FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

DIGITAL TWIN-BASED COOPERATIVE CONTROL TECHNIQUES FOR SECURE AND INTELLIGENT OPERATION OF DISTRIBUTED MICROGRIDS

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL AND COMPUTER ENGINEERING

by

Ahmed Aly Saad Ahmed

2021

To: Dean John Volakis
College of Engineering and Computing

This dissertation, written by Ahmed Aly Saad Ahmed, and entitled Digital Twin-Based Cooperative Control Techniques for Secure and Intelligent Operation of Distributed Microgrids, having been approved in respect to style and intellectual contents, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Sundaraja Sitharama Iyengar

Kemal Akkaya

Stavros V. Georgakopoulos

Tarek Youssef

Osama A. Mohammed, Major Professor

Date of Defense: March 15, 2021

The dissertation of Ahmed Aly Saad Ahmed is approved.

Dean John Volakis
College of Engineering and Computing

Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2021

DEDICATION

For their endless support, love, and sacrifice, I dedicate this work.

To my Beloved Parents, my Daughters Rovan, Rawan, Maryam and Dear Wife Samah.

ACKNOWLEDGMENTS

I would like to thank my supervisor, Professor Osama Mohammed, for supervising this work, and for providing me with financial support through appointing me as a Research Assistant at the Electrical and Computer Engineering Department at FIU. I would also like to thank Professor Mohammed for making me a part of the Energy System Research Laboratory (ESRL). I have gained a lot of skills and experience at ESRL, which has first-class equipment I needed to experimentally verify my results. This helped me complete my doctoral studies. Also, as my doctoral research started to gain traction, Professor Mohammed provided me opportunities to grow within my professional career inside and outside the university, such as encouraging me to serve as the vice-chair of the IEEE PES Student Branch Chapter and allowing me to serve as a judge or organizer in several other professional activities.

I would also like to thank my committee members for their support. I also like to acknowledge the support from Prof. S. S. Iyengar, Prof. Kemal Akkaya, Prof. Stavros and Dr. Tarek Youssef. I would like to acknowledge the research support provided by the Department of Electrical and Computer Engineering at Florida International University.

Finally, thanks are also due to all the graduate members and undergraduate student scholars at the Energy Systems Research Laboratory, whose discussions, contributions, and assistance helped me achieve my research goals. I am also grateful to the FIU community and department staff.

ABSTRACT OF THE DISSERTATION

DIGITAL TWIN-BASED COOPERATIVE CONTROL TECHNIQUES FOR SECURE AND INTELLIGENT OPERATION OF DISTRIBUTED MICROGRIDS

by

Ahmed Aly Saad Ahmed

Florida International University, 2021

Miami, Florida

Professor Osama A. Mohammed, Major Professor

Networked microgrids play a key role in constructing future active distribution networks for providing the power system with resiliency and reliability against catastrophic physical and cyber incidents. Motivated by the increasing penetration of renewable resources and energy storage systems in the distribution grids, utility companies are encouraged to unleash the capabilities of the distributed microgrid to work as virtual power plants that can support the power systems. The microgrids nature is transforming the grid and their control systems from centralized architecture into distributed architectures. The distributed networked microgrids introduced many benefits to the future smart grids, it created many challenges such as the absence of centric oversight, the lack of robustness against renewable uncertainty and vulnerability to cyberattacks. These challenges and issues imposed the necessities to transform the control system architecture form classical decision making to holistic, hierarchical multi-vision distributed smart decision making.

In this dissertation, a data-centric oversight layer is added on top of the energy cyber-physical system to collect the required information by the internet of things (IoT) technologies and provision it to the cloud virtual space. This layer has relatively unlimited

computational and communication resources that can guide the distributed cyber system to secure, reliable, efficient and intelligent operation. By adding the data-informed model philosophy (Digital Twin) into this centric layer can answer real-time What-IF questions, enhance the control system resiliency, provide the control system with guidance toward the global optimal objective and provide situational and security awareness.

The dissertation extended the developed control system resiliency by providing multi-mode of operation according to the cyber system state. The distributed multi-agent control system is designed to be security-aware without the centric oversight via developing distributed cyberattack observer that can detect and identify the attacked neighbors by extracting the cyber graph and the consensus control features and compare it with the healthy characteristics.

Finally, the controller itself is armed with an independent mode of operation, which makes the controller work with the local information only to guarantee stable and optimal operation. The developed techniques and ideas we experimentally tested and evaluated on the FIU smart grid testbed.

TABLE OF CONTENTS

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

LIST OF ACRONYMS

ACRONYMS	DETAILS
ACPF	Alternating Current Power Flow
AHP	Analytical Hierarchy Process
AI	Artificial Intelligence
API	Application Programming Interface
AWS	Amazon Web Service
BESS	Battery Energy Storage System
BSS	Battery Storage System
CCGT	Combined Cycle Gas Turbine
CL	Constant Impedance Load
CM	Coordination Manager
CPL	Constant Power Load
CPS	Cyber Physical System
CT	Current Transformer
DCNMG	Direct Current Networked Microgrid
DCPF	Direct Current Power Flow
DCS	Distributed Control System
DDS	Data Distribution Service
DER	Distributed Energy Resources
DG	Distributed Generation
DL	Deep learning

DoS	Denial of Service
DQN	Deep Q learning
DT	Digital Twin
ECPS	Energy Cyber Physical System
ESS	Energy Storage System
EV	Electric Vehicle
FD	Fast Dynamics
FDIA	False Data Injection Attack
FLD	Flexible Load
GPS	Global Positioning System
GT	Gas Turbine
HDMPC	Hierarchically Distributed Model Predictive Control
HPL	Heavy Pulsed Load
HTTPs	Hypertext Transfer Protocol Secure
IC	Interlinking Converter
ICC	Interlinking Converter Controller
IED	Intelligent Electronic Device
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
JSON	JavaScript Object Notation
LD	Load

LO	Luenberger Observer
MG	Microgrid
MM	Mathematical Morphology
MPC	Model Predictive Control
µPMU	Micro Phasor Measurement Unit
MQTT	Message Queuing Telemetry Transport
MVAC	Medium Voltage Alternating Current
MVDC	Medium Voltage Direct Current
NMG	Networked Microgrid
OPF	Optimal Power Flow
OTA	On-The-Air
PCC	Point of Common Coupling
PE	Power Electronics
PEMS	Predictive Energy Management System
PHS	Pumped Hydro Storage
PLC	Programmable Logic Controller
QoS	Quality of Service
RES	Renewable Energy Source
SCESS	SuperCapacitor Energy Storage System
SD	Slow Dynamics
SE	Structing Element
SM	Supervisory Manager

SoC	State of Charge
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TES	Thermal Energy Storage
VPP	Virtual Power Plant
vRES	Variable Renewable Energy Source
VT	Voltage Transformer
XML	Extensible Markup Language
N_A	Number of interconnected grid areas
CM_O	Coordination manager for O^{th} area
n_e	Number of energy units
$P_{g,i}, P_{L,i}$	Injected (generation) and absorbed (load) power for i^{th} energy unit
$\eta_{g,i}, \eta_{L,i}$	Generation and loading efficiencies for i^{th} energy unit
C_i, SOC_i	Energy storage capacity and state of charge for i^{th} energy unit
$d_{in,i}$	Original infeed power for i^{th} energy unit
$d_{cg,i}$	Fuel infeed for i^{th} conventional generation unit
$d_{re,i}$	Original input for i^{th} renewable energy unit
$d_{L,i}$	Required demand for i^{th} Load unit
ψ_i	Power shedding/curtailment for i^{th} energy unit
m	Number of grid buses
$P_{in,j}, P_{out,j}$	Input and output power for j^{th} bus
n_x, n_{x_O}	Number of SM and CM state-space variables

$n_u, n_{u_\mathcal{O}}$	Number of SM and CM manipulated variables
$n_d, n_{d_\mathcal{O}}$	Number of SM and CM measured disturbances (energy unit's power infeed)
$n_I, n_{I_\mathcal{O}}$	Number of SM and CM state-space inputs
$n_v, n_{v_\mathcal{O}}$	Number of grid and areas interconnected buses
$n_y, n_{y_\mathcal{O}}$	Number of SM and CM state-space outputs
$n_{v_{sh}}$	Number of interconnected coupled areas tie-lines
$\Delta t^{sm}, \Delta t^{cm}$	SM and CM control time horizon
$x^{sm}(k)$	SM state vector at time k, $x^{sm} \in \mathbb{R}^{n_x}$
$\mathcal{I}^{sm}(k)$	SM input vector at time k, $\mathcal{I}^{sm} \in \mathbb{R}^{n_I}$
$u^{sm}(k)$	SM manipulated input vector at time k, $u^{sm} \in \mathbb{R}^{n_u}$
$d^{sm}(k)$	SM measured disturbance vector at time k, $d^{sm} \in \mathbb{R}^{n_d}$
$y^{sm}(k)$	SM output vector at time k, $y^{sm} \in \mathbb{R}^{n_y}$
$y^{sm}(0)$	SM output vector at initial condition
$x^{sm}_{min}, x^{sm}_{max}$	State variables limits
$u^{sm}_{min}, u^{sm}_{max}$	Manipulated variables limits
$y^{sm}_{min}, y^{sm}_{max}$	Outputs limits
A^{sm}	SM state-space states modeling matrix, $A^{sm} \in \mathbb{R}^{n_x \times n_x}$
Γ^{sm}	SM state-space input modeling matrix, $\Gamma^{sm} \in \mathbb{R}^{n_x \times n_I}$
B^{sm}_u	SM state-space manipulated input modeling matrix, $B^{sm}_u \in \mathbb{R}^{n_x \times n_u}$
B^{sm}_d	SM state-space measured disturbances modeling matrix, $B^{sm}_d \in \mathbb{R}^{n_x \times n_d}$
E^{sm}_v	SM state-space grid interconnection modeling matrix, $E^{sm}_v \in \mathbb{R}^{n_v \times n_u}$

C^{sm}	SM state-space output modeling matrix, $C^{sm} \in \mathbb{R}^{n_y \times n_x}$
$x_{\mathcal{O}}^{cm}(p)$	CM state vector at time p, $x_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{x_{\mathcal{O}}}}$
$\mathcal{I}_{\mathcal{O}}^{cm}(p)$	CM input vector at time p, $\mathcal{I}_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{I_{\mathcal{O}}}}$
$u_{\mathcal{O}}^{cm}(p)$	CM manipulated input vector at time p, $u_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{u_{\mathcal{O}}}}$
$d_{\mathcal{O}}^{cm}(p)$	CM measured disturbance vector at time p, $d_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{d_{\mathcal{O}}}}$
$u_{\mathcal{O}}^{sh}(p)$	Interconnected coupled areas tie-line power vector at time p, $u_{\mathcal{O}}^{sh} \in \mathbb{R}^{n_{v_{sh}}}$
$y_{\mathcal{O}}^{cm}$	CM output vector at time p, $y_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{y_{\mathcal{O}}}}$
$y_{\mathcal{O}}^{cm}(0)$	CM output vector at initial ccondition
$A_{\mathcal{O}}^{cm}$	CM state-space states modeling matrix, $A_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{x_{\mathcal{O}}} \times n_{x_{\mathcal{O}}}}$
$\Gamma_{\mathcal{O}}^{cm}$	CM state-space input modeling matrix, $\Gamma_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{x_{\mathcal{O}}} \times n_{I_{\mathcal{O}}}}$
$B_{u_{\mathcal{O}}}^{cm}$	CM state-space manipulated input modeling matrix, $B_{u_{\mathcal{O}}}^{cm} \in \mathbb{R}^{n_{x_{\mathcal{O}}} \times n_{u_{\mathcal{O}}}}$
$B_{d_{\mathcal{O}}}^{cm}$	CM state-space measured disturbances modeling matrix, $B_{d_{\mathcal{O}}}^{cm} \in \mathbb{R}^{n_{x_{\mathcal{O}}} \times n_{d_{\mathcal{O}}}}$
$E_{v,\mathcal{O}}^{cm}$	CM state-space grid interconnection modeling matrix, $E_{v,\mathcal{O}}^{cm} \in \mathbb{R}^{n_{v_{\mathcal{O}}} \times n_{u_{\mathcal{O}}}}$
$E_{v,\mathcal{O}}^{sh}$	Interconnected coupled areas tie-line modelling matrix $E_{v,\mathcal{O}}^{sh} \in \mathbb{R}^{n_{v_{sh}} \times n_{u_{\mathcal{O}}}}$
$C_{\mathcal{O}}^{cm}$	CM state-space output modeling matrix, $C_{\mathcal{O}}^{cm} \in \mathbb{R}^{n_{y_{\mathcal{O}}} \times n_{x_{\mathcal{O}}}}$
$J^{sm}, J_{\mathcal{O}}^{cm}$	SM and CM objective function
$e^{sm}, e_{\mathcal{O}}^{cm}$	SM and CM reference tracking error
R^{sm}, R^{cm}	SM and CM reference

$\Delta u^{sm}, \Delta u_{\mathcal{O}}^{cm}$	SM and CM ramping rates
$\omega^{sm}, \omega_{\mathcal{O}}^{cm}$	SM and CM objective function weighting coefficients
$\delta u_{t,\mathcal{O}}^{cm}$	CM target tracking error for area $\mathcal{O}$
P_L, P_{shd}	Demand and load shedding power
P_{re}, P_{cur}	Renewable output and curtailment power
P_{cg}	Conventional generation output power
E_{eq}, Z_{eq}	Nanogrid Thevenin equivalent voltage and impedance
V_{ngi}	The converter output voltage of i^{th} nanogrid
I_{ngi}, P_{ngi}	Converter output current and power of i^{th} nanogrid
V_{dc}	DC voltage at PCC of DC distribution
C	Overall equivalent capacitance at PCC
I_{Tr}, P_{Tr}	Transmitted power from the interconnected nanogrids cluster at PCC
R_i, L_i	Resistance and the inductance of the interlinking converter filter
$\Delta V_l, I_l$	the distribution voltage drop and current of l^{th} segment.
R_l, L_l	Resistance and the inductance of distribution l^{th} segment.
P_{loss}	Total power losses of the interconnected nanogrids cluster
r_i	Sharing factor of i^{th} nanogrids
r_{rule}	Sharing factor rule at PCC that submitted to the leader agent
A	The adjacency matrix of the communication graph $\mathcal{G}$
D	In-neighbors degree matrix of the graph $\mathcal{G}$
x_i	State of i^{th} agent that needed to achieve the consensus
$\mathcal{L}$	Laplacian matrix of the graph $\mathcal{G}$ for certain adjacency matrix

B	pinning matrix of the selected leader
ψ	Change in Laplacian matrix due to the attack
u_i	consensus control law of i^{th} node
$\varphi_{V_{ngi}}$	Secondary control local objective of i^{th} nanogrid
φ_{r_i}	global distribution cluster objective of i^{th} nanogrid
$k_p^{V_{ng}}, k_I^{V_{ng}}$	proportional and integral gain of the secondary control PI voltage control
k_p^P, k_I^P	the proportional and integral gains of the secondary control PI sharing factor control
k_{Ptr}, k_{Vdc}	the proportional gain of the PCC power and voltage tertiary control
$P_{ngi,max}$	Maximum power sharing of i^{th}nanogrid
t_a	Cyber-attack time
θ_a	Cyber-attack discrete signal
u_a	Cyber-attack false data injection
k_a	Cyber-attack gain
$\widetilde{u_i}$	Control law of i^{th} node under cyber-attack
f	The signal under MM processing
g	Probing set of MM structuring element
$\oplus$	MM dilation operation
$\ominus$	MM erosion operation
∇_{mmg}^{w}	Morphological gradient of w^{th} level
ρ	Cyber-attack detection threshold

Q_b, Q_{sc}	Battery and supercapacitor capacity
R_b	Battery internal resistance
R_{ssc}, R_{psc}	Supercapacitor series and parallel internal resistances
C_{sc}	Supercapacitor capacitance
R_{Lb}, R_{Lsc}	DC/DC converter inductor resistance
L_b, L_{sc}	DC/DC converter inductor inductance
C_{ib}, C_{isc}	DC/DC converter input capacitance
C_{ob}, C_{osc}	DC/DC converter output capacitance
R_{kb}, R_{ksc}	ESS module – MVDC bus link resistance
L_{kb}, L_{ksc}	ESS module – MVDC bus link inductance
D_b, D_{sc}	Steady-state ESS converter switching duty
$\bar{V}_b, \bar{V}_{sc}$	Steady-state ESS module output voltage
$\bar{I}_{Lb}, \bar{I}_{Lsc}$	Steady-state ESS module inductor currents
$\delta I_{Lb}, \delta I_{Lsc}$	Small-signal ESS inductor currents
$\delta V_{ib}, \delta V_{isc}$	Small-signal ESS input voltages
$\delta V_b, \delta V_{sc}$	Small-signal ESS output voltages
$\delta I_b, \delta I_{sc}$	Small-signal ESS output currents
$\delta SOC_b, \delta SOC_{sc}$	Small-signal ESS State-of-Charge
δH_{sc}	Supercapacitor small-signal voltage
$\delta D_b, \delta D_{sc}$	Small-signal converter switching duty
δV_{dc}	Small-signal MVDC bus voltage
τ_e	Generator exciter time-constant

R_f, L_f,C_f	Generator equivalent circuit resistance, inductance and output filter capacitance
R_{kg}, L_{kg}	Generator – MVDC bus link resistance and inductance
δE_d, δI_d	Small-signal generator equivalent electromotive force and armature current
δV_g, δI_g	Small-signal generator output voltage and current
$\delta \psi_f$	Small-signal generator rotor flux linkage
I_{CPL}, P_{CPL}	Steady-state constant power load current and power
R_{CPL}^0	Initial constant power load equivalent negative resistance
I_{PL}, P_{PL}	Steady-state pulsed load current and power
I_{CL}, R_{CL}	Steady-state constant impedance load current and power
C_{link}	MVDC bus link equivalent capacitance
δI_{PL}, δI_{CL}	Small-signal pulsed load and constant impedance load currents

Chapter 1 Introduction

Large scale penetration of renewable energy in the distribution grid enhances the smart grid flexibility, energy market reliability and greener communities. To integrate a larger share of renewables in the distribution network, intelligent distributed microgrids must be designed to integrate the distributed generators, distributed storage systems and smart loads into the future smart grid [1], [2]. That requires reliable, resilient, secured, reconfigurable and intelligent control and management architectures.

The current architecture of the power system control and management was built based on centralized architectures and algorithms [3], [4]. The growth of distributed energy resources (DERs) deployment enforces the power system to depend mainly on the distributed control/management algorithms. Shifting the power system from bulky centralized generation, single-way power flow and passive distribution network design toward distributed generation, two-way power flow and peer-to-peer active distribution design impose many complexities and challenges in the power system operation and control [5]. This shift transformed the grid decision making infrastructure into distributed control architecture, which despite its benefits, it causes security, resiliency, and efficiency issues. The cooperative networked microgrids can support the grid by voltage regulation, feeder decongestion, efficiency improvement and market transactions improvements via making a consensus on a certain control/optimization objective using the secondary distributed control architecture [6], [7].

The main drawback of distributed algorithms is their dependence on limited peer-to-peer information broadcast. Each controller or manager is implemented locally to satisfy a

certain local objective and is limited when it comes to the global objective, which is transmitted by only the information from its neighbors [3], [5]. On one hand, the local objective can be satisfying the local energy balance, local voltage stabilization, or maximizing the local profits. On the other hand, the global objective can be equal power-sharing among different DERs, voltage stabilization at the point of common coupling (PCC), or synchronizing distributed energy entities.

The distributed control systems (DCSs) use the local measurements of each agent and its correlated neighbors to estimate its new control/management objective. To estimate the updated control law, the consensus algorithm was utilized. The consensus algorithm (protocol) aims to make the distributed control/management agents reach an agreement on a transmitted message if there is a central authority (leader) or reach an agreement on an average quantity if the system is fully distributed [8], [9].

Creating a flexible active distribution network depending on the networked microgrids increases the complexity of the energy cyber-physical system and impose many challenges and threats against reliable operation. The fully distributed decision-making infrastructures lack the global vision, which makes the control system unable to deal with not only the uncertainty and the variability of the renewable resources but also it makes the system cannot handle unexpected emergencies [10]–[12]. Also, the missing of the centric oversight due to the distributed control reduces the hosting capacity of the renewable resources, cause inefficient operation of the energy storage and impact the overall system situational awareness [3], [5].

The widespread use of networked controllers, and networked sensor in the energy cyber-physical system creates avenues for security threats and many back doors for cyberattacks. In the distribution system, the system is very vulnerable to be compromised by attackers because of the low-security level. Compromising a control agent or a sensor for a single microgrid can disturb the control law and degrade the active distribution network operation, which eventually can interrupt the power and dismantle the distribution feeders into isolated islands. The distributed microgrid infrastructure could be affected by many types of vulnerabilities as false data injection attacks and denial of service attacks. The attack can be launched on the communication link among the controllers, sensor links or on the controller itself [11]–[16].

To enhance networked microgrid security, two solutions can be utilized. The first one is the Information Technology (IT) based security solutions that focuses on data encryption, authentication, key management, and privacy preservation. The second solution is redesigning the control system to be resilient against cyber-attacks. To address these problems, a centric oversight is required to support the cyber-physical system by the effective operation guidelines, authenticate the control agents' activities and enhance the system observability [11].

1.1 Distributed Microgrids in Smart Grid

The NMGs is shaping the modern smart grids by impacting the grid from the level of distribution up to the bulky generation level. The microgrid as a physical system is defined as an autonomous small power system that controls, optimizes and manages the distributed resources, energy storage and the various types of loads within a distinct electrical

boundary [17]–[20]. The scale and the capacity of the microgrids can be wildly classified according to the distributed grid levels from milligrid (MV level) through microgrid to the nanogrid (LV level).

As shown in Figure 1.1, the networked microgrids (NMG) defined as the aggregation of interconnected microgrids to transform the distribution system into virtual power plants. The NMG can be based on the rooftop and community-scale solar systems attached with storage system up to a larger capacity and different type of resources as an industrial microgrid. The NMGs are highly reconfigurable as a physical system and they can work in the grid-connected or the islanded modes. The cyber system of the NMGs includes complex, large-scale, wide-spread heterogeneous and spatially controllers, sensors, computation, communication links, communication middleware, which in spite of its capabilities and benefits, has many challenges and drawbacks [20].

One of the basic and vital physical components in the NMGs is the power electronic inverter/converter. The dynamic interaction among resources, storage systems, loads or generally among microgrids is mainly dependent on the inverters. The active distribution network voltage regulation, the power sharing among energy units and the power dispatch are controlled via the networked inverters [19]. By using power inverters to interconnect such DERS, microgrids, the system reliability, stability, and power quality can be improved. The high-capacity addition of power electronic inverters in microgrids, that influence advanced software-concentrated controllers and communication topologies, makes them vulnerable to cyber-attacks. Since the future distribution system depends

mainly on the power electronics inverter, and data corruption can disrupt the interconnected inverter wide-area stability and synchronization.

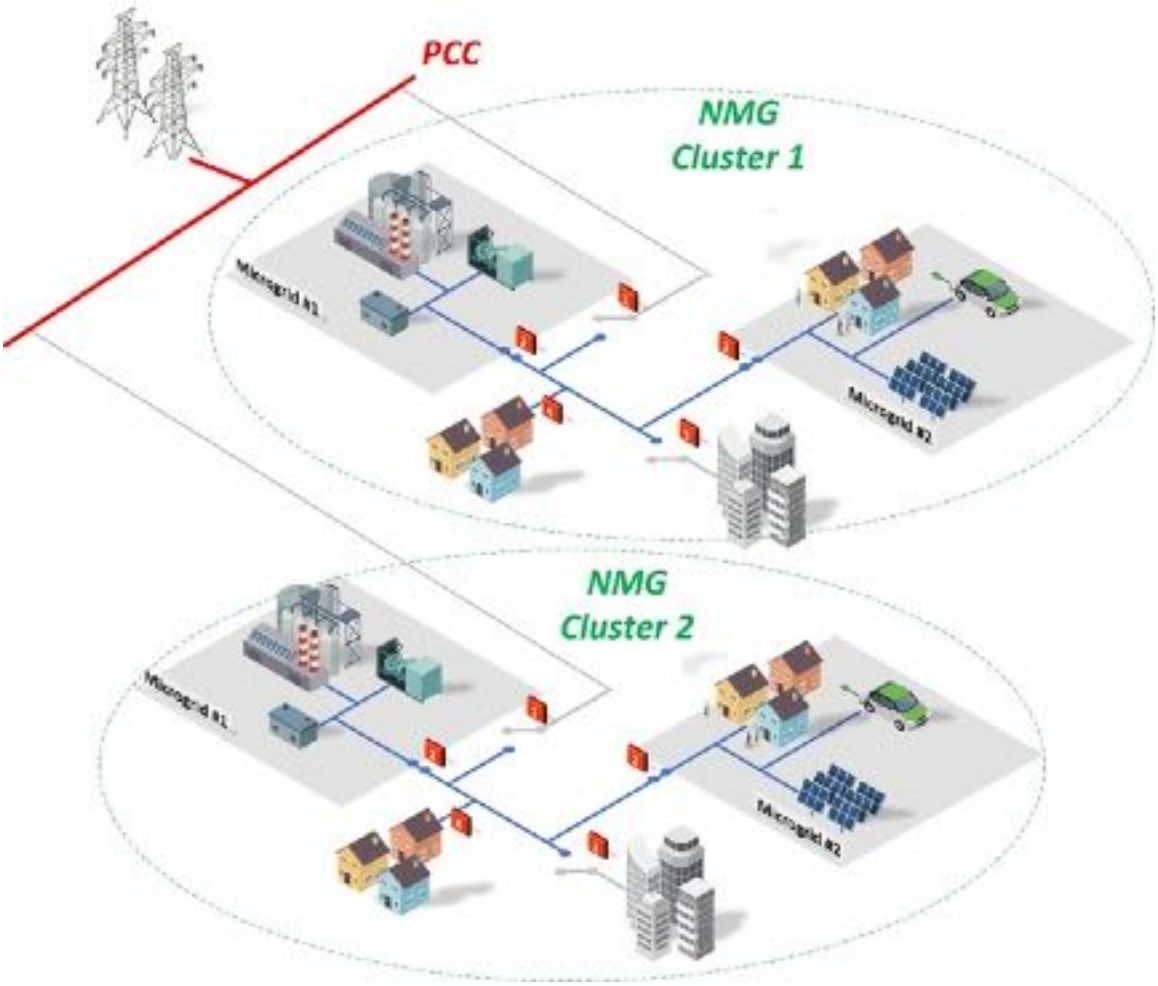


Figure 1.1: Networked microgrid infrastructure.

The NMGs benefits can be achieved by a well-designed control/management methodology. The energy generation shifted from one-way power flow into two-way power flow (from/to prosumer), from the centralized energy market into a free distributed market. In addition, the geographical distribution of the DERs encourages the trend of distributed decision-making architecture.

1.2 Microgrids control architectures

In the wide-plant systems, the control system can be classified into three architectures (centralized, decentralized and distributed) control. As shown in Figure 1.2, the centralized controller gets the entire feedback information of the physical system and apply the control law then it sends the control actions back to the system actuators. In the decentralized approach, the system has many controllers, which work independently using only the local information to make the decisions. In the distributed architecture, the system is divided into many cooperating subsystems, each subsystem has its local controller but unlike the decentralized control system, each controller communicates with its neighbors to achieve the control objective. Table 1.1 contains a comparison between each control architecture with respect to the Pros and Cons [3].

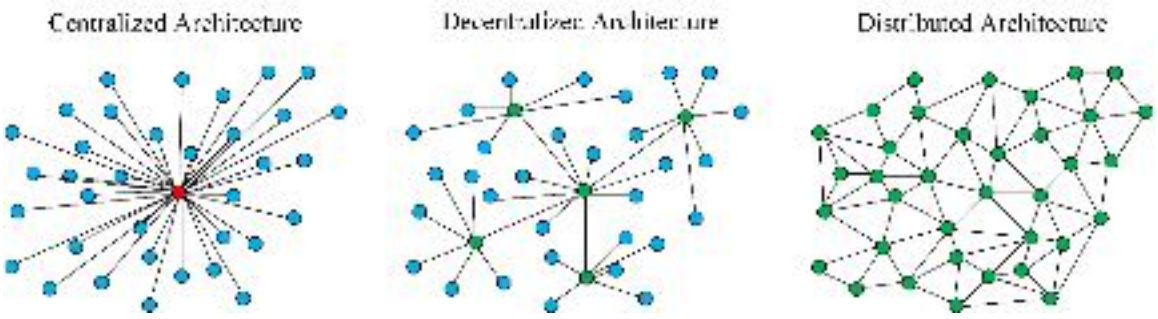


Figure 1.2: Control System architecture classification.

Usually, the NMGs control strategy has three fundamental roles; maintain the voltage and frequency stability, satisfy proper power sharing among MGs and achieve economic operation. To satisfy the previous objectives, a hierarchical control strategy is used. This strategy contains three layers (primary, secondary and tertiary) control [4]. The primary control layer applied locally and interact directly with the device (power electronics

converter) to respond to fast dynamics as load variation within milliseconds. It uses the droop control to set the reference voltage and frequency to the inner control loops and reduces the circulating current.

Table 1.1: A comparison between the control system architectures concerning the pros and cons.

	Centralized Control	**Decentralized Control**	**Distributed Control**
Pros	• Have better knowledge about the global system behavior (centric oversight). • Could achieve the best performance if it is applied properly.	• Less computational burden and enough flexibility. • Could work autonomously without communication (with local info only).	• Can behave close performance as centralized control and the closed loop stability is achievable. • Flexible, scalable, low bandwidth and less computational requirement.
Cons	• Suffer from a single point of failure. • Sophisticated control design. • Requires high communication bandwidth and computation burden. • lacks scalability, successful attack leads to catastrophic damage.	• Bad control performance. • Cause unstable behavior of the global system due to the lack of coordination. • Optimal global objective cannot be satisfied.	• Vulnerable to cyber-attacks. • Lacks the robustness with the existence of the data uncertainty or communication failure. • Lacks for centric authority (no agent aware about the overall environment).

The main purpose of the secondary control layer is to regulate, restore, synchronize the voltage and the frequency. It has a slower response as compared with the primary control layer (in seconds). For the purpose of economic operation, optimal power flow and utility integration, the tertiary control layer is designed.

Considering the control system architecture, the primary control is a local decentralized autonomous control. The secondary control layer can be built based on centralized or distributed control architecture. Also, the tertiary control layer can be a centralized or distributed structure. In the NMGs operation, the distributed secondary cooperative control is applied among the adjacent microgrids. The secondary control agents in each microgrid can share/collect information from the other microgrids to coordinate the operation for the overall active distribution network. To aggerate the benefits of the NMGs, the secondary and tertiary control layers should coordinate by forming a networked cooperated distributed control system [6], [21].

1.3 Networked Microgrid Control Challenges and Requirements

The dependence on the distributed control/optimization although its benefits created many challenges and issues that characterized by the distributed architecture nature. The fully distributed approach cannot satisfy the global objective because it has limited local and neighboring information only. That could impact the efficient operation and magnifying the uncertainty effect on the entire system operation. For instance, the renewable variability and uncertainty can disturb the distributed energy management by taking improper decisions that reduce the hosting capacity of the renewables. Also, the distributed controllers cannot be well-coordinated since it does not have the global

information in a centric place, which easily cause achieving a suboptimal solution [14], [16], [22]. A centric guide is required to support the multiagent controllers with global optimal guidance.

The security threats are extremely high in the distributed systems especially the large-scale distributed decision making in the active distribution grids. By compromising a single agent or multi-agents in the distributed control system can disturb the control law. Therefore, this movement to the networked multi-agent systems requires security-aware controllers to be resilient against a cyberattack or failure wither on the controller itself or the communication among the agents. To provide the NMGs with the required level of guidance, situational awareness, optimality rules and security insights, a data-centric entity should be present. Also, the distributed controller should have the ability to change the mode of operation by depending only on the local information in case of a complete failure in the communication network. It should respond autonomously to the cyber or the physical contingency event by reconfiguring the control algorithm and work independently.

These previously discussed challenges require the existence of a central authority that can provide the data centricity but how to add this capability without suffering from the centralized architecture drawback that is the question.

1.4 Problem statement

Today, the energy world is moving rapidly from centralized power plants based on fossil fuels to distributed virtual power plants based on renewable energy resources (RES). As the penetration of RES rises in the grid, many challenges such as variability and uncertainty in the grid appear. These challenges create difficulties in the power system

operation and control of frequency, voltage, and congestion. To integrate a high share of RES, the distributed renewable energy utilization represents a flexible and reliable solution to enhance RES dispatchability [1]. The emergence of distributed energy resources (DER) in the form of the interconnected microgrid and nanogrid clusters introduce an incentive to the customers to be prosumers. It also create peer-to-peer transaction power trading. Although the high performance of centralized control and optimization solutions has high complexity, low reliability and lacks scalability for further expansion [5]. Moreover, centralized control systems has high computational and communication burden and poor fault tolerance capabilities. Motivated by the inherently distributed nature of DERs, networked cooperative control systems are receiving a wide attention from researchers [14]–[16], [21], [23]–[26]. This only needs local communications links among neighbors to achieve control, optimization or management objective..

The distributed control and management frameworks are more flexible, scalable, reliable and resilient, which results from the controllability redundancy and smart control algorithms [5], [25], [26]. Many power system controllers, optimization algorithms and management strategies are shifting to be in the distributed architecture for making the decisions. For example, distributed economic dispatchers, optimally distributed energy management systems, cooperative control, and optimization and load shedding algorithms. Notwithstanding the advantages of the distributed cooperative control systems and their emerging applications. These frameworks lack the robustness with the existence of data uncertainty. The distributed energy control and management systems increase the vulnerability of the interconnected smart grids to adversaries and communication failures

[5]. Due to the absence of a central supervisor, the distributed systems face the risk of cyber-attacks. In addition, due to the cooperative nature of making a control decision, the optimal control objective cannot be satisfied, lose the interconnected power systems synchronization and eventually expose the multi-agents system to instability. There are many malicious attacks that can threats the distributed networked control system; as availability attack in form of Denial of Service (DoS), data integrity attack in form of the false data injection and conditionality attacks in form of violating privacy.

1.5 Research objective

The main objective of this dissertation is to provide secured cooperative control/management techniques to mitigate the cyber-physical attacks on the interconnected smart grids. The control and management should enhance the scalability, robustness, security, stability, coordination, and optimal operation of the cooperative control techniques for the interconnected smart grids as microgrid, nanogrids and virtual power plants (VPPs). In this paradigm, different control architectures as decentralized, distributed and hierarchically distributed should be redesigned to deal with the cyber-physical attacks and the data uncertainty [27]–[29]. The research question is how to merge the benefits of centralized, decenteralized and the distributed architectures by designing a data-centric layer. This will provide the distributed controllers with the centric oversight, guidance, awareness and global vision. Also, how can this platform avoid the drawbacks of the centralized structure. This platform should also consider the interdependences among the cyber communication, middleware, controllers, and the newly emerging physical system (as the interconnected power electronics devices). In the practical world

of the ECPS, what is the suitable system that can host this data-centric layer to guarantee the proper level of interoperability.

The digital twin is a precise cyber clone of the energy cyber-physical system that matches the same dynamics, features, and functionality of the system simultaneously in a virtual space. Digital twin computation components procedure data from the controllers, event log, sensors, forecasting data, and operational data to inform the physical systems about the findings, guidelines, global control objectives, predictive insights findings and anomaly detection to make necessary changes in the physical space or adapt system parameters if there is a necessity [30]–[35].

Therefore, a cloud-based digital twin that includes both the cyber and physical model will be implemented to watch and guide the distributed control layer. That will give a centralized oversight without increasing the communication and computational burden. In addition, coordinated defense mechanisms should be embedded in the distributed controllers and distributed observers to support the global control/management objective. Both the digital twin and the distributed controllers should watch each other and guarantee overall security and mitigation against an attack or data uncertainty. In light of the internet of things (IoT) technologies, security-aware control systems should be provided with aid data and model identification to ensure safe and stable system operation [34]. The developed security-aware control systems and the data-distribution service (DDS) will be introduced as the digitized integrated solution for the newly constructed peer-to-peer energy systems. The experimental validation will be provided to evaluate the different control and management systems.

The major objective of this dissertation is to change the classical vision to power system control by shaping the future distributed decision-making system. The purpose is to shift the classical control infrastructure from a short vision for a single operation state into a multi-vision considering the future state of operation and the historical experience. Figure 1.3 shows the vision of the developed system in this dissertation.

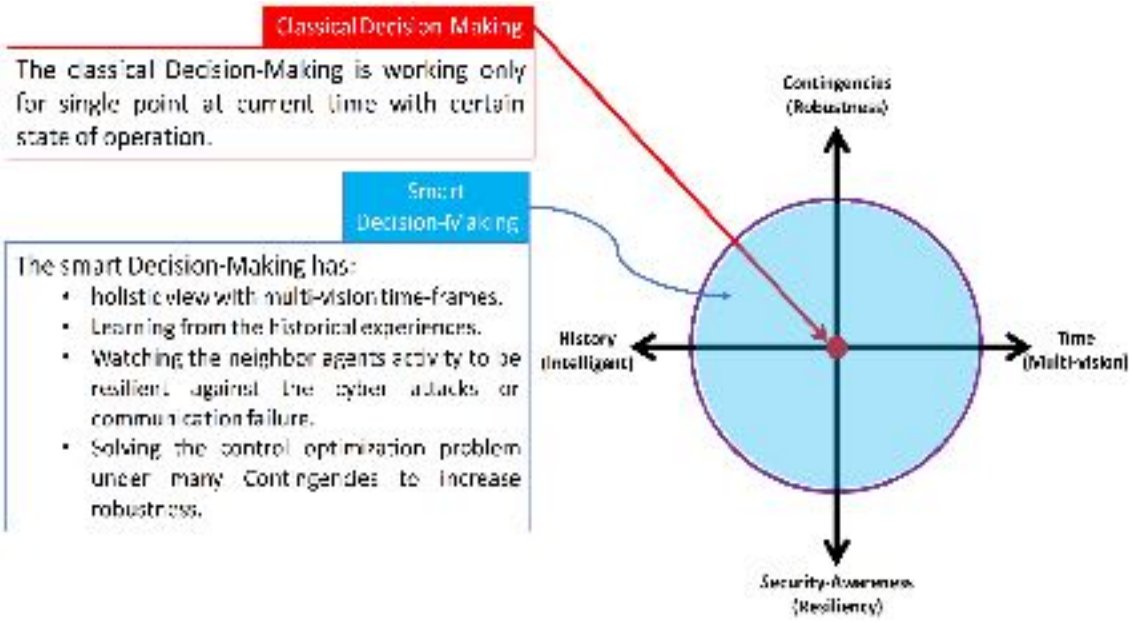


Figure 1.3: Migration from classical decision-making to smart decision-making.

The research problem will focus on:

- Developing a coordinated multi-layer energy management system for integrating a high penetration of renewable resources in the interconnected smart grids to enhance robustness and security while maximizing profit.
- Developing a decentralized control system to enhance the voltage stability, proper power-sharing, and resilient operation for DC microgrid/nanogrids.

- Achieving cyber-physical attack mitigation via designing digital twin-based cooperative control and optimization techniques for the interconnected smart grids.
- Utilizing the Internet of Things (IoT) technologies and the data-driven digital twin approach to design a security-aware distributed control strategy for the interconnected microgrids/nanogrids clusters.
- Validating and evaluating the developed control and energy management systems experimentally using cyber-physical test-bed systems.

1.6 Original contribution of this dissertation

The original contribution of this desertion is to develop novel methodologies that utilize digital transformation (Industry 4.0) to integrate the distributed generation/storage, secure transactive energy management/control and achieve resilient risk management. To accomplish this goal, a comprehensive study of the future requirements of the active distribution grids control, optimization, management, and communication is achieved. The main objective of the study is to investigate how the future distribution network will depend on the digital transformation from the level of the building (networked nanogrids) to the level of the primary distribution system (networked microgrids). Although the digital transformation will bring benefits to the energy infrastructure for both the utility and the consumer, it will create many challenges such as dealing with high share renewables and expose the widespread networked sensors/controller to cyberattacks.

Firstly, a study is performed to decide what is the proper decision-making architecture that can enhance the distributed microgrid resiliency, reliability, observability and security.

Since the digital transformation will convert the distribution system into a distributed infrastructure, the study proved that merging the performance of the centralized control architecture and the flexibility of the distributed control architecture can lead to an integrated control system with the full benefits and without the drawback of both architectures. This integrated control system is named the hierarchically distributed control system. It keeps the feature of the distributed networked control system and adds a data-centric layer on top. Data centricity can be achieved easily thanks to digital transformation technologies like the internet of things (IoT), cloud computing and communication middleware. The cloud computing capability and the availability of the data gives the dynamic model the ability to implement the Digital Twin (DT) of the energy cyber-physical system. To address the future Industry 4.0 requirements, the developed architecture is shaped, designed, formulated, implemented, tested and verified.

After building the foundation of the DT of the ECPS, the DT shadow is formulated, described and implemented on the cloud system. Also, a generic standard was developed to put the rules of the data-driven dynamic model that can use the asset shadow to be the life replica of an asset. Both the cyber model and the physical model of the ECPS are developed. Furthermore, the DT model is classified into fast dynamics and slow dynamics DTs to serve different applications.

To enhance the intelligence of the DT, the DT constructor engine was developed to automatically construct the custom DT according to the application in real-time. Since the practical implementation is vital to prove the validity of the developed technique, a practical environment was designed and implemented on the cloud to be the DT playground

that can help the grid operator/planner to test, validate and deploy future application, solution and/or study.

To test and verify the developed platform, the Amazon Web Services (AWS) cloud system is used to implement the ECPS DT [36]. AWS, communication middle wares, embedded edge controllers and networked sensor are used to verify the platform effectiveness. Many solutions are introduced depending on the DT. The developed strategy expands the control time horizon into multiple visions to overcome the forecasting error in the high penetration of variable renewable energy resources forecasting error. An aggregated mathematical model using state-space representation is formulated in the cloud to implement the hierarchically distributed model predictive control system. The novelty in the develped model is the concentration on the holistic optimal cost-effective operation of the grid in the first layer and ensuring the robust solution against the high variability of RES in the smaller areas. The data-centricity based DT is utilized to guarantee an effective operation of the renewables with maximum profit, less cost, maximum renewable utilization, and minimum load shedding under high uncertainty level. The DT gives the power system area's coordination managers that are distributed in the lower layer the centric oversight and guided it to the global optimality.

Also, the energy management system was made to be adaptive with different operation plans that can work autonomously according to the system state of operation wither in normal operation or under emergency. The technique used data centricity and the Analytical Hierarchy Process (AHP) to dispatch the resources and the ESSs for safer and reliable operation.

The work in this dissertation utilizes centric oversight to watch the distributed control system activity to detect, identify and mitigate the cyberattack on the NMGs control system. The DT based solution is utilized to watch the multi-agent control system reported activities. The DT platform on the cloud generates parallel data-informed models to estimate the cyber-physical system states and sort their residues. Then, a conflict logic algorithm detects and identifies the attack/failure. In the control layer, a modified consensus algorithm uses the updated desired control objective and the confirmed failure/attack to mitigate the global control objective. The developed method was able to discover and mitigate multi-coordinated cyber-attacks.

Because failure is not an option in some energy infrastructure, the dependence on the centralized DT is not 100% safe to guarantee resiliency. Without centralized oversight, the distributed control system should be designed to be security aware. In this dissertation, we designed a digital processing-based observer to extract the cyber graph dynamical characteristics for the neighbor agent's data and compare it with a pre-defined threshold. The system studied is an interconnected Nanogrids, which are coupled by a DC/DC converter to share the power and support the grid at the point of common coupling. The developed Mathematical Morphology (MM) processing technique was able to discriminate between the attacked and the healthy agents. The infected agent was excluded from the graph adjacency matrix to retrofit the consensus and achieve the control objective.

Finally, the distributed observer in previous work still depends on communication to prevent the misleading activity among the controllers. As a last defense, the distributed controller should be designed to work independently without depending on communication

to satisfy the control objective. For this dissertation, a decentralized small-signal model predictive control system was utilized to work with only the local information. MPC uses the small-signal model for prediction estimation. The MPC and its optimizer solve the problem to stabilize the voltage and maintain a proper power-sharing policy. It uses the local voltage information, filtration, and the system model to satisfy the control law without a cyber system.

1.7 Dissertation organization

This dissertation is organized in ten chapters, including this chapter, which introduces the literature review and identify the contributions of this dissertation.

Chapter 2 provides an overview of the cyber-physical system needs to data-centricity and the digital twin overall description. In addition, the foundation of the physical and the cyber asset's shadows, Industrial Internet of Things (IIoT) technologies and how it shapes the digital twin. The shadow state update time requirements are also discussed.

Chapter 3 provides the digital modelling for the cyber system, the physical system and their interaction. The chapter developed different types of models to cover most of the applications and solutions that are built based on the digital twin. Also, the models are designed to include both the fast dynamic and slow dynamic models to serve multi-time scale applications.

Chapter 4 presents the practical implementation of the digital twin platform to be the playground of the digital for real implementation. The chapter discusses how the Amazon Web Service (AWS), IoT technology, embedded computers, communication middle wares

and the main algorithms are implemented. A basic provisioning example is introduced for testing the overall system performance to shadowing multiple controllers from the edge control system to the cloud.

Chapter 5 introduces the first application/solution of the DT playground to improve the distributed management system in the smart grid operation. The chapter develops the DT playground as the centralized supervisory manager layer that guides the coordination managers (distributed decision-makers) to the global optimality. The chapter shows the usage of the hierarchically distributed model predictive control technique to achieve optimal and robust operation under high share renewables. The chapter concluded with the practical implementation of a practical smart grid testbed.

Chapter 6 extends the functionality of the energy management system by providing it with the ability to adapt automatically according to the power system status (normal operation, emergency operation or user-defined plan). The chapter introduces also the analytical hierarchy approach to perform the changes in real-time. Two scenarios are states to validate the performance of the developed strategy.

