement and increased complexity of information and communication technologies (ICT) which render connectivity more convenient enlarging the cyber-attack surface. The majority of cyber-attacks are inexpensive, easy to launch, effective and have a low risk of detection. The chemical, nuclear, healthcare, financial services, transportation and energy sectors are all endangered and securing and protecting critical infrastructures against cyber-attacks became more and more challenging. As it provides essential services to the other sectors, the electricity sector is debatably the most complex of all. The evolving electric grid increasingly relies on ICTs to ensure enhanced control and automation paving the way to more frequent and sophisticated cyber-attacks. In fact, the first real attack which targeted the electricity sector was the unprecedented cyber-attack that compromised the Ukrainian power grid in December 2015. This cyber-attack resulted in a widespread outage depriving 700,000 customers from electricity for several hours [10]. The attackers were able to find vulnerable access points to penetrate and compromise the Ukrainian power grid although industry standards for cyber security were employed. North American experts claim that the U.S. power grid is not protected against such breaches and the Ukrainian attack is easily repeatable [11]. As a matter of fact, in 2014, the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) detected the threat agents behind the Ukrainian attack attempting to target the U.S. electric sector. Although the attack never occurred, an increased risk for potential future attacks on the U.S. critical infrastructure is anticipated [12].

The microgrid is considered as an important element in power systems as it provides improved energy delivery to local customers, higher renewable distributed energy resources (DER) penetration and has the ability to operate autonomously as a self-contained power system entity [13]. The advanced capabilities and functionalities provided by microgrids are enabled by means of a communication infrastructure vulnerable to cyber-attacks similar to the ones perpetrating the large power systems. As microgrids are gaining increased importance amongst

stakeholders operating critical loads and requiring reliable and efficient energy delivery, a detailed analysis of their cyber security is compulsory before their deployment.

1.2. Microgrid Operation

1.2.1. Microgrid Definition and Benefits

The Department of Energy (DOE) defines the microgrid as "A group of interconnected loads and DERs with clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid and can connect and disconnect from the grid to enable it to operate in both grid-connected or islanded mode." [14].

A microgrid may be connected to the distribution system at one point, notably the point of common coupling (PCC), and features various DERs, including inverter-interfaced renewable energy resources, fossil fuel based rotating machines, energy storage systems (ESS) and controllable loads. Microgrids have the ability to seamlessly shift from islanded to grid-connected mode and vice versa, necessitate the deployment of a microgrid controller to manage the DERs and loads and require information exchange among the various entities [15].

The ability of microgrids to integrate renewable energy sources into distribution networks on a large scale increases their value and interest amongst utility engineers and provides greater efficiency and flexibility in the evolving electric grid. By employing local energy sources to supply local loads, microgrids reduce the energy losses in transmission and distribution further increasing the efficiency of the electric grid. Microgrids can provide continuous operation even when the main electric grid is down and can ensure faster grid response and recovery by operating as a grid resource, strengthening the electric grid resiliency against disturbances [14].

1.2.2. Microgrid Operation and Control

The smooth and reliable operation of microgrids featuring highly intermittent renewable DERs with various characteristics and power capacities necessitates power and energy management strategies coordinating by means of a communication infrastructure. The communication network required by the microgrid controller to provide a mechanism for the

exchange of information enhances the operation and dynamics of the microgrid; however, it introduces access points and vulnerabilities that may be exploited by attackers [16].

1.2.2.1. Microgrid Controller EMS Functions

Microgrid controllers can have a large subset of functions, such as frequency and voltage control, energy and load management, seamless reconnection to the grid and transition from grid-connected to islanded operation. The energy management system (EMS), the microgrid controller's most critical function is typically employed to coordinate the various DERs available to provide continuous and smooth operation of the microgrid in the multi-minute time frame, particularly in autonomous mode, in the absence of a connection to the main electric power system (EPS) [17, 18]. The EMS can assume two configurations, either centralized or decentralized. The centralized topology is typically more suitable in islanded microgrids, as it provides better coordination amongst the DERs, resulting in improved microgrid performance metrics (fuel consumption, levelized cost of electricity, energy sourced by renewables) [17-19].

The EMS manages the DERs local controllers and dispatches power set-points to the various resources in order to optimize specific objectives while respecting the system constraints. The main objectives include maximizing the power sourced by the renewable DERs, minimizing fuel consumption, emissions and levelized cost of energy [20]. These objectives need to be achieved while respecting some imposed requirements and limitations including DERs capacity limits, cost of generation, energy and reserve limits, load levels, safety restrictions, environmental impacts and maintenance intervals [21].

1.2.2.2. Power Management Strategies

The DERs primary power control loops compensate for the power mismatch during the inter-dispatch period, the period between EMS dispatch set-points updates. The local controllers coordinate to improve the microgrid dynamic response, restore the voltage and frequency during and after transient events and ensure power sharing amongst the various DERs [22, 23].

The microgrid DERs can be classified into grid-feeding, grid-forming and grid-supporting resources, each of which provides specific functions in the microgrids.

Grid-Forming DER

When operated in the islanded mode the microgrid's grid-forming or isochronous DER maintains the system's voltage and frequency and compensates for the fluctuations caused by the renewable energy sources and load. The grid-forming voltage and frequency are used as the reference for the rest of the grid-feeding or grid-supporting DERs [22, 24].

Grid-Feeding DER

The grid-feeding DERs are primarily renewable DERs which inject power and do not actively regulate the system voltage and frequency [25]. These DERs commonly employ a power-electronic interface, operated as a current-controlled voltage source inverter (VSI) to interface with the grid [22]. In grid-connected mode, the grid-feeding DERs can operate in parallel, in contrast to the islanded mode of operation, where they require the deployment of a grid-forming or grid-supporting DER to properly operate.

Grid-Supporting DER

The microgrid grid-supporting DERs may or may not participate in voltage and frequency support. Depending on their mode of operation, these DERs can function with or without a grid-forming DER in both grid-connected and islanded microgrids.

1.2.3. Microgrid Communication Network and Information Exchange

The EMS relies on a wide variety of information and employs different decision-making techniques to achieve the specified objectives while ensuring operation within the defined constraints [18, 19, 21]. Initialization parameters are first used by the EMS to operate the DERs and include: 1) the regulatory constraints on DER operation, emissions and system efficiency, 2) the DER equipment specifications, 3) the present and forecasted load values 4) the present and forecasted weather data, 5) the load types (critical, curtailable and reschedulable) for load control. The data that needs to be continuously communicated to the EMS to evaluate operating set-points and commands that allow global centralized control of the DERs include: the varying cost of energy from the different sources, the mode of operation of the DERs in terms of the power

management strategies employed, the energy and power generated by the DERs and that demanded by the loads.

In contrast to conventional power systems, microgrids employ wired and wireless communication technologies to provide a distributed and hierarchical communication infrastructure for energy delivery and microgrid management [26, 27]. These communication technologies should ensure fast and reliable exchange of commands and controls between the microgrid entities. The microgrid communication infrastructure needs to be reliant to standardized communication protocols with high performance. The Distributed Network Protocol (DNP3) and Modbus protocols and the International Electrotechnical Commission (IEC) standard, IEC 61850, are widely used in microgrid communication systems. Every protocol corresponds to a communication model that represents the microgrid entities. Modbus is an application layer legacy protocol that employs a client-server communication technique. The client represents any peripheral device that processes information and sends it to the server which runs application software. A client-server communication model could represent the microgrid system whereby the DERs and loads are modeled as clients and the microgrid central controller represents the server [28]. The DNP3 protocol can also be used in microgrids and it is based on a Master/Slave model whereby the master represents a control center and the slave or outstation models the field devices. Unlike Modbus, DNP3 slave can send unsolicited responses to the master, the protocol includes time-stamped events and data quality information and multiple data types can be encapsulated in a single DNP3 message [29]. The IEC 61850 standard was initially designed for substation automation whereby three levels are defined: the process, the bay and the substation levels. Three different protocols are supported: Manufacturer Message Specification (MMS), Generic Object Oriented Substation Events (GOOSE) and Sampled Measured Values (SMV) modeling the messages at the different levels [30]. In order to exchange information at the various levels, MMS protocol employs a client-server unicast communication model whereas GOOSE and SMV use the concept of publisher-subscriber multicast-based communication. The IEC 61850 configures intelligent electronic devices (IED) with different data attributes and functionalities developed by different manufacturers to ensure interoperability. Depending on the type of the application employed, communication requirements such as latency are specified. The IEC 61850 protocol has been recently gaining importance in distribution automation and it provides a suitable representation of the microgrid and its information exchanged.

1.2.4. Simulation Platforms for Cyber-Physical Systems Modeling

The IEEE P2030 defines three separate interoperability architecture perspectives (IAP) that together comprise the smart grid: the Power System IAP defined in terms of power elements and their interoperability, the Communication Technology IAP defined in terms of communications elements and networks and the Information Technology IAP defined in terms of information flows, entities and protocols used to exchange that information [31]. In order to perform a detailed cyber security analysis for power grids, the three IAPs need to be modeled and interfaced.

The co-simulation of heterogeneous systems has previously gained a lot of importance in various research areas but remains a relatively new topic for power systems analysis and control. Just like power systems, microgrids are undergoing radical changes and evolving towards more flexible infrastructures and technologies at the generation, sensing, control and monitoring levels to form the so called “smart grid”. To fully benefit from the capabilities of these advanced technologies, the deployment of a communication network becomes mandatory. More attention has been recently directed towards modeling the smart grids’ communication networks and information exchange layers and interfacing these models with the simulated power system. One of the very first co-simulation tools modeling the power system with its underlying communication network was EPOCHS [32]. Off-the shelf power system and communication network simulators were used to model the different layers and a software mediator was employed to interface and synchronize the simulators. The time-synchronization process is based on a simple time-stepped approach whereby the different simulators run respectively and halt at fixed step-points to allow information exchange. One major drawback of this method is that if information needs to be exchanged in the inter-synchronization period, it will be kept in a queue until the next synchronization point. This process leads to an accumulation of errors jeopardizing the fidelity of the simulations, especially the time-critical ones. VPNET [33] and Powernet [34] employ synchronization algorithms similar to the one implemented in EPOCHS and therefore result in the same type of errors accumulation. In addition, these tools are not suitable for large scale power networks. Another emerging solution is the use of real-time simulators to accurately represent the real-world power system. The simulators could be interfaced with network emulators to overcome the time-synchronization and

data exchange issues faced in non-real-time simulations [35]. For instance, the research works done in [36, 37] use OPNET and OPAL-RT which provide real-time operation of the power system and its corresponding communication network whose interface ensures time-synchronization. Although useful for simplified modeling of power systems, these setups do not provide detailed modeling of the power system components, the control strategies implemented and the communication protocols employed.

1.3. Microgrid Cyber Security

1.3.1. Cyber Security Objectives and Cyber-Attacks Types

Centralized control strategies necessitate two-way information flow between the microgrid controller and the DERs local controllers [19], and are enabled through a microgrid communication network, adhering to the defined communication protocols. This reliance on ICTs along with communication protocols, such as internet protocol (IP) based protocols, enhances the operation and control of the microgrid; however, it creates potential vulnerabilities and access points which can be maliciously exploited by cyber-attackers [38-41]. As per the National Institute of Standards and Technology (NIST) guidelines, cyber-attacks are classified into three levels: attacks compromising availability, confidentiality and integrity [42]. Cyber-attacks compromising confidentiality allow threat agents to eavesdrop on the communication network to acquire information that could reveal the identity of the customers and their electricity usage. These attacks have a less significant impact on the microgrid main functions' operation. Cyber-attacks compromising data integrity cause malicious modification of information flowing in the grid. These attacks can result in corruption of the measurements or commands exchanged in the grid leading to a disruption or malfunction of the microgrid critical control functions such as voltage and frequency regulation, energy and load management, islanding and resynchronization. A typical example of attacks jeopardizing the data integrity of the grid is False Data Injection (FDI) cyber-attacks. As for the loss of availability, it is caused by attacks whose main purpose is to block, delay or corrupt the communications so as to make network resources unavailable to the system nodes that require information exchange [43]. Whether launched from one source or from multiple

sources, DoS and Distributed DoS (DDoS), are typical examples of cyber-attacks jeopardizing the availability of the grid and can be initiated by sending malformed packets to the attack target, performing network/transport or application layer flooding attacks by exhausting the bandwidth, the processing capacity of the routers or the network resources or by exhausting the server resource [41, 44]. DoS and DDoS cyber-attacks impact the communication network performance and make the network resources and services unavailable to legitimate users requiring this information [38, 41].

1.3.2. Cyber-Attack Impact Assessment

Various studies have investigated the impact of FDI and DoS/DDoS cyber-attacks on the operation of the power system and the communication network, respectively. FDI cyber-attacks targeting the power system state estimation were introduced in [45]. It was shown that with complete knowledge of the power system configuration, an attacker could inject into meters, false data which bypasses bad data detection schemes modifying the state estimation outputs and resulting in erroneous decisions. Load redistribution (LR) attacks, a special type of FDI, were presented in [46]. The attack consists of a cooperative manipulation of load measurements and line power flows, misleading the state estimation and resulting in a false economic dispatch. As such, the non-optimal dispatch causes unnecessary load shedding and the power flows exceeding the lines' capacities result in more pronounced curtailments. The research in [46] is further extended in [47] to propose bi-level and tri-level models to identify the most damaging immediate and delayed LR attack which impact is quantified in terms of the increased operational cost. To overcome the limitations of [45-47] requiring full knowledge of the system configurations, the studies performed in [48, 49] showed that knowledge of the local attacking region's parameters is sufficient to successfully launch an undetectable FDI attack. The impact of FDI cyber-attacks which maliciously modify the sensor measurements on the operation of control systems is evaluated in [50, 51] on the operation of voltage [52] and angle stability control loops [53, 54] and have showed that the effectiveness of the attack depends on its magnitude, target and location. FDI cyber-attacks jeopardizing the operation of automatic generation control (AGC) are investigated in [55, 56] and their impact is quantified in terms of frequency instability and loss of load. Different types of FDI cyber-attacks including constant injection, bias, positive and negative compensation, scaling, ramp, pulse and random cyber-attacks are proposed and tested in [57, 58]. In [59],

tampering with the load sensor measurements showed to cause incorrect load management decisions, such as unnecessary load shedding or DER disconnection, in a microgrid system.

Most of the studies investigating DoS and DDoS cyber-attacks evaluate their impact on the communication network performance. For instance, a traffic flood was conducted in [39] to cause a DoS cyber-attack on a power grid communication network implementing the DNP3 protocol. It was shown that the attack could result in phase transition in the delay performance of the DNP3 protocol and that shorter DNP3 packets are more immune to such intrusions. An SYN flood attack is launched in [60] against phasor measurement units (PMU) in a distribution network and results in large traffic congestions disrupting the data sent to the controller causing wrong decision making. The impact of DoS and DDoS attacks which compromise one or many network devices respectively to launch SYN flood and compromise the utility server responsible for demand response (DR) was evaluated in [61]. The DoS attack did not affect the overall operation of the power grid as it resulted in a slight reduction in the average number of packets received by the smart meters. In the case of a DDoS, 89.7% of the meters were not able to communicate with the server. The partial unavailability of the DR mechanism in the majority of the meters in the event of a DDoS would cause an unsafe mode of operation, especially during critical peak periods when load shedding is necessary.

Although cyber-attacks could be performed using different techniques, could target different power system entities and their impact on the power system operation could vary in intensity, it could be concluded that power grids do not fundamentally embed cyber security and their underlying infrastructure is not inherently built to resist cyber-attacks. In addition, very few are the studies analyzing the cyber security of microgrid systems which too are prone to cyber intrusions that could severely impact their operation. Hence, before the deployment of microgrids as a solution for reliable and efficient energy delivery, their underlying infrastructures should be designed with cyber security and resiliency in mind.

1.3.3. Cyber-Attack Prevention Strategies

Prevention of cyber-attacks targeting the grid's integrity and availability is commonly achieved by improving the information security techniques applied. In order to prevent FDI and DoS/DDoS cyber-attacks, measures such as the inclusion of data integrity checking, encryption message protocols and authentication mechanisms are to be employed [41-44, 62] [63, 64]. The

NISTIR standard presents a list of approved algorithms for encryption by means of symmetric key, such as the Advanced Encryption Standard (AES) and Triple-Data Encryption Algorithm/Standard (TDEA/TDES) [65-67], and asymmetric or public key, such as the Digital Signature Algorithm (DSA), Digital Signature Standard (DSS), Rivest–Shamir–Adleman (RSA) digital signature and Elliptic Curve Digital Signature Algorithm (ECDSA) [68, 69]. Accordingly, Cipher-based Message Authentication Code (CMAC), Galois/Counter Mode (GCM) and its specialization GMAC, and the Hash Message Authentication Code (HMAC) are approved message authentication algorithms [70-72]. However, if not properly deployed, these measures might negatively impact the microgrid operation [73]. Unencrypted or weakly encrypted network protocols expose the authentication keys and data payload enabling attackers to obtain credentials, access the network devices and decrypt encrypted traffic using the same keys. For instance, standard well-documented protocols used in plain-text create a vulnerability and enable session hijacking and MITM attacks allowing malicious tampering of the data exchanged between the devices. Accordingly, insecure key exchange and storage, or inadequate authentication and data protection between clients and access points could result in insufficient authentication and enable attacks on authentication keys facilitating session injection and hijacking, DoS/DDoS and MITM attacks. The verification of the integrity of a message protocol and data should be performed before any data routing and processing. A lack of data integrity checking and security monitoring, inadequate security architectures, poorly configured security equipment and failure to detect and block compromised traffic in valid communication channels could significantly impact the grid operation and result in buffer overflows, the compromise of the devices and servers, MITM and DoS/DDoS cyber-attacks. Network segregation, single and multipath routing [58], the employment of virtual local area networks (VLAN) along with priority tagging and communication redundancy are other prevention means that could also be employed at the communication network layer.

Utilities tend to protect their power assets against potential cyber-attacks through conformity to security guidelines and regulations and through the application of the aforementioned defense mechanisms and prevention strategies. Although effective in some scenarios, the conformity to security regulations and most of the currently implemented prevention strategies cannot ensure a comprehensive protection of the power grids, as seen following the success of the Ukraine attack. Just like the large EPS, microgrids are prone to cyber disturbances

and embedding resiliency into their control infrastructure is, therefore, necessary [57]. Hence, as prevention means are bypassed, detection mechanisms need to be put in place to localize the compromised entities and post-attack recovery plans must be proposed to ensure enhanced resiliency.

1.3.4. Cyber-Attack Detection

Different control strategies have been proposed in the literature to detect cyber-attacks compromising data integrity of smart grids and cyber-physical systems in general. The research work performed in [74] analyzed cyber-attacks on sensors and actuators on a generalized continuous-time linear control system model. The limitations in attack detection and identification have been presented by defining algebraic and graphical conditions. Centralized and distributed filters are developed to detect and identify, when feasible, arbitrary errors inserted by the attacker to vulnerable sensors and actuators. In a similar effort, [75] identifies the maximum number of sensors that could be compromised in a linear control system in order for attack detection and recovery to be possible. The study shows that by identifying sensor attacks, state estimation could be properly performed by disregarding the malicious sensors and relying on the trusted ones. The ability of conducting perfect state estimation in the presence of compromised sensors is hence equivalent to the ability of performing perfect identification. Different efforts have been put in order to solve the problem of robust state estimation in deterministic systems [76] and [77], and in stochastic and uncertain systems [78, 79] to reconstruct the system's state in the event of a limited number of cyber-attacks.

The aforementioned strategies rely on the assumption that the attacker has partial access to the system and cannot manipulate all the sensors measurements. To overcome this constraint, [80] proposes a moving target scheme to detect cyber-attackers having knowledge of the system state and measurements. The proposed control scheme consists of adding extraneous states with time-varying dynamics known by the defender and hidden from the attacker that are correlated to the original states. Additional sensors are also introduced in the system to measure the extraneous states. As such, as the original states are maliciously varied by the attacker, the extraneous states will be impacted. The dynamics of the additional states vary fast enough so that the attacker cannot identify the extraneous system. Conducting unidentifiable attacks on sensors requires the attacker to have knowledge of the system model. This creates limitations on the number of identifiable

attacks which would require adding more sensing to withstand more attacks or designing systems resilient to a small number of attacks. The study performed in [81] argues that limiting the attacker's knowledge of the system model reduces the ability to conduct unidentifiable attacks. Changing the dynamics of the system model in a time varying manner, unknown to the attacker, would force the attacker to launch unambiguously identifiable attacks allowing the defender to perform proper state estimation without requiring more sensing. The design of the time-varying dynamics, acting as a moving target, is discussed in this paper and the performance of the proposed control strategy is evaluated for deterministic and stochastic systems.

The concept of adding noise to the control commands to detect cyber-attacks, or what is commonly known as physical watermarking, is another common approach to detect cyber intrusions in cyber physical systems and is discussed in [82]. The cyber-attacker considered is assumed to have no knowledge of the system model and is only capable of performing a replay attack causing the repetition of the sensors' measurements to cause disruption of the control system in steady-state. As compared to other detection means, the noisy control authentication enhanced attack detection on the expenses of the controller performance. Physical watermarking is further analyzed in [83] to detect replay attacks on sensors using different watermarked inputs. An algorithm was developed to evaluate the statistical properties of the watermarked input based on the trade-off between the detection performance and the tolerable control performance loss. The concept of physical watermarking is further extended in [84] to detect an attacker with knowledge of the system model, the true system outputs and a subset of the control inputs. As such, the attacker can design stealthy virtual outputs and insert damaging inputs to the system. Physical watermarking has proved to enhance the ability of the defender to detect replay and stealthy attacks with or without knowledge of the system model, sensor measurements, and a subset of the control inputs. This detection enhancement however results in a degradation of the control performance. In addition, if the attacker gains access to all the control inputs and sensors measurements of the system, the watermark detector would fail.

In the area of distributed control approaches, a distributed control strategy is proposed in [85] to enable the wireless network nodes to evaluate any arbitrary function of the node values in the presence of malicious agents. A broadcast communication model is assumed and a linear iterative strategy is employed to define the information exchanged by the nodes. A malicious node is detected whenever it updates its values arbitrarily without following the linear strategy. The

study shows that under specific connectivity requirements it is possible for the nodes to calculate any arbitrary functions even in the presence of malicious nodes. Although distributed control strategies ensure resilience in the event of cyber disturbances, they could only defend against a limited number of attacks. In addition, if the attacker has knowledge of the system model and data exchanged he/she would be able to extract the needed information to maliciously tamper with the nodes' updates without being noticed by the defender.

Detecting DoS and DDoS cyber-attacks is typically performed by monitoring the operation of the communication network layer. Signature-based and anomaly-based intrusion detection schemes (IDS) could be employed to identify suspicious network activity enabling the detection of DoS/DDoS and FDI cyber-attacks. Knowledge or signature-based IDSs create databases of all the cyber-attacks that could possibly compromise the communication network. Based on these patterns, known attacks could be easily detected without generating any false positives. The widely used open-source Snort [86] tool is a typical example of such IDSs. The major drawback of such schemes is their inability to detect unknown or slight variations in the attack patterns. Anomaly-based IDSs on the other hand, make use of the model of normal communication network behavior and identifies any variant as anomaly. D-WARD [87] is a widely used anomaly-based detection scheme which uses a model for the normal system traffic and continuously monitors the two-way traffic flow between the network peers to identify anomalous behavior. Trade-offs between the ability to detect all the attacks and misidentifying a normal behavior as an attack should be performed when implementing such IDSs. IDSs could also be setup to monitor the behavior of the grid underlying physical process governed by the power system theories. For instance, a model-based attack detection and mitigation scheme is proposed in [55] and tested in [88] for AGC compromised by integrity cyber-attacks. The attacker modifies the sensor measurements to cause wrong control commands drifting the system frequency to unstable operating points. The cyber-attack detection mechanism evaluates, based on forecasts, an estimate of the expected control commands which are compared to the real-time commands using statistical and temporal characterization. A set of rules are defined to ensure that the commands that are not anomalous conform to the power system theory. The parameters of the anomaly based detection scheme are tuned in order to minimize the false negative and false positive rates in the studied attack period. When the attacks are detected, an educated guess of the real commands is evaluated to replace the compromised commands. The proposed strategy could be employed if the attacker has knowledge

of the system model, the sensors measurements and all of the actuators commands. However, the detection and mitigation schemes highly depend on the load forecasts whose reliability is affected by faults and unexpected load changes and which could be maliciously manipulated by cyber-attackers. These limitations could not be disregarded as in such scenarios, instead of enhancing the cyber resiliency of the system, the proposed scheme would lead to very high rates of false negatives and false positives deteriorating the operation of the grid.

1.3.5. Resilient Control for Cyber-Attack Mitigation

The strategies and techniques mentioned in the previous section cannot always guarantee cyber-attack detection. Even if they do, they do not always ensure instantaneous attack detection. Therefore, a resilient microgrid control infrastructure should be designed to account for, counteract and survive both, detected and undetected cyber-attacks. This section first reviews the decentralized and distributed power and energy management strategies which the microgrid could employ in the event of detected FDI and DoS/DDoS attacks targeting microgrids centralized controller. The control loops that could be added to the DERs primary controllers to provide frequency support in the event of unplanned power imbalances or undetected FDI cyber-attacks in low inertia microgrids are then presented.

1.3.5.1. Power and Energy Management Strategies for Mitigation of Cyber-Attacks on Microgrid Centralized Controller

Different control strategies could be employed to mitigate FDI and DDoS cyber-attacks compromising the microgrid centralized EMS operation which maliciously modify or cause disruption of the information exchanged between the controller and the DERs. A distributed network control approach is proposed in [89] to define a strategy for each network node to follow when updating its internal state. A numerical design procedure is employed to determine how the node's state will include the neighboring nodes' states so that the updates of the nodes closest to the actuators can ensure a stable operation of the plant. The numerical design is modified and a distributed scheme is presented to ensure stable operation in the event of packet drops and node failures. The research works performed in [90, 91] suggest cooperative control techniques whereby each DER monitors the behavior of its neighbors, using multicast communications, and isolates

the misbehaving DERs from the network. These strategies make use of communications which could be intruded, only operate in the event of partial system compromise and assume that it is guaranteed that the leader DER is secure and cannot be attacked using methods such as in [41, 43, 44, 62, 92]. Another common practice that could be employed to mitigate the centralized EMS single-point of failure drawback is to operate the DERs in droop control mode as it relies on local measurements and does not require communications resulting in high reliability and flexibility [93-95]. However, when in conventional droop control mode, two or more DERs could actively participate in the regulation of the voltage and the frequency [19]. Although this control strategy is highly flexible and it could be used in the event of unreliable or lost information exchange due to FDI or DDoS cyber-attacks, it has drawbacks such as its slow and oscillatory dynamic response and it results in poor performance as renewable DERs are integrated [96]. Methods such as angle droop replacing frequency droop [97], the addition of a derivative term to the static droop characteristics [98], adaptive decentralized droop [99] and non-linear droop control [100] could be employed to enhance the performance of the traditional droop control method.

There are many benefits of operating the ESS in grid-forming mode, as will be explained in chapter 4. If this power management strategy is employed, managing the ESS SoC is of paramount importance as a cyber-attack which causes violation of its energy limits would restrain its ability to regulate the microgrid voltage and frequency. Decentralized SOC management algorithms are proposed in [101, 102] however most applicable only in grid-connected microgrids. In [103, 104], the ESS reference frequency is adjusted based on SOC limits in order to manage the SOC in a decentralized manner. Active power limits ensuring that the ESS provides its isochronous functions and compensates for the loads and renewable DERs variability are not accounted for. As the SOC reaches its lower or upper limits a frequency decrease or increase signals load shedding or renewable generation power curtailment to allow the ESS to charge or discharge, defeating the main purpose for which microgrids were designed; maximizing the hosting capacity of renewable DERs and providing continuous power supply to the loads. These strategies do not perform adequately in the presence of other dispatchable DERs in the islanded microgrid as supplementary control loops for the DERs are required for coordination and sufficient compensation.

1.3.5.2. Enhanced Primary DER Control for Frequency Support

If detection means are bypassed or do not operate instantaneously, the microgrid DERs and their circuit breakers could operate based on maliciously tampered power set-points or commands creating sudden power imbalances in the grid. Therefore, it is imperative that the DERs local controllers be equipped with loops that provide transient and steady-state compensation of such events, especially in low inertia microgrids where small power imbalances could result in very severe voltage or frequency excursions.

Various robust control architectures have been proposed to tackle the problem of low-inertia microgrids subject to load disturbances or generation outages. For instance, the study in [105] utilizes a multivariable H_∞ approach to design a centralized controller, robust to system nonlinearities, to ensure power sharing among low-inertia DERs in the event of disturbances. Another multi-input multi-output (MIMO) robust controller, designed via μ synthesis, is proposed in [106] to control the DERs and ESS to minimize the battery size and reduce frequency variations in the presence of model uncertainties. These robust controllers enhance the system stability but require communications with the microgrid entities which expose them to a high risk of cyber intrusions. Many variants of droop control have also been proposed in the literature [107-109]. These control loops are local to the DERs and they improve the microgrid stability and power sharing capabilities. However, the DERs equipped with droop control only do not provide inertia support to low-inertia microgrids [110]. The concept of virtual inertia has therefore been proposed to mimic both, the steady-state and the transient characteristics of synchronous generators by applying the swing equation to provide inertia support. For instance, dynamic frequency control support by distributed energy storage was proposed in [111] to generate short-term compensation following a disturbance and operate as a synthetic inertia. The ESS generates power to reduce the rate of change of the frequency and the frequency nadir. The synthetic inertia is tuned such that it activates before the initiation of the load shedding schemes, it provides contribution at least until the remaining resources primary controllers compensate to restore imbalance, and its end of delivery is progressive to avoid creating additional sudden imbalances. The proposed control strategy has been tested in the event of generation outages in an isolated power system with high penetration of renewable energy and it enhanced the frequency response while reducing the amount of load shedding and in some of the scenarios avoiding it. An ESS operated as a virtual

synchronous generator has been proposed in [112] to emulate the inertia of synchronous generators in an autonomous wind-diesel power system. The active power contribution provided by this ESS is proportional to the rate of change of the frequency and an inertia gain. Three different values of the gain were tested to evaluate the performance of the ESS in enhancing the frequency response. As compared to small values of the gain, higher values resulted in a reduction in the maximum deviation in the diesel generator rotor speed following a disturbance but also caused the system to become slower and more oscillatory. In order to dampen the oscillations resulting from a high value of the inertia gain, the damping properties of synchronous generators were emulated together with virtual inertia in [113]. This control strategy was applied to an ESS operated as a virtual synchronous machine added to a PV-hydro microgrid to reduce the frequency variations and the rate of change of the frequency. The active power contribution associated with virtual inertia is evaluated in proportion to the rate of change of the frequency excursion and an inertia gain to provide transient frequency support, while the damping contribution is proportional to the frequency excursion and a damping gain and is added to return the frequency to its nominal value. The gains associated with the inertia and damping contributions are constant values evaluated as the ratio of the nominal power of the ESS to be deployed to the maximum rate of change of the frequency and the frequency excursion, respectively. Accordingly, an oscillation damping approach is developed in [114] for a virtual synchronous generator operated in a grid with a non-negligible power angle. As a result, active and reactive power are no longer independent and are both affected by the angle and voltage changes, making the system's swing equation more complicated to realize and control. Linear control theory is employed to linearize the non-linear swing equation and decouple the voltage deviation and the damping factor. The proposed strategy has been tested for different damping factor values and proved to damp the oscillations with a trade-off between smaller frequency overshoot and shorter response time. The study performed in [115] proposes a modified droop controller for inverter-interfaced DERs to improve the transient frequency response in a droop controlled microgrid in the event of disturbances. The proposed controller evaluates the droop gain in proportion to virtual inertia, computed as a function of the frequency derivative. The modified droop controller only operates in the event of disturbances improving transient frequency response and reducing unnecessary load or generation curtailment outweighing the capabilities of conventional droop control strategies. A combined virtual inertia and droop control strategy is proposed in [116] for doubly-fed induction generators (DFIG) to

regulate the frequency in the event of microgrid load disturbances. The droop and virtual inertia gains are evaluated based on a trial and error approach and they are continuously adjusted depending on the wind speed conditions. The variable coefficient strategy ensured fast response to the rate of change of frequency and temporary frequency support due to virtual inertia, and a permanent frequency support due to droop control. Another combined droop and virtual inertia control scheme is introduced in [23] to variable speed wind turbines controllers to provide transient inertial response and permanent droop-based compensation in the event of generation outages. Different values of the inertia gain are tested and the parameter which increases the frequency nadir without highly increasing the time to restore steady-state is selected. The power reserve required to enable the droop function in over-frequency scenarios is also selected with a trade-off between enhanced frequency response and higher energy losses. The proposed strategy is also tested under normal operating scenarios during wind fluctuations showing that droop control provides the same results as the combined controller. In fact, virtual inertial response showed to be the most effective in the event of fast frequency changes resulting from large disturbances as opposed to droop control which operates in relatively slower events.

1.4. Problem Statement

With the large integration of renewable intermittent energy resources, it became challenging to control the microgrid especially in the absence of the EPS operating as an infinite bus. A microgrid controller which coordinates and controls the various DERs using communication technologies and based on predefined communication protocols is therefore indispensable for smooth and continuous operation. Theory and real-world scenarios have proven that communication networks are never utterly secured and impenetrable. As a result, threat agents could gain unauthorized access, modify, steal, block or corrupt the information exchanged in microgrid systems causing the maloperation of the critical control functions they provide. The severity of the impact a cyber-attack could have on the microgrid operation depends on many factors that will be explained throughout this thesis. To the best of the author’s knowledge, the literature still lacks a detailed cyber security analysis for microgrid systems.

FDI cyber-attacks which compromise the microgrid data integrity by maliciously modifying the measurements sent or the commands received by the DERs to or from the microgrid

controller could result in large disturbances in the system. This is mainly due to the fact that microgrids are extensively deploying static power-electronic interfaced DERs which provide enhanced dynamic performance but result in a microgrid with very low inertia. As a consequence, slight attack-induced power disturbances would yield severe voltage and or frequency excursions imperiling the microgrid stability. If not instantaneously detected and mitigated, cyber-attacks of this type lead to the initiation of protection schemes causing nuisance load shedding and generation disconnection that might conclude with a microgrid blackout. Another significant example is DoS/DDoS cyber-attacks which are being extensively launched recently due to their simplicity and the very severe impact they could engender. In fact, such attacks make the information and services requested by the targeted resources unavailable endangering the critical control functions provided by the microgrid. For instance, a DoS/DDoS cyber-attack can make the commands or measurements sent to or from the microgrid controller unavailable affecting the DERs operation and the controller's decision-making process resulting in violation of the power and energy management requirements.

Ensuring resiliency of the microgrid to cyber-attacks cannot be guaranteed by solely implementing prevention measures and guidelines applicable at the communication network infrastructure. In fact, various scenarios showed that even with these strategies deployed, exploitable holes and vulnerabilities still exist. Hence, the need for building resiliency at the microgrid control infrastructure arises. Both, the primary and secondary control levels need to embed enhanced control loops and be able to shift to fallback control modes to ensure robustness of the microgrid control infrastructure and ability to survive and operate in the presence of undetected attacks and to counteract and mitigate detected attacks. An in-depth cyber-attack impact assessment, facilitated by a quantification of microgrid specific performance indices, is compulsory before proposing effective mitigation methods and developing a cyber resilient control infrastructure for microgrid systems.

1.4.1. Thesis Statement

The main goal of this thesis is to perform a detailed analysis of cyber security for islanded microgrids filling the research gap found in the literature. This first requires the development of microgrid benchmark test systems which model the power system, information exchange and communication network layers and their interconnection. Quantification of the impact of cyber-

attacks on the operation of islanded microgrids having various configurations and operating under different control modes would then be possible. Primary control loops and fallback mitigation strategies that ensure the survivability and resiliency of the microgrid primary and secondary control infrastructure against cyber-attacks are then proposed, implemented and validated. A cyber resilient control infrastructure for microgrid systems is developed and recommendations and best practices for cyber security are concluded.

1.4.2. Research Objectives

Cyber-attack impact quantification

Various factors affect the impact that cyber-attacks can have on the microgrid operation and they include the type of DERs employed, the microgrid configurations, the secondary controller architecture and the primary power management strategies local to the DERs. Benchmark test systems modeling and interfacing the microgrid power system, communication network and information exchange layers in real-time need to be developed to allow proper modeling of the cyber-attacks and provide a basis for cyber security analysis. Microgrid specific performance indices should be defined to provide a mean for quantitative assessment of the cyber-attacks' impact on the operation of critical control functions. The impact assessment facilitates the proposition of mitigation strategies and the performance indices provide a mean for quantifying and testing the performance and effectiveness of the strategies in counteracting cyber-attacks.

Control loops for enhanced survivability of microgrids in the event of cyber-attacks compromising data integrity

After quantifying the impact of cyber-attacks compromising the microgrid data integrity, solutions need to be proposed to ensure that the microgrid control infrastructure can survive and operate resiliently in the event of such attacks, whether they are detected or not. Primary control loops, which provide transient and steady-state voltage and frequency support, need to be implemented, and adaptive load management schemes, ensuring post-attack power and energy balance, need to be designed to compensate for sudden power imbalances induced by FDI cyber-attacks which successfully bypassed the detection schemes employed. The performance of the control strategies needs to be evaluated for different microgrid configurations and under different operating scenarios.

Fallback energy management strategy for DoS/DDoS cyber-attacks mitigation

DoS/DDoS cyber-attacks can target one or many entities in the microgrid causing loss of some or all the information exchanged over the communication network resulting in maloperation of critical power and energy management control functions. A mitigation strategy which operates in the event of such cyber-attacks needs to be proposed. The microgrid should shift to a fallback control strategy which provides the primary and secondary power and energy management functionalities even in the event of lost data. The proposed strategy should ensure safe and secure operation of the microgrid when the communications cannot be trusted and its effectiveness should be evaluated and its performance should be validated for different microgrid control architectures and configurations.

Multi-Stage Cyber Resilient Control Infrastructure and Recommendations for Enhanced Cyber Security

In order to investigate cyber security for islanded microgrid systems, a cyber resilient control infrastructure which embeds security into the grid's design should be proposed. The infrastructure should combine different mitigation strategies and operate at different stages to provide voltage and frequency stability, power and energy management and enhance the ability of the grid to provide continuous power supply and host renewable DERs while operating economically in the presence of detected and undetected FDI and DDoS cyber-attacks in the system. As such, even if conventionally applied prevention and detection means are bypassed, the grid would be designed to survive, respond and recover from cyber-attacks targeting data integrity and availability. A parametric study should be performed to evaluate the performance of the proposed infrastructure under different operating conditions. Recommendations and best cyber security practices could then be concluded.

1.5. Claims of Originality

The outcomes of this thesis build upon existing research work and supplement the emerging field of microgrid cyber security by providing the following research contributions:

1. Development of a real-time HIL benchmark co-simulation platform to enable the analysis of microgrid cyber security. The microgrid power system layer, comprising power-electronic

interfaced, synchronous machine (SM) based and renewable DERs with their underlying power management control strategies, is interfaced with the communication network and information exchange layers, employing legacy and modern communication protocols. Different hardware and software are employed to provide detailed modeling of the microgrid constituting layers, to ensure interoperability, real-time operation, no accumulation of errors, and increased flexibility of the platform to be adapted to larger systems overcoming the drawbacks of setups found in the literature.

2. Formulation of the microgrid cyber security problem and the need for a cyber resilient control infrastructure [117, 118]. Mapping cyber events modeled on the microgrid communication network layer to physical impacts evaluated on the power system layer: Modeling cyber-attacks compromising data integrity and availability of microgrid systems in specific, quantification of the attack's parameters causing infringement of the microgrid power and energy management control functions, along with quantitative assessment of the attacks' impact by means of specific performance indices.
3. Development of mitigation strategies and post-attack recovery plans applied at the control layers of SM based and 100% inverter-interfaced microgrids targeted by cyber-attacks, accounting for both, detected and undetected attacks. The performance of primary control strategies, commonly applied in the context of physical disturbances, is evaluated in the context of undetected FDI cyber-attacks to enhance the microgrid survivability and provide fast transient and permanent steady-state compensation [119, 120]. A rule-based fallback control algorithm is developed to provide power and energy management functions in the event of DoS/DDoS cyber-attacks causing partial or total loss of communication [121].
4. Development of a multi-stage cyber resilient control infrastructure which embeds cyber security into the microgrid's design and operates at different stages to provide frequency stability, power and energy management and enhance the ability of the microgrid to host renewable energy and supply critical loads while operating economically, in the event of FDI and or DoS/DDoS cyber-attacks. Recommendations and best practices for enhanced microgrid control and resiliency are concluded.

1.6. Dissertation Outline

Chapter 2: Microgrid Underlying Layers for Cyber Security Analysis and Cyber-Attack Modeling

The three constituting layers allowing analysis of the cyber security of microgrid systems, namely the power system, communication network and information exchange layers, are presented in this chapter. The methods used to model the layers and interface them to operate as a single entity while overcoming the downfalls of similar platforms available in the literature are explained. The various vulnerable access points to threat agents are presented and the cyber-attacks that could target the microgrid system are mathematically modeled with more emphasis attributed to attacks compromising data integrity and grid availability. Performance indices which allow the quantification of the cyber-attacks impact on the microgrid operation and the evaluation of the effectiveness of proposed mitigation solutions are defined. Operating bounds are evaluated to facilitate the selection of the cyber-attacks parameters so as to cause severe impacts and result in an infringement of the microgrid power and energy management requirements. The steps followed and the assumptions made in order to ensure cyber resilience and survivability of the microgrid in the event of detected or undetected cyber-attacks are finally presented.

Chapter 3: Control Loops for Enhanced Survivability of Microgrids against FDI Cyber-Attacks

Primary control loops, typically applied in the context of physical events, are added to the power-electronic interfaced DERs to enhance the microgrid survivability in the event of FDI cyber-attacks on the EMS, when detection schemes have been bypassed or haven’t operated in a timely manner. The control loops emulate virtual inertial response mimicking SMs operation and may be combined with droop control for additional cyber-attack compensation. The impact of the FDI cyber-attacks is quantified by means of reliability indices which facilitate the evaluation of the performance and effectiveness of the control loops. Adaptive load management strategies are also proposed to provide a second layer of cyber-attack compensation. Two microgrid configurations are investigated: SM based and 100% inverter-interfaced islanded microgrids. The results are validated on the real-time hardware-in-the-loop (HIL) co-simulation setup.

Chapter 4: Fallback Energy Management Control Strategy for DoS/DDoS Cyber-Attack Mitigation

A fallback control mitigation strategy is proposed to enhance the resiliency of microgrids against DoS/DDoS cyber-attacks compromising the communication network and causing the loss of information exchanged between the DERs and the microgrid controller in a microgrid operating the ESS as the grid-forming DER. A rule-based fallback control strategy is proposed in order to distribute the energy management functions of the EMS among the microgrid DERs. Advanced supplementary control loops added to the DERs primary controllers are proposed to provide coordination between the DERs without the reliance on vulnerable communication links. A detection mechanism allowing transition to the fallback control architecture is proposed. The DDoS cyber-attack is modeled, its impact is quantified and the performance of the proposed fallback mitigation strategy is tested and evaluated on the real-time HIL co-simulation setup for SM based and 100% inverter-interfaced islanded microgrids.

Chapter 5: Multi-Stage Cyber Resilient Control Infrastructure and Recommendations for Enhanced Cyber Security

A multi-stage cyber resilient control infrastructure extends and complements the work done in the previous chapters to ensure that, by design, microgrid systems could resist and survive FDI and or DoS/DDoS cyber-attacks while operating reliably and efficiently. For the sake of generality, the microgrid system considered operates a SM based DER as the grid-forming resource. The proposed strategy implements among others the control strategies of chapters 3 and 4 which are adjusted to ensure transient and steady-state stability, power and energy management, enhanced microgrid ability to supply critical loads and host renewable energy, and economic operation in the event of cyber disturbances. A parametric analysis is conducted to evaluate the performance of the proposed infrastructure and test its ability to adapt to the different operating conditions. Recommendations and best cyber security practices drawn from the research work performed are then concluded.

Chapter 6: Summary and Conclusions

The results and major contributions of this thesis are presented in this chapter. The applicability of the proposed analyses and methods to the practical engineering environment is

also highlighted. Finally, potential future research work that builds upon and supplements the contributions of this thesis is proposed.

Chapter 2

Microgrid Underlying Layers for Cyber Security Analysis and Cyber-Attack Modeling

2.1. Introduction

In this chapter, the microgrid power system along with its underlying information and communication network layers are separately modeled then interfaced to form the interconnected system. Assessment of the impact of different types of cyber-attacks on the microgrid power system operation along with validation and testing of the effectiveness of mitigation strategies employed at the control layer in enhancing the grid's resiliency when subjected to cyber disturbances will then be made possible.

The co-simulation platform developed in this chapter to interface the power system, communication network and information layers of a microgrid system overcomes the drawback of the tools presented in the literature [32-34], [36, 37]. For instance, the platform does not employ synchronization algorithms which halt the different simulators at fixed time-steps to enable information exchange leading to an accumulation of errors. In addition, it models the power system components, the underlying control strategies and the communication protocols in details, it

employs real-time simulators to accurately represent real-world microgrid systems, and it is easily extendable to model large scale power networks. The co-simulation tool is later used throughout the thesis to validate the concepts and theories proposed as it helps:

- Develop and evaluate the performance of different primary power control strategies and secondary EMSs modeled on digital controllers using HIL simulations
- Model and simulate different microgrid communication network components and topologies and information exchange based on legacy and modern communication protocols
- Credibly model real-world cyber-attacks exploiting the vulnerabilities of the microgrid communication network and information exchange layers, quantify their impact and evaluate and test the effectiveness of proposed mitigation solutions

Although implemented to model a specific microgrid system, the setup described in this chapter can be easily modified to represent any other power system as it incorporates all the building blocks needed at the power system, information and communication network levels.