Chapter 7 addresses the utilization of the DT centric oversight to secure the networked microgrids control system against cyberattacks. The chapter introduced how the DT constructor generates the physical and cyber systems twins. Also, the chapter states the usage of the Luenberger observer to estimate the states and calculates the residues. Then, a detailed discussion is done to explain the cooperative algorithms on both cloud and edge controllers. Finally, the solution is validated by experimenting with two different types of attacks on different distributed controllers.

Chapter 8 provides the solution of the mathematical morphology based distributed observer to extract the cyber graph features and discriminate between the healthy and the infected control agents. The chapter starts with an overview of the networked nanogrids architecture alongside its control system layers. The chapter also introduced the mathematical morphology formulation and presented how it can be implemented to detect and identify the compromised agent. Finally, different types of a cyberattack are emulated to test the effectiveness of the defense mechanism.

Chapter 9 adds the last line of defense be designing an autonomous decentralized and independent control strategy, which depend only on the local information without communication. The chapter discusses the ability of the developed resilient controller to manage the energy storage operation even under the full absence of the communication network. This method is applied in a critical power system (MVDC shipboard power system). The small-signal model predictive control is presented after the onboard energy units' models. Finally, the strategy is validated by testing the controllers under normal operation and critical mission operation.

Chapter 10 concludes with a summary of the dissertation outcomes, the significance of this research as well as recommendations for future work related to its topic.

Chapter 2 Cyber-Physical System Digital Twin Foundation

The future smart grid and smart cities will be extremely complex cyber-physical system (CPS). Many industrial, commercial, and residential systems are going toward implementing networked controllers, sophisticated sensors and embedded Artificial Intelligence devices. This emerging CPS creates new avenues for not only improving this wide-area interconnected systems but also creates new solutions, better understanding and even new markets [37], [38].

The IoT infrastructure can provide better capabilities to the smart interconnected systems such as smart cities, intelligent transportation, smart power grid and even the healthcare system. Although the benefits of the IoT, it has many challenges that are resulted from huge data to collect, handle and process. To deal with such huge data and make it informative, a data centricity platform should be shaped. The management of the IoT data is a key element to leverage the benefits. This can include data aggregation, processing, computation and making insightful decisions [39], [40].

2.1 Cloud Aided CPS

In industrial systems as the energy sector, IoT technologies as smart sensors, networked controllers, embedded AI devices can make the operation of such systems autonomous, smart and efficient. Despite these abilities, the cloud computing platform is required to give centric oversight to the IoT networked devices. The cloud system can provide more flexibility, better scalability and huge computing abilities to the industrial CPS. For instance, the Electrical Vehicle (EV) industry requires regular healthy monitoring, maintenance services and software updates after-sale to guarantee safe operation and to

close the manufacturing cycle by improving the next production cycle. To do that, the cloud platform is a perfect unique solution. The integration between the IoT technologies and cloud computing attracted the attention of large companies like GE, Siemens, Tesla and IBM to push toward more solving research and development questions [41], [42].

The interaction between the IoT sensors, controllers, actuators and communication gateways that are built to introduce decision-making services for the physical system on one side with the cloud platform on the other side creates a new industrial revolution (Industry 4.0).

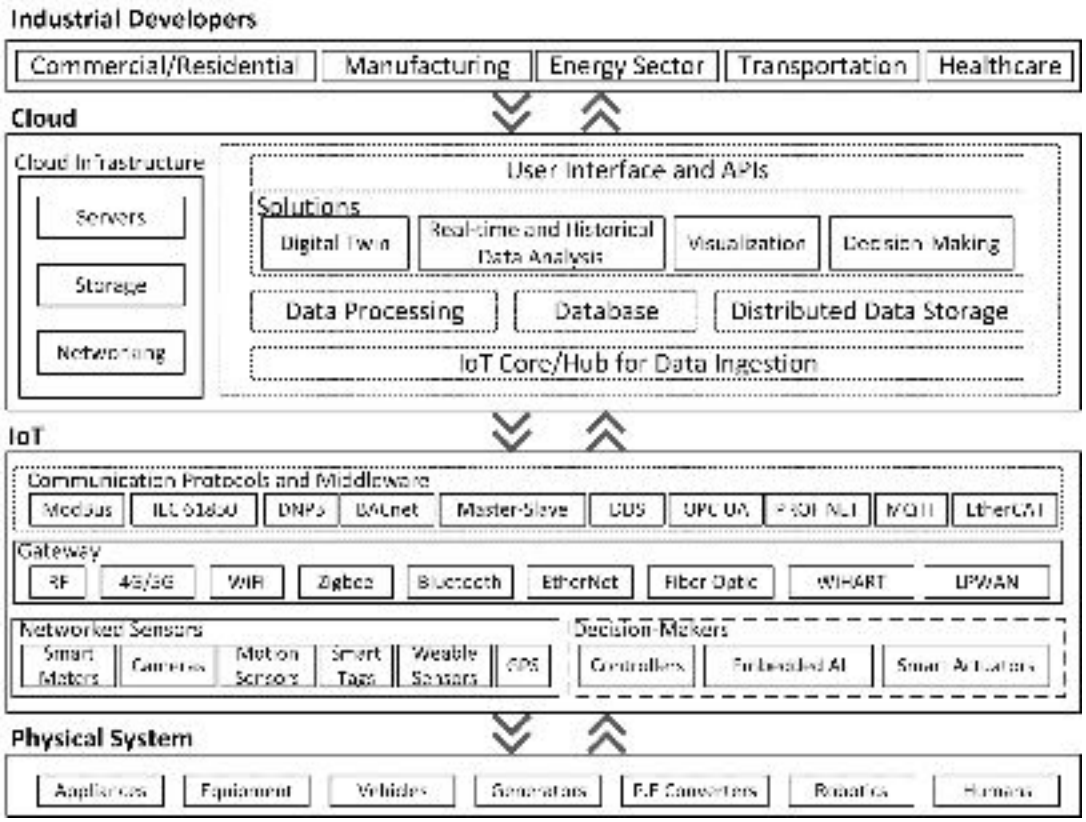


Figure 2.1: The networked cyber-physical system supported by IoT and cloud computing services.

Figure 2.1 shows the CPS that is shaped by the IoT and supported by cloud connectivity. As shown, the bottom layer is the physical assets as the appliances in the buildings, the equipment in commercial or industrial systems, vehicles in the transportation infrastructure, generators, and power electronics (P.E) converters in the energy sector and last but not least the humans/robotics everywhere.

The cyber system layer is on top of the physical system and can be classified into three main components: the networked sensor/decision-makers component, the communication gateways and the communication protocols/middleware. The networked sensors as smart meters, cameras, motion sensors, smart tags, GPS and wearable sensors for humans. The decision-makers can be summarized into the controllers, embedded AI or smart actuators. To interlink between these cyber assets, communication gateways that are based on a variety of communication infrastructure are utilized. These gateways can be radio frequency (RF), cellular (4G/5G), Wi-Fi, Zigbee, Bluetooth, Ethernet, Fiber Optic medium, Wireless Highway Addressable Remote Transducers (WiHART) or Low Power Wide-Area Network (LPWAN). For the purpose of the interface between the communication infrastructure and the software interaction, the communication protocols and middleware are utilized. In industry, the protocols/middleware such as ModBus, IEC 61850, DNP3, BACnet, Master-Slave, DDS, OPC-UA, PROFINET, MQTT and EtherCAT are utilized heavily and it can be selected according to the application [43].

The previously described layers of networked cyber-physical system are provisioned on the cloud system (virtual space) for data centricity-based insights. The cloud system has a physical system that host CPS, which includes the computing servers, storage systems

and physical networking. On the cloud physical system, the virtual platform is living, and it contains the IoT core/hub for data registration and ingestion. On top of the IoT core layer, the data can be routed to different services like data processing, database software, distributed data storage systems. Finally, the beneficial solutions and application that transform the data into useful information are hosted as computing services as real-time and historical data analysis, visualization, decision making. In addition, the digital-twin can be implemented to fuse the information from the data, examination, and the dynamic models to serve many other solutions as situational awareness, security auditing, guidance and running what-if investigations.

To leverage the full capability of the Cloud aided CPS, the cloud platform should be developed to have a set of application programming interfaces (APIs) to give the industrial developers in all domains the ability to build customized applications/solutions.

2.2 Networked CPS Digital Twin

The idea of the digital twin was firstly developed in 1970 by NASA during the Apollo 13 mission [44]. Recently, the great development and innovation in the domains of IoT, cloud computing, and big data encouraged many industries to utilize it for better handling with the data-centricity and the huge information availability. While the Digital Twin Consortium is working to standardize every aspect of the DT technology, it has many definitions. The DT is defined as the model that includes the last sensor information for matching a physical device. Also, it is defined as the virtual replicas/models of the physical object/thing.

In this thesis, we are putting the foundations to enhance the DT by including not only the physical replicas, which is defined previously but also by including the cyber system and its interaction with the physical system. The CPS digital twin can create a comprehensive digital clone of the CPS in the virtual space for better understanding the relationship between the large scale non-linear physical and cyber system.

To create a DT for a physical or cyber asset, the related data should be collected as the asset's states, manufacturing data and operation data. The output of the DT should replicate what could happen in the real world but cannot tell what's currently happening. The degree of the living model accuracy and complexity varies depending on the implementation of the model, what are the desired results and what is the application/solution that uses this DT. For instance, the DT of an ESS could mimic the state of charge (SOC) estimation with respect to the charging/discharging and how the SOC can be affected by temperature. On the other hand, the DT model is different if it is built to replicate the chemical reaction relation with the ramping rate abilities.

Generally, the digital twin model could combine CPS telemetry sensors, controllers' states, machine learning models and dynamic models. If the DT included only the last states of the controller/sensor, the DT called device shadow. Then, using shadow the dynamic model can be driven. Also, if the shadow states are stored in a database for a certain time horizon, the deep learning model can be supplied to predict a future state. Figure 2.2 shows how three modes of DT can be fused to make a decision. Then, the decisions can be sent to the IoT layer by updating the desired states portion in the shadow. The DT is an application-oriented platform. According to the required solution timeframe, the DT

timescale is defined. Some applications need to work in real-time by 1:1 ratio, another application can work on delayed decision-making and some applications require faster than real-time rates (prediction-based solutions).

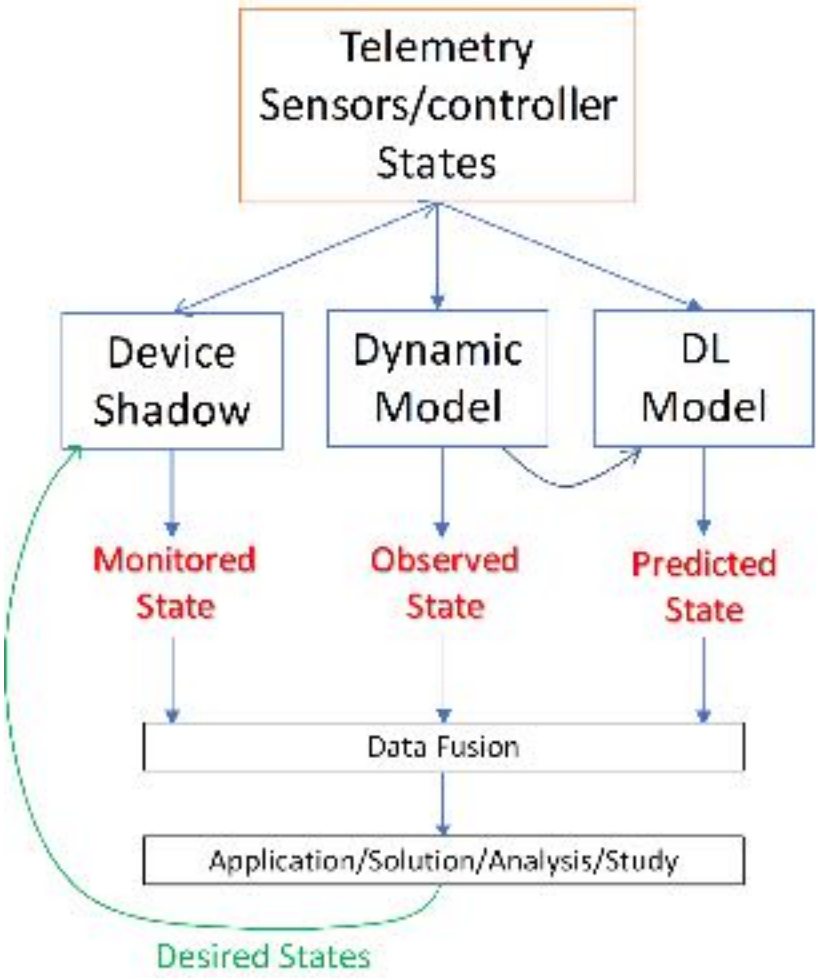


Figure 2.2: the CPS digital twin structure.

2.3 Digital Twin Elements

The DT was designed based on four main elements: the DT shadow, the DT models, the DT constructor and the DT playground. Figure 2.3 depicts the construction of the developed CPS DT. To represent a thing digitally in the virtual space, many immutable

and changeable attributes related to different aspects such as features, capabilities, structures, working states and operating conditions can be utilized to describe this thing.

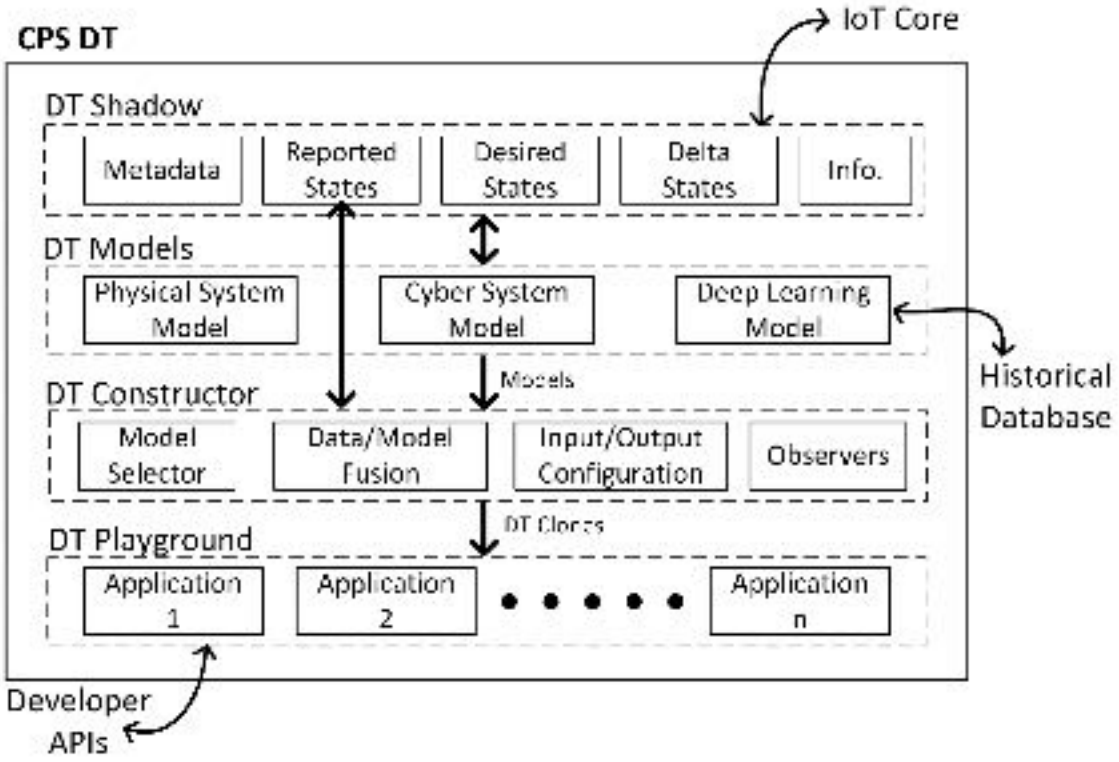


Figure 2.3: CPS DT Elements

2.3.1 DT Shadow

The DT shadow has the last status of the assets and it includes the asset's metadata, reported states, desired states, the delta states and generic real-time transaction information.

Shadow Metadata: A physical thing φ or a cyber thing θ has the metadata $\mathcal{M} = \{\rho_1, \rho_2, \ldots, \rho_{n_\rho}\}$ that contains a set of n_ρ immutable properties ρ. The metadata can include the manufacturer registration, design characteristics, standard limitations and the recommended rating conditions. For instance, a physical thing of DERs has power ratings,

ramping capabilities, thermal withstand characteristics, voltage limitations, manufacturing information, etc. Additionally, a cyber thing as the controller has specific bandwidth, data model structure, processing capabilities, functional blocks, etc. The knowledge of the metadata is vital for DT formulation, as it provides the virtual space with the ability to be aware of a thing's original specifications, which impact the physical thing's lifetime and the cyber thing's security.

Shadow Reported States: The information is collected from sensors and controllers to update the physical asset by setting the last reported set of states $x^{rep} = \{x_1^{rep}, x_2^{rep}, \ \dots, \ x_{n_x}^{rep}\}$, which contains n_x reported states for a thing.

Shadow Desired States: The target guidance states from the DT are recorded as the desired states in the shadow by setting the desired states $x^{des} = \{x_1^{des}, x_2^{des}, \ \dots, \ x_{n_x}^{des}\}$

Shadow Delta States: Some Applications requires recording the difference between the desired and the reported states $x^{\Delta} = x^{des} - x^{rep}$. The DT recognizes the reported state compliance with the desired state by calculating the difference between the desired state and the reported state.

Shadow Connectivity Information: The connectivity info includes the registration of the transaction between the asset and the cloud in real-time. It can include the shadow update version (sequence), the client token and the update timestamp.

2.3.2 DT Model

The DT model as stated previously can include the cyber model, physical model, and deep learning model. According to the solution requirements, the DT model type can be

defined. In addition, the application timeframe determines the need for the model resolution as the slow dynamic model or the fast-dynamic model. The DT model a set of parameters that map the relation between an input U that usually driven from the DT shadow or the database and an output Y that is estimated.

2.3.3 DT Constructor

According to the required DT solution, the DT can be automatically constructed. The DT playground sends a request to the DT constructor by defining the DT type, the input/output requirements and the timescale. The model selector chooses the required models that create the DT and then the input/output is configured by merging the models into one model. Finally, the model is automatically shaped as an observer for the full state estimation.

2.3.4 DT Playground

The DT playground is designed to be a programmable platform that can host the solution/application and have access to the DT shadows, models and the constructed DT clones. According to pre-developed APIs, the user/developer can build an application. The application can use one DT clone or multiple parallel clones in real-time based on the developer definitions.

2.4 Energy CPS Digital Twin

With the emergence of distributed energy resources (DERs), with their associated communication and control complexities, there is a need for an efficient platform that can digest all the incoming data and ensure the reliable operation of the power system. The digital twin (DT) can unleash tremendous opportunities and can be used at the different

control and security levels of power systems. The energy CPS digital twin can be implemented in real-time based on the internet of things (IoT) and cloud computing technologies.

One of these ECPS is the Future power distribution systems, which consists of multiple entities that interact with each other in real-time. The increased adoption of distributed energy resources and active prosumers in the power network will result in more data sharing and processing. A microgrid represents the basic building block of future power systems, where a microgrid's an agent/operator should ensure load-generation balance in its territory while interacting with other microgrids' agents or the distribution system operator [45]. From a holistic perspective, the future active distribution system can be viewed as a network of interconnected microgrids. The emergence of these interconnected microgrids can increase the efficiency of the system and ensure the reliable operation of the power grid during normal and extreme conditions. However, with such interconnected networks, there will be much more complexity, data communication and processing.

To mitigate these kinds of issues and to harness the usage of the insights available from the collected data, Industry 4.0 has emerged as the next industrial revolution, with the internet of things (IoT) and cloud computing as cornerstones of its deployment [46]. In that domain, many researchers have started to investigate the potential of IoT in different applications. Among these different applications is the energy-cyber-physical system. The deployment of IoT in that domain can be used to converge the current power system into the synergetic cyber-physical system that is the smart grid [47], [48]. In [49], IoT high-level framework for the design of information and communication technologies systems

for smart microgrids was developed. The authors described the different applications that can be realized when the power system becomes a part of an IoT framework, and the potential information flow associated with different applications.

Turning the current power grid into an IoT technology-dependent one means that many data are harvested from the physical assets' sensors and the cyber assets' controllers. This will greatly affect our current understanding of the energy sector [29], [33], [50]–[54]. An example of the sensors and data shared in a microgrid can be found in [55], where energy management as a cloud service was explored to provide a control platform for a residential microgrid. With the incoming stream of data and operational real-time requirements as well as the potential cyber-attacks on the communication network, there is a need for a conceptual framework that can monitor, collect, harness, and interact with the physical components to ensure their optimal operation. The digital twin (DT) concept arises as a promising solution that can provide such a framework and unleash many opportunities and gains that are associated with the flow of data and real-time interaction.

Many studies in the literature have started developing and describing conceptual designs and applications of digital twins. A description of the expected main building blocks for a general cyber-physical system was introduced in [56]. In [57], the authors presented a digital twin architecture for the security of an industrial automation system, where they developed a security-oriented digital twin for the Programmable Logic Control (PLC) software update process. In [31], the author provided a cloud-based digital twin for a cyber-physical system with an application to the social internet of vehicles for driving assistance application.

Few researchers have started to deploy and implement the digital twin for power system applications. To date, and to the best of our knowledge, there is not much literature that describes an actual design and implementation of a digital twin in the electric power-grid domain. In [58], the authors provided a general first-steps description of the implementation of a digital twin of a single microgrid. No details or implementation are provided. Therefore, this thesis tries to cover this gap by providing a detailed explanation and implementation of a low-cost, open-source-based and close-to-market proof of concept for a digital-twin framework for power system applications. The developed framework can be used in many applications of power systems, ranging from the simple monitoring of the system and actual control and interaction with the physical system to attack detection on the communication layer.

2.5 ECPS DT Architecture Description

In modern power systems, the microgrid is a vital infrastructure that enables higher renewables penetration in the deep distribution grid. The microgrid contains different distributed generation resources (DERs), energy storage systems (ESSs) and flexible loading, which transform the distribution grid into a fleet of virtual power plants. At this level of the networked microgrids, a huge number of assets, sensors, meters, actuators and controllers will be connected to the Internet through heterogeneous IoT communication networks. Figure 2.4 shows the developed cloud-based digital twin architecture, which could be the strategic technology that coordinates, facilitates, aggregates and provides centric oversight guidance for the new distribution system infrastructure. The developed digital twin is illustrated as a virtual replica for both the physical and cyber layers of the

networked microgrids. The physical layer consists of many assets (things) such as DERs, ESSs, fixed loads, flexible loads, DC/DC converters, DC/AC inverters, cables, transmission lines, transformers and circuit breakers. The power electronic converters are considered as the main vital actuators that fully control the distribution grid. It can flexibly route the power flow in the power lines and guarantee proper power-sharing among DERs and ESSs inside a microgrid or between the networked microgrids. The interconnected microgrids forms clusters that are connected to the power system point of common coupling (PCC) through an IC_{pcc} and a step-up transformer.

The edge cyber system space contains networked sensors/intelligent electronic devices (IEDs) that communicate with each other through an internet protocol such as transmission control protocol/internet protocol (TCP/IP). The sensors monitor the physical assets by widespread current transformers, voltage transformers, temperature and weather transducers, micro-phasor-measurement units ($\mu PMUs$), fault locators and protective relays. In addition, the cyber system makes decisions using the networked controllers as a distributed secondary control system that is responsible for voltage regulation, frequency synchronization, and active and reactive power sharing control. On top of the secondary controllers is the tertiary control system, which is responsible for energy management, market operations and the major global control/optimization object. The cyber control layer and its communication network take the power system automation control and protection decisions during the normal and abnormal conditions based on the feedback from the networked sensors. With this level of complex transactions among the cyber things and between the physical and cyber things, centric oversight is required to autonomously

monitor, operate, analyze and understand the cyber-physical energy system. The virtual space is developed as a centric oversight layer, which can deal with such complex systems using multiple coordinated cloud services.

The cloud system is utilized to implement the developed virtual space. The physical things are monitored by the sensors' measurements and hosted in the IoT core of the physical system. Regarding the control system in cyberspace, the controllers' states are hosted as cyber things in the IoT core. The last states of both the cyber and physical things are kept as a shadow on the cloud.

For both the cyber and physical things, a serviceless computing function—which is a low cost, simplified microservice—is used to monitor the data activity and take/activate local actions or launch another computing service/application according to pre-defined logic settings. The IoT shadow states are considered as the shadow twin for the energy cyber-physical system (ECPS). The shadow twin contains the metadata and the last states for the physical and the cyber assets. This shadow can be used for different power system applications, even with intermittent measurement updates. Additionally, the cyber twin state-space model and the physical twin state-space model are used to enhance the digital replica of the ECPS.

Multiple services are deployed to manage, filter, analyze and store data for better utilization among the energy system applications and solutions. The developed digital twins are cooperatively utilized to represent the actual ECPS, which could extend the virtual space capabilities for many different applications in the future.

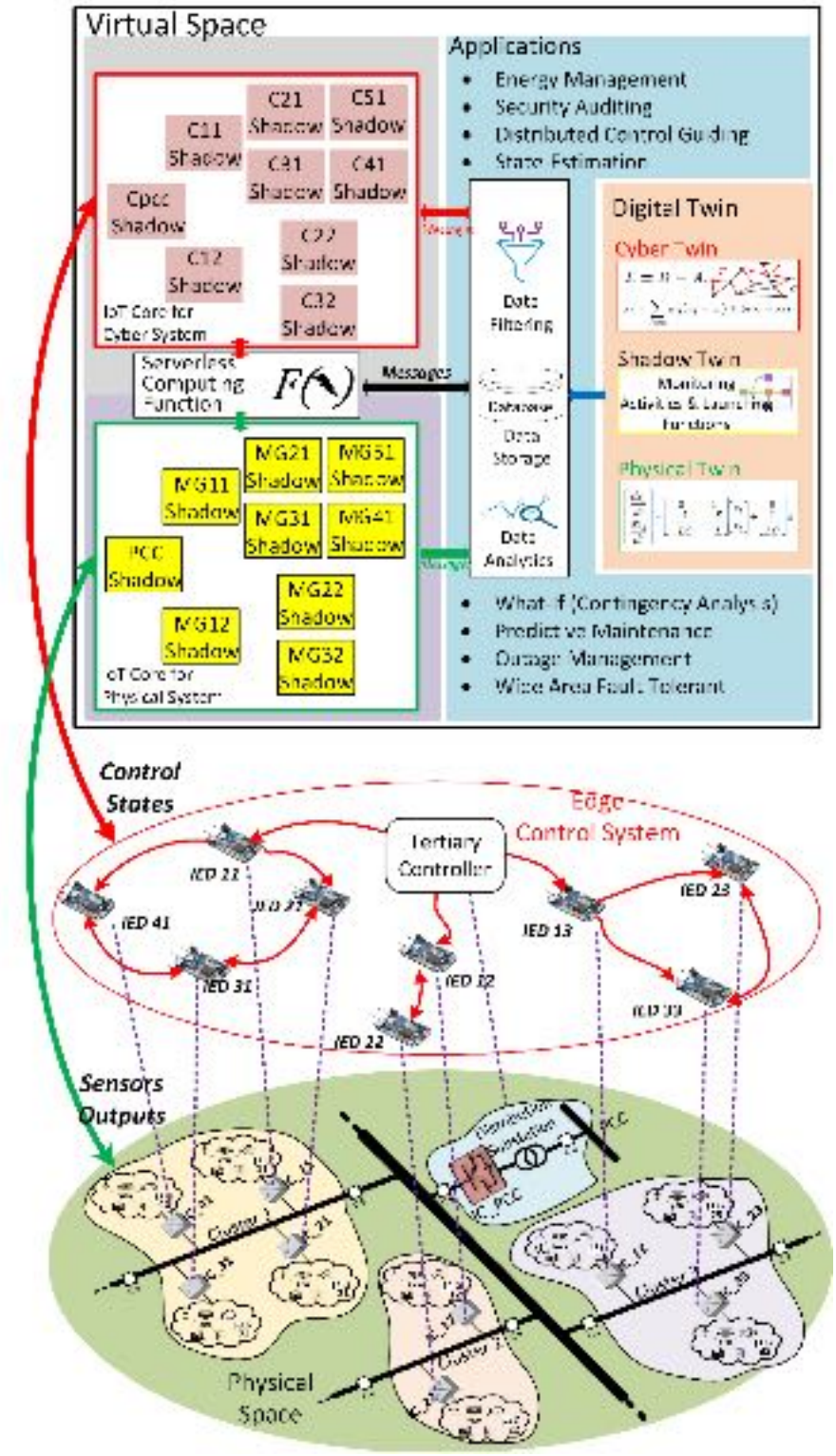


Figure 2.4: The architecture of the developed energy cyber-physical system (ECPS) digital twin.

For instance, energy management, security auditing, distributed control guidance, power system state estimation, what-if scenarios, predictive maintenance for energy assets, outage management, wide area fault tolerance and power system restoration are promising applications that could enhance future distribution grid reliability and security. Additionally, the scalability feature of the IoT in the energy systems will provide an incentive for power system designers, operators and researchers to better understand the new distribution grid capabilities.

Chapter 3 Energy CPS Digital Twin Modelling

The Degree of complexity and the accuracy of the DT is defined according to the application and the type of analysis or the outputs that are required to be implemented. The purpose of the DT in this chapter is to discover the physical balancing mismatch, the cyber control system convergence, and the hybrid CPS consistency.

3.1 DT Dynamic Modelling Platform

Usually, the modelling and simulation of the power system are running off-line with manual settings to study contingency analysis, plan an outage for maintenance, or future planning for example. The developed DT playground uses the IoT data to give the model life and inherit a very close real-time behavior of the power system. However, the following models can cover many applications for the power system DT playground, the DT models are not limited to the following model types.

3.1.1 Cyber Dynamics Model Structure

The cyber system can be implemented using a different formulation based on the cyber system duty. In the power system industry, the networked control systems play the main role to exploit the available resources to maintain the power continuity at maximum efficiency and with a higher level of resiliency. The newly designed control infrastructure is based on the distributed multi-agent controller which agree on a global objective alongside satisfying the local objectives.

The resilient distributed control system is mainly depending on the control agents and their communication channels. The control effort is done cooperatively and if any agent is disturbed or the communication failed, the agreement among the secondary control agents

(SCAs) cannot be reached. The purpose of the DT for the cyber is system is to continuously guarantee the reliability and the connectively of the control agents.

In Figure 3.1, to implement the digital replica of the cyber system, the topology reading module is developed. It uses the shadow of the control agents reported states and transform it into the cyber graph topology and the features of the multiagent connectivity as the adjacency matrix, the degree and the Laplacian matrix. The constructed DT clones can be constructed from The IoT shadow by using the method ***(I/OQueryShdw())*** and/or the stored data in the cloud-based database by using the method ***(I/OQueryDB())***.

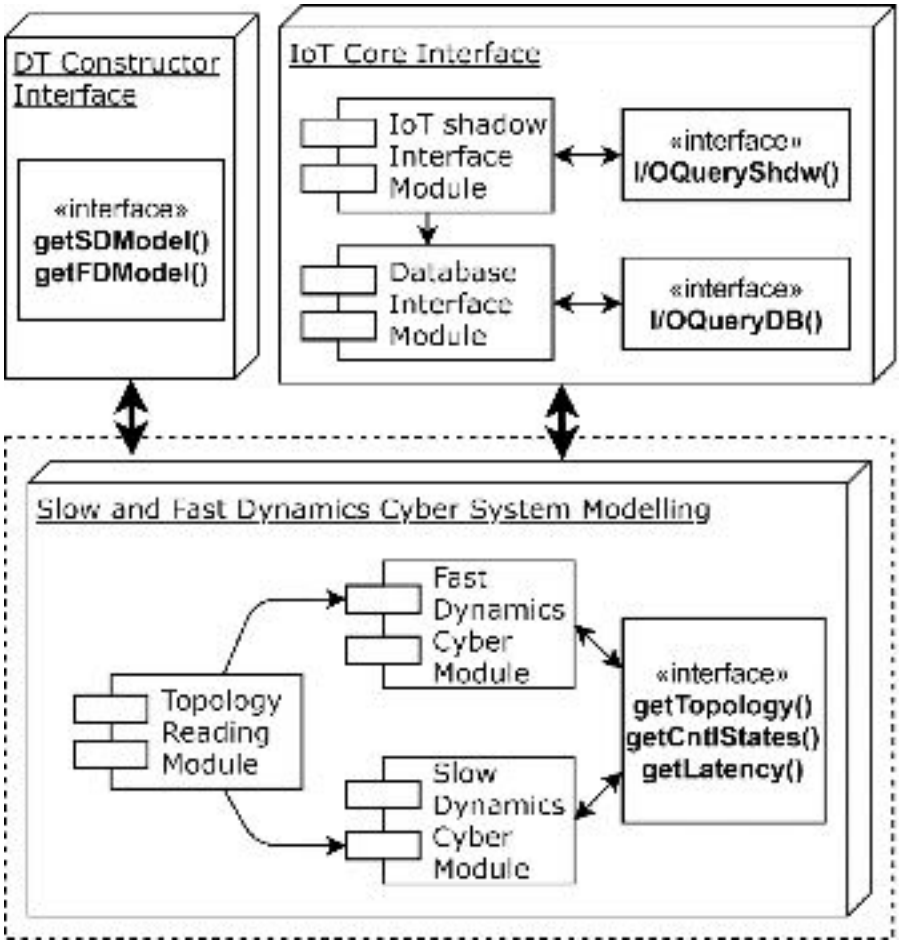


Figure 3.1: cyber dynamic model modules and interfaces.

To model the exact control behavior of the SCAs, the graph features is used to construct the fast and the slow dynamics of cyber models as discussed in the following part. The interfaces functions are developed to be the topology shadow ***(getTopology())***, the control states ***(getCntrlStates())*** and the estimated communication latency ***(getLatency())*** is implemented to get the cyber system DT.

The fast and slow dynamics of the cyber graph is mainly depending on the communication bandwidth among the control agents. It can be represented in the model by controlling the sampling rate of the consensus rule update. The cyber communication bandwidth sampling time τ_m is represented as a set of the fast and slow communication rate $\tau^{\theta} = \{\tau_{FD}^{\theta}, \tau_{SD}^{\theta}\}$. To merge the cyber and the physical DT models, the DT constructor uses the functions ***(getSDModel())*** to get the slow dynamics model and the function ***(getFDModel())*** to get the faster dynamics model.

3.1.2 Physical Dynamics Model Structure

The digital twin nature is based on the life model and the model specifications is an objective-oriented model. According to the application of the DT, the modelling methodology, response and accuracy are defined. In the developed DT playground for the power system and energy applications, the power system model can be classified into three different modelling types. Figure 3.2 shows the developed physical modelling modules and their interfaces for DT implementation.

As shown in Figure 3.2, the first type is the steady-state power system modelling, which can provide real-time snapshot-based studies as load flow analysis, line loading violation, voltage profile deviation and contingency assessment analysis. The steady-state modelling

is considered as a snapshot-based slow dynamic. Based on the accuracy requirements of the DT application, the steady-state modelling module is selected among three types: DC power flow analysis (DCPF), AC power flow analysis (ACPF) and optimal power flow analysis (OPF). These modules can be interfaced with the other modelling modules according to the application objectives. The interface with this module is executed by three methods ***(getDCPF(), getACPF(), getOPF())***.

The second type of slow modelling module is for the economic and market real-time analysis. The developed modelling methodology is based on a generic energy node state-space formulation for each energy source, energy storage system, load and grid connectivity. This model is designed to be independent to simplify the economic dispatch study, market operation, and optimal power commitment. The second module capabilities can be extended for certain applications that care about the security-constrained market operation by interfacing the generic energy node module with the steady-state modules. Based on the selected case study, the modules interface class methods are called ***(getEconDispatch(), getMarketAnalysis())***.

In the third type, the fast dynamics power system modelling techniques contains four modules as shown on the right-hand side of Figure 3.2. The transient stability module is responsible for transient stability assessment, fault critical clearing time and dynamic voltage stability. The large-signal and small-signal stability modules are provided for the large and small disturbance effect on the stability, respectively. The fourth module is responsible for modelling multi-domain models as electro-mechanical interaction and/or power-electronics converter interaction with the grid. This type has four methods:

performing transient stability analysis ***(getTSA())***, analyzing the effect of large or small disturbances ***(getLSSA(), getSSSA())*** and getting the result of multi-domain simulation ***(getMDHA())***.

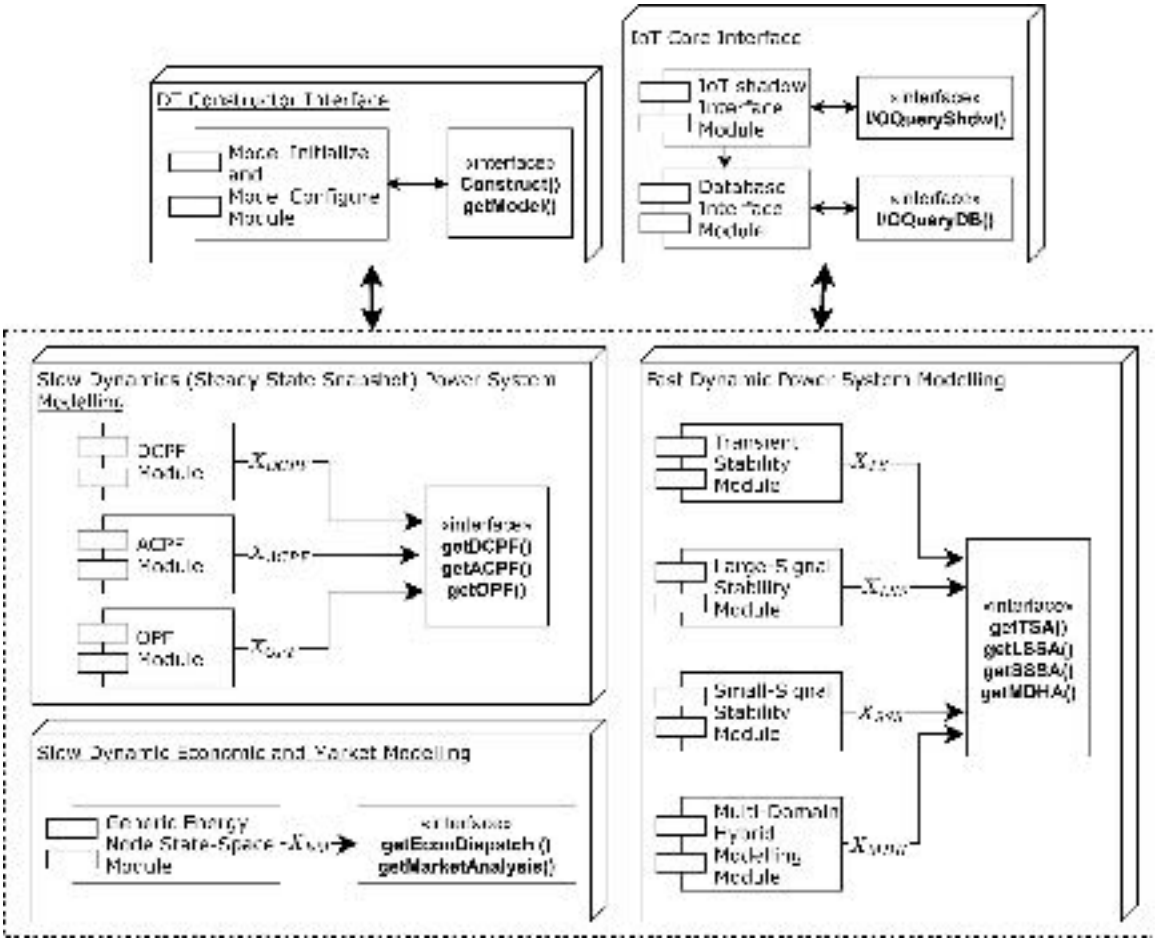


Figure 3.2: physical dynamic model modules and interfaces.

These different modules can be merged by using the DT constructor interface methods ***(Construct() and getModel())***, which includes the module that is responsible for the modelling initialization and configuration. According to the application, the model modules are selected and merged and initialized based on the last shadow states that are coming from the IoT core interface modules. The input/output (I/O) interface between the

modules and the IoT core for both the shadow and the databases are performed by the query filtering instructions ***(I/OQueryShdw(), I/OQueryDB())***.

3.2 Generic Formulation of the CPS DT Model

By combining the last sensory/control updates and the model, the DT can replicate the real system digitally. The model is mathematically formulated to describe the static and dynamic features of the thing and enhanced by full or partial information from the edge. The DT can simulate the normal and abnormal behaviors of an asset. In addition, the data-driven models leverage data analytics to describe, understand and predict the dynamical activity numerically. Exploiting the historical knowledge data, event logging and their counteractions in the deep-learning technologies can equip the DT model with the capability of recommending corrective actions during a contingency and effectively operating the ECPS during normal healthy operation.

Generally, the physical asset $\varphi \in \Phi$ is represented by the physical set of states X^{Ψ}, which is measured by a sensor $\psi \in \Psi$. The physical dynamic is defined by A^{Φ}, B^{Φ}, C^{Φ}, D^{Φ} parameter matrices. The physical system with control input U^{Ψ} is represented in state-space form as

$$\left.\begin{aligned} \dot{X^{\Psi}} &= A^{\Phi}X^{\Psi} + B^{\Phi}U^{\Psi} \\ Y^{\Psi} &= C^{\Phi}X^{\Psi} + D^{\Phi}U^{\Psi} \end{aligned}\right\} \tag{3.1}$$

To provide the cyber model the flexible compatibility with the physical model, the cyber system dynamics is developed to be in the linear time-invariant state-space representation. A cyber thing $\theta \in \Theta$ represents a controller state $x^{\theta} \in \mathrm{X}^{\Theta}$, which uses the sensor measurement and the cyber graph $\mathcal{G}$ to control the physical asset φ. The cyber

dynamic is defined by A^{Θ}, B^{Θ}, C^{Θ}, D^{Θ} parameter matrices. The cyber system dynamics is given by,

$$\left.\begin{aligned} \dot{X^{\Theta}} &= A^{\Theta}X^{\Theta} + B^{\Theta}U^{\Theta} \\ Y^{\Theta} &= C^{\Theta}X^{\Theta} + D^{\Theta}U^{\Theta} \end{aligned}\right\} \tag{3.2}$$

The digital twin model was developed to be a multi-purpose function. It can be used by many applications. According to the required solution, the DT model is defined by the sampling time, the known inputs and the desired outputs. The previous ECPS physical and cyber twins can be hybridized to replicate the cyber-physical system's behavior as follows,

$$\begin{bmatrix} \dot{X}^{\Theta} \\ \dot{X}^{\Psi} \end{bmatrix} = \begin{bmatrix} A^{\Theta} & \mathbf{0} \\ B^{\Phi}C^{\Theta} & A^{\Phi} \end{bmatrix} \begin{bmatrix} X^{\Theta} \\ X^{\Psi} \end{bmatrix} + \begin{bmatrix} B^{\Theta} \\ \mathbf{0} \end{bmatrix} [U^{\Theta}] \tag{3.3}$$

$$[Y^{\Theta\Psi}] = [\mathbf{0} \quad C^{\Phi}] \begin{bmatrix} X^{\Theta} \\ X^{\Psi} \end{bmatrix} \tag{3.4}$$

where $Y^{\Theta\Psi}$ is the hybrid model output and the disturbance pair D^{Φ} , D^{Θ} are ignored for simplification. Using the hybrid twin models, the unknown states and the forecasted behavior can be predicted based on the present shadow states.

3.3 ECPS DT Model Formulation

As previously discussed, the DT model is application-oriented and the DT model for the energy CPS cannot be a single definite model for all solutions. In this section, a variety of DT models are developed for the purpose of the distributed control guidance, energy management, cybersecurity auditing and authentication. In addition, the DT model was covered for both the fast and slow model dynamics. The following model development was implemented for the networked distributed microgrids in the active distribution network.

3.3.1 Physical System DT Model

The ECPS is assumed to contain a set of subsystems that are physically interconnected to balance the generation and demand mix and controlled through coordinated multi-agents that are linked using a cyber communication graph to ensure a common goal. The degree of the complexity of the DT model depends on the nature of the application, the possible actions and the physical asset itself.

The developed ECSP DT model was divided according to the application's nature into two models: a low-bandwidth (slow dynamics) DT model and a high-bandwidth (fast dynamics) DT model. On one hand, the applications that require the low-bandwidth model are energy management, market operation, situational awareness monitoring and predictive maintenance. These applications are performed periodically every large time span, and they usually depend on long-term historical data to predict long-term future operation strategies and management actions. On the other hand, the high-bandwidth applications are real-time outage management, what-if contingency analysis, secondary control guidance and system restoration. The following subsections present the developed DT model.

3.3.1.1 Slow Dynamics Physical Model

Suppose a distribution grid has o^{th} interconnected energy units. These energy units can be distributed generation (such as a solar, wind or conventional generator), Energy Storage Systems (ESSs) such as a battery storage system or thermal storage system, fixed loads or flexible loads (such as an electric vehicle parking garage or nanogrids). Figure 3.3 shows the low-bandwidth physical model of an energy unit. Generally, the energy unit can be represented as a generic energy node with an original infeed source ξ from the energy

resource as the solar irradiance or the required demand. If the infeed energy is storable with capacity $\mathcal{H}$, the node can represent an ESS or flexible load. If the energy cannot be stored, the node represents a generation or the fixed load and $\mathcal{H} = 0$.

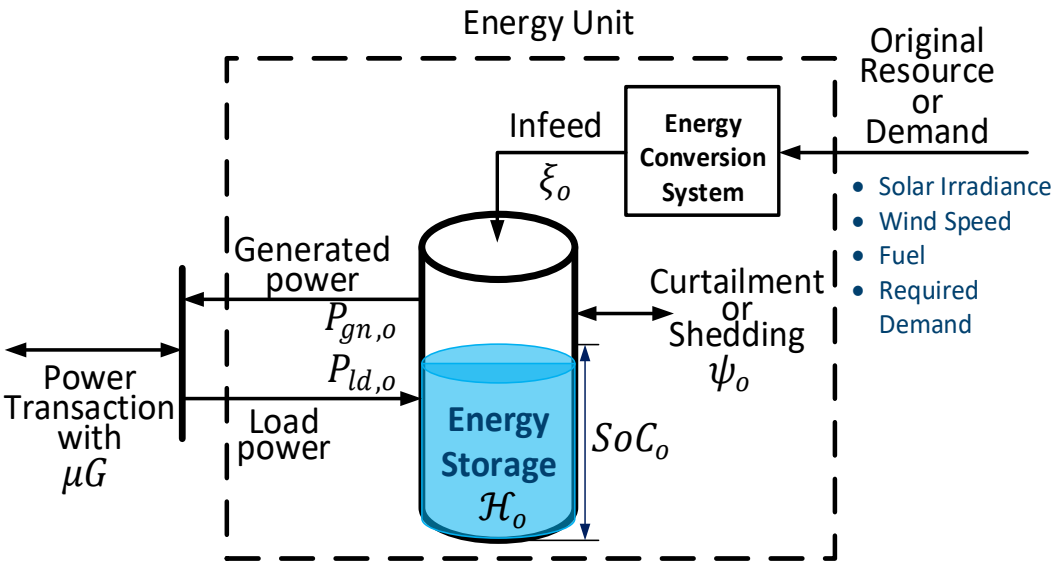


Figure 3.3: slow dynamics physical model of the digital twin.

In the case of representing the renewable resource as solar or wind and where excessive power is present, the power curtailment can be represented by $\psi < 0$. In the case of representing the loading, ψ represents the load shedding and $\psi > 0$. When the generic node has $P_{ld} = 0$, it represents a generation mode. Additionally, if the generated power $P_{gn} = 0$, the unit represents the load. If both the generation mode and loading mode exist, the node represents an ESS. The generic mathematical formulation of the o^{th} energy unit representations are:

$$\mathcal{H}_o \dot{SoC}_o = -\eta_{gn,o}^{-1} P_{gn,o} + \eta_{ld,o} P_{ld,o} \pm \xi_o + \psi_o - \varrho_o (SoC_o - SoC_o^{(0)}) \qquad (3.5)$$

where SoC_o and $SoC_o^{(0)}$ are the state of charge and the initial state of charge of the o^{th} energy unit. In addition, η_{ld} and, η_{gn} are the efficiency of the generation and loading operation, and ϱ_o is a variable that represents the flexible load controllability. Table 3.1 shows possible mathematical formulations for different energy unit types according to (3.5) and from applying the energy unit constraints.

Table 3.1: energy unit mathematical formulation.

Type	Constraints	State-Space Model
Conventional	$\mathcal{H}_o = 0, P_{ld,o} = 0, \psi_o = 0$	$0 = -\eta_{cgn,o}^{-1} P_{cgn,o} + \xi_{cgn,o}$
Renewable	$\mathcal{H}_o = 0, P_{ld,o} = 0, \psi_o < 0$	$0 = -\eta_{rgn,o}^{-1} P_{rgn,o} + \xi_{rgn,o} + \psi_{cur,o}$
ESS	$\xi_o = 0, \psi_o = 0$	$\mathcal{H}_{s,o}\, \dot{SoC}_{s,o} = -\eta_{sgn,i}^{-1} P_{sgn,o} + \eta_{sld,o} P_{sld,o}$
Fixed Load	$\mathcal{H}_o = 0, P_{gn,o} = 0, \psi_o > 0$	$0 = \eta_{ld,o} P_{ld,o} - \xi_{ld,o} + \psi_{shd,o}$
Flexible Load	$P_{gn,o} = 0, \psi_o = 0$	$\mathcal{H}_{fld,o}\, \dot{SoC}_{fld,o} = \eta_{fld,o} P_{fld,o} + \xi_{fld,o} - \varrho_o (SoC_{fld,o} - SoC_{fld,o}^{(0)})$

3.3.1.2 Fast Dynamics Physical Model

The purpose of the DT is to represent the power system's dynamics and the effect of the networked microgrids on the distribution grid's point of common coupling. The DC microgrid mainly consists of four components: sources, a DC/DC converter, loads and distribution cables. The large-signal dynamical equations that represent the transient response are derived as a linear time-invariant differential equation. The main focus of this physical model is to represent the transactions among the networked microgrids. Therefore, the intra-microgrid transactions are ignored here, as they are already covered in the low-bandwidth model. Each microgrid contains several interconnected sources and loads that can be characterized by a Thevenin equivalent circuit. Thus, the individual microgrid i is modelled by a controllable voltage source and its passive components of resistance, inductance and capacitance.

Figure 3.4 illustrates a networked DC microgrid under study. The grid contains two clusters of microgrids: the first cluster has five microgrids, and the second one has three microgrids. Usually, the practical DC power system was connected to the major grid via a point of common coupling (PCC). The equivalent model of each microgrid's equivalent voltage sources is shown at the bottom of Figure 3.4, which identifies the primary control system of the DC/DC converter. Since the control objective of the secondary controllers in cyberspace is power-sharing, the voltage and the current references are formulated in the model to make the power-sharing factor the reference of the controlled microgrid output.

Generally, the DCNMG dynamics of i^{th} microgrids can be described by:

$$\left.\begin{aligned} L_i \frac{d\tilde{I}_i}{dt} &= E_i^* - r_i\tilde{I}_i - v_i^t \\ C_i \frac{dv_i^t}{dt} &= \tilde{I}_i - I_i^t \end{aligned}\right\} \tag{3.6}$$

where $\tilde{I}_i$ is the i^{th} microgrid converter average inductor current, E_i^* is the reference voltage at the i^{th} microgrid v_i^t is the microgrid terminal voltage and I_i^t is the transmitted current from/to microgrid i to the grid. In addition, R_i, L_i and C_i are the equivalent resistance, inductance and capacitance of each microgrid i.

It is assumed that the microgrid output is controlled by the reference signals of the terminal voltage $V_i^{t,ref}$ and the output reference power P_i^{ref} using the droop control characteristics as follows,

$$E_i^* = V_i^{t,ref} - k_i(P_i^{ref} - P_i) \tag{3.7}$$

where k_i is droop coefficient and the output power can be represented in terms of power-sharing factors $P_i = P_{i,max} x_i$. Therefore, if $\beta_i = k_i P_{i,max}$, the controlled voltage in (3.7) can be rewritten as follow.

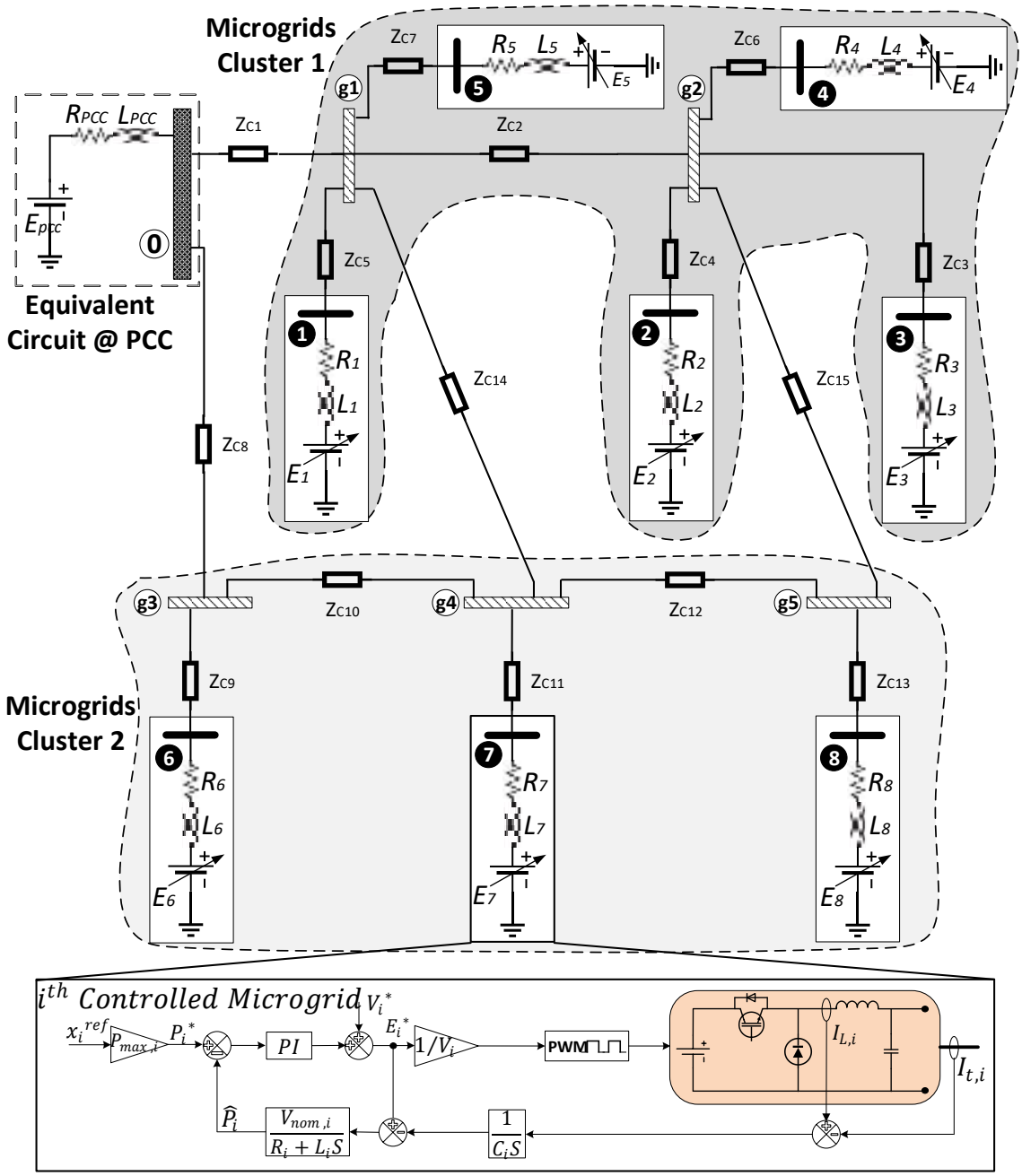


Figure 3.4: NMGs fast dynamics model.

$$E_i^* = V_i^{t,ref} - \beta_i(x_i^{ref} - x_i) \tag{3.8}$$

The microgrid terminal t_i is connected to the distribution grid nodes g_j which has voltages $v_o^g = \left[v_o^g, \dots, v_m^g\right]$ and the transmitted current to the grid nodes can be described as,

$$I_i^t = \sum_{j \subset m} I_j^g = \sum_{j \subset m} y_{ij}^{tg}(v_i^t - v_j^g) \tag{3.9}$$

where y_{ij}^{tg} is the line or cable admittance between the nodes t_i and g_j. Since the balancing and power flow is the purpose of the model, the electrometric transients are ignored which leads that the grid interconnection model is represented as follows,

$$\begin{bmatrix} I^t \\ I^g \end{bmatrix} = \begin{bmatrix} Y^{tt} & Y^{tg} \\ Y^{gt} & Y^{gg} \end{bmatrix} \begin{bmatrix} V^t \\ V^g \end{bmatrix} \tag{3.10}$$

According to (3.6) and (3.8)-(3.11)(3.10), the balancing dynamics in matrix notation can be written as,

$$\left.\begin{aligned} L\frac{d\tilde{I}}{dt} &= V^{t,ref} - \beta X^{ref} - R\tilde{I} - V^t \\ C\frac{dV^t}{dt} &= \tilde{I} - I^t \\ I^t &= Y^{tt}V^t + Y^{tg}V^g \\ I^g &= Y^{gt}V^t + Y^{gg}V^g \end{aligned}\right\}. \tag{3.11}$$

where $X^{ref} = [x_1^{ref}, \dots, x_n^{ref}]^T$, $V^{t,ref} = [v_1^{t,ref}, \dots, v_n^{t,ref}]^T$. To ensure the equilibrium of the dynamics in (3.11) is analyzed in steady-state such that $V^t = V^{t,ref} - \beta X^{ref} - RI^t$ as,

$$\left.\begin{aligned} I^t &= Y^{tt}V^{t,ref} - \beta Y^{tt}X^{ref} - RY^{tt}I^t + Y^{tg}V^g \\ I^g &= Y^{gt}V^{t,ref} - \beta Y^{gt}X^{ref} - RY^{gt}I^t + Y^{gg}V^g \end{aligned}\right\} \tag{3.12}$$

whose re-arranging yields,

$$\left.\begin{aligned} I^t &= (Y^{tt^{-1}} + R)^{-1}V^{t,ref} - \beta\left(Y^{tt^{-1}} + R\right)^{-1}X^{ref} \\ &\quad +Y^{tg}(1 + RY^{tt})^{-1}V^g \\ I^g &= (Y^{gt} - Y^{gt}R(Y^{tt^{-1}} + R)^{-1})V^{t,ref} \\ &\quad -(\beta Y^{gt} - Y^{gt}R\beta(Y^{tt^{-1}} + R)^{-1})X^{ref} \\ &\quad (Y^{gg} - Y^{gt}Y^{tg}R(1 + RY^{tt})^{-1})V^g \end{aligned}\right\} \tag{3.13}$$

The system achieves the equilibrium if the controlled values $V^{t,ref}$ and X^{ref} are chosen to guarantee that the system in (3.11) is solvable. By mapping the system in (3.11) to the physical system generic formulation in (3.1), the physical system states and inputs are $X^{\Psi} = [\tilde{I}, V^t]^T, U^{\Psi} = [V^{t,ref}, X^{ref}, I^t]^T$, respectively. The physical system dynamical parameters are derived from (3.11) as follows,

$$\begin{aligned} A^{\Phi} &= \begin{bmatrix} -RL^{-1} & -L^{-1} \\ C^{-1} & 0_n \end{bmatrix} \\ B^{\Phi} &= \begin{bmatrix} L^{-1} & -\beta L^{-1} & 0_n \\ 0_n & 0_n & -C^{-1} \end{bmatrix} \\ C^{\Phi} &= [I_n] \end{aligned} \tag{3.14}$$

3.3.2 Cyber System DT Model

The distribution system that contains NMG can be considered a virtual power plant. The aggregated power from the NMG is controlled by the tertiary controller at PCC (leader) and the multi-agent cooperated controllers at each microgrid (followers) [11], [12], [16], [59]–[61]. The PCC tertiary controller objective is to satisfy the energy management optimal update, which is the reference power-sharing P_{pcc}^{ref} by aggregating it from the NMGs sharing P_i. Since the NMG contains different scales of microgrids, the sharing capability of each microgrid is different. Therefore, the PCC agent ($agent\ 0$) is described by the sharing factor $x_0 = P_0/P_{0,max}$ and each microgrid sharing capability is defined as

$x_i = P_i/P_{i,max}$. The PCC agent control objective is to achieve certain reference common power-sharing factor as follows,

$$\begin{aligned} &\min_x \left(x_0^{ref} - x_0(x_i)\right) \\ &s.t. \qquad 0 \le x_0 \le 1 \\ &\qquad\quad 0 \le P_0 \le P_{0,max} \end{aligned} \tag{3.15}$$

where $P_{0,max}$ is the maximum power-sharing capability at the PCC.

The secondary distributed controllers cooperate to achieve a consensus on the main leader control objective. According to the graph theory, the cyber communication is a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ that determines the cyber state coupling of the agents' dynamics where $\mathcal{V} = \{0,1, \dots, n\}$ is the vertex set with a set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the coupling between the control agents.

Agent 0 is the main leader for the system, and it is connected to the leaders of microgrids clusters i^l, which is connected to several i followers. The edge $(i,j) \in \mathcal{E}$ represents the cyber state of i^{th} agent will influence the dynamics of j^{th} agent according to weighing factor w_{ij}, which is represented as a global adjacency matrix $\mathcal{A} \in \mathbb{R}^{(n+1)\times(n+1)}$, which is described as,

$$[\mathcal{A}]_{ij} = \begin{cases} w_{ij} > 0 & if \;\; i,j \in \mathcal{E} \\ 0 & otherwise \end{cases} \tag{3.16}$$

The secondary control agent model is used to emulate the cyber graph by implementing the model on the right-hand side of Figure 3.5 for every agent and use the weighting factors

$a_{i,j}$ to represent the communication link connectivity and the degree of populating the control update rules to the rest of the cyber graph.

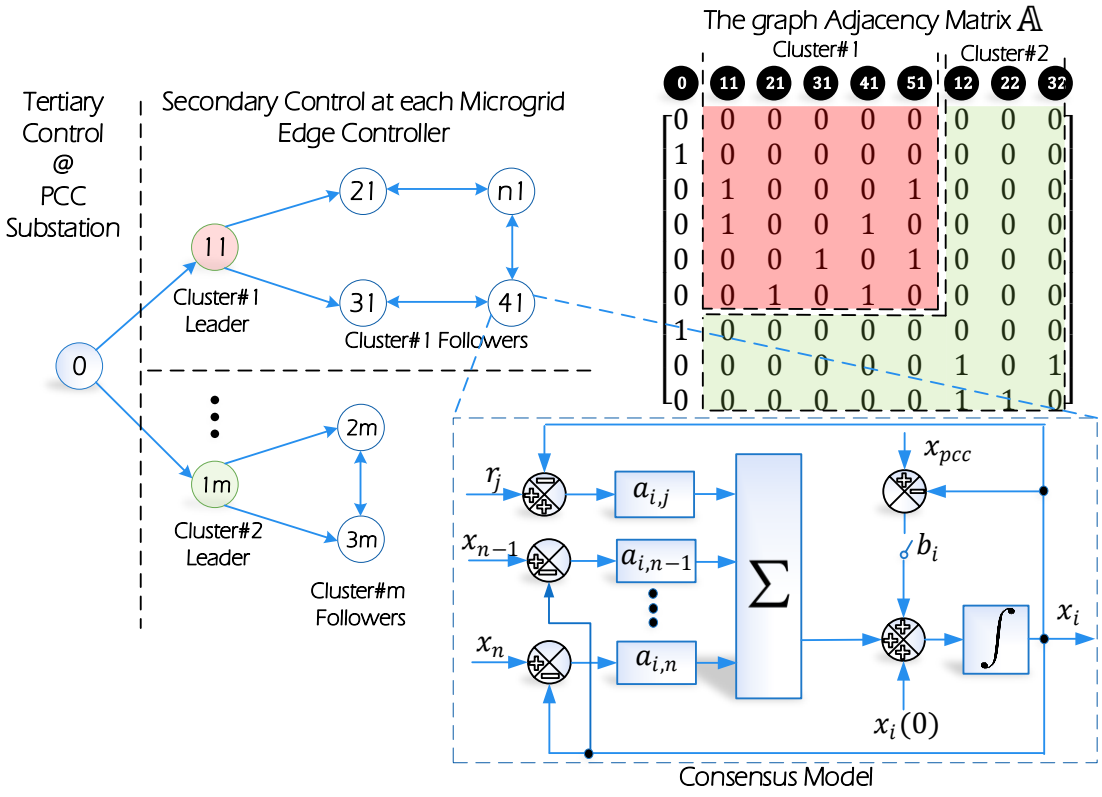


Figure 3.5: distributed control model

The graph Laplacian matrix is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A}$, were $\mathcal{D} = diag\{d_i\}$, is the in-neighbours degree matrix and $d_i = \sum_{j \in n_i} w_{ij}$.

Remark 1: The leader-follower consensus protocol can be implemented in the following discrete-time form for k^{th} samples to achieve an agreement on the steady-state control leader such that, $\lim_{k \to \infty} x_i(k) = x_0^{ref}\ \forall i \in n$ that was provided by the tertiary controller as formulated in Algorithm A2 in [62],

$$\delta_{ij}(k+1) = \delta_{ij}(k) + w_{ij}(x_j(k) - x_i(k)) \tag{3.17}$$

$$x_i(k+1) = \varepsilon.\delta_{ij}(k+1) + g_i.x_0 \tag{3.18}$$

where δ_{ij} is an intermediate updating of the control law for an agent i by j^{th}neighbours, ε is a constant to regulate the consensus speed and g_i is the pinning gain, which characterizes the spanning tree at the leader.

The dynamics of the consensus protocol can be modelled as a set of interacting agents that achieve a common goal x_0. The local neighborhood tracking error e_i of a controller i is formulated as,

$$e_i = \dot{x}_i = \sum_{j \in n_i} w_{ij}(x_j - x_i) + g_i.(x_0 - x_i) \tag{3.19}$$

$$\dot{X} = -(\mathcal{L} + G).X + G\underline{\mathbf{1}}x_0 \tag{3.20}$$

The leader takes the role of controlling the graph in a distributed manner using the consensus protocol $u_i = \iota e_i$, were ι is a constant gain, which was chosen to ensure the synchronization among agents. The synchronization error with the leader can be represented as $\delta_i = x_i - x_0$.

The consensus was achievable under the input u_i to the leader state x_0 and the synchronization error with the leader $\delta_i = x_i - x_0$ is decaying to zero, $\delta_i \to 0$ if the dynamical matrix of the cyber graph is stabilizable. The global dynamical error under the control mechanism u_i be formulated as,

$$\left.\begin{array}{c} \dot{\delta} = \dot{X} - \dot{X}_0 \\ \dot{\delta} = ((I_n \otimes \mathcal{A}) - \iota(\mathcal{L} + G))\delta \\ \dot{\delta} = A^c \delta \end{array}\right\} \tag{3.21}$$

were A^c represent the error closed dynamical matrix. The solution is written as,

$$\delta(t) = e^{A^c t}\delta(0) \tag{3.22}$$

By mapping the cyber system dynamics in (3.20) into the generic DT model in (3.2), the cyber states $X^{\Theta} = X^{ref}$, the graph control input $U^{\Theta} = X_0$, the cyber system dynamics are $A^{\Theta} = -(\mathcal{L} + G)$, $B^{\Theta} = \iota G\underline{1}$, $C^{\Theta} = I_n$.

These developed models of the ECPS cannot be handled as a data-informed models without input/output configuration, shadow synchronization and observer prototypical. To transform these models into a usable DT clones, the DT playground was developed and discussed in the following chapter.

Chapter 4 Practical Implementation of the Energy CPS Digital Twin Playground

This chapter presents an Internet of Things based digital clone of the energy cyber-physical system that can serve many applications in the power system as monitoring, resilient control, management, security, situational awareness and planning. The developed framework can create a digital twin of the physical power system components, cyber control layer and their interaction in real-time. The framework provides the power system with reliable, efficient and secure operations during the normal state and makes the system survivable against catastrophic risks. The developed framework leverages the emerging of IoT and cloud computing technologies to create a safe playground to test, validate, plan and study the new ideas in a real like system. Unlimited applications can be implemented for the power system to run in parallel, which gives the ECPS the ability to follow the Industry 4.0 revolution and achieve the power grid digitalization.

4.1 Overall Energy Cyber-Physical Digital Twin Playground Platform Description

The developed digital twin playground is a real-time digital clone of the power system that holds both the last power system state and data-informed ECPS dynamic models to mimic the power system behavior. That will give the grid operator the ability to monitor, operate, secure, design, test, validate, plan and study the current and future energy cyber-physical system. Figure 4.1 shows an overview of the developed platform.

4.1.1 Energy Cyber-Physical System Description

The distribution grid is considered as the higher complex part, so it is selected to show the developed power system DT playground. On the left-hand side, the energy cyber control system is on top of the energy physical power system. The physical system contains

power electronics-based interconnected microgrids that are working as virtual power plants to perform power distribution clusters and it is coupled to the rest of the grid via an interlinking converter (IC). The cyber networked control system contains secondary and tertiary control systems that are working hierarchically to manage the microgrids, DGs and loads interactions.

The physical distribution system includes the microgrids clusters on each feeder that contains many types of energy units as distributed generators (DGs), Energy Storage Systems (ESSs), Fixed Loads (LD) and Flexible loads (FLD). Besides, the emerging power electronics devices, which is the main factor to regulate the power flow and maintain system stability. It is assumed that the primary controllers of the power electronic devices are a part of the physical system. The physical space was monitored via sensors as voltage transformers (V.Ts) and current transformers (C.Ts), which translated to digital form through micro-phasor-measurement-units ($\mu PMUs$).

In cyberspace, the tertiary controller interacts with the utility to manage the power at the point of the common coupling (PCC). The tertiary control system was implemented on the distribution substation and it is responsible for deciding on the transmitted power at the PCC to support many objectives as both the energy market transactions and the system ancillary services. To aggregate the miniature power units the distribution grid, the secondary control agents are working cooperatively to achieve an agreement on the tertiary control global objectives and to satisfy the local control objectives locally in the individual microgrid. Those agents are coordinating via communication links and achieve the agreement using the consensus algorithm.

4.1.2 The Developed Digital Twin Playground

The developed platform can be implemented on a commercial or private cloud system, which provides many on-demand cloud computing services as computer processing resources, connectivity, virtual machines, IoT core, data pipelines, data storages and machine learning engines. The monitored physical system was provisioned in the cloud IoT core system via internet communication protocols. In the same way, the cyber control states are shared from the controllers to the IoT core. These cyber and physical states living on the cloud as a digital shadow and contain the latest information about the physical or the cyber asset. Once the data sent to the IoT core, it can be accessed by any service on the cloud. To manage the data access inside the cloud system for the DT purpose, the data interface function was developed. Also, the event detection function was implemented on a service less computing function to trigger many DT applications in real-time.

As shown in Figure 4.1, the reported shadow states are sent to the dynamic model module. The dynamic model module was equipped with fast dynamics (FD) models and slow dynamics (SD) models for both the cyber and the physical systems. Also, a separate deep learning model was developed to perform cyber and physical behavior prediction. The developed module is scalable and flexible to add more models according to future applications. These models are built to run in real-time as a digital replica of the ECPS and ready for any application in the digital playground. The DT playground contains a DT constructor engine and the applications environment to let the grid operator customize the applications and their objectives.

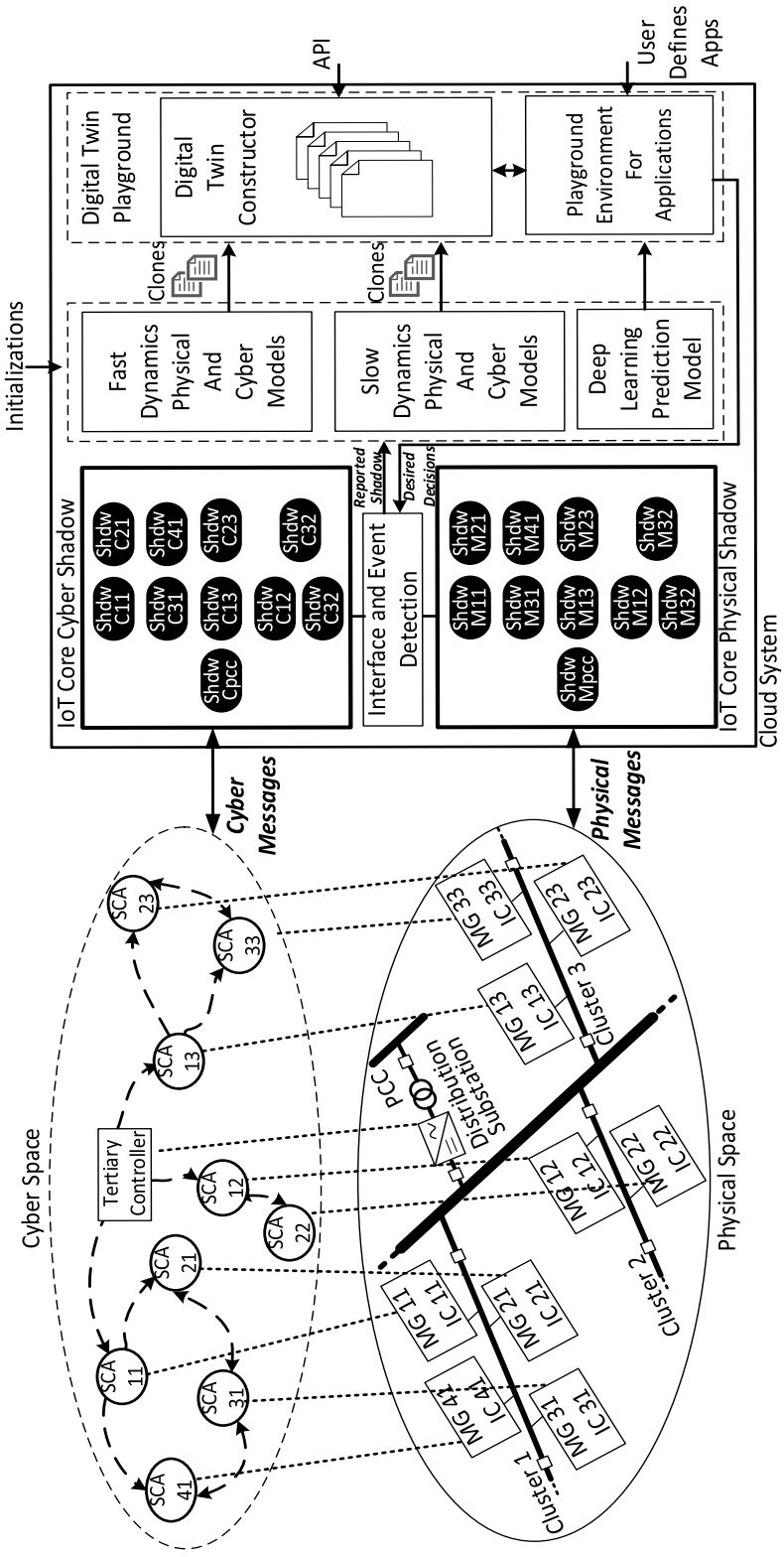


Figure 4.1: The Developed Digital Twin Playground.

The DT constructor is an algorithm that is responsible for constructing a DT clone by defining the required model type, the twin input/output configuration, model merging/hybridization and the full state observer design, which estimate the unknown states, solve what-if scenarios, and answer the future unforeseen questions. The DT constructor can be programmed by a predefined Application Programing Interface (API).

The playground environment was introduced to create a user-friendly interface for custom applications. It uses the living DTs and predicted behaviors to give the grid operator a fearless capability of running actual real-time studies with unlimited scale but the cloud system. After that, the decisions can be returned to the ECPS by setting the desired states on the asset's shadow.

4.2 ECPS Things-To-Cloud Service Transactions

To implement the digital twin, the model's degree of complexity should be carefully considered to avoid adding extra complexity to the system. The developed digital twin uses the state-space representation of the ECSP by aggregating the individual microgrid resources into a single equivalent model. That will reduce the communication and the computational burden without reducing the benefits of potential applications and solutions. As shown in Figure 4.2 the IoT device makes decisions locally within the microgrid, but it will be kept aware of the global centric objective with regular over-the-air programming (OTA) updates of its settings.

The ECSP is represented in the cloud by the sensor measurements from the physical assets φ and the control states from the cyber assets θ. Figure 4.2 depicts the AWS cloud hosting the energy IoT, computing services and their transactions. Suppose the distribution

grid has n microgrid (μG) clusters, each μG cluster has m microgrids and the i^{th} μG has o^{th} assets. Each asset is connected to the microgrid main bus by an interlinking power electronics converter IC_o, and each μG is linked to the distribution grid by an interlinking converter IC_i.

On one hand, the microgrid physical assets can be classified into four main types, the distributed generator (DG), ESS, fixed load (LD) and flexible loads (FLD). An asset o is monitored by a current transformer C.T and voltage transformer V.T, which are used to calculate various physical power system states using $\mu PMUs$. The asset physical state is represented by a set of calculated parameters $x_\varphi = \{P, Q, f, V\}$ that are the active power, reactive power, power frequency and voltage, respectively.

On the other hand, cyberspace is a set of distributed controllers, which are communicating with each other to cooperatively satisfy a control objective x_θ. The control objective can be active/reactive power-sharing, voltage regulation and/or frequency synchronization. This is cooperatively performed by the interlinking converters' secondary distributed controllers ICC. The ICCs are connected via cyber communication links, and the control states interpret the cyberspace transactions alongside the interactions with the physical assets. The AWS was used to extend the cloud system functionality to the IoT devices ($\mu PMUs, ICC$) to perform the data gathering and analysis and act locally on the cyber edge. The IoT GG channels are developed to perform higher-speed calculations locally to be able to act quickly in the case of a critical power system status. The data transaction between the sensors, controllers' edge and cloud is implemented based on the message queuing telemetry transport (MQTT) protocol. To preserve privacy and reduce

the complexity and computational burden, the data pipelines service was used to filter and prepare the data for cloud computing services. The IoT core along with the lambda service less functions was implemented to easily and securely interact with various cloud computing applications.

Besides the DT functions, different services on the cloud are developed to build different applications. For instance, the AWS SageMaker was used to build, train and test the deep-learning models that are launched on the edge of cyberspace. Data filtering, routing and management services are implemented to prepare the data for each application according to the requirements. AWS SageMaker was also used to build applications for the centric guidance to the distributed controllers; what-if contingency scenarios for outage management provide security auditing based on the anomaly detection functionality. In addition, IoT data analytics and data storage are used to implement offline applications for power system planning and physical assets' predictive maintenance. Cyber things can be used to coordinate between different applications.

Figure 4.3 illustrates the cyber/physical thing registration process on the IoT core on the AWS cloud. The IoT Software Development Kit (SDK) was launched on the physical or the cyber asset. The asset registry contains the asset policy, which was used to authorize the device to perform the IoT connectivity. Each asset has the required certificates and keys that are required to initiate the message transactions. The communication was implemented by the asset gateway using MQTT WebSocket or hypertext transfer protocol secure (HTTPs) protocols, and it should be authorized by the IoT core to verify the thing's identity. Then, the gateway sends the message to the rule engine, which is responsible for

assessing the incoming messages published into the IoT core. That determines the action of structured query language (SQL) filtering or rerouting the data to different cloud services based on pre-defined settings.

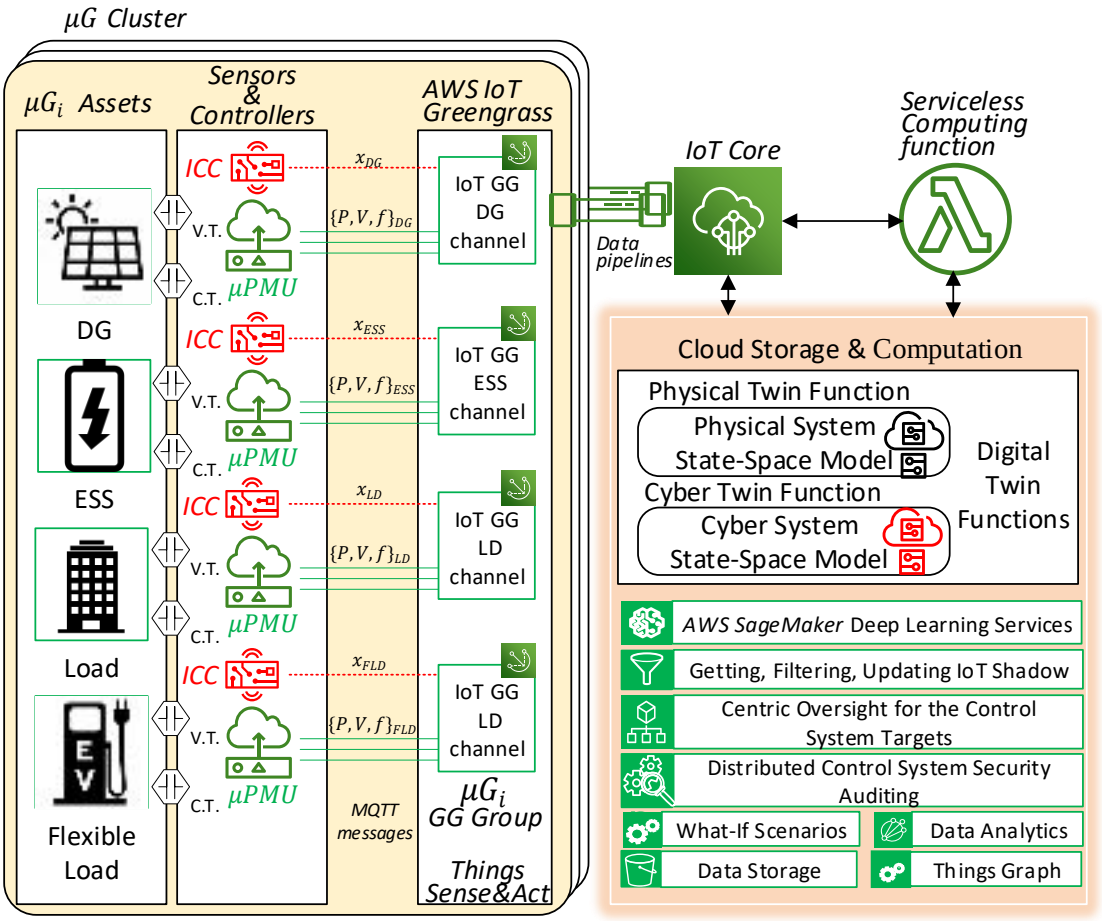


Figure 4.2: Data transaction between ECPS and cloud services.

The vital process of the DT is the update process for the device shadow. The shadow state of an asset is a JavaScript object notation (JSON) file that is used to store/retrieve the last state of a thing. The shadow can be accessed regardless of whether the thing is connected to the Internet or not. It contains the shadow desired and reported states, immutable metadata, updated version, transaction token and timestamp.

The Lambda serviceless function automatically executes a predefined logic function when required without provisioning. The messages are used later for different cloud computing solutions and end-user/operator applications. The IoT application programming interface was used to interact with the data for different applications.

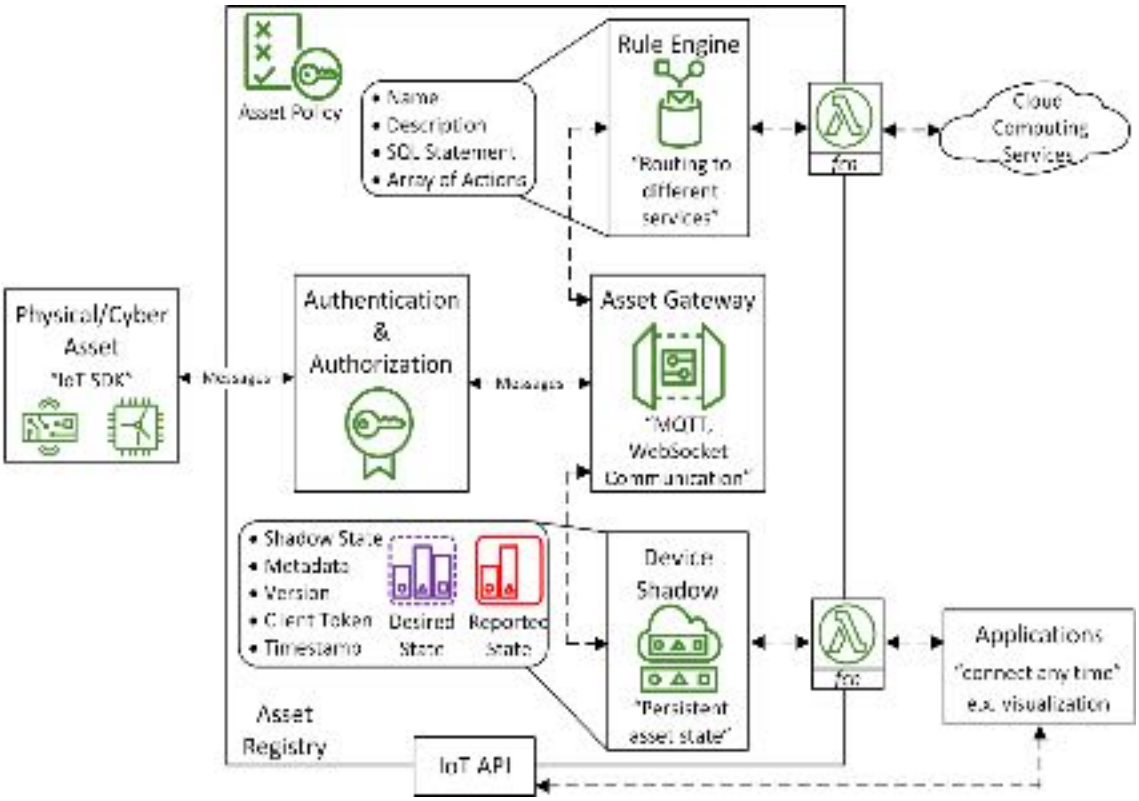


Figure 4.3: Physical/cyber thing registration on the IoT core.

4.3 Digital Twin Playground

The DT playground contains three components, that are working to produce the DT clones for different parallel applications. The DT constructor engine selects the model's types that are required for certain DT application. Then, the models are merged and configured to be one hybrid model. Finally, the hybrid model was added into the Luenberger Observer (LO) set up to estimate the system full state.

4.3.1 DT Constructor Engine

As shown in Figure 4.4, when a DT clone is requested for a certain application or study, the models' types are selected according to the application specifications from the previously discussed models as fast dynamics physical model, fast dynamics cyber model, slow dynamics physical model and slow dynamics cyber model. At that time, the healthy reported shadow states will define the known and the unknown states alongside the required estimated states to define the state-space inputs and outputs. After that, a series of state-space representation was used to merge the models into one hybrid model. The CPS hybrid models are combined into a single concatenation dynamical model as in the system in (3.3) and (3.4).

The Luenberger observer setup was used to put the constructed model into real-time interaction with the real physical/cyber system to estimate the full internal state by removing the noise and ride through the disturbance. Since the Luenberger observer delivers zero dynamics error if and only if the gain is chosen in the strictly stable region, the Luenberger weights are modified based on the predictions from a pre-trained deep-learning model, which has access of the last shadow states. The LO was constructed firstly for the full healthy state as,

$$\left.\begin{array}{c} \widehat{\mathcal{X}}_i(h+1) = \Lambda\widehat{\mathcal{X}}_i(h) + \Gamma\mathcal{U}_i(h) + \ell_i(\mathcal{Y}_i(h) - \widehat{\mathcal{Y}}_i(h)) \\ \widehat{\mathcal{Y}}_i(k) = \Upsilon\widehat{\mathcal{X}}_i(h) \end{array}\right\} \tag{4.1}$$

where $\widehat{\mathcal{X}}_i$ and $\widehat{\mathcal{Y}}_i(k)$ are the estimated states and outputs that is calculated according to the control input $\mathcal{U}_i$ and the shadow states $\mathcal{Y}_i$. Λ, Γ and Υ are hybrid merged model parameters. The LO weights ℓ_i was selected such that the eigenvalues of $(\Lambda - \ell\Upsilon)$ is stabilizable.

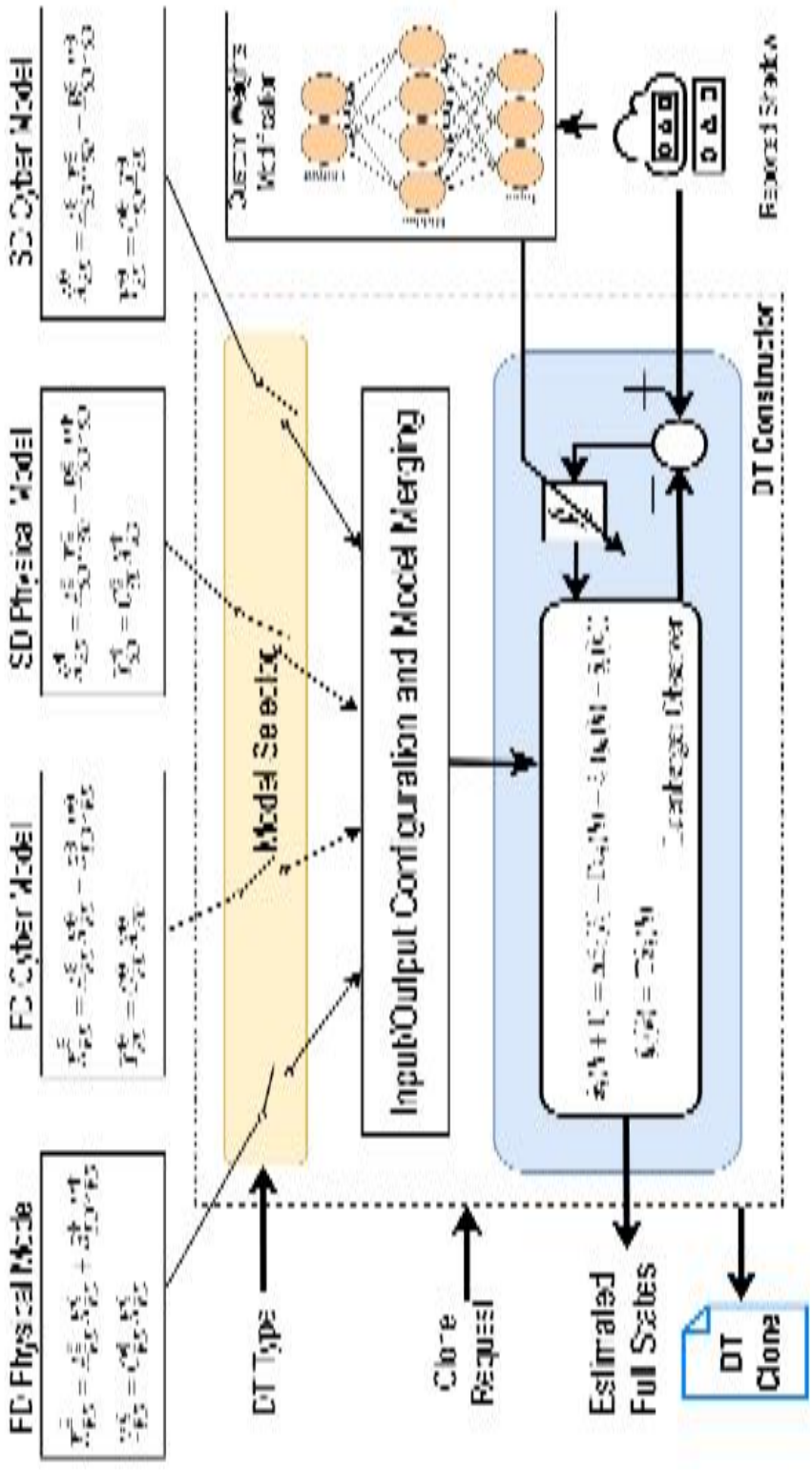


Figure 4.4: DT constructor architecture.