Most of the work available in the literature either investigates cyber security from a communications perspective by modeling the cyber-attacks, evaluating their impact and proposing mitigations solutions applied at the network's layer or analyses cyber-attacks that compromise the large power system control functions such as state estimation and electricity market operations [122-124]. Very few are the studies that perform an analysis of cyber-attacks targeting microgrid systems' critical control functions from the power system, communications and information exchange perspectives. As the microgrid constituting layers are presented and interconnected, the chapter proceeds with a rigorous modeling of cyber-attacks which compromise the microgrid data integrity and availability, namely FDI and DoS/DDoS cyber-attacks. The steps that need to be followed by the attacker along with the assumptions considered are first explained succeeded by mathematical modeling of the FDI and DDoS cyber-attacks. Specific performance indices are defined to allow quantitative assessment of the cyber-attacks' impact and evaluation of the effectiveness of proposed mitigation solutions applied at the control layer in enhancing the resiliency and robustness of the microgrid in the event of cyber-attacks. The selection criteria of the cyber-attacks' parameters which violate the power and energy requirement of microgrid systems are then mathematically formulated. The assumptions made and the steps followed to

develop a microgrid control infrastructure which can survive undetected cyber-attacks and counteract detected cyber-attacks are finally presented.

2.2. Microgrid Constituting Layers

2.2.1. Co-simulation Platform Implementation

The three layers forming the microgrid systems are presented in Fig. 2.1. The microgrid real-time HIL co-simulation setup details and configuration are provided in Appendices A and C. The microgrid feeder and DERs along with the primary power management strategies defined in Appendix B and section 2.2.2.2 are modeled on a real-time digital simulator. The microgrid feeder and DERs measurements are sent using the IEC 61850 GOOSE messaging protocol, over a communication network, to the microgrid EMS which in turn evaluates dispatch set-points to operate the DERs. The real-time simulator provides an interface to publish and subscribe to IEC 61850 GOOSE messages. Therefore, the measurements and commands sent from/to the DERs are published/subscribed to over the communication network. Correspondingly, at the second end, another real-time simulator subscribes to and publishes the IEC 61850 measurements and commands which are exchanged over analog inputs and outputs with the National Instruments (NI) -cRIO digital controller. Additional details regarding the IEDs and their configuration in reliance with the IEC 61850 standard are provided in section 2.2.3 and Appendix C. The communication network emulator, OPNET, has a System-in-the-Loop (SITL) module which provides interconnection capabilities between the hardware and the software running the communication network. Therefore, the real-time simulator running the microgrid feeder and DERs could be seamlessly connected to the communication network emulated in OPNET which also connects to the second simulator running the EMS controller information exchange interface resulting in no accumulation of errors. The NI-cRIO connects over the IP network with the computer running the EMS script (formulated in section 2.2.2.1) to perform the optimization and generate dispatch set-points that are sent back to the real-time simulator which forwards them over the communication network to the microgrid DERs. As such, the three constituting layers of the microgrid system, namely the power system, communication network and information exchange layers are modeled and interconnected to form a closed loop and operate as a single entity.

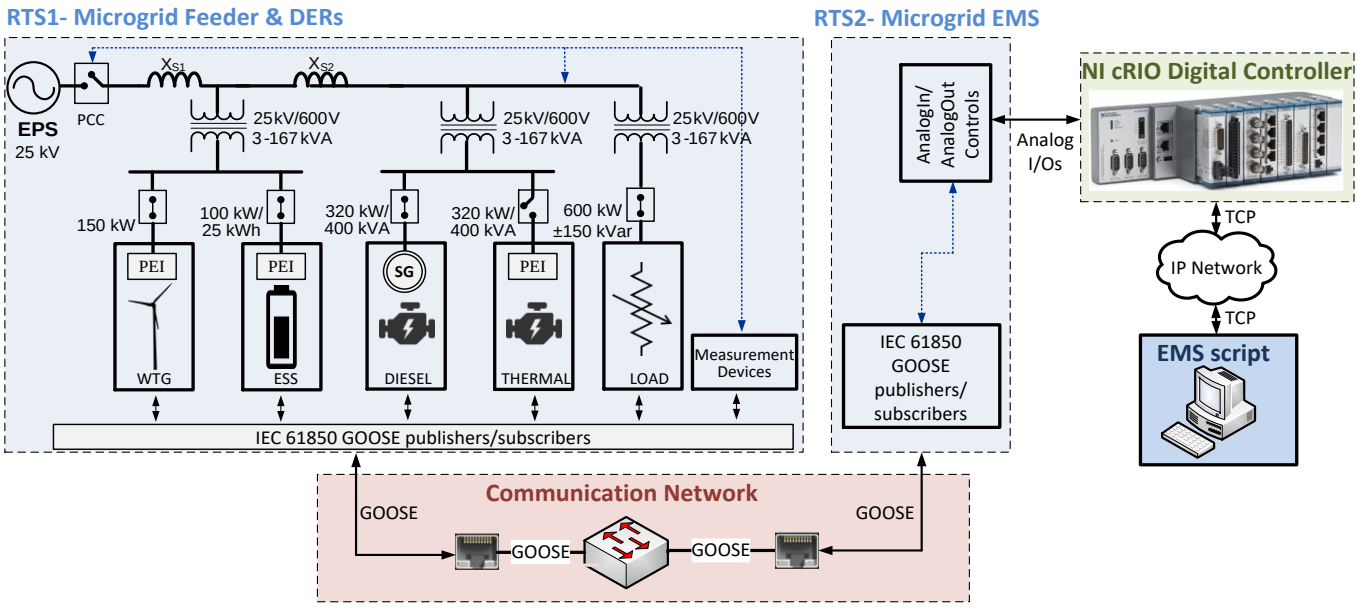

Fig. 2. 1: Microgrid system constituting layers

2.2.2. Microgrid Power System Layer

The microgrid power system layer consists of the DERs, loads and their underlying control infrastructure. The DERs typically employed in a microgrid system consist of SM based DERs, ESSs and renewable resources. Details pertaining to the modeling of the microgrid feeder, DERs and loads are provided in Appendix B. The extensive deployment of distributed renewable energy and energy storage resources in microgrids is technically feasible via the employment of power-electronic inverters to interface these DERs with the electric grid [125]. These power-electronic interfaces decouple the rotating masses from the electric grid (i.e. type 4 wind turbine generator (WTG)) or interface systems with no inertia (i.e. photovoltaics (PV), ESSs); hence they provide a poor voltage and frequency response in the event of disturbances, due to the lack of kinetic energy [115]. Managing the DERs power and energy and controlling the power-electronic interfaces is, therefore, a major concern when operating microgrids in an islanded mode [94]. The power and energy management strategies deployed throughout this thesis for DERs control and coordination are proposed and formulated in this section.

2.2.2.1. Microgrid EMS Function

The objective of the EMS employed throughout this thesis is to minimize the average cost of energy in the islanded microgrid. The objective function is formulated as follows:

$$\min\{C_d(t) + C_{ESS}(t) = \sum c\,(\alpha + \beta\, P_d(t) + \gamma\, P_d(t)^2) + \sum c_{ESS} P_{ESS}(t)\} \quad (2.\ 1)$$

Whereby $C_d(t)$ represents the cost of the power produced by the diesel generator at time t, $C_{ESS}(t)$the operational cost of the ESS, c the cost in \$/liters of diesel, α, β and γ the diesel generator quadratic parameters, c_{ESS} the levelized cost of the battery in \$/kWh, P_d and $P_{ESS}$the active power produced by the diesel generator and the ESS respectively. c_{ESS} represents the levelized cost of the ESS in \$/kWh, evaluated the average total cost of building and operating the ESS over its lifetime, divided by the total energy generated by the ESS over its lifetime.

The following constraints are to be met:

1) Active power balance:

$$P_{residual}(t) = P_L(t) - \sum_{\forall\, j \in RDER} P_j(t) = \sum_{\forall\, l \in\, dDER} P_l(t) \quad (2.\ 2)$$

Where $P_{residual}$ is the residual active power calculated as the load power P_L minus the power generated by the renewable DERs, RDER and dDER represent the renewable and the non-renewable DERs, respectively.

2) DERs capacity limits:

$$P_{DER}^{min} \leq P_{DER}(t) \leq P_{DER}^{max} \quad (2.\ 3)$$

Where $P_{DER}$is the active power generated by the DER, P_{DER}^{min} and P_{DER}^{max} the DER minimum and maximum active power limits.

3) Limits on ESS stored energy:

$$E_{ESS}^{min} \leq E_{ESS}(t) \leq E_{ESS}^{max} \quad (2.\ 4)$$

Where E_{ESS} is the energy stored in the ESS, E_{ESS}^{min} and E_{ESS}^{max} the ESS minimum and maximum energy limits.

4) ESS stored energy:

$$E_{ESS}(t) = E_{ESS}(t-1) - \eta P_{ESS}(t)\Delta t \quad (2.\ 5)$$

Where η is the ESS efficiency, P_{ESS} its active power and Δt the EMS dispatch period.

2.2.2.2. Power Management Strategies and Microgrid Configurations

The DER primary power control loops compensate for the power mismatch during the inter-dispatch period, the period between EMS dispatch set-points updates, whereby the local controllers coordinate to regulate the microgrid voltage and frequency. The local control loops are directly connected to the DERs and they do not rely on vulnerable communications to operate the resources. These control loops are therefore assumed to be secure, limiting the attackers' ability to maliciously tamper with their settings. Typically, in an islanded microgrid, one DER operates as the isochronous generator forming the microgrid voltage and frequency while the remaining DERs may or may not assist in providing voltage and frequency support [22, 23, 25].

Isochronous DER Power Control

In a SM based microgrid, a SM such as the diesel generator or a power-electronic interfaced ESS could operate as the grid-forming or isochronous DER. When operated as the isochronous, the diesel generator sets the voltage and the frequency of the microgrid; a voltage reference is fed to the excitation system and the mechanical power of the machine is set in accordance with a frequency reference and a proportional integral (PI) gain as shown in Fig. 2.2. In the case where the ESS is operated as the isochronous resource, its power-electronic interface is operated as a current-controlled VSI (Fig.2.3) whose dq-frame currents are dispatched in accordance to the primary controller set-points. This local control consists of two loops (Fig. 2.4); the outer regulates the grid frequency and voltage to their reference values and the inner controls the active and reactive power set-points. In such a configuration, active power mismatches are associated with frequency deviations.

In 100% inverter-interfaced microgrids, the ESS is operated as a voltage-controlled VSI. As shown in Fig. 2.5 the inverter control, in that case, consists of an outer loop to regulate the grid voltage and an inner one to regulate the inverter current. The frequency of the grid-side voltage is imposed and set to the nominal frequency by a virtual phase-locked-loop (PLL). Active power mismatches, in this case, are associated with voltage deviations.

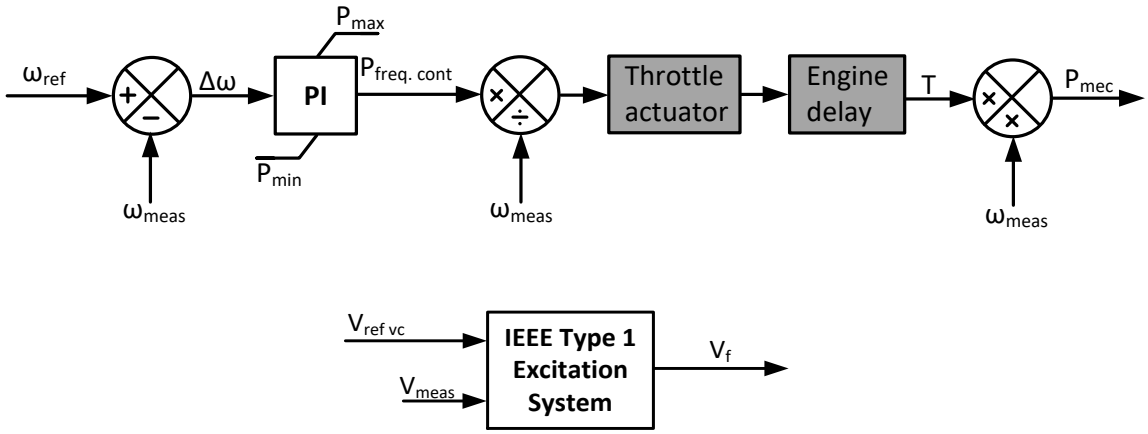

Fig. 2. 2: Synchronous generator with diesel engine operating in isochronous mode (upper) active power control loop (lower) reactive power control loop

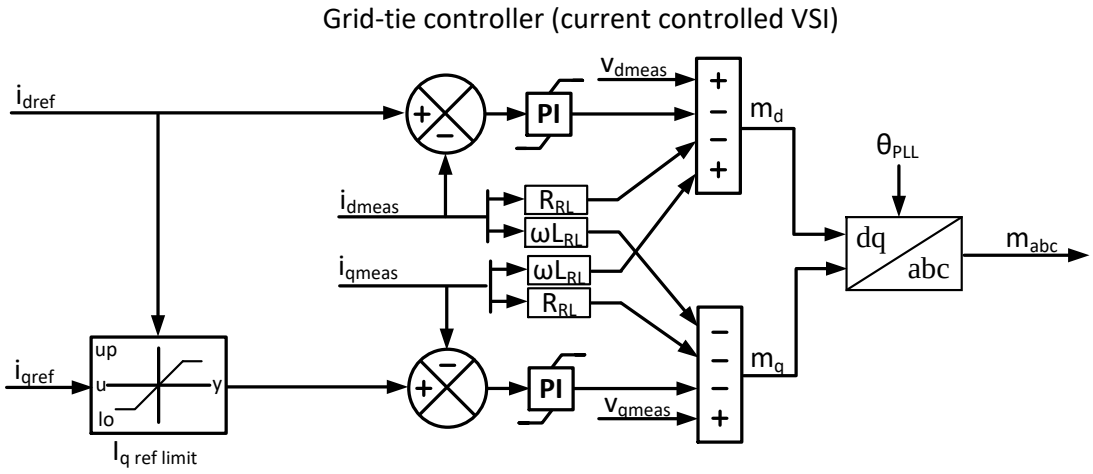

Fig. 2. 3: Grid-tie inverter control loops used for the ESS operating as a current source

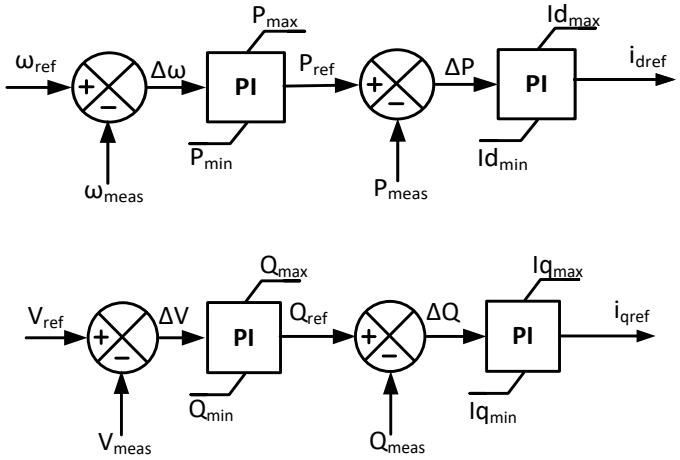

Fig. 2. 4: ESS current-controlled VSI for SM based microgrids (upper) active power control loop (lower) reactive power control loop

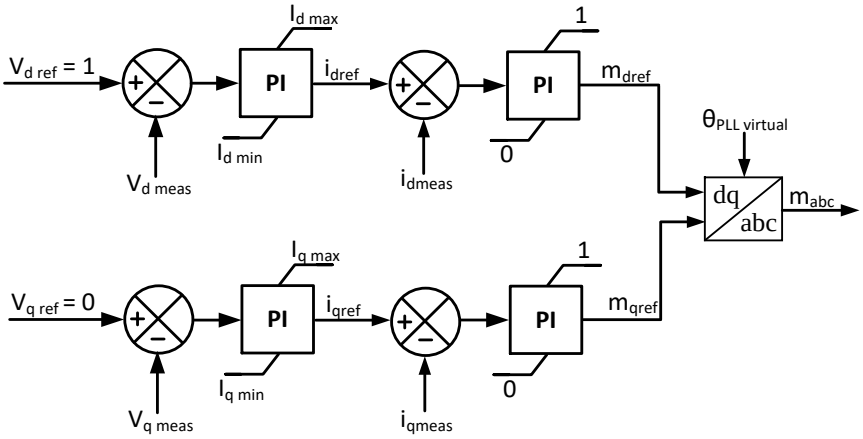

Fig. 2. 5: ESS voltage-controlled VSI for 100% inverter based microgrids

Grid-supporting DERs Power Control

The grid-supporting DERs can be directly connected to the grid through a rotating machine (i.e. SM based microgrids) or decoupled from the grid through a power-electronic interface (i.e. 100% inverter-based microgrids). The grid-supporting DERs in the microgrid may or may not participate in voltage and frequency support. Depending on their mode of operation, these DERs can function with or without a grid-forming DER in both grid-connected and islanded microgrids. Typically, the DERs are dispatched fixed active and reactive power references and are equipped to provide an additional power contribution based on frequency and voltage droops [126-129]. The active and reactive power droop contributions are specified in proportion to the deviations of the frequency and voltage from their reference values and the droop gains specified by the microgrid controller [25] as shown in Figs. 2.6 and 2.7. Droop control provides power sharing capabilities for the DERs and regulates the amount of power generated in accordance with the voltage and frequency profiles to ensure proper microgrid operation mimicking the self-regulation ability of synchronous generators [22]. A power smoothening contribution could also be added to the ESS fixed active power set-point and droop compensation to smoothen the high frequency power oscillations (greater than 1 Hz) generated by the renewable WTGs (Fig. 2.7).

Renewable DERs Power Control

The renewable DERs consist of grid-tie inverters with DC-links fed from DC-DC converters following their corresponding maximum power point tracking (MPPT) curves. The power generated by the DERs is typically evaluated in accordance with the wind speed or the solar irradiance and the corresponding MPPT curves as shown in Fig. 2.8. Supplementary control

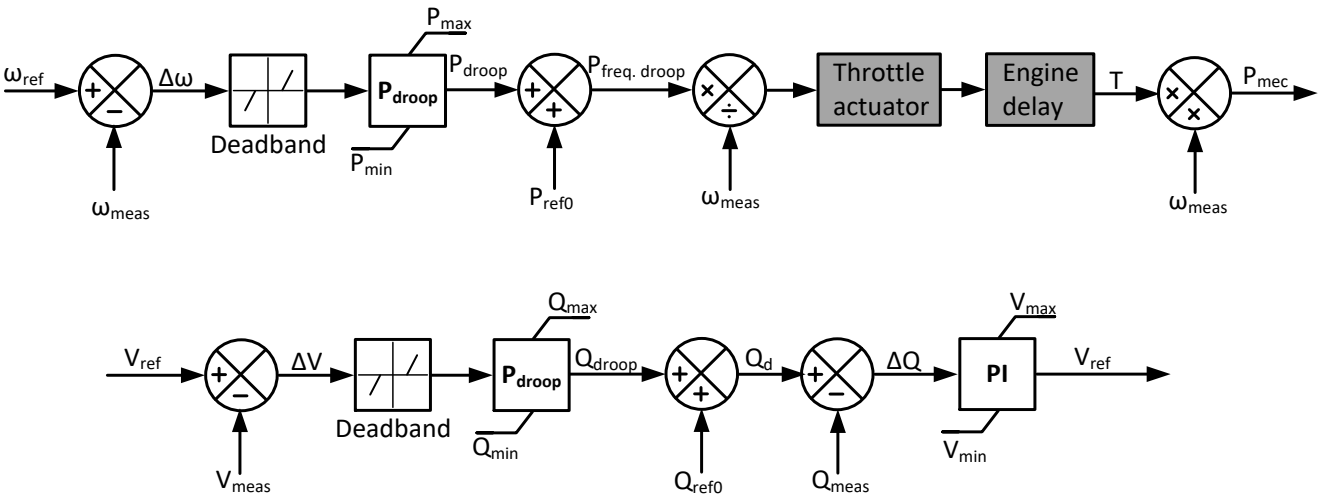

Fig. 2. 6: Synchronous generator with diesel engine operating in grid-supporting mode (upper) active power control loop (lower) reactive power control loop

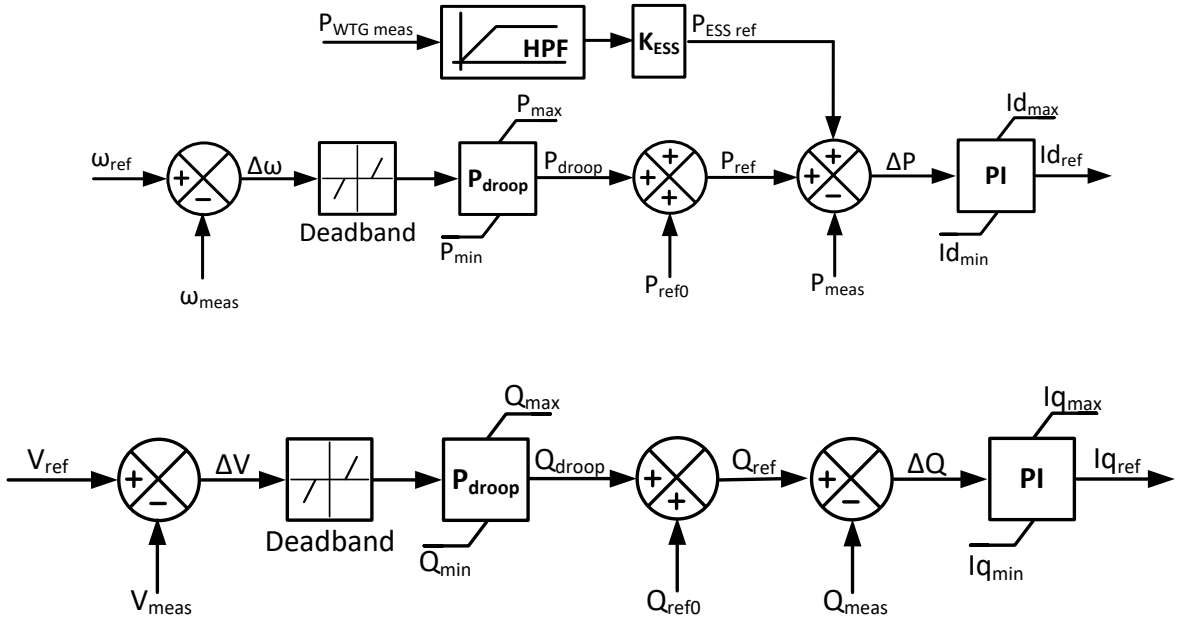

Fig. 2. 7: ESS operating in grid supporting mode (upper) active power control loop (lower) reactive power control loop

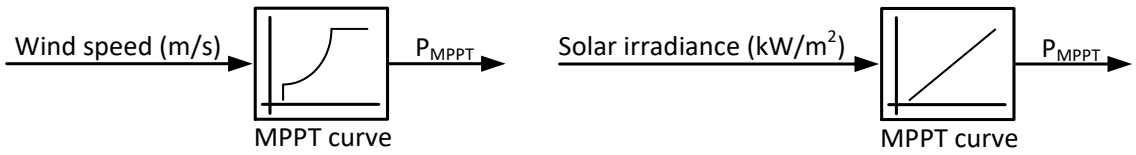

Fig. 2. 8: Look up tables used to emulate the WTG or PV DER

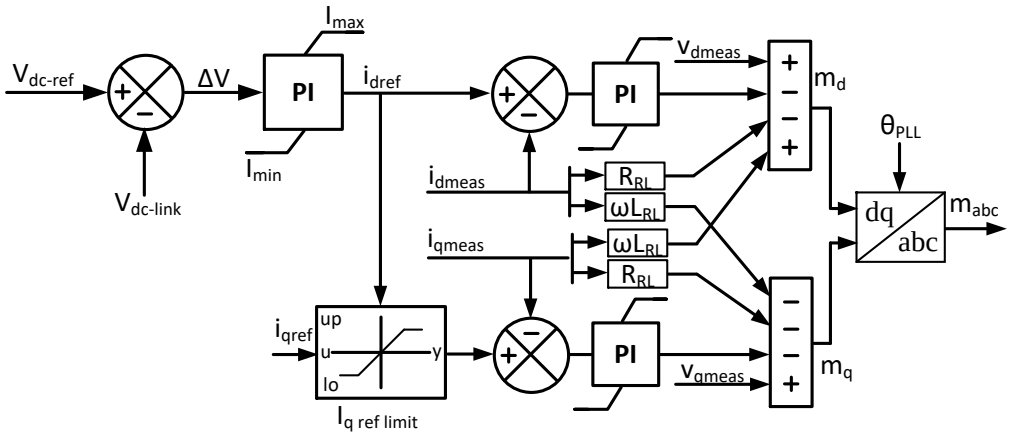

Fig. 2. 9: Renewable DER (WTG, PV) current-controlled VSI

functions can be added to the grid-feeding DERs local controllers in order to establish a reserve; a concurrent example is the deployment of functions featuring active power curtailment for frequency regulation [23]. The renewable DER power-electronic interface is operated as a current-controlled VSI with an outer loop that generates an inverter current reference to maintain a DC-link voltage (Fig. 2.9). The iq_{ref} current reference is dispatched in accordance to a primary controller, whose limits are defined by the converter ratings, prioritizing active power. In islanded mode, the DERs require the presence of an isochronous generator setting the grid voltage and frequency.

2.2.3. Microgrid Communication Network and Information Exchange Layers

The selection of the microgrid communication protocols, network topology and architecture depends on many factors including cost, operational constraints and most importantly the control objectives. As previously explained, the microgrid control architecture is assumed to be a centralized one whereby: 1) on a primary level, the DERs and their corresponding local controllers whose functions are defined based on the power management strategies employed, are tightly coupled and operate based on local measurements without the reliance on a communication network, and 2) on a secondary level, the microgrid EMS gathers statuses and measurements from the DERs and evaluates dispatch set-points and commands that are exchanged over a communication network.

Acting as an interface between the power system devices and the communication network, IEDs are configured to enable the exchange of measurements and commands between the DERs, loads and EMS. The IEC 61850 standard is recently gaining interest in distribution automation due to its real-time and low latency GOOSE messaging protocol and will be employed to exchange information between the microgrid DERs and EMS information exchange interface as it provides a suitable representation of microgrid systems. The IEC 61850 specifies for every IED a logical device to which corresponds one or many logical nodes defining the device's functions [130, 131]. The GOOSE protocol publisher/subscriber mechanism is defined such as the publisher writes values to a local buffer at the sending IED while the subscriber, at the receiving IED, reads the data from a local buffer [132]. The DERs and loads measurements obtained at the microgrid side are sent over the communication network to the EMS which evaluates dispatch set-points and circuit breaker commands that are sent back to the DERs and loads. At the microgrid side, a publisher is configured for every DER whose measurements are needed by the EMS and a subscriber is configured for every dispatchable DER requiring power set-points from the EMS to operate. Accordingly, at the microgrid controller EMS side, subscribers subscribe to the DER measurements and statuses and publishers publish the dispatch set-points and commands to the DERs.

A combination of real and simulated network elements is used to model the microgrid communication network. In fact, the communication network connecting the microgrid feeder and DERs to the EMS information exchange interface is simulated using the network emulator OPNET and consists of Ethernet links which connect the DERs' IEDs to the microgrid controller EMS interface through a switch to allow the exchange of IEC 61850 GOOSE messages. On the other hand, the microgrid digital controller performing the EMS functions is connected through analog channels to the EMS information exchange interface. The digital controller also connects over the IP network with its HMI which runs the EMS script to allow the exchange of measurements needed by the EMS to generate commands and dispatch set-points that are sent back to the digital controller over the IP network based on the transmission control protocol (TCP)/IP protocol.

2.3. Cyber-Attacks Modeling and Impact Quantification

Interest is attributed in this thesis to the analysis of cyber-attacks which impact is apparent on the operation of the microgrid power system layer. Cyber-attacks compromising the microgrid data integrity and availability are therefore considered; although cyber-attacks which target the grid confidentiality could severely affect the grid operators and customers' security and privacy, they will not be covered in this thesis as they do not directly affect the microgrid power system operation. FDI and DoS/DDoS cyber-attacks are typical examples of cyber-attacks compromising data integrity and availability and will be rigorously defined and modeled in this section. Various studies have analyzed cyber-attacks which jeopardize reactive power control in power systems. For instance, [52] evaluates the impact of data integrity attacks on reactive power control commands sent to operate voltage control devices causing abnormal voltage conditions and drifting the system to unstable operating points. Accordingly, the study performed in [133] showed how cyber-induced network delays targeting static VAR compensator (SVC) controllers, could affect the reactive power distribution in the power system, causing it to surpass the transient stability margins and possibly making it unstable. The main focus of this thesis though will be attributed to cyber-attacks which compromise the active power and energy management functionalities provided by microgrid controllers. Cyber-attacks compromising reactive power control are outside of the scope of the thesis.

2.3.1. FDI Cyber-Attack Modeling and Performance Indices

An FDI cyber-attack which tampers with the microgrid controller EMS dispatch set-points and commands sent to operate the DERs is modeled on the microgrid information exchange layer. The cyber-attacker is assumed to have valid credentials to connect to the IP network connecting the digital controller to its human machine interface (HMI). Different tools could then be used to allow the attacker to gain unauthorized access to the microgrid controller HMI and perform malicious actions without being noticed by the grid's operators. By doing so, the attacker can

maliciously modify the DERs set-points and circuit breakers' commands generated by the EMS before being sent over analog channels to the real-time simulator running the microgrid controller. The FDI attack which tampers with the EMS dispatch set-point consists of simply adding a bias to the DER dispatch set-point such that:

$$P_{DER\_FDI}(i\Delta t) = P_{DER}(i\Delta t) + B\,(t_A) \quad (2.6)$$

$$\text{s.t.} \qquad B(t) = \begin{cases} B & \text{if } t \geq t_A \\ 0 & \text{elsewhere} \end{cases}$$

Whereby $P_{DER\_FDI}(t)$ is the modified DER active power at time t (kW) and $B(t)$ the bias value at time t (kW), t_A the time of the attack (s), Δt the EMS dispatch period (s) and T the duration of the simulation.

The value of the index i in equation (2.6) and (2.7) is a constant which could take one of the values $\left[1, \dots, {}^{T}/_{\Delta t}\right]$ and is evaluated based on the time of the attack such that $(i-1)\Delta t < t_A \leq i\Delta t$.

The FDI cyber-attack which modifies the commands sent to operate the microgrid DERs circuit breakers causing malicious unplanned disconnection or reconnection of the DER is modeled as follows:

$$P_{DER\_FDI}(i\Delta t) = |c-1|\,P_{DER}(i\Delta t) \quad (2.7)$$

$$\text{s.t.} \quad c = \begin{cases} 1 \text{ if the circuit breaker is open} \\ 0 \text{ if the circuit breaker is closed} \end{cases}$$

Whereby c is the binary value specifying the DER's circuit breaker status.

In the case of a microgrid operating with a large mix of low inertia power-electronic interfaced DERs the FDI attacks will cause system-wide power imbalance, resulting in large voltage or frequency excursions. If the DERs primary controllers cannot compensate for the large power imbalances to regulate voltage and frequency, protective schemes limiting the cyber attack's burden will initiate.

Performance indices are employed to evaluate the cyber-attacks' impact and the effectiveness of the proposed mitigation solutions in counteracting the FDI cyber-attacks targeting SM based and 100% inverter-interfaced microgrids. In SM based microgrids, active power disturbances resulting from the FDI cyber-attacks are associated with frequency excursions. While in 100% inverter-interfaced microgrids, cyber-induced active power imbalances result in voltage

excursions. This is due to the fact that in SM based microgrids, the synchronous generators rotating masses provide kinetic energy in the event of frequency deviations. Therefore, the frequency is directly coupled to the rotational speed of the synchronous generators and thus to active power balance [134]. On the other hand, microgrids deploying inverter-interfaced DERs only, lack this kinetic energy. In addition, low and medium voltage microgrid systems are typically resistive with a very low inductance as compared to the resistance resulting in a small power angle [22]. Therefore, in 100% inverter-interfaced microgrids, the voltage amplitude mainly depends on the active power flow, while its frequency is mainly affected by the reactive power injection.
The indices considered are therefore defined as follows:

- Frequency and voltage nadirs f_{nadir} and V_{nadir}, specifying the lowest value observed in the frequency and voltage responses in SM based and 100% inverter-interfaced microgrids targeted by FDI cyber-attacks, respectively (Hz and p.u.):

$$f_{nadir} = \min(f(t_A + m\Delta t)) \qquad \forall m = 0,1,2,\dots,end \tag{2. 8}$$

$$V_{nadir} = \min(V(t_A + m\Delta t)) \qquad \forall m = 0,1,2,\dots,end \tag{2. 9}$$

- The time to restore the frequency t_{rest_SM} and the voltage t_{rest_inv} back to their nominal operating values after the occurrence of the cyber event in SM based and 100 % inverter-interfaced microgrids, respectively (s):

$$t_{rest\_SM} = t(f = f_{nom}) - t_A \tag{2. 10}$$

$$t_{rest\_inv} = t(V = V_{nom}) - t_A \tag{2. 11}$$

- The amount of load unserved due to the initiation of load shedding schemes in the post-attack period (kW).

2.3.2. DDoS Cyber-Attack Modeling and Performance Indices

Although there are different strategies that could be followed to successfully perform a DDoS cyber-attack, such as UDP, TCP, ICMP flood and Smurf attacks, [135] in this thesis, a TCP SYN flood is performed to compromise the microgrid centralized controller EMS, depriving the DERs from receiving updated dispatch set-points. The TCP SYN flooding attack exploits the TCP protocol three-way handshake mechanism, limited in maintaining half-open connections. The steps required to launch the attack consists of the following:

1) The attacker connects to the IP network and scans for vulnerable hosts with abundant resources enabling them to perform powerful attacks.
2) The attacker exploits the vulnerabilities and gains access to the hosts. The attacker controls the compromised hosts to send, using fake IP addresses as a source, a large number of SYN packets to the victim, the host running the microgrid EMS script and HMI.
3) As the victim receives the SYN packets, it replies with an SYN-ACK and waits for some time to receive an ACK response to establish the connection.
4) Due to the fictitious source address, no ACK would be returned to the victim creating a large number of half-open connections. These unestablished connections cause the connection queues and memory buffer to fill up consuming the victim's resources. As all the resources are exhausted, legitimate TCP users, mainly the digital controller, would be denied service and would no longer be able to communicate with the targeted host.

As a result of the flooding, the DERs measurements sent from the digital controller are no longer sent over the network and therefore do not reach the compromised host running the optimization engine. This can be clearly observed on the controller HMI which no longer updates the DERs measurements as they vary on the grid side. The optimization script terminates in the absence of input measurements and no longer evaluates dispatch set-points to operate the DERs. Therefore, the EMS dispatch set-points sent over the analog channels will no longer be updated and the IEC 61850 GOOSE commands sent to operate the DERs will be held at a value equal to the one generated prior to the attack. The dispatchable DERs dispatch set-points resulting from the application of the DDoS cyber-attack are formulated as follows:

$$\mathrm{P_{DER\_DDoS}}\big((\mathrm{i}+\mathrm{j})\Delta\mathrm{t}\big) = \mathrm{P_{DER}}\big((\mathrm{i}-1)\Delta\mathrm{t}\big) \quad \text{for } \mathrm{j} = 0, 1, \dots, {}^{\mathrm{T_A}}/_{\Delta\mathrm{t}} \tag{2. 12}$$

Whereby, $P_{DER\_DDoS}(t)$ is the dispatch set-point sent to operate the DER at time t following the DDoS attack (kW), $P_{DER}(t)$ the dispatch set-point generated by the EMS at time t, t_A the time of the attack (s), T_A the attack period (s), Δt the EMS dispatch period (s) and T the duration of the simulation.

The value of the index i is a constant which could take one of the values $\left[1, \dots, {}^{\mathrm{T}}/_{\Delta\mathrm{t}}\right]$ and is evaluated based on the time of the attack such that $(\mathrm{i}-1)\Delta\mathrm{t} < \mathrm{t_A} \leq \mathrm{i}\Delta\mathrm{t}$. The index j is introduced

in (2.12) to show that all the dispatch set-points sent to the DER at each EMS update after the attack will be equal to the one generated before the attack.

The DDoS cyber-attack causes loss of information sent to and from the microgrid - controller. As a result, the microgrid feeder and DERs will have to operate in a fully-decentralized manner. The dispatchable DERs primary control loops inherently rely on the information received by the EMS to operate properly. Therefore, in the absence of supplementary or enhanced control loops which account for this unplanned loss of information large frequency excursions will result activating the protection schemes and causing unnecessary load and or generation curtailment. In order to quantify the impact of the DDoS cyber-attack and to evaluate the effectiveness of the mitigation strategies applied, the following indices will be calculated as follows:

- The maximum and minimum frequencies f_{min} and f_{max} which specify the lowest and highest values in the frequency response in the post-attack period (Hz), respectively in SM based microgrids:

$$f_{min} = min(f(t_A + mt_s)) \quad \forall m = 0,1,2,\dots,\frac{T_A}{t_s} \tag{2. 13}$$

$$f_{max} = max(f(t_A + mt_s)) \quad \forall m = 0,1,2,\dots,\frac{T_A}{t_s} \tag{2. 14}$$

Where t_s is the simulation time step (s) and T_A the attack period (s).

- The maximum and minimum voltage V_{min} and V_{max} which specify the lowest and highest values in the voltage response in the post-attack period (Hz), respectively in 100% inverter-interfaced microgrids:

$$V_{min} = min(V(t_A + mt_s)) \quad \forall m = 0,1,2,\dots,\frac{T_A}{t_s} \tag{2. 15}$$

$$V_{max} = max(V(t_A + mt_s)) \quad \forall m = 0,1,2,\dots,\frac{T_A}{t_s} \tag{2. 16}$$

- The amount of load not served (kWh)

$$E_{\text{L not served}} = \sum_{t=0}^{T} P_{\text{L Base Case}}(t)\Delta t - \sum_{t=0}^{T} P_{\text{L served}}(t)\Delta t \tag{2. 17}$$

Whereby, $P_{L\,served}(t)$ is the load served at time t in kW, $P_{L\,Base\,Case}(t)$ the load served under normal operating conditions at time t in kW and Δt the time step.

- The amount of generation curtailed (kWh)

$$E_{\text{shed}} = \sum_{t=0}^{T} P_{\text{Base Case}}(t)\Delta t - \sum_{t=0}^{T} P_{\text{generated}}(t)\Delta t \tag{2. 18}$$

Whereby, $P_{generated}(t)$ is the active power generated by the DER at time t (kW) and $P_{Base\ Case}(t)$ the power generated by the DER at time t under normal operation (kW).

- The average cost of energy ($/kWh)

$$\text{Cost} = \frac{\sum_{t=0}^{T}(C_d(t)+C_{ESS}(t))\Delta t}{\sum_{t=0}^{T} P_{L\ served}(t)\Delta t} \quad (2.\ 19)$$

Whereby C_d and C_{ESS} are the costs of operating the diesel generator and the ESS as defined in section 2.3.

2.3.3. Cyber-Attacks Parameters Selection

Whether FDI or DDoS, the cyber-attacks considered in this thesis compromise the microgrid controller EMS operation by modifying the set-points and commands or by disabling the communication. In order for the attack to have a significant impact on the microgrid operation, its parameters could be selected to maximize the violation of the power and energy constraints stipulated by the secondary control formulated in section 2.2.2.1.

The study performed in [118] showed that a microgrid which features an isochronous DER inherently provides additional robustness and resilience to cyber-attacks than a microgrid operating the dispatchable DERs in droop control mode. For this reason, the power management strategies employed in this thesis will always consist on microgrids featuring a grid-forming DER. Consequently, the microgrid considered will feature one grid-forming DER that could be an SM or an ESS, renewable DERs, dispatchable generators and loads. Power balance is met when:

$$P_{\underset{DER}{isochronous}}(t) = P_{residual}(t) - \sum_{\forall\ q \in DDER} P_q(t) \quad (2.\ 20)$$

Whereby, $P_{\underset{DER}{isochronous}}(t)$ is the active power generated by the isochronous DER at time t (kW), and DDER the dispatchable DERs which are not operating in isochronous mode.

To ensure that the isochronous DER always has enough power to provide its functions in forming and regulating the microgrid voltage and frequency, the following condition must apply:

$$P^{min}_{\underset{DER}{isochronous}} \leq P_{\underset{DER}{isochronous}}(t) \leq P^{max}_{\underset{DER}{isochronous}} \quad (2.\ 21)$$

Whereby, $P^{min}_{\underset{DER}{isochronous}}$ and $P^{max}_{\underset{DER}{isochronous}}$ are the minimum and maximum active power limits of the isochronous resource (kW).

Assuming that the microgrid features only one dispatchable DER, in order for the FDI cyber-attack to cause violation of the EMS power balance constraints, the bias should be evaluated such that one of the following conditions is violated:

$$B(t_A) \leq P_{residual}(i\Delta t) - P_{DDER}(i\Delta t) - P^{min}_{\substack{isochronous \\ DER}} \quad (2.\ 22)$$

$$B(t_A) \geq P_{residual}(i\Delta t) - P_{DDER}(i\Delta t) - P^{max}_{\substack{isochronous \\ DER}} \quad (2.\ 23)$$

Accordingly, in the case where the FDI attack tampers with the DER circuit breaker command (2.22) and (2.23) still apply with a bias value equal to the DER active power prior to the attack. Based on the same line of reasoning, the following conditions should be violated in order for the DoS/DDoS cyber-attack to cause a violation of the power balance constraints set by the EMS to ensure that the isochronous resource provides its main functions:

$$P_{DDER}\big((i-1)\Delta t\big) \leq P_{residual}\big((i+j)\Delta t\big) - P^{min}_{\substack{isochronous \\ DER}} \quad (2.\ 24)$$

$$P_{DDER}\big((i-1)\Delta t\big) \geq P_{residual}\big((i+j)\Delta t\big) - P^{max}_{\substack{isochronous \\ DER}} \quad (2.\ 25)$$

In the case where the ESS is operated as the grid-forming DER, the ESS should not only operate within its power limits, the energy bounds defined in (2.4) also need to be respected to ensure proper operation. Using (2.4) and (2.5), the ESS energy could be written as:

$$E_{ESS}\,(t) = E_{ESS}(t-\Delta t) + \eta\Delta t(P_{residual}(t) - \textstyle\sum_{\forall\, q\in DDER} P_q(t)) \quad (2.\ 26)$$

Assuming the microgrid features only one dispatchable DER, one of the following conditions should be violated for an FDI attack to cause exhasution of the isochronous ESS energy limits:

$$B(t_A) \leq P_{residual}(i\Delta t) - P_{DDER}(i\Delta t) - \frac{\left(E^{min}_{ESS} - E_{ESS}((i-1)\Delta t)\right)}{\eta\Delta t} \quad (2.\ 27)$$

$$B(t_A) \geq P_{residual}(i\Delta t) - P_{DDER}(i\Delta t) - \frac{\left(E^{max}_{ESS} - E_{ESS}((i-1)\Delta t)\right)}{\eta\Delta t} \quad (2.\ 28)$$

Accordingly, a successful DoS/DDoS cyber-attack resulting in the exhaustion of the ESS energy could be performed if one of the following conditions is violated:

$$P_{DDER}\big((i-1)\Delta t\big) \leq P_{residual}\big((i+j)\Delta t\big) - \frac{\left(E^{min}_{ESS} - E_{ESS}((i+j-1)\Delta t)\right)}{\eta\Delta t} \quad (2.\ 29)$$

$$P_{DDER}\big((i-1)\Delta t\big) \geq P_{residual}\big((i+j)\Delta t\big) - \frac{\left(E^{max}_{ESS} - E_{ESS}((i+j-1)\Delta t)\right)}{\eta\Delta t} \quad (2.\ 30)$$

It is important to mention that an attacker who manages to gain access to information pertaining to the microgrid configuration, generation mix, power and energy management strategies employed, and DERs power and energy limits would be able to reformulate equations (2.20) through (2.30). This would enable the attacker to launch cyber-attacks inflicting the most severe impacts violating the power and energy management functionalities provided by the microgrid controller.

2.4. Cyber-Attack Prevention, Detection and Mitigation: Strategy Followed and Assumptions

Before proceeding to chapter 3, it is important to first present the strategy followed and the assumptions made in this thesis. When analyzing cyber security of cyber-physical systems, it is imperative to consider all the possible scenarios and to account for the limitations of the different schemes employed to enhance cyber resiliency. Therefore, in this thesis the following assumptions are made:

1- As mentioned in section 1.3, the prevention schemes currently deployed in smart grids and cyber-physical systems in general, have proved to be efficient in different scenarios; however, real-world scenarios have shown that they either have limitations or are not being properly deployed and hence are being bypassed. Cyber-attackers are assumed to have the skills required to bypass the prevention strategies deployed and to successfully launch cyber-attacks.

2- Cyber-attack detection: Detection methods such as physical watermarking and moving target cannot be applied to detect the FDI attacks considered in this thesis as they are typically implemented to detect attacks on sensor measurements. In fact, the attacks covered in this thesis consider attackers who gain access to the microgrid EMS and modify the controller's commands and set-points. At this access level, the extraneous states and their varying dynamics along with the physical watermark would all be known by the attacker defeating the main assumptions set by those detection schemes.

   Therefore, the work performed in this thesis assumes that an IDS which monitors both, the network activity and the physical processes and their underlying power system theories of

the microgrid is employed to detect FDI and DDoS cyber-attacks. Regardless of the type of the IDS deployed and the rules set, false alarms and missed detections are impossible to be avoided [136]. The thesis will therefore tackle the problem of quantifying the impact of detected and undetected FDI and DDoS cyber-attacks and evaluating the performance of different control strategies in mitigating their effects on the microgrid system operation.

3- Fault detection: It is assumed that fault detection schemes are also employed to detect the physical faults that could occur in the microgrid and that post-fault strategies are implemented to isolate and mitigate them [137-139]. Just like cyber-attack detection schemes, the fault detection schemes also result in missed detections and false alarms. Therefore, the same strategies followed to enhance the survivability of the microgrid in the event of undetected cyber-attacks will be followed in the case of undetected faults. In fact, if not detected, both events would result in the degradation of the microgrid operation and therefore adding control loops to compensate for the impact they induce would enhance the grid reliability.

The research work performed in this thesis is not intended to propose advanced solutions for cyber-attack and fault detection, instead it focuses on evaluating the impacts of cyber-attacks, testing and proposing potential solutions applied at the control level to enhance the microgrid resiliency and survivability. Therefore, for the sake of completeness, it is necessary to account for the scenarios where detection schemes are successful and the ones where they are not.

The block diagram of Fig. 2.10 presents the steps followed in the upcoming chapters in order to ensure microgrid resiliency in the event of the FDI and DDoS cyber-attacks presented in section 2.3 while taking into account that the detection schemes cannot always guarantee successful attack detection. The enhanced local control loops that could be added to the DERs to provide voltage and frequency support in the event of undetected FDI cyber-attacks causing sudden transient disturbances are presented in chapter 3. The fallback control strategy responsible for power and energy management in the event of cyber-attacks is proposed in chapter 4. Finally, the combination of the different schemes operating at three different levels to provide a multi-stage cyber resilient control infrastructure for microgrid systems is presented in chapter 5.