4.3.2 DT Playground and Applications Environment

As discussed in the last section, the DT constructor engine is designed to feed multiple applications with the DT clones according to the application requirements. The DT playground is the container that is used to launch the DT applications. In Figure 4.5, the DT constructor distributes the DT clones over the Applications (Apps.). The real-time reported shadow states are fed into each application's DT according to the type of the DT. The resulted computations and decision that are taken is updated also under the desired shadow sate field in the IoT core to reflect the DT decision into the edge controllers.

Many parallel applications can be launched in the cloud as ECPS environment for real-time reinforcement learning, grid optimization, power system security auditing, what-if analysis, microgrid fault-tolerant, and situational awareness. Figure 4.5 shows how some of these applications can be implemented in the DT playground.

The grid optimization Application utilizes the first clone (DT 1) as a predictor to optimize the grid operation by minimizing the fuel cost and losses while maximizing the benefits and renewable energy usage. Also, the DT predictor helps to cope with the variability and uncertainty of the large-scale PV and Wind energy penetration without violating the power system constraints. The DT 1 uses the shadow states updates to dynamically dispatch and aggregate the power from wide-area power system primary and secondary distribution to give the distributed controllers of the networked microgrid the life centric oversight, which effectively operate the grid.

The second DT (DT 2) represents the life model to answer the operator what-if question for various kind of study as the on-line N-1 contingencies, N-k contingencies and the power

system state estimation. Also, the What-If scenario App. can be autonomously configured using the operator APIs to define the recommended steps and decisions if an event is detected. For instance, if a large generator or a vital power transmission line is tripped, the real-time update of the DT 2 will use the last system topology and develop decisions such as rerouting the power to decongest the overloaded lines, load shedding to restore the stability or activating ESSs to restore the system to its normal state. The existence of the on-line DT with the last system state will accelerate the restoration process, prevent the cascaded outage, and minimize the blackout region.

The cybersecurity of the distributed control graph is very critical for the secondary and tertiary control systems. In this application, two DTs (DT 3, DT 4) are utilized to check the consistency of the distributed control actions with the physical system real-time states. DT 3 is designed as a physical system observer to estimate the physical system full state and DT 4 provides the cyber system dynamics. For instance, if the distributed SCA is working to make consensus on certain power-sharing and one of the control agents is attacked. The Satisfiability Modulo Theory is developed to authenticate the cyber control action by comparing the cyber states (DT 4 estimates) and the last physical measurements (DT 3 estimates) to detect the attacked control agent and isolate it from the control process. The benefits of that the cloud centricity can discover even the multiple coordinated attacks on the cyber system.

Since the power system is a highly non-linear complex system, the regular decision making, control and management techniques cannot guarantee the safe operation of the grid especially during the risks of catastrophic situations.

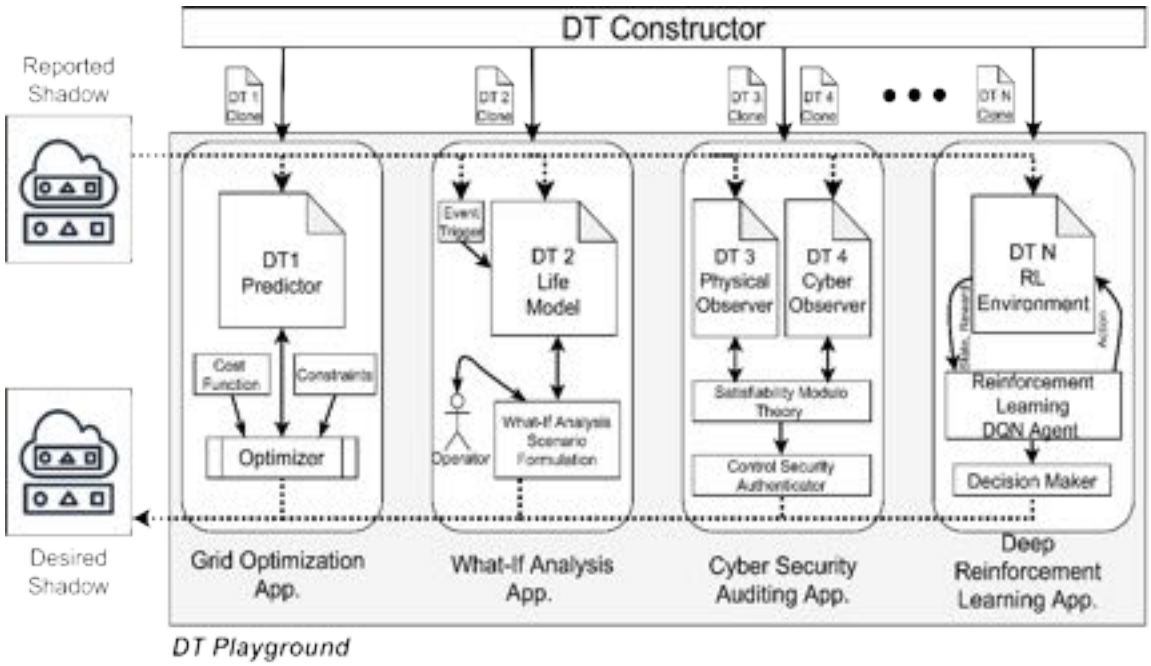


Figure 4.5: DT Playground and Applications Environment.

The deep reinforcement learning (RL) techniques can get the best possible actions to take for unexpected cases in a fast and autonomous way without human intervention. The RL requires an environment to learn and after many iterations of taking actions, observing the states and collecting the rewards, the controller can provide out of the box solutions. Adding the life DT as a safe environment, which the RL agent can manipulate and get real feedback from the system can boost the abilities not only during the learning process but also with the real-time interaction with the grid. Also, the actions taken by the agent will be safe since it is a digital clone. In this Application, a deep Q network (DQN) is utilized as an RL agent to deal with the DT N environment.

4.4 Digital Twin Practical Experimental Implementation

The ECPS DT is demonstrated by implementing the physical and the cyber layers of the networked microgrids (MG) using interconnected embedded computers as a multi-

agent platform. Figure 4.6 shows eight microgrids' agents and a single PCC agent that is executed on nine Raspberry Pis™ and communicate using Wi-Fi [63].

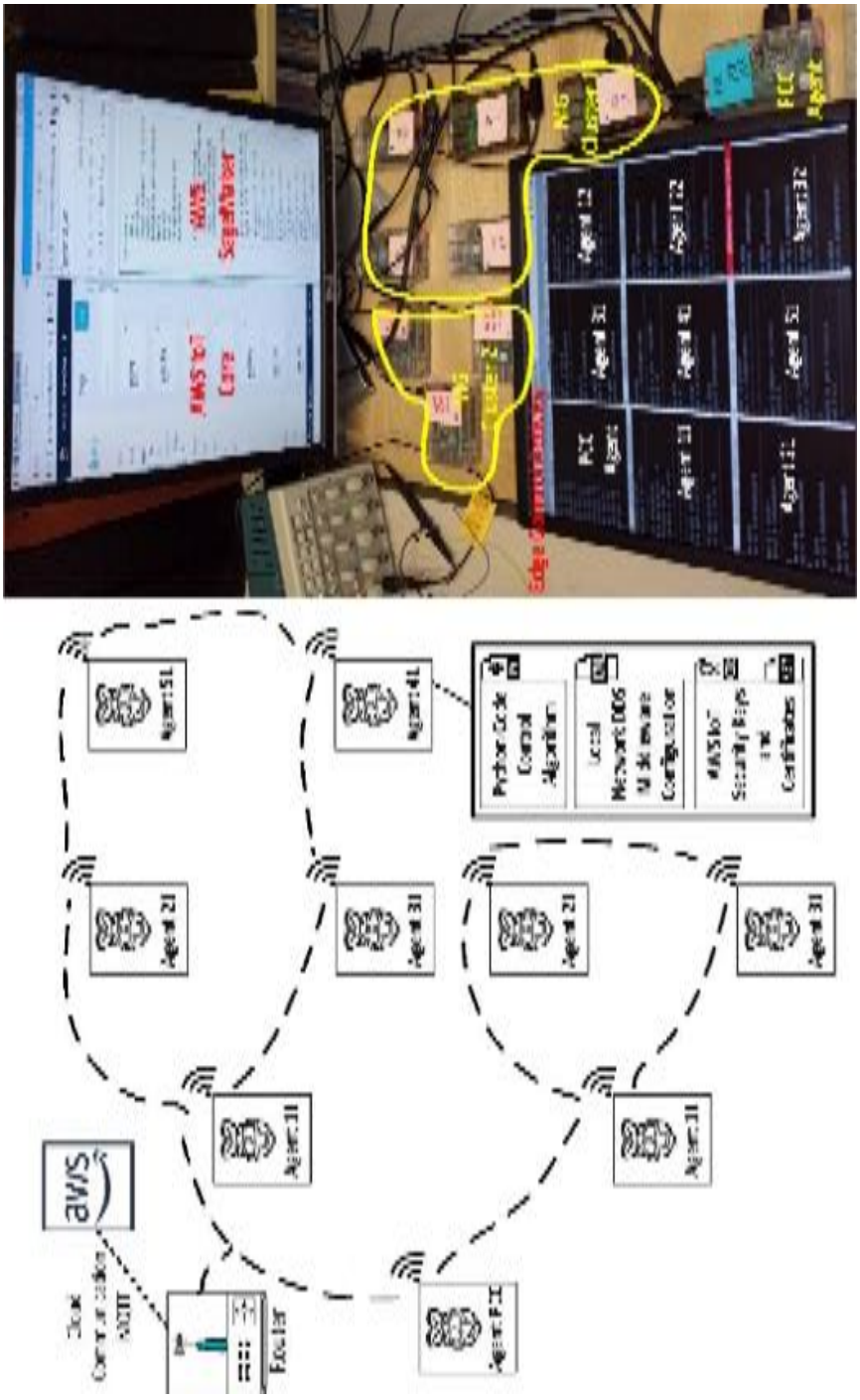


Figure 4.6: Practical ECPS DT implementation.

The Data Distribution Service (DDS) communication middleware was used to launch the data sharing among the distributed controllers/sensors as a cyber layer [64]. The DDS uses the publication/subscription mechanism without a message broker for the data sharing, which guarantees high-speed connectivity among the networked microgrids, and communication configuration is performed in extensible markup language (XML) files for each agent. The Python programming language is used beside the AWS cloud system. The ECPS-to-AWS communication is performed via the Message Queuing Telemetry Transport (MQTT) protocol, and the data are initially hosted on the AWS IoT core [65].

Figure 4.7 shows the distributed consensus control algorithm that is implemented on each control agent in the cyber system and its interaction with the DT on the AWS cloud. Firstly, the agent is initialized with the adjacency weighting factors. Then, DDS communication is used to listen to the agent's neighbor and continuously check for an event that requires a consensus on new sharing power.

After the agent neighbor's data are accepted, the local control objective is updated based on the consensus rule. Finally, the pre-event and post-event states are reported by using the MQTT update function on the AWS cloud. Moreover, the desired state or DT-based guides are submitted to the edge via the MQTT get to function. These signals can be configured according to the applicable nature of the DT.

Figure 4.8 shows the implemented DT on the cloud system. Practically, the AWS SageMaker is used to perform the required computations and DT functions. This service can hold parallel instances of computation by utilizing the IoT core shadow data or the data stored in the database.

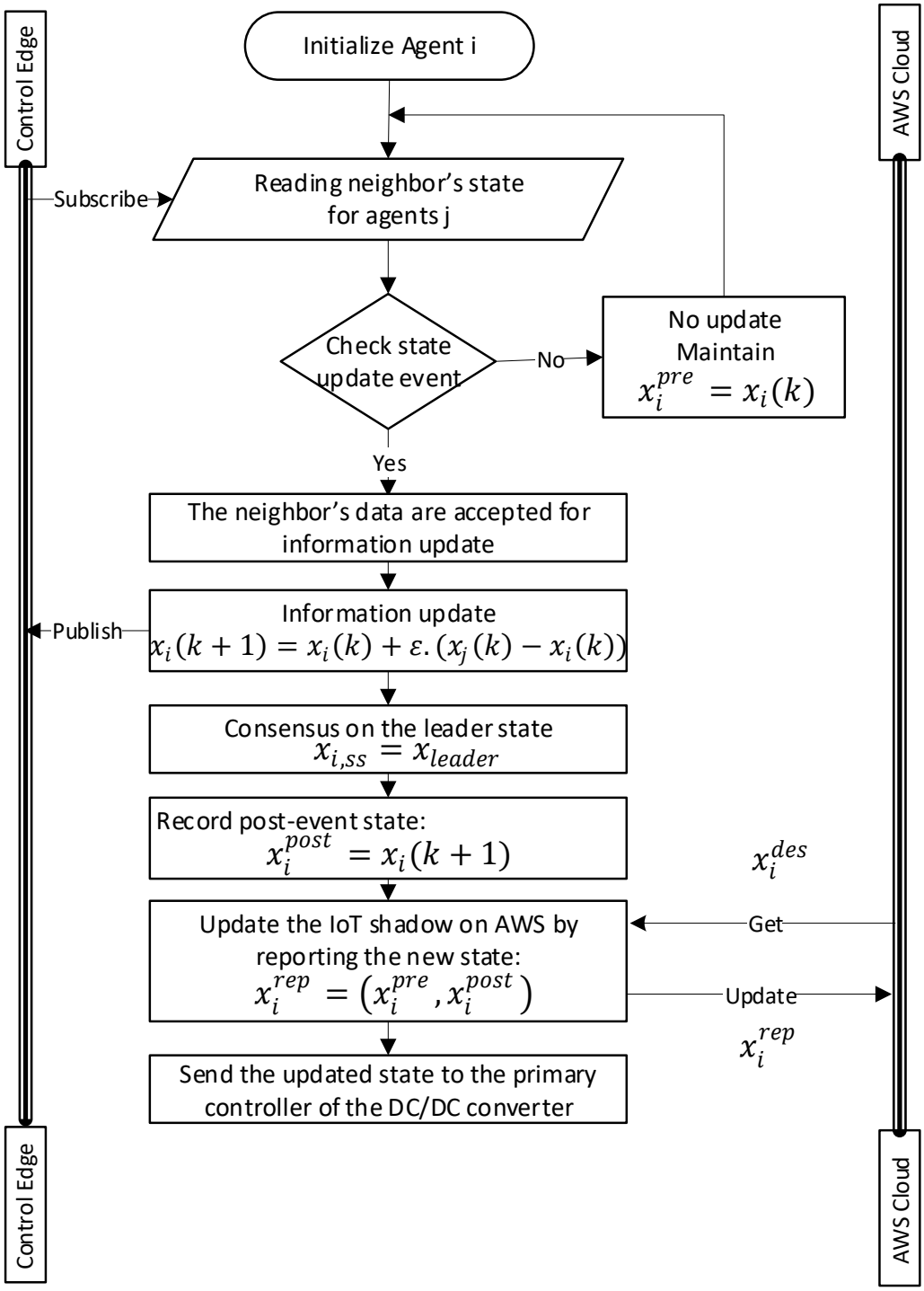


Figure 4.7: Distributed controller algorithm on the edge interaction with the DT on the AWS cloud.

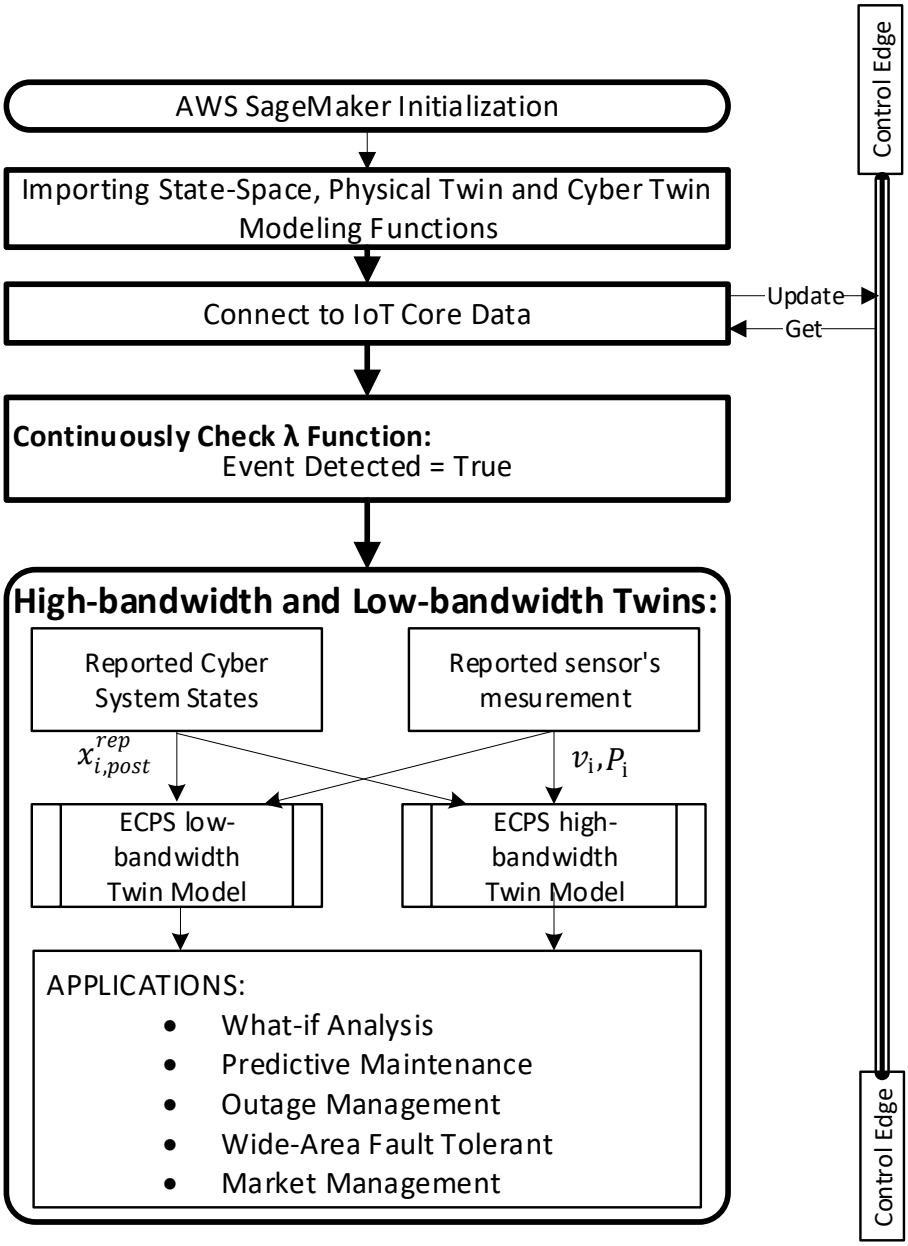


Figure 4.8: DT implementation on AWS cloud.

The parallel instances can be implemented and scaled according to the required application. The state-space modelling of the physical and cyber twin model is implemented and imported as functions to implement the low and high-bandwidth physical DT alongside the cyber DT models on the AWS SageMaker.

To reduce communication bandwidth and minimize the computational burden, the AWS Lambda function is used to trigger the application by continuously monitoring the detected event. Using the models previously discussed in (3.5), (3.11) and (3.19)–(3.20), the digital replica of the energy cyber-physical system is constructed to be utilized by different applications.

Both the reported sensor measurements (voltages v_i and injected power P_i) and the reported post-event cyber states ($x_{i,post}^{rep}$) are ported to the online Digital Twin models. According to the applicable nature, the desired commanding and decisions can be submitted back to the edge to achieve the requirements.

In the same way, after the application decisions are made, the desired commands are set back to the desired shadow state on the IoT core. The controller on the edge gets the desired states as centric oversight guidelines, which are used to guarantee the global system operation objectives. Thus, the DT creates digital parallel environments for the safe application of the control command on the twin before giving the edge controllers the final guides.

4.5 ECPS DT Experimental Initial Test Results

The first case study is implemented using the low-bandwidth model. Two clusters of microgrids are implemented on MATLAB/SIMULINK as a detailed physical model, and the CPS data are sent to the AWS cloud IoT core in terms of shadow states. The system contains a collection of diesel generators (conventional generators), PV–wind mixtures (renewable generators), ESSs and loads (fixed and flexible). On the other hand, the AWS has the state-space representation as shown in Table 3.1 to construct the physical twin and

the system in (3.20) to represent the cyber model. The model uses the loading profile and the forecasted renewable power to estimate the dispatching of the resources. Figure 4.9 and Figure 4.10 shows matching between the DT model and the physical states.

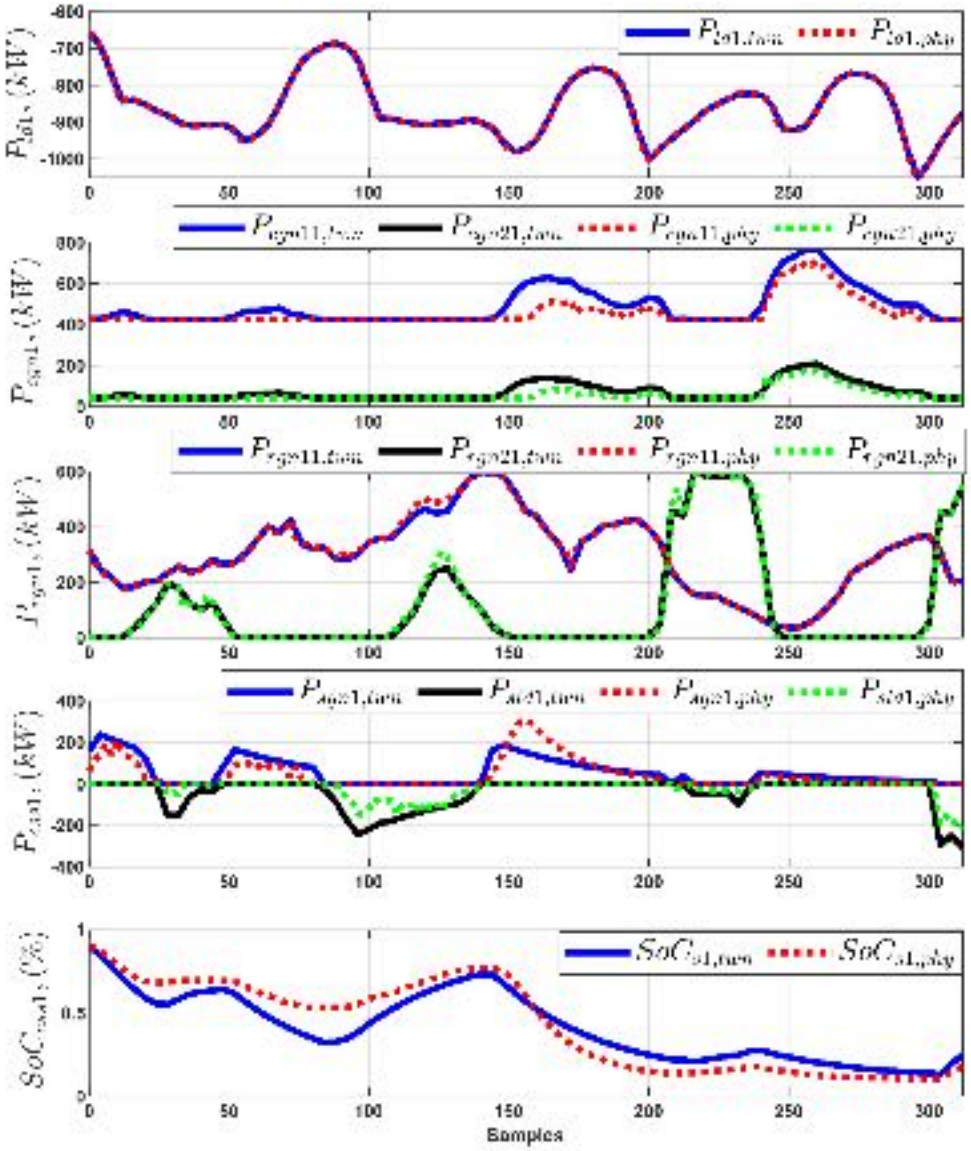


Figure 4.9: A comparison between the low-bandwidth physical DT model and the physical measurements for MG cluster 1.

The low-bandwidth model has a 15 min time slot for the AWS shadow update rate. Figure 4.9 depicts a close relationship between the digital twin estimated states and the

physical states of first cluster states, which are the aggregated demand, conventional generation, renewable generation, aggregated ESS charge/discharge power and state of charge. The second cluster, which is shown in Figure 4.10, presents the ability of the DT to mimic the physical response. The high-bandwidth twin model is evaluated as shown in Figure 4.11 and Figure 4.12.

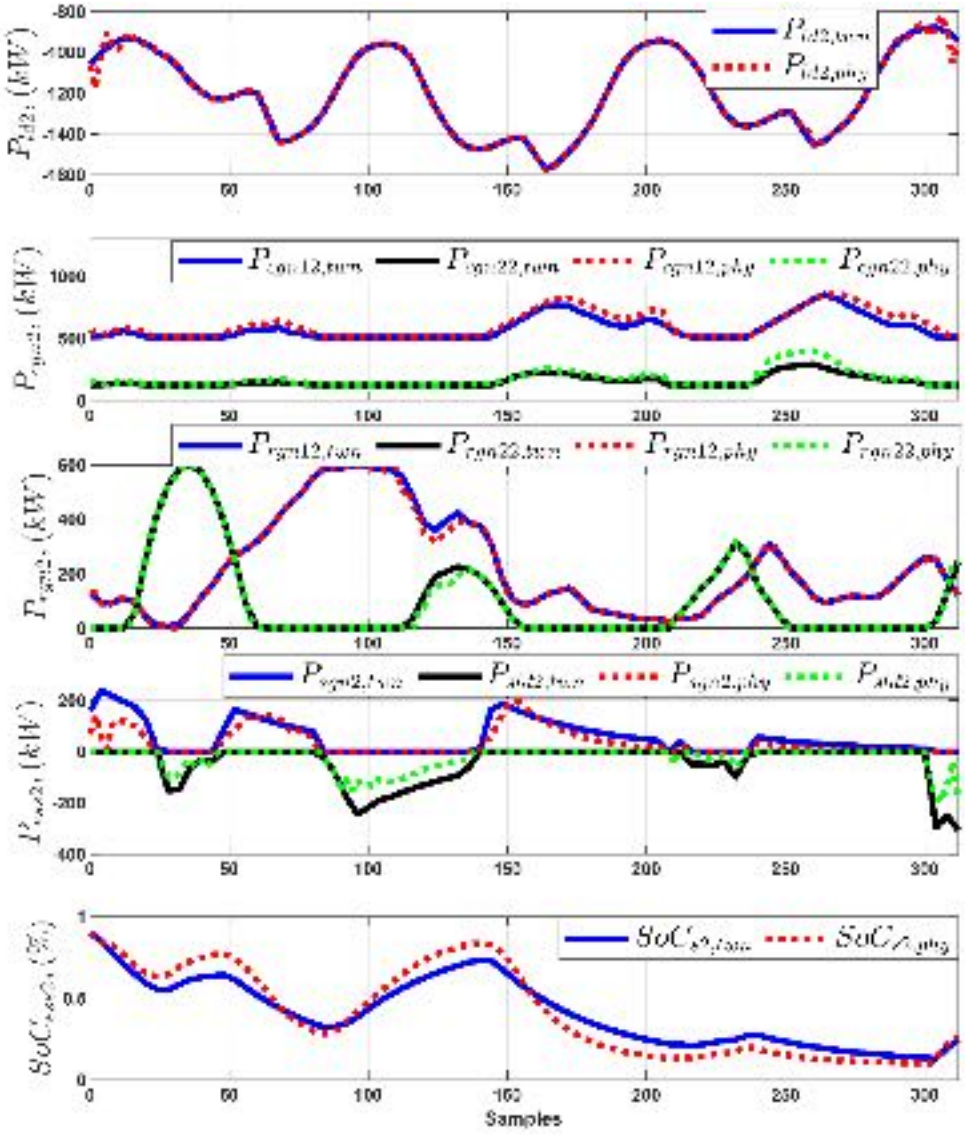


Figure 4.10: A comparison between the low-bandwidth physical DT model and the physical measurements for MG cluster 2.

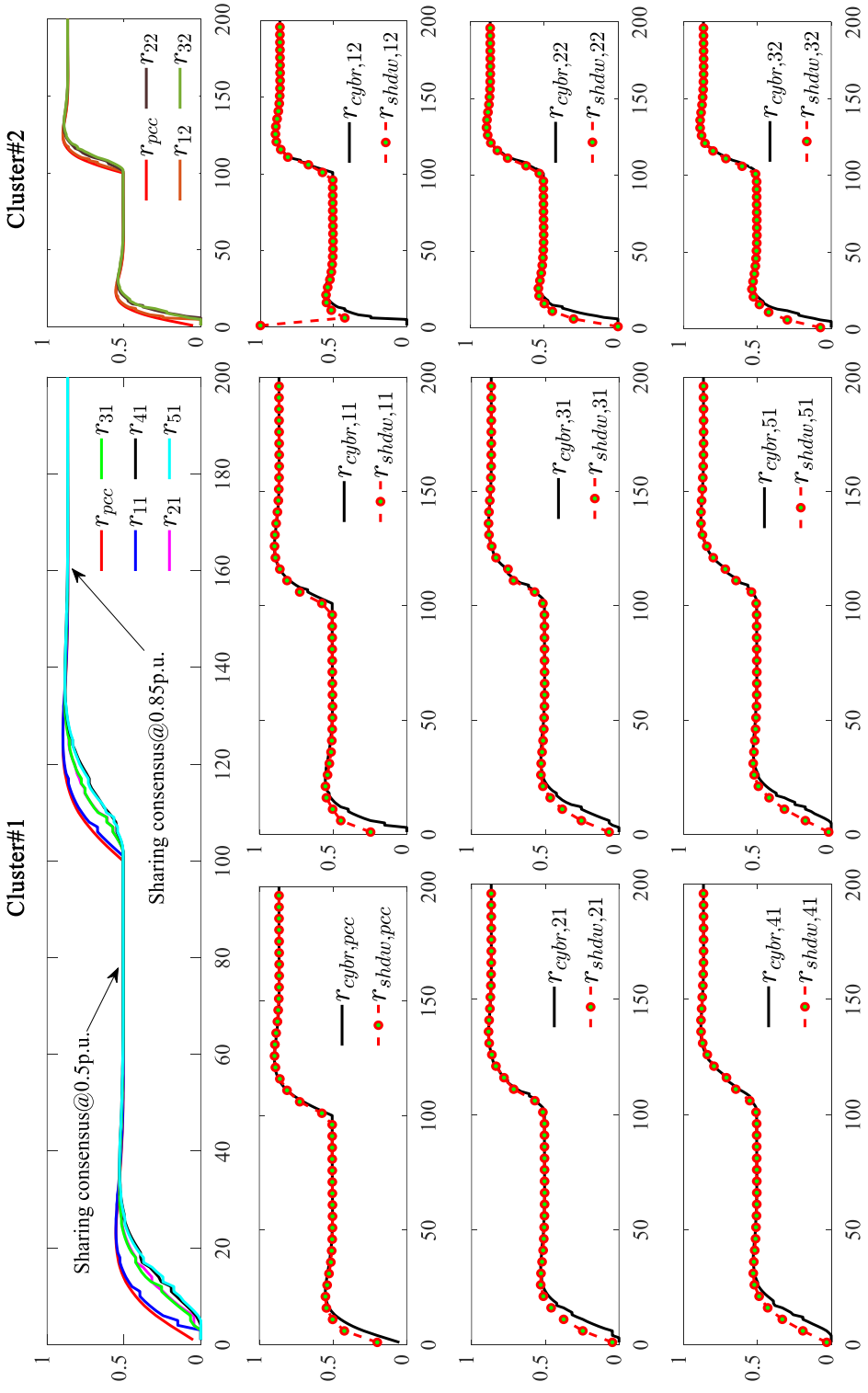


Figure 4.11: A comparison between the cyber states and the shadow states on the AWS.

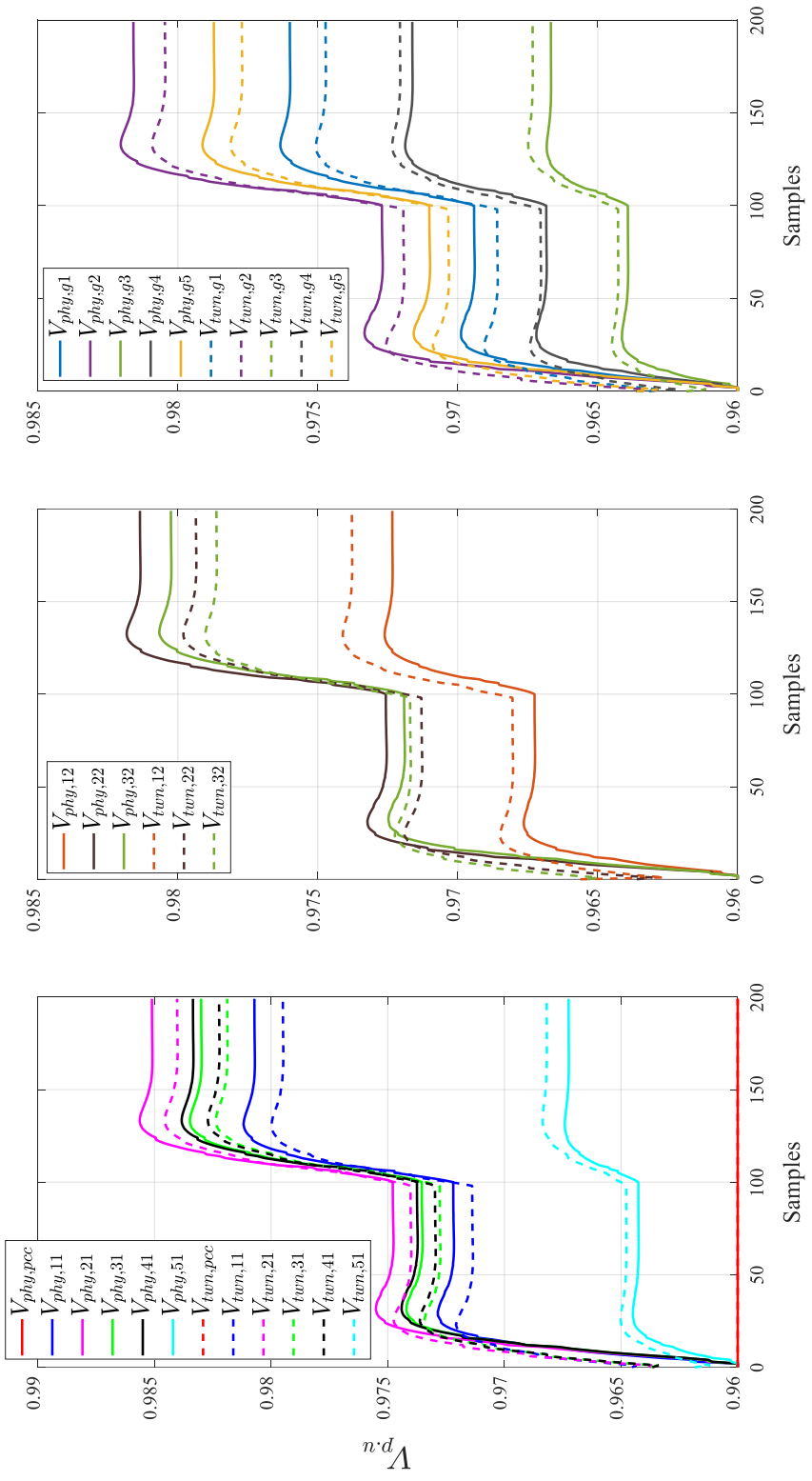


Figure 4.12: A comparison between the cyber DT model and the cyber states.

The secondary distributed control system controls the microgrids' interlinking converters to share the power among the microgrids to support the voltage at the PCC. The implemented control agents on the embedded computers send their information (sharing factors) to the AWS cloud. The implemented DT in AWS SageMaker uses the sharing factor shadows to estimate the voltage at each bus in the interconnected microgrids. The figures show that the DT can replicate the actual system.

Figure 4.11 illustrates the power-sharing factor consensus under two consecutive changes (0.5 and 0.85 per unit in the reference at the PCC. The delay between the cyber edge states (black) and the shadow updates (red dots) is due to the Wi-Fi communications. The provisioned shadow states are used to drive the high-bandwidth model to mimic the physical voltage measurements at each bus, which show a very close response as illustrated in Figure 4.12.

The results showed the ability of the developed models to be a live digital replica of future power systems. The authors are currently developing a combination of deep learning and the DT to implement a wide-area situational awareness system by considering the stability, reliability and resiliency of the globally interconnected power system. The developed DT aims to guarantee to mimic the dynamics and events in real time.

Chapter 5 Digital Twin-Based Smart Grid Management

The smart grid energy management of the variable renewable energy resources presents many challenges to the grid operation. An optimized solution to manage the available resources is necessary to achieve reliable operation. This chapter presents the Hierarchical Distributed Model Predictive Control (HDMPC) to solve the energy management problem in a multi-time frame and multi-layer optimization strategy. The HDMPC combines the centric oversight of the digital twin-based management layer and a downstream layer, which hosts the distributed coordinated management layer. The information exchange and interoperability between different layers are provided through the data-centric communication approach. The DT-based supervisory manager (SM) works to present the grid operator with certain operational plans and gives the guidelines to the CM (lower layer). The CM has the responsibility to coordinate the relationship between the centralized optimization objectives and the physical power system layer. The developed HDMPC control was verified both numerically as well as experimentally. The obtained simulation results show that the control strategy developed here is successful and combines the benefits of both the centralized and distributed control for a global solution of the grid operation problem. The experimental results demonstrate the feasibility of the real-time implementation of the developed system for deployment to control future smart grid assets.

5.1 Introduction

Variable renewable energy sources are important for future smart grid operational plans. The high penetration of these resources creates a challenge for smart grid operation and management. Power variability and uncertainty has problematic stochastic nature. In

addition, the accommodation of new technologies, such as distributed generation, prosumer integration, microgrids and electric vehicles increase the system complexity in all levels of operation. All these sources of complexity are significantly magnified in the case of large scale system management [1], [66], [67]. The grid management problem is a control problem and works to determine the input set-points for all energy units to balance the generation/load combination at a minimum cost under certain system conditions. Therefore, the grid management problem is considered as an optimization problem and has the ability to optimize the grid operation under the high level of uncertainty of the sources [67]–[70]. Model Predictive Control (MPC) is widely applied to high-end control technology with high performance and has many industrial applications [71]. MPC major advantages are a combination of control and optimization solutions. It can handle a multivariable optimization problem simply with minimum error [72], [73].

From the control architecture point of view, to manage the future grid under these challenges, many distinct control strategies are demonstrated to solve these problems as centralized, decentralized and distributed control systems. The centralized control could achieve the best performance if it is applied properly. However, large-scale systems with a high number of states, inputs and outputs become an enormous computational and communication burden. The centralized control system imposes higher complexity for the large systems and lacks scalability for further expansion plans [68], [69], [74]. On the other hand, the decentralized control strategy has many advantages, such as less computational burden and enough flexibility. However, the decentralized approach has bad performance especially in large-scale systems [72].

Distributed control techniques were successfully introduced in order to achieve close performance as centralized control [74]–[77]. Benefits relating to the flexible topology of the decentralized control alongside with the closed-loop stability performance is guaranteed in distributed control philosophy especially in large-scale networked systems as power system and chemical system plants [78]–[81]. Nevertheless, the design and coordination among these controllers are very complex, especially for large-scale systems like the electrical grid. Additionally, every local controller could be coordinated with its neighbors only and the global control performance is not achieved [3], [21], [67], [72], [73], [82]. Although the application of the cooperative distributed control in large-scale power system has the same decent performance as the centralized control in nominal conditions, it lacks robustness with the existence of the data uncertainty or communication failure [23], [83], [84]. In order to consider the uncertainty, the authors in [24] introduced the hybrid Q-learning adaptive approach with the distributed MPC to cope with the uncertainty effect. In [84], a comparison between the centralized, distributed and hierarchical distributed control reveals that under uncertain data, the hierarchical distributed MPC achieve robustness. In addition, the hierarchical cooperative distributed model predictive control is introduced in [85] to deal with the communication error and delay issues. Correspondingly, the hierarchical distributed MPC is introduced in many research works [5], [86]–[88]. The multi-layer hierarchical control system can deal with the multi-vision control objective in a clear way. Any system can be decomposed into different layers with the purpose of not only breaking the problems in size, but also reducing the calculation frequency as the size of the problem increases.

Since the control and communication infrastructures are dependent, both architectures noticeably depend on the nature of the smart grid application. There are many communication approaches in smart grid applications, like message-centric and data-centric approaches [21]. The data-centric approach is preferred over the message-centric approach in the context of smart grid application due to interoperability and system expandability. The data distribution service (DDS), which has a unique feature to improve smart grid communication, can be used in many smart grid applications as a middleware [64], [89], [90]. In this chapter, by combining the effectiveness of centric oversight of the DT on the cloud and MPC as a predictive optimization technique. The DT based HDMPC is introduced for the energy management strategy in the smart grids. The contributions of this work can be summarized as follows,

1) A new energy management strategy for smart grid operation is introduced. The developed strategy expands the control time horizon into multiple visions to overcome the forecasting error in the high penetration of variable Renewable Energy Resources (vRES) forecasting error, which enhance the robustness of the smart grid operation.

2) An aggregated mathematical model using state-space representation is formulated for the large-scale energy system. In addition, a large-scale model decomposition technique is developed to deal with the high variability and uncertainty in the smaller balancing areas. The novelty in the developed model is the concentration on the holistic optimal cost-effective operation of the grid in the first layer and ensuring the robust solution against the high variability of RES in the smaller areas

3) A model predictive control optimization problem is hierarchically formulated using the aggregated (DT model) and the decomposed models into the centralized (SM) and distributed (CM) management layers. Furthermore, the coordination between the hierarchical layers is implemented in terms of translating the grid operator plans into a stream of set points to the physical layer controllers. The coordination is established to provide both global and local optimal operation with maximum security with a higher vRES share.

4) A data-centric middleware is designing and implemented based on Data Distributed Service (DDS) to exchange the information, control command and provide interoperability between different layers and controllers. DDS ensure data availability and increase the data flow flexibility in case of any communication failure.

5) A practical smart grid testbed and AWS cloud computing, which merge the real-time cyber and physical systems implementation to verify the developed system.

5.2 Energy Management System Description

According to the hierarchical control strategy, the developed management system is organized into three layers. Each layer has its own function, deals with certain grid parts and sees the grid in different time horizons. The first layer represents the physical system, which has the primary control and deals directly with each unit in the large-scale system. In addition, the primary control drives the control action with a minimum control time horizon (e.g. 5 min.). The upstream layer is considered as the coordination between the overall system management (supervisory) and the downstream physical system controllers. It deals with a set of interconnected units (grid area) and gives the management guides to

the physical system every CM time horizon. The supervisory manager is established on the top of the hierarchical management system. It interacts generally with the overall system via the coordination manager and it works in a higher time horizon (e.g. 15 min.).

As shown in Figure 5.1, the physical layer contains interconnected energy units, which consist of conventional generation units (as for thermal, coal or nuclear), renewable generation units (as solar, wind and hydro), storage units and demand units. The large-scale physical system is classified into multiple interconnected areas, $\mathcal{O} = 1,2, \dots, N_A$. The second layer is the Coordination Management (CM) layer, which has a manager for each area $CM_{\mathcal{O}}$. After that, the Supervisory Managers (SM), which is based on the DT gives the guides to the CMs and gets the feedback to derive the overall system according to the overall operational plans and objectives that are given by the grid operator.

The design and implementation of the upper two layers are introduced. Each layer is supposed to satisfy certain functions. SM is responsible for the whole grid operation and it is considered the main interface with the human operator. The management/control horizon of SM is set to hour-ahead in order to meet the grid and market changes in appropriate time. Therefore, the load and vRES forecasting is set to be every 1 hour. SM concerns only the aggregated overall system management (individual unit operation is not supported). Finally, SM works for the interaction between large-scale market operations. CM has an area management role and works directly with the physical grid controllers and coordinates the relationship between the centralized SM and the physical system layer. The control/management action scanning frequency is set to be lower than the higher layer and higher than the physical layer.