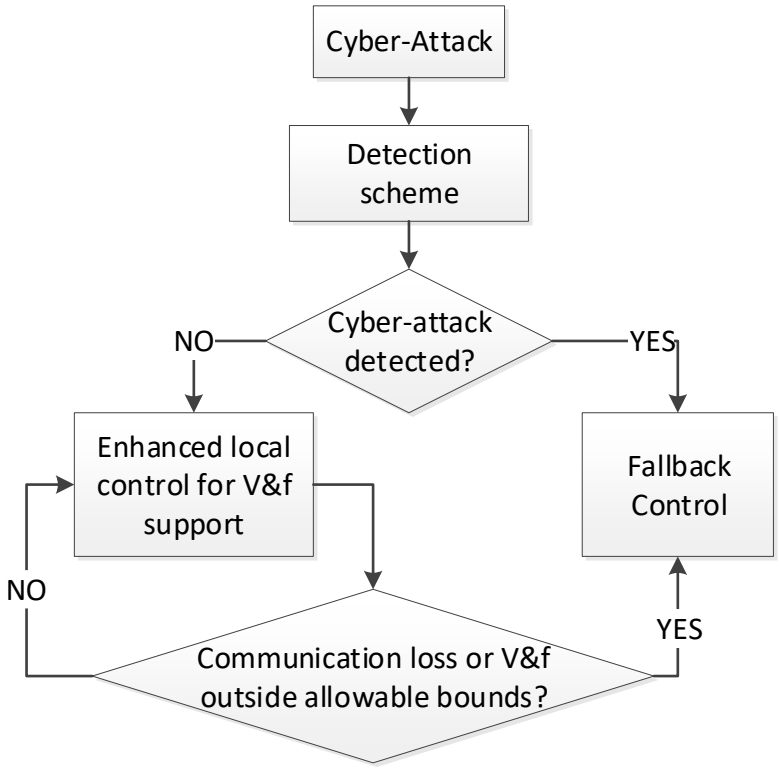

Fig. 2. 10: Block diagram of the strategy followed for cyber resiliency

2.5. Conclusion

Communication networks are becoming part and parcel of smart power grids as they provide, amongst others, real-time sensing, monitoring and control capabilities. Just like large power systems, microgrids also require a communication network to provide these advanced capabilities. This reliance on ICTs creates access points to cyber intruders which could launch cyber-attacks affecting the microgrid operation. To study and analyze microgrids operation, the power system and its underlying communication network and information exchange layers must all be modeled and seamlessly interfaced, especially when cyber security is of concern. The majority of the co-simulation platforms presented in the literature either suffer from synchronization issues which cause an accumulation of errors or do not provide detailed modeling of the three underlying layers.

This chapter started by detailing the microgrid underlying power system, information exchange and communication network layers. The layers were seamlessly interfaced to form the real-time HIL co-simulation platform used throughout this thesis to perform impact assessment

studies and to test the performance of the proposed cyber-resilient control methods in the event of cyber-attacks. The chapter proceeded with a listing of the steps that any attacker could follow and the underlying assumptions that allow launching of FDI or DDoS cyber-attacks. The cyber-attacks were then mathematically modeled, and performance indices were defined to enable quantification of the attacks' impact and evaluation of the effectiveness of the mitigation strategies proposed in the upcoming chapters. Bounds on the cyber-attacks' parameters were evaluated such that the main requirements of the microgrid controller, being power and energy management, are violated maximizing the impact the cyber-attack could have on the microgrid operation. Finally, the steps followed and the assumptions made in the upcoming chapters to survive and react to cyber-attacks were presented. The upcoming chapter analyzes FDI cyber-attacks on the microgrid controller EMS in the event where the implemented detection strategy fails to detect the attacks. The performance of local control strategies, commonly implemented to compensate for physical disturbances, applied in the context of undetected FDI cyber-attacks to provide transient and steady-state voltage and frequency regulation is evaluated. Adaptive load shedding schemes are proposed to ensure power and energy balance. The impact of the cyber-attacks is evaluated using the predefined performance indices and the performance of the control schemes is evaluated for SM and 100% inverter-interfaced microgrids on the real-time HIL co-simulation platform presented in this chapter.

Chapter 3
Control Loops for Enhanced Survivability of Microgrids against FDI Cyber-Attacks

3.1. Introduction

The primary power management control strategy employed to locally operate the DERs, along with the type of DERs and their penetration levels largely impact the microgrid transient voltage and frequency stability. The extensive reliance on power-electronics interfaced DERs results in microgrids with very low inertia. In low inertia microgrids, small active power imbalances cause large voltage or frequency excursions, especially when operating in islanded mode, in the absence of an EPS operating as a slack bus [59, 140, 141]. FDI cyber-attacks which compromise the microgrid controller EMS and maliciously tamper with the dispatch set-points and the commands sent to operate the dispatchable DERs and circuit breakers were modeled in the previous chapter. A list of the schemes that could be employed to detect cyber-attacks compromising data integrity and their limitations were presented in section 1.3.4.1. As stated in the previous chapter, it is of paramount importance to account for all the scenarios and possible failures that could occur in the system when analyzing cyber security. This chapter investigates FDI cyber-attacks compromising

the data integrity of microgrid systems in specific, when attackers have successfully bypassed the detection schemes employed. Chapter 5 further analyzes the scenarios where the FDI cyber-attacks have been successfully detected and proposes potential mitigation solutions. The impacts of the FDI cyber-attacks on the operation of SM and 100% inverter-interfaced microgrids are quantified using specific performance indices. Virtual inertial response which could be combined with droop control, employed in the literature to provide frequency support in the event of generation and load outages, is added in this chapter to the power-electronic interfaced DERs local controllers of SM based and 100% inverter interfaced microgrids to evaluate its performance in improving the frequency and the voltage response in the event of undetected FDI attacks. Adaptive load management schemes are also proposed to provide post-attack power and energy balance. The FDI cyber-attacks' impact is quantified and the ability of the control loops to enhance the grid survivability is evaluated for SM and inverter-interfaced microgrids modeled on the real-time HIL co-simulation platform presented in the previous chapter.

3.2. Control Loops for FDI Cyber-Attacks Mitigation

3.2.1. SM Based Microgrids

3.2.1.1. Combined Droop and Virtual Inertial Response

If data integrity cyber-attacks detection schemes do not operate in a timely manner or are successfully bypassed by attacker, an FDI cyber-attack which tampers with the microgrid EMS dispatch set-point or commands sent to operate the DER or its circuit breaker results in active power disturbances, that could induce large frequency excursions in SM based microgrids. The amplitudes of the excursions largely depend on the microgrid inertia and the grid-forming resource's dynamic response and ability to compensate for the attack. Therefore, it is critical that the fast-acting power-electronic interfaced DERs local controllers have the ability to provide frequency support, especially when the FDI cyber-attack targets microgrids with very low inertia or when the isochronous DER has a very slow dynamic response.

In order to benefit from the fast-acting capabilities of ESSs as proposed in [112-114], a combined virtual inertia and droop controller added to the ESS local control is presented in this section. The virtual inertia and droop control loops are similar to the ones deployed in [116] and [23] and are applied to the ESS control. The proposed enhanced control is tested in order to ensure improved transient and permanent frequency support in the presence of FDI attacks such as the ones previously described in section 2.3.1. The virtual inertia controller employed emulates the inertia of synchronous generators. The ESS injects/absorbs active power $P_{inertia}$(pu) in proportion to the reference speed ω_{ref}(p.u.), the rate of change of the frequency excursion $d(\omega_{ref} - \omega_{meas)}/dt$ and the equivalent inertia H_{eq} as shown in the lower block diagram of Fig. 3.1 and formulated in (3.1). The common differentiation operation is hypersensitive to the noise in the frequency measurements and will therefore pickup the high frequency components of its input signal and amplify the noise. A low-pass filter, with a bandwidth which ensures that important system dynamics are not filtered out, is therefore employed to smoothen the derivative of the input signal [110, 116, 142].

$$P_{inertia} = 2H_{eq}\omega_{ref}\frac{d(\omega_{ref}-\omega_{meas})}{dt} = K_{inertia}\frac{d(\omega_{ref}-\omega_{meas})}{dt} \quad (3.1)$$

As for the droop control scheme, an active power contribution proportional to the frequency deviation from the reference value is generated as in (3.2):

$$P_{droop} = K_{droop}(\omega_{ref} - \omega_{meas}) \quad (3.2)$$

Where K_{droop} is the droop gain and ω_{meas} is the measured speed (p.u.).

The combined control shown in Fig. 3.1, is achieved by adding the active power contribution of each of the control loops. The resulting combined active power correction $P_{combined}$ is then added to the EMS active power dispatch set-point for the ESS P_{ref0}:

$$P_{DER} = P_{ref0} + K_{droop}(\omega_{ref} - \omega_{meas}) + K_{inertia}\frac{d(\omega_{ref}-\omega_{meas})}{dt} \quad (3.3)$$

The virtual inertia and droop controllers only activate when active power imbalances result in frequency excursions exceeding the bounds set by their corresponding Dead Zone block (Fig. 3.1). The Selector block of Fig. 3.1 generates as output the active power compensation pertaining to the selected control loop, i.e. droop control, virtual inertial response or the combined droop and virtual inertial controller. This would enable testing of the different control strategies deployed separately or combined.

The combined virtual inertia and droop controller could be considered as a conventional proportional derivative (PD) controller. A lot of research has been performed in order to optimally tune such controllers [143]. The focus of the work, in similarity to the studies reviewed in section 1.3.5.2 [23], [111], is to evaluate the performance of the combined controller in enhancing the system's stability in the event of cyber-attacks. Therefore, the droop and inertia gains are tuned such that they provide transient and steady-state compensation reducing the frequency nadir, the amount of load energy curtailed and the time needed to restore the frequency back to its nominal value without inducing unwanted oscillations. In fact, as explained in section 3.4.1.3, the gains are evaluated for the worst-case FDI cyber-attack such that the selected gains could also provide maximum compensation when the attacks are less severe.

3.2.2. Inverter-Interfaced Microgrids

The mitigation strategy proposed hereafter consists of a two-layer cyber-resilient control strategy applied to 100% inverter-interfaced microgrids targeted by FDI cyber-attacks such as the ones formulated in section 2.3.1. On one hand, supplementary control loops based on the concept of virtual inertial response, are added to the VSI primary controllers to respond to the voltage excursions resulting from the attack. On the other hand, in the event where supplementary control is not sufficient to compensate for the attacks, an adaptive load management scheme which ensures active power balance is proposed.

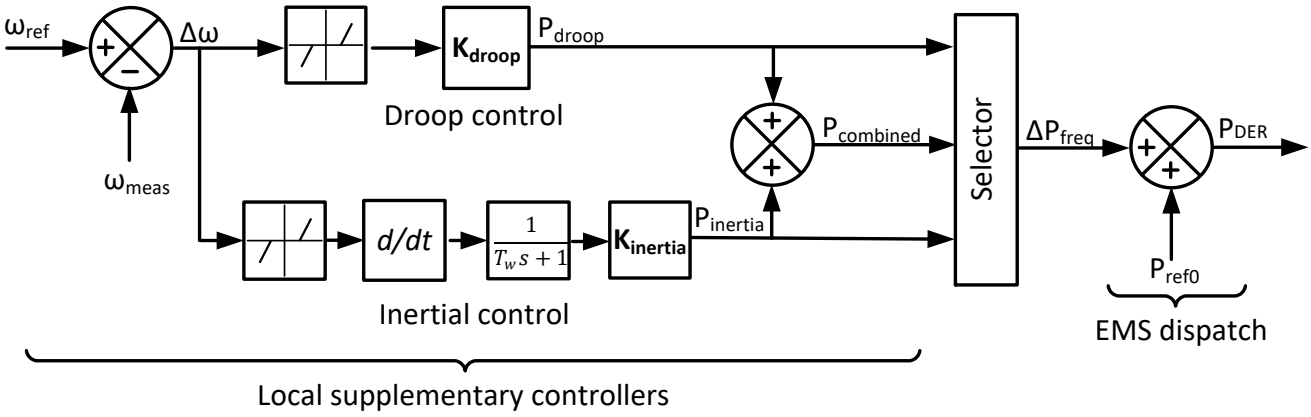

Fig. 3. 1: ESS VSI supplementary combined control

3.2.2.1. Supplementary Control for VSIs

The tight coupling between active power and voltage in an inverter-interfaced islanded microgrid causes FDI cyber-attacks inducing active power imbalances to result in voltage excursions. As a solution and in analogy with the virtual inertia concept applied to regulate frequency excursions, a virtual inertial controller based on voltage variations and their rate of change is proposed and added to the ESS and WTG primary control loops to provide transient voltage support in the event of FDI attacks. With reference to Fig. 3.2, the inner current regulation control loop of the ESS voltage-controlled VSI is modified to include a virtual inertia contribution. As the voltage deviation becomes steeper, an amount of current representing the virtual inertia contribution is added to the d-frame current reference to provide voltage support.

Fig. 3.3 shows the supplementary control loop associated with virtual inertia added to the WTG MPPT controller. The WTG SM rotor speed specifies based on the MPPT curve, the active power that should be generated by the turbine. A virtual inertia active power contribution proportional to the voltage excursions and their rate of change is added to this term to set the WTG power reference. The ESS current contribution and the WTG power contribution are limited by the ESS maximum inverter current and the WTG dynamics. Therefore, in the event of large active power disturbances causing the isochronous generator and WTG to saturate, virtual inertia would not be sufficient to provide complete compensation and voltage regulation. Deployment of load management strategies as discussed in section 3.3.2.2 will then be necessary.

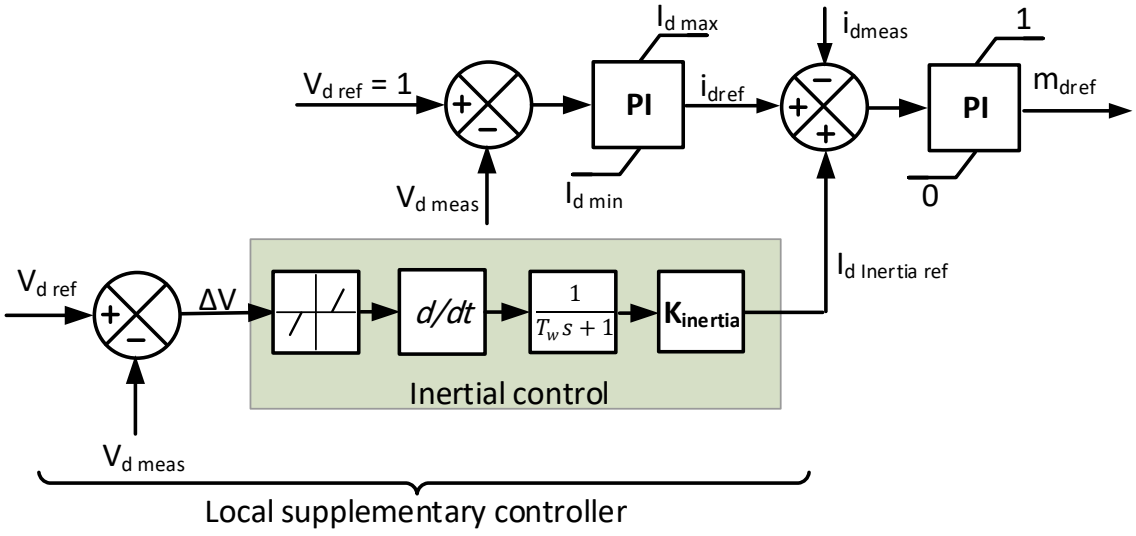

Fig. 3. 2: Supplementary control loop for the voltage-controlled VSI

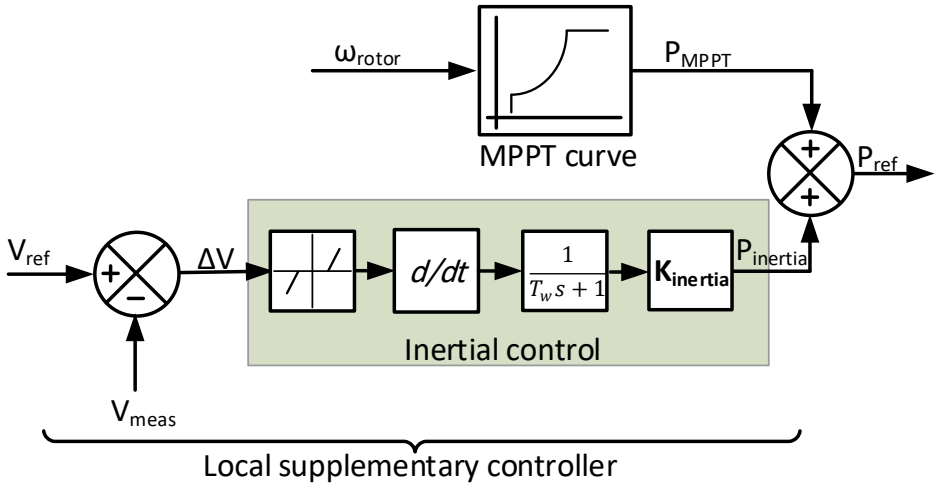

Fig. 3. 3: Supplementary control loop for the current-controlled VSI

3.2.2.2. Adaptive Load Management

Load management strategies that shed non-critical loads to compensate for under-voltage events have been proposed in the literature. In [144] the amount of load to be shed is evaluated as a function of the energy deficit and the energy demanded by controllable loads. Another load shedding scheme consists of analytically estimating the voltage amplitude, its slope and the inverter d-frame current in order to evaluate the amount of load to be curtailed [145]. This chapter proposes a centralized adaptive load management scheme to compensate for active power imbalances resulting from cyber-attacks, in the event where the isochronous generator and the supplementary control loops added to its local controller saturate and are no longer capable of compensating for the imbalance. Given that the active power changes cause voltage deviations in the case of an inverter-interfaced microgrid in analogy to frequency deviations in the case of a microgrid with rotating machines, the traditional load management strategy employed (table 3.1) is based on the under frequency load shedding (UFLS) scheme proposed in the North American Electric Reliability Corporation (NERC) standard [146]. While the traditional scheme solely depends on the severity of the excursions, the adaptive load shedding scheme developed is activated only if two conditions are concurrently satisfied: 1) the voltage at the PCC reaches a voltage threshold i.e. 0.9916 p.u. and 2) the current reference of the isochronous ESS's inverter reaches its maximum rated value. The voltage threshold has been evaluated in accordance with the frequency threshold proposed in the NERC standard for UFLS in SM based microgrids. In fact, in SM based microgrids, the first block of loads is shed as the frequency nadir is equal to 59.5 Hz

equivalent to 0.833 %. Therefore, in analogy to the traditional UFLS scheme, the first voltage threshold for UVLS in 100% inverter-interfaced microgrids was set to 0.9916 p.u. These two conditions ensure that the voltage excursion arising is due to the inability of the DERs to generate more power and provide balance. In such an event, the amount of load to be shed is calculated as the product of the voltage deviation and the currents generated by the DERs. It is important to mention that adaptive load management schemes will require the deployment of adaptive relays, additional transformers and circuit breakers than possibly needed in the case of traditional UVLS.

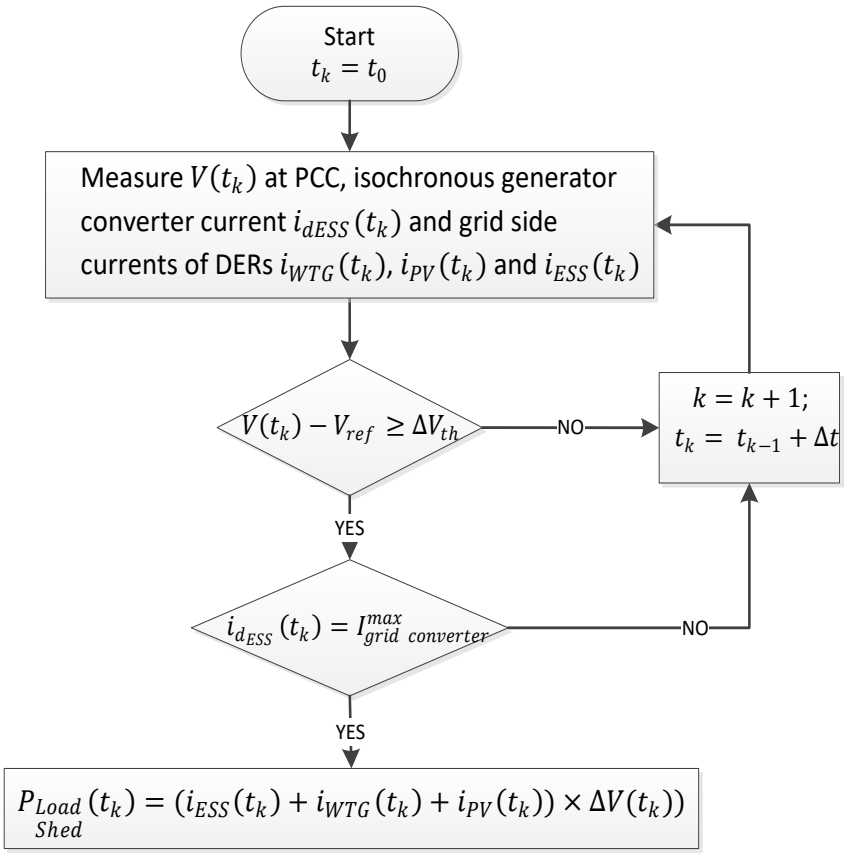

Fig. 3. 4: Under voltage load shedding algorithm

Table 3. 1: Traditional load management

Voltage Threshold (p.u.)	Total time (s)	Load shed at stage (%)	Cumulative load shed (%)
0.9750	10.0	3	31
0.9816	0.30	7	28
0.9850	0.30	7	21
0.9883	0.30	7	14
0.9916	0.30	7	7

In reference to Fig. 3.4, V represents the measured voltage at the PCC, V_{ref} the reference voltage set to 1 p.u., ΔV_{th} the minimum permissible voltage deviation selected to be 0.0084 p.u. i_{ESS}, i_{PV} and i_{WTG} represent the grid-side currents of the ESS, PV and WTG, respectively. i_{dESS} is the ESS inverter current and $I_{grid\ converter}^{max}$ is its maximum allowable value, t_k is the time at the kth simulation and Δt is the simulation sample time.

3.3. Microgrid System Overview

A 25 kV distribution system adapted from a utility feeder and reconfigured as a microgrid is used as the test network. The microgrid is composed of a type-4 full converter WTG, a PV system, a diesel generator, an ESS fed from a lithium-ion battery and controllable loads. Two islanded microgrid configurations are considered in this chapter: SM based and 100% inverter-interfaced microgrids. The connected DERs, their primary control mode and their corresponding ratings for both configurations are shown in tables 3.2 and 3.3. Coordinating with the local primary control loops of each DER, the microgrid controller dispatches the power set-points to maintain power balance and controls the statuses of the circuit breakers on a multi-minute or event basis. Traditional UFLS and under voltage load shedding (UVLS) schemes which shed blocks of loads based on the frequency and voltage deviation are implemented. The microgrid systems are modeled on the real-time HIL co-simulation setup detailed in chapter 2 and in the appendices. The setup is used to implement the FDI cyber-attacks as described in section 2.3.1, to quantify their impact and to evaluate the effectiveness of the control strategies proposed by evaluating the previously defined performance indices.

3.4. Real-Time HIL Co-Simulation Results

3.4.1. FDI Cyber-Attack on SM Based Microgrids

3.4.1.1. Test Cases

The FDI cyber-attack considered in this section targets the dispatch set-point sent from the EMS to operate the ESS. The base case represents the microgrid operation in the event of an FDI cyber-attack when no supplementary control loops are added to the ESS VSI. This test case is

developed to evaluate the impact of the FDI cyber-attack on the microgrid operation. Three other case studies are developed; in case 1 droop control is only added to the ESS VSI, case 2 employs supplementary virtual inertial response control loops and case 3 is a combination of cases 1 and 2 whereby the proposed combined droop and virtual inertia control is deployed. The base case will be compared to the three case studies to test the performance of the droop control, the virtual inertial response and the proposed combined control in mitigating the impact of FDI cyber-attacks. Traditional UFLS schemes that shed loads in the event of disturbances are employed for all the test cases to restore the frequency back to its operating point and ensure balance in the islanded microgrid. The post-attack performance indices previously defined in chapter 2 are evaluated in table 3.4 for every test case under two scenarios; one where there is sufficient power that could be provided by the isochronous resource to supply the load at the time of the FDI cyber-attack (S1) and the second where even if the grid-forming DER operates at its maximum at the time of the attack, power balance cannot be restored (S2).

Table 3. 2: SM based microgrid DERs ratings

Connected DERs	DER Ratings	Power Management Strategies
WTG	150 kW	Pmode: MPPT Qmode: Fixed power factor
Diesel Generator	320 kW	Pmode: Frequency control Qmode: Voltage Control
ESS	100kW/100 kWh	Pmode: Fixed active power Qmode: Fixed reactive power

Table 3. 3: 100% inverter-interfaced microgrid DERs ratings

Connected DERs	DER Ratings	Power Management Strategies
WTG	150 kW	Pmode: MPPT Qmode: Fixed power factor
PV	50kW	Pmode: MPPT Qmode: Fixed power factor
ESS	125kW/125 kWh	Pmode: Frequency control Qmode: Voltage Control

3.4.1.2. Impact Assessment

The investigated FDI cyber-attack maliciously manipulates the dispatch set-point of the ESS operated in fixed PQ mode when the diesel generator is the isochronous resource, responsible for

the inter-dispatch voltage and frequency regulation of the SM based islanded microgrid. The FDI cyber-attack is applied and its impact is evaluated on the real-time HIL co-simulation platform developed as detailed in chapter 2 and the appendices. For the first scenario, a -80kW bias value is applied at $t_A = 10$ sec, whereas for the second, $B(10) = -100$ kW.

Scenario 1- Available active power

Figs. 3.5 shows the active power generated by the DERs when a FDI attack compromising the microgrid controller HMI maliciously modifies the ESS dispatch set-point while the power available in the grid is sufficient to compensate for the cyber induced imbalance. Large frequency excursions streaming from the FDI attack result at the microgrid load side and are plotted in Fig. 3.6 for the different test cases. For the base case, in the absence of supplementary control loops, a frequency nadir of 59.32 Hz results from the FDI cyber-attack. These excursions initiate the UFLS schemes causing 22.4 kW of unserved load as illustrated in Fig. 3.7. It is important to mention that although the bias selected in that case is not confined to the bounds set in (2.22), (2.23), (2.27) and (2.28) therefore does not violate the EMS power and energy management requirements, the frequency excursions initiating the protection schemes at the time of the application of the attack are due to the inability of the isochronous diesel generator to provide fast compensation owing to its slow dynamic response.

Scenario 2- Shortage of active power

Figs. 3.8 illustrates the active power generated by the DERs when a similar FDI attack targets the ESS dispatch set-point. In this scenario, the value of the FDI cyber-attack bias is selected so as to violate the power management requirements as defined in equation (2.23) of chapter 2. As the isochronous DER does not have enough capacity to compensate for the cyber-induced imbalance, an amount of load would have to be shed to restore the system's balance. The system's frequency response is plotted in Fig. 3.9 causing a frequency nadir as low as 58.89 Hz as the attack is performed and no mitigation strategies are applied. Fig. 3.10 shows that up to 21% of the load was curtailed in order to counteract the impact of the attack and restore the frequency back to its nominal value.

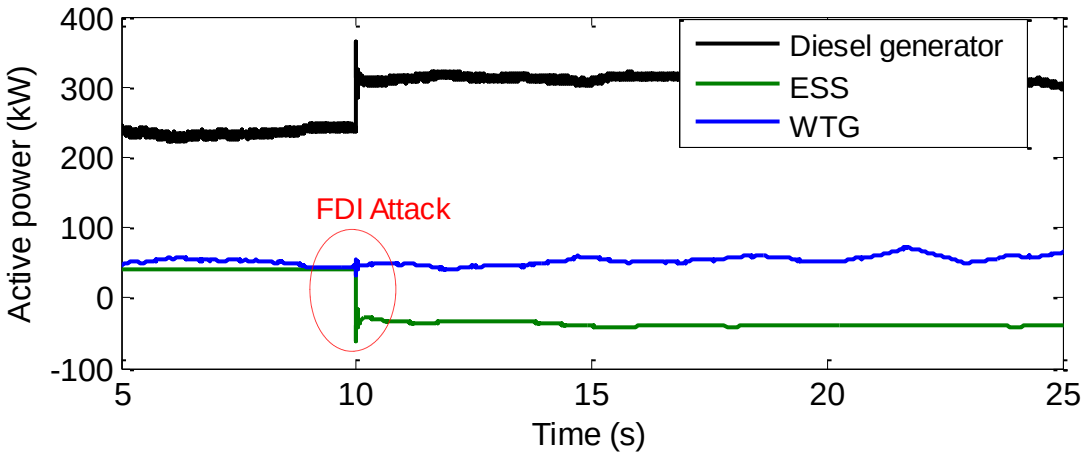

Fig. 3. 5: S1- DER power injections subject to an FDI attack on ESS set-point

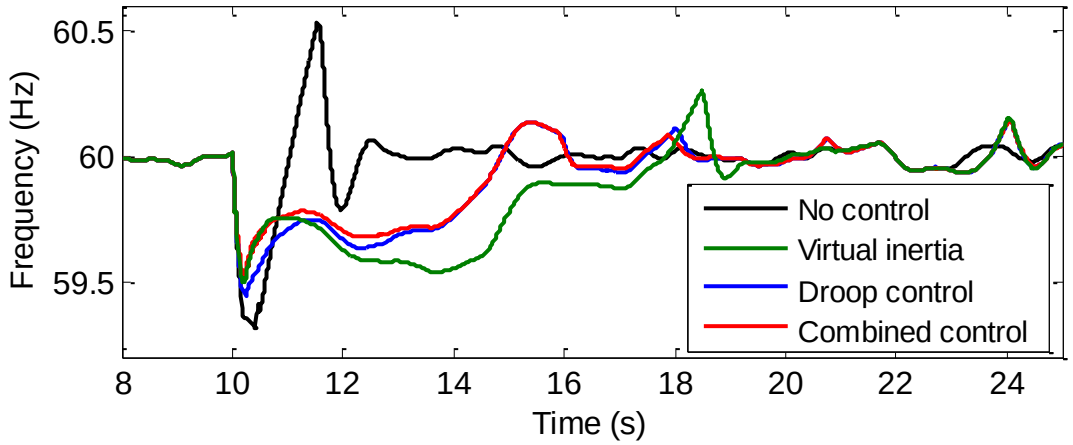

Fig. 3. 6: S1 - Frequency response subject to an FDI attack on ESS set-point

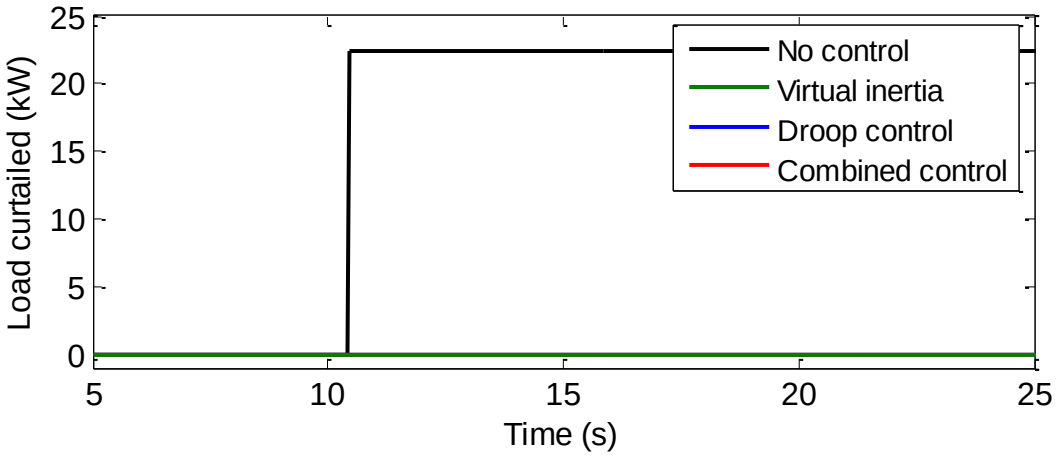

Fig. 3. 7: S1 - Load shed due to UFLS – FDI attack on ESS set-point

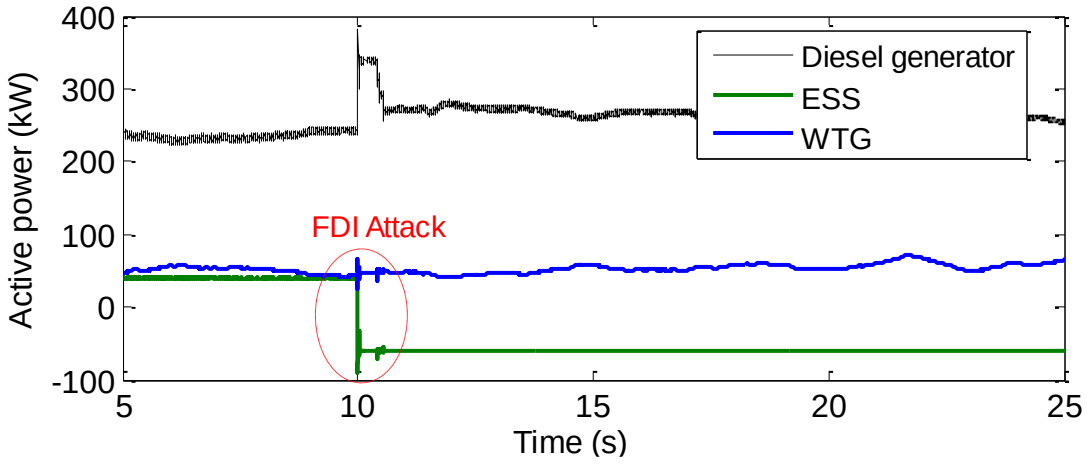

Fig. 3. 8: S2 - DER power injections subject to an FDI attack on ESS set-point

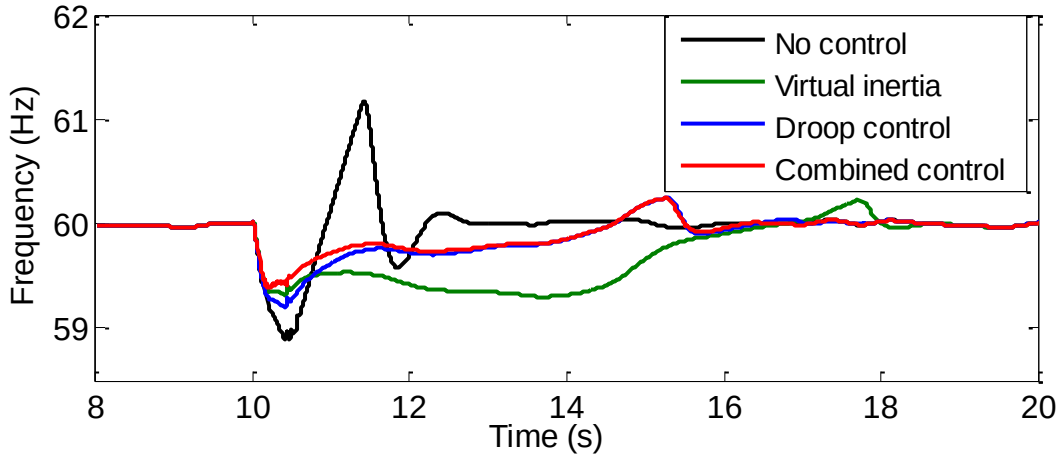

Fig. 3. 9: S2 - Frequency response subject to an FDI attack on ESS set-point

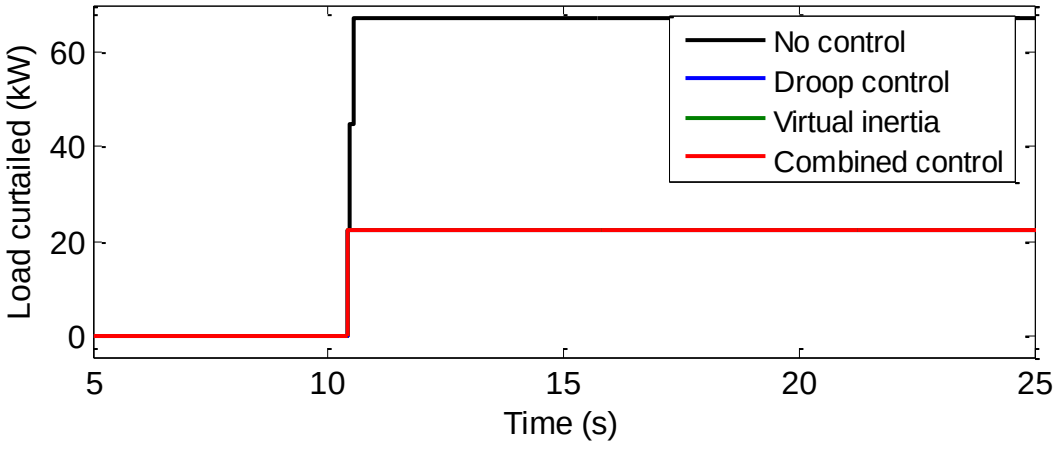

Fig. 3. 10: S2 - Load shed due to UFLS – FDI attack on ESS set-point

3.4.1.3. Mitigation Strategy Performance Evaluation

The performances of the supplementary control loops for droop, virtual inertia and combined droop and virtual inertia are tested and compared to the base case for the two scenarios.

Combined Control Parameters Selection

The virtual inertia and droop gains used for the combined controller presented in this chapter are selected such that:

1) The virtual inertia compensates for the transient event caused by the cyber-attack. Therefore, it increases the frequency nadir and provides more time to the grid-forming DER local controller to restore the balance hence minimizing the amount of load curtailed.
2) The droop control provides permanent compensation and reduces the time needed to restore the frequency back to its nominal operating value.

In order to select the values for the gains, the FDI cyber-attack which causes the worst-case imbalance is launched. As such, the selected combined controller's parameters will also provide compensation for attacks which are less severe.

Fig. 3.11 shows the frequency response for values of inertia gains ranging from 0 to 40 while the droop gain is set to 0. Figs. 3.12 and 3.13 show that as the inertia gain increases to values beyond 30, there is only a slight improvement in the frequency nadir and in the time needed to restore the frequency back to 60 Hz. In addition, an inertia gain equal to 35 or higher causes the ESS output to oscillate creating instabilities. It could also be seen from Fig. 3.14 that values lower than 20 cause large amounts of load energy to be curtailed. In order to increase the frequency nadir and to postpone the activation of the protection schemes, giving more time to the grid-forming DER to ramp up and reduce/eliminate the power imbalance, an inertia gain equal to 30 is selected for the simulations.

Fig. 3.15 plots the microgrid frequency response for different values of the droop gain ranging from 0 to 40 while the inertia gain is set to 0. It could be seen that high values of the droop gain would result in steady-state frequency errors. While values above 15 would only activate one stage of load curtailment, they will significantly increase the time needed to restore the frequency back to 60 Hz (Fig. 3.16). In order to minimize the time needed to restore the frequency back to its nominal operating point, a droop gain equal to 14 will be used in the simulations. The combination

of virtual inertia and droop control would therefore result in a high frequency nadir, a shorter time to restore the frequency back to 60 Hz and a limited amount of load energy curtailed.

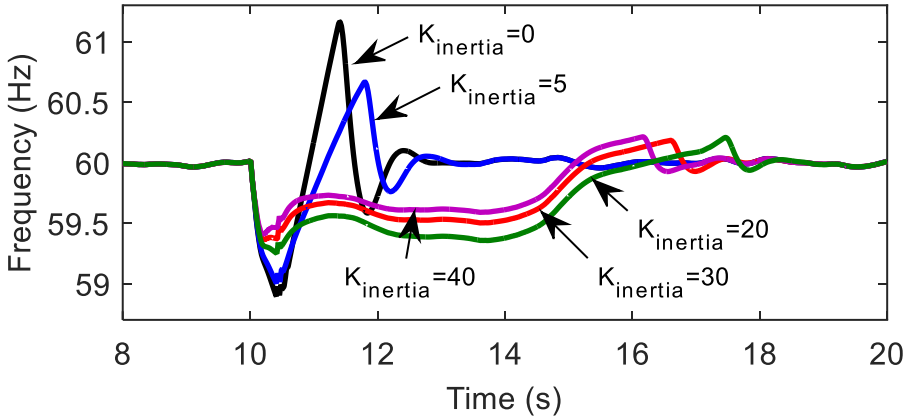

Fig. 3. 11: Microgrid frequency response for different values of inertia gain

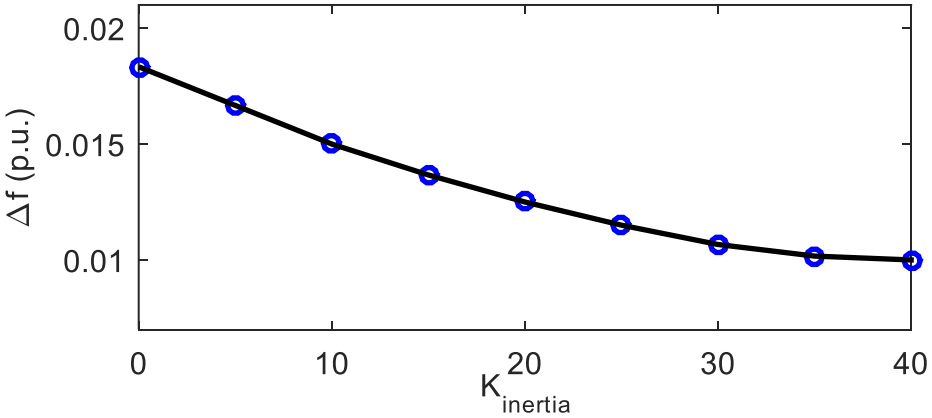

Fig. 3. 12: Frequency deviation from nominal value

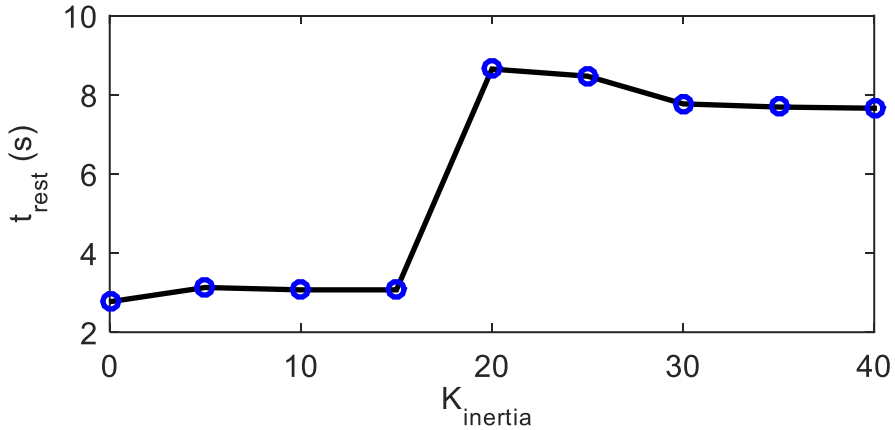

Fig. 3. 13: Time needed to restore the frequency back to nominal value

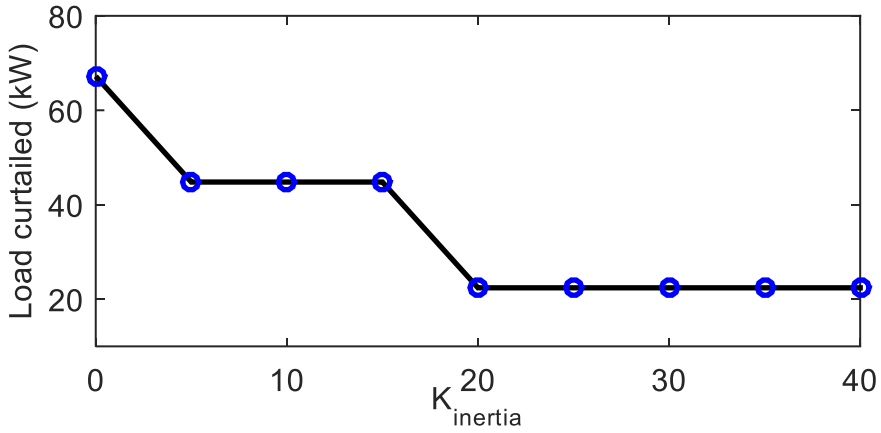

Fig. 3. 14: Load energy curtailed

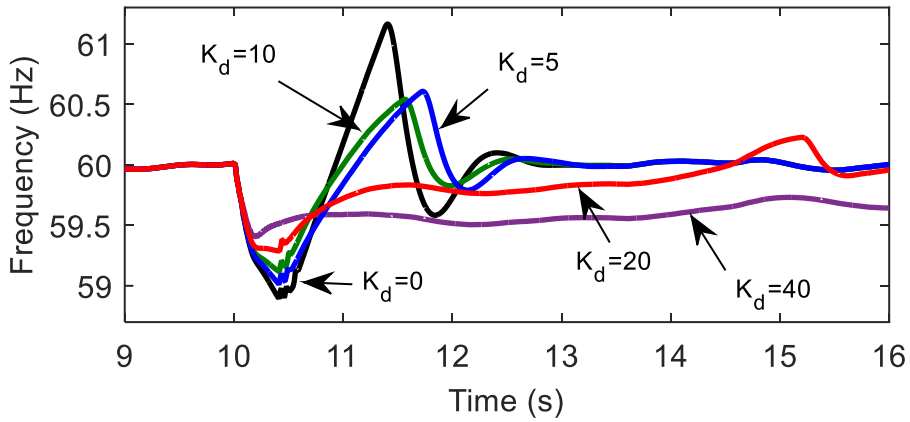

Fig. 3. 15: Microgrid frequency response for different values of droop gain

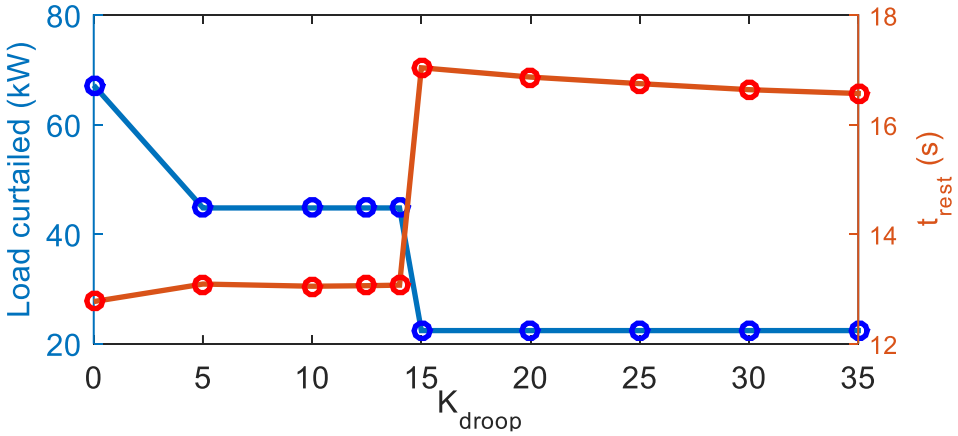

Fig. 3. 16: Load energy curtailed and time needed to restore frequency back to nominal value

Scenario 1- Available active power

As compared to the base case, the application of the droop control alone results in a 0.11 Hz reduction in the frequency excursion, whereas virtual inertia enhances the frequency response even more with a 0.18 HZ reduction in the excursion (Fig. 3.6). Although virtual inertial response provides a better performance than the droop control in terms of frequency nadir, it

requires more time to restore the frequency back to 60 Hz. The combined controller benefits from the advantages of both control schemes as it results in a higher frequency nadir and the same frequency restoration time as the droop control strategy. The controllers' post-attack active power compensations are plotted in Fig. 3.17. The droop controller responds and provides compensation in proportion to frequency excursions resulting in a slow but permanent frequency enhancement. As for the virtual inertial response, it only operates and provides compensation when the rate of change of the frequency excursion is significantly high, explaining the fast transient cyber-attack compensation. The three cases tested enhance the system's frequency response by making use of the available active power to supply the loads so that load curtailment is no longer required and the microgrid ability to provide continuous power supply is maximized.