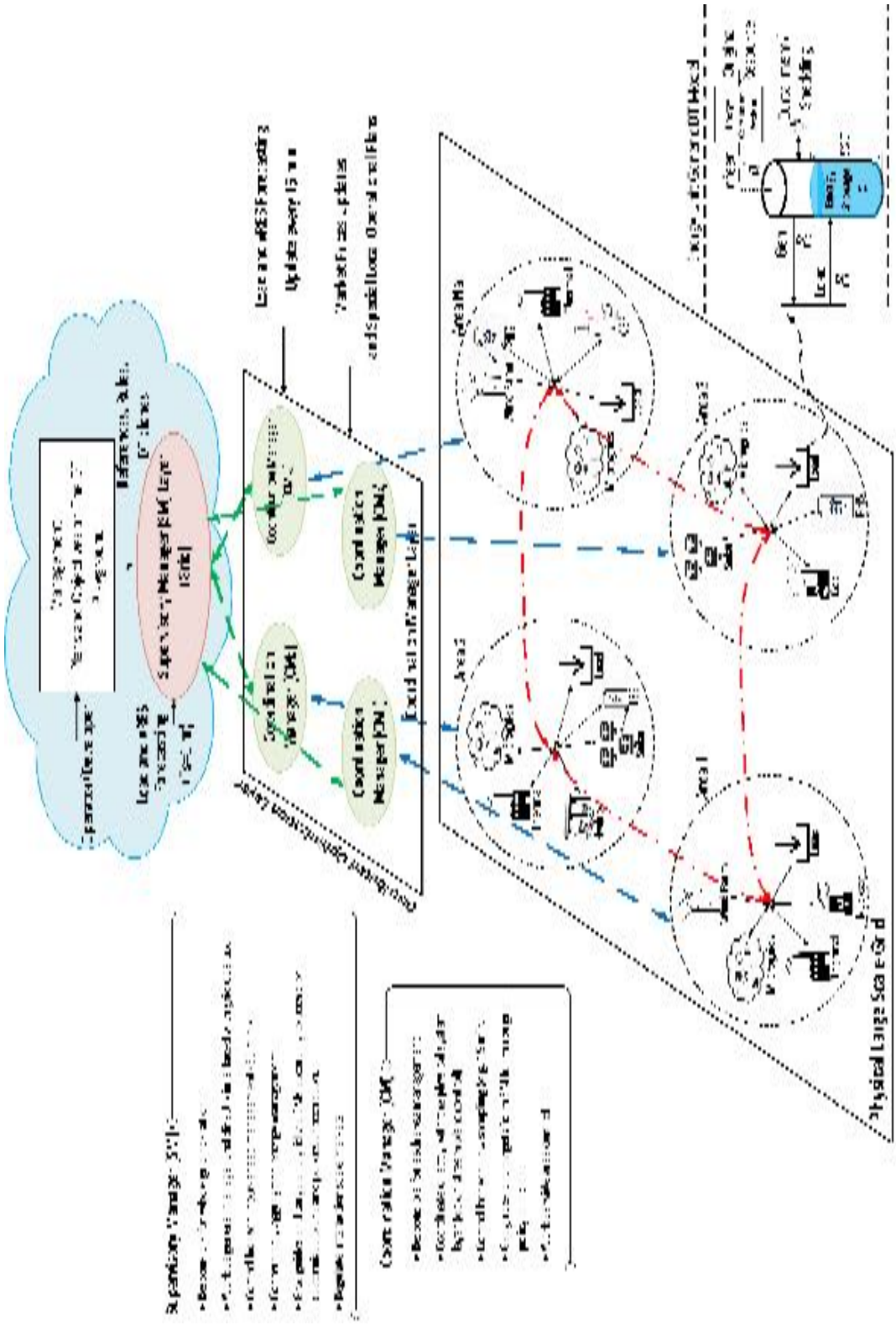


Figure 5.1: The DT-based HDMPC energy management strategy.

The CM deals as a wide area control system and it gets guides and targets from SM to satisfy the global grid policies and plans. This layer has a smaller forecasting time horizon for load and vRES as a disturbance. CM gets the market price updates or special local operation plan changes upon the local changes. The physical system feedback is reflected CM and CM, feedback is reflected in SM.

The Step-by-Step description of the developed energy management system is listed as follows:

1) The grid operator assigns the management operational plans, requirements and market transactions rules on the cloud for the digital twin playground.
2) The SM objective function and the DT model is constructed according to the operator plan needs by assigning the objective function's weighting factors and the constraints.
3) The SM optimizer solves the optimization problem iteratively, which is subjected to the demand and renewables hourly forecasting alongside the references trajectory to generate the manipulated power setpoints.
4) The DT dynamic model is used to calculate the setpoints and the actual feedback from the system to adjust the future stet-points.
5) The SM optimizer solves for the current slot and predicts the future slots according to a pre-defined prediction horizon.
6) The best SM solution is published to the CM layer as a target for guiding the distributed control system layer through the global optimality.

7) In the second layer, each area in the distributed layer should follow its own objective weights, forecasted measured disturbances and DT targets without any information from its neighbouring areas.
8) The CM optimizers solve the control problem by the same steps in 3 to 6 with a more detailed area model and local data.
9) The CM provides its optimal solution of the manipulated power setpoints to the physical layer downstream controllers
10) The CM layer gets the feedback from the physical system to correct its trajectory and submits its feedback to the cloud again for future time slots.

If one of the communication links between CM and SM is subjected to a failure, this one will activate the conventional distributed architecture and the data exchange will be between it and neighbors CM. The exchanging data flow is enabled by the DDS middleware using the QoS policy, which is aware of the lost data.

5.3 DT Modelling for The SM Layer

5.3.1 Energy Units Modelling

As discussed in Section 3.3.1.1, In order to obtain large-scale modeling, the energy systems are simplified and represented as a comprehensive power node, and mathematically formulated using the state-space equations. Besides the model in (3.5) and Table 1.1, the interconnected grid configuration is represented by the balancing equation of the generation/load combination. The representation of the power system depends on each layer specifications. In the physical layer, the model is formed in detail for each individual unit in the system. In contrast, the CM layer is assigned to represent the

aggregation of each area in the grid. On the other hand, the supervisory layer works with the overall aggregated grid model.

$$0 = \sum_{i=1}^{n_e} P_{g,i} - \sum_{i=1}^{n_e} P_{L,i}$$
$$0 = \sum_{j=1}^{m} P_{in,j} - \sum_{j=1}^{m} P_{out,j} \quad (5.1)$$

5.3.2 Hierarchical Layers Modelling

A large number of units imposes extra complexity to the modelling process, therefore an aggregation process with respect to an energy type to make the optimization problem less complexity. These aggregations not only provide the simplicity of the model but also affords better abstraction to set the grid operator's commands and operational plans.

In the light of the aggregated DT model in the supervisory manager, the coordination managers should work to satisfy the optimal targets from the SM and deal with variable, uncertain and unforeseen changes in a smaller time horizon. Consequently, the grid model should be decomposed into areas breakdown and that represents another grand challenge. In order to formulate the decomposed model, the vital data should be defined for such a system to exchange it within the CM layer and between SM, CM and physical layers. According to the pre-defined operational plans, the exchanged data and the coordination configuration are defined to achieve the required performance.

For instance, the key variable to be exchanged between the two layers is the interconnected shared or transmitted power between neighbor areas. According to the pre-

defined price of area-to-area power transactions, the SM define the optimal amount of power to be transferred to satisfy both the profit and security perspective. After that, the CM layer should follow this SM target by dispatching the power among the energy units to achieve the target of the transmitted amount.

Model Predictive Control is the developed technique in the two hierarchical layers of management. MPC depends mainly on the simplified model by obtaining the state-space model. The upper management layer (SM) depends on the overall grid DT, while the lower management layer subjects to the overall model decomposition in terms of interconnected areas. The mathematical formulation of the hierarchical model is divided into two representations as follows. Figure 5.2 shows the decomposition of the overall grid model into portioned areas.

5.3.2.1 Supervisory Manager Layer Modelling

Suppose an interconnected power system grid is represented as i^{th} energy has n_u manipulated variables and the grid interconnection points are n_v . In order to describe the grid in a simplified way, the system is characterized by the state-space form using a linear discrete-time model as follows,

$$\left.\begin{aligned} x^{sm}(k+1) &= A^{sm}x^{sm}(k) + \Gamma^{sm}\mathcal{J}^{sm}(k) \\ 0 &= E_v^{sm}u^{sm}(k) \\ y^{sm}(k) &= C^{sm}x^{sm}(k) + y^{sm}(0) \end{aligned}\right\} \tag{5.2}$$

where $\Gamma^{sm} = [B_u^{sm} \quad B_d^{sm}]$, $\mathcal{J}^{sm} = [u^{sm}(k)^T \quad d^{sm}(k)^T]^T$. The SM model outputs $y^{sm}(k)$ is directly depends on the states $x^{sm}(k)$, and has initial conditions $y^{sm}(0)$.

Equation (5.2)(5.1) represents the aggregated system discrete model, which is used to design the SM controller. It characterizes the system using the state-space parameters A^{sm},Γ^{sm} E_v^{sm} *and* C^{sm}. Those parameters are calculated according to the energy units' model and the grid interconnection. The controller uses the model to predict the system response to the control input u^{sm} and generates the proper control action, which satisfies the error between the reference trajectory and the system output, y^{sm}, which represents the storage system state of charge. It is worth mentioning that the model is forced by the load and renewable energy profiles, which are represented here as a disturbance d^{sm}.

Although the large-scale physical system representation might add complexity to the system, the overall system model aggregation works to reduce this issue, and to enforce the model effectiveness. The detailed model is decomposed as discussed in the following section. Moreover, the states and the controlled inputs are limited by the following constraints,

$$\left.\begin{array}{l} x_{min}^{sm} \le x^{sm} \le x_{max}^{sm} \\ u_{min}^{sm} \le u^{sm} \le u_{max}^{sm} \\ y_{min}^{sm} \le y^{sm} \le y_{max}^{sm} \end{array}\right\}, \quad \forall\, k \tag{5.3}$$

5.3.2.2 Coordination Manager Layer Modelling

The coordination role of the lower management layer (CM) makes the overlap between the centralized management layer (SM) and the physical system layer of the power system. The whole system model is decomposed into multiple distributed managers. Each individual manager in the CM layer has the responsibility to give the setpoints to the physical system controller.

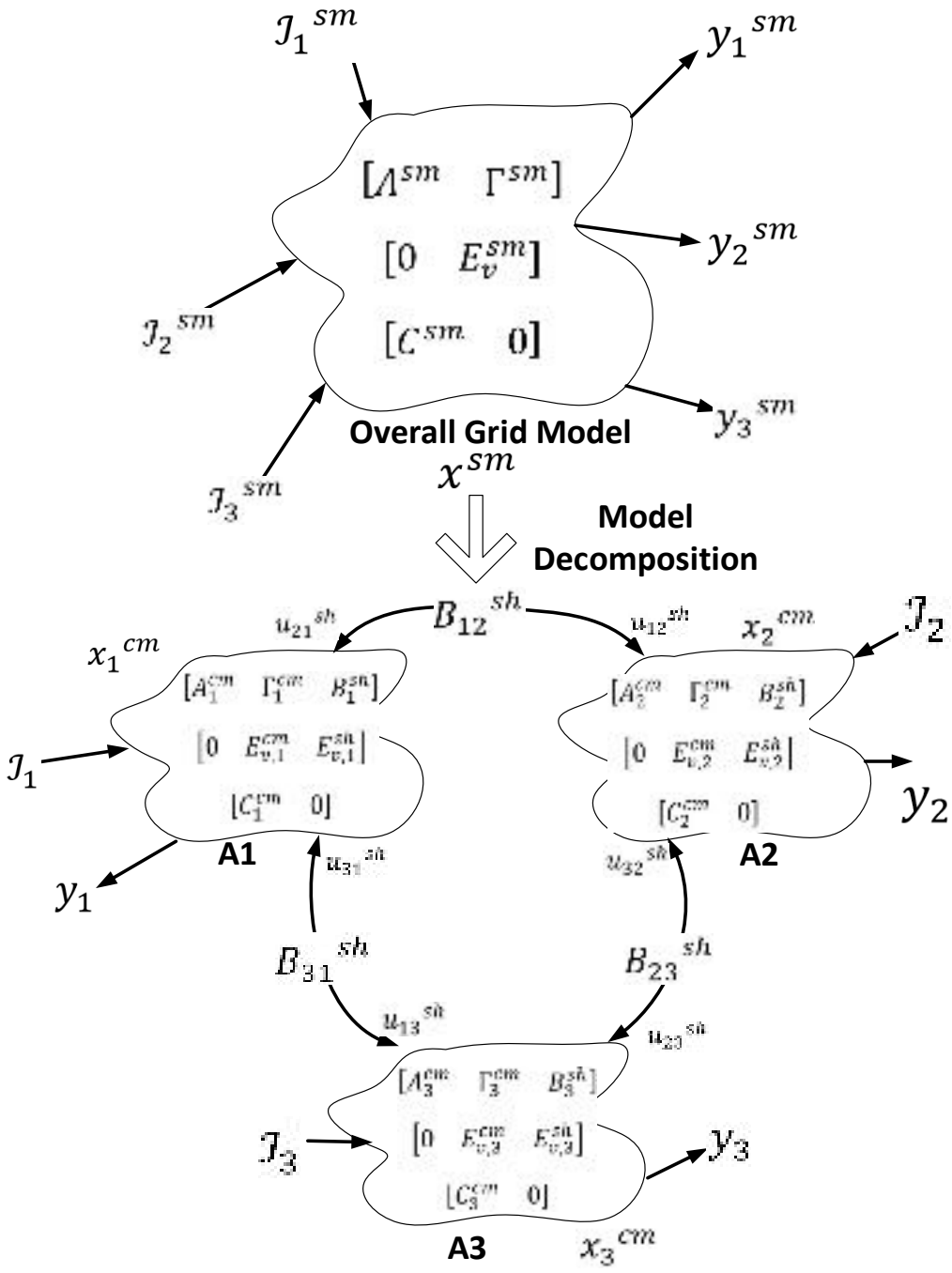


Figure 5.2: Overall system model decomposition.

According to the nature of the power system topology, the power system areas are connected to each other via tie lines. Therefore, each MPC has its own model of a certain area. In order to manage the physical system via distributed managers, the availability of

centralized data has a vital role to guide the distributed optimization problem to satisfy the global system objective. The centralized information from SM is utilized in the CM layer for the purpose of guiding and targeting, which represents the overall management strategy.

Consider a unified power system consists of $\mathcal{O}^{th}$ subsystems (areas), and the control action time is taken every p. The sampling time here is Δt^{cm}, and it is hierarchically smaller than SM input sequence $\Delta t^{cm} < \Delta t^{sm}$. By the same way as SM layer, each area is represented as follows,

$$\left.\begin{array}{c} x_{\mathcal{O}}^{cm}(p+1) = A_{\mathcal{O}}^{cm} x_{\mathcal{O}}^{cm}(p) + \Gamma_{\mathcal{O}}^{cm} \mathcal{I}_{\mathcal{O}}^{cm}(p) + B_{\mathcal{O}}^{sh} u_{\mathcal{O}}^{sh}(p) \\ 0 = E_{v,\mathcal{O}}^{cm} u_{\mathcal{O}}^{cm}(p) + E_{v,\mathcal{O}}^{sh} u_{\mathcal{O}}^{sh}(p) \\ y_{\mathcal{O}}^{cm}(p) = C_{\mathcal{O}}^{cm} x_{\mathcal{O}}^{cm}(p) + y_{\mathcal{O}}^{cm}(0) \end{array}\right\} \quad (5.4)$$

where $\mathcal{I}_{\mathcal{O}}^{cm}(p) = [u_{\mathcal{O}}^{cm}(p)^T \quad d_{\mathcal{O}}^{cm}(p)^T]^T$ is the vector of the manipulated inputs and measured disturbances. On the other hand, the interconnection described by nodes and edges within the same area, which is obtained by $E_{v,\mathcal{O}}^{cm}$, and the shared power between each area, and its neighbor is described in the matrix. The model decomposition should guarantees $\sum_{\mathcal{O}} n_{x_{\mathcal{O}}} = n_x$, $\sum_{\mathcal{O}} n_{u_{\mathcal{O}}} = n_u$, $\sum_{\mathcal{O}} n_{d_{\mathcal{O}}} = n_d$ *and* $\sum_{\mathcal{O}} n_{v_{sh}} = n_v$.

As discussed in the SM layer model, the aggregated system is decomposed into multiple state-space models for each area (CM). In (5.4), the parameters $A_{\mathcal{O}}^{cm}, \Gamma_{\mathcal{O}}^{cm}, E_{v,\mathcal{O}}^{cm}$ and $C_{\mathcal{O}}^{cm}$signify each area. In addition, the parameters $\mathrm{B}_{\mathcal{O}}^{\mathrm{sh}}$ and $\mathrm{E}_{\mathrm{v},\mathcal{O}}^{\mathrm{sh}}$ represent the interconnected tie-lines between one area and its neighbors. In this model, the local controller drives each area by generating its local control inputs $u_{\mathcal{O}}^{cm}$ and the coupled control action $u_{\mathcal{O}}^{sh}$ to track $y_{\mathcal{O}}^{cm}$ and use the guidance of $u_{\mathcal{O}}^{sh}$ from the upper layer (SM). The decomposition process provides an accurate model to take the decision within one area to achieve the proper local

performance and with limited guidance data from the upper layer to accomplish the system global performance.

5.4 DT based HDMPC

The management control actions are performed by a certain number of controllers, which arranged hierarchically in different timeframes. The top management layer (SM) behaves for slow interactions between the overall aggregated energy systems in terms of areas distributed interaction. On the other hand, the bottom layer (CM) consider the faster and aggressive variations due to the variability of the intermittent RES in a single area. Usually, the direct management actions are applied in the forms of set-points for each unit controller in the physical system. On the other hand, the SM uses the DT to calculate the targets (reference signals) for the CMs to satisfy the global optimization objective. Additionally, as the operational plans changes from one case to another, the targets definition and coordination for customized plans is not enough. The objective function should be changed to weaken or strengthen a certain part to change the operation plan according to the grid status. MPC can be manipulated to achieve this feature by adaptively changing the constraints and the weighting factors in real-time to make the objective function flexibly orientated by the operator perspective. In Figure 5.3(a), the overall block diagram of the detailed procedures for the three layers is illustrated. Each manager in the top two layers is designed as a single MPC performs to minimize the cost function and has an individual function. Figure 5.3(b) shows the evaluation of CM set-points guided with SM target.

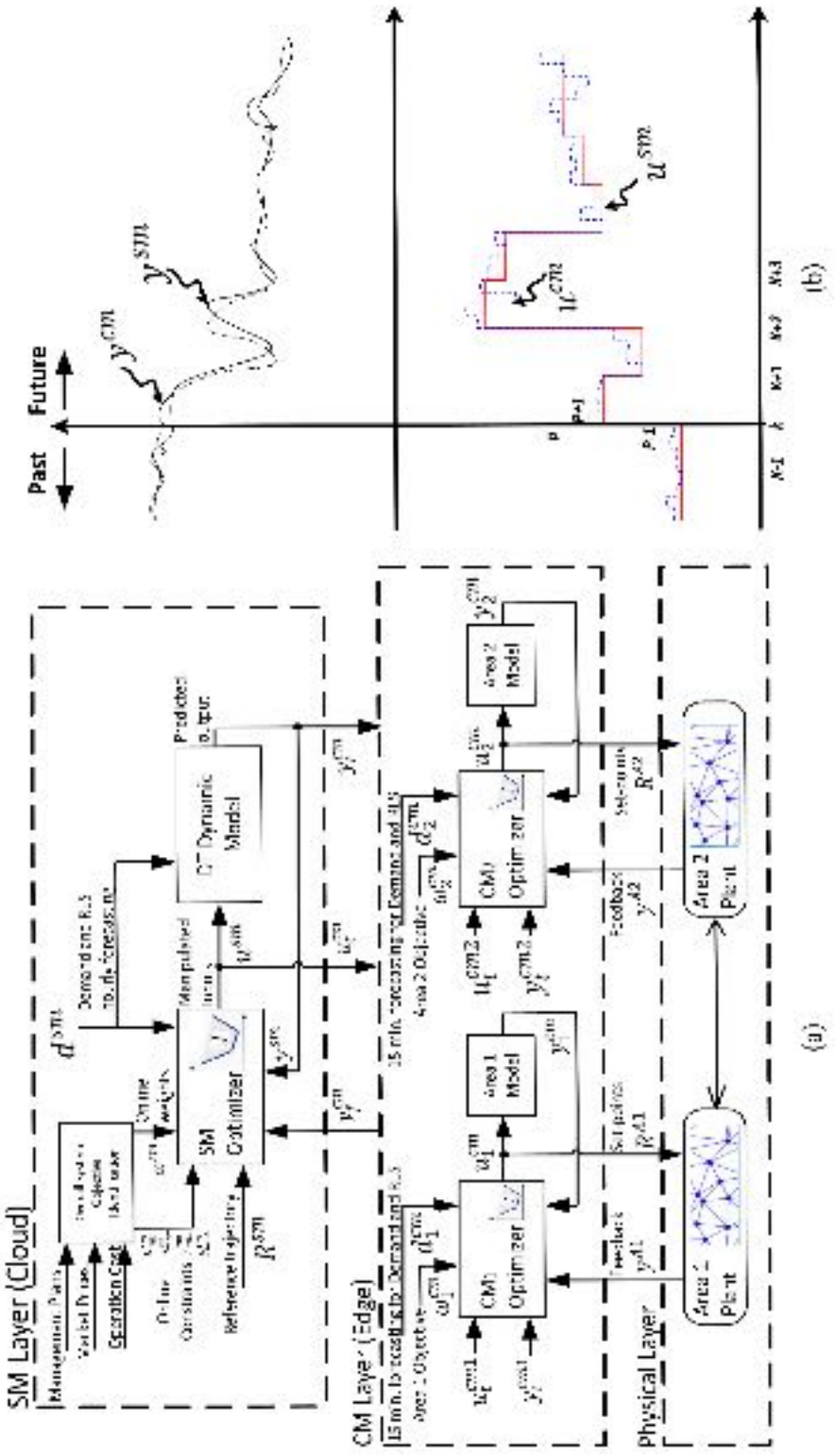


Figure 5.3: The management strategy, (a) Block diagram, (b) SM and CM comparison.

Both SM and CM work together to support the global system objectives to reduce both model and objective function complexity at maximum reliability. In Figure 5.3(a), the data exchange between the upper and the lower layers is denoted by u_t^{cm}, y_t^{cm} and y_f^{cm}. Firstly, SM reads the feedback data y_f^{cm} from CM layer, which is a sub-set from y_O^{cm} to reduce the communication and computational burden. Then, the SM calculates the guidance u^{sm} based on the feedback and the SM layer model. After that, a sub-set of the SM control actions, which is denoted by u_t^{cm} alongside with a sub-set of predicted system outputs are submitted to t, the CM layer as global system targets for the next time-slot. The following section discusses control system objective for SM and CM layers, which are optimized in MPC to generate the proper control inputs and control guidance from CM and SM, respectively.

5.4.1 Supervisory Manager MPC Design

SM is primarily aimed to manage centrally the overall grid to minimize the cost of the long-term operation (hourly) and derive the targets for the manipulated control actions for the next layer (CM). For each time slot k, the quadratic optimizer function minimizes the following function as a central management objective,

$$\min_{\Delta u^{sm}, u^{sm}} J^{sm} = \sum_{z=1}^{ph^{sm}} \left[\sum_{i=1}^{n_y} e^{sm}(k+z|k)^T . Q_{y^{sm}} . e^{sm}(k+z|k) + \sum_{i=1}^{n_u} u^{sm}(k+z|k)^T . R_{u^{sm}} . u^{sm}(k+z|k) + \sum_{i=1}^{n_u} \Delta u^{sm}(k+z|k)^T . R_{\Delta u^{sm}} . \Delta u^{sm}(k+z|k) \right] \quad (5.5)$$

where J^{sm} is subject to system limits and the fixed-mixed constraints (5.1)-(5.4).

The optimization function (5.5) penalizes the error between reference and output values $e^{sm}(k+z|k) = y^{sm}(k+z|k) - R^{sm}(k+z|k)$, the energy cost for each manipulated power and the penalty due to ramping capabilities. The cost function is solved for prediction horizon ph^{sm}. The system weights $\omega^{sm} = \{Q_{y^{sm}}, R_{u^{sm}}, R_{\Delta u^{sm}}\}$ is used to achieve certain operation plans.

5.4.2 Coordination Manager MPC Design

The MPC of CMs has the purpose to provide a stream of set-points R^{A_O} to the physical system controllers to overcome the variability of the intermittent resources, which needs fast response. This layer MPC works in a distributed-cooperative way under the guidance of the SM layer to guarantee the energy management system performance. Similarly, the quadratic CM_O optimizers minimize the following optimization function for each area in the grid,

$$\begin{aligned}\min_{\Delta u_O^{cm}, u_O^{cm}} J_O^{cm} = \sum_{z=1}^{ph^{cm_O}} \Bigg[& \sum_{i=1}^{n_{y_O}} e_O^{cm}(p+z|p)^T . Q_{y_O^{cm}} . e_O^{cm}(p+z|p) \\ & + \sum_{i=1}^{n_{u_O}} u_O^{cm}(p+z|p)^T . R_{u_O^{cm}} . u_O^{cm}(p+z|p) \\ & + \sum_{i=1}^{n_{u_O}} \Delta u_O^{cm}(p+z|p)^T . R_{\Delta u_O^{cm}} . \Delta u_O^{cm}(p+z|p) \\ & + \sum_{i=1}^{n_{u_t}} \delta u_{t,O}^{cm}(p+z|p)^T . F_{\delta u_{t,O}^{cm}} . \delta u_{t,O}^{cm}(p+z|p) \Bigg]\end{aligned} \tag{5.6}$$

where $e_O^{cm}(p+z|p) = y_O^{cm}(p+z|p) - y_{t,O}^{cm}(p+z|p)$, and the error between trajectory targets of inputs and the actual set-points is expressed as $\delta u_{t,O}^{cm}(p+z|p) = u_O^{cm}(p+z|p) - u_{t,O}^{cm}(p+z|p)$. The energy production costs and market prices for the

energy units are re-estimated to represent the coordination manager layer time-frame, $\omega_{\mathcal{O}}^{cm} = \{Q_{y_{\mathcal{O}}^{cm}}, R_{u_{\mathcal{O}}^{cm}}, R_{\Delta u_{\mathcal{O}}^{cm}}, F_{\delta u_{t,\mathcal{O}}^{cm}}\}$.

5.5 Data Centric Based CPS Implementation

In large-scale smart grids, the real-time collected data is massive, and has dynamic and stochastic data locations. The data management has many complex challenges for monitoring and smart grid application utilization. The data-centric method based on Data DDS is used as a middleware to increase the robustness and the scalability of the data exchange system between the developed hierarchically distributed managers by utilizing distributed peer-to-peer communication. Since the data model in the data-centric approach is driven directly from the system data model without needs for defining preset of message structure, the DDS enhance the integration RES control agents. The DDS middleware plays a crucial role in the developed system, because a large amount of exchanged data and information between the layers managers should be of high flexibility, interoperability and availability. The DDS is driven from the system data model, which allows mapping standard data models, like IEC 61850, into DDS.

Figure 5.4 shows DDS implantation for the developed hierarchical management system. Data topics are classified into multiple domains. SM domain works between SM and CM layers and controlled via domain controller with Quality of Service (QoS) polices. SM gets the system initial conditions from CMs and publishes the manipulated inputs after solving the SM objective function to be the targets of CM layer. Then, each CM subscribes for the required information to calculate the local controller's set-points after solving the local area objective function. The CMs set points are published in multiple domains $CM_{\mathcal{O}}$ to be

utilized at the end for physical system controller's assignments. After that, a set of gateways subscribe to get set-points stream and assign it to Energy Unit Controllers (EUCs). Finally, the measured feedback is published to the upper layer's domains.

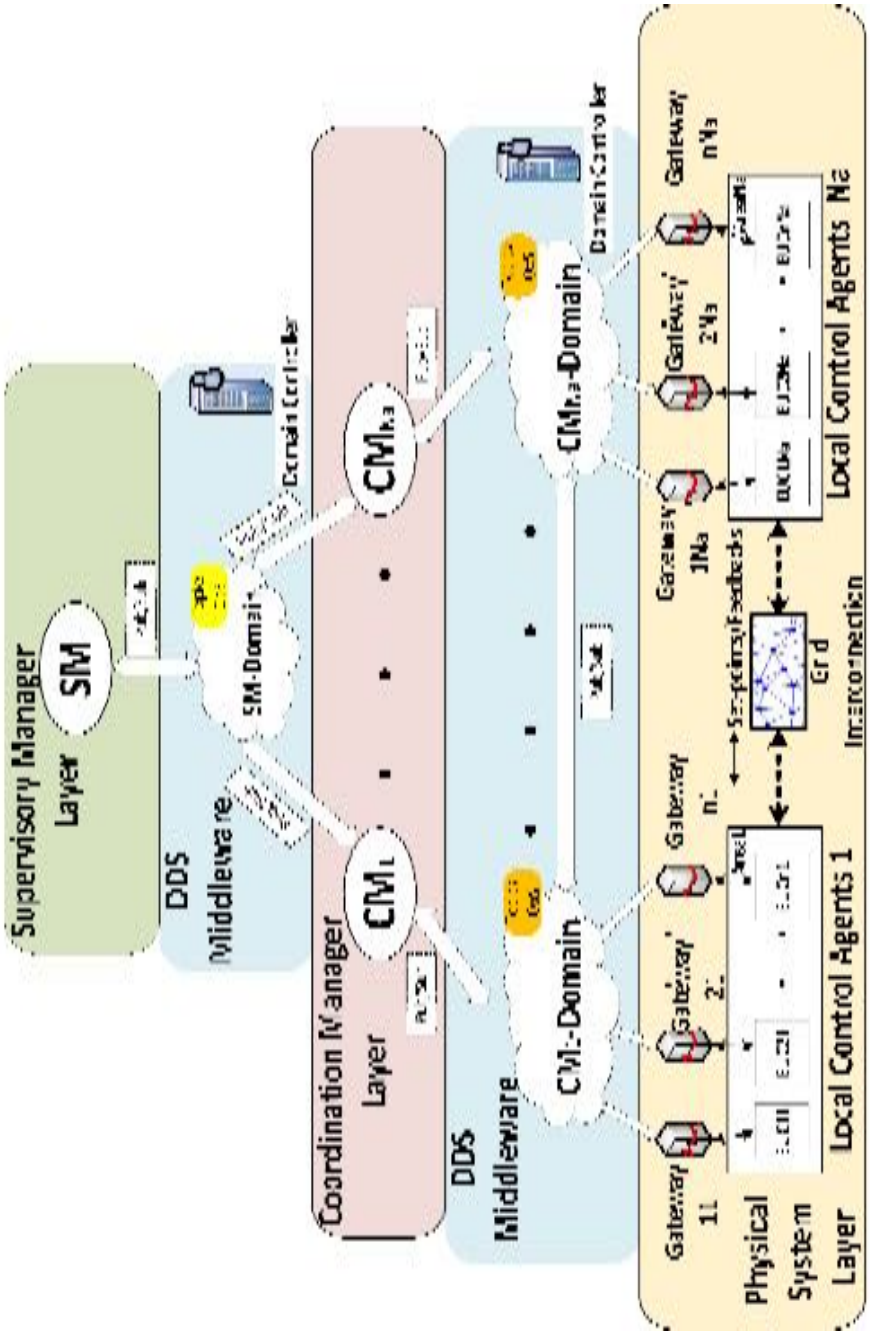


Figure 5.4: DDS infrastructure implantation.

According to the developed DDS infrastructure, the developed management system can work as a distributed control system, if the central manager (SM) fails under any circumstances and thanks to QoS rules that give domain controllers the ability to transfer the mode from hierarchical distributed management into distributed management.

5.6 Results and Discussion

To validate the performance of the developed management strategy, the modified IEEE 39-bus, which is depicted in Figure 5.5, has been utilized as a large-scale system under study. The case study contains four interconnected areas. A variety of energy unit types with different power ratings is used to emulate the real power system. The system under study is simulated using MATLAB/SIMULINK. The SM and the four areas CMs are designed and implemented on separate machines (computers) to represent the real-time simulation environment and the connection between those machines is implemented using the DDS toolbox in MATLAB/SIMULINK. The conventional energy generations such as Nuclear, Old Coal, New Coal, Combined Cycle Gas Turbine (CCGT) and fast Gas Turbine (GT) are distributed in the four areas with a total capacity of 3705 MW (61%) as shown in the figure. On the other hand, two types of renewable energy (wind and solar) have a total share of 2372 MW (39%). In addition, Pumped Hydro Storage (PHS), Thermal Energy Storage (TES) and Battery Storage System (BSS) are installed in different area with different power ratings with the aggregation of 785 MW. As illustrated in Figure 5.5, the four areas are interconnected by 6 tie lines that are indicated in solid blue lines. In this simulation, the geographical climatological data is taken from four different areas in Texas to emulate proper variance in the wind and solar forecast [91].

SM solves the optimization problem and generates the target signals of the manipulated variables for CM layer. It is assumed that the load and RES forecasting of both the SM and CM time visions is 60min. and 15min., respectively. The reason behind this time-horizon assumption is based on the RES forecast variability and uncertainty. The large balancing areas forecasting error is lower than the smaller areas.

The simulation time window is 60 hours with hourly sampling for the SM layer and a quarter-hour sampling for the CM layer. The energy units and power lines are constrained to their limits. The IEEE 39-buses connectivity is modelled using the previously discussed modelling.

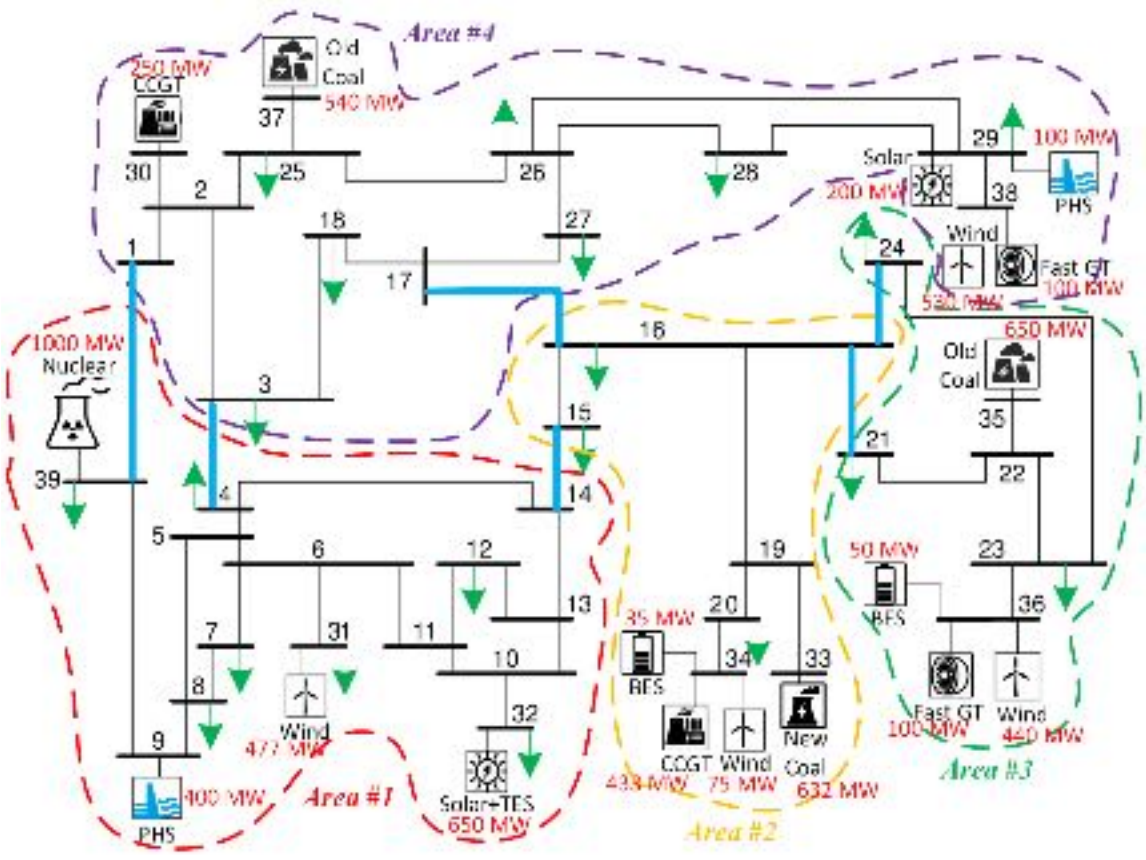


Figure 5.5: Modified IEEE 39-bus under study.

Figure 5.6 and Table 5.1 show the results of this case study. The figure displays the comparison between the performance of the three approaches (centralized, hierarchically distributed and distributed) in the four areas of the grid. The comparisons are in terms of the area's aggregated demand, load shedding, renewable share, renewable curtailment, conventional outages and SOC of the energy storage are shown in Figure 5.6(a) to Figure 5.6(f), respectively.

As discussed before, the centralized approach has the best performance but lacks reliability and robustness due to the centralized decision. The distributed MPC and HDMPC are compared with the centralized MPC with respect to performance. In Figure 5.6(a), the aggregated load of the developed method shows a very close dispatched load to the centralized in the four areas, while the distributed has power shortage, especially in the first area.

More details are shown in Figure 5.6(b), where the load shedding amount registered lower occurrence frequency in case of the HDMPC than in distributed approach especially in areas 1 and 4. This shows the ability of the HDMPC in giving good comparable results as the centralized controller without being less reliable as the centralized one.

In terms of achieving the optimal usage of renewable resources, Figure 5.6(c) and Figure 5.6(d) show the renewable share and renewable curtailment, respectively. It is clear that the total renewable curtailment is reduced for the developed strategy when it is compared with the distributed approach. The previous results show that the developed technique is not only increasing the system security by reducing the load shedding but also wisely and efficiently uses renewables.

As it can be seen in Figure 5.6(e), the conventional high-cost power is significantly reduced in the HDMPC method than compared to the distributed method. The developed method was successfully able to deal with the high variability of renewable power although the limited ramping capability of the conventional generation. The developed management system utilizes the predicted solution of the SM layer to calculate the future set points of the ESSs and the flexible resources as fast GT to overcome the variability during the narrower time slot, which attains the global optimization.

The usage of the EES is illustrated in terms of the *SOC* comparison between the three approaches in Figure 5.6(f). In area 1 and 4, the distributed and HDMPC has the same behaviour because the aggregated demand in those areas is relatively high and they should use their stored energy.

However, the unique advantage of the developed method appears, due to the only local vision of the distributed approach, appears when the ESS in area 2 and 3 store energy although the other two linked areas need power. In contrast, the SM succeeded to guide the CMs in these areas to intelligently charge/discharge the ESSs, so it can support the overall system security.

For more validation, the developed technique is compared with centralized and distributed approaches in terms of cost, load shedding and RES spilled energy as shown in Table 5.1. Figure 5.7 shows the area-to-area power transactions through the tie lines. The figure shows that the HDMPC exactly tracked the power transactions as in centralized, which achieves higher performance. In contrast, In the distributed case the tie lines power cannot track the optimal transactions.

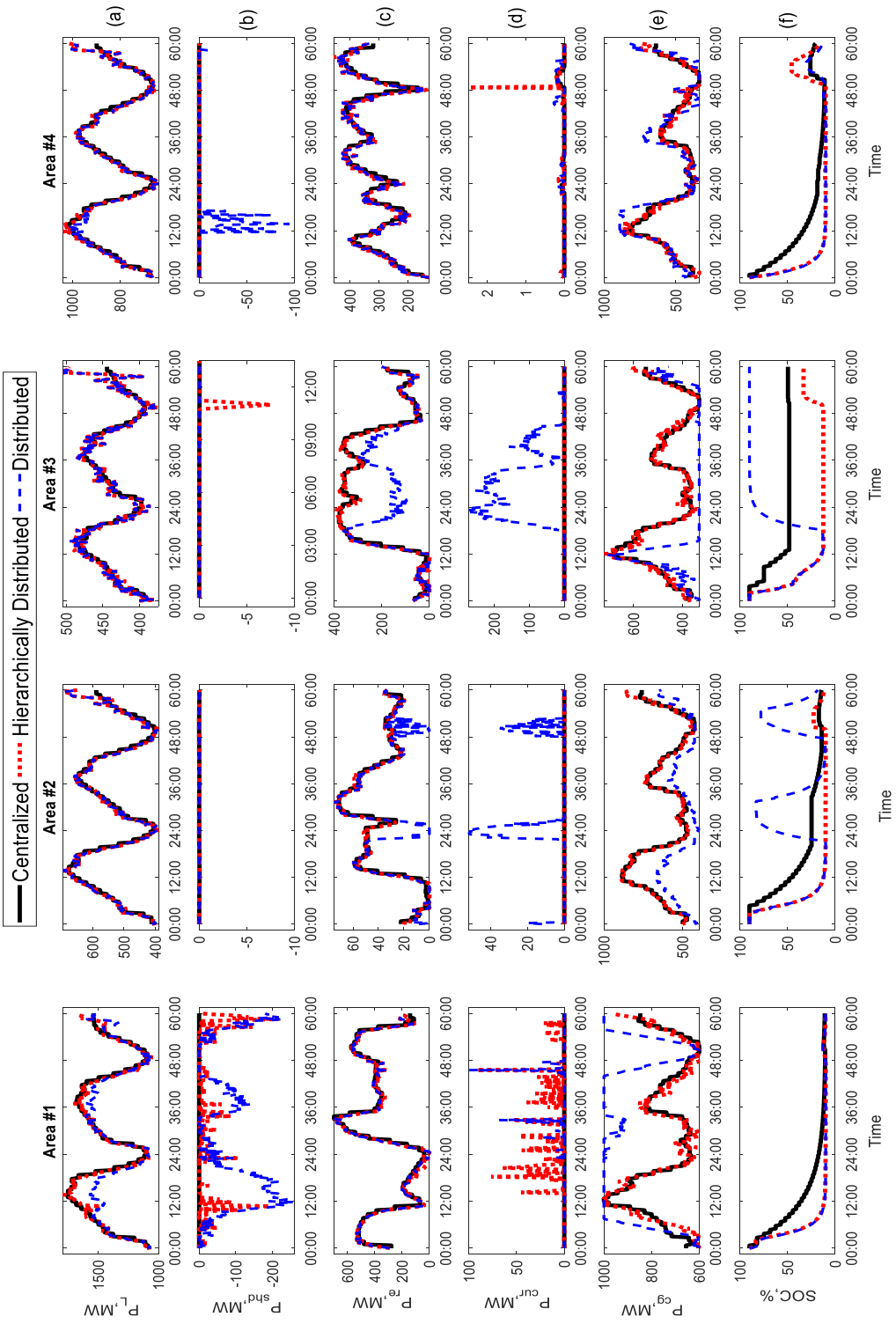


Figure 5.6: Performance comparison between centralized, hierarchically distributed approaches. (a) demand, (b) load shedding, (c) renewable share, (d) renewable curtailment, (e) conventional outages, (f) ESS state-of-charge.

Table 5.1: Comparison between centralized MPC, HDMPC and Distributed MPC Approaches.

Area	Class	Unit Type	Unit price, $/GWh	Centralized MPC		HDMPC		Distributed MPC	
				Energy, GWh	Cost, k$	Energy, GWh	Cost, k$	Energy, GWh	Cost, k$
1	Conv.	Nuclear	60	44.64	668.6	44.52	667.8	55.02	825.3
	RES	Wind	25.5	10.55	67.26	10.21	65.09	10.42	66.45
		Solar	17.5	10.65	47.12	10.59	46.86	10.63	47.04
	ESS	PHS	8.1	0.888	18	0.996	19	0.968	1.96
		TES	20	0.135	0.675	0.139	0.695	0.146	0.73
	Penalty	Shedding	1000	0	0	0.84	840	4.66	4660
		Curtailment	100	0	0	0.351	35.1	0.09	9
2	Conv.	New Coal	60	27.25	408.7	27.4	411	22.84	342.6
		CCGT	100	9.57	239.2	9.64	241	7.91	197.7
	RES	Wind	25.5	2.155	13.74	2.15	13.7	1.9	12.11
	ESS	BES	50	0.037	0.462	0.047	0.588	0.17	2.13
	Penalty	Shedding	1000	0	0	0	0	0	0
		Curtailment	100	0	0	0	0	0.252	25.2
3	Conv.	Old Coal	75	25	468.7	25.14	471.3	21.45	402.2
		Fast GT	120	2.41	72.3	2.464	73.9	1.63	50.9
	RES	Wind	25.5	12.17	77.58	12.13	77.33	8.2	52.28
	ESS	BES	50	0.034	0.425	0.06	1	0.132	1.65
	Penalty	Shedding	1000	0	0	0.003	3	0	0
		Curtailment	100	0	0	0	0	3.93	393
4	Conv.	Old Coal	75	21.41	401.4	21.48	402.7	22.24	417
		CCGT	100	6.53	170.7	6.56	171.5	7.45	196.2
		Fast GT	120	2.41	72.3	2.42	72.6	2.56	79.8
	RES	Wind	25.5	16.3	103.9	1.55	10.51	1.64	10.45
		Solar	17.5	3.54	15.66	3.51	15.53	3.5	15.49
	ESS	PHS	8.1	0.214	0.433	0.328	0.664	0.263	0.533
	Penalty	Shedding	1000	0	0	0	0	0.175	175
		Curtailment	100	0	0	0	0	0	0
Total Cost				-	2532	-	3624	-	2355

By referring to the best performance in centralized, the developed hierarchically distributed is better than distributed approach. The energy unit cost, curtailment energy and load-shedding penalties are depicted in Table 5.1. The summarized results show the energy utilization for 60 hours and the Cost for each energy unit type in the four areas. The centralized method has zero sheddings and curtailment power, so it has the minimum cost.

Due to a large amount of load shedding and renewable curtailment in the distributed method, it has a higher penalty cost and total cost. In contrast, the HDMPC has a slight increase in the spilled and not served loading so it has a lower total cost than the distributed MPC approach.

Furthermore, an extra validation is demonstrated by comparing the performance between centralized, Distributed and HDMPC approaches under different forecasting error in RES profiles as shown in Table 5.2. It is clear that the effect of forecasting error (uncertainty) degrades the performance for the three approaches. The centralized approach sees the least impact and the HDMPC is very close to the centralized method. As seen, the HDMPC approach has better performance than distributed one even with large error as high as 30%.