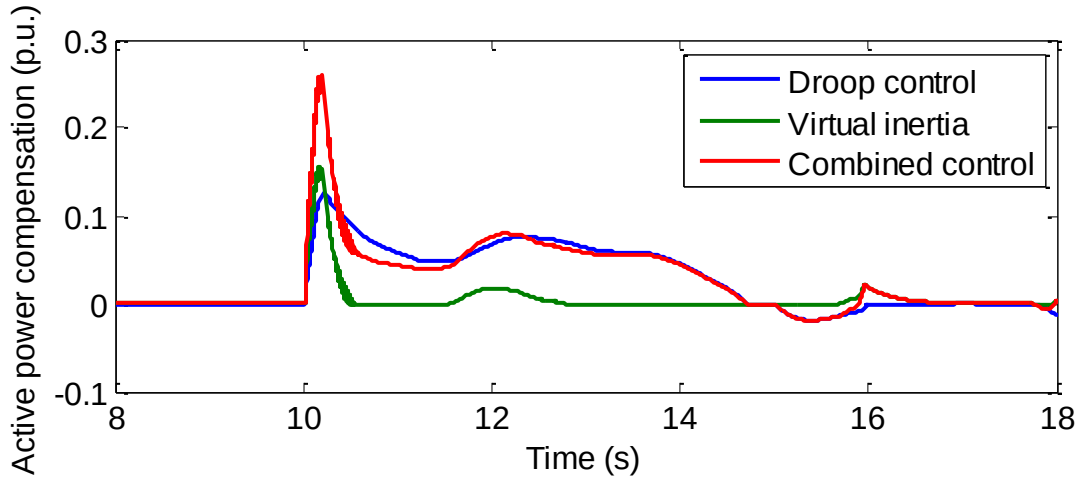

Fig. 3. 17: S1 - ESS power compensation from supplementary controllers –FDI attack on ESS set-point

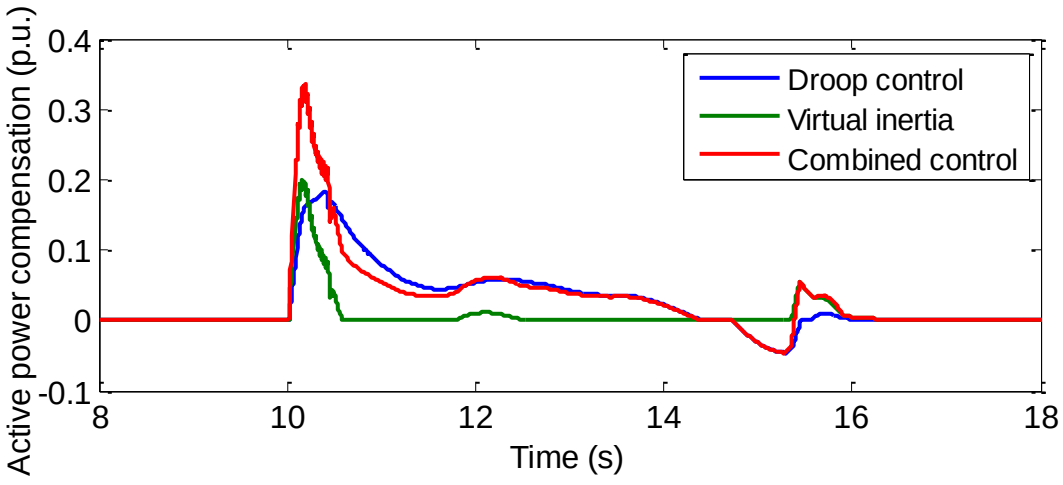

Fig. 3. 18: S2 - ESS power compensation from supplementary controllers - FDI attack on ESS set-point

Table 3. 4: Performance indices SM based microgrid

		Frequency Nadir (Hz)	Load Unserved (kW)	Frequency restoration(s)
Base Case	S1	59.32	22.4	3
	S2	58.89	67.2	2.86
Droop control	S1	59.43	0	8.31
	S2	59.2	22.4	6.26
Inertial Response	S1	59.5	0	10.09
	S2	59.32	22.4	8.56
Combined Control	S1	59.51	0	8.31
	S2	59.4	22.4	6.26

Scenario 2- Shortage of active power

Figs. 3.8-3.10 plot the frequency response, load shed and power compensation due to an FDI attack that causes a shortage of active power in the grid. In addition to the diesel generator slow dynamic response, the grid-forming DER, in that case, does not have enough capacity to provide compensation for the cyber-attack. As compared to the case where no control is applied, virtual inertial response and droop control significantly enhance the frequency nadir. The application of virtual inertia results in a better frequency nadir than that obtained when droop control is employed but takes longer to restore the frequency back to its nominal value. When combined, virtual inertia and droop control result in a frequency nadir higher than that obtained when operated alone and a time of restoration equal to that resulting from the application of droop. As compared to the base case, whether combined or not, virtual inertial response and droop control significantly reduce the amount of load curtailed. In fact, only the first stage of load shedding is initiated, as compared to 3 stages for the base case.

Controllers' Performance Comparison

The performance of the combined droop and inertia controller implemented in this chapter is compared to that of other control strategies proposed in the literature and reviewed in section 1.3.5.2. The latter strategies consist of adding supplementary control loops to the power-electronic interfaced DERs to provide virtual inertial response and or droop compensation in the event of physical disturbances such as generation outages [23], sudden load increase [116], and sudden

variations in the solar irradiance [113]. In order to have the same basis for the comparison, the biases of the FDI cyber-attacks launched are selected such that they result in the same amount of frequency excursions induced by the different physical disturbances. As such, the performance of the different control loops in enhancing the frequency response could be evaluated. Amongst the data provided in the different studies, the frequency nadir is an important measure calculated in the three studies conducted in [23], [113] and [116] to quantify the impact of the disturbances and evaluate the performance of the proposed control strategies in mitigating them. Therefore, the frequency nadir is used here to evaluate the frequency excursions from the respective nominal frequencies. Per unit values are used as the nominal frequencies vary depending on the system studied. The frequency excursion Δf (p.u.) is evaluated as follows:

$$\Delta f = \frac{f_{nom} - f_{nadir}}{f_{nom}} \quad (3.\ 4)$$

Whereby, f_{nom} is the nominal frequency (50 or 60 Hz depending on the system studied) and f_{nadir} is the frequency nadir (Hz).

Table 3.5 shows the frequency excursions resulting from the physical disturbances studied in [116], [23] and [113] and the FDI cyber-attacks launched in this study to engender a similar impact creating a basis for comparison. The excursions are evaluated for the scenarios where: 1) no control is applied, and 2) the control strategy proposed in the study is applied. The percentage of reduction in the frequency excursion is calculated to facilitate the comparison of the control strategy implemented in this study to the other methods. It could be noted from the table that the different control strategies provide more contribution as the cyber or fault induced disturbance is more severe. In fact, the disturbances in [116] and [23] cause power imbalances which do not exceed 17% as compared to the 40.4% imbalance caused by the sudden variation in the solar irradiance in [113]. This further explains the higher percentage in frequency excursion reduction after the application of the control strategies obtained in case 3 as compared to cases 1 and 2.

As mentioned in section 3.2.1.1, the control loops associated with the combined virtual inertia and droop controller implemented in this study are similar to the ones presented in [116] and [23], however, the tuning of their parameters is done differently. In fact, in this study, the droop and inertia gains are tuned such that for the worst-case attack scenario the combined controller increases the frequency nadir, reduces the frequency restoration time and the amount of load curtailed without inducing unwanted oscillations. As such, the controller would provide the

maximum possible compensation in the event of both, the worst-case cyber-attack and the less severe ones. In fact, it can be seen from the results obtained that for the different attack severity levels, the combined controller implemented in this study reduced the frequency excursions more than the other strategies. The strategies proposed in the other studies compensate for disturbances and enhance the frequency; however, the virtual inertia and droop constants tuning is done for some disturbances and do not have as objective to generate the maximum possible compensation to restore the frequency. As a result, the combined controller implemented in this chapter results in a higher percentage of frequency excursion reduction, as compared to the other strategies. The study performed in [23] evaluates the time needed by the virtual inertia, droop and the combined controller to restore the frequency back to a steady-state value after the disturbance. In fact, this study confirms the results that were obtained in this chapter, as it showed that virtual inertia provides more transient compensation than droop control to increase the frequency nadir but requires more time to restore the frequency to a steady-state value. It was also shown that a combination of both schemes would provide transient and permanent frequency regulation by reducing the nadir and the restoration time.

3.4.2. FDI Cyber-Attack on Inverter Interfaced Microgrids

3.4.2.1. Test Cases

The FDI cyber-attack considered in this section maliciously modifies the command sent to the DER circuit breaker and is formulated as in (2.7). The base case represents the microgrid operation in the event of an FDI cyber-attack when no supplementary control loops are added to the ESS and the WTG VSI and protection schemes are deactivated. Three other case studies are developed; in case 1 virtual inertial response is added to the ESS and WTG VSIs, in case 2 traditional UVLS schemes are employed in addition to the supplementary virtual inertial response control loops and in case 3 virtual inertial response along with the adaptive load management scheme proposed in section 3.2.2.2 are implemented. The base case is compared to the three case studies to test the performance of the proposed supplementary local control loops and the adaptive load management strategy in mitigating the impact of FDI cyber-attacks. The post-attack performance indices previously defined are evaluated in table 3.6 for every test case under two

Table 3. 5: Controllers performance comparison

		Δf **without control (p.u.)**	Δf **with control (p.u.)**	**Percentage** Δf **reduction (%)**
C1	**Sudden load increase [116]**	0.0145	0.00916	0.534
	FDI attack $\boldsymbol{B(t) = 75.8\ kW}$	0.0145	0.0085	0.6
C2	**Generation outage [23]**	0.028	0.016	1.2
	FDI attack $\boldsymbol{B(t) = 79.3\ kW}$	0.028	0.008833	1.9167
C3	**Sudden variation in solar radiation [113]**	0.1385	0.01416	12.43
	FDI attack $\boldsymbol{B(t) = 89\ kW}$	0.1385	0.01	12.85

scenarios; one where the amount of load to be supplied is low so as to have sufficient available power at the time of the FDI cyber-attack (S1) and the second operating at a high loading level causing a shortage of power at the time of the cyber-attack (S2).

3.4.2.2. Impact Assessment and Performance Indices

The cyber-attack considered in this section consists of tampering with the PV system's circuit breaker status causing its sudden unplanned disconnection at 20 seconds. The impact of this FDI cyber-attack is evaluated hereafter for the two scenarios previously defined. The total load that needs to be served is set to 150 kW in S1 and 240 kW in S2.

Scenario 1- Available active power

In this scenario, the low amount of load to be served ensures that additional active power is available from the isochronous DER to compensate for the power imbalance caused by the disconnection of the PV streaming from the FDI cyber-attack. The active power generated by the various DERs and load in the absence of control are shown in Fig. 3.19. The PV disconnection results in a 38.95 kW active power reduction at 20 s. In the pre-attack period, the isochronous ESS is operating at around 0 kW and is therefore capable of compensating for the imbalance resulting from the cyber-attack. The system voltage measured in the event of the cyber-attack is shown in Fig. 3.20 when no control is applied, when virtual inertial control is added and when the load management schemes are employed. In the absence of control, the voltage nadir reaches a value of 0.9139 p.u. and the excursion is cleared after 1.49 seconds of the cyber event. It is clear in this

scenario that the local DERs control loops are capable of ensuring post-attack active power balance; however, they cannot eliminate the large transient voltage excursions. Hence, the need of supplementary control loops to enhance the voltage profile in the event of such cyber disturbances.

Scenario 2: Shortage of active power

In this scenario, the high loading level results in a shortage of active power after malicious disconnection of the PV. Fig. 3.23 shows that prior to the application of the attack and as the PV was connected, the load was supplied and the ESS had available active power headroom. However, as the PV breaker is triggered by the cyber-attack causing the loss of 38.95 kW, the WTG and the ESS local controllers cannot compensate for the imbalance due to their limited capacity. The microgrid voltage for the four control cases is shown in Fig. 3.24. When no control is applied, the voltage nadir after the application of the FDI attack reaches 0.9136 p.u. As the isochronous DER operates at its maximum capacity in the post-attack period, the voltage was not brought back to its reference value and more severe deviations resulted.

3.4.2.3. Mitigation Strategy Performance Evaluation

Scenario 1- Available active power

As compared to the base case, adding supplementary control loops associated with virtual inertial response to the ESS and the WTG local controllers results in an increase in the voltage nadir to a value of 0.9756 p.u. and a similar voltage restoration time (Fig. 3.20). The ESS and WTG contributions from virtual inertial response are illustrated in Fig. 3.21. Fig. 3.22 shows the amount of load shed resulting from the application of the traditional and adaptive load shedding schemes. Given that the activation of the traditional schemes depends solely on the voltage magnitude, large amounts of load are curtailed regardless of the system's DERs states. In this scenario, the traditional UVLS scheme initiated right after the application of the FDI cyber-attack and curtailed 31.5 kW of loads justifying the short voltage restoration time as compared to the other cases. The voltage nadir resulting from the application of the traditional UVLS scheme is similar to that obtained when virtual inertia is applied alone or with the adaptive UVLS scheme. The adaptive load management schemes initiate only if, in addition to the detection of a voltage excursion, the maximum capacity of the isochronous DER is reached. In this scenario, the primary

DERs' control loops supplemented by virtual inertial response were sufficient in ensuring transient voltage regulation in response to the cyber-attack without requiring activation of the adaptive load shedding scheme and unnecessary loss of load.

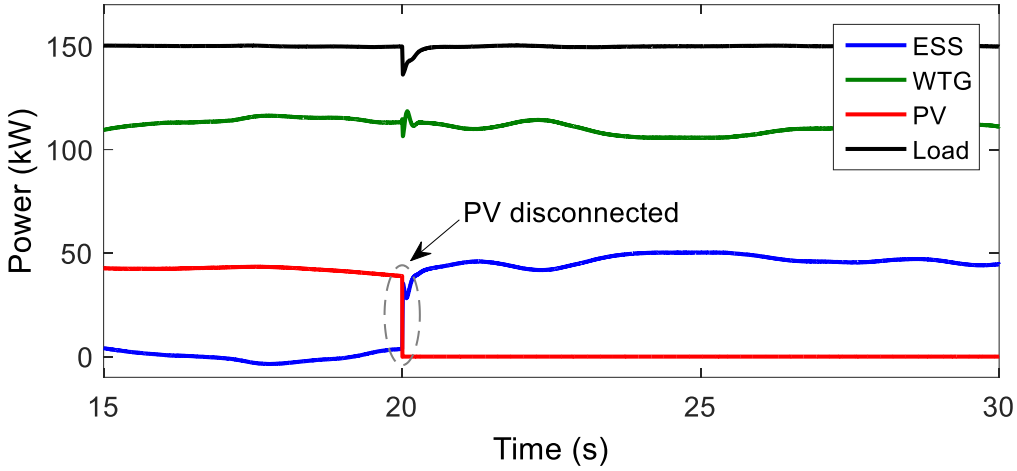

Fig. 3. 19: S1 - DER power without supplementary control & UVLS – FDI on DER circuit breaker command

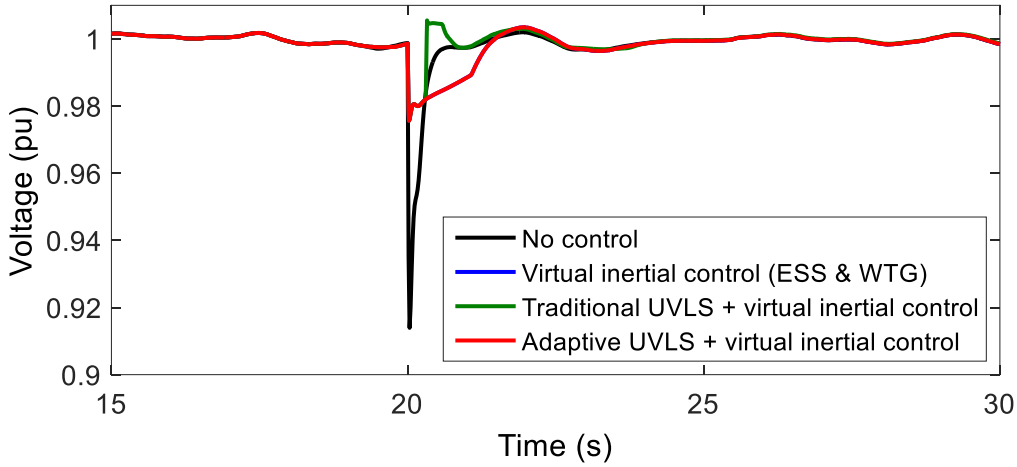

Fig. 3. 20: S1 - System voltage with supplementary control & UVLS – FDI on DER circuit breaker command

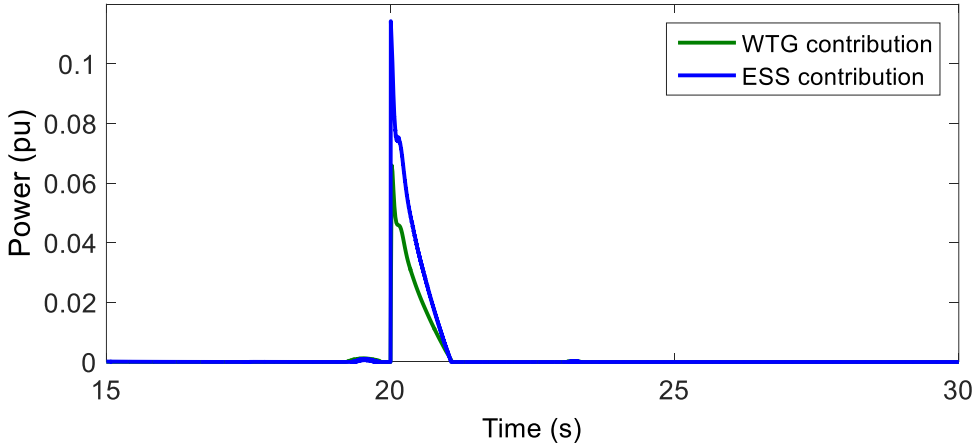

Fig. 3. 21: S1 - DER supplementary VIR control power contribution – FDI on DER circuit breaker command

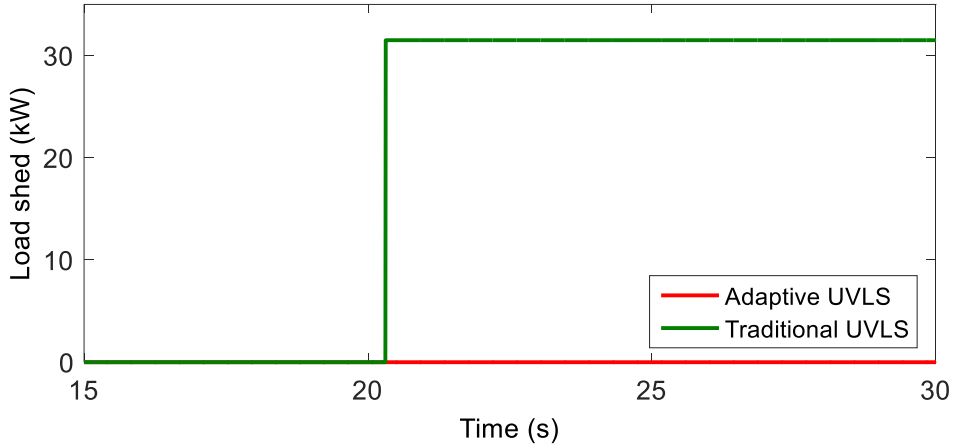

Fig. 3. 22: S1 - Non-critical load shed – FDI on DER circuit breaker command

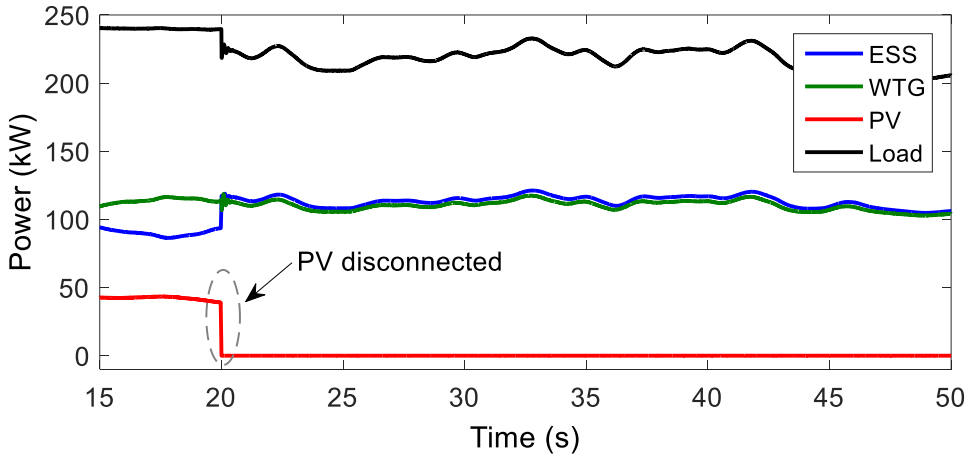

Fig. 3. 23: S2 - DER power without supplementary control & UVLS – FDI on DER circuit breaker command

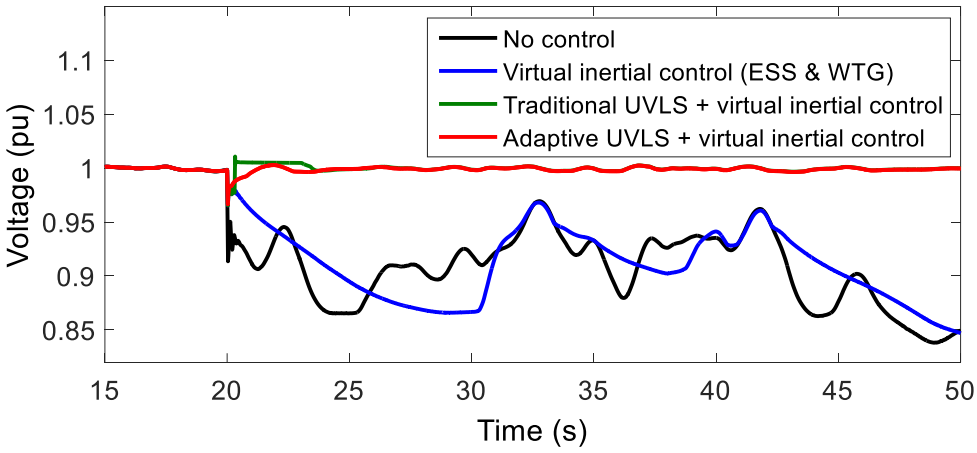

Fig. 3. 24: S2 - System voltage with supplementary control & UVLS – FDI on DER circuit breaker command

Scenario 2: Shortage of active power

As shown in Fig. 3.23, the PV disconnection streaming from the FDI cyber-attack in this scenario causes the isochronous ESS not to have enough headroom to provide attack compensation and restore the power balance and the voltage. The contribution from virtual inertial response plotted in Fig. 3.25 is limited by the ESS's maximum capacity justifying the degradation of the voltage profile even with the supplementary control loops added to the ESS VSI. In such a situation, the deployment of load management schemes is essential to restore the active power balance and the voltage stability. The traditional and adaptive schemes were employed and tested. As shown in Fig. 3.24, and as compared to the traditional scheme, the proposed adaptive UVLS scheme supplemented with virtual inertial response results in a higher voltage nadir and a shorter time to restore the voltage profile. In addition, the traditional strategy causes an activation of the fourth stage of load shedding and curtails 67.2 kW as compared to only 17.13 kW of unserved load as the proposed strategy is applied (Fig. 3.26). In fact, the adaptive load management strategy sheds an amount of load that is equal to the cyber-induced power imbalance minus the post-attack contributions of the supplementary virtual inertia control loops.

Table 3. 6: Performance indices 100% inverter-interfaced microgrids

		Voltage Nadir (p.u.)	**Load Unserved (kW)**	**Voltage restoration (s)**
Base Case	S1	0.9139	-	1.49
	S2	0.9136	-	--
Inertial Response	S1	0.9756	-	1.49
	S2	0.9654	-	--
Inertial Response + Traditional UVLS	S1	0.9756	31.3	1.3
	S2	0.9654	67.2	5.89
Inertial Response + Adaptive UVLS	S1	0.9756	0	1.49
	S2	0.9666	17.13	5.59

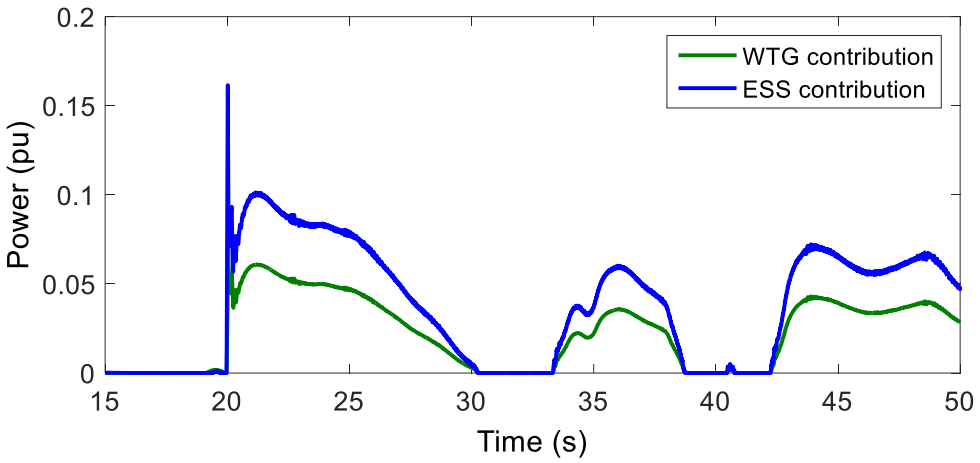

Fig. 3. 25: S2 - DER supplementary VIR control power contribution – FDI on DER circuit breaker command

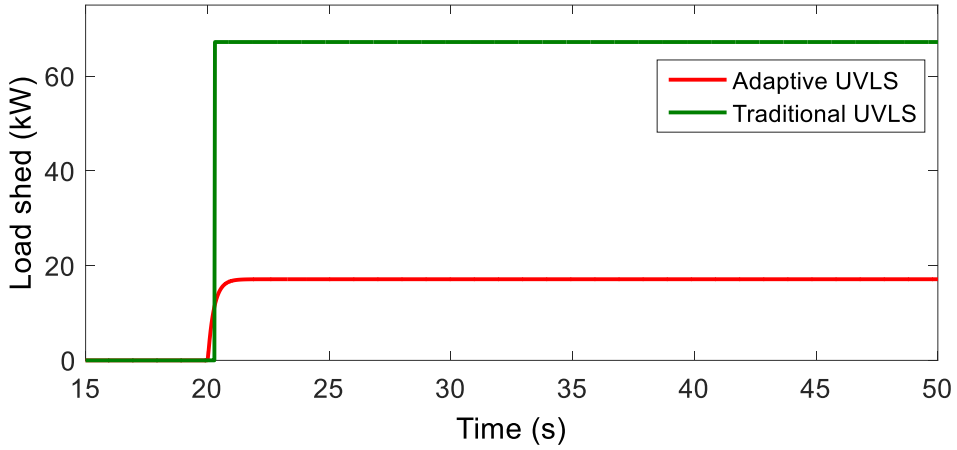

Fig. 3. 26: S2 - Non-critical load shed – FDI on DER circuit breaker command

3.5. Conclusion

Microgrids are increasingly employing static power-electronic interfaced DERs such as PV systems, WTGs and ESSs resulting in no or very low inertia. Therefore, slight disturbances will cause large voltage or frequency excursions, especially in the absence of the EPS operating as the slack bus. In addition, a centralized controller requiring a communication network to provide a mechanism for the exchange of information with the DERs local controllers is essential to ensure stable and autonomous operation of islanded microgrids. This reliance on communication technologies creates access points and cyber vulnerabilities that may be maliciously exploited. FDI cyber-attacks constitute a major threat to the resiliency of islanded microgrids and can, if undetected, cause large active power imbalances and result in DER maloperation and even a grid

blackout. In this chapter, FDI cyber-attacks which compromise the key control functions provided by the centralized microgrid controller by gaining unauthorized access to its HMI, bypassing detection schemes such as physical watermarking, were investigated. FDI cyber-attacks which are successfully detected are further considered in chapter 5. Control loops associated with virtual inertial response and droop control were added to the power-electronic interfaced DERs to provide frequency and voltage support improving the microgrid survivability in the event of undetected FDI cyber-attacks. Adaptive load management schemes were proposed to provide post-attack power and energy balance. The impact of the attacks and the effectiveness of the control strategies were validated using a real-time HIL co-simulation testing platform modeling a 25 kV distribution system adapted from a utility feeder and reconfigured as a microgrid. SM based and 100% inverter-interfaced islanded microgrid configurations were considered; the performance indices and the mitigation solutions corresponding to every configuration were evaluated and tested.

The impact of FDI cyber-attacks compromising the EMS dispatch set-point sent to operate one of the DER was evaluated for an SM based microgrid. Control loops combining droop and virtual inertial response were added to the ESS local control to counteract the cyber-attack. The simulation results showed that virtual inertial control achieved fast transient compensation in the event of an attack-induced active power disturbance; whereas, droop control provided a slower permanent compensation of FDI attacks. Performance indices, including frequency nadir, time to reach stability and amount of load loss were evaluated. The proposed solution proved to enhance the transient and steady-state frequency stability by limiting unnecessary load shedding and reducing the amount of frequency excursion in an acceptable time.

Another FDI cyber-attack targeting the status control commands sent by the centralized microgrid controller to enable/disable the DERs circuit breakers was also analyzed in this chapter. The impact of the attack on the operation of a 100% inverter-interfaced islanded microgrid was assessed. A two-layer cyber-resilient control consisting of local control loops for virtual inertia and an adaptive load management strategy was proposed to mitigate the impact of the cyber-attack. Virtual inertial response was added to the WTG and the ESS VSIs, based on voltage variations and their rate of change. The controllers provided transient voltage regulation by smoothing the ramps streaming from the cyber-attack. In addition, the adaptive load management strategy proposed to overcome the DERs rated capacity limits ensured rapid post-attack recovery, active power balance and voltage profile restoration. Performance indices including voltage nadir,

amount of load unserved and voltage restoration time were evaluated in order to quantify the attack's impact and test the performance of the proposed control strategies in enhancing the resiliency and survivability of the microgrid control infrastructure when subjected to undetected cyber disturbances. The following chapter investigates DDoS cyber-attacks causing complete loss of information exchange in the microgrid. The performance indices defined in chapter 2 are evaluated to quantify the impact of the cyber-attacks. A fallback control mitigation strategy which ensures coordination between the DERs to ensure voltage and frequency regulation, power and energy management in the event of the DDoS cyber-attacks is proposed and its performance is evaluated on the real-time HIL co-simulation platform for SM based and 100% inverter-interfaced microgrids.

Chapter 4

Fallback Energy Management Control Strategy for DDoS Cyber-Attack Mitigation

4.1. Introduction

In the previous chapter, FDI cyber-attacks have been investigated. This chapter will consider DDoS attacks targeting the islanded microgrid communication network and resulting in total loss of communication between the secondary microgrid controller EMS and the DERs primary control. The impact of the attack on the microgrid operation is investigated and a potential mitigation strategy is proposed.

In islanded microgrids featuring renewable DERs on a large scale, the ESS is typically operated as the grid-forming DER, setting the voltage and frequency of the grid, and increasing the hosting capacity of intermittent generation. One major drawback of operating the ESS as the isochronous generator is its power and energy ratings along with its state-of-charge (SOC) limitations. In addition, the ESS might be limited by the base power that it could provide as compared to larger synchronous generating units. However, the fast-acting power-electronic interfaced storage system has the capability of operating as a load or a generating unit, increasing the usability of renewable energy resources by coinciding their generations with the peak demand.

To operate continuously as the isochronous resource, the microgrid controller dispatches the controllable DERs and manages the loads, to control the ESS power and SOC while providing it the necessary reserve to regulate the voltage and the frequency. In this operating mode, the ESS is considered as the islanded microgrid most critical DER and a cyber-attack which results in the violation of its power and/or SOC constraints can severely impact its ability to regulate the microgrid voltage and frequency, and its capacity to compensate for the intermittent renewable generation. The mitigation solutions that could be applied at the microgrid control layer to provide power and energy management functionalities without relying on the centralized EMS have been reviewed in section 1.3.5.1. Distributed control strategies are either resilient to a limited number of compromised nodes [89] or assume that a master node is unattackable [90, 91]. Other fully-decentralized strategies either result in poor and oscillatory performance [96] or ensure decentralized power and energy management by curtailing inexpensive renewable energy and load [103, 104]. This chapter argues that a fallback control mitigation strategy operating the DERs based on enhanced primary control loops and ensuring coordination among the different resources by means of local measures, overcomes the drawback of the strategies available in the literature. The proposed strategy can in fact enhance the microgrid ability to continuously supply critical load and to host inexpensive renewable energy without affecting the system stability and without relying on a secure master. In addition, the fallback control enhances the microgrid resiliency if one [121] or all the nodes were compromised.

4.2. Microgrid Configuration and Cyber-Attack Model

4.2.1. Power and Energy Management Strategies

Two islanded microgrid configurations are considered in this chapter: SM based and 100% inverter-interfaced microgrids. Typically, in an islanded microgrid, one DER operates as the isochronous generator forming the microgrid voltage and frequency while the remaining DERs may or may not assist in providing voltage and frequency support [22, 23, 25]. In this chapter, the ESS is operated as the isochronous DER to compensate for the renewable DERs fluctuations. In SM based microgrids, active power mismatches are associated with frequency deviations and the

ESS power-electronic interface is operated as a current-controlled VSI. In contrast, in 100 % inverter-interfaced microgrids, the active power imbalances result in voltage excursions and the isochronous ESS power-electronic interface is operated as a voltage-controlled VSI. The primary control loops pertaining to the ESS power-electronic interface for SM based and 100% inverter-interfaced microgrids are shown in Figs. 2.3 and 2.4, respectively.

The renewable DERs power-electronic interface operates as a current-controlled VSI based on the MPPT curves, as explained in chapter 2. The corresponding control loops are shown in Figs. 2.8 and 2.9. Dispatchable or grid-supporting DERs are also employed and they operate based on fixed active and reactive power set-points as shown in Fig. 2.6. They may or may not provide voltage and frequency support by applying voltage and frequency droop respectively.

The EMS employed in this chapter updates the DERs primary control set-points on a 5 minutes basis. The EMS objective is to minimize the average cost of energy in the islanded microgrid subject to the various constraints defined in section 2.2.2.1 of this thesis.

4.2.2. DDoS Cyber-Attack Model

The microgrid communication network considered in this chapter interconnects the EMS and the IEDs associated with the different DERs to exchange measurements needed by the EMS to generate dispatch set-points for the dispatchable resources while respecting energy and power constraints. This chapter considers an attacker who has gained valid credentials to connect over the LAN connecting the EMS information exchange interface with the engine performing the EMS optimization. As a result, and based on the steps described in chapter 2, the attacker can launch a DDoS cyber-attack which compromises the communication network and results in loss of information exchanged between the EMS and the microgrid DERs and loads. The EMS decision-making process is majorly affected by the ESS SOC measure based on which the remaining DERs are dispatched so as to manage the ESS power and SOC while providing the necessary reserve for this isochronous resource to regulate the voltage and frequency. As such, the EMS is crucial to provide along with power and energy management, voltage and frequency regulation functions and a DDoS cyber-attack can result in severe consequences on the overall microgrid operation. The evaluation of the performance indices defined in chapter 2 will facilitate the quantification of the impact such a DDoS cyber-attack could engender.

4.3. Fallback Control Strategy

In the following, a fallback mitigation strategy that ensures the resiliency of the islanded microgrid against DDoS cyber-attacks disrupting the communication between the microgrid controller EMS and the DERs is proposed. In order to attain the objective of the proposed mitigation strategy, the following sub-objectives need to be achieved.

1) The ESS should operate in autonomous mode to manage its power and SOC and continue assuming its functions as the grid-forming DER, whereby it forms and regulates the grid voltage and frequency while compensating for the variations from the loads and the renewable DERs
2) The uncompromised dispatchable DERs should coordinate with the ESS without relying on vulnerable communication links to contribute to the cyber-attack mitigation

4.3.1. DDoS Cyber-Attack Detection and Transition to Fallback Operation

In the event of a DDoS cyber-attack, the microgrid measurements and EMS dispatch set-point will no longer be exchanged over the communication network. As a result, the DERs will operate based on the dispatch set-points received prior to the application of the DDoS. If the DDoS launching time is selected such that the power and/or the energy limits are violated as in (2.24), (2.25) and/or (2.29), (2.30), large frequency or voltage excursions will result at the islanded SM based or inverter-interfaced microgrid PCC, respectively. The fallback control mitigation strategy proposed in the upcoming sections will be activated based on (4.1) and (4.2) for SM based and 100% inverter-interfaced microgrids, respectively.

$$Fallback\ Control = \begin{cases} ON & if \begin{array}{c} FDI\ or\ DDoS\ cyber-attack\ detected\ or \\ Communication\ loss\ or \\ f(t+kt_d) \geq f_{max} \quad or\ f(t+kt_d) \leq f_{min} \end{array} \\ OFF & elsewhere \end{cases} \tag{4.1}$$

$$for\ k = 0, t_s, \dots, 1 \qquad and \qquad s.t. \quad t_d < t_{protection}$$

$$Fallback\ Control = \begin{cases} ON & if \quad \begin{array}{c} FDI\ or\ DDoS\ cyber-attack\ detected\ or \\ Communication\ loss\ or \\ V(t+kt_d) \geq V_{max} \quad or\ V(t+kt_d) \leq V_{min} \end{array} \\ OFF & elsewhere \end{cases} \tag{4. 2}$$

$$for\ k = 0, t_s, \dots, 1 \qquad and \qquad s.t. \quad t_d < t_{protection}$$

Whereby, $f(t)$ and $V(t)$ are the frequency and voltage at time t (Hz and p.u.), f_{min}, f_{max} the minimum and maximum frequency limits (Hz), V_{min}, V_{max} the minimum and maximum voltage limits (p.u.), t_d the time of detection of the attack (s) and $t_{protection}$ the time of activation of the protection schemes (s).

It is important to mention that the time of detection of the DDoS cyber-attack is set to be negligibly lower than that of activation of the protection schemes in order to ensure that the system shifts to the fallback control strategy which restores normal operation without causing unnecessary load and renewable energy curtailment.

4.3.2. Rule-Based Algorithm – Standalone ESS Control

Supplementary control loops are added to the ESS primary control in order to provide decentralized power and SOC management functions along with voltage and frequency regulation. The active power of the ESS should be properly controlled in order to manage and maintain the SOC in the desired operating region. In SM based microgrids, the active power generated or absorbed by the storage system is evaluated in accordance with the frequency reference (Fig. 4.1a). Therefore, in order to control the ESS active power and SOC, the input frequency reference should be modified. On the other hand, in 100% inverter-interfaced microgrids, the frequency of the grid-side voltage is imposed and set to the nominal frequency by a virtual PLL and the ESS active power can be controlled by adjusting the input voltage reference (Fig. 4.1b). Fig. 4.1 shows the ESS local controllers with the supplementary loops pertaining to frequency and voltage reference control, whereby Δf_{SOC} and ΔV_{SOC} correspond to the SOC management contributions in SM based and inverter-interfaced microgrids respectively.

As the SOC surpasses its maximum or minimum permissible limits, the ESS is forced to stop discharging or charging, respectively. Therefore, limits on the PI controller which set the ESS active power reference in accordance with the SOC in an SM based microgrid are defined as per the diagram shown in Fig. 4.2. In the case of 100% inverter-interfaced microgrids, the maximum

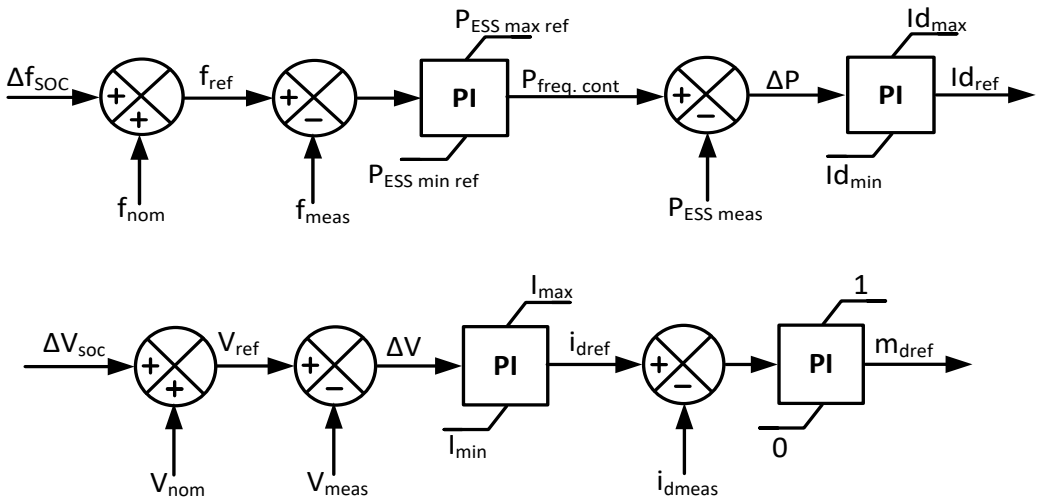

Fig. 4. 1: Proposed ESS local SOC and power control loop for (upper) SM based (lower) 100% inverter-interfaced microgrids

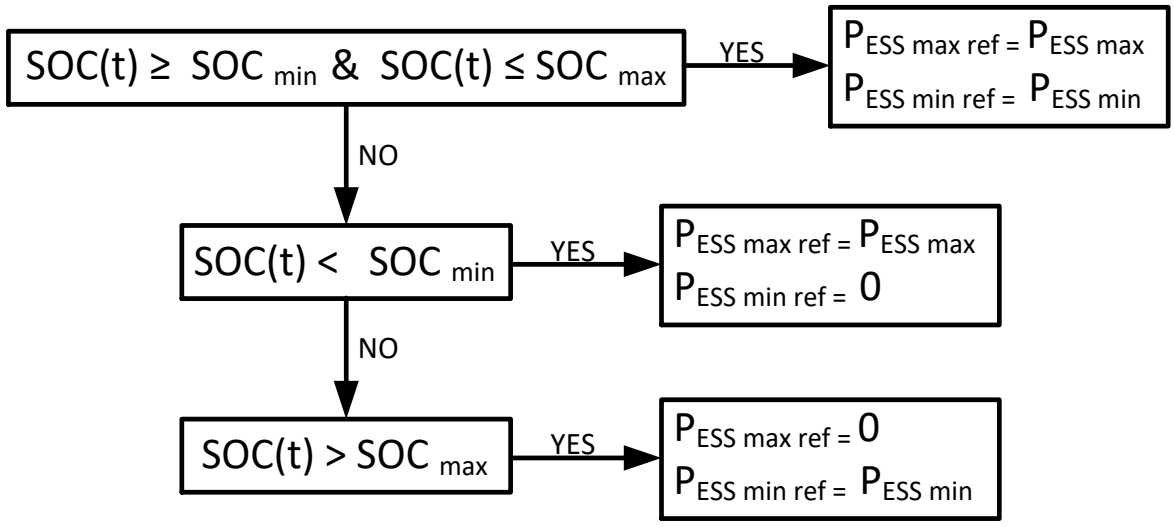

Fig. 4. 2: ESS PI controller power saturation limits

and minimum current limits are evaluated according to the same rules to limit the output of the PI controller setting the d-frame current reference.

The rule-based algorithm employed for frequency reference control associated with SOC management of SM based microgrids is explained hereafter. The same concepts apply for inverter-interfaced microgrids with the main difference being that a voltage reference control strategy is employed based on the same rules, SOC and active power limitations. Accordingly, identical equations are used to evaluate the change in the ESS voltage reference ΔV_{SOC} for SOC management in an inverter-interfaced microgrids whereby f_{max}, f_{min} and f_{nom} are replaced by V_{max}, V_{min} and V_{nom} being the maximum, minimum and nominal voltage values.

Four SOC limits are defined for the ESS; the maximum and minimum critical SOC limits, SOC_{max} and SOC_{min}, that the ESS should not exceed at all times, and the upper and lower bound SOC limits, SOC_{ub} and SOC_{lb}, forming the desired operating region. The frequency deviation Δf_{SOC} corresponding to the SOC management loop is evaluated in accordance with the rule-based algorithm shown in Fig. 4.3 and developed to ensure that the local controller manages the ESS SOC and active power. Given that the ESS operates as the isochronous DER, its main functions, being frequency and voltage regulation, are prioritized over SOC management.

The desired SOC operating region [SOC_{lb} ; SOC_{ub}] is further divided to include two bounds SOC_{low} and SOC_{high}that need to be surpassed for the SOC management and frequency reference control to activate. In this operating dead-band, the frequency reference is equal to its nominal value. As the SOC exceeds these high or low limits, the ESS local controller increases or decreases the reference frequency, controlling the ESS power exchange with the microgrid. When the SOC surpasses the upper or lower bounds, the frequency reference is maintained at its maximum or minimum permissible values, not to trigger DER disconnection and load shedding protection schemes.

With reference to Figs 4.1, 4.3-4.5 the following equations are defined, whereby $\Delta f_{SOC}(t)$ represents the change in the ESS frequency reference resulting from the SOC management loop at time *t*, f_{max} and f_{min} the maximum and minimum allowable frequency limits, f_{nom} the nominal frequency, SOC_{low} and SOC_{high} the low and high SOC limits.

$$\Delta f_{SOC1}(t) = \Delta f_{SOC}(t-1) \tag{4. 3}$$

$$\Delta f_{SOC2}(t) = (f_{max} - f_{nom})\left(\frac{SOC(t) - SOC_{high}}{SOC_{ub} - SOC_{high}}\right) \tag{4. 4}$$

$$\Delta f_{SOC3}(t) = (f_{max} - f_{nom}) \tag{4. 5}$$

$$\Delta f_{SOC4}(t) = (f_{min} - f_{nom})\left(\frac{SOC_{low} - SOC(t)}{SOC_{low} - SOC_{lb}}\right) \tag{4. 6}$$

$$\Delta f_{SOC5}(t) = (f_{min} - f_{nom}) \tag{4. 7}$$

The variation in the frequency reference resulting from the SOC management loop $\Delta f_{SOC}$is not solely dependent on the SOC operating bounds; it also varies based on active power limits set to ensure that the ESS properly performs the isochronous DER functions. The active power reference of the ESS includes both an AC and a DC component associated with frequency regulation, and a DC component associated with the SOC management loop (4.8), (4.9).

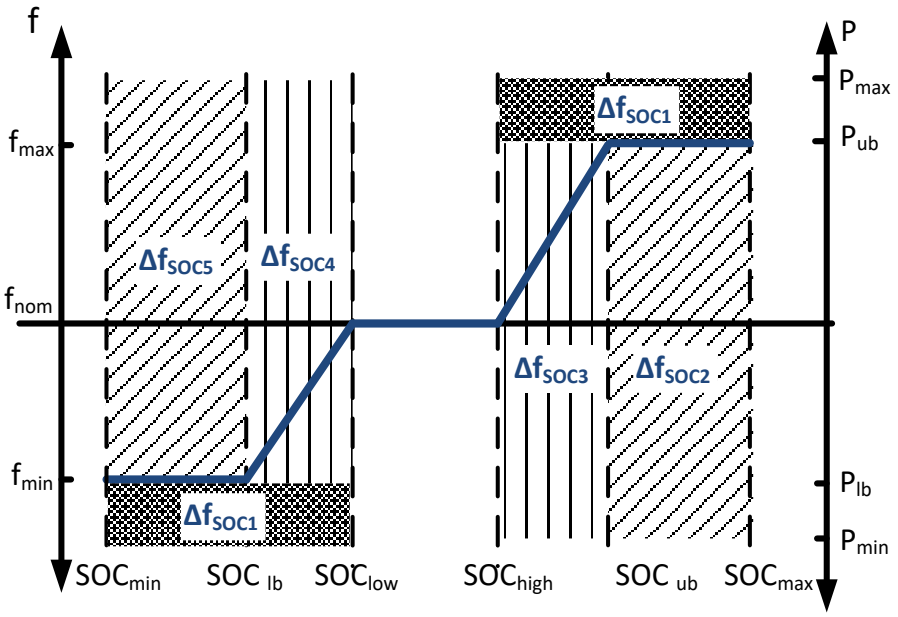

Fig. 4. 3: Frequency control for autonomous ESS power & SOC management

$$P_{ESS\,ref} = P_{f\,regulation} + P_{SOC\,management} \quad (4.\,8)$$

$$P_{ESS\,ref} = (P_{DC} + P_{AC})_{f\,regulation} + P_{DC\,SOC\,management} \quad (4.\,9)$$

In order to ensure that the isochronous DER has enough headroom to compensate for the load and renewable DERs variations, upper and lower active power boundaries, $P_{ESS\,ub}$ and $P_{ESS\,lb}$, are imposed to limit the DC component of the reference power. As the reference power reaches these limits the frequency contribution Δf_{SOC} from the SOC management loop is maintained at its last value which, if added to the nominal frequency, does not violate the defined power limits (4.3).

4.3.3. Coordinated Control for Power and Energy Management

As the ESS SOC management loop modifies its voltage or frequency reference to control its power exchange with the microgrid, the dispatchable DER's local controllers should respond to the bias and adjust their power output to charge/discharge the ESS in a coordinated manner. Fig. 4.5 shows the active power control loop of the dispatchable diesel generator. When the reference is equal to its nominal set-point, the DERs operate based on the fixed active power dispatch set-points. An additional active power contribution associated with the ESS power and energy management is added to that fixed power reference. A low-pass filter is employed to limit the

contribution only to long-term frequency excursions associated with the isochronous DER power and energy management. A conventional droop controller whose contribution is added to the resultant active power reference is employed to compensate for the short-term excursions produced by the renewable DERs.

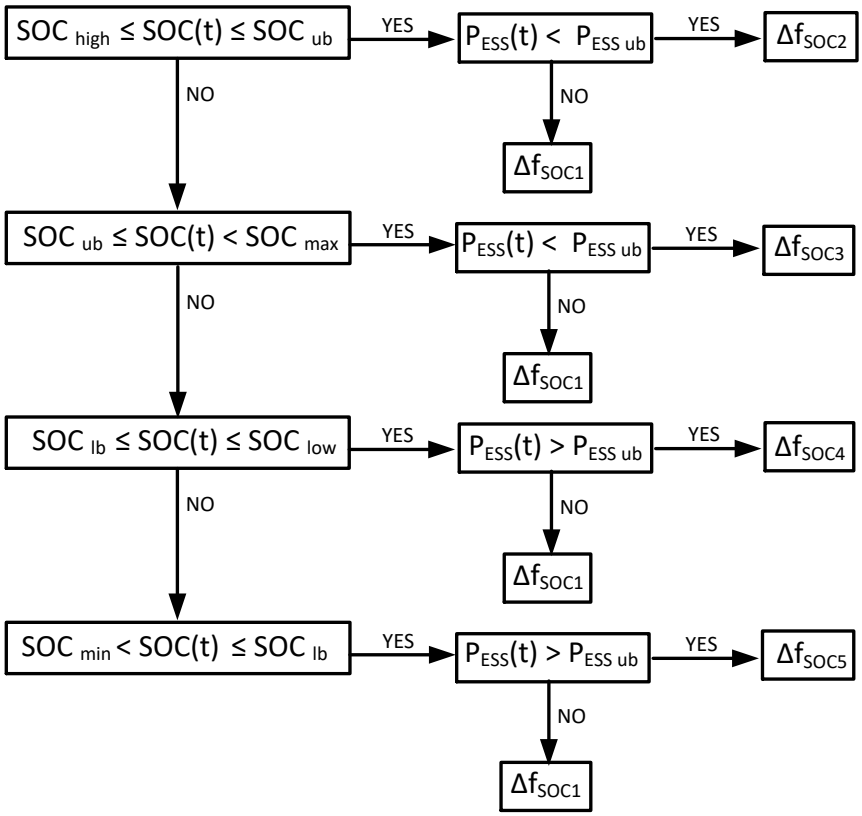

Fig. 4. 4: Rule-based algorithm for the evaluation of Δf_{SOC}

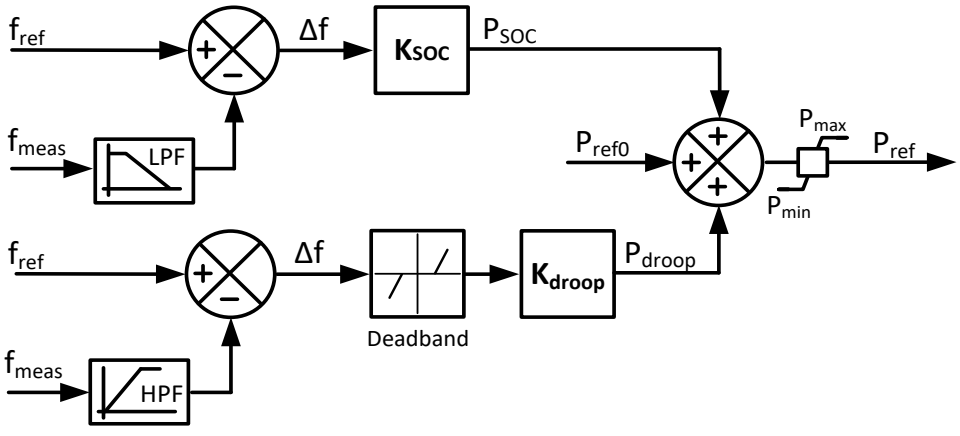

Fig. 4. 5: Dispatchable DER SOC compensation control loop

The DERs should be capable of compensating for the worst-case scenario whereby the isochronous ESS operating at its maximum or minimum capacities is forced to shift from discharging to charging or vice versa. Therefore, the gains associated with the grid-forming DER power and energy management control loop should be tuned in a way that the sum of the contributions from the dispatchable DERs is sufficient to cover the transition and compensate the mismatch. The gains can be evaluated as in (4.10) and (4.11) such that when the frequency reference is set to its maximum or minimum value by the ESS local power and SOC manager, the sum of the DERs contributions is greater or equal to the ESS maximum or minimum capacity limits.

$$\left(f_{ref} - f_{min}\right) \sum_{\forall l \in dDER} K_{SOC} \geq P_{ESS\,max} \tag{4. 10}$$

$$\left(f_{ref} - f_{max}\right) \sum_{\forall l \in dDER} K_{SOC} \leq P_{ESS\,min} \tag{4. 11}$$

The coordinated control for power and SOC management of inverter-interfaced thermal DERs in 100% inverter-based microgrids is designed in a similar manner. The only difference is that the frequency measures f_{ref}, f_{meas} in Fig. 4.3 and f_{min}, f_{max} in (4.4) - (4.7) are replaced by their corresponding voltage measures V_{ref}, V_{meas} , V_{min} and V_{max}.

4.4. Microgrid System Overview

A 25 kV distribution test-line reconfigured as a microgrid was employed throughout this work as the testing platform. The inverter-interfaced DERs used consist of a WTG and an ESS. The WTG is modeled as a type-4 full converter wind turbine and is operated in MPPT mode and at unity power factor for active and reactive power control. A grid-tie inverter also models the ESS fed from a lithium-ion battery. The ESS is operated as the isochronous generator that forms the microgrid's voltage and frequency. Average models are used to represent the power converters to significantly improve computational speed performance. Two microgrid configurations are considered: an SM based microgrid employing a diesel generator directly connected to the microgrid and a 100% inverter-interfaced microgrid employing a thermal DER connected to the grid through a power-electronic interface. The ratings of the DERs are tabulated in table 4.1. The 24 hour load and wind power profiles, shown in Fig. 4.6, were taken from the Ontario Independent Electricity System Operator (IESO) website [147] and the Waterloo weather station [148],

respectively. The wind speed profile includes stochastic variations characterized by the Kaimal power spectral density [149]. The simulation results shown in the next section were obtained using the load and wind profiles for the period from 8:00 to 8:15 as it reflects a fast decrease in the residual power intensifying the impact of a DDoS cyber-attack and resulting in a rapid violation of the isochronous resource energy constraints as per (2.30). The DER parameters used by the EMS optimization are tabulated in table 4.2.

The real-time HIL co-simulation setup used and the DDoS cyber-attack model are described in section 2.3.2 and Annexes C and D. The setup allows assessment of the impact of the DDoS cyber-attack on the operation of the microgrid critical control functions and evaluation of the performance of the fallback control strategy in mitigating the attack and enhancing the microgrid resiliency and robustness.

4.5. Real-Time HIL Co-Simulation Results

4.5.1. Test Cases

The operation of the rule-based algorithm for standalone ESS control and that of the DERs supplementary control for coordination were first tested using simulation. Real-time HIL co-simulations were performed in order to accurately model the DDoS attack and validate the proposed fallback control mitigation strategy.

Table 4. 1: DERs ratings

DERs	Ratings
WTG	150 kVA, 150 kW
ESS	250 kVA/100 kW, 33.3 kWh
Thermal DER	400 kVA, 320 kW

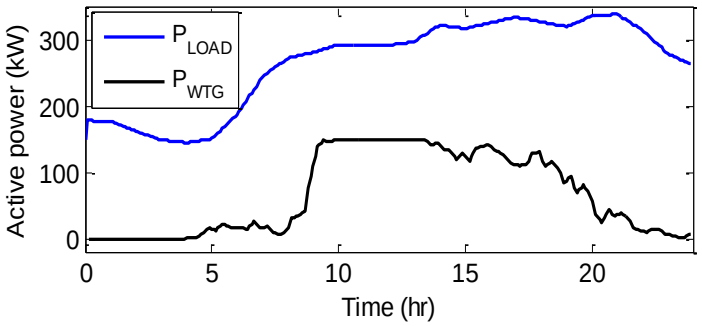

Fig. 4. 6: Load & wind power profiles

Table 4. 2: EMS Parameters

Parameter	P_{DER}^{min}	P_{DER}^{max}	E_{ESS}^{min}	E_{ESS}^{max}	ɳ
Value	96 kW	320 kW	35	70	0.96

The base case represents the microgrid operating under normal conditions in the absence of an attack in the system. The results will be compared to the case where a DDoS cyber-attack is applied after 2 minutes of the start of the simulation and where no mitigation means are implemented. A third case study which consists on applying the DDoS cyber-attack and implementing the proposed fallback control mitigation strategy will also be studied to evaluate the effectiveness of the developed strategy. The test cases will be analyzed and compared for both SM (case 1) and 100% inverter-interfaced (case 2) microgrid configurations.

The SOC operating limits are set to: $\mathrm{SOC_{max}} = 80\%$, $\mathrm{SOC_{min}} = 20\%$, $\mathrm{SOC_{ub}} = 70\%$, $\mathrm{SOC_{lb}} = 35\%$,$\mathrm{SOC_{high}} = 65\%$ and $\mathrm{SOC_{low}} = 40\%$. The ESS upper and lower limits associated with active power reserve, such that the ESS has headroom to compensate generation and load variability, were set to be 70 and -70 kW, respectively. The maximum and minimum power and energy limits are used by the EMS to evaluate the DER dispatch set-points. As per the IEEE 1547 standard, the maximum and minimum allowable frequency limits are 60.5 and 59.3 Hz. The voltage limits were set to±2% of the nominal voltage. After the violation of these bounds, load shedding and generation disconnection protection schemes can initiate based on local voltage or frequency measurements. Table 4.3 shows the performance indices calculated to quantify the physical impact of the attack and to evaluate the effectiveness of the proposed fallback control mitigation strategy. The performance indices are quantified in the presence of protection schemes which initiate such that the renewable DER is first disconnected to reduce the transients in the frequency/voltage responses and an amount of load proportional to the frequency/voltage excursions is shed to restore active power balance in SM/inverter based microgrids, respectively.

4.5.2. Case 1 – DDoS Attack on SM Based Microgrids

4.5.2.1. Normal Operation

In this scenario, the EMS gathers the DERs measurements and generates active power dispatch set-points so as to manage the power and energy in the microgrid system. As the residual power decreases, the sum of the active power generated by the diesel generator and the ESS decreases to maintain power balance (Figs. 4.7 and 4.8). In addition, as the ESS SOC approaches its maximum limit, the EMS dispatches a lower set-point for the diesel generator so that the ESS could start discharging, maintaining the SOC between its permissible bounds (Fig. 4.9). The

isochronous resource is therefore always available and can provide its main function and regulate the islanded microgrid frequency (Fig. 4.10).

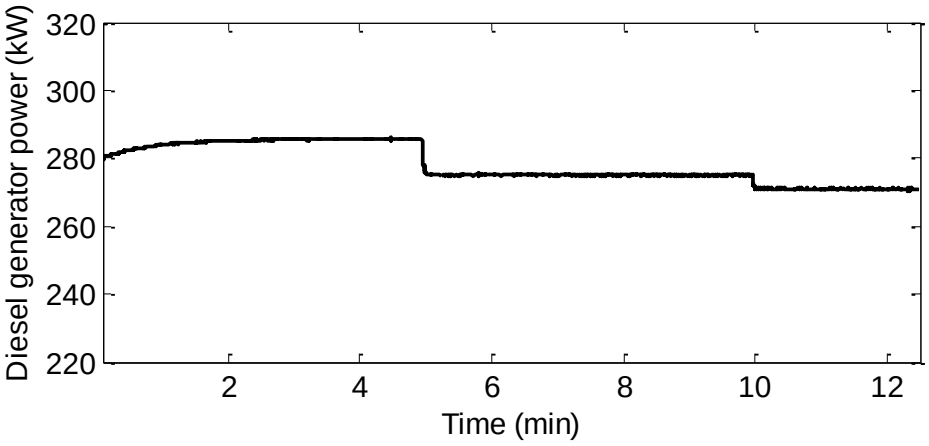

Fig. 4. 7: Case 1 - Normal Operation: Diesel generator power

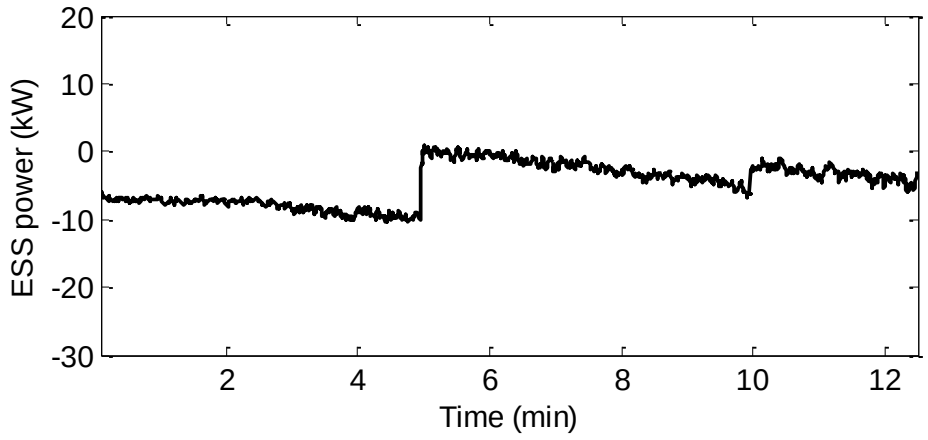

Fig. 4. 8: Case 1 - Normal Operation: ESS power

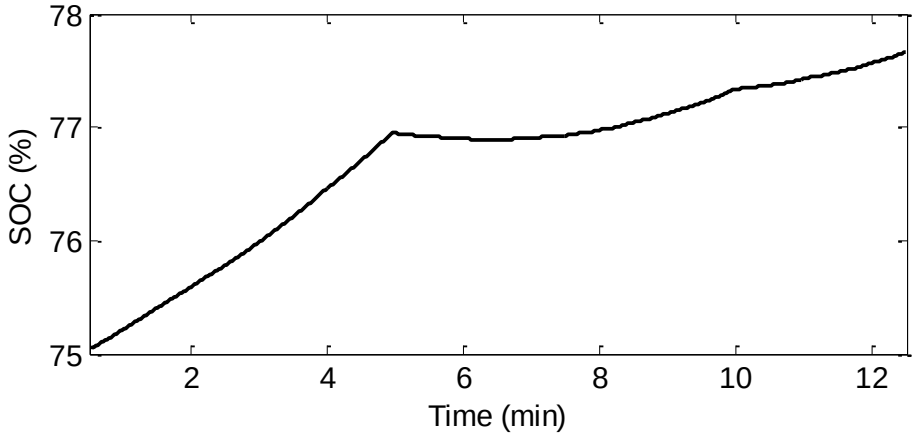

Fig. 4. 9: Case 1 - Normal Operation: ESS SOC

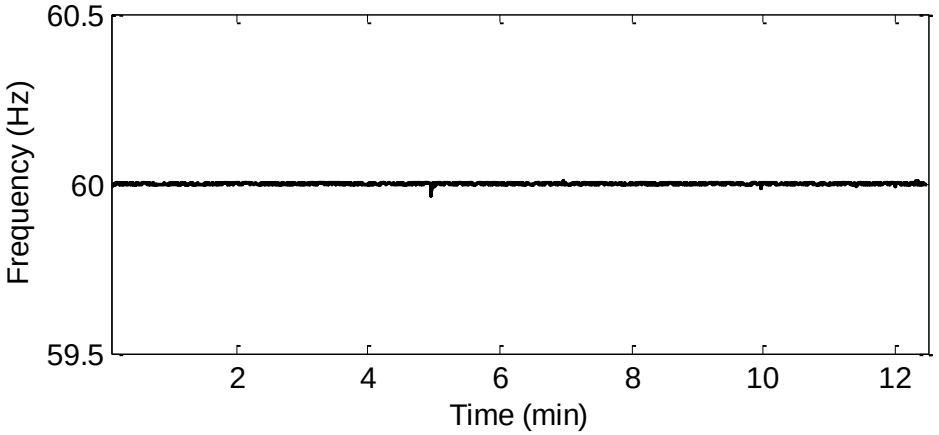

Fig. 4. 10: Case 1 - Normal Operation: Microgrid system frequency

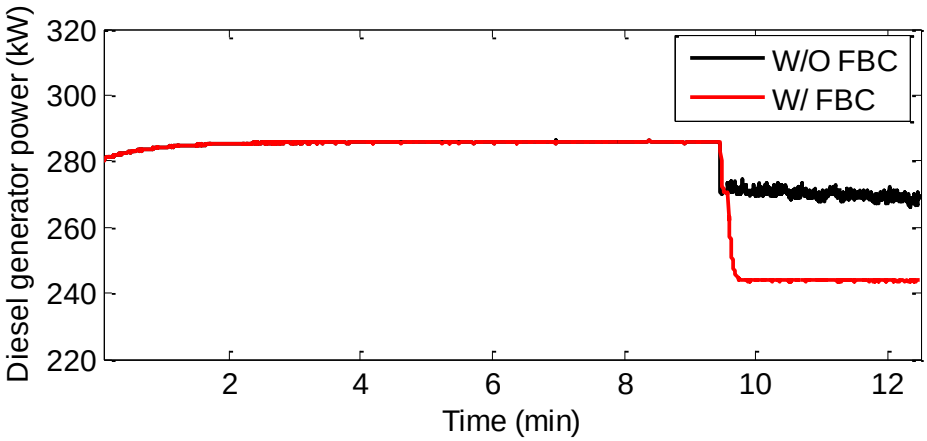

Fig. 4. 11: Case 1 - Diesel generator power with & without fallback control

4.5.2.2. DDoS Attack Impact Assessment

As the DDoS cyber-attack is applied after 2 minutes of the start of the simulation, the diesel generator will operate based on the last dispatch set-point it received from the EMS prior to the attack (Fig. 4.11). In reference to the base case, as the residual active power decreases and the ESS SOC approaches its maximum limit (Fig. 4.12), the diesel generator is supposed to decrease its active power to ensure power balance and energy management. As a result of the attack, the isochronous DER will have to compensate for the imbalance caused by the diesel generator to maintain the frequency close to its nominal value (Fig. 4.13). As a result, the ESS keeps on decreasing its active power until the maximum SOC is reached leading to an infringement of the SOC management constraints as defined in (2.30). As the SOC reaches its maximum bound, a hard limit is set on the ESS generated active power forcing it to stop discharging and implying that the grid-forming resource can no longer provide its function and regulate the frequency. In the absence

of mitigation strategies, large frequency excursions exceeding the permissible limits result at the PCC if the protection schemes are not initiated, as shown in Fig. 4.14. The frequency could only be restored back to its nominal value if protection schemes are activated curtailing wind generation (Fig. 4.15) and load (Fig. 4.16) reducing the microgrid capacity to host renewables and to provide continuous power supply to the loads.

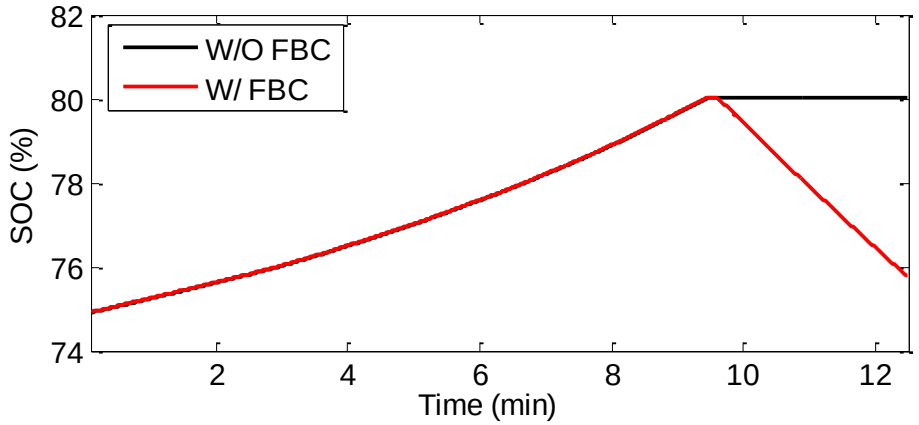

Fig. 4. 12: Case 1 – ESS SOC with & without fallback control

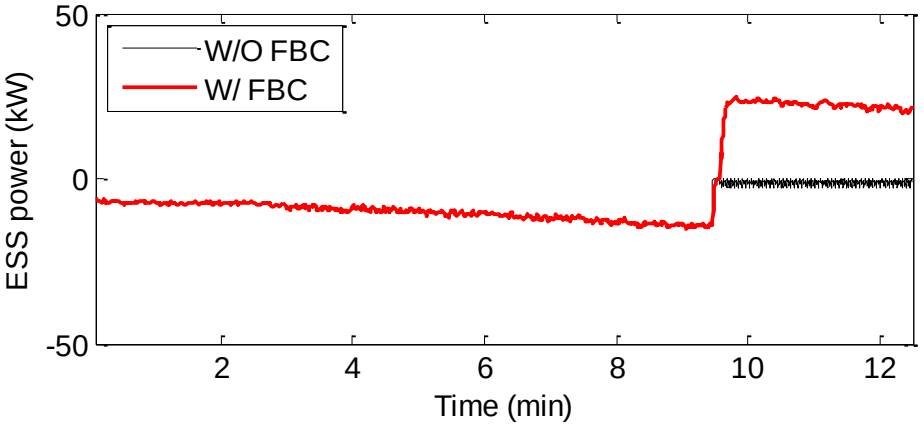

Fig. 4. 13: Case 1 - ESS power with & without fallback control

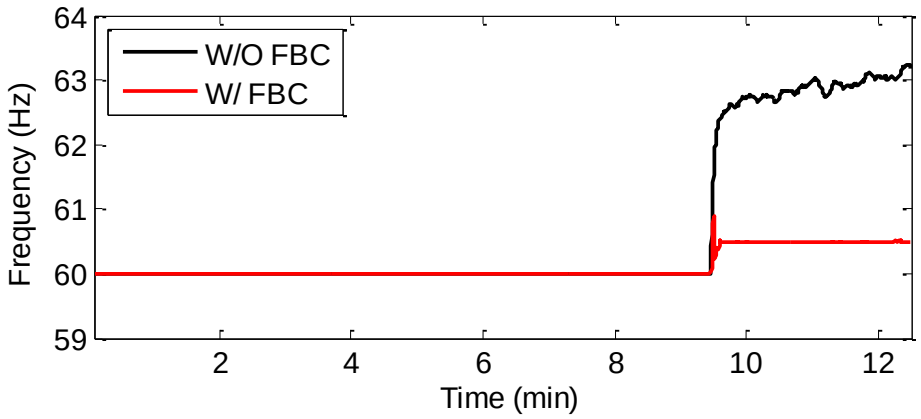

Fig. 4. 14: Case 1 – Microgrid system frequency with & without fallback control

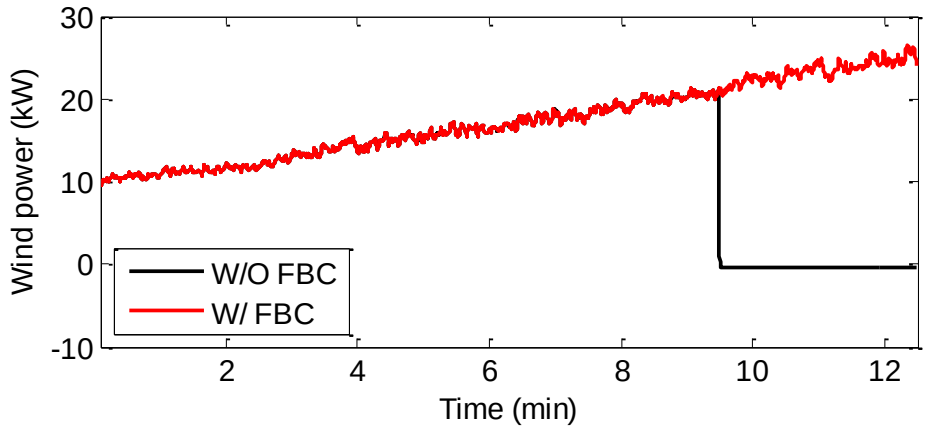

Fig. 4. 15: Case 1 – WTG power with & without fallback control

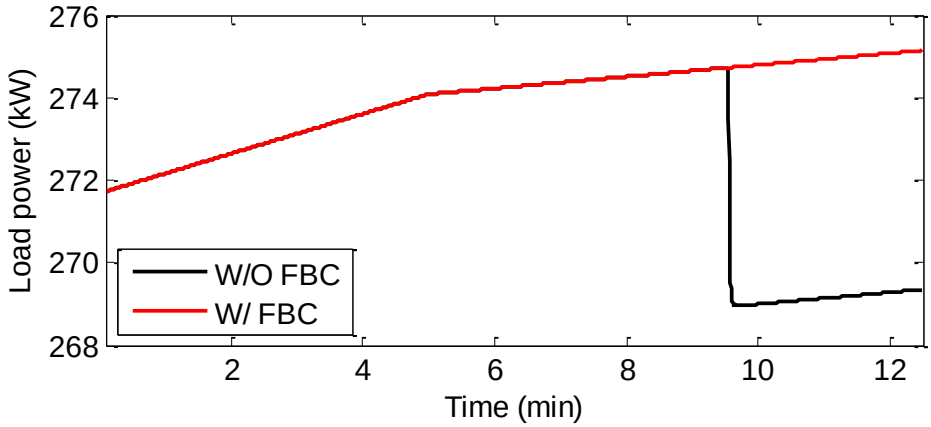

Fig. 4. 16: Case 1 – Load power served with & without fallback control

4.5.2.3. Fallback Control Performance Testing

As previously explained, the system transitions to the fallback control topology as soon as the frequency exceeds its permissible operating region for a specific amount of time. As the fallback control strategy is applied, the ESS increases its frequency reference (Fig. 4.17). This frequency reference change actuates the diesel generator supplementary control loops associated with power and energy management to dispatch less power (Fig. 4.11), giving more headroom to the ESS to start discharging (Fig. 4.13) so as to decrease its SOC (Fig. 4.12) and operate between SOC_{ub} and SOC_{high}. The diesel generator active power contribution is plotted in Fig. 4.18 and it corresponds to the amount needed by the ESS to shift from charging to discharging and reduce the SOC to values contained in the desired operating bounds. The gain associated with the diesel generator supplementary control loop for power and SOC management is set to 35% in that case to ensure that when the frequency reference is adjusted to its maximum value, the diesel generator contribution is equivalent to the ESS minimum active power.

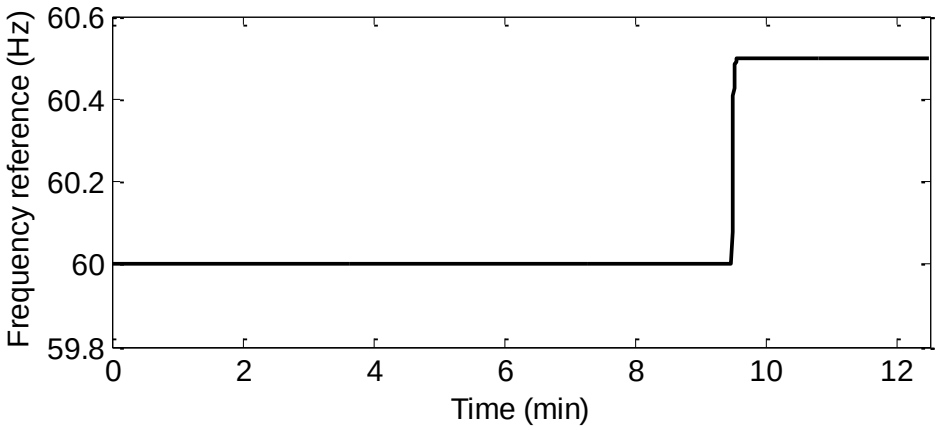

Fig. 4. 17: Case 1 – Frequency reference change with fallback control

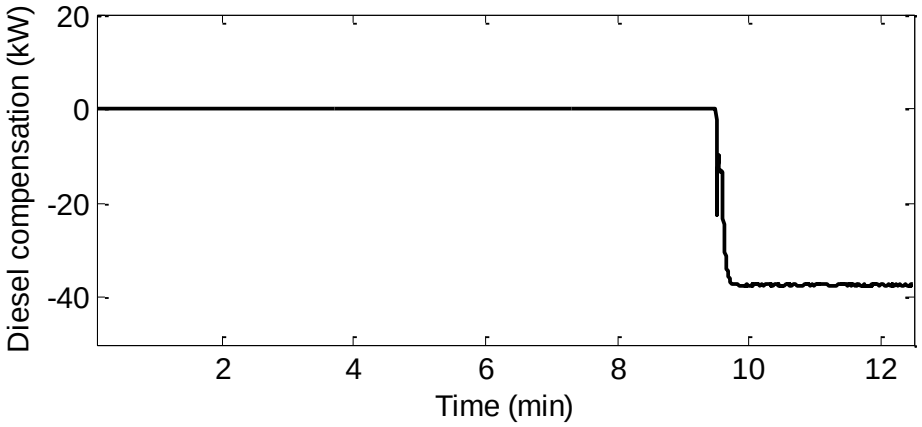

Fig. 4. 18: Case 1 - Diesel generator compensation for decentralized energy management

4.5.3. Case 2 – DDoS Attack on Inverter-Interfaced Microgrids

The simulation results presented in this section prove the applicability of the fallback mitigation strategy to 100% inverter-interfaced microgrids.

4.5.3.1. Normal Operation

Under normal operating conditions, and in the absence of a DDoS cyber-attack affecting the microgrid communication network, the EMS dispatched the DERs such that it manages the ESS SOC and ensures power balance in the 100% inverter-interfaced microgrid (Figs. 4.19 -4.21). As power and energy constraints are not violated, the grid-forming ESS will always have enough capacity and headroom to compensate for the intermittency of the renewable DERs and to ensure power balance while regulating the microgrid voltage (Fig. 4.22)

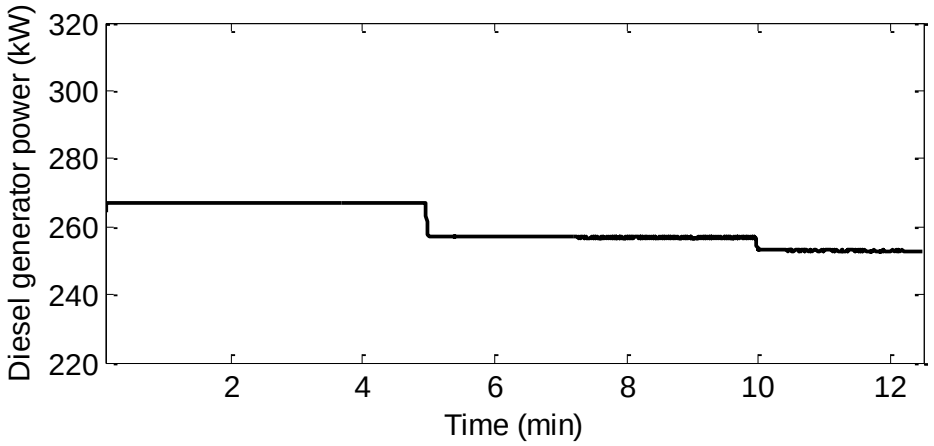

Fig. 4. 19: Case 2 – Normal Operation: Diesel generator power

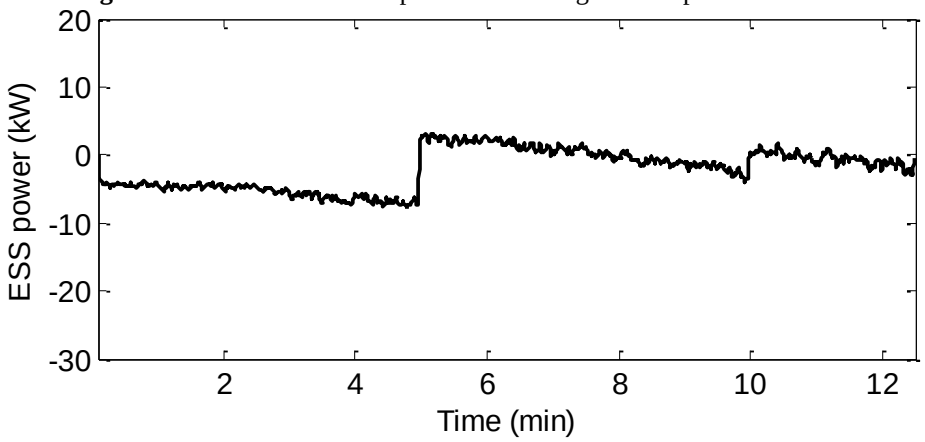

Fig. 4. 20: Case 2 – Normal Operation: ESS power

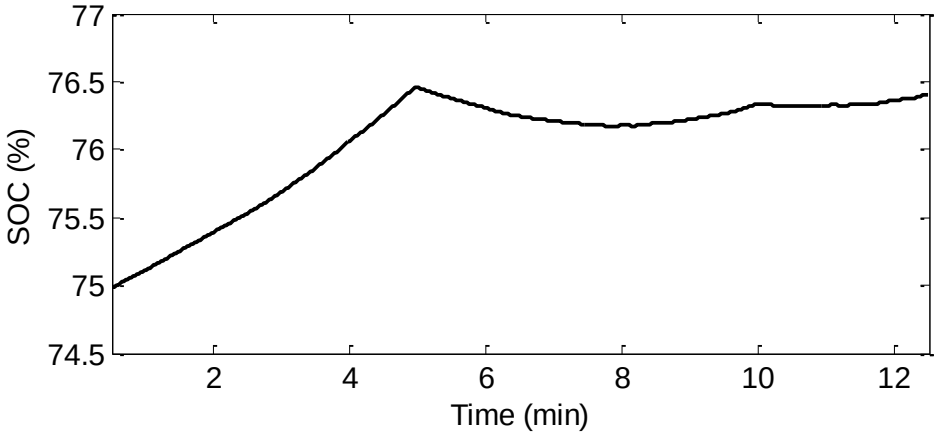

Fig. 4. 21: Case 2– Normal Operation: ESS SOC

4.5.3.2. DDoS Attack Impact Assessment

With reference to Figs. 4.23-4.26, when the fallback control is not applied, the DDoS attack causes the SOC minimum permissible limits to be reached forcing the ESS to stop discharging.

This results in active power mismatches that cannot be compensated by the dispatchable DER local controller. In 100% inverter-interfaced microgrids the active power imbalances are translated into voltage excursions rather than frequency excursions as in the case of SM based microgrids. As the ESS active power is limited, the DER no longer has enough headroom to compensate for the varying load and renewable energy and it becomes incapable of providing its isochronous

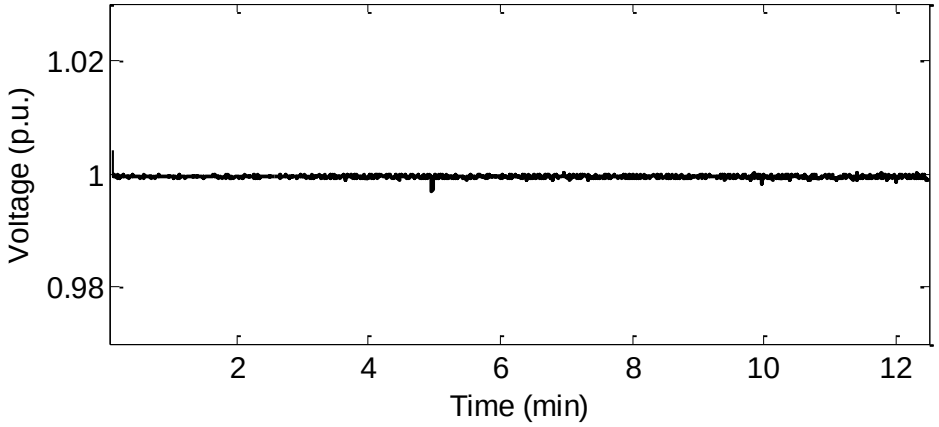

Fig. 4. 22: Case 2 – Normal Operation: Microgrid system frequency

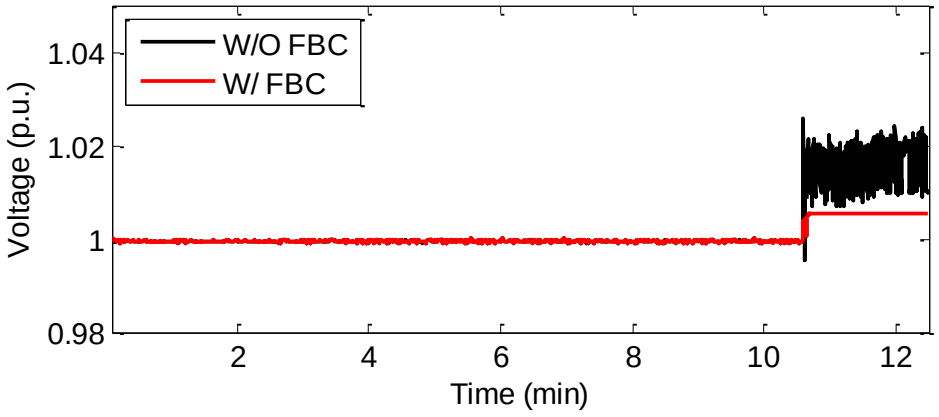

Fig. 4. 23: Case 2 – Microgrid system voltage with & without fallback control

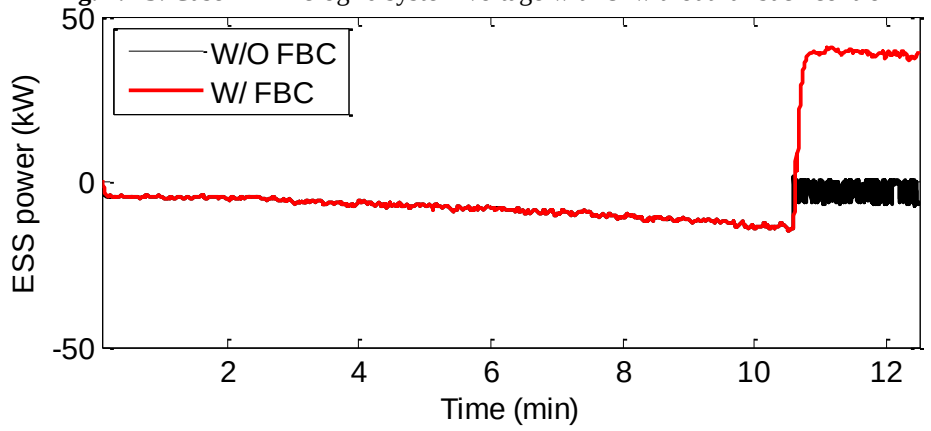

Fig. 4. 24: Case 2 – ESS power with & without fallback control

functions regulating the microgrid's voltage. Fig. 4.23 clearly shows the severe voltage excursions resulting from the DDoS cyber-attack and triggering the protection schemes (Figs. 4.27 and 4.28).