Table 5.2: Performance Under Different Forecasting Errors

Energy, GWh	Centralized MPC		HDMPC		Distributed MPC	
	Error, 10%	Error, 30%	Error, 10%	Error, 30%	Error, 10%	Error, 30%
Total	193.79	191.23	179.66	177.13	173.48	169.39
Shedding	0.65	3.274	1.02	4.2	6.27	13.33
Curtailment	0.45	0.62	0.46	0.96	5.69	10.59

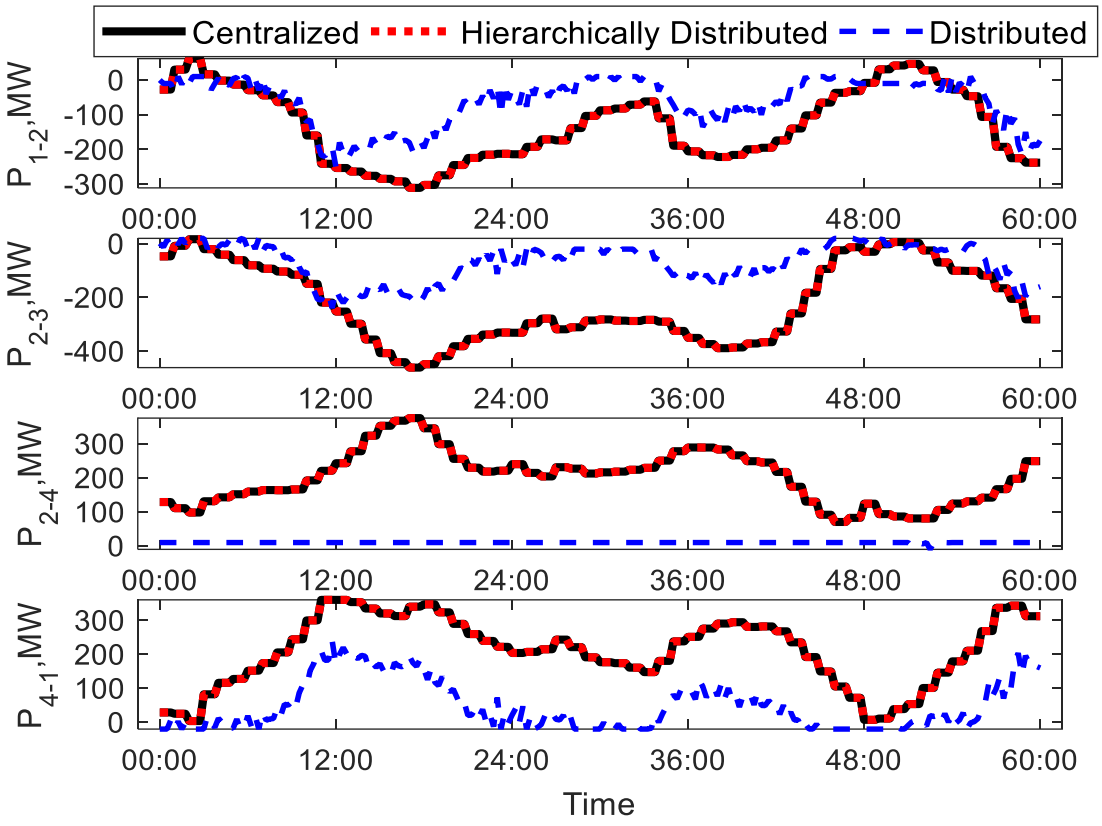


Figure 5.7: Area-to-area power transaction comparison.

The developed methodology performance depends on the prediction horizon assumption. The prediction horizon samples should be wisely selected according to the mean value of the expected forecasting error of RES and it mainly depends on the RES type, location and weather conditions. Although the slight impact on the prediction horizon selection, the ph should cover the tradeoff between the maximization of the profit (maximize RES utilization) or maximizing security (load shedding).

In Table 5.3, the IEEE 39-bus is tested under different prediction horizons. According to the results, the best performance is achieved for a prediction horizon, $ph = 10$. As shown, when $ph = 1$ and 5 are chosen, the load shedding and renewable curtailment

energy are higher than in the case of selecting $ph = 20$, the renewable curtailment performance is improved but the load shedding (security) is violated. Therefore, the previous results in Table 5.1 are achieved when $ph = 10$.

Table 5.3: Performance Under Different MPC Prediction Horizons

Energy, GWh	$ph = 1$	$ph = 5$	$ph = 10$	$ph = 20$
Total	178.19	179.57	180.164	180.05
Shedding	2.817	1.437	0.843	0.957
Curtailment	0.63	0.46	0.351	0.322

5.7 Experiential Validation

The developed energy management system prototype is implemented based on the laboratory-based smart grid Testbed by reconfiguring the generation and storage units to represent the large-scale power system grid characteristics. The testbed system has integration with many smart grid protocols and DDS middleware is implemented and adopted to interact with those protocols.

The network is studied for experimental validation. Four Motor-Generator units are characterized to simulate the Coal, Gas, Nuclear and CCGT characteristics as ramping capability and operational power limits. The demand pattern is set to 4.2 KW soft-variable loads. Moreover, a 72 KW bidirectional inverter is used to simulate the RES and ESS combination to simplify the experimental implementation. As shown in Figure 5.8, a two-area interconnected power system is modelled using state-space representation for both SM (aggregated) and CM (decomposed) layers. A scaled-down experimental evaluation is used to validate the developed solution.

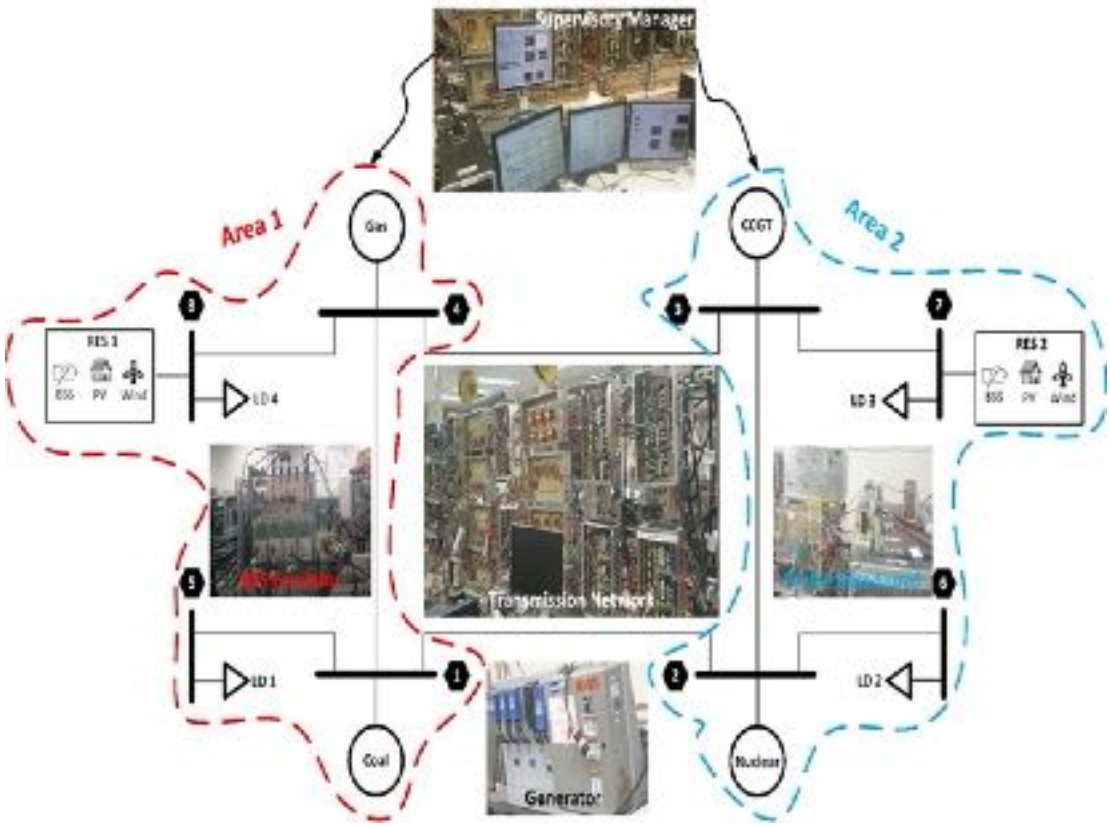


Figure 5.8: Verification of the developed technique on the Testbed.

The physical system controllers succeeded to achieve CM set-points ($P_{1,CM}, P_{2,CM}$) as shown in Figure 5.9. $P_{1,a}$ and $P_{2,a}$ are the two areas conventional aggregated power. The CM output power, $P_{re+ess,CM}$, which represents the RES and ESS total output is compared to actual inverter measurements, $P_{re+ess,a}$. Finally, the load CM trajectory guidance set points, $P_{L,CM}$ is tracked by the actual measured load, $P_{L,a}$.

Traditionally, the legacy message-centric architecture, such as the Open Platform Communication (OPC) server, is used as a communication middleware in systems like SCADA to exchange data. This kind of middleware suffers from inefficiency, low scalability, high latency and high cost of the message broker implementation. The modern

complex smart grid, which has big data, sensors and communication, will need high performance and long-term scalable growing middleware. Therefore, the data-centric method will provide the mission-critical interoperability requirements for the smart power grid. In order to prove the critical feature of the data-centricity, Figure 5.10 shows an experimental comparison between the performances of the developed HDMPC in case of without data-centric (using OPC) and with data-centric (using DDS).

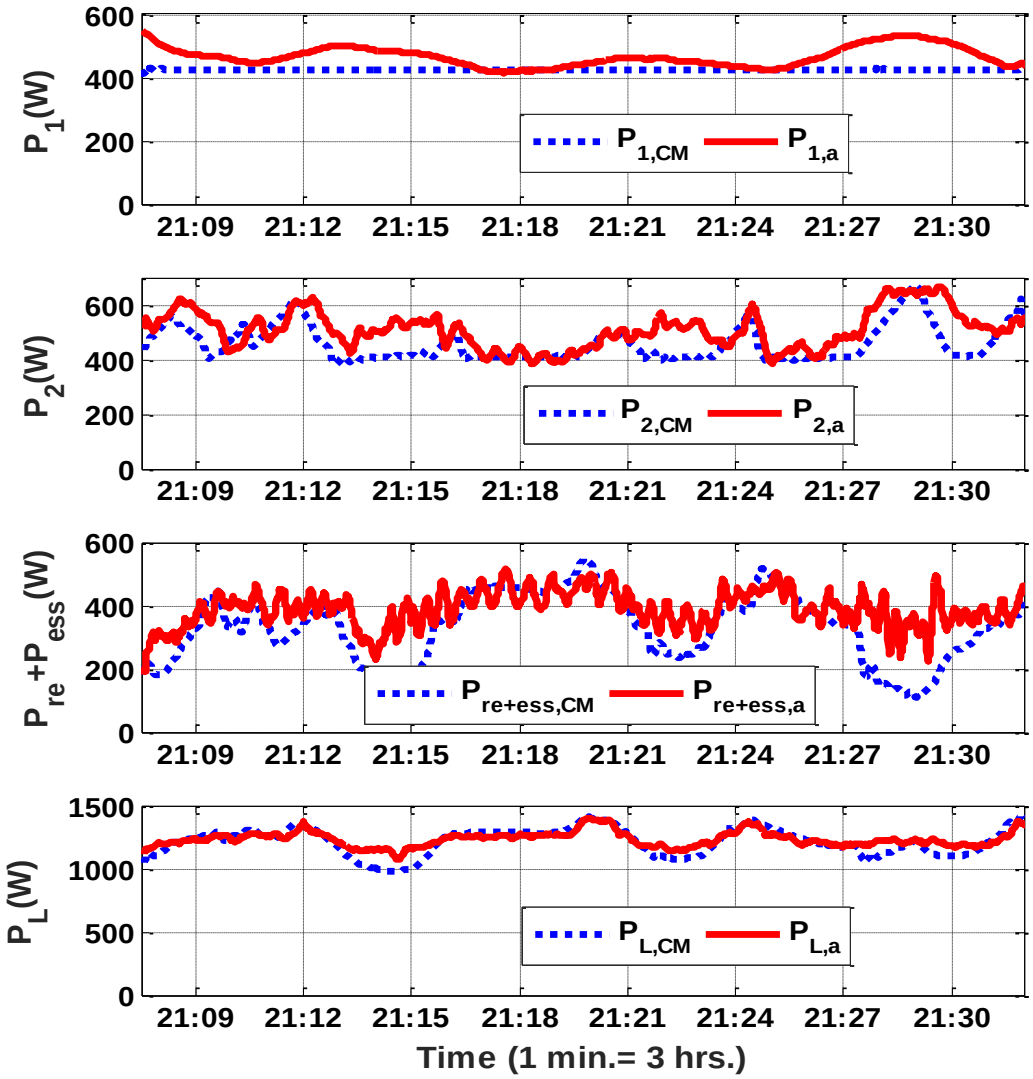


Figure 5.9: Experimental Results.

In Figure 5.10(a), the load shedding behaviour is better with DDS as compared to the message-centric OPC (without data-centric). The communication middleware without data-centric suffers from high latency and misalignment of data availability, which cause belated decisions. In addition, Figure 5.10(b) depicts the high share of RES in the case of data centric as compared to the behaviour of the OPC case. Table 5.4 shows the accumulative energy and cost comparison for the studied time window. The total load shedding energy and the total RES curtailed energy is greater in the case without data-centricity than the case of with data-centricity, which increase the penalty cost.

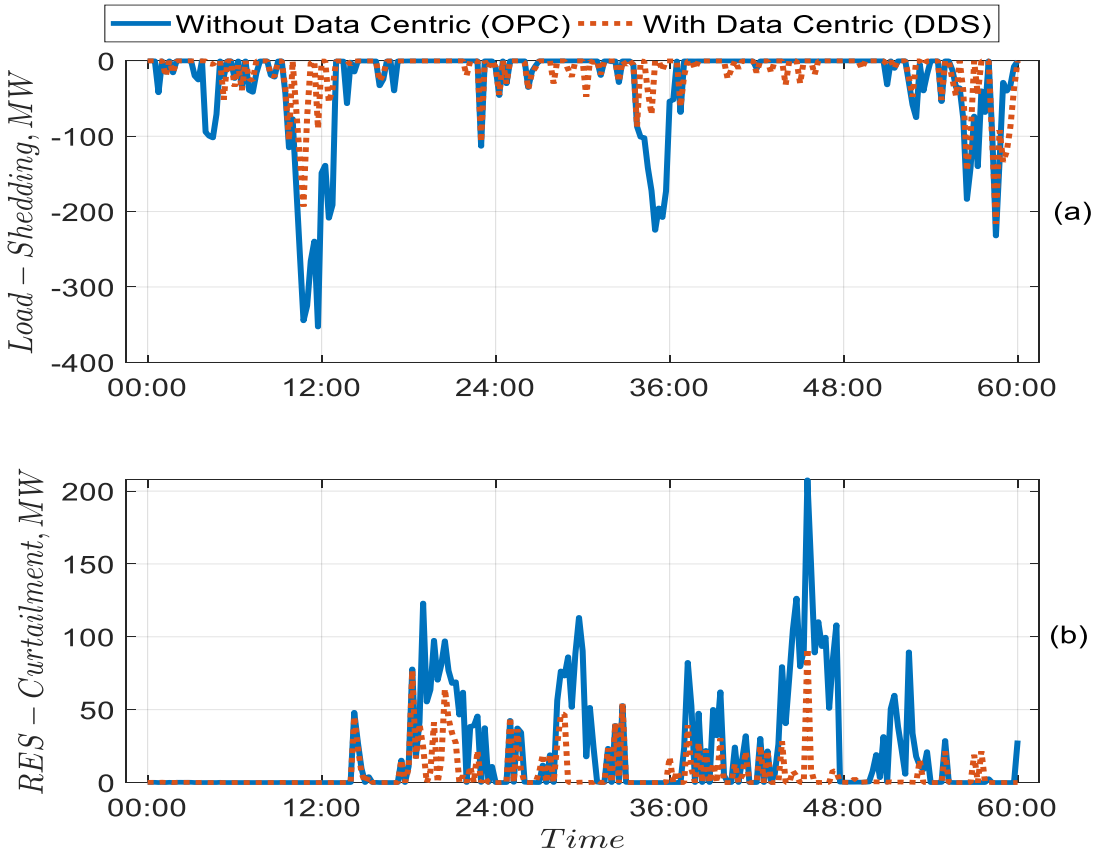


Figure 5.10: An experimental performance comparison of the HDMPC without data-centric and with data-centric communication middleware. (a) Load shedding behavior. (b) RES curtailment behavior.

Table 5.4: Performance Comparison Between Without and With Data-Centric

Middleware	Load Shedding Energy, GWh	RES Curtailed Energy, GWh	Penalty Cost, *k$*
Without Data-Centric (OPC)	1.84	1.234	1963.4
With Data-Centric (DDS)	0.846	0.357	881.7

5.8 Summary

The chapter presented the design and implementation of an HDMPC-based energy management strategy for smart grids. The developed methodology combines the benefits of both centralized and distributed control approaches to solve and decompose the complex management objective function of the large-scale power system. Applying the HDMPC technique successfully achieved good performance of system management to integrate a high share of RES and it solved the variability issue with maximum security at minimum cost. The DDS middleware-based data-centric was presented to ease the hierarchical control communication focusing only on the control/optimization objective rather than the communication problems. It has been clearly illustrated that the developed management technique can manage the grid with higher performance than the distributed approach and with high reliability and scalability when compared with the centralized approach. Verifications were successfully conducted in a laboratory scale smart grid testbed.

Chapter 6 Intelligent Adaptive Energy Management

In this chapter, the digital twin and the optimizer are adapted autonomously in real-time according to the power system state to make the management decisions became smarter. The variability and uncertainty of renewable energy increase the difficulty of power system management extremely. Also, the problem becomes more challenging if the variable energy has a large penetration. The developed strategy depends on robust optimization under unforeseen contingencies and uncertain changes in intermittent resources output. Adaptive digital twin based predictive control is used to manipulate the power system energy unit's set-points to maximize profit at maximum security. Simulation studies are conducted to validate the effectiveness of the introduced strategy. The results show that the developed strategy is successfully able to maximize profit not only in normal operation case but also in the case of severe contingencies. In addition, the management strategy is flexible for customized plans of the grid operator and it is scalable for system extensions. The developed strategy helps the management system to increase the free renewable energy sources share at the minimum cost with maximum security.

6.1 Introduction

The new smart grids infrastructure must be designed to cope with variable, unforeseen and uncertain characteristics of the renewable energy at an acceptable degree of reliability and security [92]. The classical energy management system address only real-time conditions without extra consideration of the full holistic vision of the dispatching problem. Besides, the ability of the classical management system is very difficult to keep the power reserve track the fluctuations with the full care of the constraints without violation. In

addition, the current dispatching approach needs the high computational capability to proceed in a central management system [67], [92], [93]. With the advent of market sharing, the dispatching problem becomes more difficult when the management system has an aim of the operating system with maximum profits [67].

In the literature, the researchers interested in assessing the management system via active load management as in [94]. Real-time consumption scheduling is introduced in [95]. The stochastic MPC used in [96] to dispatch generation and storage. Great valuable research in [96], [97] uses the smart grid technology to solve the cost problem in the case of large random wind power. Other authors consider the micro-grid management as in [98], [99]. All previous literature considers only the dispatching problem without introducing an adaptive solution for the management problem that can adapt the management problem with the system state. It does not only need to be an adaptive problem and constraints but also it needs to change the system model and objective philosophy. System robustness has a vital role in maintaining system security besides the profit objective function. The developed technique mainly depends on the MPC [100]–[102]. It is an autonomous intelligent optimal control technique rely on the system DT model that is implemented on the cloud.

MPC use the DT model that is driven by the real-time shadow updates and the forecasted disturbance to generate the set-points of generation units, Energy Storage Systems ESS, demand, and shedding or spilled energy. The major advance in the Predictive Energy Management System (PEMS) is its ability to not only maximize profits or minimize the cost but also to enhance the system security under contingencies or unforeseen changes in

the power system. Therefore, the developed is strong and can deal with the large variability and uncertainty of the vRES if the system contains large vRES penetration. PEMS can utilize the system resources to use it in many customized automatic operation plans upon the grid operator requirements. Based on the Analytical Hierarchy Process (AHP) technique, the DT model and the optimization problem are modified by defining the management priority [103]. The developed scheme has the ability to expand to add extra energy. In addition, MPC is simple to build, the optimization function has the low computational burden, and thanks to a simplified power balancing DT, which ease the large-scale system implementation.

6.2 Adaptive Model Predictive Control

The DT constructor is used in real-time to build the DT model. The model parameters, the DT inputs and the estimated outputs are configured based on real-time situational awareness. The forecasting of the wind or solar output is difficult and the grid operation with RES large penetration is the most significant challenge. The dispatching problem should be solved in a predictive way to overcome unexpected ramp-rates. MPC is a promising technique to make predictive control in real-time. The main idea of the MPC is to solve the control problem in optimization and the solution is in a prediction horizon at each time sample. MPC is a robust and dynamically behaved framework, which can deal with the rapid and unpredictable changes in large-scale vRES. The optimizer should be designed to maximize profits by minimizing vRES curtailment and at the same time minimizing load shedding. Besides, the optimizer reduces the dependability on fossil fuel conventional generations with reasonable usage of the storage system.

The optimization problem was implemented to be adapted according to the required objectives. For instance, during a contingency, the objective is to maximize the served load rather than maximizing renewable utilization. The management problem is a multi-objective problem so the weighting factor of the optimization problem can be adapted to respond to the system online status. The general mathematical formulation for the prediction control problem is divided into three objective functions. The first one is minimizing the difference between the reference storage state of charge and its predicted value with the notation J_{soc}. The second one is the cost function J_P of the manipulated power with different types itself and the target developed value. Finally, the objective function $J_{\Delta P}$ of maintaining the manipulated power rate of change limited by weighting factors. The Adaptive optimization function is defined as follows,

$$J_{soc} = \sum_{b=1}^{n_{soc}} \sum_{a=1}^{p} \left\{ \mathcal{L}_b^{soc} . \omega_{a,b}^{soc} [soc_b^*(c+a|c) - soc_b(c+a|c)] \right\}^2 \tag{6.1}$$

$$J_P = \sum_{b=1}^{n_P} \sum_{a=0}^{p-1} \left\{ \mathcal{L}_b^{P} . \omega_{a,b}^{P} [P_b(c+a|c) - P_b^*(c+a|c)] \right\}^2 \tag{6.2}$$

$$J_{\Delta P} = \sum_{b=1}^{n_P} \sum_{a=0}^{p-1} \left\{ \mathcal{L}_b^{\Delta P} . \omega_{a,b}^{\Delta P} [P_b(c+a|c) - P_b(c+a-1|c)] \right\}^2 \tag{6.3}$$

$$\text{Minimize} \qquad J(c) = J_{soc}(c) + J_P(c) + J_{\Delta P}(c) \tag{6.4}$$

$$\begin{aligned} s.t. \qquad & SOC_{min} \leq SOC(c) \leq SOC_{max} \\ & P_{min} \leq P(c) \leq P_{max} \\ & \Delta P_{min} \leq \Delta P(c) \leq \Delta P_{max} \\ & P_{disch}(c) . P_{ch}(c) = 0 \end{aligned} \tag{6.5}$$

where the parameters and variables are current control interval c, prediction horizon p, number of ESS units manipulated output n_{soc}, number of manipulated power set-points n_P, scaling factor for bth manipulated ESS outputs $\mathcal{L}_b^{soc}$, Scaling factor for bth manipulated power set-points $\mathcal{L}_b^P$, scaling factor for bth manipulating ramp-rate $\mathcal{L}_b^{\Delta P}$, tuning weights/costs for bth manipulated outputs $\omega_{a,b}^{soc}$, tuning weights/costs for bth manipulated power set-points $\omega_{a,b}^P$, tuning weights/costs for bth manipulated variables ramp-rates $\omega_{a,b}^{\Delta P}$, reference ESS state of charge outputs for b^{th} units SOC_b^*, predicted ESS state of charge outputs for bth units SOC_b, developed power set-points for bth units P_b, and targeted power set-points for bth units P_b^*.

The system constraints play an important role to define the main rules of management strategy. These constraints limits could be changed in real-time according to the power system state and emergencies. The model that represented in the state-space model is defined as constraints for the system. In addition to, the limitation of manipulated variables set-points, ESSs state of charge, the ramp-rate capability of power units and the main rule of when ESS charge or discharge.

6.3 Intelligent Adaptive Energy Management Strategy

In conventional energy management systems, the schedule of the generation units submitted by the grid operator based on the scheduled maintenance and the holistic view of the system based on the load forecasting data. In other words, the EMS should make the RES submit the operation schedule upon the value of load minus RES value, the system schedule should be close to real-time power scheduling and dispatching. In this chapter, we developed a management strategy based on the submitted predictive profile of load

minus vRES. PEMS commands the system by generations, storages, loads, curtailed vRES and load shedding amounts set-points to satisfy the constraints at minimum cost with maximum security.

PEMS main idea is shown in Figure 6.1. Firstly, the model, initial constraints and initial weights/costs were established in the MPC optimizer. The predicted load profile, wind power profiles, and solar irradiance profiles are assigned as a disturbance d to the optimizer and the state-space model.

MPC starts to read the reference objective value of the state of charges r, and then it works to solve the optimization problem J and calculate the manipulated power set-points P to satisfy reference and constraints with the initial weights'. At each sample of the predicted disturbance, MPC schedule and dispatch the future set-points to follow changes in vRES. The actual load flow is calculated according to each set-points which fed on MPC. On the other hand, the actual infeed da, contingencies, and events are simulated as a validation of the robustness of the PEMS. Disturbances like generation unit trip, scheduled maintenance or line trip contingencies are simulated as worst cases might occur during the operation of large-scale vRES.

Figure 6.2 illustrates how adaptive MPC work. The real-time MPC adapter is used to modify the state-space model, new constraints, and new weights. After that, MPC solves the optimization objective function according to the new parameters and by taking into consideration the future predicted vRES and load profiles. Finally, MPC sends new modified setpoints to the actual model. This kind of adaptive PEMS help the management strategy to be robust, dependable and securely operate the power system even in the case

of large-scale vRES presence. PEMS is designed to give the ability of the operator to put any management plans.

The management process was modified according to reading the actual model measurements after the first prediction horizon at sample $a + c$. The adaptation of actual system based on disturbances alongside the customized plans or requirements of the grid operator is used to edit the model, constraints, and weights. If there is any unscheduled disturbance, upon the type and amount of the disturbance, the constraints are corrected to meet the new system state. Then, the scaling weight factors are modified to make system security is the first priority and only reasonable care for maximizing profit. Finally, if any customized plans are required, the constraints, weights, and model are modified to meet new requirements with maximum possible revenues at maximum reasonable security.

The system status analyzer estimates the system by supervising the manipulated output error, forecasting error and storage system performance and provides the real-time MPC adaptation algorithm to support the controller with the proper control performance. The real-time adaptation algorithm is built based on Analytical Hierarchically Process.

AHP is an organized method for shaping and analyzing complex decisions, based on mathematics. There are many applications of AHP as ranking, choosing, prioritization, resources allocation and management. AHP is utilized to solve the multi-criterion problem to priorities the weighting effect of the MPC scaling factors of the manipulated variables and its ramping rate to achieve certain criteria according to the system status and the operator plans. As shown in Figure 6.3, the AHP organization is formed to adapt the MPC controller.

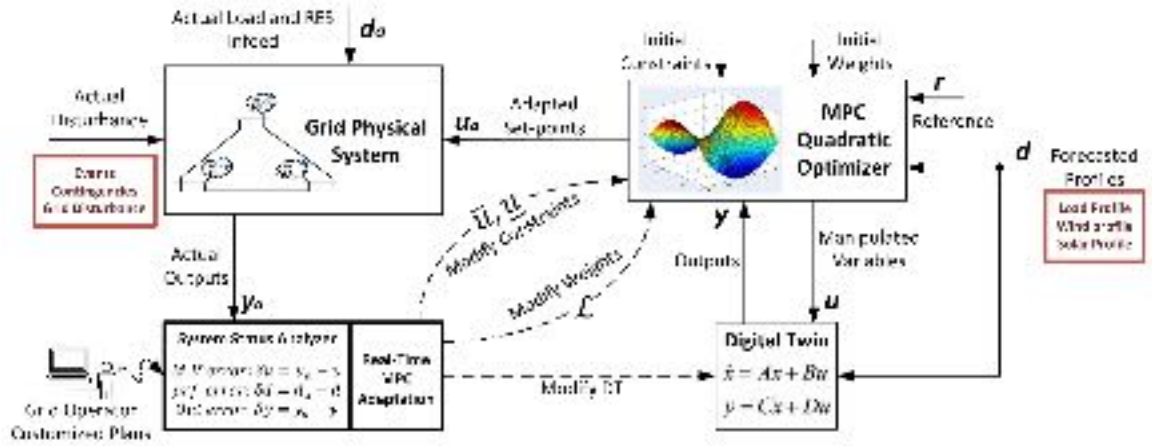


Figure 6.1: Predictive Energy Management Strategy.

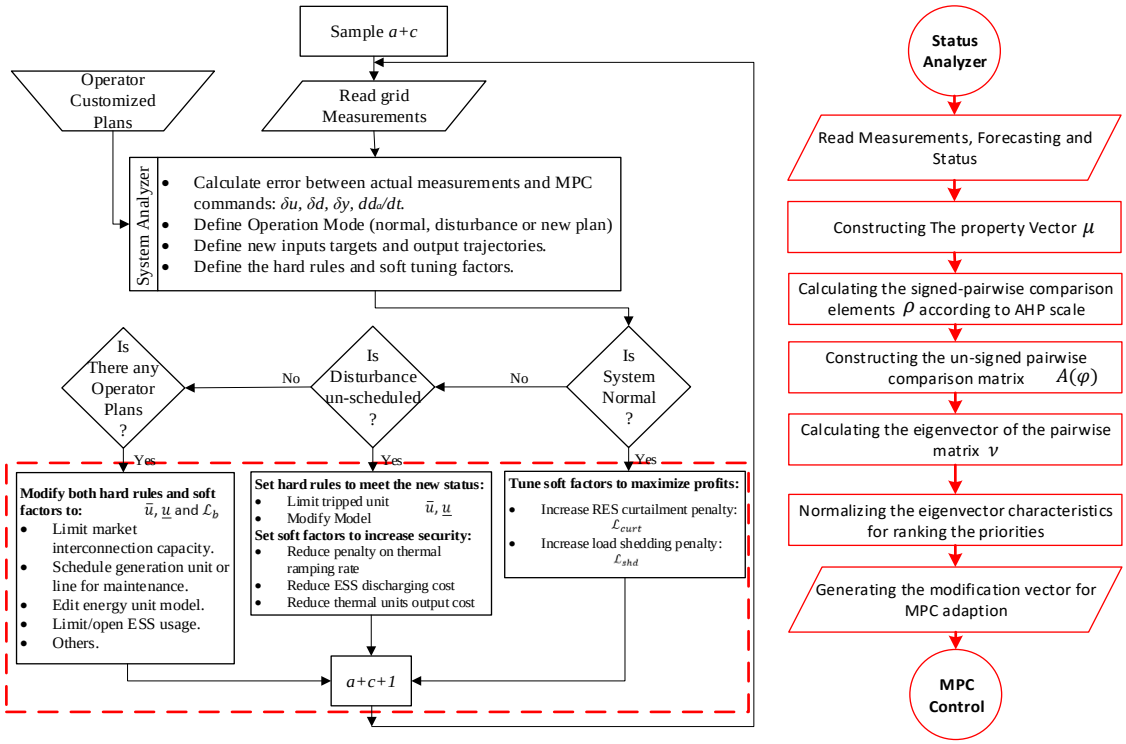


Figure 6.2: Adaptive PEMS flowchart.

The main goal of the adapter is to define the task-oriented control adaption vector for MPC in the light of system status and the operator scenario. In the second level of the

hierarchical system is the sub-goals, which define the orientation of the task to be the normal operation, a customized operation plan or a response to a disturbance/outage.

In order to achieve the required task, there are four criteria to select or even balance between them. The criteria are selected or prioritized to maximize the profit, security, flexibility and vRES share. Lastly, the AHP has several alternative factors to determine to satisfy certain criteria to achieve a certain goal.

Mathematically, suppose a vector μ has the property values for i^{th} alternative importance/effect concerning the four criteria [103],

$$\mu = [\mu_1, \mu_2, \dots, \mu_m] \tag{6.6}$$

where m is the total number of the competitive alternatives.

The AHP pairwise comparison elements ρ is calculated as follows,

$$\rho_{i,i+1} = \Delta\alpha . \Delta\mu^{-1} . (\mu_i - \mu_{i+1}) \tag{6.7}$$

where μ_i and μ_{i+1} are the two comparative property and $\Delta\alpha$ the difference between the maximum and minimum values of AHP scale.

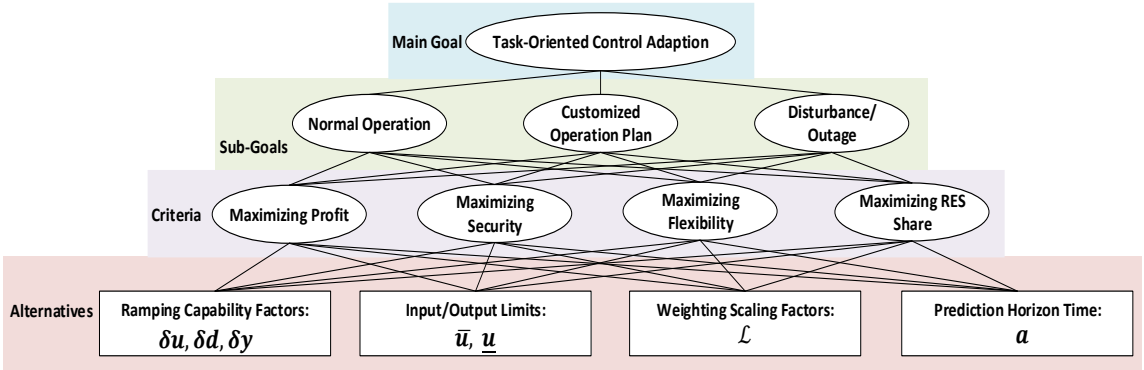


Figure 6.3: Task-oriented control adaption based on AHP.

On the other hand, the, $\Delta\mu$ is the difference between the maximum and minimum value of each property. For simplification, the signed comparison elements should be converted to an unsigned comparison matrix according to the following equation.

$$\omega_{i,i+1} = \begin{cases} 1 + \left|\rho_{i,i+1}\right|, & if\ \rho_{i,i+1} \geq 0 \\ (1 + \left|\rho_{i,i+1}\right|)^{-1}, & otherwise \end{cases} \tag{6.8}$$

The pairwise comparison matrix is constructed in the following form.

$$A(\omega) = \begin{bmatrix} 1 & \omega_{12} & \cdots & \omega_{1m} \\ \omega_{21} & 1 & \ldots & \omega_{12} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{m1} & \omega_{m2} & \ldots & 1 \end{bmatrix} \tag{6.9}$$

The eigenvector of the matrix A is the characteristic vector of the square matrix. The matrix A is analysed to determine the eigenvalue or characteristic elements value λ of the characteristic vector ν determined by, $A.\upsilon = \lambda.\nu$. The effect of the adapted factors/alternatives is prioritized according to the required sub-goal. The priority list and weighted values are calculated as follows,

$$\hat{v}_i = \nu_i.\left(\sum_{i=1}^{m} \nu_i\right)^{-1} \tag{6.10}$$

where $\hat{v}_i$ and ν_i are the normalized and non-normalized priority factors. The normalized adaption vector $\hat{v}_i$ is fed to MPC to modify it according to the real-time status.

6.4 Case Study

To illustrate and validate the developed PEMS, the remainder of this part discusses the PEMS applied in a well-known case study of WSCC 9-bus [104]. The model has been adapted to outfit the different generation and storage types. Figure 6.4 shows the developed simulation study system. The wind farm is coupled to bus 6 while a PV solar plant with BSS is connected to bus 9, PHS system is working on bus 7. The units of conventional

generation, renewable generation, storages, and demand is formulated. The state-space input vector, states vector and disturbance profiles vector are formulated as follows,

$$\begin{bmatrix} \dot{soc}_{PHS} \\ \dot{soc}_{BSS} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}_{\dot{x}} = \begin{bmatrix} \frac{\eta_{PHS,ch}}{C_{PHS}} P_{PHS,ch} - \frac{{\eta_{PHS,dch}}^{-1}}{C_{PHS}} P_{PHS,dch} \\ \frac{\eta_{BSS,ch}}{C_{BSS}} P_{PHS\_ch} - \frac{{\eta_{BSS,dch}}^{-1}}{C_{BSS}} P_{BSS,dch} \\ \eta_{d1} P_{d1} - P_{shed1} \\ \eta_{d2} P_{d2} - P_{shed2} \\ \eta_{d3} P_{d3} - P_{shed3} \\ {\eta_{gas}}^{-1} P_{gas} - d_{gas} \\ {\eta_{ccgt1}}^{-1} P_{ccgt1} - d_{ccgt1} \\ {\eta_{ccgt2}}^{-1} P_{ccgt2} - d_{ccgt2} \\ {\eta_{w}}^{-1} P_{w} + P_{w\_cur} \\ {\eta_{s}}^{-1} P_{s} + P_{s\_cur} \end{bmatrix}_{u} + \begin{bmatrix} 0 \\ 0 \\ d_{d1} \\ d_{d2} \\ d_{d3} \\ 0 \\ 0 \\ 0 \\ -d_{w} \\ -d_{s} \end{bmatrix}_{d} \tag{6.11}$$

$$\begin{aligned} u = [&P_{gas}, d_{gas}, P_{ccgt1}, d_{ccgt1}, P_{ccgt2}, d_{ccgt2}, P_{d1}, P_{shed1}, P_{w}, P_{w_{cur}}, \dots \\ &P_{d2}, P_{shed2}, P_{PHS_{ch}}, P_{PHS_{dch}}, P_{d3}, P_{shed3}, P_{s}, P_{s_{cur}}, P_{BSS_{ch}}, \dots \\ &P_{BSS_{dch}}, P_{1-4}, P_{4-5}, P_{5-6}, P_{3-6}, P_{6-7}, P_{7-8}, P_{8-2}, P_{8-9}, P_{9-4}], \\ x = [&SOC_{PHS}, SOC_{BSS}]^{T}, \\ d = [&P_{d1}, P_{d2}, P_{d3}, P_{w}, P_{s}]^{T}. \end{aligned} \tag{6.12}$$

$$0 = \begin{bmatrix} 1&0&1&0&1&0&-1&0&1&0&-1&0&1&-1&-1&0&1&0&1&-1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&-1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&-1&0&1&-1&0&0&0&0&0&0&0&0&0&0&1&-1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&-1&-1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&1&0&1&-1&0&0&0&0&0&0&1&-1 \end{bmatrix} . u \tag{6.13}$$

$$\begin{cases} \mathrm{P_{PHS_{disch}}(c).P_{PHS_{ch}}(c) = 0} \\ \mathrm{P_{BSS\_disch}(c).P_{BSS\_ch}(c) = 0} \end{cases}$$
$$P_{min} \le u \le P_{max}, \Delta u_{min} = -P_{max}, \Delta u_{max} = P_{max} \tag{6.14}$$
$$SOC_{min} \le x \le SOC_{max}$$

The optimization problem was solved by minimizing the objective function in (6.4). In this case study, the objective function is subject to (6.11) to (6.14). The weights of the state

of charge and change in power are set to zeros for this case. This means that the value of the output state of change and the change in manipulated power do not care about the optimization problem. This value of the initial weights changes by scaling factors with time according to the actual system state or actual model. The following part discusses two different simulation scenarios.

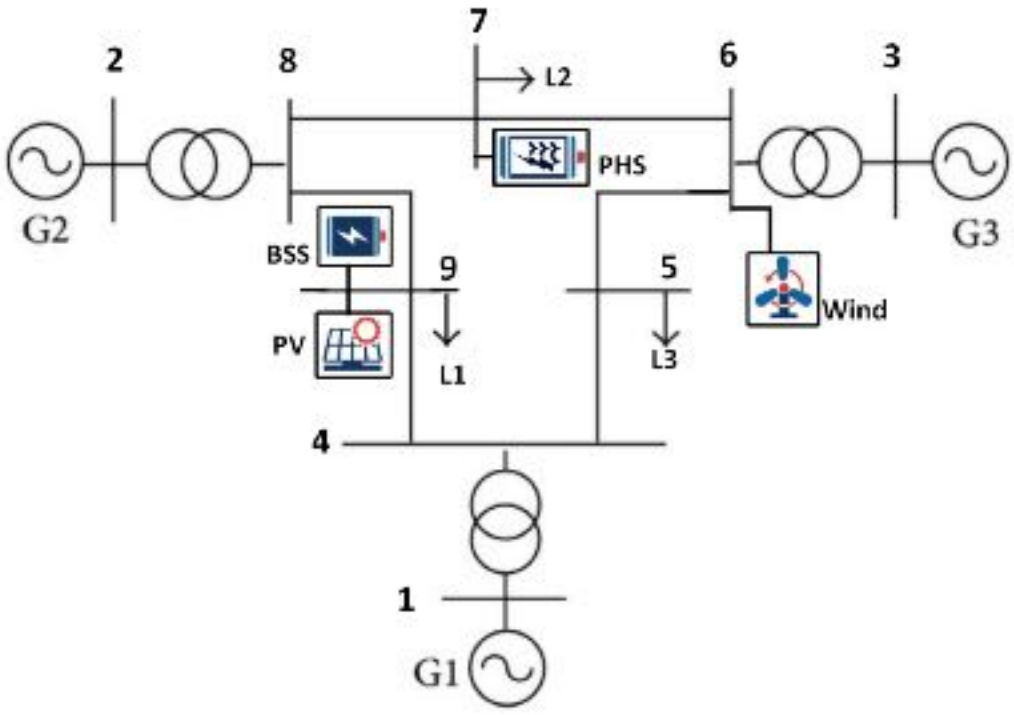


Figure 6.4: Modified WSCC 9-bus case study.

6.4.1 Scenario 1: Normal Operation with Customized Plan

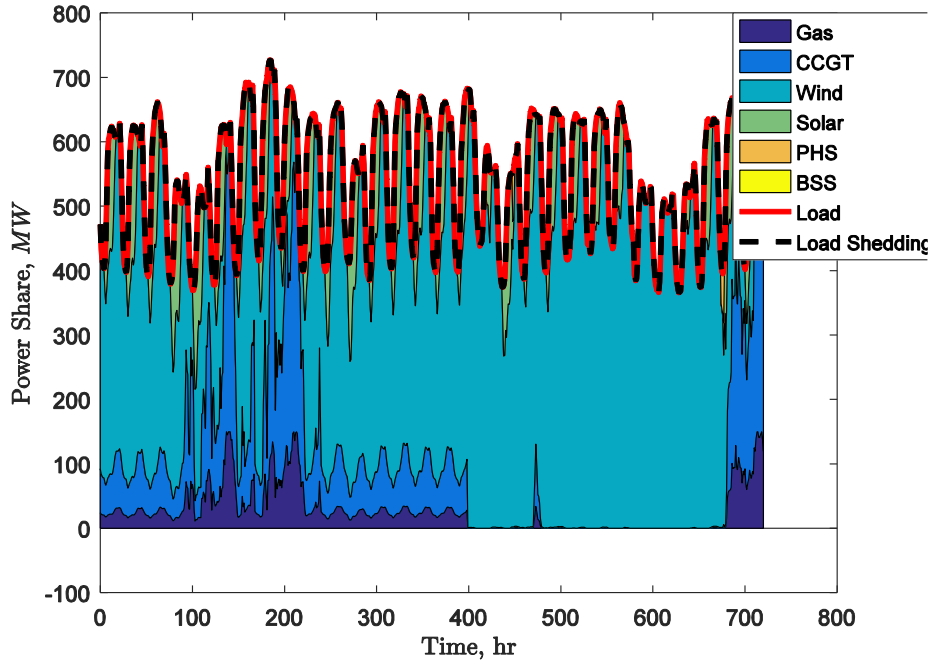
In this scenario, the system is a normal operation with the initial constraints and weights/costs. The operator changes the system's operation strategy for the specific plan after 400 hours. The customized plan of operation is set to switch from maximizing available flexibility to maximum profit via maximizing usage of renewable energy sources.

The value of the scaling factor for the manipulated variable power of wind and solar are set as $\mathcal{L}_b^w = \frac{1}{7}, \mathcal{L}_b^s = 0$. Figure 6.5(a) shows the power-sharing for all source's types alongside the required load and the amount of load shedding. The manager dispatches the minimum conventional generation cost by keeping a considerable amount of flexibility before the operation plan customized.

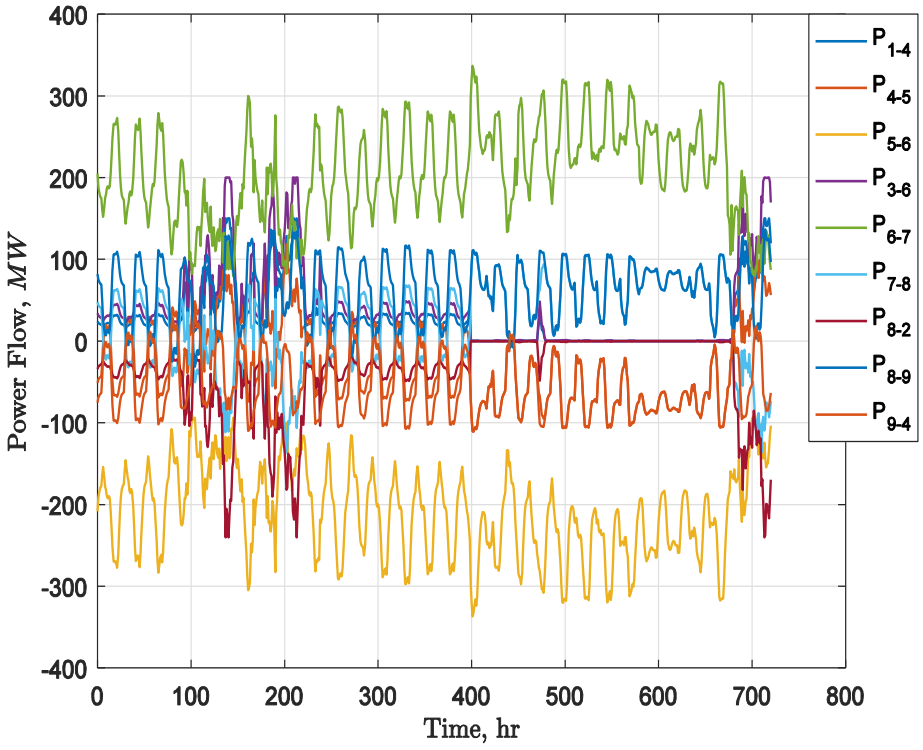
After that, almost the conventional sources such as gas and combined cycle generators are shut down and the maximum amount of renewable energy is used. The value of power flow in transmission lines is derived as shown in Figure 6.5(b). As noted, there is a repair rate of change in transmitted power during the period of high wind variability. The generation system energy and cost for a month are summarized in Table 6.1.