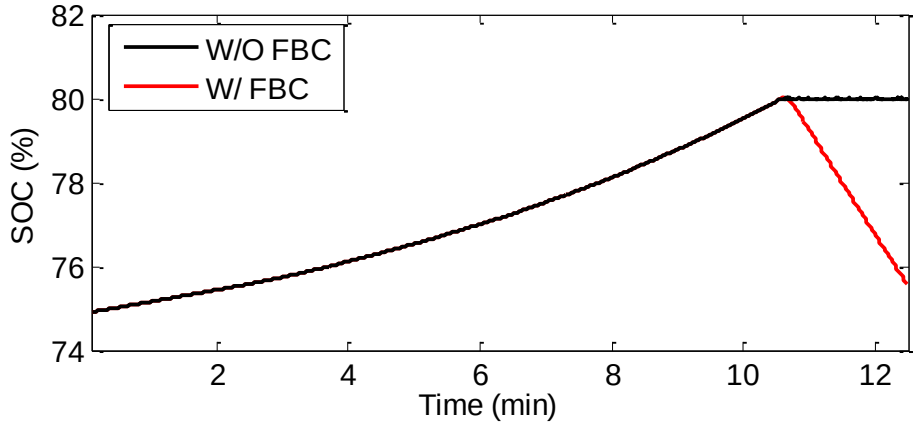

Fig. 4. 25: Case 2 – ESS SOC with & without fallback control

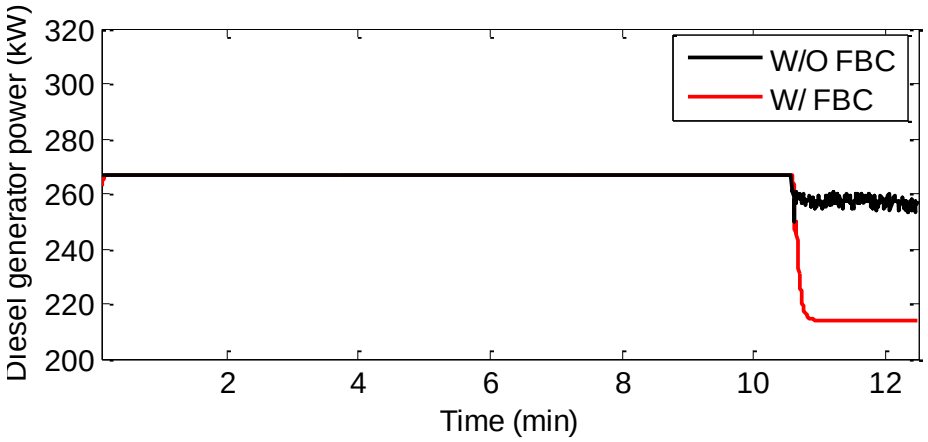

Fig. 4. 26: Case 2 – Thermal DER power with & without fallback control

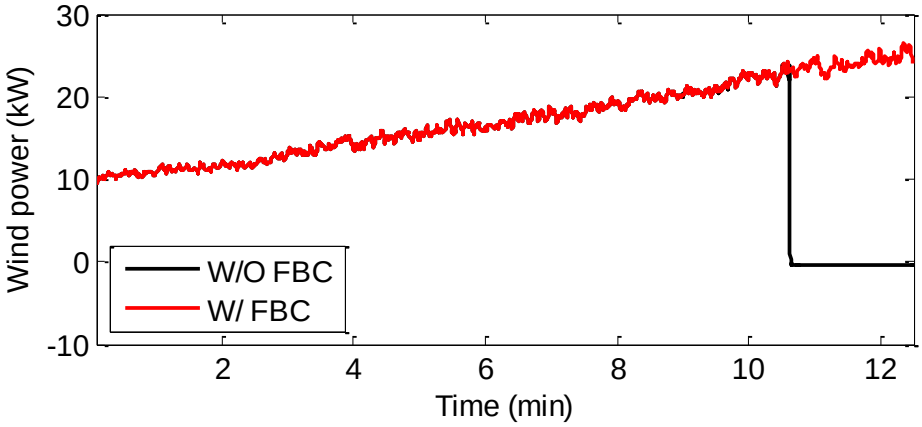

Fig. 4. 27: Case 2 – WTG power with & without fallback control

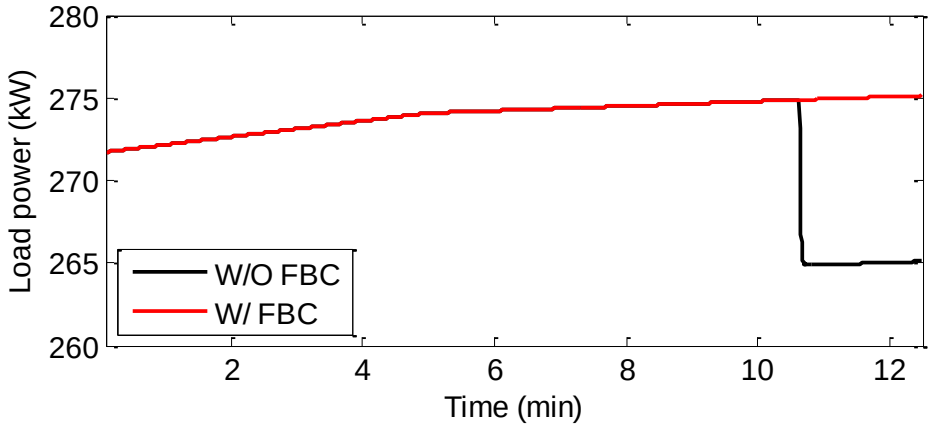

Fig. 4. 28: Case 2 – Load power served with & without fallback control

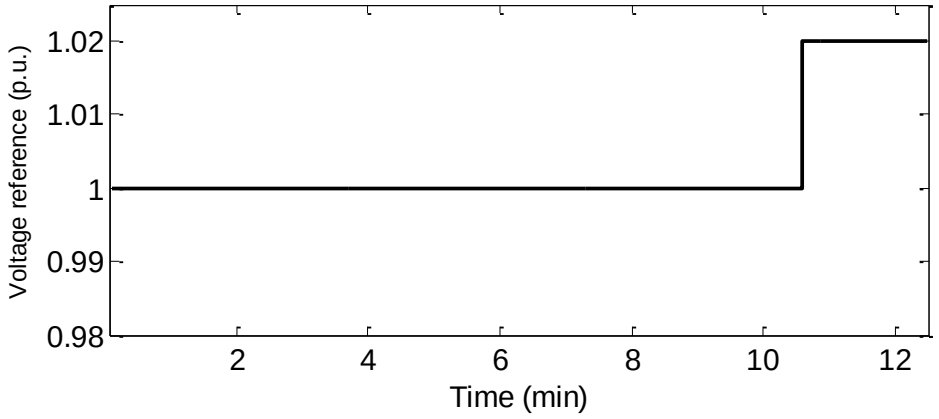

Fig. 4. 29: Case 2 – Voltage reference change with fallback control

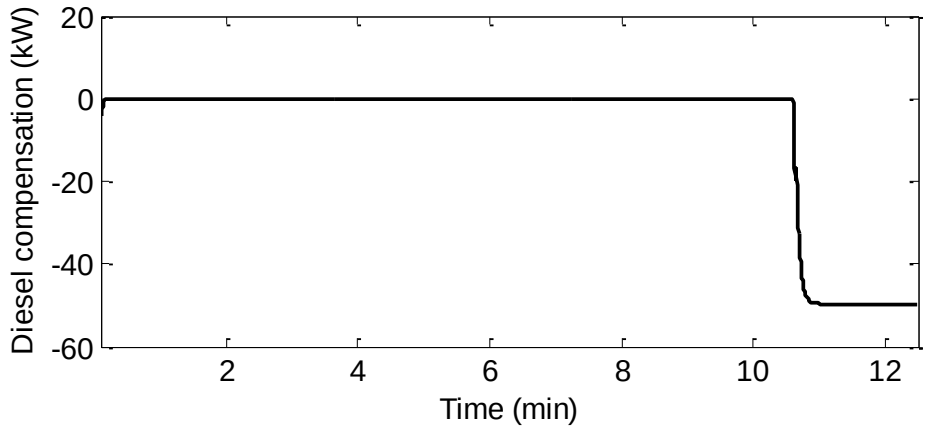

Fig. 4. 30: Case 2 – Thermal DER compensation for decentralized energy management

4.5.3.3. Fallback Control Performance Testing

Figs. 4.23 and 4.25 show the ability of the fallback controller to manage the SOC while ensuring that the ESS continues to provide the grid forming capabilities and regulates the voltage

in the post-attack period. It can be observed from Figs. 4.24 and 4.26 that the proposed strategy provides coordination between the isochronous ESS and the dispatchable DER. For instance, as the voltage exceeds its permissible limit for a specified amount of time, the fallback control initiates and the ESS performs the adjustment of the voltage reference based on the rule-based algorithm (Fig. 4.29). The dispatchable DER supplementary control loop for power and energy management is activated and the DER responds to the voltage bias and provides attack compensation (Fig. 4.30). The dispatchable DER supplementary control loop gain for SOC management is set to 30% to ensure that when the voltage reference is adjusted to its maximum value, the DER contribution is equivalent to the ESS minimum active power.

Performance indices quantifying the impact of the attack and the effectiveness of the proposed fallback controller are summarized in Table 4.3. It can be concluded that in the event of a DDoS attack disrupting the communication between the microgrid DERs and their secondary controller, the fallback strategy not only increases the hosting capacity of renewable energy and ensures reliable power supply to the loads but also results in a lower average cost of energy.

It is important to mention that in the absence of a mitigation solution, larger amounts of load and renewable energy would be curtailed if the DDoS cyber-attack is not directly detected and the communication network restored. The proposed fallback mitigation strategy distributes the power and energy management functions of the EMS amongst the DERs and would never initiate load or renewable energy curtailment schemes due to DDoS cyber-attacks. Although the average cost of energy when the fallback control strategy is applied is close to that obtained under normal operating conditions, this will not always be the case since the proposed strategy's main objective

Table 4. 3: Performance indices

	Renewable Energy Shed (kWh)	**Load Energy Not Served (kWh)**	**Average Cost of Energy ($/kWh)**
Case 1–Base Case	0	0	0.3591
Case 1-w/o FBC	5.7036	1.3562	0.3689
Case 1-w/ FBC	0	0	0.3571
Case 2-Base Case	0	0	0.3318
Case 2-w/o FBC	3.6603	1.4806	0.34
Case 2-w/ FBC	0	0	0.3313

is to ensure power and energy management without accounting for the cost. Therefore, from an economic point of view, shifting back to a centralized EMS architecture after detection of the attack and restoration of the communication network would always be desired. The fallback control strategy will however always be more economical than the case where no control is applied since in the latter case, load and renewable energies are curtailed and conventional costly resources are used instead of the inexpensive renewable DERs.

4.6. Conclusion

In islanded microgrids with a large penetration of renewable energy, operating the ESS as the grid forming DER has various advantages that were previously explained. When in isochronous mode, the ESS sets and regulates the microgrid voltage and frequency. It is the function of the EMS to manage the power and the energy in the microgrid to ensure that the isochronous resource always has enough headroom to compensate for power imbalances and intermittent penetration of renewable generation in order to regulate the voltage and the frequency. A DDoS cyber-attack compromising the microgrid communication network and causing loss of information exchange between the DERs and the centralized EMS was investigated in this chapter. The impact of the attack has been quantified by means of performance indices and the effectiveness of the proposed mitigation strategy has been validated for both 100% inverter-interfaced and SM based microgrids, using the real-time HIL co-simulation setup. In the post-attack period, the ESS energy is depleted and the DER no longer has enough headroom to compensate for active power variations and provide its voltage and frequency regulation functions. As the remaining DERs control loops are not inherently designed to provide compensation in such events, the protection schemes will be initiated causing unnecessary curtailment of generation and loads.

A fallback control strategy was proposed to mitigate the impact of the DDoS cyber-attack. Based on local frequency measures, the DDoS cyber-attack is sensed and the microgrid shifts from the centralized control topology to the fallback architecture; whereby the power and energy management functions initially provided by the centralized EMS are distributed amongst the DERs. Supplementary control loops are added to the DERs such that the isochronous resource modifies its frequency or voltage reference to signal to the dispatchable DERs the need to provide compensation and ensure power and energy management. As a result, the ESS power and energy

are always managed to keep the isochronous resource available at all times to compensate for the load and renewable DERs variations and to regulate the islanded microgrid voltage and frequency. The performance indices evaluated showed that the proposed technique enhanced the microgrid resiliency against DDoS cyber-attacks as it maximized the grid's capacity to host renewable generation and to continuously supply critical loads, promoted coordination between DERs for power and energy management and reduced the average cost of energy. The upcoming chapter further analyzes DDoS and FDI cyber-attacks targeting microgrids operating the SM in grid-forming mode and proposes a multi-stage cyber resilient control infrastructure which enhances the microgrid resiliency and survivability in the event of detected and undetected cyber-attacks.

Chapter 5
Multi-Stage Cyber Resilient Control Infrastructure and Recommendations for Enhanced Cyber Security

5.1. Introduction

The previous chapters provided a detailed analysis of cyber-attacks which compromise the microgrid data integrity and availability. The impact of FDI and DDoS cyber-attacks was quantitatively evaluated by means of microgrid specific performance indices and potential mitigation strategies were proposed. Before concluding this thesis, a cyber resilient control infrastructure which implements among others the aforementioned control strategies in a coordinated manner needs to be proposed and tested under different attack scenarios. In this chapter, a multi-stage cyber resilient control infrastructure is developed to ensure transient and steady-state stability, power and energy management and reliable operation in the event of cyber-attacks targeting the microgrid data integrity and availability. A parametric analysis is conducted to evaluate the performance of the cyber resilient control infrastructure and test its ability to adapt to the different operating conditions.

With a high penetration of renewable energy into the grid, operating the ESS as the grid-forming DER has numerous benefits that were detailed in chapter 4. For the sake of generality and

in order to analyze cyber-attacks targeting microgrid systems, it is imperative to investigate the case of microgrids featuring an SM based DER operating as the grid-forming resource. In fact, operating the SM as the grid-forming DER provides many advantages as the resource is typically larger than power-electronic interfaced DERs and it has additional reserve capacity to ensure power balance and regulate the voltage and the frequency of the islanded system [19].

The multi-stage cyber resilient control strategy developed in this chapter proposes enhanced control loops added to the microgrid DERs and loads to distribute power and energy management functions amongst the grid-forming DER, which operates as a master, and the remaining DERs and loads operating as slaves. As such, it ensures power and energy balance, transient and steady-state frequency stability while maximizing the microgrid capacity to host renewable energy and to supply loads without relying on vulnerable communications. The proposed strategy has three operating stages that initiate consecutively based on the severity of the cyber-attack and the generation mix: 1) the dispatchable DERs local controllers employ control loops to compensate for transient events that could result from undetected FDI attacks, 2) if a cyber-attack is detected, or the frequency exceeds the permissible bounds, the grid-forming DER shifts to a decentralized control mode whereby it modifies its frequency reference to locally signal to the remaining DERs the need to provide compensation. The grid-supporting ESS local controller employs functions which detect the change of control mode and respond to the grid-forming DER signals, 3) in the case of limited capacity of the grid-forming and grid-supporting DERs, the renewable DERs and the loads are controlled locally to curtail the amount of energy which restores balance. The different control loops added to the DERs and loads to enhance the resilience of the microgrid control infrastructure to resist cyber-attacks are detailed below. Recommendations and best cyber security practices drawn from this work are then concluded in this chapter.

5.2. Microgrid Configuration and Cyber-Attacks Models

In this chapter, the SM based diesel generator is operated as the isochronous DER which forms and regulates the microgrid voltage and frequency to compensate for the renewable DERs fluctuations and load variations in the inter-dispatch period. The active power local control loops

pertaining to the diesel generator were detailed in chapter 2 and are shown in Fig. 2.2. The microgrid considered also features an ESS operating as the grid-supporting DER based on fixed active and reactive power set-points as shown in Fig. 2.7. The DER may or may not provide voltage and frequency support by applying voltage and frequency droop control. A WTG is also employed and its power-electronic interface operates as a current-controlled VSI based on the MPPT curves, as explained in chapter 2. The corresponding control loops are shown in Figs. 2.8 and 2.9. The EMS employed in this chapter updates the DERs primary control set-points on a 5 minutes basis. The EMS objective is to minimize the average cost of energy in the islanded microgrid subject to the various constraints defined in section 2.2.2.1 of this thesis.

An FDI cyber-attacks which gains access to the IP network, and gains control over the microgrid EMS HMI is modeled as described in section 2.3.1. The cyber-attacker maliciously tampers with the commands sent from the EMS to operate the dispatchable DERs (2.6). The FDI cyber-attack parameters are selected such that the microgrid power management requirements are violated as formulated in (2.22) and (2.23). Furthermore, a DDoS cyber-attack which gains access to the IP network connecting the microgrid digital controller and the engine performing the EMS operation is also launched and analyzed. As in the previous chapter and as formulated in chapter 2, the DDoS cyber-attack results in complete loss of information exchange between the EMS and the microgrid feeder, DERs and loads. The cyber-attack parameters, in that case, are selected such that the microgrid power management requirements are violated as formulated in (2.24) and (2.25).

5.3. Multi-Stage Cyber Resilient Control Infrastructure

The block diagram shown in Fig. 5.1 summarizes the different stages of the cyber resilient control infrastructure developed in this chapter. As the EMS commands sent to operate the DERs are maliciously modified, corrupted or blocked due to the FDI and or DDoS cyber-attacks launched, the system should start relying on local measures to ensure stable and reliable operation. Therefore, as shown in the block diagram, the frequency is employed as the measure for attack detection and post-attack reaction. Combined virtual inertial response and droop control is added to the grid-supporting DER and operates at all times to provide compensation for the transient

events streaming from undetected FDI attacks. As the power-electronic interfaced DER reaches its maximum capacity delimited by the converter ratings, the frequency would start surpassing the allowable bounds. The frequency measurements are monitored at the grid-forming DER side and as soon as they exceed the bounds for a specific amount of time, indicating the violation of the microgrid power management requirements, or as a cyber-attack is detected or communication is lost, the system shifts to the decentralized mode of operation. The supplementary control loops associated with the grid-forming diesel generator activate and vary the frequency. Consequently, the dispatchable grid-supporting ESS supplementary controller responds to the frequency change and vary their active power to provide attack compensation. Load and renewable energy curtailment schemes will only activate when both the grid forming DER and the dispatchable ESS reach their maximum or minimum power capacities; this event could be detected by monitoring the local frequency measures such that load and renewable energy curtailment schemes only activate when the system's frequency is less than the minimum or greater than the maximum allowable limits, respectively. Firm frequency bounds and timeouts are set such that the supplementary control loops for the DERs and loads do not oppose one another and provide compensation at the same time. The master-slave configuration of the decentralized control scheme along with the control loops proposed for the mitigation of transient events and coordination of the DERs and load to provide cyber-attack compensation are presented in the following subsections.

In reference to Fig. 5.1, t_s is the simulation time step, t_{OF} the time period after which over frequency generation disconnection schemes initiate (s), t_{UF} the time period after which under frequency load shedding schemes initiate (s), t_d the time period after which the DoS/DDoS cyber-attack is detected (s), $P_L(t)$ the load power at time t (kW), $P_{L-forecast}(t)$ the load forecast at time t (kW), $P_{L-shed}(t)$ the amount of load to be shed at time t (kW), $P_{RDER}(t)$ the renewable DER power at time t (kW), $P_{MPPT}(t)$ the renewable DER active power following the MPPT curve at time t (kW), $P_{RDER-shed}(t)$ the amount of renewable power curtailed at time t (kW), $P_{DDER}(t)$ the non-renewable dispatchable DER power at time t (kW), $P_{ref0}(t)$ active power reference sent to dispatch the DER at time t (kW), $P_{droop}(t)$ the active power contribution from droop control at time t (kW), $P_{VI}(t)$ the active power contribution from virtual inertial response at time t (kW), $P_{comp}(t)$ the active power compensation resulting from the transition to the decentralized control mode at time t (kW).

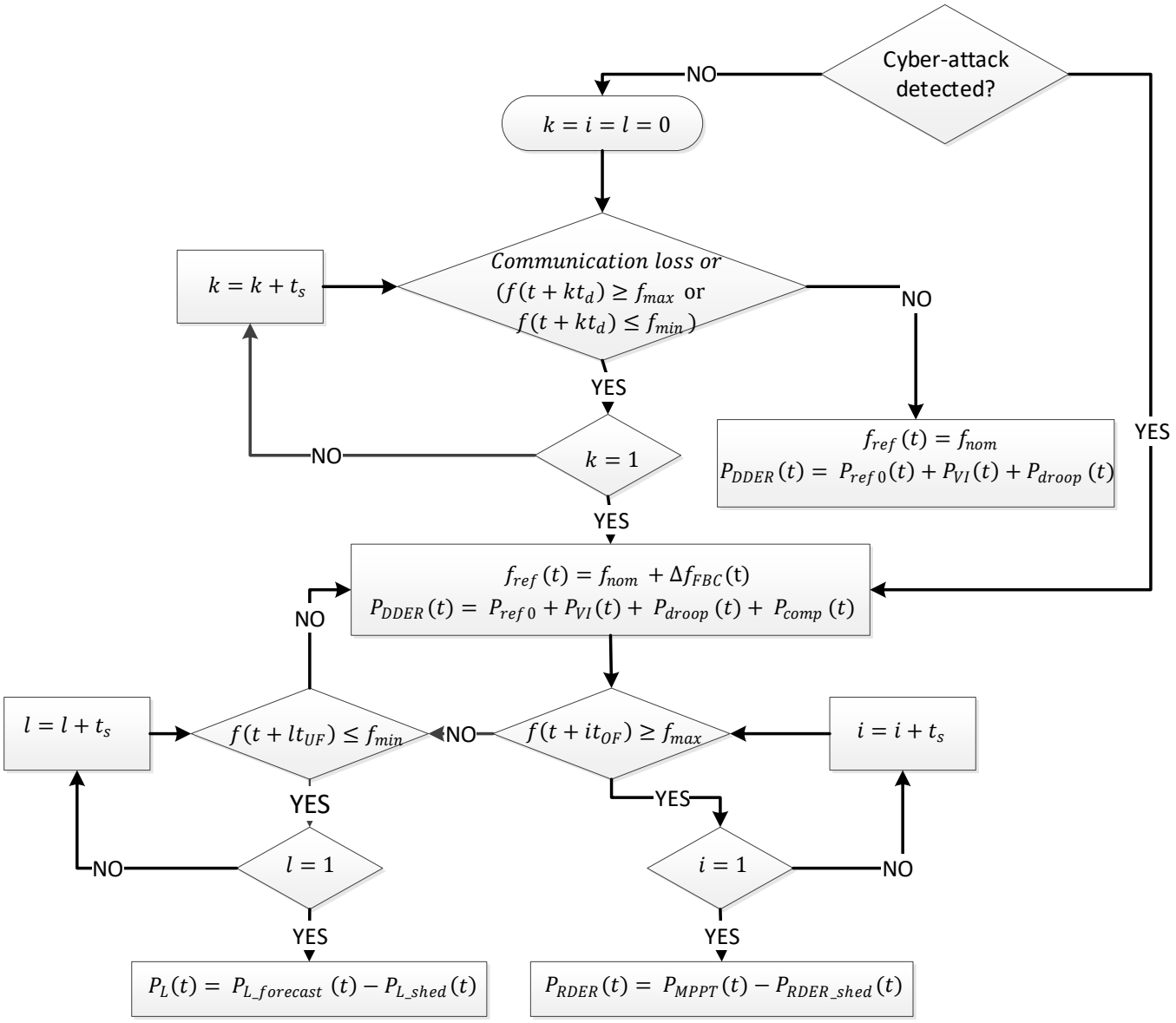

Fig. 5. 1: Multi-stage control algorithm block diagram

5.3.1. Supplementary Control for Grid-Supporting Power-Electronic Interfaced DERs

The amplitude of the frequency excursions engendered by FDI cyber-attacks largely depends on the microgrid inertia and the grid-forming resource's dynamic response and ability to

compensate. Therefore, it is critical that the fast-acting power-electronic interfaced grid-supporting ESS local controller has the ability to provide frequency support, especially when an FDI cyber-attack is undetected or not detected in a timely manner targets microgrids with very low inertia operating a DER with a very slow dynamic response, such as a diesel generator, as the isochronous resource. Therefore, enhanced supplementary control loops, incorporating virtual inertial response and droop control, are added to the ESS local controller to provide transient and steady-state frequency support respectively. The virtual inertia controller provides fast compensation for the transients typically induced by FDI cyber-attacks by emulating SMs' inertia allowing the ESS to inject/absorb active power in proportion to the frequency excursion, its rate of change and the equivalent inertia (Fig. 5.2). As for the droop control, an active power contribution proportional to the frequency deviation is generated to provide permanent compensation as per (3.2).

As explained in what follows, in the event where the combined droop and virtual inertia control provide their maximum compensation or when a cyber-attack is detected, normal operation would only be restored if power management is handled locally. The grid-forming DER would vary its frequency reference in accordance with Fig. 5.3 and (5.1) to signal the need for compensation. Therefore, control loops need to be added to the grid-supporting ESS local controller to provide, using local frequency signals, means for coordination with the isochronous resource and compensation of the disturbances resulting from the attack. Fig. 5.2 shows the dispatchable DER local control loop whereby an active power compensation P_{comp} is added to the DER compromised reference power and combined controller contribution to account for the long-term frequency deviations associated with frequency reference control for power management.

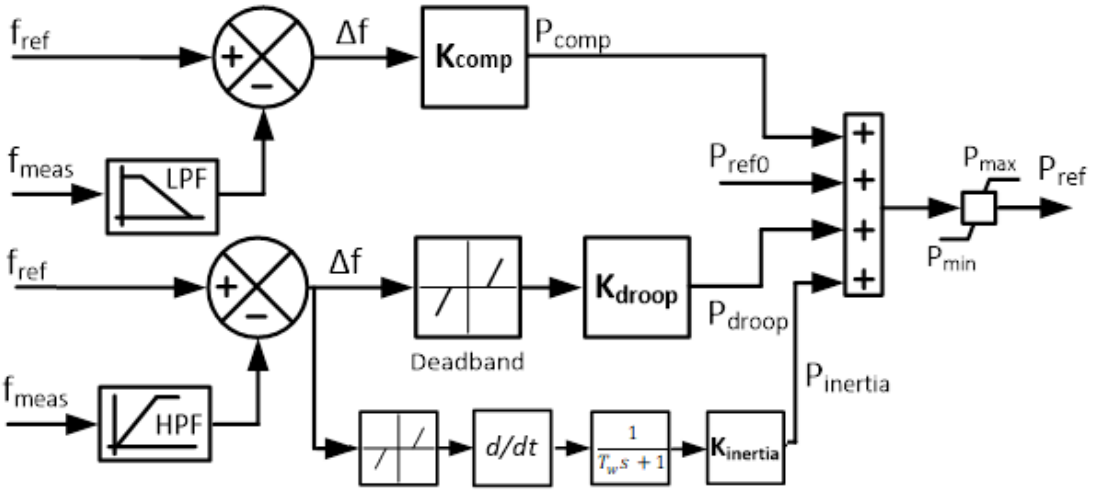

Fig. 5. 2: Supplementary loops for grid-supporting DER decentralized control

5.3.2. Decentralized Control of Grid-Forming Master DER

If the cyber-attacks bias and/or launching time is selected such that the power management functions are violated as in (2.22) through (2.25), and/or the contribution provided by the combined virtual inertia and droop controller added to the power-electronic interfaced ESS has reached its limits, large frequency excursions resulting in nuisance load and energy curtailment would activate in the absence of supplementary control. In order to counteract such impacts, distributing the power and energy management functions amongst the DERs which coordinate without relying on communication is proposed. Upon detection of cyber-attacks, or abnormalities in the frequency response and before exceeding the maximum and minimum frequency limits, the grid-forming DER shifts to the decentralized mode of operation as per (4.1) to restore normal operation without causing unnecessary load and energy curtailment.

The proposed strategy has been introduced in chapter 4, in the event of a DDoS cyber-attack when the ESS is operated as the grid-forming DER. The strategy is extended here to mitigate different cyber-attacks as the SM based diesel generator operates as the isochronous resource. Six power limits are defined such that: $P_{min} < P_{lb} < P_{low} < P_{high} < P_{ub} < P_{max}$. The maximum and minimum critical power limits, P_{max} and P_{min}, that the grid-forming DER should not exceed at all times, the upper and lower bound limits, P_{ub} and P_{lb}, forming the desired operating region, and the low and high limits, P_{low} and P_{high}, which initiate the proposed control strategy once exceeded. This strategy consists of modifying the frequency reference of the isochronous resource so as to respect the power constraints in the event of erroneous EMS commands or complete/partial loss of information exchange with the EMS. The frequency change $\Delta f(t)$ added to the DER nominal frequency reference at time t is evaluated as in (5.1) whereby f_{nom} is the nominal frequency, and

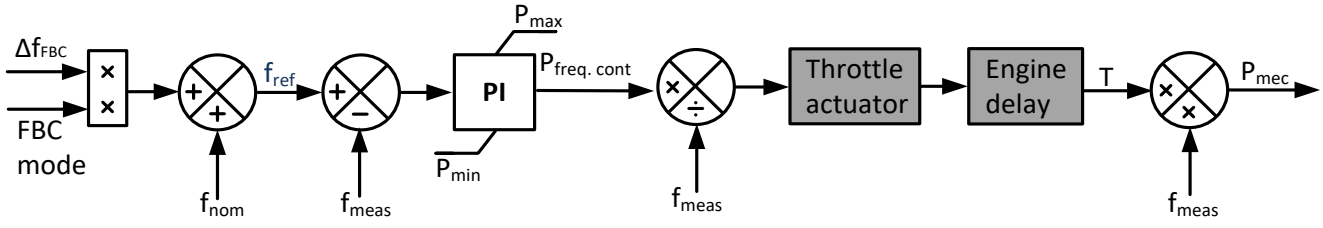

Fig. 5. 3: Isochronous DER supplementary control for power management

P(t) the grid-forming DER power at time t. The local control loop for the grid-forming diesel generator is illustrated in Fig. 5.3. Upon detection of the attack based on local frequency measures, the decentralized control mode activates initiating frequency reference control.

$$\Delta f(t) = \begin{cases} (f_{min} - f_{nom})\left(\frac{P(t)-P_{high}}{P_{ub}-P_{high}}\right) & \text{if } P_{high} \le P(t) \le P_{ub} \\ (f_{min} - f_{nom}) & \text{if } P_{ub} \le P(t) \le P_{max} \\ (f_{max} - f_{nom})\left(\frac{P_{low}-P(t)}{P_{low}-P_{lb}}\right) & \text{if } P_{lb} \le P(t) \le P_{low} \\ (f_{max} - f_{nom}) & \text{if } P_{min} \le P(t) \le P_{lb} \\ \Delta f(t-1) & \text{if } P(t) \le P_{low} \text{ or } P(t) \ge P_{high} \end{cases} \quad (5.1)$$

5.3.3. Supplementary Control for Adaptive Load and Renewable Energy Curtailment

Conventional protection schemes initiate as the frequency excursions exceed the allowable bounds for a specified amount of time and disconnect the DER. Traditional load shedding schemes curtail blocks of loads resulting in unnecessary load loss or rely on communicated information to shed the necessary amount of load that restores balance. In this chapter, the attacker is assumed to have gained access to the microgrid communication network and can, therefore, spread throughout the network to engender more damages. Therefore, the proposed supplementary control will not rely on communication links that have a considerable risk of being compromised. In addition, the proposed control will only shed the amount of energy which restores normal operation. Figs. 5.4 and 5.5 show the supplementary control loops added to the renewable DER and loads to compensate for the attack in the event where the grid-forming and grid-supporting DERs have reached their maximum or minimum power capacities and more or less power is needed, respectively. In this scenario, the maximum and minimum frequency references set by the isochronous DER in the decentralized mode would be exceeded and energy curtailment becomes necessary. The control loop added to the renewable DER operates in the event of over frequencies exceeding the maximum allowable limit. An active power contribution proportional to the frequency excursion is added to the MPPT reference power of the DER to reduce its energy, restore power balance and operate the frequency in between the allowable limits. Accordingly, an amount of load power proportional to the frequency excursion in under frequency scenarios is shed to restore to restore normal operation. The gains associated with the supplementary loops are selected

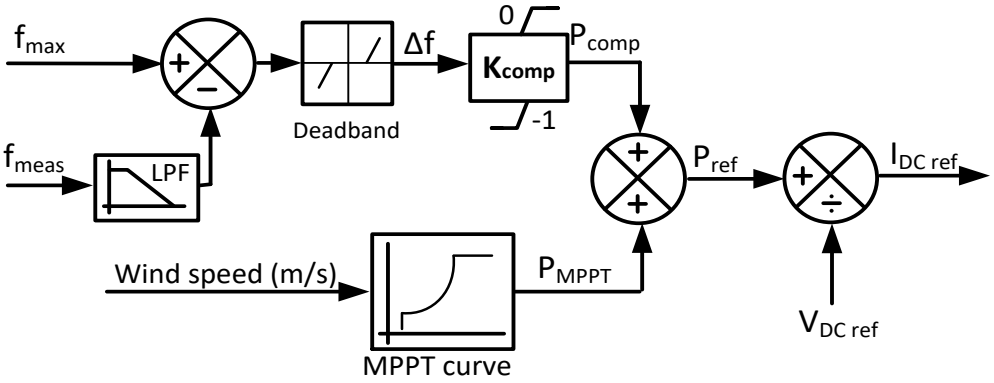

Fig. 5. 4: Supplementary control for renewable DER decentralized control

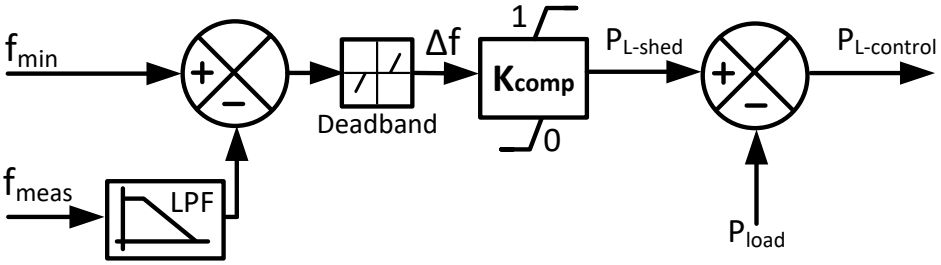

Fig. 5. 5: Supplementary control loops for load decentralized control

such that the amount of energy shed exactly corresponds to the amount of imbalance, maximizing the microgrid capacity to host renewable energy and supply loads.

5.4. Microgrid System Overview and Test Cases

The testing platform considered in this study is based on a 25 kV distribution system adapted from a utility feeder and reconfigured as an islanded microgrid. The inverter-interfaced DERs used consist of a 150 kW WTG and a 100 kW/ 125kWh ESS. The WTG is modeled as a type-4 full converter wind turbine and is operated in MPPT mode. The ESS is operated in fixed PQ mode and a 320 kW diesel generator is operated as the isochronous DER that forms the microgrid's voltage and frequency. The DER parameters used by the EMS optimization are tabulated in table 5.1. The real-time HIL co-simulation setup developed is described in chapter 2 and Appendix C and the simulation time step is set to 50 µs. The EMS dispatches set-points every 5 minutes and the FDI and DDoS cyber-attacks previously formulated are launched after 4 minutes of the start of the simulation so that their impact is apparent at the second EMS dispatch. The

performance of the proposed multi-stage cyber resilient control infrastructure is evaluated under different operating conditions. Different residual power levels are thus considered as plotted in Fig. 5.6.

Table 5. 1: Energy resources' parameters

Parameter	P_{DER}^{min}	P_{DER}^{max}	P_{ESS}^{min}	P_{ESS}^{max}	E_{ESS}^{min}	E_{ESS}^{max}	ɳ
Value	96 kW	280 kW	-70 kW	70 kW	35 kWh	87.5 kWh	0.96

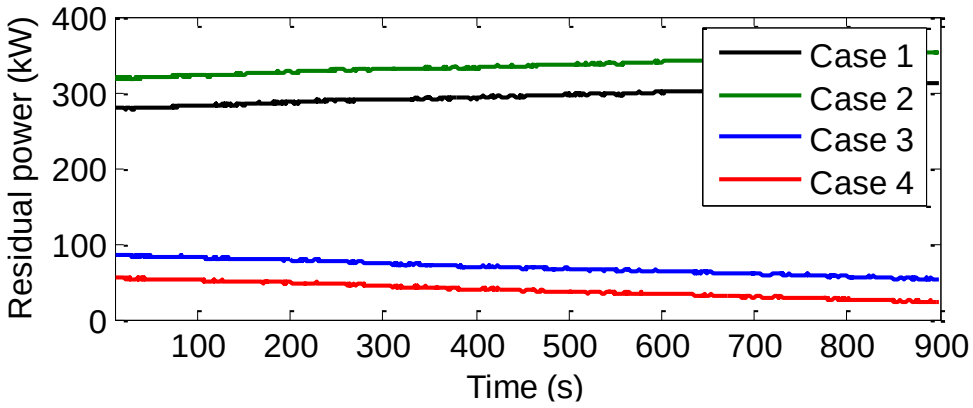

Fig. 5. 6: Residual power for the different test cases

5.5. Real-Time HIL Co-simulation Results

5.5.1. The Case of FDI Cyber-Attacks

The impact of FDI attacks and the effectiveness of the proposed cyber resilient control infrastructure are evaluated under two scenarios: 1) high and increasing residual power causing the attack to violate the EMS requirements as stipulated in (2.23) (Fig. 5.6 – Case 2) low and decreasing residual power causing the violation in (2.22) (Fig. 5.6 – Case 3).

1) Scenario 1 – High loading level – Available active power for FDI attack compensation

An FDI attack with a -30 kW bias is applied to the ESS set-point (Fig. 5.7). If not detected, this attack requires a surge in the power from the diesel generator which has a very slow dynamic response. This would result in large frequency excursions which would have been cleared if the grid-forming DER had enough power headroom to restore balance and regulate the frequency.

As shown in Figs. 5.8 and 5.9, as the diesel generator reaches its maximum limit, very large frequency excursions result (protection schemes are not applied in Fig. 5.8 to show the attack severity). As the proposed cyber resilient control is employed, the combined virtual inertia and droop controller initiates first to provide a fast transient compensation for the slow dynamic response of the diesel generator and a steady-state contribution from droop control (Fig. 5.10). It is important to note that for lower bias values, the combined controller contributions would suffice to restore normal operation. However, a large bias value is selected to test the effectiveness of shifting to a decentralized control mode and evaluate the performance of the proposed multi-stage control infrastructure. Hence, after a certain time delay and as the combined ESS controller reaches its limit, the decentralized control initiates, the diesel generator decreases its frequency reference, and the ESS responds to the bias by increasing its active power to provide additional headroom to the isochronous DER to regulate the frequency and balance power. Unlike the case where no control is applied (Fig. 5.11), the proposed strategy makes use of the DERs capacities without necessitating load shedding.

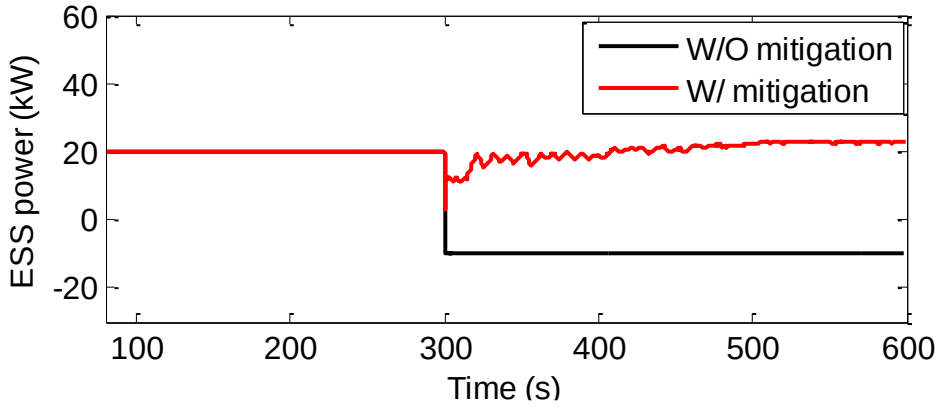

Fig. 5. 7: FDI – S1 - ESS power with & without control

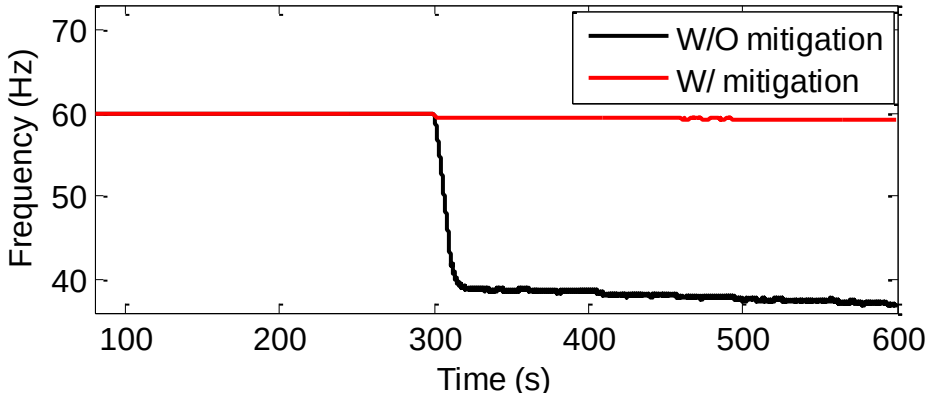

Fig. 5. 8: FDI – S1 – System frequency response with & without control

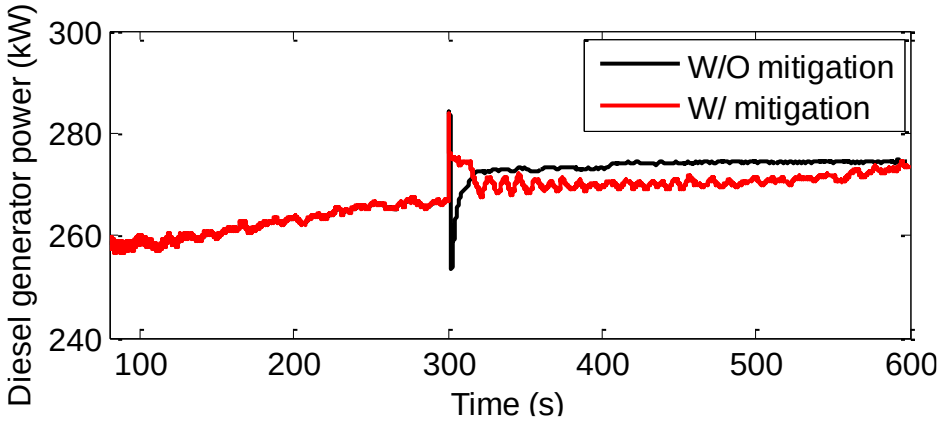

Fig. 5. 9: FDI – S1 - Diesel generator power with & without control

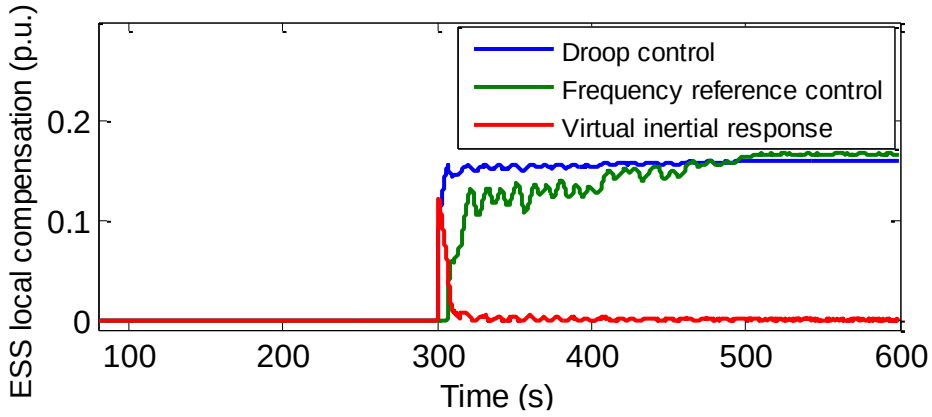

Fig. 5. 10: FDI – S1 - ESS power contribution for cyber-attack compensation

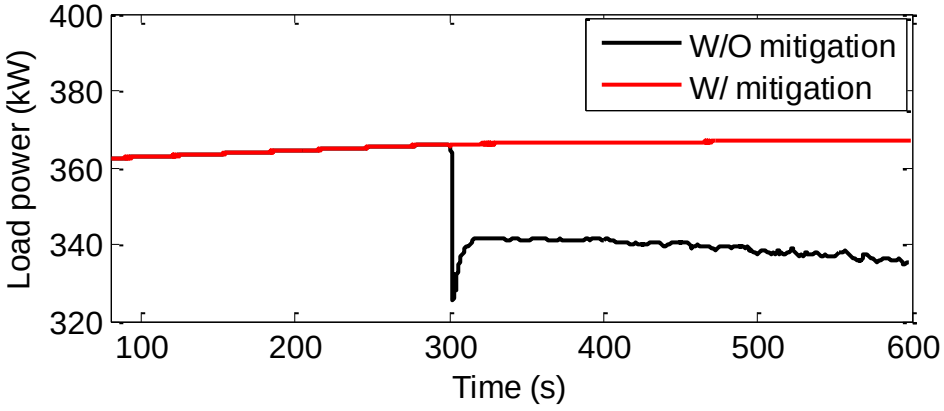

Fig. 5. 11: FDI – S1 - Load power with & without control

2) Scenario 2 - Low loading level – Available active power for FDI attack compensation

An FDI attack with a 40 kW bias is analyzed. The attack severity in the absence of control and protection schemes can be clearly observed in the frequency response which collapses right

after the attack application (Fig. 5.12). Figs. 5.13-5.15 show that as the ESS set-point is modified, large amounts of renewable energy should be curtailed to restore balance. Upon application of the proposed mitigation strategy, the virtual inertia controller provides the active power surge needed to compensate for the transient event and enhance the frequency profile increasing the nadir and requiring no generation disconnection. The frequency reference control would then be activated

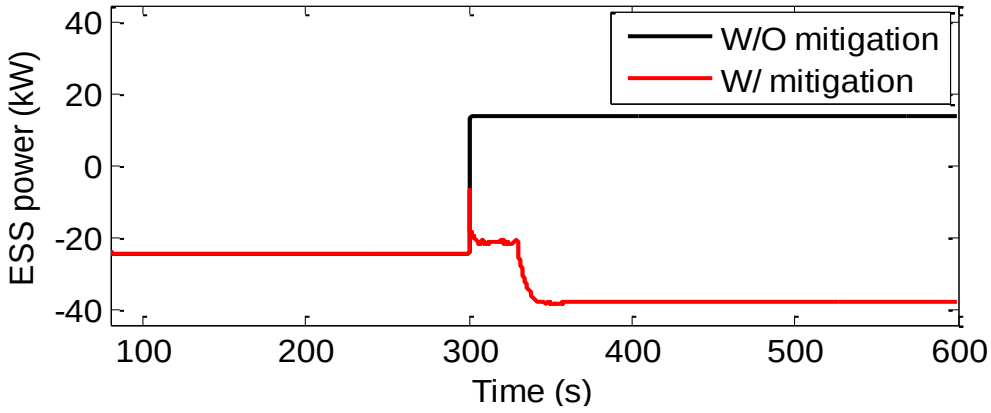

Fig. 5. 12: FDI – S2 - ESS power with & without control

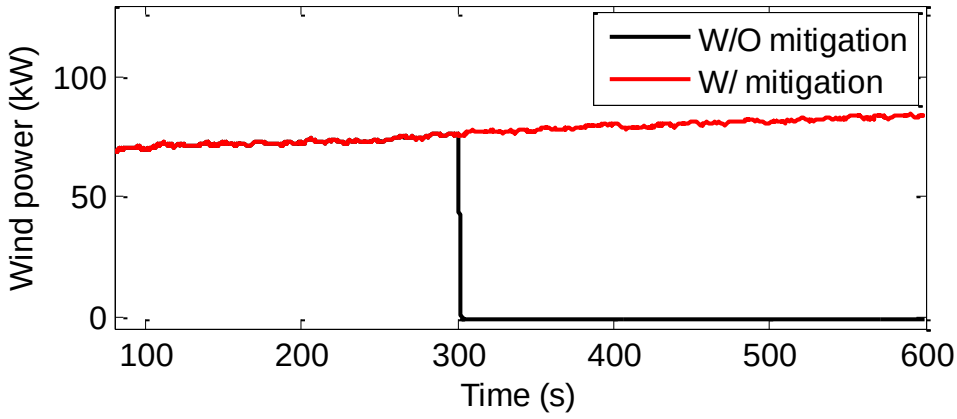

Fig. 5. 13: FDI – S2 -Wind power with & without control

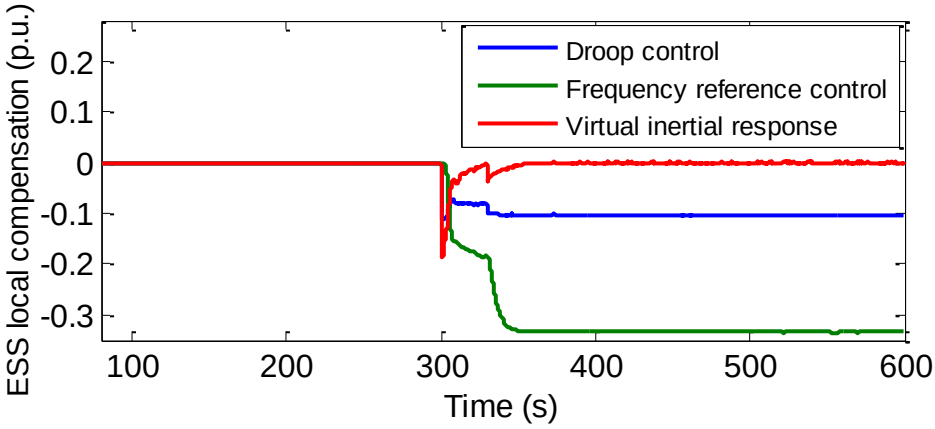

Fig. 5. 14: FDI – S2 -ESS power contribution for cyber-attack compensation

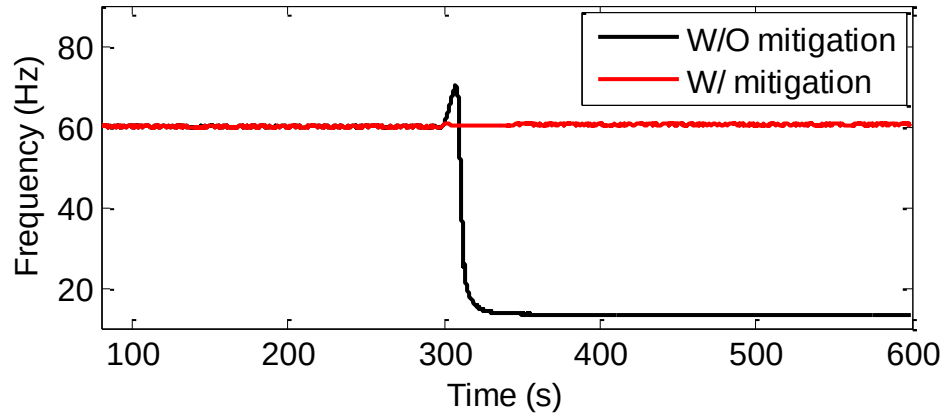

Fig. 5. 15: FDI – S2 – System frequency response with & without control

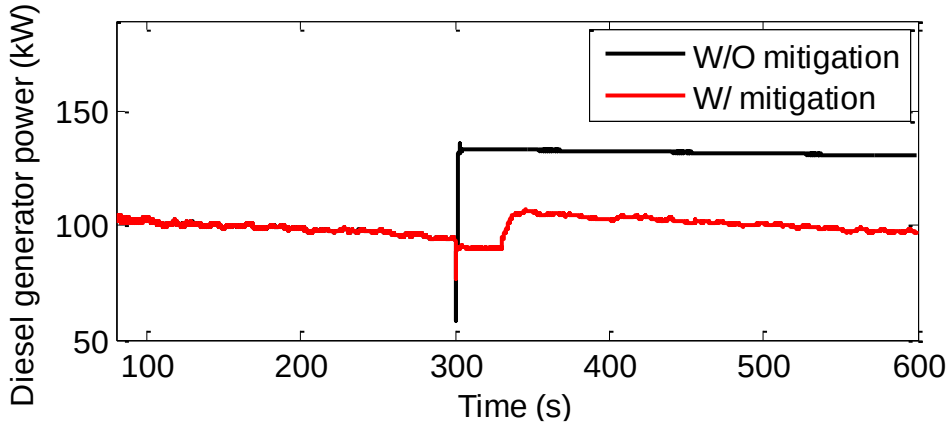

Fig. 5. 16: FDI – S2 -Diesel generator power with & without control

as the combined controller provides its maximum compensation, signaling to the ESS the need to provide less power to allow the grid-forming DER to balance demand and supply and regulate the frequency.

5.5.2. The Case of DDoS Cyber-Attacks

The impact of the DDoS attack and the performance of the cyber resilient control are evaluated in the cases of high and increasing residual power causing the diesel generator to operate at its minimum violating the power management requirement lower bound (2.25) (scenarios 1 and 2) and low and decreasing residual power causing the violations formulated in (2.24) (scenarios 3 and 4).The DDoS cyber-attack is analyzed for two-scenarios: available active power whereby the ESS and the diesel generator have enough capacity to compensate for the attack (scenarios 1 and 3, Fig. 5.6 - Cases 1 and 3) and that of power shortage whereby the resources saturate following the DDoS attack (scenarios 2 and 4 Fig. 5.6 - Cases 2 and 4).

1) Scenario 1 – High residual power level – Available active power for DDoS cyber-attack compensation

Fig. 5.17 shows the IEC 61850 GOOSE message received by the ESS in the post-attack period (black) held at their pre-attack value. As the residual power increases, the isochronous DER generates more power to compensate for the imbalance caused by the DDoS, until it eventually reaches its maximum limit (Fig. 5.18). If the protection schemes are not activated, large frequency excursions result (Fig. 5.19). Restoring the frequency back to its nominal value requires load shedding to provide headroom for the isochronous DER to vary its power to regulate the voltage and frequency (Fig. 5.20).

The system shifts to the decentralized control mode as soon as the attack is detected based on local frequency measures (4.1). Subsequently, the grid-forming DER decreases its frequency reference in accordance with (5.1) to signal the need for more power. The grid-supporting ESS

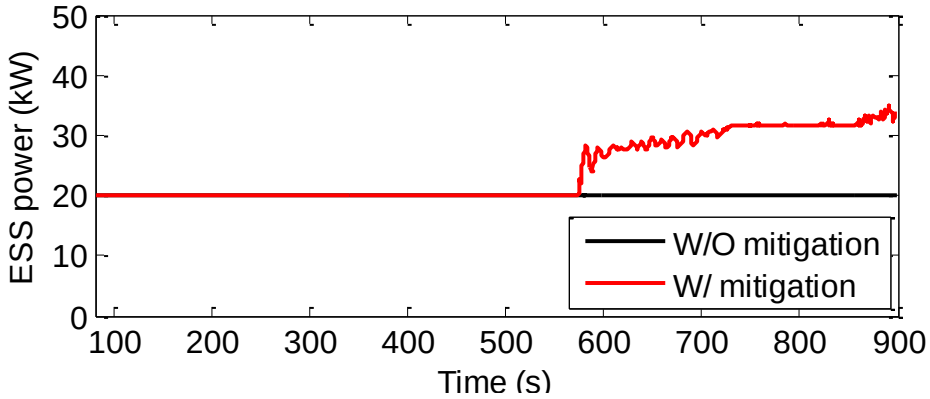

Fig. 5. 17: DDoS - S1- ESS power with & without control

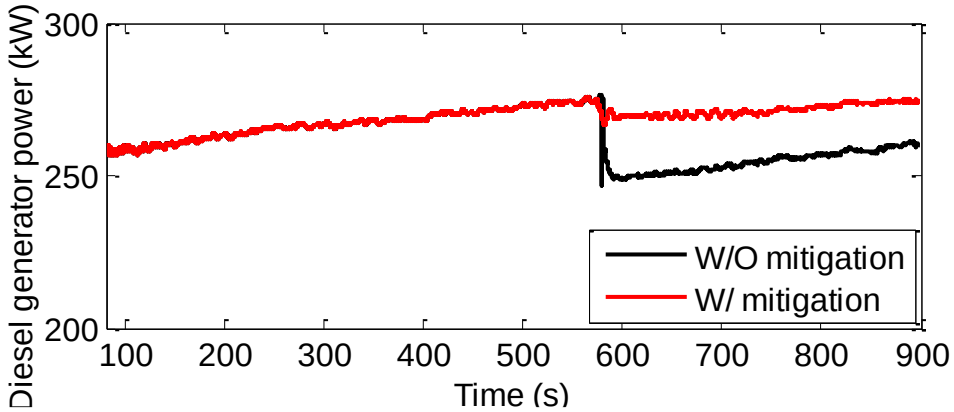

Fig. 5. 18: DDoS - S1- Diesel generator power with & without control

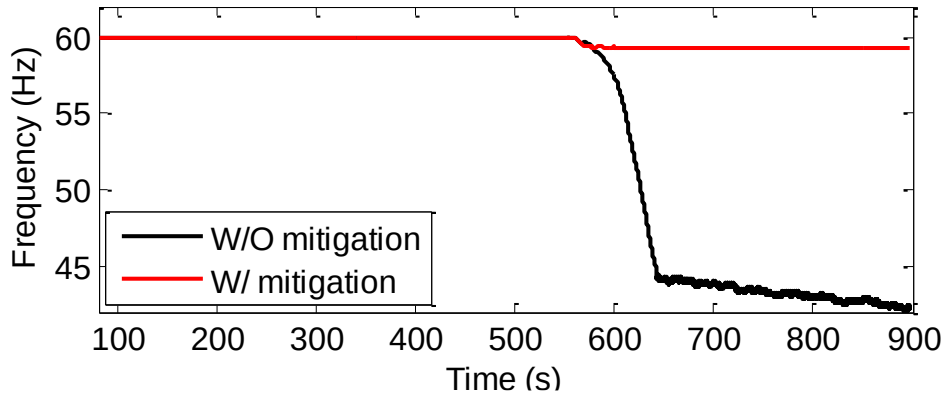

Fig. 5. 19: DDoS - S1- System frequency response with & without control

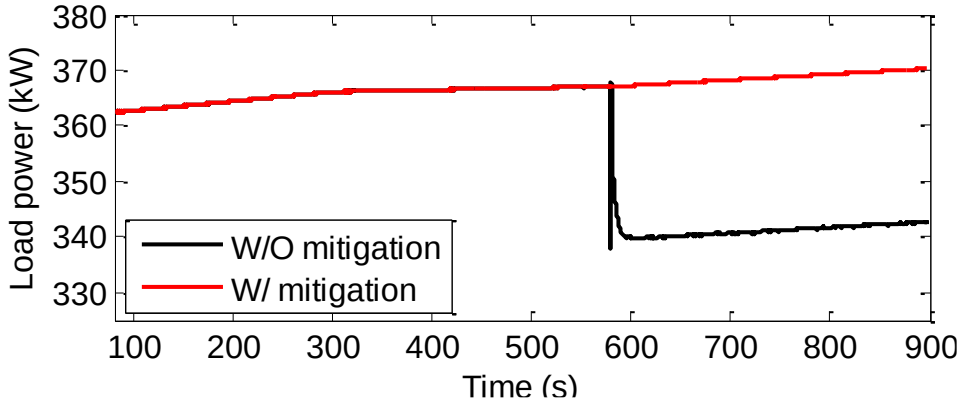

Fig. 5. 20: DDoS - S1- Load power with & without control

supplementary control loop responds to the bias and generates more power to compensate for the imbalance resulting from the ESS and giving more headroom to the diesel generator to regulate the frequency. The coordination amongst the DERs ensures that the frequency does not exceed the limits set by the IEEE 1547 standard causing no activation of protection schemes and increasing the grid capacity to continuously supply the loads

2) Scenario 2 – High residual power level – Shortage of active power for DDoS cyber-attack compensation

In this scenario, the effectiveness of the proposed strategy is evaluated for the case where, even if operated at their maximum, the ESS and diesel generator do not have enough capacity to supply all the loads necessitating load curtailment. As the conventional local control loops are not inherently designed to provide resiliency and compensate for the attack, large frequency excursions would result (Fig. 5.21) in the absence of cyber resilient control, initiating load shedding at an early stage (Fig. 5.22). As the DDoS is detected, the decentralized control is

activated and the diesel generator starts decreasing its frequency reference signaling the ESS to generate more power (Fig. 5.23). In that case, the residual power keeps on increasing and as the grid-forming DER and the ESS reach their maximum power limits (Fig. 5.24), the supplementary control loops for load control would be activated limiting the load curtailment to just the necessary amount needed to regulate the frequency. In fact, the mitigation strategy makes use of all the available DERs power capacities before resorting to energy curtailment.

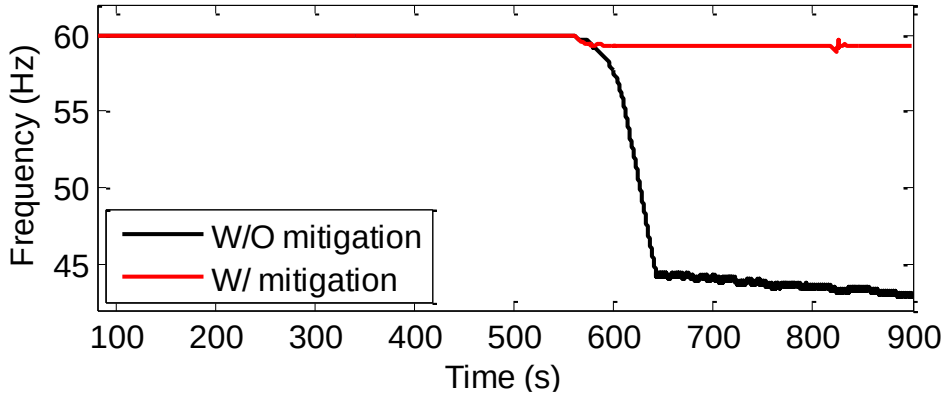

Fig. 5. 21: DDoS – S2- System frequency response with & without control

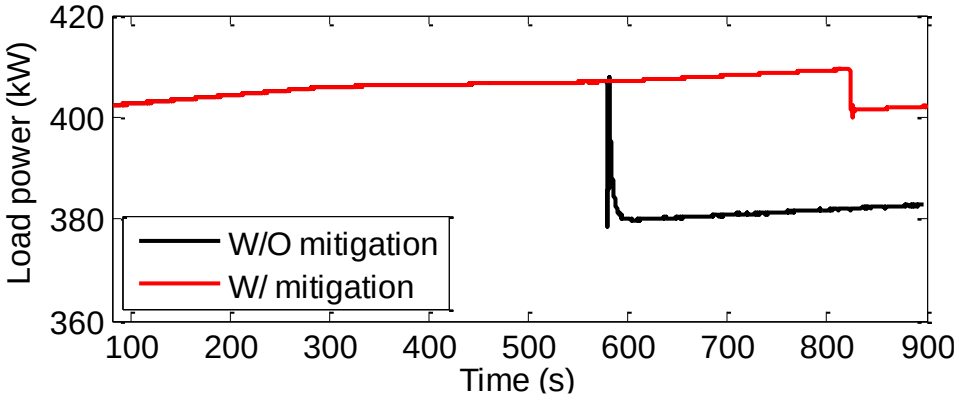

Fig. 5. 22: DDoS – S2- Load power with & without control

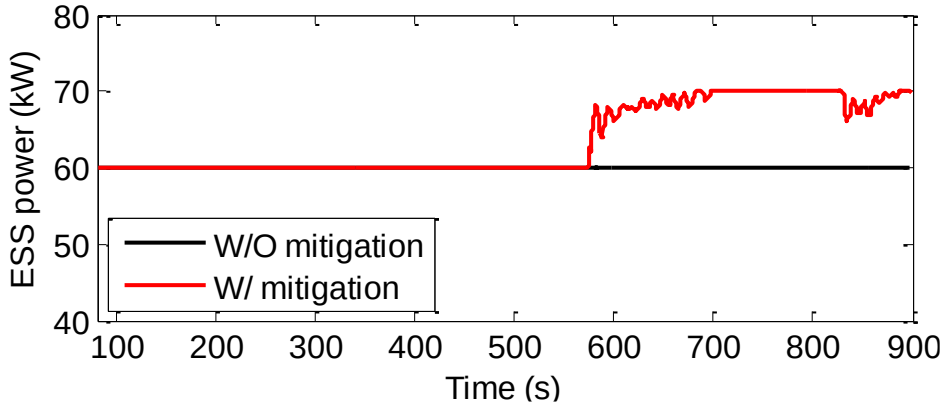

Fig. 5. 23: DDoS – S2- ESS power with & without control

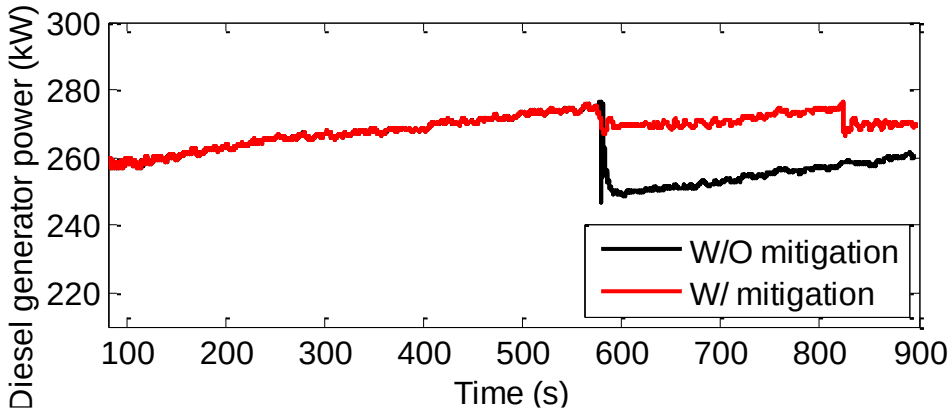

Fig. 5. 24: DDoS – S2- Diesel generator power with & without control

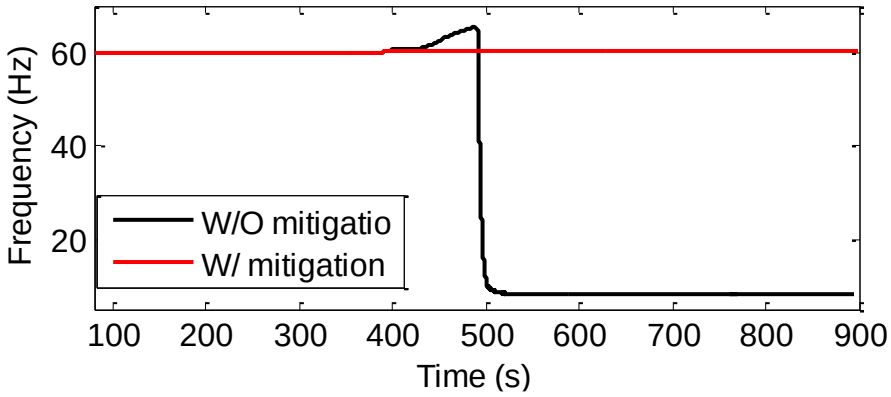

Fig. 5. 25: DDoS – S3- System frequency response with & without control

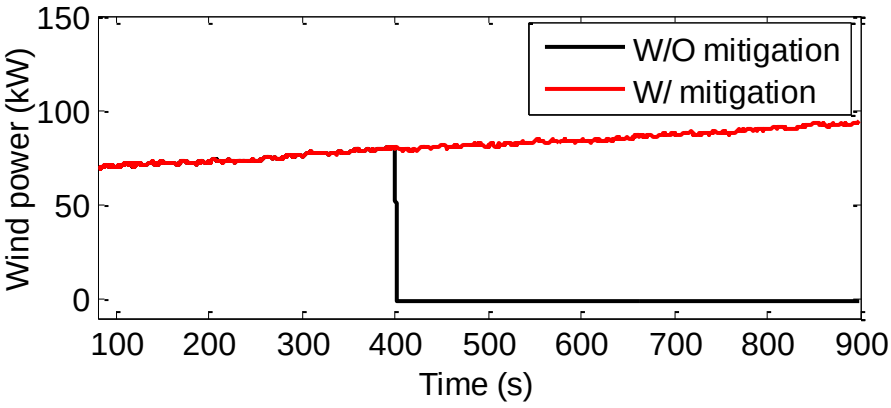

Fig. 5. 26: DDoS – S3- Wind power with & without control

3) Scenario 3 – Low residual power level – Available active power for DDoS cyber-attack compensation

In the event of low loading levels, the frequency collapses in the absence of resilient control (Fig. 5.25), causing the disconnection of the WTG to provide headroom for the isochronous DER to regulate the frequency (Fig. 5.26). As the system shifts to decentralized control, the diesel

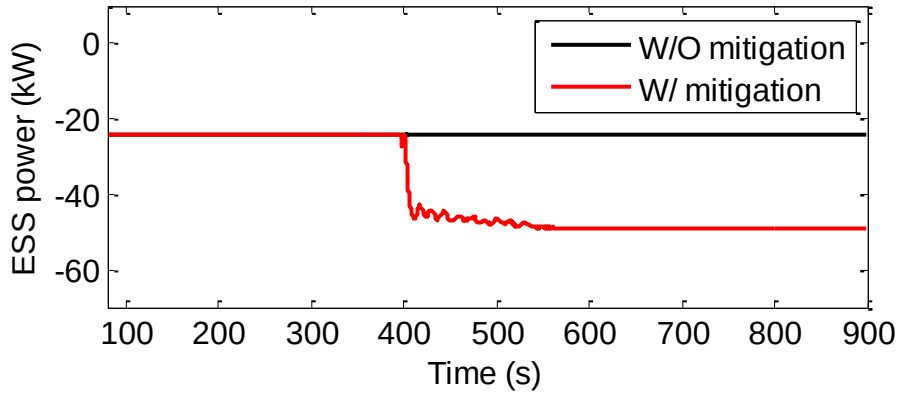

Fig. 5. 27: DDoS – S3- ESS power with & without control

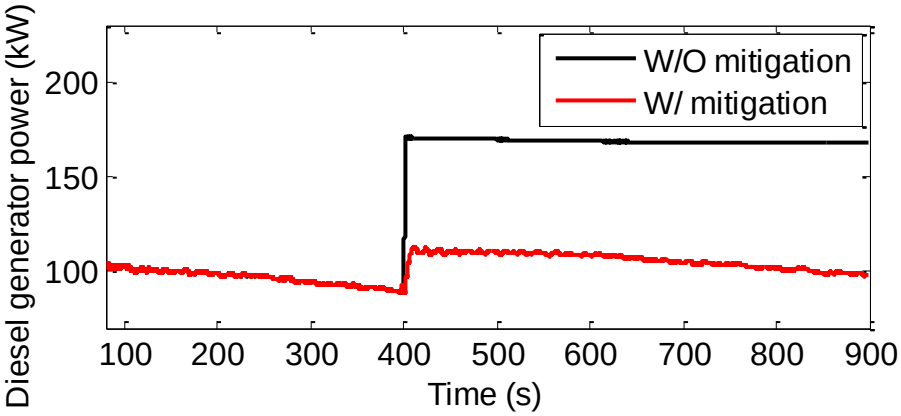

Fig. 5. 28: DDoS – S3- Diesel generator power with & without control

generator augments its frequency reference to signal the excess of power in the system. The ESS responds to the bias and decreases its active power (Fig. 5.27) allowing the diesel generator to shift to the desired active power region (Fig. 5.28) whereby it could regulate the frequency necessitating no wind energy curtailment.

4) Scenario 4 – Low residual power level – Shortage of active power for DDoS cyber-attack compensation

The performance of the supplementary control loop added to the WTG to reduce its active power without causing complete disconnection of the DER and high amounts of inexpensive energy not harvested is evaluated. If conventional protection schemes are applied and the isochronous resource reaches its minimum capacity in the post-attack period, large frequency excursions causing the disconnection of the WTG occur (Figs. 5.29 and 5.30). If the proposed decentralized control strategy is applied, the ESS responds to the isochronous DER frequency change and compensates for the attack (Fig. 5.31). As the residual power further decreases, the

DERs would eventually reach their minimum power capacities and would no longer be able to provide compensation (Fig. 5.32). The supplementary control added to the WTG will in that case initiate and reduce the DER power to maintain the frequency between the allowable bounds. The proposed cyber resilient control only sheds an amount equal to the system's imbalance maximizing the microgrid capacity to host renewable generation.

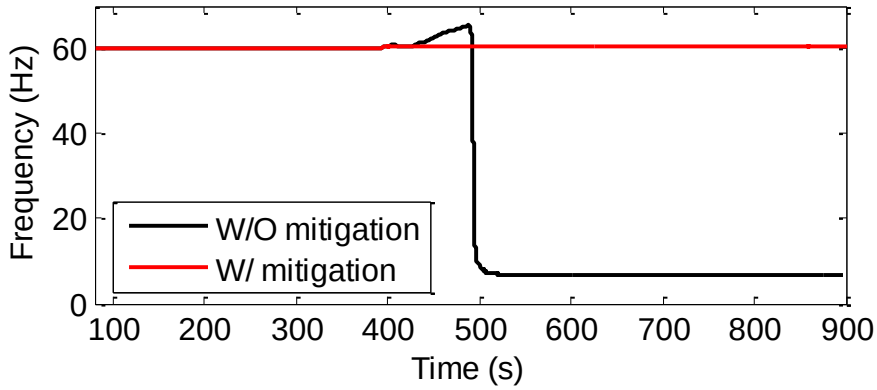

Fig. 5. 29: DDoS – S4- System frequency response with & without control

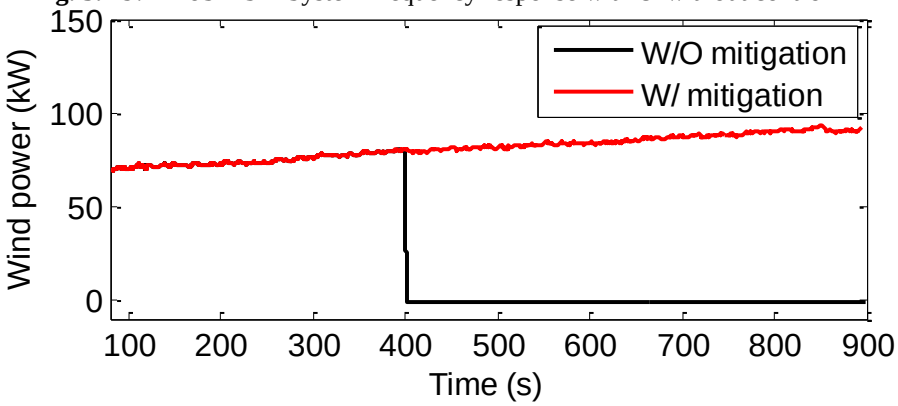

Fig. 5. 30: DDoS – S4- Wind power with & without control

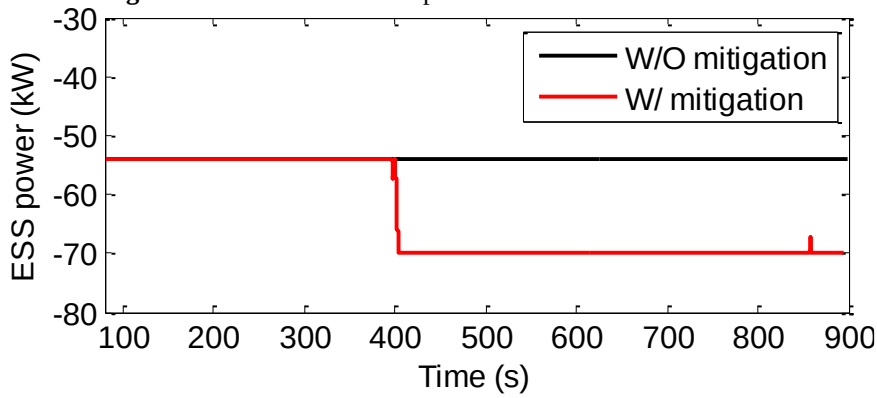

Fig. 5. 31: DDoS – S4- ESS power with & without control

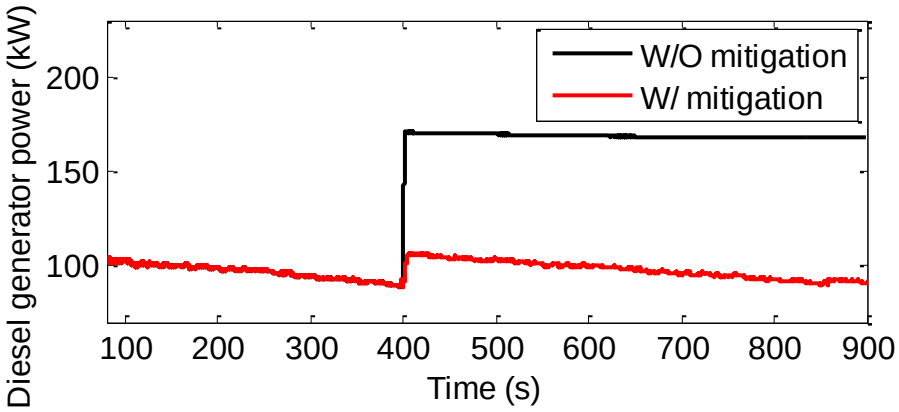

Fig. 5. 32: DDoS – S4- Diesel generator power with & without control

Table 5. 2: Performance indices for impact assessment and resiliency quantification

		Min/Max Frequency (Hz)	Renewable Energy Shed (kWh)	Load Not Served (kWh)	Average Cost of Energy ($/kWh)
FDI	S1 – No Control	36.8 / 60	0	13.6	0.2645
	S1 - Control	59.3 / 60	0	0	0.2483
	S2 – No Control	13.4 / 70.4	40.4	0	0.3315
	S2 - Control	59.9 / 60.5	0	0	0.3195
DDoS	S1 - No Control	42.1 / 60	0	9.1742	0.2505
	S1 - Control	59.3 / 60	0	0	0.2481
	S2 - No Control	42.8 / 60	0	9.16	0.2133
	S2 - Control	58.9 / 60	0	0.71	0.2122
	S3 - No Control	8.2 / 65.6	47.95	0	0.3962
	S3 - Control	59.9 / 60.5	0	0	0.3335
	S4 - No Control	6.7 / 65.6	48.06	0	0.5379
	S4 - Control	59.8 / 60.7	0.56	0	0.4414

5.5.3. Discussion and Recommendations for Cyber Resiliency

The performance indices defined in chapter 2 are evaluated in Table 5.2 for the 6 cases to quantify the impact of FDI and DDoS attack and to evaluate the effectiveness of the proposed

multi-stage cyber resilient control infrastructure in providing reliable operation in the presence of cyber-attacks. It could be concluded, that in the cases of available active power, the conventional control loops cause large amounts of load or wind energy to be curtailed. The combined virtual inertia and droop control added to the grid-supporting DERs provides fast transient and steady-state compensation reducing the minimum and maximum frequency to acceptable values as FDI attacks are launched. As for the decentralized control strategy, it proved to be effective in the event of DDoS and FDI attacks as it distributes the EMS functions among the DERs and features coordination to compensate for the attacks requiring no energy curtailment. In the case of shortage of active power, the decentralized controller makes use of all the DERs capabilities before resorting to energy curtailment. As such the proposed control only sheds the necessary amount to restore balance in the system (only 0.17% of load in scenario 2 and 0.69% of the wind in scenario 4 as compared to 2.26% and 59.85% when no control is applied). Although not designed to ensure economic operation, the cyber resilient control infrastructure operates the DERs so as to respect all the EMS constraints and maximize the microgrid capacity to host inexpensive renewable energy and to supply loads, becoming considerably more economical than the case where no control is applied.

Before concluding this thesis in the upcoming chapter, it is mandatory to present the main recommendations drawn from the research work performed. These recommendations mainly include the following:

1- Raising awareness on the importance of cyber security and the risk associated with successful cyber intrusions

   Utilities tend to disregard the importance of cyber security until cyber-attackers successfully gain control over their systems causing severe damages. In order to change the generalized perception that cyber security is not a first interest matter, the impact of cyber intrusions should be highlighted and a platform for knowledge sharing among grids' stakeholders should be created. This would promote the development of advanced cyber security initiatives.

2- Impact quantification by means of specific performance indices

   Performance indices need to be defined in order to quantify the level of cyber security, resilience and robustness. These measures allow the assessment of the attacks' impact fostering awareness raising and enabling the proposition of mitigation strategies. In addition, they facilitate the measurement of the maturity level of the mitigation solutions put in place

on both the power system, communication network and information exchange layers and the selection of the most effective strategy to be employed.

3- The need for a robust and resilient grid – Cyber security by design

The cyber-attacks' impact assessment studies performed in this thesis proved that attacks could engender severe damages which jeopardize the operation of the grid, in terms of stability, reliability and efficiency, and result in large monetary losses. In addition, the ever-increasing complexity of industrial systems and ICTs will pave the way in the near-future to more sophisticated and frequent cyber-attacks. There exist numerous methods, previously reviewed, that could be applied to prevent cyber-attackers from penetrating the microgrid communication network and launching attacks. However, various cyber-attacks were still successfully perpetrated against industrial control systems and power grids although these prevention means were put in place. Typically, only after being targeted by cyber-attacks, that grid operators tend to implement additional security measures which come at a very high cost. To limit the damage that could be engendered by cyber intrusions, the grid control and communication infrastructures must be designed to embed cyber security in order not only to prevent but also to be able to react and recover from cyber-attacks.

4- The need for a standardized end-to-end cyber security strategy

The grids' power system and communication network layers are becoming more interdependent and networks are becoming more interconnected increasing the grids' exposure and vulnerability to cyber intrusions. Therefore, it becomes necessary to develop and implement a standardized end-to-end cyber security strategy at all levels of the communication, information exchange, and power system and control layers.

5- Trade-off between cost and benefits

Typically, cyber security is not embedded into the grids' design due to the high cost associated with the implementation of the necessary infrastructure. In order to better understand the trade-off between cost and resiliency, the monetary losses engendered by cyber-attacks along with the impacts derived should be quantified and compared to the cost resulting from embedding cyber security into the grid's design.

5.6. Conclusion

The concepts, theories and simulation results presented in this chapter complements the research work performed in chapters 2, 3 and 4 to provide an in-depth analysis of islanded microgrid systems compromised by FDI and or DDoS cyber-attacks. A multi-stage cyber resilient control infrastructure that distributes the EMS functions amongst the DERs and loads by adding enhanced supplementary loops to their primary controllers is proposed to ensure that microgrids could resist cyber-attacks and operate reliably without relying on vulnerable communications. Local frequency measures are used to initiate the control stages: 1) combined virtual inertia and droop control operate to provide transient and steady-state stability in the event of cyber-induced transient events, 2) decentralized control which allows coordination between the isochronous and grid-supporting DERs initiate as the combined controller provides its maximum compensation, 3) as grid-forming and grid-supporting DERs reach their limits and as a last resort, loads and renewable DERs supplementary controllers are initiated only shedding the amount of energy which restores normal operation. A real-time HIL co-simulation platform was used to implement the attacks, quantify their impacts and validate the proposed cyber resilient control strategy. A parametric analysis was conducted in order to evaluate the performance of the proposed infrastructure under different operating scenarios. The strategy ensured transient and steady-state frequency stability, promoted coordination between the DERs and loads operating in a decentralized manner to manage power and energy, maximized the microgrid capacity to host renewable generation and supply critical loads, and reduced the average cost of energy enhancing the grid resilience and robustness in the event of cyber-attacks. The chapter concludes with the cyber security recommendations that could be drawn from the proposed research work. Also detailed, were the best practices that should be applied in order to highlight the importance of cyber security, the impact that cyber-attacks could engender and the need to implement, at the design phase, measures for enhanced resilience, robustness and reliability of the grid in the event of cyber intrusions. The upcoming chapter concludes the thesis, restates the main contributions and presents recommendations for future research work in the area of microgrid cyber security.

Chapter 6

Summary and Conclusions

6.1. Thesis Summary

The rapid development of microgrids streams from the value they bring in terms of resilience, high integration of renewable DERs, and the ability to operate in both grid-connected and islanded modes. In order to benefit from these advanced capabilities, microgrids require real-time and reliable two-way flow of information. As the microgrid moves toward modernization, the development of a communication infrastructure becomes mandatory. The reliance on ICTs to provide advanced microgrid capabilities including remote monitoring, maintenance and advanced control enhances the microgrid operation, however, creates potential vulnerabilities and access points which can be maliciously exploited by cyber-attackers. Large efforts are made to protect power assets against potential cyber-attacks through conformity to security guidelines and regulations and application of defense mechanisms and mitigation strategies at the communication network layer. The conformity to security regulations and most of the currently implemented defense strategies cannot ensure a comprehensive protection for power grids, as seen following the success of the Ukraine attack. If not designed with cyber security in mind, just like any smart grid, microgrids which are considered as a potential solution to maximize the hosting capacity of renewable generation and continuously supply critical loads could be compromised, defeating the main purpose for which they were initially developed. Very little effort has been put to evaluate

the impact of cyber-attacks and propose mitigation methods applied at the control layer to ensure resilient operation of the microgrids in the event of cyber intrusions.

This thesis provides a cyber security analysis for microgrids targeted by cyber-attacks. Different cyber-attacks compromising the microgrid data integrity and availability have been modeled and benchmark test systems along with advanced real-time simulation testing platforms have been developed to perform impact assessment studies and propose and validate novel mitigation strategies applied at the microgrid control layer.

Chapter 2

Before analyzing the impact that cyber-attacks have on the microgrid operation and proposing mitigation strategies to ensure resilient operation, the power system, information exchange and communication network layers constituting a microgrid system need to be modeled and interfaced. Hardware and software were used to model the DERs and loads along with their underlying power and energy management strategies and a communication network allowing the exchange of information based on legacy and modern communication protocols. The microgrid constituting layers were interfaced in real-time to form a single entity allowing the analysis of microgrid cyber security. Mathematical models of the cyber-attacks of interest were provided and bounds ensuring that the attacks' parameters violate the microgrid control requirements were set. Performance indices allowing quantification of the attacks' impacts and testing of the proposed control strategies in mitigating these impacts were also defined. The assumptions made in the thesis regarding cyber-attack prevention and detection were stated, and the steps that need to be followed to ensure enhanced microgrid resiliency and survivability in the event of detected and undetected cyber-attack were presented.

Chapter 3

FDI cyber-attacks which tamper with the EMS dispatch set-points and the commands sent to control the DERs circuit breakers were analyzed. Control loops added at the DERs primary control level comprising virtual inertia and droop control were tested and adaptive load managements schemes were proposed to enhance the microgrid survivability in the event of undetected FDI cyber-attacks. Performance indices were evaluated to quantify the impact of FDI cyber-attacks on the operation of SM based and 100% inverter-interfaced microgrids. These indices facilitated the

evaluation of the effectiveness of the control loops in enhancing the resiliency of the microgrid when subject to FDI attacks.

Chapter 4

Cyber-attacks compromising the microgrid availability, namely DDoS cyber-attacks causing loss of information exchange in the microgrid, were analyzed. A rule-based fallback control strategy was proposed to mitigate DDoS attacks such that it distributes the power and energy management functions of the microgrid controller among the DERs. Supplementary control loops were added to the dispatchable DERs primary controllers to coordinate based on local signals with the grid-forming DER which is designed to vary its voltage or frequency reference to request compensation from the dispatchable DERs. Performance indices were defined and calculated to assess the impact of the DDoS attack and to evaluate the effectiveness of the proposed mitigation strategy in enhancing the resiliency of SM based and 100% inverter interfaced microgrids.

Chapter 5

A multi-stage cyber resilient control infrastructure combining and extending the strategies proposed in the previous chapters was developed. The proposed strategy enhances the microgrid control infrastructure to ensure that cyber security is embedded into the microgrid's design. The strategy operates at three different stages which are activated based on the attack detection mechanism and the local frequency measures requiring no reliance on vulnerable communication links. Enhanced control loops are added to the dispatchable DERs local controller to provide fast transient and permanent steady-state frequency stability. At a second stage, and as the attack's severity increases the system shifts to a decentralized control mode whereby grid-supporting and grid-forming DERs coordinate to manage the power and energy. The third control stage would initiate as a last resort to shed the necessary amount of load and renewable energy as grid-forming and grid-supporting DERs have provided maximum compensation. The proposed control infrastructure has been validated on the real-time HIL co-simulation setup in the event of FDI and DDoS cyber-attacks under different operating conditions. The strategy showed to increase the microgrid ability to host inexpensive renewable energy and supply critical loads, and to regulate the frequency, manage power and energy and operate economically in the presence of cyber intrusions. The set of recommendations and best practices to be applied for enhanced cyber security were finally presented.

6.2. Conclusions

The work performed in this thesis becomes more and more pertinent as microgrid systems evolve to integrate more renewable generation, operate autonomously, and provide smart monitoring and control capabilities facilitated by the deployment of communication networks vulnerable to cyber intrusions. As the tools employed to conduct cyber-attacks are constantly evolving and the attackers' capabilities are outpacing the prevention means and defense strategies implemented at the communication network layer to protect the power industry from cyber-attacks, strengthening the grid's control infrastructure to resist and operate reliably in the event of cyber disturbances becomes mandatory. This thesis tackles this problem as it provides a detailed analysis of cyber-attacks jeopardizing the microgrid critical functions and proposes novel cyber resilient mitigation strategies reinforcing the microgrid control layer to resist cyber intrusions.

In order to provide a complete analysis of microgrid cyber security, the thesis starts by providing a detailed modeling of the microgrid underlying layers. Hardware and software were interfaced to model the power system, information exchange based on different protocols and communication network layers of microgrid systems using techniques that allow overcoming the downfalls of other platforms found in the literature. The focus has been directed to FDI and DDoS cyber-attacks as their application engenders severe physical impacts on the microgrid control operation. Mathematical models of the cyber-attacks have been presented and the cyber-attacks' parameters selection criteria that need to be met to cause an infringement of the power and energy management functions of the microgrid were also rigorously defined. Microgrid specific performance indices have been defined to allow quantification of the attacks' impacts on the microgrid operation and evaluation of the performance of proposed control strategies in mitigating these impacts.

The co-simulation results showed that it suffices to tamper with one of the EMS commands sent to operate the DERs to cause large power imbalances, voltage and frequency excursions, unnecessary load curtailment and even microgrid blackout. The impact assessment studies performed facilitated the development of advanced control strategies, based on widely applicable control concepts (virtual inertial response and droop control), added to the SM based microgrid DERs primary control to provide transient and steady-state cyber-attack compensation. The proposed mitigation strategy was then modified and adapted to 100% inverter-interfaced

microgrids and a two-layer cyber resilient control was formulated to ensure cyber-attack compensation and post-attack power and energy management. The parametric studies conducted to test and evaluate the performance of the proposed strategies showed that the supplementary control loops and the adaptive load management algorithm were able to provide steady-state and transient voltage and frequency regulation by smoothing the ramps streaming from the cyber-attack, and to overcome the DERs rated capacity limits and ensuring rapid post-attack recovery, respectively.

The thesis work also showed that it suffices to gain unauthorized access to the microgrid LAN to launch a DDoS cyber-attack on the microgrid communication network causing a prevalent damage to the microgrid control operation. In fact, the impact assessment studies performed showed that the DDoS cyber-attack causes large voltage and frequency excursions, and violation of the power and energy limits which could only be remediated by generation and load curtailment, defeating the main purpose for which islanded microgrids were initially developed. A novel rule-based fallback control mitigation strategy was formulated to distribute the power and energy management functions amongst the DERs. Supplementary control loops were developed to provide means of coordination amongst the DERs without reliance on vulnerable communication mediums. The proposed fallback control algorithm was adapted to operate in both SM and 100% inverter-interfaced microgrid configurations. Performance indices quantification showed that the proposed rule-based algorithm maximises the capacity of the microgrid to host renewable generation and to continuously supply critical loads, promotes coordination between DERs for power and energy management and reduces the average cost of energy enhancing the microgrid resiliency, robustness and ability to resist cyber-attacks.

The mitigation solutions proposed were combined and extended to form a multi-stage cyber resilient control infrastructure for islanded microgrid systems. The proposed infrastructure ensures resiliency in the event of FDI and DDoS cyber-attacks and was validated for different attacks severity levels, and under diverse operating conditions (generation mix, renewable energy penetration levels, loading levels). Recommendations for enhanced cyber security, increased awareness regarding cyber-attacks and the severe impact they engender were concluded. The need to consider cyber security at the microgrid design stage and the trade-offs resulting from the implementation of cyber resilient strategies were also explained.

6.3. Recommendations for Future Work

The thesis has made a contribution in terms of assessing the impact of different cyber-attacks that have recently interested threat agents aspiring to inflict damage to the electric infrastructure and of proposing advanced mitigation methods enhancing the grid's control infrastructure to provide cyber resiliency. Although many aspects of microgrid cyber security were addressed in this thesis, many opportunities for extending the scope of this study remain and they include:

1- The mitigation strategies proposed in this thesis are applied at the microgrid control infrastructure to provide a resilient microgrid power system layer that could resist and operate in the presence of detected and undetected cyber-attacks. Other research could be directed towards proposing strategies that could be applied at the microgrid communication network layer to detect, prevent and mitigate intrusions. The real-time HIL co-simulation testbed developed could be used to evaluate the effectiveness of these strategies.

2- The co-simulation setup implemented in chapter 2 models the microgrid feeder and DERs on one real-time digital simulator. This assumption is valid for the studies analyzing the impact of cyber-attacks compromising the microgrid secondary centralized EMS operation; however, it no longer applies as information need to be exchanged between DERs on a primary level. While the proposed platform provides a wide flexibility in terms of the different power system and communication elements that could be employed and the various control strategies that could be tested, hierarchical and multi-agent based control will necessitate a more rigorous setup. Decoupling the system and running every agent requiring information exchange on a separate core of the real-time simulator, would facilitate the analysis of cyber-attacks targeting multi-agent based systems requiring peer-to-peer communication.

3- As this research analyzes the cyber security of islanded microgrids, a new research avenue would be to evaluate the impact of cyber-attacks resulting in unplanned islanding or reconnection of the microgrids to the large EPS. Strategies allowing detection and mitigation of the unplanned events could be proposed to reduce the damage they could cause to the microgrid and the EPS.

Appendix A

Simulation Tools

This appendix describes the simulation tools used throughout this thesis.

A.1 MATLAB

MATLAB m-files were used to formulate the EMS optimization script defined in chapter 2 and employed throughout this thesis and to generate plots. The Simulink toolbox was used for the modeling of the remaining microgrid building blocks, inputs and outputs. The SimPowerSystems library of Simulink was used to implement the DERs and load models along with their underlying primary power management control strategies. As for the information exchanged, whether analog inputs/outputs or IEC 61850 GOOSE messages, they were modeled using the RT-LAB libraries which include among others: Artemis, RT-EVENTS, RT-LAB and RT-LAB I/Os libraries.