Table 6.1: Consumed energy and cost for the first scenario.

Type	$Energy$ MWh	$Cost_{gen}$ $M€$
GAS	19647	1.9647
CCGT	55666	4.6759
Wind	271230	6.9165
Solar	45640	0.80327
PHS	553.8	0.004486
BSS	53.4	0.002670
Total Generation	392790	14.378
Spilled wind	233820	0.93528
Spilled solar	8345	0.008345
Load Shedding	0	0
Total cost	-	15.3216



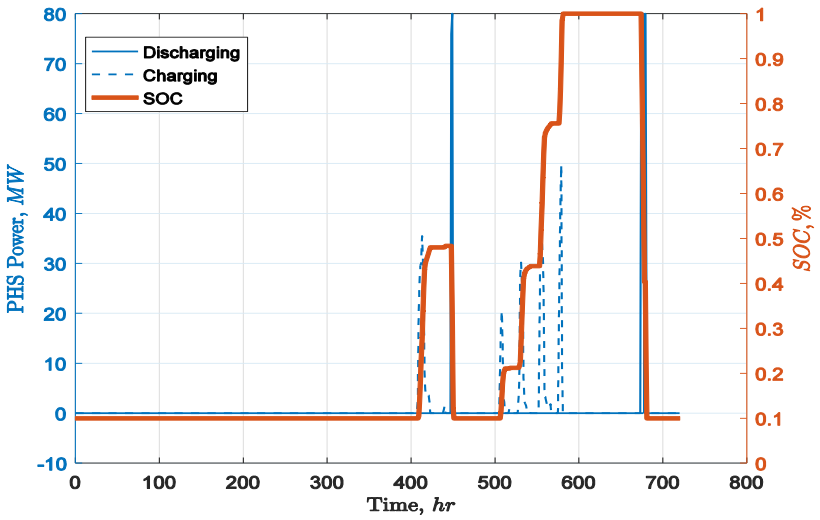
(a)



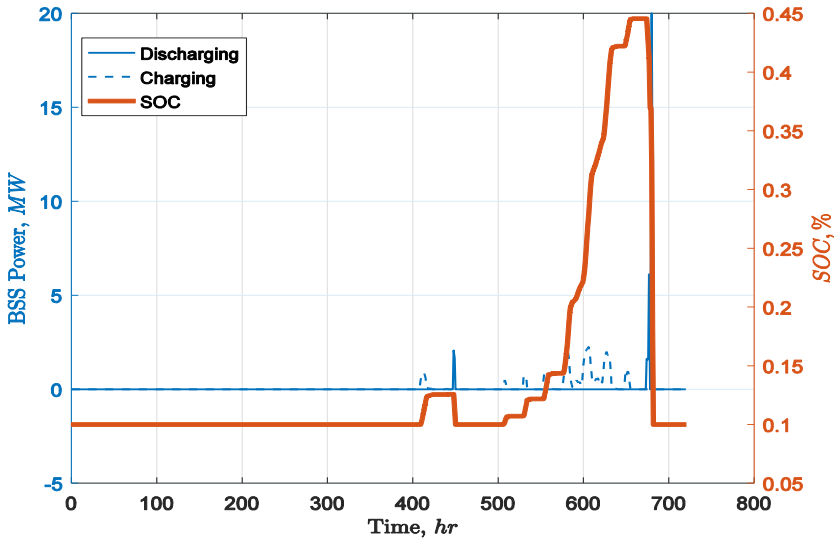
(b)

Figure 6.5: Scenario 1: Customized plan (a) Power sharing, (b) Line power flow.

ESS is managed to minimize its usage as soon as possible due to the high cost of installing it. Before the operator switching a new plan, the state of charge values for PHS and BSS is set to a minimum of about 10%. After that, the extra high free energy from wind and solar is stored and re-used again upon system needs. Figure 6.6 shows the ESS utilization during charging and discharge against the state of charge on the right-hand side.



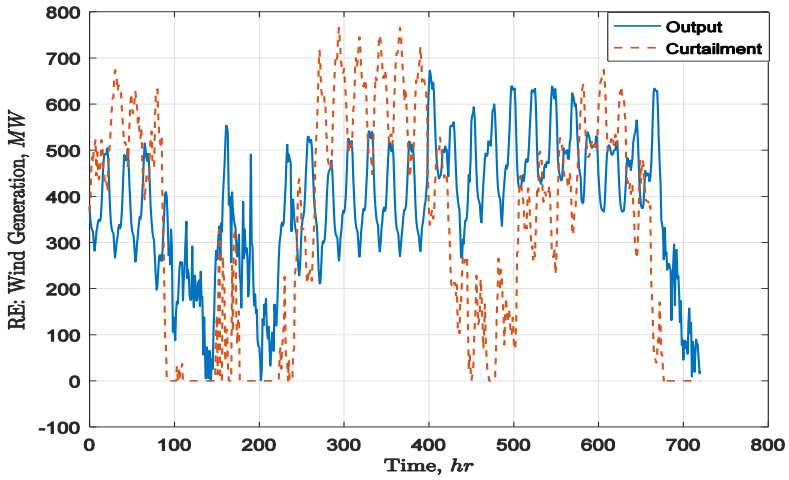
(a)



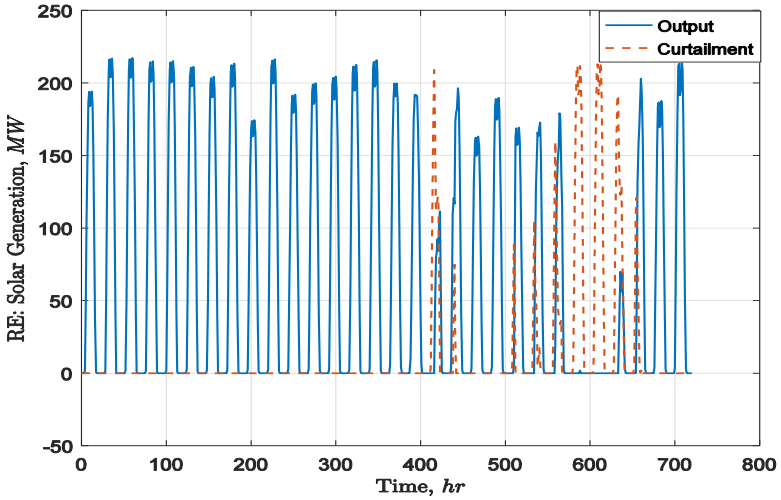
(b)

Figure 6.6: Scenario 1: Customized plan, charge/discharge cycle (a) PHS, (b) BSS.

In Figure 6.7, the renewable energy output and curtailment of wind and solar power. The curtailment is reduced in the wind and solar power after 400 hours and it increased significantly after switching to the new operation plan. The reason behind the high value of solar curtailment is the low demand at the same time window. The output values of wind experienced high variability between 100th and 250th hour and from 670th to the end.



(a)



(b)

Figure 6.7: Scenario 1: customized plan, RES output and spilled (a) wind, (b) solar.

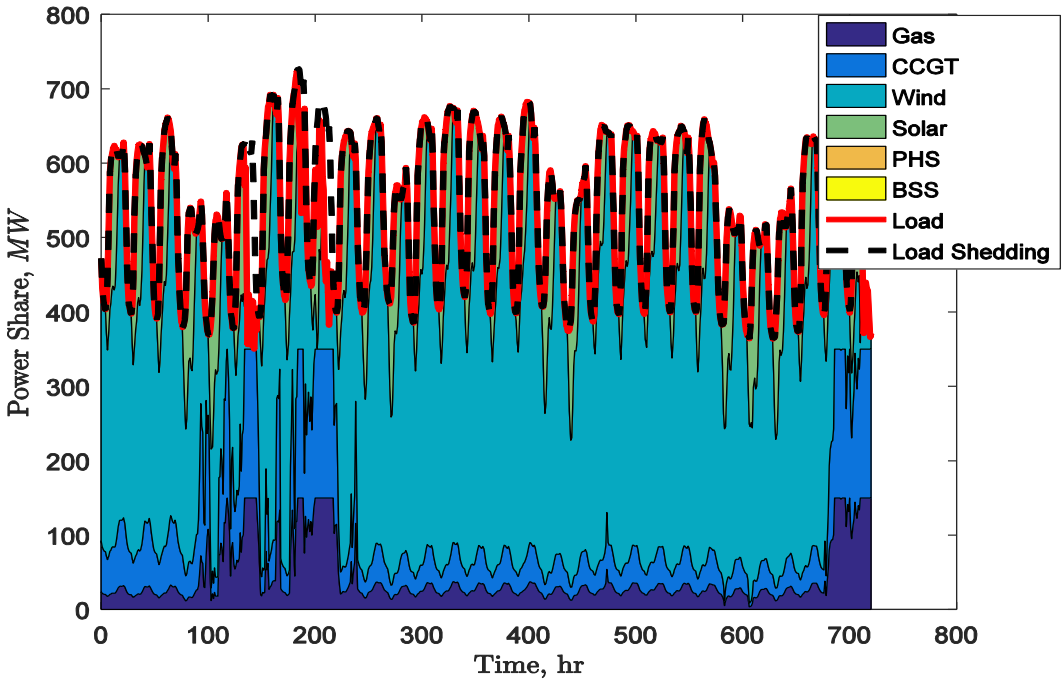
6.4.2 Scenario 2: Unscheduled Contingency

When a power system sustained to contingency like a generator trip, the dispatching problem becomes a big challenge and the risk is extra increased due to the high share of renewable energy which increases power mismatch. This scenario will be applied with and without adaption.

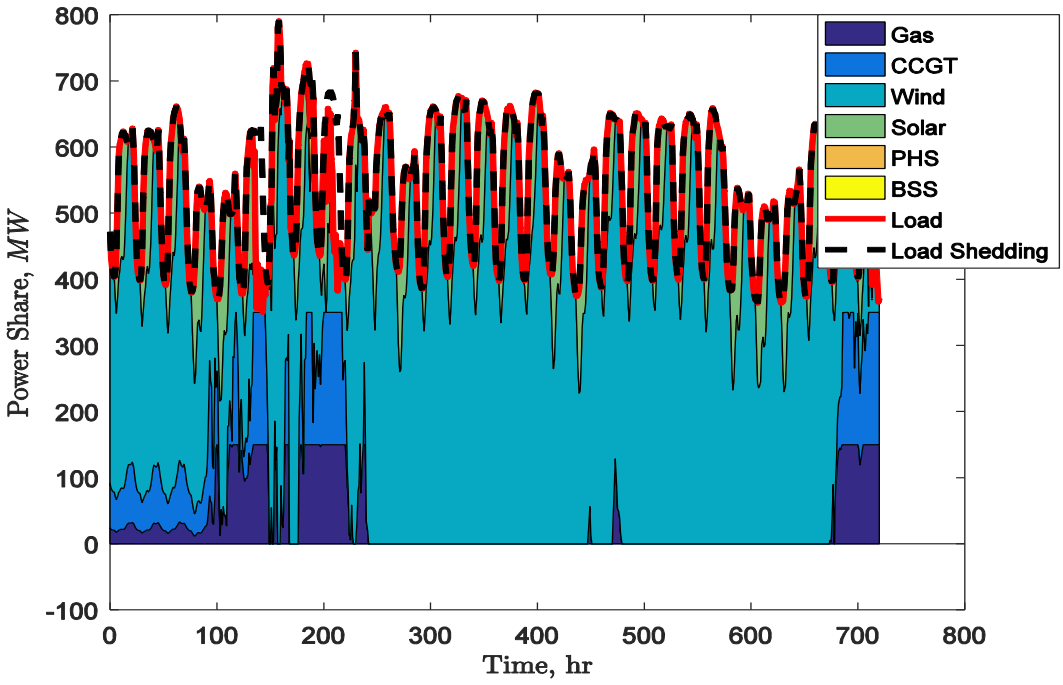
In two cases of operation, the generator at bus 2 is tripped at the 100th hour. Figure 6.8(a) shows the result during the contingency but without any adaptation in the model, constraints, or weights. After contingency, the rest of the conventional generation sources of GAS and CCGT continued to work. On the other hand, after PEMS adaptation, in Figure 6.8(b), the conventional sources are replaced by wind power and the gas generator is only working during the wind and solar shortage as seen between 450th and 480th hour.

Figure 6.9 shows a comparison of the main impact without applying the adoption and with modification. In the upper axes, a comparison between RE curtailment in two operation cases. The curtailment has the same value in two cases.

However, RES share is increased slightly after contingency to replace conventional power. In the lower axes of Figure 6.9, the state of charge of PHS and BSS is compared between without and with adaptation application. It is clear that, for both PHS and BSS, the storage systems not operated, and the state of charge stayed at the lower level of 10 percent without charge or discharge. On the other hand, both storage system is utilized in a little different depending on their individual characteristics.



(a)



(b)

Figure 6.8: Scenario 2: Unscheduled Contingency, Generator trip, (a) Without adaptation, (b) with adaptation.

The storage system played an important role during this period to reserve the load shedding. If the storage system in that part has a larger capacity, the load shedding is decreased significantly. A detailed comparison between the two cases of operation of the second scenario is shown in Table 6.2.

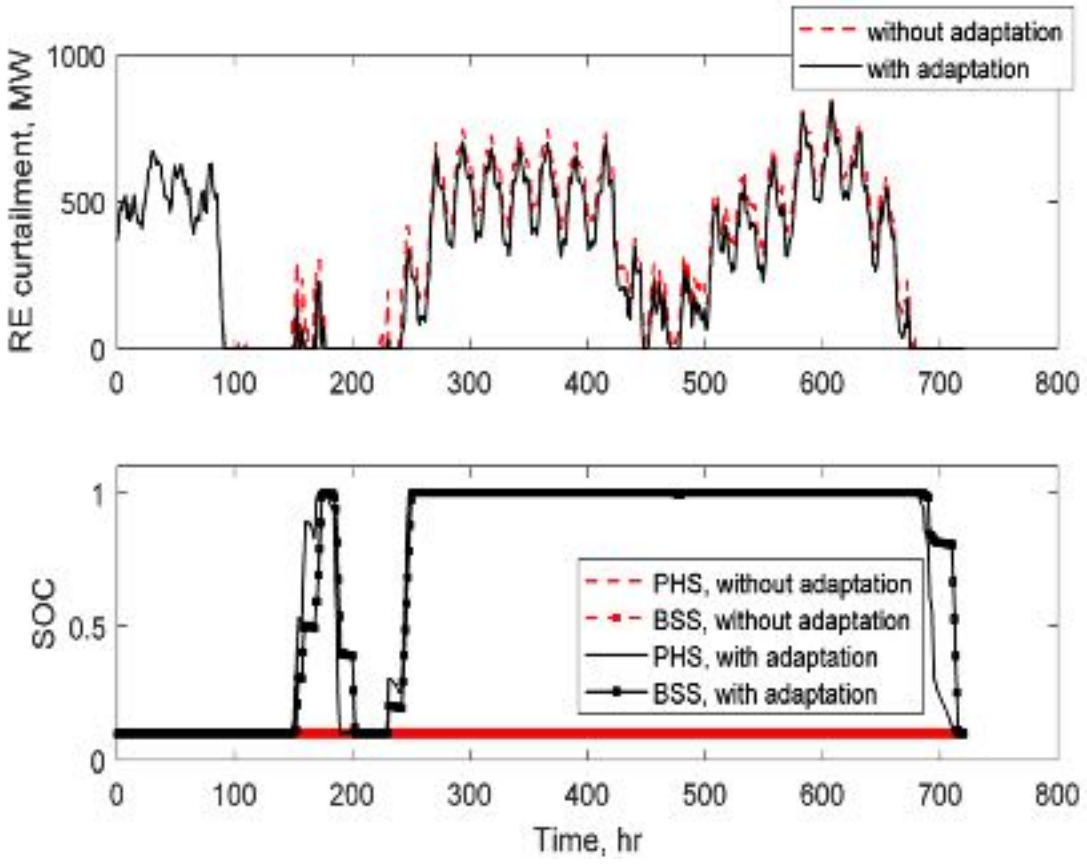


Figure 6.9: Scenario 2, RE curtailment and SOC comparison between without and with system adaptation.

The conventional sources are significantly decreased in the case of the adapted PEMS as compared with PEMS only. Of course, that is because of the tripped generator and also, the manager prefers to use free RE power. The wind power will have increased after adaptation and solar almost remains as without adoption case because already, it is fully

employed. For ESSs, both PHS and BSS are not used in case of an un-adapted case. While both are used in the most economical way to cover the power shortage after modifications. The total generated energy was slightly increased in the modified case by 2467 MWh, although, the cost of total generation is reduced by about 1.6852 $M€$. The replacement of conventional generation by RE is the main reason for the low cost after modification.

Table 6.2: comparison energy and cost values with and without adaptation for scenario 2

Type	Without PEMS adaptation		With PEMS adaptation	
	$Energy$ MWh	$Cost_{gen}$ $M€$	$Energy$ MWh	$Cost_{gen}$ $M€$
GAS	31585	3.156	24514	2.4514
CCGT	47517	3.9914	26765	2.2483
Wind	252110	6.429	281430	7.1764
Solar	53874	0.9482	53736	0.94575
PHS	0	0	845.71	0.00685
BSS	0	0	262.21	0.01311
Total Generation	385086	14.527	387553	12.8418
Spilled wind	252950	1.012	223630	0.89452
Spilled solar	111.33	0.0001	249.72	0.00025
Load shedding	6974.2	69.742	6057.8	60.578
Total cost	-	85.281	-	74.314

Also, the spilled energy of RE is decreased because of the large amount of wind power used after adaptation by about 0.117 $M€$. If the system production cost reduced without shrinking the load shedding, the developed manager loses the security requirement. Fortunately, the processes provided by the manager after adoption reduces the amount of load shedding. The load shedding cost is set to be 10,000€ . In comparison, the load

shedding cost is reduced by about $9M€$ in case of adapted PEMS than un-adapted case. Sum-up all, the developed not only succeeded to reduce the amount of load shedding, maintain security but also achieves lower cost of generation, spilled energy, and load shedding. It succeeded to reduce the cost by about $11M€$.

The developed energy management system prototype is applied based on the laboratory-based smart grid Testbed by reconfiguring the generation and storage units to represent the large-scale power system grid characteristics. The network is studied for experimental validation. A bidirectional inverter is used to simulate the RES and ESS combination to simplify the experimental implementation. Figure 6.10 shows the interconnected power system as a limited experimental setup. Figure 6.11 shows the power dispatching of the two conventional power CG1 and CG2 and the inverter works to represent the combination of the RES+EES to feed the load.

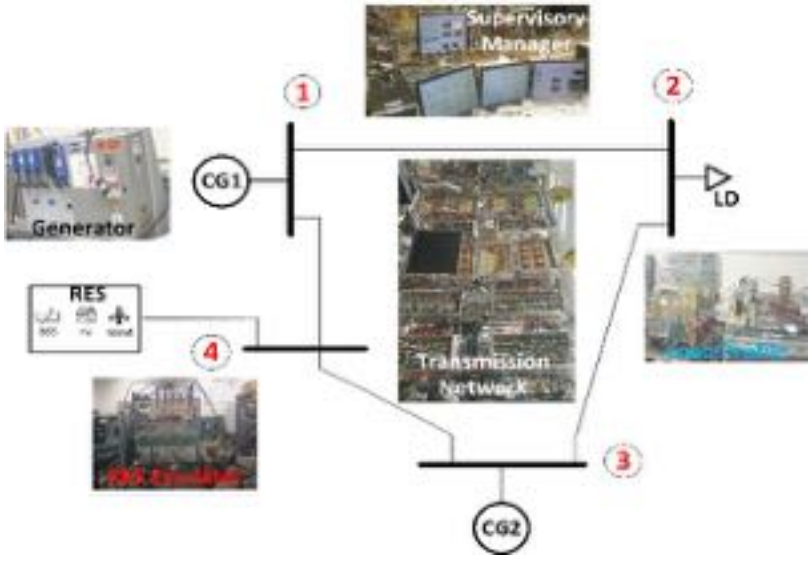


Figure 6.10: Verification of the developed technique in the test-bed.

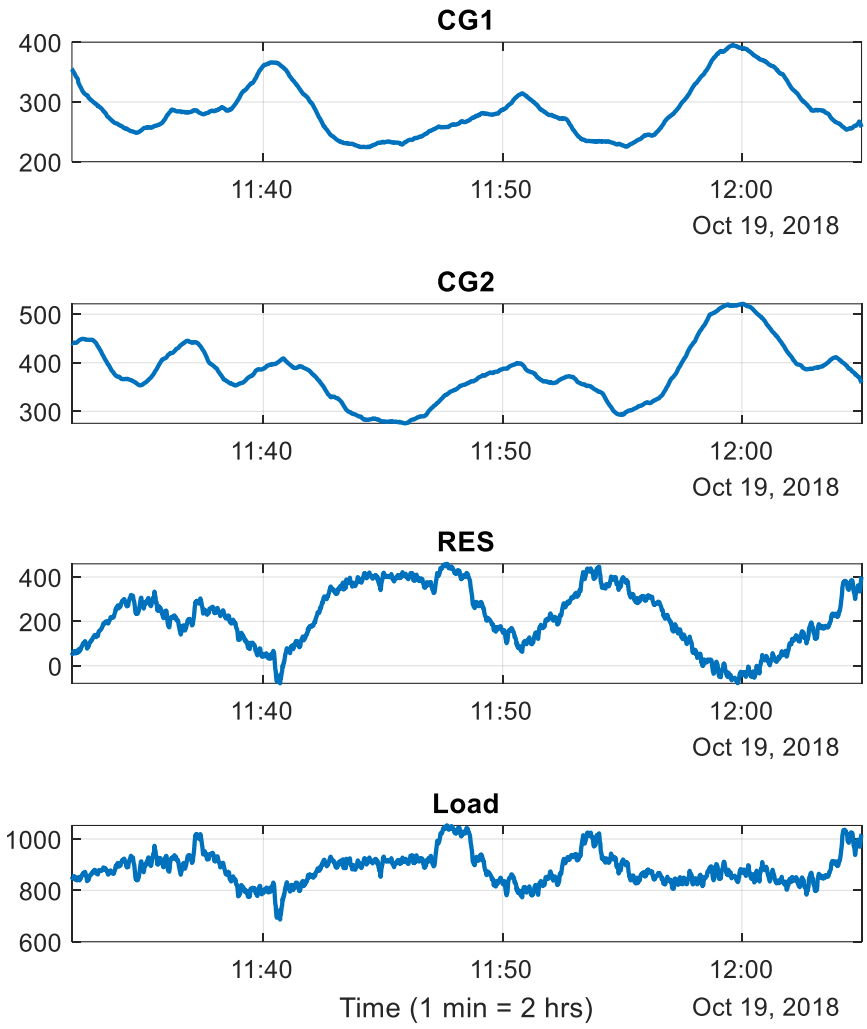


Figure 6.11: Experimental results.

6.5 Summery

This chapter developed a new management system, which has features of prediction and intelligence while dispatch, manage and control the power system units. The optimization and control problem was solved via DT based predictive control. The introduced real-time system adapter uses the actual system status to adjust the system model, constraints, objective, and weights/costs to resolve when the system sustained any contingency or unforeseen event in the grid. In addition, the management strategy is not

only followed vRES ramping but also, maximizes profits via minimizing ESS utilization. In terms of managing the difficulty of the problem in practice, it makes the operator put some plans of operations and it can readjust the operator plans if it is not feasible. The results show also that the new developed strategy not only minimizes the cost but also reduces the load shedding and reduces the spilled free renewable power.

Chapter 7 Digital Twin for Networked Microgrids Cybersecurity

The increased rate of cyber-attacks on the power system necessitates the need for innovative solutions to ensure its resiliency. This work builds on the advancement in the IoT to provide a practical framework that can respond to multiple attacks on a network of interconnected microgrids. This chapter provides an IoT-based digital twin (DT) of the cyber-physical system that interacts with the control system to ensure its proper operation. The IoT cloud provision of the energy cyber-physical and the DT are mathematically formulated. Unlike other cybersecurity frameworks in the literature, the developed one can mitigate individual as well as coordinated attacks. The framework is tested on a distributed control system and the security measures are implemented using cloud computing. The physical controllers are implemented using single-board computers. The practical results show that the developed DT is able to mitigate the coordinated false data injection and the denial of service cyber-attacks.

7.1 Introduction

rapid penetration of Renewable Energy Resources (RES) and the recent trend of transportation electrification increases the growth of networked microgrids industries in the energy sector. The recent development of the Networked Microgrid (NMG) systems converted the electrical distribution grid from passive to active networks and transformed the consumers into prosumers, which significantly increases the complexity of these systems. On one hand, the NMG physical system becomes more composite by containing multiple two-way interconnected systems such as Distributed Energy Resources (DERs), Energy Storage Systems (ESSs), flexible loads (as electric vehicles), fixed loads, power

electronics converters, transformers, cables, etc. On the other hand, the degree of the cyber system complexity is much greater due to the use of multiple infrastructures, communication protocols, controllers, Intelligent Electronics Devices (IED), smart meters, and phasor measurement units. This transforms the modern electric distribution system into a critical energy cyber-physical system (ECPS) [11], [105], [106].

The two-way power flow controllability and the transactive energy capabilities of the NMG depend mainly on many bidirectional power electronic converters, which should have a flexible, fast, and stable response to support the grid during the normal operation and the disasters. To efficiently and safely operates the NMG, proper management and control methodologies should be developed. Modern networked control systems are linked from the downstream level (nanogrids) to the upstream level (distribution substation), which are considered as an Industrial Internet of Things (IIoT) based communication infrastructure. The IIoT enables the required flexible coordination and integration among the DER's controllers and improves the overall system management. Being IoT technology-dependent, a large amount of data is harvested from the physical assets' sensors and the cyber assets' controllers, which lead to the efficient operation of the grid and securely minimizes the risk. Thus, the IoT is believed to revolutionize the way we understand the energy sector [29], [33], [107], [108, p. 10].

Usually, the control system of the NMG systems is developed as a hierarchical distributed architecture, which contains primary, secondary, and tertiary control layers. The geographical distribution of the NMG gives incentives to the designers to use the distributed control strategy to reduce the communication bandwidth and ensures the plug-

and-play flexible installation of the microgrids. Generally speaking, the coordination between agents in a distributed control system usually depends on consensus protocols [16], [59]–[61], [109]–[116]

Despite the reported benefits of the distributed control system in the literature [59], [110]–[114], [117]–[119], it is more vulnerable to cyber threats. Due to the absence of the centric oversight and the low-security level at this level of the consumer system, more cyber-attacks are inevitable [11]. In this kind of control systems, typically, the data transaction is secured using two ways. The first track is provided by IT data encryption and certificate authentication [118]. The second one focuses on the resiliency of the control system itself [11], [12], [16], [60], [61], [110]–[116], [118]–[120]. The authors in [11] presented an attack resilient control system for multiple DERs based on a neighbor watching mechanism to isolate the attacked control agent from the network graph. In [118], a resilient distributed control system is introduced to solve the packet loss problem while in [29], a distributed control system was developed. The controller was able to detect and gradually isolate the infected controller. In [110], a mathematical morphology technique was used to analyze the neighbor's dynamical features to detect, identify and mitigate the attacked agent. A trust-based and compensator-based control protocol were introduced in [16] and [60], respectively to guarantee the distributed system synchronization under sensor/actuator attacks. In [12], a reputation-based neighborhood watches method was used to detect the data integrity attack on the distributed scheduling. For the same problem, the authors in [61] developed a confidence level-based mechanism using on the top hidden communication network in parallel with the main distributed management system to detect

and isolate the attack. Kullback-Leibler (KL) divergence technique was used in [115] to determine the trust level of the distributed controllers and then isolate the faulty data source according to the divergence rates.

Regardless of the efforts that were done so far, multiple coordinated attacks on the distributed secondary and/or tertiary control systems have not received enough attention. Coordinated attacks can easily disturb the consensus among the distributed controllers. Besides, regular solutions of mitigating these kinds of attacks by excluding it from the cyber graph cannot solve the problem because the excluded agent might be a vital agent that can disturb an entire microgrid cluster. Furthermore, mixing the coordinated attacks on both sensors and controllers alongside with communication network magnifies the security concerns and impose a handicap on the IIoT benefits. Motivated by [120], the authors believe that the live data-driven model can discover the coordinated attack and provide the autonomous post-attack recovery.

In this chapter, an IoT-based digital twin (DT) for the cyber-physical networked microgrids is introduced. The cloud-based DT platform is implemented to be a centric oversight for the NMG system. The cloud system hosts the controllers (cyber things) and the sensors (physical things) into the cloud IoT core in terms of the IoT shadow. The developed DT covers the digital replica for both the physical layer, cyber layers and their hybrid interactions. The developed framework ensures the proper and secure operation of the NMG. Also, it can detect false data injection (FDIA) and denial of service (DoS) attacks on the control system whether they are individual or coordinated attacks. Once an attack is detected, corrective action can be taken by the observer-based on What-If scenarios that

ensure the safe and seamless operation of the networked microgrids (NMG). DT introduce a constructible active model to provide interaction between the defense mechanism and the attackers.

7.2 Digital Twin Based Cybersecurity System Description

Recently, IoT technologies and cloud computing advancements encourage the energy sector to utilize this digital transformation for better understanding and improving the energy system operation. The DT strategic technology is developed to get the benefits of the IIoT, the ECPS models and the advanced data analytics to understand what is happening and what will happen for the ECPS. The DT is defined as digital replica/model that includes the last information matching a thing. The DT was successfully applied recently in the industry for manufacturing, power plants, healthcare, and automotive sectors [65], [108], [121]. Figure 7.1 shows the developed DT architecture. The NMG (physical assets) under study is a DC networked microgrid (DCNMG) system in the physical space in the lower layer. The physical system is constructed by n interconnected DC microgrids clusters where each cluster contains m DCNMGs. The interconnected clusters are connected to a main Medium Voltage DC (MVDC) bus. The NMG is aggregated at the PCC with the grid through an interlinking DC/AC inverter and a step-up transformer. The primary controllers are assumed to be a part of the physical system as they are responsible for the local control of the converters. In the second layer, the edge system consists of the distributed controllers and the tertiary controller. The secondary controllers are coordinating via a cyber compunction IED-to-IED links to satisfy the objective control rule that is received from the tertiary controller.

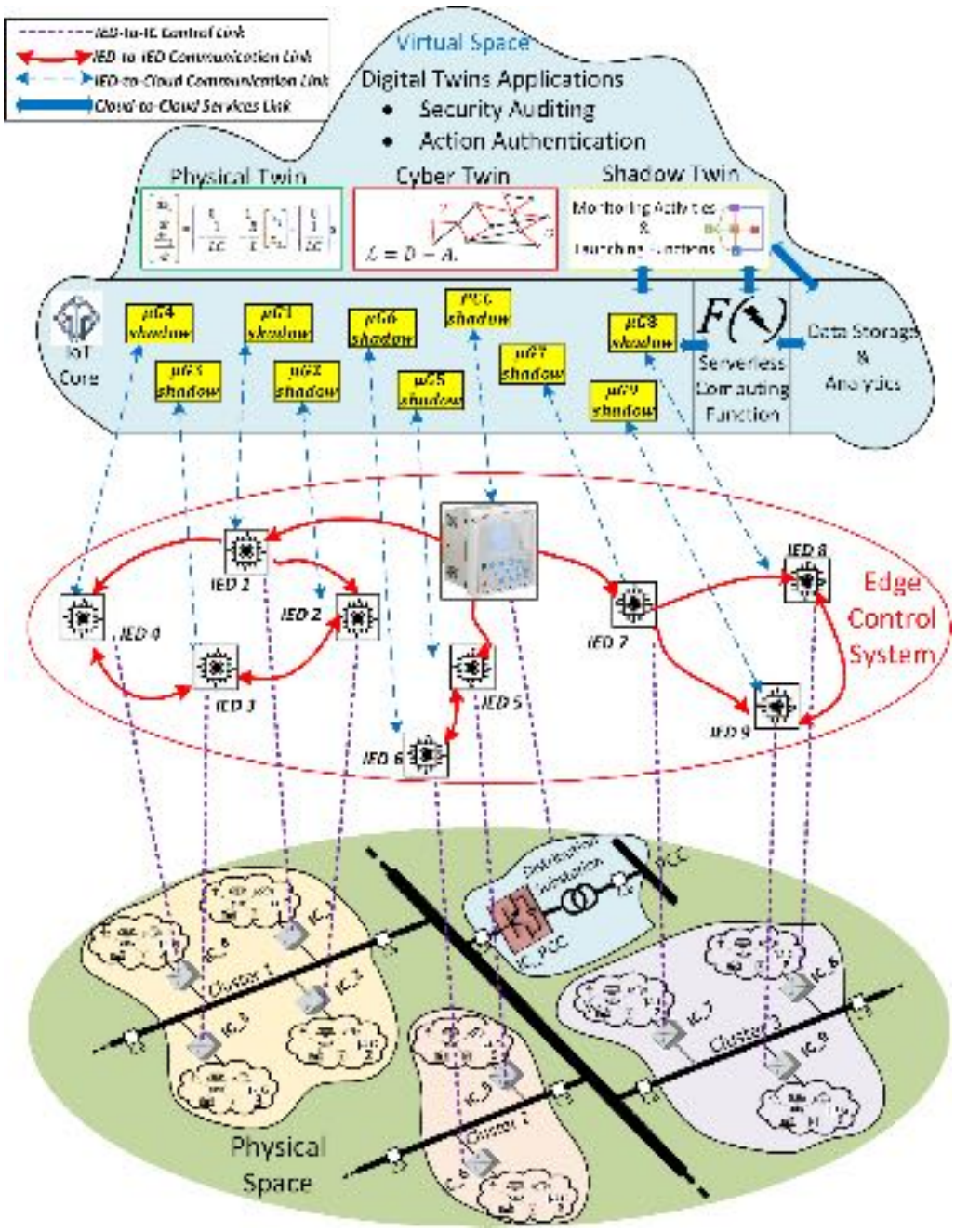


Figure 7.1: The overall system architecture of the developed DT platform for ECPS.

The tertiary control agent sends the required reference power-sharing factor to the secondary controllers' leaders for each cluster of microgrids. Then, the leader sends the control law to the cluster follower agents by the consensus protocol to make an agreement

on the leader state. The control objective is to guarantees equal relative power-sharing among microgrids. The failure in ensuring the control objective due to a communication failure or a cyber-attack causes unfair power-sharing and can disturb/collapse the voltage regulation at the PCC. Since the NMG is ruled by the balancing between the NMGs power and the PCC power, the physical DT is implemented to represent the real-time balancing according to the physical living model of the interconnected system.

In addition, the cyber-DT represents the multi-agent consensus convergence rules to guarantee the matching between the tertiary control system and the secondary control system. The hybrid CPS replica enhances the centric oversight by ensuring that the mismatch between the cyber and physical system components is decaying to zero. If the mismatch between the DT and the real-time measurements exists, the CPS failure or attack can be detected, estimated, and mitigated. Both the physical system states and the cyber control agents are connected to the virtual layer (cloud system) through the IoT core as a shadow of things. Things' shadows have the last states of the controllers/sensors, which are updated periodically by the edge controller to notify the cloud of the new states.

A service-less computing function is utilized to launch certain applications/measures according to the status of the shadow states. The focus of this chapter is the resiliency of the NMG against the cyber-attacks on the physical sensors and/or control agents. The DT dynamic model of the physical system, cyber system and their interaction are discussed in Section 3.3. The following section models and elaborates on the cyberattack on the NMGs.

7.3 Cyberattack Modelling

The IoT cyber edge system is vulnerable to different types of attacks that can threaten the communication links or the controllers themselves. A cyber-attack against control systems is usually classified into three different properties/resources available for the attack: model knowledge, disclosure resources, and disruptive resources. The following assumptions hold.

Assumption 1: An attacker can acquire at least the local data to launch an attack to disturb the consensus and the link between the secondary and primary controller is a part of the local controller.

Assumption 2: An attack on the PCC agent or its communication link with the leaders can mislead the entire distribution system.

Assumption 3: If an attacker knows the distributed control systems, consensus protocol and the network topology, he can launch a multiple coordinated attacks, which can easily mislead the distributed observers.

Assumption 4: If an attack was successfully launched on the PCC agent or the leader agents of clusters and the attack is detected, the isolation of the attacked agent cannot retrofit the consensus as that will also exclude the healthy follower agents.

Mathematically, the attack on the controller can be on the control actuator signal to the physical system and/or on the cyber graph states as follows,

$$\left.\begin{aligned} u_i^f &= u_i + \gamma_i u_i^a \\ x_i^f &= x_i + \alpha_i x_i^a \end{aligned}\right\} \tag{7.1}$$

where u_i, u_i^f are the healthy and the attacked actuator signal to the physical system. Also, x_i, x_i^f are the healthy and faulty states sent to neighborhood controllers from the physical system. The Boolean signals γ_i, α_i is representing the presence of the attack vector u_i^a, x_i^a.

Theorem 1: Suppose the cyber system (3.2) is under attack (7.1) and let Assumptions 1-4 are applied. If an agent i is attacked, then all intact agents j^{th}, which is approached by the compromised agent will have a nondecaying error as compared to the leader agent and the tertiary control objective cannot be satisfied.

Proof: According to attack model (7.1) and by applying the error dynamics (3.19)-(3.20) and substituting in the cyber system (3.2), the combined system dynamics is represented as,

$$\left.\begin{aligned} \dot{x}_i^\theta &= A^\theta x_i^\theta + B^\theta u_i^\theta + B^\theta \xi_i^\theta \\ \xi_i^\theta &= \gamma_i u_i^a - \iota\left(\sum_{j\in n_i} w_{ij}(\alpha_i x_i^a - \alpha_j x_j^a) + g_i \alpha_i x_i^a\right) \end{aligned}\right\} \tag{7.2}$$

By calculating the error dynamics with respect to the leader state and rewriting (7.2) in matrix form,

$$\left.\begin{aligned} \dot{\delta} = \dot{X} - \dot{X}_0 &= A^c\delta + (I_n \otimes B^\theta)\,\xi^\theta \\ \xi^\theta &= -\iota(\mathcal{L}+G)(\boldsymbol{\alpha}\otimes I_n)X^a + (\boldsymbol{\alpha}\otimes I_n)U^a \end{aligned}\right\} \tag{7.3}$$

So, the error dynamics that is resulted by the attack is formulated as,

$$\begin{aligned} \dot{\delta} = A^c\delta &- \iota\left(I_n\otimes B^\theta\right)(\mathcal{L}+G)(\boldsymbol{\alpha}\otimes I_n)X^a \\ &+ (I_n\otimes B^\theta)(\boldsymbol{\alpha}\otimes I_n)U^a \end{aligned} \tag{7.4}$$

By the same way in (3.21) and let the attack is launched at time τ, the solution of (7.4) is:

$$\delta(t) = e^{A^c t}\delta(0) + \int_0^t e^{A^x(t-\tau)}X^a dt + \int_0^t e^{A^u(t-\tau)}U^a dt \tag{7.5}$$

However, the first term is decaying to zero, the second and the third term is nonzero, and their steady-state values depends on the attack vectors alongside cyber system connectivity. Therefore, the PCC control objective cannot be satisfied.

7.4 IoT Shadow Representation

The shadow states represent the monitored cyber and physical states for provisioning the CPS activity every h time instant. A chosen physical sensor ψ transmits its local microgrid measurements to the virtual space (cloud) and the transmitted state is subjected to noise σ^{Ψ}. The shadow of the physical states $\mathcal{Z}^{\Psi}$ is provisioned by matrix S^{Φ} as follows,

$$\mathcal{Z}^{\Psi}(h) = S^{\Phi} C^{\Phi} X^{\Psi}(h) + \sigma^{\Psi}(h) \tag{7.6}$$

Similarly, the cyber system controller state φ is reported as a cyber shadow state $\mathcal{Z}^{\Theta}$ to the cloud by provisioning matrix S^{Θ} as follows,

$$\mathcal{Z}^{\Theta}(h) = S^{\Theta} C^{\Theta} X^{\Theta}(h) + \sigma^{\Theta}(h) \tag{7.7}$$

where the transmitted data has noise σ^{Θ}.

In addition to the periodic shadow update every sample time h, the occurrence of an event q is assumed to update the shadow to $\mathcal{Z}(t_q)$ that has the following representation,

$$\mathcal{Z}_i(h) = \{\mathcal{Z}_i(t_{q-1}), \mathcal{Z}_i(t_q), t_{q-1}, t_q, \mathcal{Z}_{\varrho}(t_q)\} \tag{7.8}$$

where t_{q-1},t_q are the times of the last two consequence events and $\mathcal{Z}^{\varrho}(t_q)$ is the reported malicious neighbor agents of i^{th}agent. Figure 7.2 shows the discrimination between the different time scales of the secondary, tertiary, and shadow updating rates. The tertiary controller and the secondary controllers update the control input every T and k time instances, respectively. The shadow updates occur every h time instance and/or every event

trigger instant t_q. To monitor the security of the system activity and reduce the communication burden with the cloud system, the shadow update is assumed to be $T \gg h > k$ during the normal periodic update.

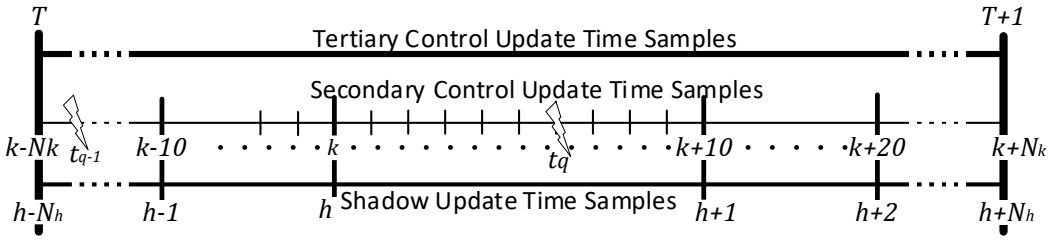


Figure 7.2: overall time-scales discrimination.

7.5 Luenberger Observer (LO) Based DT Constructor

Using the LO, multi-What-If scenarios are constructed and tested to authenticate the healthy desired control state. Given the linear system, which represents the dynamics of the CPS in (3.1)-(3.3), the LO is constructed firstly for the full healthy state as,

$$\left.\begin{aligned} \widehat{\mathcal{X}}_i(h+1) &= \Lambda\widehat{\mathcal{X}}_i(h) + \Gamma\mathcal{U}_i(h) + \ell_i(\mathcal{Y}_i(h) - \widehat{\mathcal{Y}}_i(h)) \\ \widehat{\mathcal{Y}}_i(k) &= \Upsilon\widehat{\mathcal{X}}_i(h) \end{aligned}\right\} \tag{7.9}$$

where $\widehat{\mathcal{X}}_i$ is the estimated state that is calculated according to the control input $\mathcal{U}_i$ and the measurement $\mathcal{Y}_i$. The LO is constructed by assigning the control input and the measured output based on the shadow states of the cyber and physical systems such that Λ and Υ are full ranked. According to the real-time CPS topology, the observer parameters Λ, Γ and Υ are built to represent the last shadow state. The LO gain ℓ_i is selected such that the eigenvalues of $(\Lambda - \ell\Upsilon)$ is stabilizable. During the normal healthy operation, the observer input is set to the desired state at the PCC $\mathcal{U}_i(h) = \mathcal{Z}_0(h)$ and the observer measured output is set to the reported shadow states $\mathcal{Y}_i(h) = \mathcal{Z}_i(h)$. Also, the observation error

$\left\|\mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h)\right\|_2^2$ is decaying to zero, where $\mathcal{O}_i = [\,\Upsilon_i, \Upsilon_i\,\Lambda, \ldots, \Upsilon_i\,\Lambda^{\mathfrak{t}-1}]^T$ is the block of the output parameter for the set of shadow states during time period $\mathfrak{t}$. The LO observer is rewritten as,

$$\left.\begin{array}{c} \widehat{\mathcal{X}}_i(h+1) = \widetilde{\Lambda}\widehat{\mathcal{X}}_i(h) + \tilde{\Gamma}\tilde{\mathcal{U}}_i(h) \\ \widetilde{\Lambda} = \Lambda - \ell_i\Upsilon_i \\ \tilde{\Gamma} = [\Gamma \quad \ell_i] \\ \tilde{\mathcal{U}}_i = [\mathcal{Z}_0 \quad \mathcal{Z}_i]^T \end{array}\right\} \tag{7.10}$$

If a set of the observed states are non-decaying to zero error, these states' indices are recorded in ϱ. Then, the LO is reconstructed to checking the satisfiability such that:

$$\lim_{h\to\infty} supp\left\|\mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h)\right\|_2^2 \leq TH \tag{7.11}$$

For constant TH, which is selected based on the composite noise from the cyber edge to the cloud. The observer gain ℓ_i is chosen such that $\widetilde{\Lambda}$ has the characteristic polynomial $d(s) = s^n + a_1 s^{n-1} + \cdots + a_n$ of the healthy case. To guarantee that condition, a linear coordination transformation of the observer parameter matrices is applied as proposition 2.3 in [122] as,

$$\begin{array}{c} \widetilde{\Lambda}^t = I_n \otimes \begin{bmatrix} -a_1 & -a_2 & \cdots & -a_{n-1} & -a_n \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \\ \tilde{\Gamma}^t = I_n \otimes [1 \quad 0 \quad \cdots \quad 0 \quad 0]^T \end{array} \tag{7.12}$$

The LO purpose is to estimate the suspicious data source of each set of shadow states. After that, the suspicious indices vectors are compared logically, which eventually defines the bad data source which will be discussed in Algorithm 1 and 2. The presence of the adversarial input ξ, the LO can be defined as follows,

$$\widehat{\mathcal{X}}_i(h+1) = \tilde{\Lambda}\widehat{\mathcal{X}}_i(h) + \tilde{\Gamma}\tilde{\mathcal{U}}_i(h) + \tilde{B}\xi(h) \tag{7.13}$$

which leads to the error dynamics can be derived from (7.3)-(7.4):

$$\dot{\tilde{\delta}}_i = \tilde{\Lambda}\tilde{\delta}_i + \tilde{B}\xi_i \tag{7.14}$$

The residual estimate that resulted from adversarial input is estimated as,

$$\pi_i(h) = \left\| \mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h) \right\|_2^2 - TH \tag{7.15}$$

Under an attack, $\pi_i(h)$ is non-decaying to zero according to Theorem 2 in [123].