A.2 Riverbed Modeler

The microgrid communication network is modeled using the Riverbed Modeler, also known as OPNET, a network emulator which allows modeling and detailed analysis of a broad range of wired and wireless networks. OPNET offers a SITL module which acts as an interface for connecting hardware applications to a discrete event simulation of a communication network modeled in OPNET. The Riverbed Modeler licenses used and installed on the host computer modeling the communication network include: OPNET Modeler, Simulation Runtime, Terrain

Modeling and System-in-the-Loop licenses.

A.3 RT-LAB

RT-LAB is a real-time simulation platform for high-fidelity plant simulation, control system prototyping, and embedded data acquisition and control. RT-LAB has a distributed processing capability which allows conversion of Simulink models to high-speed, real-time simulations, over one or more target computer processors. RT-LAB was used to integrate the Simulink models implementing the microgrid building blocks in real-time simulations and facilitate HIL testing.

A.4 ICD Designer

The IED Capability Description (ICD) Designer tool is used to define, edit and update substation configuration descriptions for the IEC 61850 standard compliant IEDs through a graphical user interface to create an XML formatted file. ICD Designer was used in this thesis to model the information exchanged based on the IEC 61850 GOOSE messaging protocol and define the substation configuration language (SCL) file to configure the communication, access points, logical devices, logical nodes, data sets and control blocks amongst others.

A.5 LabView

LabView is a development environment designed with a graphical programming syntax and an open architecture that enables integration of any hardware device and any software approach. LabView was used in this thesis to program the NI-cRIO digital controller and provide an interface for its operation and to connect with the EMS script running in MATLAB.

A.6 Ettercap

Ettercap is an open source tool for networks cyber security known for its ability to perform MITM, DoS/DDoS cyber-attacks on LANs. Ettercap has the ability to intercept the traffic on a network segment, capture passwords and eavesdrop on a number of communication protocols. Ettercap was used in this thesis to model the cyber-attacks.

A.7 Wireshark

Wireshark is an open source network traffic analyzer. Wireshark was used in chapter 5 of this thesis to troubleshoot and analyze the performance of the communication network emulator and of Ettercap. The packet analyzer was running on all the computers used in the co-simulation setup to ensure that hardware and software are properly interfaced and to analyze the information exchanged throughout the system.

Appendix B

DERs and Load Modeling

B.1 Load Model

Two load models are implemented and employed in this thesis: base loads and controllable loads. The base loads consist of constant impedance models while the controllable loads are modeled as a controllable constant impedance current source whose active and reactive powers can be varied in accordance with the load management schemes.

B.2 Inverter-Interfaced Renewable DER Model

Wind and solar renewable DERs are employed in this thesis. The grid-tie inverter configuration shown in Fig. B.1 is used to model these renewable DERs. The inverter is tied to the grid through an RL choke and a transformer. Its DC-link is fed from a controllable current source emulating the MPPT curves.

B.3 ESS Model

The ESS model also consists of a grid-tie inverter connected to the grid through an RL choke and a transformer as shown in Fig. B.2. The inverter's DC-link is fed from a lithium-ion battery which

model is taken from the SimPowerSystems Simulink library. The battery parameters were modified and set in accordance to specified values.

B.4 Synchronous Generator Model

The rotating machine based generator consists of an SM fed from a diesel generator connected to the grid through a transformer. The dynamics of the diesel generator are illustrated in Fig. B.3. The mechanical power P_m is dispatched in accordance to power and speed references as per the applied power management strategies. The synchronous generator system is also equipped with a

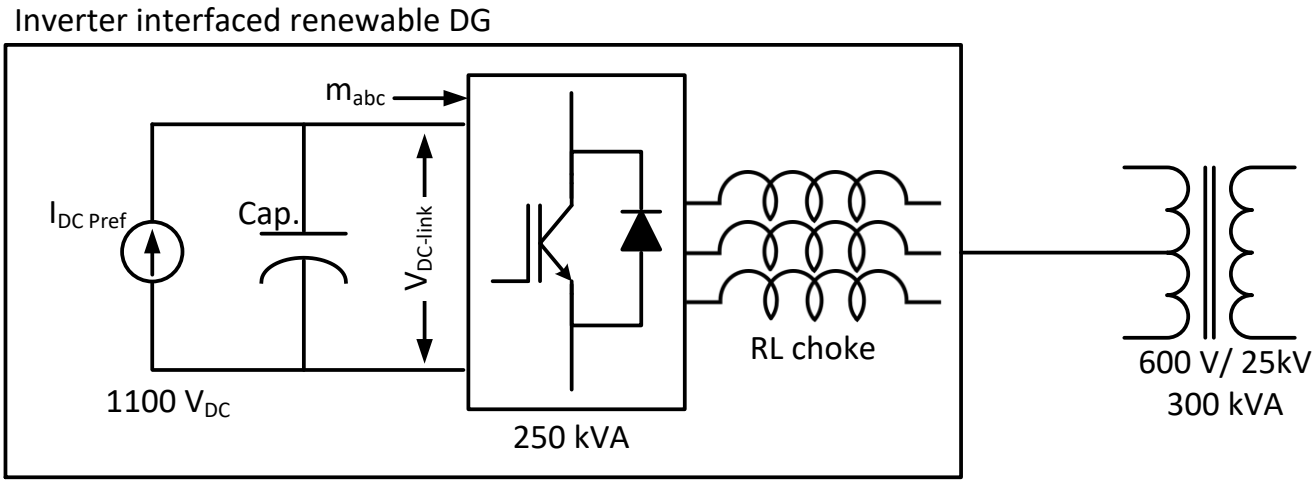

Fig. B. 1: Grid-tie inverter configuration used for inverter interfaced renewable DGs

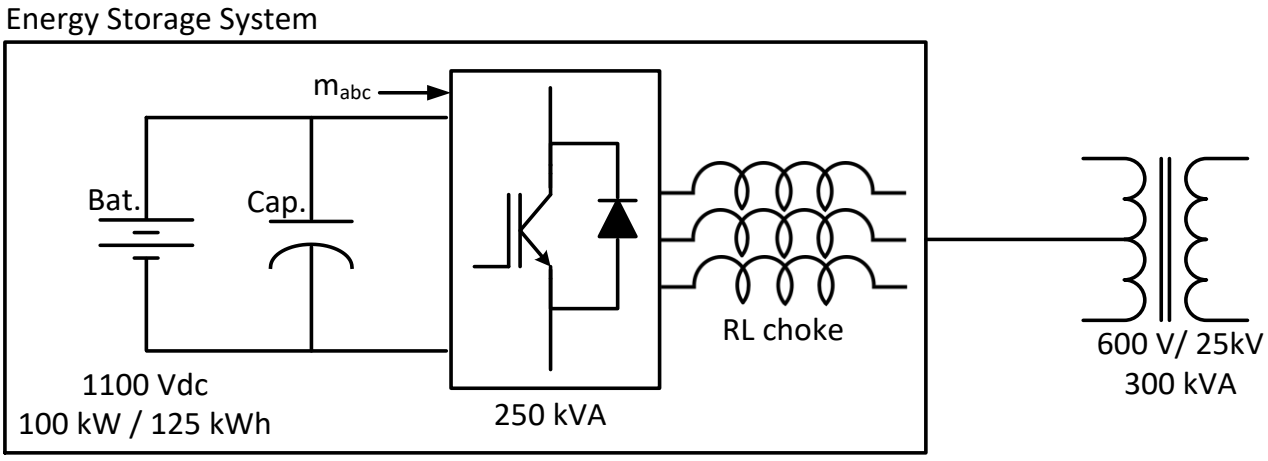

Fig. B. 2: Grid-tie inverter configuration used for the ESS

DC excitation system which controls the field voltage of the generator V_f in accordance to a reactive power mode and set-points.

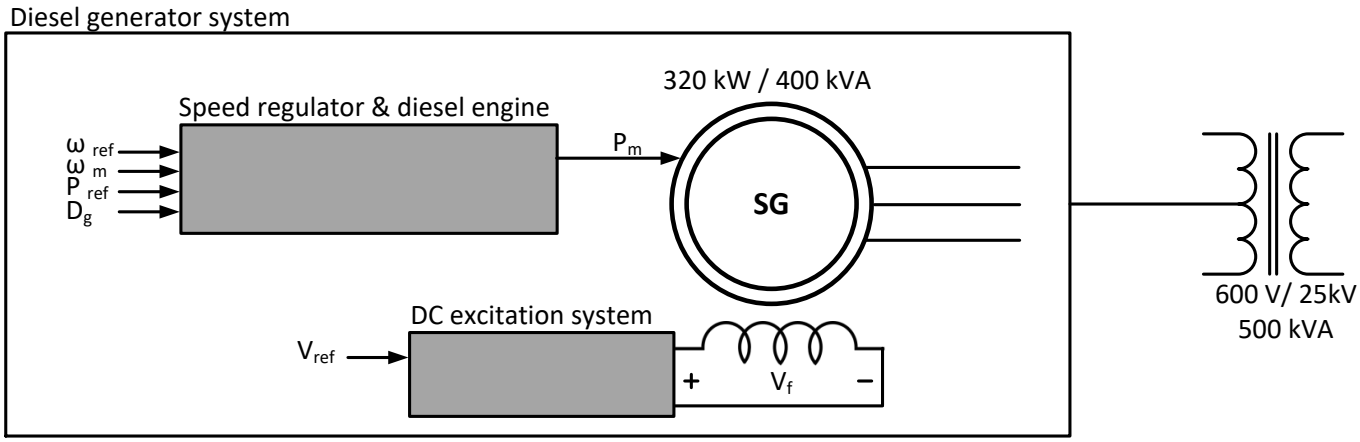

Fig. B. 3: Active power control loop for SM fed by a diesel engine

Appendix C

Real-Time HIL Co-Simulation Setup

This appendix describes the various components and building blocks of the real-time HIL co-simulation setup presented in chapter 2 and used throughout the thesis to analyze microgrids' cyber security and to validate the proposed control strategy in mitigating the impact of cyber-attacks. The co-simulation setup implemented is illustrated in Fig. C.1 and consists of the following components: 4 computers, 2 OPAL-RT real-time digital simulators, the NI digital controller NI-cRIO 9068, its analog input module NI 9220 and analog output module NI 9264, an OPAL-RT terminal to connect the analog channels, 2 Ethernet switches, a 4 ports network card and RJ-45 Ethernet cables. The software used for the setup include: MATLAB, Simulink, LabView, RT-LAB, OPNET, Wireshark and ICD Designer.

As discussed in chapter 2, adequate representation of microgrid systems would necessitate the modeling of the power system, communication network and information exchange layers. The detailed modeling of the layers along with their interfacing are presented in the following sections.

C.1 Microgrid Power System Layer Modeling

The microgrid feeder, DERs and loads are modeled as described in section 2.2 on a host computer (IP address: 132.206.62.16) running Simulink. The host computer is connected to the real-time simulator (IP address: 132.206.62.12) eth 0 port (MAC address: 00-25-90-24-A1-E6)

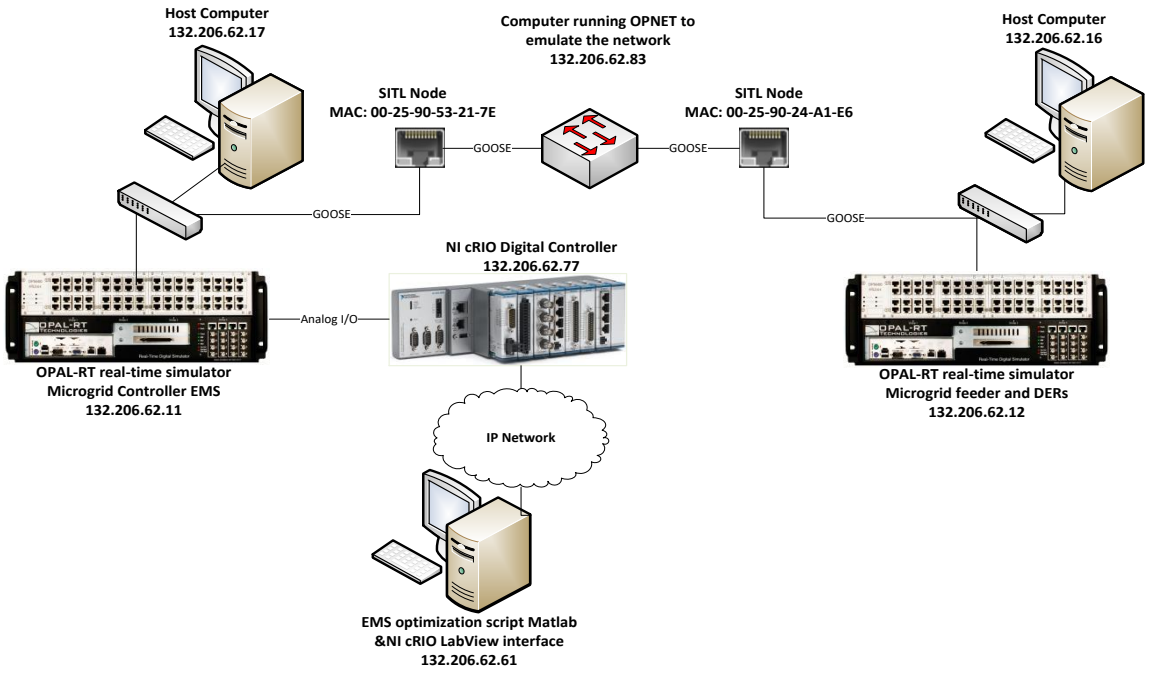

Fig. C. 1: Real-time co-simulation setup

through an Ethernet switch. The Simulink model is then loaded into RT-LAB running on the host computer to allow real-time operation of the microgrid feeder, DERs and loads on the real-time simulator. As detailed in section 2.4, different primary active and reactive power control modes could be selected to operate the DERs and evaluate the microgrid performance under various power management strategies.

The microgrid controller EMS optimization script is written as detailed in section 2.2.2.1 using MATLAB running on a host computer (IP address: 132.206.62.61). This host computer also runs LabView which connects to the NI-cRIO digital controller through the IP network. MATLAB and LabView are connected through the internal TCP connection of the host computer. The NI-cRIO analog input and output modules are connected to the OPAL-RT terminal plugged in the back of another real-time simulator (IP address: 132.206.62.11) through wires. A Simulink model is implemented on a host computer (IP address: 132.206.62.17) to represent the information exchanged with the microgrid controller EMS; i.e. the GOOSE messages sent and received from the microgrid entity and the analog inputs/outputs sent and received from the NI-cRIO. The host computer is connected to the real-time simulator (IP address: 132.206.62.11) eth 4 port (MAC address: 00-25-90-53-21-7E) through an Ethernet switch. The Simulink model is then loaded into RT-LAB running on the host computer to allow real-time operation of the microgrid controller

EMS on the real-time simulator.

C.2 Microgrid Communication Network Layer Modeling

The communication network for the microgrid system considered is modeled using OPNET and it consists of the microgrid feeder and DERs entity and a microgrid controller EMS entity connected through a switch by means of Ethernet cables. The SITL modules of OPNET are used to interface the two real-time simulators running the microgrid and the EMS with the communication network. For every SITL module modeled in OPNET, corresponds a network card implemented on the host computer running OPNET to connect to the external hardware. The IP address, mask, and gateway for each SITL interface are set so that its IP address is unique, and the mask and gateway are appropriate for connection to the physical hardware. Firewalls are also properly set so as to prevent the host computer's operating system from interfering with the SITL and terminating the connection.

The network is implemented on a host computer (IP address: 132.206.62.83) and consists of two SITL modules with the following specified MAC addresses: 1) SITL module representing the real-time simulator running the microgrid feeder and DERs (MAC address: 00-25-90-24-A1-E6), 2) SITL module representing the real-time simulator running the microgrid controller EMS (MAC address: 00-25-90-53-21-7E). The SITL modules are configured based on the MAC addresses of the switches' Ethernet ports to which the OPAL-RT simulators are connected rather than the IP addresses in order to support the GOOSE messaging protocol as it only has the physical, the data link and the application layers, as compared to the 7 layers open systems interconnection (OSI) model. The links connecting the SITL modules to the switch are duplex 10 Gbps Ethernet links. The NI-cRIO digital controller (MAC address: 00-80-2F-19-10-08) and the host computer running the EMS optimization script and LabView (MAC address: F8-B1-56-C3-C1-22) are connected to the Internet.

C.3 Microgrid Information Exchange Layer Modeling

The DERs and load measurements obtained at the microgrid side are sent over the communication network to the EMS which evaluates dispatch set-points that are sent back to the dispatchable DERs. The IEC 61850 GOOSE messaging protocol is used to enable this exchange of information. The publishers and subscribers are modeled in Simulink. At the microgrid side, a publisher is configured for every DER whose measurements are needed by the EMS and a subscriber is configured for every dispatchable DER requiring power set-points from the EMS to operate. Accordingly, at the microgrid controller EMS side, subscribers subscribe to the DER measurements and publishers publish the dispatch set-points to the DERs. An SCL is written in XML using ICD Designer to configure the various IEDs. Logical devices are defined for every entity sending or receiving information over the network. For every logical device, logical nodes are defined to represent the information sent or received from or to the IED. To properly exchange information between the IEDs, communication attributes need to be properly assigned for every IED logical device in the SCL file. A unique APP ID, MAC address and a VLAN priority are specified for each IED function defined by the logical nodes. The SCL is then loaded into the publishers and subscribers modeled in Simulink. The Ethernet adapter of the real-time simulator, the IED name, the logical device's MAC address and APP ID are all specified for every publisher and subscriber for proper information exchange.

C.4 Microgrid Constituting Layers Interfacing

In order to implement a co-simulation platform, the microgrid power system, communication network and information layers need to be connected and interfaced without accumulation of errors. The SITL module of OPNET allows the physical hardware devices running the microgrid and the EMS in real-time and the network implemented in OPNET to interact as a unified system. This interface facilitates the connection of the two real-time simulators running the microgrid feeder and DER and the microgrid central controller and serves as a data buffer for real-time packet exchange. In fact, in order to cause no accumulation of errors, the hardware and

software used to model the different microgrid constituting layers are controlled such that: i) the EMS script and LabView HMI are designed such that they only generate commands when they receive the required inputs, ii) the communication network simulation is started after the EMS engine, and waits for information to be exchanged, iii) the IEC 61850 GOOSE subscriber at the real-time simulator modeling the EMS information exchange interface is operated such that it records the time when the first set of measurements is received from the microgrid and based on that time specifies the periods when it will be re-enabled and when the publisher sending the commands to the microgrid will be enabled, iv) the real-time simulator running the microgrid system will therefore be operated at last and the publisher and subscribers at this end will be enabled every EMS dispatch update period. As such, the time when the power system simulation is started will represent the time reference of the co-simulation platform. Table C.1 summarizes the data exchange sequence between hardware and software.

Table C. 1 : Summary of information exchange

Source	Destination	Information Exchanged	Protocol
DERs publisher (OPAL-RT simulator running the microgrid feeder and DERs)	Communication network (SITL OPNET)	DERs and Load measurements	IEC 61850 GOOSE
Communication network (SITL OPNET)	Microgrid controller EMS subscriber (OPAL-RT simulator running the microgrid controller)	DERs and Load measurements	IEC 61850 GOOSE
Microgrid controller EMS (Analog I/O card connected to the OPAL-RT simulator running the microgrid controller)	NI-cRIO digital controller (connected to the Analog I/O card using wires)	DERs and Load measurements	Analog
NI-cRIO digital controller	NI-cRIO LabView Interface (through the Internet)	DERs and Load measurements	TCP
NI-cRIO LabView interface	MATLAB running the optimization script (through an internal TCP connection on the host computer)	DERs and Load measurements	TCP
MATLAB running the optimization script (through an internal TCP connection on the host computer)	NI-cRIO LabView interface (through the IP network)	DERs and Load dispatch set-points and circuit breakers commands	TCP
NI-cRIO LabView interface (through the Internet)	NI-cRIO digital controller	DERs and Load dispatch set-points and circuit breakers commands	TCP
NI-cRIO digital controller (connected to the Analog I/O card using wires)	Microgrid controller EMS (Analog I/O card connected to the OPAL-RT simulator running the microgrid controller)	DERs and Load dispatch set-points and circuit breakers commands	Analog
Microgrid controller EMS publishers (OPAL-RT simulator running the microgrid controller)	Communication network (SITL OPNET)	DERs and Load dispatch set-points and circuit breakers commands	IEC 61850 GOOSE
Communication network (SITL OPNET)	Dispatchable DERs subscribers (OPAL-RT simulator running the microgrid feeder)	DERs and Load dispatch set-points and circuit breakers commands	IEC 61850 GOOSE

Appendix D

DDoS Cyber-Attack Modeling

This appendix provides a detailed modeling of the DDoS cyber-attack defined in chapter 2. The DDoS cyber-attack modeled targets the microgrid EMS and is implemented using Ettercap as shown in Fig. D.1. The attack assumes that the attacker has valid credentials to connect over the IP network connecting the microgrid digital controller to the EMS script. For better performance, the Ettercap tool was installed on a virtual Linux machine created on the host computer (IP address: 132.206.62.48). In order to allow packets sniffing, the computer running Ettercap has been connected to the IP network. After scanning for hosts connected to the network, the PC running LabView and the EMS optimization script (IP address: 132.206.62.61) is identified, as Ettercap not only gathers the addresses but also a description of the hosts. A plugin "dos_attack" is provided by Ettercap and allows users to launch DDoS attacks against a victim IP address. The plugin first scans the victim to find open ports, then starts to flood these ports with SYN packets, using a fake IP address as the source. Then it uses fake ARP replies to intercept packets for the fake host. When it receives SYN-ACK from the victim, it replies with an ACK packet creating established connections with the fake source and half-opened connections with the victim. Different instances of Ettercap are used with different fake IP addresses as sources in order to exhaust the victim's resources and cause a DDoS attack. As a result of the attack, and as the victim's resources are consumed, a connection between the digital controller and the host running the EMS script and LabView could no longer be established and information could no longer be exchanged. It is important to mention that it only takes seconds for the attack to become effective and cause the

loss of the connection between the two entities. Even if the attack is cleared, restoring the connection would require human intervention.

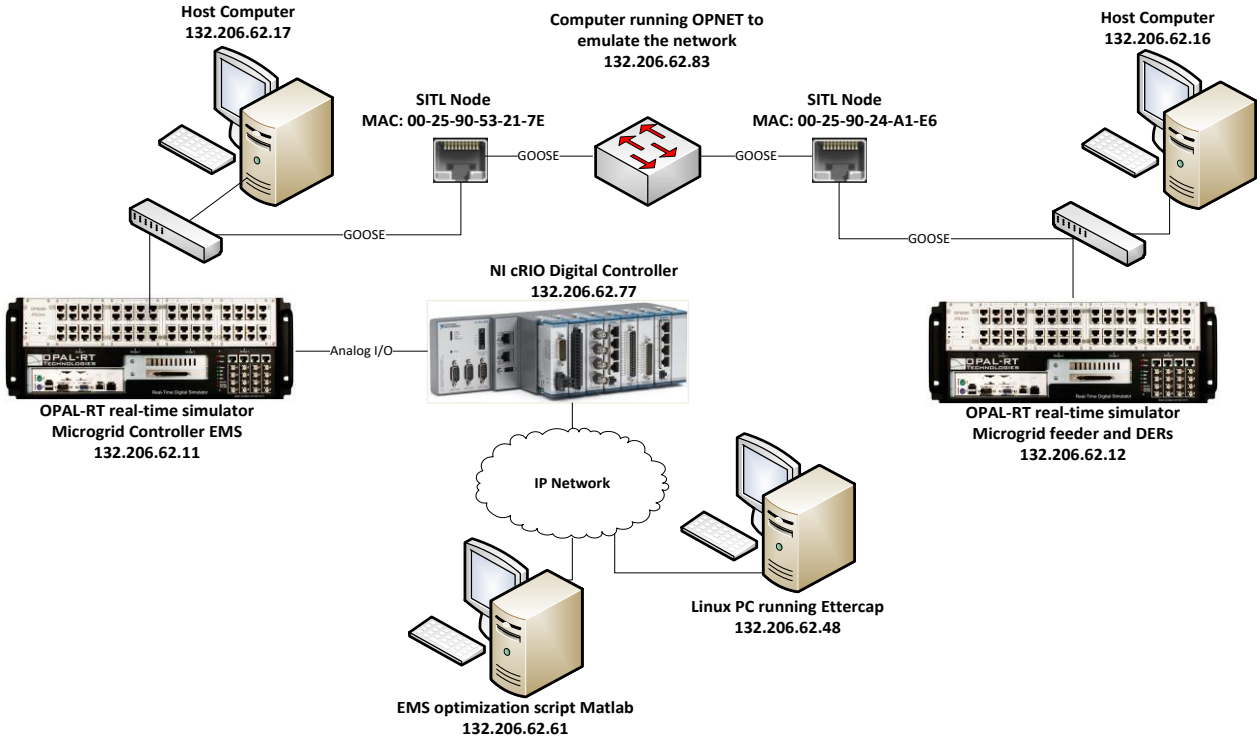

Fig. D. 1: Cyber-attack modeling on the co-simulation setup

References

[1] "Cyber war ‘more deadly’ than nuclear weapons," in *THE DAY*, ed, 2015.

[2] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, pp. 49-51, 2011.

[3] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, pp. 91-93, 2011.

[4] G. Weston, "Foreign hackers attack Canadian government," in *CBC*, ed, 2011.

[5] A. S. M. Egan, "Chase, NYSE Websites Targeted in Cyber Attacks," in *FOXBusiness*, ed, 2012.

[6] "Cyber Attack News," in *ABC News*, ed, 2016.

[7] "U.S. Suspects Hackers in China Breached About 4 Million People’s Records, Officials Say," in *THE WALL STREET JOURNAL*, ed, 2015.

[8] (2017, May 2017). *Cyber-attack: Europol says it was unprecedented in scale*. Available: http://www.bbc.com/news/world-europe-39907965

[9] P. Mccausland, S. Petulla, and A. Jamieson. (2017, May 2017). *Global Cyberattack Hits 150 Countries, Europol Chief Says*. Available: http://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121

[10] E. Groll, "Did Russia Knock Out Ukraine’s Power Grid?," Foreigh Policy2016.

[11] IEEE. (2016) Cybersecurity AT U.S. Utilities due for an Upgrade. *Spectrum IEEE*. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7459104

[12] B. Brasso, "Cyber attacks against critical infrastructure are no longer just theories," in *FireEye*, ed, 2016.

[13] C. Colson, M. Nehrir, and R. Gunderson, "Distributed multi-agent microgrids: a decentralized approach to resilient power system self-healing," in *Resilient Control Systems (ISRCS), 2011 4th International Symposium on*, 2011, pp. 83-88.

[14] Departement of Energy. *Microgrids*. Available: http://energy.gov/oe/office-electricity-delivery-and-energy-reliability

[15] W. Bower, D. Ton, R. Guttromson, S. Glover, J. Stamp, D. Bhatnagar, *et al.*, "The Advanced Microgrid Integration and Interoperability," SANDIA National Laboratories2014.

[16] E. Bou-Harb, W. Lucia, N. Forti, S. Weerakkody, N. Ghani, and B. Sinopoli, "Cyber Meets Control: A Novel Federated Approach for Resilient CPS Leveraging Real Cyber Threat Intelligence," *IEEE Communications Magazine,* vol. 55, pp. 198-204, 2017.

[17] D. E. Olivares, C. A. Cañizares, and M. Kazerani, "A centralized energy management system for isolated microgrids," *Smart Grid, IEEE Transactions on,* vol. 5, pp. 1864-1875, 2014.

[18] D. E. Olivares, C. A. Cañizares, and M. Kazerani, "A centralized optimal energy management system for microgrids," in *Power and Energy Society General Meeting, 2011 IEEE,* 2011, pp. 1-6.

[19] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management," *Power and Energy Magazine, IEEE,* vol. 6, pp. 54-65, 2008.

[20] M. Ross, C. Abbey, F. Bouffard, and G. Joos, "Multiobjective Optimization Dispatch for Microgrids With a High Penetration of Renewable Generation," *Sustainable Energy, IEEE Transactions on,* vol. 6, pp. 1306-1314, 2015.

[21] R. Firestone and C. Marnay. (2005, 6 May 2016). *Energy manager design for microgrids*. Available: https://escholarship.org/uc/item/6fm1x870

[22] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodríguez, "Control of power converters in AC microgrids," *Power Electronics, IEEE Transactions on,* vol. 27, pp. 4734-4749, 2012.

[23] I. D. Margaris, S. Papathanassiou, N. D. Hatziargyriou, A. D. Hansen, and P. Sørensen, "Frequency control in autonomous power systems with high wind power penetration," *Sustainable Energy, IEEE Transactions on,* vol. 3, pp. 189-199, 2012.

[24] A. Yazdani and R. Iravani, *Voltage-sourced converters in power systems: modeling, control, and applications*: John Wiley & Sons, 2010.

[25] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *Power Systems, IEEE Transactions on,* vol. 21, pp. 1821-1831, 2006.

[26] G. Stanciulescu, H. Farhangi, A. Palizban, and N. Stanchev, "Communication technologies for BCIT smart microgrid," 2012.

[27] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks,* vol. 57, pp. 1344-1371, 2013.

[28] Modbus, "Modbus application protocol specification V1.1b3," 2012.

[29] "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010),* pp. 1-821, 2012.

[30] I. E. Commission, " IEC/TR 61850 Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines," ed, 2013.

[31] IEEE, "IEEE P2030 Recommended Practice for Implementing an IEC 61850 Based Substation Communications, Protection, Monitoring and Control System," ed, 2016.

[32] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, vol. 21, pp. 548-558, 2006.

[33] W. Li, A. Monti, M. Luo, and R. A. Dougal, "VPNET: A co-simulation framework for analyzing communication channel effects on power systems," in *Electric Ship Technologies Symposium (ESTS), 2011 IEEE*, 2011, pp. 143-149.

[34] V. Liberatore and A. Al-Hammouri, "Smart grid communication and co-simulation," in *Energytech, 2011 IEEE*, 2011, pp. 1-5.

[35] F. Guo, L. Herrera, R. Murawski, E. Inoa, C.-L. Wang, P. Beauchamp, *et al.*, "Comprehensive real-time simulation of the smart grid," *IEEE Transactions on Industry Applications*, vol. 49, pp. 899-908, 2013.

[36] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *Power & Energy Society General Meeting, 2015 IEEE*, 2015, pp. 1-5.

[37] M. Armendariz, M. Chenine, L. Nordstrom, and A. Al-Hammouri, "A co-simulation platform for medium/low voltage monitoring and control applications," in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, 2014, pp. 1-5.

[38] D. V. Dollen, "Report to NIST on the Smart Grid Interoperability Standards Roadmap—Post Comment Period Version," 2009.

[39] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Military Communications Conference, 2010-MILCOM 2010*, 2010, pp. 1830-1835.

[40] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 5-20, 2013.

[41] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39-53, 2004.

[42] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References " 2010.

[43] I. E. Commission, "IEC TS 62351-6," 2007.

[44] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 2046-2069, 2013.

[45] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, p. 13, 2011.

[46] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid,* vol. 2, pp. 382-390, 2011.

[47] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems,* vol. 23, pp. 1731-1738, 2012.

[48] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid,* vol. 5, pp. 1665-1676, 2014.

[49] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid,* vol. 6, pp. 1686-1696, 2015.

[50] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM symposium on information, computer and communications security*, 2011, pp. 355-366.

[51] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 73-83, 2009.

[52] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Power and Energy Society General Meeting, 2011 IEEE*, 2011, pp. 1-6.

[53] B. Chen, K. L. Butler-Purry, and D. Kundur, "Impact analysis of transient stability due to cyber attack on FACTS devices," in *North American Power Symposium (NAPS), 2013*, 2013, pp. 1-6.

[54] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, 2013, pp. 1-5.

[55] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *Smart Grid, IEEE Transactions on,* vol. 5, pp. 580-591, 2014.

[56] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *Power Systems, IEEE Transactions on,* vol. 30, pp. 223-232, 2015.

[57] A. M. Melin, E. M. Ferragut, J. Laska, D. L. Fugate, and R. Kisner, "A mathematical framework for the analysis of cyber-resilient control systems," in *Resilient Control Systems (ISRCS), 2013 6th International Symposium on*, 2013, pp. 13-18.

[58] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *Selected Areas in Communications, IEEE Journal on,* vol. 30, pp. 1108-1118, 2012.

[59] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks,* vol. 6, pp. 2-13, 2011.

[60] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," *Smart Grid, IEEE Transactions on,* vol. 6, pp. 2444-2453, 2015.

[61] K. I. Sgouras, A. D. Birda, and D. P. Labridis, "Cyber attack impact on critical smart grid infrastructures," in *Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES*, 2014, pp. 1-5.

[62] S. Zhang and V. Vittal, "Wide-area control resiliency using redundant communication paths," *Power Systems, IEEE Transactions on,* vol. 29, pp. 2189-2199, 2014.

[63] V. Kounev, D. Tipper, A. A. Yavuz, B. M. Grainger, and G. F. Reed, "A Secure Communication Architecture for Distributed Microgrid Control," *IEEE Transactions on Smart Grid,* vol. 6, pp. 2484-2492, 2015.

[64] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE,* vol. 50, pp. 38-45, 2012.

[65] M. J. Dworkin, "Recommendation for block cipher modes of operation: The XTS-AES mode for confidentiality on storage devices," 2010.

[66] W. C. Barker and E. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher: NIST Special Publication 800-67, Revision 2," 2012.

[67] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV2001.

[68] P. Gallagher, "Digital signature standard (dss)," *Federal Information Processing Standards Publications, volume FIPS,* pp. 186-3, 2013.

[69] J. Jonsson, K. Moriarty, B. Kaliski, and A. Rusch, "PKCS# 1: RSA Cryptography Specifications Version 2.2," 2016.

[70] M. J. Dworkin, "Recommendation for block cipher modes of operation: The CMAC mode for authentication," 2016.

[71] M. J. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," 2007.

[72] J. M. Turner, "The keyed-hash message authentication code (hmac)," *Federal Information Processing Standards Publication*, 2008.

[73] NIST, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," ed, 2010.

[74] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," *IEEE Transactions on Automatic Control,* vol. 58, pp. 2715-2729, 2013.

[75] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control,* vol. 59, pp. 1454-1467, 2014.

[76] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control,* vol. 61, pp. 2079-2091, 2016.

[77] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *American Control Conference (ACC), 2015*, 2015, pp. 2439-2444.

[78] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, *et al.*, "Robustness of attack-resilient state estimators," in *ICCPS'14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)*, 2014, pp. 163-174.

[79] Y. Nakahira and Y. Mo, "Dynamic state estimation in the presence of compromised sensory data," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, 2015, pp. 5808-5813.

[80] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, 2015, pp. 5820-5826.

[81] S. Weerakkody and B. Sinopoli, "A moving target approach for identifying malicious sensors in control systems," in *Communication, Control, and Computing (Allerton), 2016 54th Annual Allerton Conference on*, 2016, pp. 1149-1156.

[82] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Transactions on Control Systems Technology*, vol. 22, pp. 1396-1407, 2014.

[83] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems*, vol. 35, pp. 93-109, 2015.

[84] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, 2014, pp. 3757-3764.

[85] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, pp. 1495-1508, 2011.

[86] *Snort: The Open Source Network Intrusion Detection System*. Available: https://www.snort.org/

[87] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, 2002, pp. 312-321.

[88] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of Attack Resilient Control for AGC," in *Resilience Week (RWS), 2016*, 2016, pp. 125-129.

[89] M. Pajic, S. Sundaram, G. J. Pappas, and R. Mangharam, "The wireless control network: A new approach for control over networks," *IEEE Transactions on Automatic Control*, vol. 56, pp. 2305-2318, 2011.

[90] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Transactions on Smart Grid*, vol. 7, pp. 2923-2932, 2016.

[91] W. Zeng, Y. Zhang, and M.-Y. Chow, "Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units," *IEEE Transactions on Industrial Informatics,* 2015.

[92] NIST, "Guidelines for Smart Grid Cybersecurity," 2014.

[93] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization," *IEEE Transactions on Industrial Electronics,* vol. 58, pp. 158-172, 2011.

[94] J. M. Guerrero, M. Chandorkar, T.-L. Lee, and P. C. Loh, "Advanced control architectures for intelligent microgrids, part I: decentralized and hierarchical control," *IEEE Transactions on Industrial Electronics,* vol. 60, pp. 1254-1262, 2013.

[95] T. L. Vandoorn, B. Meersman, J. D. De Kooning, and L. Vandevelde, "Directly-coupled synchronous generators with converter behavior in islanded microgrids," *IEEE Transactions on Power Systems,* vol. 27, pp. 1395-1406, 2012.

[96] E. Planas, A. Gil-de-Muro, J. Andreu, I. Kortabarria, and I. M. de Alegría, "General aspects, hierarchical controls and droop methods in microgrids: A review," *Renewable and Sustainable Energy Reviews,* vol. 17, pp. 147-159, 2013.

[97] C. K. Sao and P. W. Lehn, "Autonomous load sharing of voltage source converters," *IEEE Transactions on Power Delivery,* vol. 20, pp. 1009-1016, 2005.

[98] G. Yajuan, W. Weiyang, G. Xiaoqiang, and G. Herong, "An improved droop controller for grid-connected voltage source inverter in microgrid," in *Power Electronics for Distributed Generation Systems (PEDG), 2010 2nd IEEE International Symposium on,* 2010, pp. 823-828.

[99] Y. A.-R. I. Mohamed and E. F. El-Saadany, "Adaptive decentralized droop controller to preserve power sharing stability of paralleled inverters in distributed generation microgrids," *IEEE Transactions on Power Electronics,* vol. 23, pp. 2806-2816, 2008.

[100] J. Bryan, R. Duke, and S. Round, "Decentralized generator scheduling in a nanogrid using DC bus signaling," in *Power Engineering Society General Meeting, 2004. IEEE,* 2004, pp. 977-982.

[101] D. Wu, F. Tang, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, "Autonomous active power control for islanded ac microgrids with photovoltaic generation and energy storage system," *Energy Conversion, IEEE Transactions on,* vol. 29, pp. 882-892, 2014.

[102] H. Liu, Z. Hu, Y. Song, and J. Lin, "Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands," *Power Systems, IEEE Transactions on,* vol. 28, pp. 3480-3489, 2013.

[103] M. ROSS, C. ABBEY, Y. BRISSETTE, and G. JOÓS, "A Novel Isochronous Control Strategy for Coordination of Distributed Energy Resources in an Islanded Microgrid," presented at the CIGRÉ Canada Conference, Toronto, Ontario, 2014.

[104] J. G. de Matos, F. SF e Silva, R. de S, and A. Luiz, "Power control in ac isolated microgrids with renewable energy sources and energy storage systems," *Industrial Electronics, IEEE Transactions on,* vol. 62, pp. 3490-3498, 2015.

[105] M. Hossain, H. R. Pota, M. A. Mahmud, and M. Aldeen, "Robust control for power sharing in microgrids with low-inertia wind and PV generators," *IEEE Transactions on Sustainable Energy,* vol. 6, pp. 1067-1077, 2015.

[106] Y. Han, P. M. Young, A. Jain, and D. Zimmerle, "Robust control for microgrid frequency deviation reduction with attached storage system," *IEEE Transactions on Smart Grid,* vol. 6, pp. 557-565, 2015.

[107] Y. W. Li and C.-N. Kao, "An accurate power control strategy for power-electronics-interfaced distributed generation units operating in a low-voltage multibus microgrid," *IEEE Transactions on Power Electronics,* vol. 24, pp. 2977-2988, 2009.

[108] J. He and Y. W. Li, "An enhanced microgrid load demand sharing strategy," *IEEE Transactions on Power Electronics,* vol. 27, pp. 3984-3995, 2012.

[109] C.-T. Lee, C.-C. Chu, and P.-T. Cheng, "A new droop control method for the autonomous operation of distributed energy resource interface converters," *IEEE Transactions on Power Electronics,* vol. 28, pp. 1980-1993, 2013.

[110] J. Liu, Y. Miura, and T. Ise, "Comparison of dynamic characteristics between virtual synchronous generator and droop control in inverter-based distributed generators," *IEEE Transactions on Power Electronics,* vol. 31, pp. 3600-3611, 2016.

[111] U. Delille, B. Francois, and G. Malarange, "Dynamic frequency control support by energy storage to reduce the impact of wind and solar generation on isolated power system's inertia," *Sustainable Energy, IEEE Transactions on,* vol. 3, pp. 931-939, 2012.

[112] M. Torres and L. A. Lopes, "Virtual synchronous generator control in autonomous wind-diesel power systems," in *Electrical Power & Energy Conference (EPEC), 2009 IEEE*, 2009, pp. 1-6.

[113] U. Tamrakar, D. Galipeau, R. Tonkoski, and I. Tamrakar, "Improving transient stability of photovoltaic-hydro microgrids using virtual synchronous machines," in *PowerTech, 2015 IEEE Eindhoven*, 2015, pp. 1-6.

[114] T. Shintai, Y. Miura, and T. Ise, "Oscillation damping of a distributed generator using a virtual synchronous generator," *IEEE transactions on power delivery,* vol. 29, pp. 668-676, 2014.

[115] N. Soni, S. Doolla, and M. C. Chandorkar, "Improvement of transient response in microgrids using virtual inertia," *Power Delivery, IEEE Transactions on,* vol. 28, pp. 1830-1838, 2013.

[116] J. Zhao, X. Lyu, Y. Fu, X. Hu, and F. Li, "Coordinated microgrid frequency regulation based on DFIG variable coefficient using virtual inertia and primary frequency control," *IEEE Transactions on Energy Conversion,* vol. 31, pp. 833-845, 2016.

[117] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," in *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, Waterloo, ON, Canada, 2016, p. 1.

[118] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Cyber Security Analysis of Islanded Microgrids Controllers," in *Proceedings of the CIGRE Canada Conference on the Future Power Systems and Grid Resiliency*, Vancouver, BC, Canada, 2016.

[119] M. Chlela, "Cyber-Resilient Control of Inverter Based Microgrids," presented at the IEEE Global Conference on Signal and Information Processing, Greater Washington, D.C., USA, 2016.

[120] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Power and Energy Society General Meeting (PESGM), 2016*, Boston, MA, U.S.A, 2016, pp. 1-5.

[121] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks," *IEEE Transactions on Smart Grid*, 2016.

[122] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, pp. 659-666, 2011.

[123] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, pp. 1244-1253, 2013.

[124] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, pp. 1362-1370, 2012.

[125] Z. Miao, A. Domijan Jr, and L. Fan, "Investigation of microgrids with both inverter interfaced and direct AC-connected distributed energy resources," *Power Delivery, IEEE Transactions on*, vol. 26, pp. 1634-1642, 2011.

[126] P. Piagi and R. H. Lasseter, "Autonomous control of microgrids," in *2006 IEEE Power Engineering Society General Meeting*, 2006, p. 8 pp.

[127] M. C. Chandorkar, D. M. Divan, and R. Adapa, "Control of parallel connected inverters in standalone AC supply systems," *IEEE Transactions on Industry Applications*, vol. 29, pp. 136-143, 1993.

[128] R. H. Lasseter, "MicroGrids," vol. 1, pp. 305-308, 2002.

[129] H. Moussa, A. Shahin, J.-P. Martin, S. Pierfederici, and N. Moubayed, "Optimal Angle Droop for Power Sharing Enhancement with Stability Improvement in Islanded Microgrids," *IEEE Transactions on Smart Grid*, 2017.

[130] International Electrotechnical Commission, "IEC/TR 61850 Communication networks and systems for power utility automation – Part 7-4: Compatible logical node classes and data object classes," ed, 2010, p. 179.

[131] International Electrotechnical Commission, "IEC/TR 61850 Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources logical nodes ", ed, 2009, p. 179.

[132] International Electrotechnical Commission, "IEC/TR 61850 Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)," ed, 2010, p. 179.

[133] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids," in *PES General Meeting| Conference & Exposition, 2014 IEEE*, 2014, pp. 1-5.

[134] T. L. Vandoorn, J. C. Vasquez, J. De Kooning, J. M. Guerrero, and L. Vandevelde, "Microgrids: Hierarchical control and an overview of the control and reserve management strategies," *Industrial Electronics Magazine, IEEE*, vol. 7, pp. 42-55, 2013.

[135] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, 2000, pp. 2275-2280.

[136] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*, 2008, pp. 495-500.

[137] E. Sortomme, S. Venkata, and J. Mitra, "Microgrid protection using communication-assisted digital relays," *IEEE Transactions on Power Delivery*, vol. 25, pp. 2789-2796, 2010.

[138] H. Al-Nasseri, M. Redfern, and F. Li, "A voltage based protection for micro-grids containing power electronic converters," in *Power Engineering Society General Meeting, 2006. IEEE*, 2006, p. 7 pp.

[139] M. A. Zamani, A. Yazdani, and T. S. Sidhu, "A communication-assisted protection strategy for inverter-based medium-voltage microgrids," *IEEE Transactions on Smart Grid*, vol. 3, pp. 2088-2099, 2012.

[140] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, pp. 1-6.

[141] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 226-231.

[142] T. Kerdphol, F. S. Rahman, Y. Mitani, M. Watanabe, and S. Küfeoğlu, "Robust Virtual Inertia Control of an Islanded Microgrid Considering High Penetration of Renewable Energy," *IEEE Access*, 2017.

[143] K. H. Ang, G. Chong, and Y. Li, "PID control system analysis, design, and technology," *IEEE transactions on control systems technology*, vol. 13, pp. 559-576, 2005.

[144] D. Michaelson, H. Mahmood, and J. Jiang, "A predictive energy management strategy with pre-emptive load shedding for an islanded PV-battery microgrid," in *Industrial Electronics Society, IECON 2013-39th Annual Conference of the IEEE*, 2013, pp. 1501-1506.

[145] I. J. Balaguer, Q. Lei, S. Yang, U. Supatti, and F. Z. Peng, "Control for grid-connected and intentional islanding operations of distributed power generation," *Industrial Electronics, IEEE Transactions on*, vol. 58, pp. 147-157, 2011.

[146] NERC, "Automatic Underfrequency Load Shedding," 2012.

[147] IESO. (2009). *Zonal demands Southwestern Ontario*. Available: http://www.ieso.ca/Pages/Power-Data/default.aspx#report

[148] University of Waterloo. (2009). *Waterloo Weather Station Data*. Available: http://weather.uwaterloo.ca/data.html

[149] C. Nichita, D. Luca, B. Dakyo, and E. Ceanga, "Large band simulation of the wind speed for real time wind turbine simulators," *Energy Conversion, IEEE Transactions on*, vol. 17, pp. 523-529, 2002.