7.6 Digital Twin Based Secured Control System

The developed cloud-based DT provides an end to end security audit solution for the ECPS even with multiple coordinated attack scenarios. The developed solution has two parts; the first one is implemented on the cyber edge and the second part is built as a function on the cloud. The following subsections discuss the two parts.

7.6.1 Digital Twin Cloud Algorithm

The physical, cyber and cyber-physical twin models are built as auxiliary functions as discussed in Section III. Algorithm 1 shows the DT algorithm that is implemented on the cloud. The DT models' functions are imported and the connection with IoT core and shadow services are launched. Then, the DT is constructed based on the LO by mapping the shadow states to the LO input vector. The system is assumed to be secure initially by setting $q = 0$. The DT loop starts by continuously estimating the ECPS full states. If a conflict between the shadow states and the estimated state is detected or a security audit is requested by a control agent, the authentication and auditing functions will be initiated at t_q. This function is discussed in Algorithm 2. The purpose of the function is to return the

secured observer and states, which are used to reconstruct the healthy model after the event $\Xi_{t_{q+1}}$. The healthy desired state is updated on the IoT shadow, which will be used later by the edge controllers.

To guarantee a healthy estimation of the desired control action and to discriminate between the healthy and the attacked state, Algorithm 2 is used. The shadow states $\mathcal{Z}_{t_q}$ and the conflicted agents ϱ_{t_q}that were determined in Algorithm 1 are utilized to define the malicious agents and their number ϱ and N_ϱ. Then, parallel DT observers will run by configuring the inputs with the malicious data sources $\tilde{\mathcal{U}}_\varrho$.

Algorithm 1 Digital Twin Algorithm on Cloud

Initialize DT model and import auxiliary functions
Connect to IoT Core and Shadow Service
Construct full state DT using LO such that:
$\tilde{u}_i = \begin{bmatrix} \mathcal{Z}_0 & \mathcal{Z}_s \end{bmatrix}^T$, $rk(\tilde{\Lambda})$ is full
Initialize security event function $q = 0$
while $True$ **do**
    Estimate the full state, $\hat{x}_i(h+1) = \tilde{\Lambda}\hat{x}_i(h) - \tilde{\Gamma}\tilde{u}_i(h)$
    if $\exists\ i$ s.t $|\mathcal{Z}_i(h) - \mathcal{O}_i\hat{x}_i(h)|_2^2 \leq TH \vee q \neq 0$ **then**
        Launch security authentication and audit function,
        $\Xi_{t_{q+1}}(\eta, \tilde{\Lambda}, \tilde{\Gamma}, \hat{x}) = AuthAudit\left(\mathcal{Z}_{t_q}, \varrho_{t_q}\right)$
        Reconstruct DT with the healthy model Ξ_{t_q-1}
    else
        Keep the full DT $\Xi_{t_{q+1}} = \Xi_{t_q}$
    Update $\mathcal{Z}_s^{desr}(h)$ ▷ update desired shadow → edge

For each malicious data source, the residues (7.15) is calculated, normalized and sorted ascendingly to choose the most suspicious data source indices $\mathcal{J}$. For each iteration, the indices $\mathcal{J}$, its Boolean representation Ω_ϱ and their estimated states $\tilde{x}_\mathcal{J}$ are stored. Finally, the indices of the confirmed attacked agents $\mathcal{F}$ are calculated as,

$$\mathcal{F} = supp\left[\bigwedge_{\varrho=1}^{N_\varrho} \Omega_\varrho\right] \tag{7.16}$$

and the equivalent secured LO is rebuilt using the healthy states η based on (7.12) to be returned to Algorithm 1.

Algorithm 2 AuthAudit $\left(\mathcal{Z}_{t_q}, \varrho_{t_q}\right)$

Input $\mathcal{Z}_i^{\Psi}(t_q), \mathcal{Z}_i^{\Theta}(t_q), \mathcal{Z}_i^{\varrho}(t_q)$ ▷ from IoT shadow
Define ϱ, N_ϱ and $\tilde{\mathcal{U}}_\varrho$ ▷ parallel DT observers
for $\varrho \in 1, 2, ..., N_\varrho$ **do**
    Construct DT for conflict case ϱ with $\tilde{\mathcal{U}}_\varrho$ such that,
    $rk(\tilde{\Lambda})$ is full
    Compute the residues for i^{th} shadow state,
    $\pi_i(t_q) = \left\| z_i(t_q) - \mathcal{O}_i \hat{\mathcal{X}}_i(t_q) \right\|_2^2 - TH$
    Normalize the residues, $\pi_i = \pi_i / \|\mathcal{O}_i\|_2^2$
    Sort the residues ascendingly, $\pi_{sort}\ \forall i$
    Choose maximum residues indexes,
    $\mathcal{J} = \text{Max}(\pi_{\text{sort}}).\text{Index}$
    Convert non-zero indices $\mathcal{J}$ into Boolean vector Ω_ϱ
    Store $\mathcal{J}$, Ω_ϱ and $\hat{\mathcal{X}}_{\mathcal{J}}$
Confirm the attacked agents/sensors indices,
$\mathcal{F} = \text{supp}\left[\Lambda_{\varrho=1}^{N_\varrho} \Omega_\varrho\right], \eta = \neg\mathcal{F}$
Transform $\tilde{\Lambda}, \tilde{\Gamma}$ according to η and (7.12)
Return $\eta, \tilde{\Lambda}, \tilde{\Gamma}, \hat{x}_\eta$

7.6.2 Resilient Distributed Control Algorithm

In the NMG, the leader nature is different as compared with the follower's nature. The attack on the leader can cause a complete disruption for the microgrid cluster. Therefore, the developed methodology in this work is to have a maximum security level by authenticating every incoming update from the PCC agent. However, the followers depend on their neighbors to estimate the control update and the isolation of the attacked follower

can retrofit the control system back to consensus. Consequently, one algorithm for the leaders and a different one for the followers are developed to guarantee the system security without increasing the system complexity or utilizing higher communication bandwidth.

7.6.2.1 Cluster's Leader agent algorithm

Algorithm 3 shows the secured control for the leader i^l of MG cluster. Firstly, the agent is initialized by assuming a secure state. The leader subscribes on edge for the main leader (PCC) state.

Algorithm 3 Cluster's Leader Resilient Control Algorithm

Initialize MG cluster's leader i^l agent, $x_{i^l}, \varrho_{i^l}, \omega_{0,i^l}$
$k = 0$
while $True$ **do**
    Receive PCC agent 0 state,
    $x_0(k)$ ▷ subscribe on edge
    if $(|\Delta x_0(k)| > 0) \vee (q = 1)$ **then**
        Control update event triggered,
        Receive desired shadow state,
        $\mathcal{Z}_{i^l}^{des} = \left\{\hat{x}^{des}(h), \mathcal{F}\right\}$ ▷ get IoT Shadow
        if $\left(x_0(k) \neq \hat{x}^{des}(h)\right) \vee (\mathcal{F} = PCC)$ **then**
            Declare PCC agent attacked and excluded,
            Cloud DT is tertiary controller,
            $x_{i^l}(k+1) = \hat{x}^{des}(h)$
        else
            PCC state accepted, $x_0(k)$
            $x_{i^l}(k+1) = x_0(k)$
        Send new state to neighbours,
        $x_{i^l}(k+1)$ ▷ publish to edge
        Send reported state, $\mathcal{Z}_{i^l}$ ▷ update IoT shadow
        Send secured state to i^l primary controller
    else
        No Update, $x_{i^l}(k+1) = x_{i^l}(k)$
    $k = k + 1$

If a change in the leader state or a security event is triggered, the desired shadow state x_{il}^{des} is received from the IoT shadow. Either the received PCC state from the edge does not match the DT desired or the DT already confirmed that agent 0 is attacked. The PCC is excluded and the DT on the cloud became a tertiary controller temporary by directly utilizing the DT estimated desired $x_{il} = \hat{x}^{des}$. If the PCC healthy, the edge update is accepted. Afterwards, the updated state is published to the edge, the cloud IoT shadow is updated, and the primary controller of this MG is actuated by this healthy control action.

7.6.2.2 Follower agent algorithm

Algorithm 4 is implemented on the follower agents. After initialization and receiving the neighbor's data from the edge, the update event is checked by watching if the neighbor's states change exceeds ϵ or the security event q is triggered. Then, The Kullback-Leibler divergence KL_i is used to check if the neighbors diverge from the consensus.

$$KL_i(x_j \parallel x_{j+1}) = \sum_{j \in n_i} x_j \,.\log\left(\frac{x_j}{x_{j+1}}\right) \tag{7.17}$$

where x_j and x_{j+1} are the neighbors of the follower agent i. An auditing request q will be activated if $KL_i > \aleph$. The desired estimated state by DT is received from the IoT shadow $\hat{x}^{des}$. A neighbor agent is marked as a malicious agent if it has the highest KL. Then, the shadow is updated by states $\mathcal{Z}_{if}^{\Psi}, \mathcal{Z}_{if}^{\Theta}$ and the candidate malicious index $\mathcal{Z}_{if}^{\varrho}$. The cloud DT feedback is received from Algorithm 1 and 2 that ensures the healthy desired state $\mathcal{Z}_{if}^{des}$. The adjacency matrix wights are modified according to $\mathcal{F}$. Finally, using the healthy state, the consensus is updated, and the secured final state is published to the edge and updated on the cloud IoT shadow.

Algorithm 4 Followers Resilient Control Algorithm

Initialize MG follower i^f agent, $x_{i^f}, \varrho_{i^f}, \omega_{i^f,j^f}$
$k = 0$
while $True$ **do**
    Receive $j^f h$ follower agent state,
    $x_j(k)\ \forall j = \{1, 2, ..., n_i\}, j \neq i$ ▷ subscribe on edge
    if $(|\Delta x_j(k)| > \epsilon) \vee (q = 1)$ **then**
        Control update event triggered,
        Estimate Kullback-Leibler divergence KL_i, (38)
        if $|KL_i| > \aleph$ **then**
            Malicious activity detected, DT audit request,
            $\widehat{\mathcal{X}}^{des}(h)$ ▷ get IoT Shadow
            Find diverged neighbours from desired $\widehat{\mathcal{X}}^{des}$
            Send reported state to the cloud,
            $\mathcal{Z}_{i^f} - \left\{\mathcal{Z}^{\Psi}_{i^f}, \mathcal{Z}^{\Theta}_{i^f}, \mathcal{Z}^{\varrho}_{i^f}\right\}$ ▷ update IoT shadow
            Receive the desired state and attacked agent,
            $\mathcal{Z}^{des}_{i^f} = \left\{\widehat{\mathcal{X}}^{des}(h), \mathcal{F}\right\}$ ▷ get IoT Shadow
            Exclude the attacked agent, $\omega_{i^f,\mathcal{F}} = 0$
        else
            Neighbours state $x_j(k)$ accepted, $\omega_{i^f,j^f} = 1$
        Information update until consensus
        Send new state to neighbours,
        $x_{i^f}(k+1)$ ▷ publish to edge
        Send reported state,$\mathcal{Z}_{i^f}$ ▷ update IoT shadow
        Send secured state to i^f primary controller
    else
        No Update, $x_{i^f}(k+1) - x_{i^f}(k)$
    $k = k + 1$

7.7 Practical Implementation on the DT Playground

The developed system is implemented practically by developing two main platforms. Locally, the distributed controllers are implemented on embedded single board computers. Remotely, cloud computing is implemented on AWS cloud vendor. We implemented an event-based callback function to trigger the data interaction based on the events. The cloud communication has higher latency compared to edge communication. Performance

analysis of the local DDS communication and the remote MQTT communication will be discussed in the next section. It is worth mentioning that the sampling rate of the edge control system and the shadow sampling rate are assumed to be $k = 0.2\ s$ and $h = 2\ s$, respectively. The thresholds are set as $\epsilon = 0.01$, $\aleph = 0.035$ and $TH = 0.05$.

Numerous components involved in the ECPS requires a flexible, reliable and integrated system that can deal with the IoT complexities. The cloud computing services cover these needs by including computing servers, databases, networking, analytics, intelligence over the internet. Figure 7.3 shows the functional block diagram of the implemented services.

7.7.1 AWS IoT core

The IoT Core is a cloud service that enables things to connect securely and interact with different cloud services and applications. Each thing is registered on the cloud. The IoT policy is created to control the access and allows/denies a predefined service to be accessed by the thing. Then, the created policies are attached to each thing's certificate. On the edge of the things, each sensor/controller is configured by attributing the generated keys and certificates to its device. One of the default settings in the thing policy is the access of the MQTT message broker to the thing. The MQTT communication protocol is used to interact (get and update) with the shadow of the things on the AWS cloud. The thing shadow is a JSON payload that is used to store and retrieve the things' last states.

The contents of the shadow file are shadow states, asset metadata, update version, client token and the timestamp of the last transaction. The shadow has two categories: the reported states $\mathcal{Z}_i$ and the desired states $\mathcal{Z}_i^{des}$. The metadata holds a tuple of the constant parameter of each microgrid as the power and voltage ratings, the location, the owner, and

the updated version. Also, one of the main IoT core components is the rule engine, which is the filters, that takes actions on the fly based on predefined rules. The actions can be activated by a cloud microservice function, which is the AWS Lambda function.

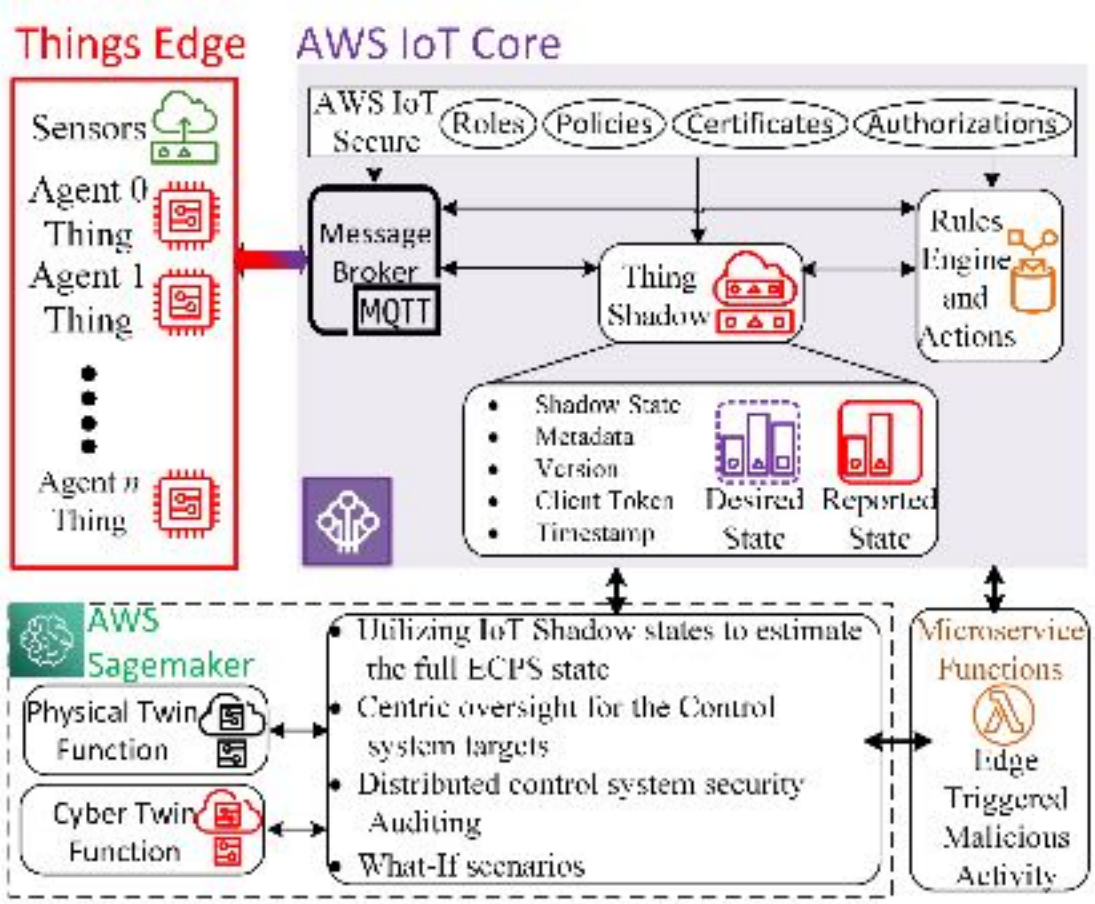


Figure 7.3: Digital Twin Description.

7.7.2 AWS Lambda function

The AWS *lambda*-Function is a service less computing function that can trigger a computing service in response to a detected event or a predefined logic/task. In this research effort, the security audit event q is managed by the lambda-function. Besides, it can update the tertiary control and management objective, launch a response to grid

ancillary service during a contingency, guide the secondary control layer or response to restoration request after a blackout.

7.7.3 AWS SageMaker

The AWS SageMaker is integrated and managed computing service. In this work, the physical twin, the cyber twin, and the hybrid ECPS models are implemented as functions to be imported by different tasks and applications. In addition to the centric oversight and security auditing applications, the SageMaker is used to guide the distributed controllers and runs what-if scenarios using LO based DT.

7.7.4 Attack Emulation

The false data injection attacks are artificially soft coded and is implemented on each controller to emulate the attacker. The attacked agent, attack vector, and the attack time instant are predefined according to the required emulation. For the attacks on the edge controllers, the artificial attack agent is can join the network, subscribe to data, and publish under the topic name of the infected real agent. Also, it has been designed to be able to publish/subscribe /to the cloud messages.

According to the required study, the attacker agents can be configured to launch an attack on the link between the infected agent and its neighbor(s). Also, the attacker agent is configured to mislead the cloud by reporting a healthy state to it while publishing faulty data to the edge. By the same emulator, the multi-coordinated attacks can be launched on multiple agents to degrade the consensus. This can be done by activating the soft-coded attacks on multiple agents simultaneously. The Denial of Service (DoS) attacks, network delay and packet loss emulation is implemented using network emulation software. In this

work, NETEM tool is utilized. The network corruption, the switched delay and the packet loss probability functions are used to implement the DoS, the delay, and the packet loss, respectively.

7.8 Results and Discussion

To validate the effectiveness of the developed technique, multiple scenarios are tested.

7.8.1 False Data Injection Attack

Figure 7.4 shows the first scenario of multiple coordinated attacks on the first cluster's leader (agent 1) and agent 4, at $k = 55$ and $k = 75$, respectively. The Figure 7.4(a) shows the states on the edge cyber system. The edge system detected a malicious activity, and the suspected agents were 1, 4 and 5. The left axis in Figure 7.4(b) shows the reported IoT shadow states and the desired state. On the right-hand axis of the second subplot, the attacked agents are depicted. Agent 5 has been temporarily declared as an attacked during $h = 3$ to 4 because of the delay produced by the algorithms' initialization. In addition, the divergence of Agent 5 away from the desired state at $h = 10$ to 12 is resulted from the attack on agent 4. The DT based authentication can find the new healthy desired state and confirm that Agents 1 and 4 are attacked. Therefore, even though Agent 5 has been subjected to delay and misleading, the agent succeeded to use the estimated healthy PCC desired state to retrofit its consensus dynamics by comparing both neighbors with the DT desired state and mitigate the attack by excluding Agent 4 from the cyber graph. As shown in Figure 7.4(c), The DT estimations for the injected power from each microgrid and the voltage at the PCC are very close to the actual simulation.

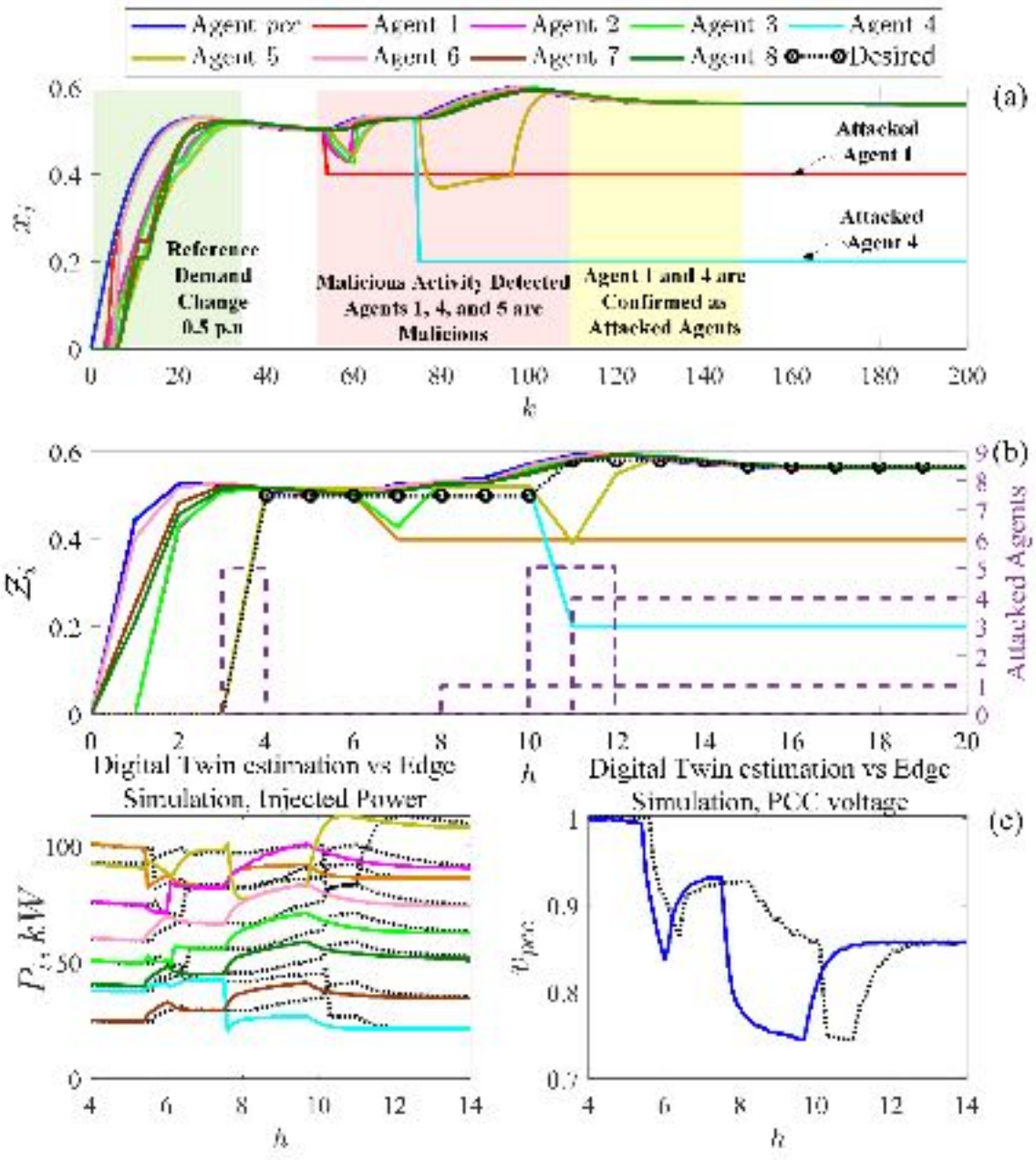


Figure 7.4: Response under the multiple attacks on agents 1 and 4 with mitigation.

Figure 7.5 shows the second scenario where Agent 4 is attacked by injecting $x_4 = 0.95$ instead of $x_{i,s.s} = 0.5$. However, the actual value of 0.5 was sent to the cloud to mislead the algorithm by reporting the healthy state. On the edge control system, the attack disturbed the consensus between $k = 75$ to 110. On the cloud, the DT succeeded to

calculate the healthy desired sharing factor state. Based on the ECPS twin model, the DT realized that the edge control system is attacked.

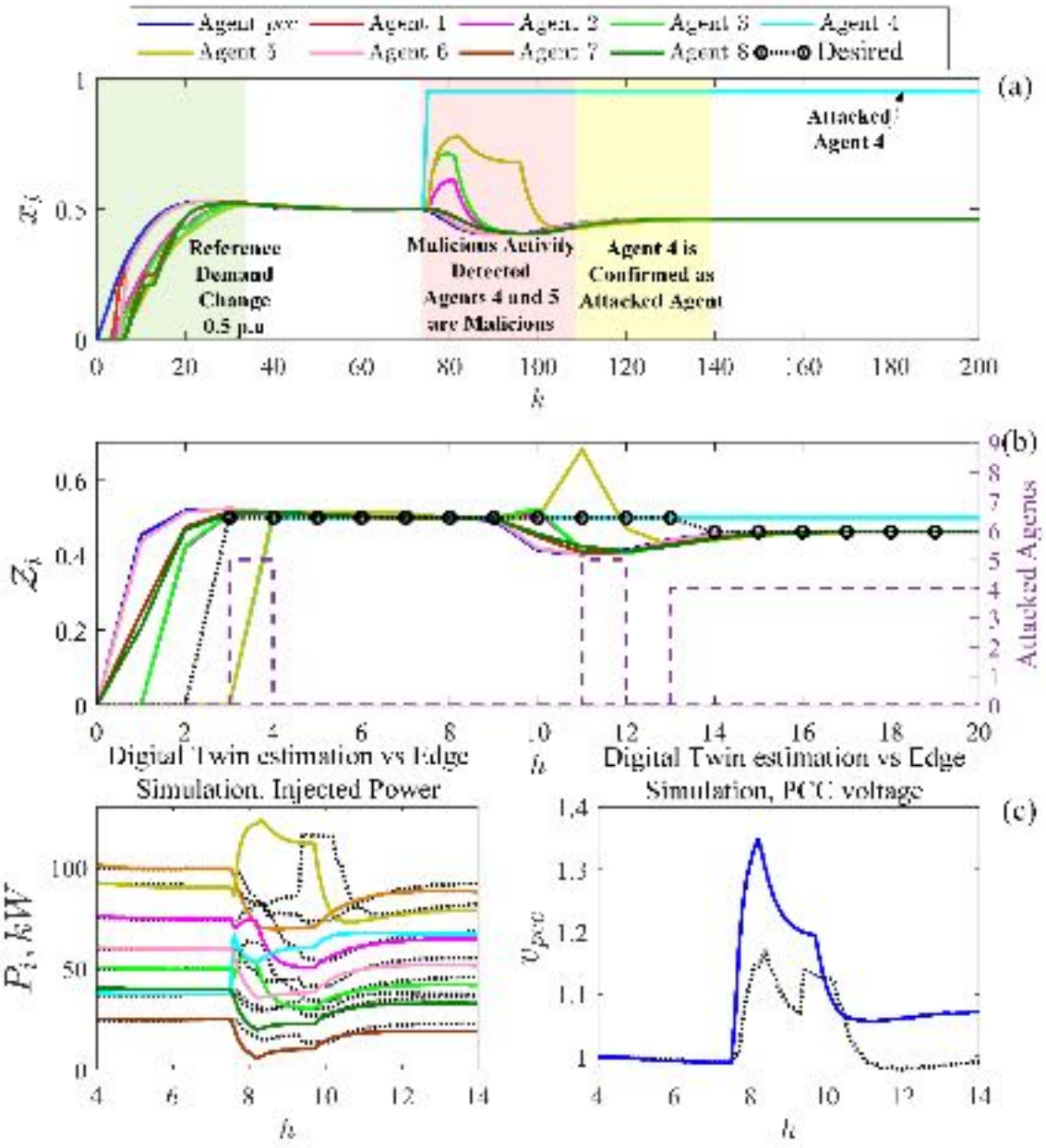


Figure 7.5: Response for the attack on agent 4 and cloud misleading with mitigation.

It authenticated that the PCC tertiary control shadow state and the PCC sensor state are matching. However, until this time, the DT suspected only Agent 5 (healthy agent).

Between $h = 12$ to 13, the DT could not know the attacked agent because Agent 4 is still misleading them by submitting the healthy state. On the other side, the security auditing algorithm is running. Both Agent 5 and 3 used the desired state and ensured that Agent 4 is attacked. Based on that reported malicious activity, the DT confirmed the attack regardless of the deception. Finally, the neighbor agents succeeded to isolate the attacked agent. The developed algorithm was able to discriminate between the healthy and the attacked agents even with multiple attacks and the cloud DT is misled.

Figure 7.6 depicts the summation of total residues of ECPS states for the LO based DT that running during the security audit analysis. The first scenario has higher residues as compared to scenario#2 because the malicious agents in scenario#1 are higher than scenario#2 and the execution time to decay to zero residues is higher in the first scenario.

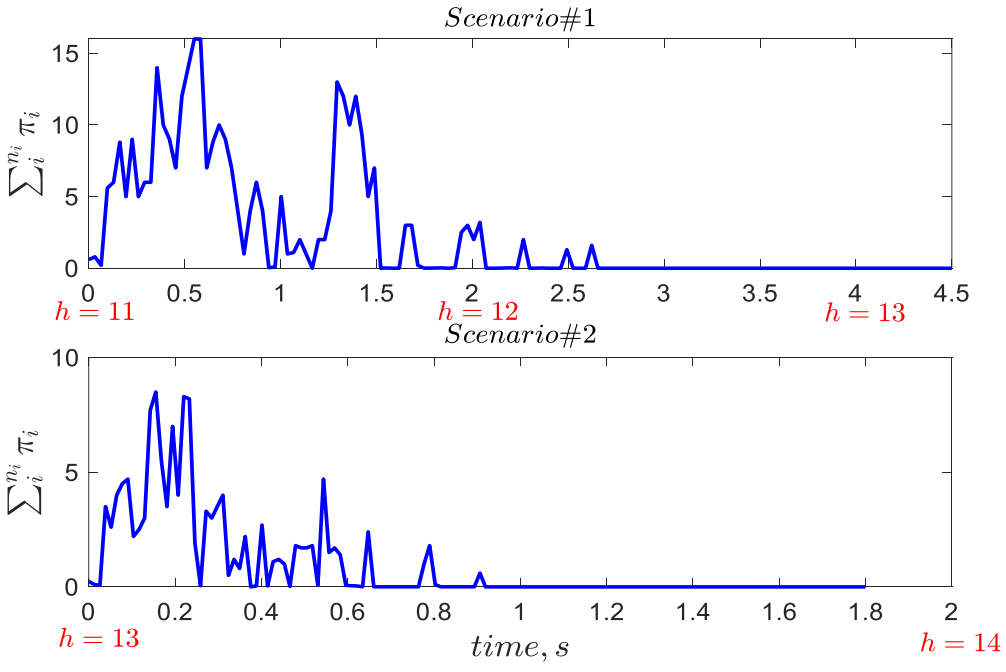


Figure 7.6: Total residues during DT based security audit for Scenarios 1 and 2.

7.8.2 Denial of Service Attack

Scenario # 3, DoS attack is tested on the communication link between the PCC and the leaders. The tertiary controller at PCC requested 40% increase in sharing power but this new command is intercepted by corrupting the communication between the PCC agent and the leaders (agent 1 and 6) as shown in Figure 7.7.

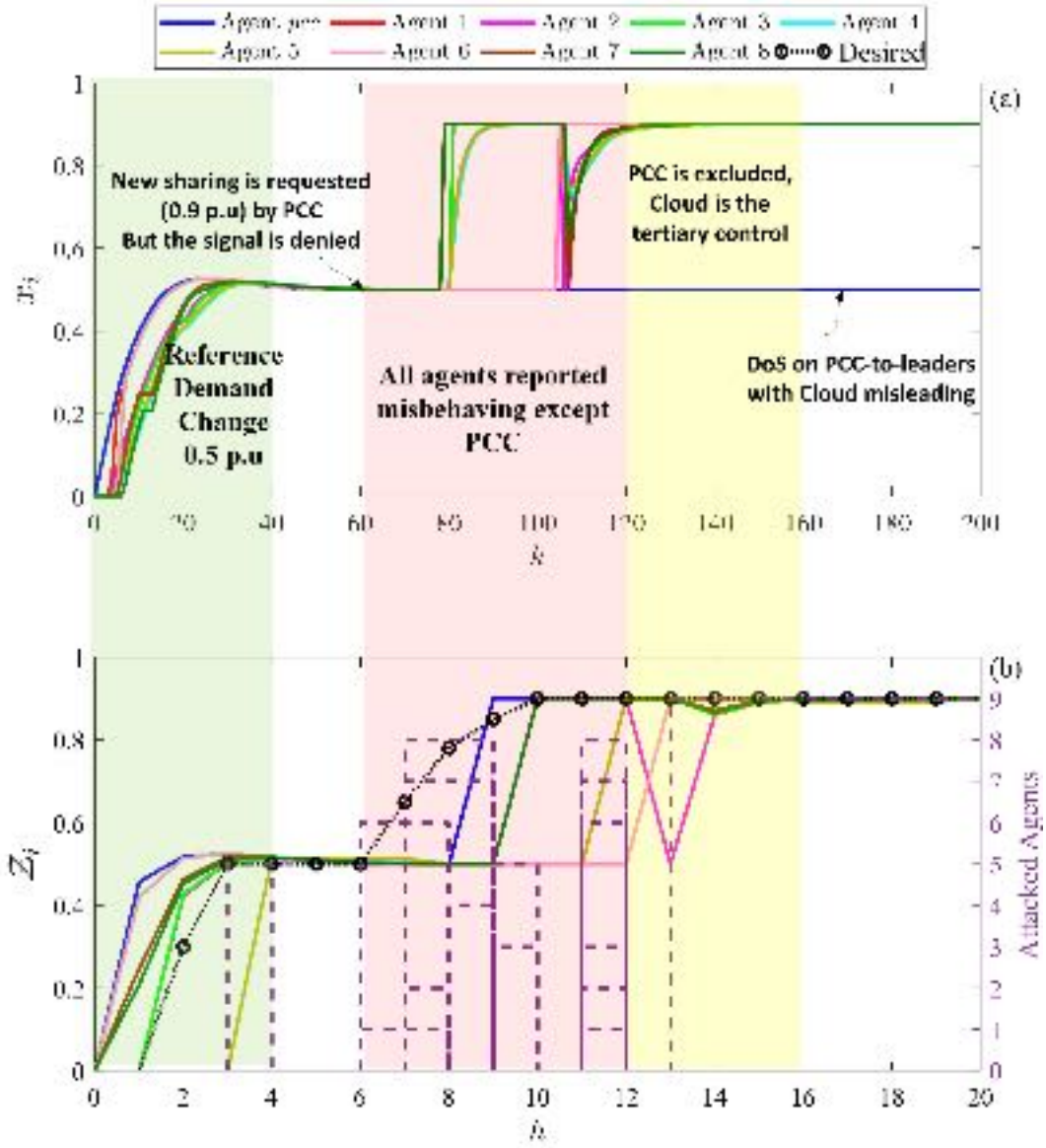


Figure 7.7: Response for DoS attack on link between the PCC and leader agents.

Primarily, all agents reported a malicious activity due to the difference between the DT shadow state and the edge state, which triggers the PCC authentication function (Algorithm 2). The LO based DT is reconstructed for the reported measurements. The DT observation is used to check the residuals and the healthy desired value is estimated according to Algorithm 1 and 2. Figure 7.7(b) shows the shadow of the sharing factors on the cloud and the detected malicious agents using the DT algorithms.

Almost all agents after the attack was a suspicious agent between h=6 and h=12 without a certain definition of the infected agent. However, at t=13 the DT algorithms were able to ensure that the PCC agent is the infected source of information. Finally, the developed platform succeeded to declare that the PCC-to-MG's leader communication links are attacked, and the cloud-based DT became the tertiary controller temporarily and all agents are retrofitted to the healthy state.

7.8.3 Communication Platform Performance

The performance of the communication platform is tested for both intra-edge communication (DDS) and edge-to-cloud communication (MQTT). The average intra-edge latency for all agents during previously discussed scenarios is shown in Figure 7.8. As shown, the maximum latency recorded in this test is $594\ \mu s$, which ensures the message delivery using DDS near to the real-time.

To estimate the edge-to-cloud communication delay, two events case study is demonstrated to measure the latency. As shown in Figure 7.9, the reference sharing factor changes from 0% to 50% at t=1s, then at t=21s the tertiary command is updated from 50% to 90%. Also, to test the effect of a large delay and packet loss on the performance, the

NETEM network emulation tool is used to emulate a delay and packet loss on published data from Agent 2 to both the edge and the cloud. The packet loss is emulated randomly during the whole test to be 5% and a 2s delay is added intentionally between t=24s and t=26s. Also, the test is made more challenging by setting the update reporting rate between the edge and the cloud to be one second only.

As illustrated in Figure 7.9(a), the edge controllers normally follow the leaders without any noticeable effect of the packet loss on the consensus. Although the 2s delay causes a slight disturbance in the consensus dynamics, the communication graph connectivity remains stable and achieved an agreement. Also, the same effect is reflected in the cloud shadow as shown in Figure 7.9(b).

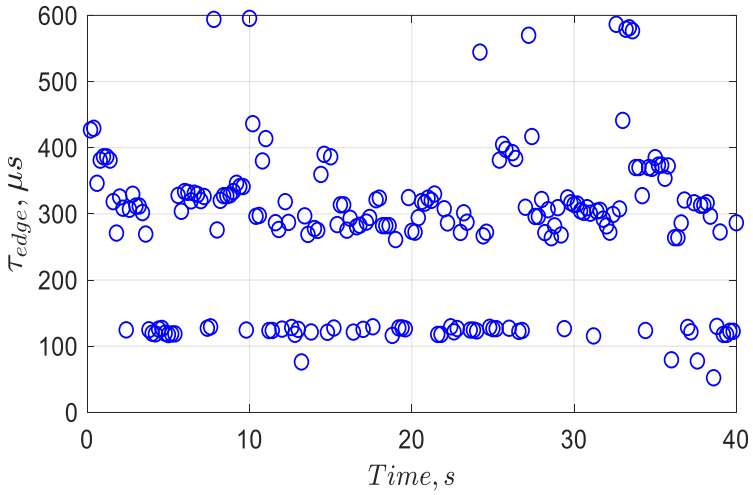


Figure 7.8: Average agent-to-agent time delay in the edge (DDS communication).

To precisely measure the delay between the edge and the cloud. The output data from Agent 2 is stamped by the departure time and the arrival time is stamped and collected on the cloud. The difference between the two timestamps is depicted in Figure 7.9(c) and

zoomed in Figure 7.9(d). Except for the 2s delay period, the measured delay between the edge and the cloud did not exceed 300 milliseconds.

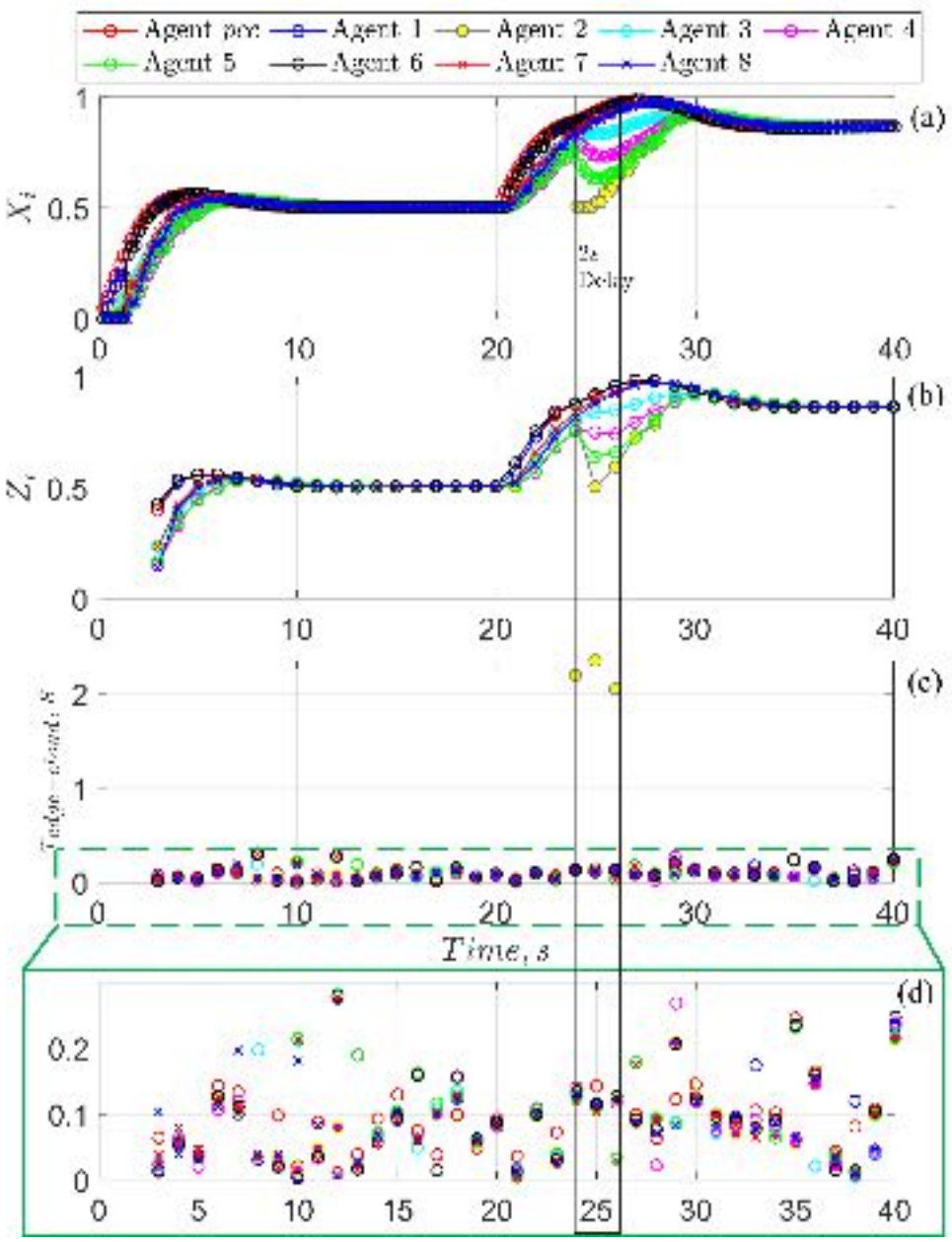


Figure 7.9: The performance under 2 s delay and 5% packet loss on the communication output from agent 2 to the edge and the cloud channels.

Another test is performed to study the effect of the message size, a 256 B JSON message is tested. The average and maximum recorded delay under the best QoS effort are shown in Table 7.1 for both DDS and MQTT middleware.

Table 7.1: Communication Performance Under Delay For 256 B Messages.

Middleware	Unicast/ Multicast	QoS	$\tau_{,av}$ (ms)	τ_{max} (ms)
Edge-edge, DDS	Unicast	Best effort	0.252	0.454
	Multicast	Best effort	0.275	0.622
Edge-cloud, MQTT	Unicast	Level 1	105	301

7.9 Summary

In this chapter, mathematical formulation, and implementation of an IoT based digital twin (DT) for the resiliency of interconnected microgrids was developed. The developed DT was validated using a practical setup of the distributed control system and Amazon Web Services (AWS). The developed framework was able to quickly detect and mitigate different kind of attacks such as false data injection, denial of service, and coordinated attacks. Future research of this work will consider the fusion of deep learning and LO to enhance the speed, accuracy, and predictability of the attacks.

Chapter 8 Security-Aware Distributed Control for Interconnected Nanogrid Resiliency

The reliable performance of the smart grid is a function of the configuration and cyber-physical nature of its constituting systems. Beside the centric oversight that is supported by the cloud layer by means of the digital twin, the distributed control system should be designed to respond to cyberattacks without the centric layer. In the previous chapter, the control system security is watched by a top layer, which depends on the healthy communication/provisioning of the ECPS in the cloud. If the communication failed, attacked or the cloud service is not available, the networked control layers should be aware of cybersecurity. Therefore, this work develops a secured distributed control framework for future smart grids. The work presents a distributed control framework that is secured by means of signal processing tools and consensus protocols. The work models the physical and cyber systems, showing the effect of the different types of cyber-attacks and their mitigation. The developed framework is based on the use of graph theory and consensus protocol to achieve a global control objective among the different agents in the system. Also, the developed algorithm is equipped by the mathematical morphology algorithm as a distributed security observer that is able to analyze the system behavior and detect and mitigate malicious actions. By comparing the dynamical characteristics of the cyber graph dynamics with the healthy states' dynamics, the attack can be detected, identified, and then isolated. The developed cyber-physical system and algorithm are modeled and implemented through MATLAB/Simulink. The results showed the ability of the developed algorithm in achieving the global power objective and voltage profiles while mitigating different kind of attacks.

8.1 Introduction

In recent years, the traditional AC grids become one of the main bottlenecks for expanding the expenditure of renewable resources. It has a rigid design with a complex centralized large-scale generation [124]–[126]. However, the DC grid architecture is expected to increase as an alternative technology to facilitate the integration of the distributed renewable resources in the power distribution networks. The DC distributed grid system can efficiently match renewable power fluctuation and improve peer-to-peer power transactions [125].

As a basic building block of the DC grid, the DC nanogrid can be defined as a local power distribution system, consisting of a single household or community building. In a nanogrid scale, the small-size distributed renewable energy resources can be penetrated easily because it faces less technical and regulatory barratries [126]. The up-scaling of the interconnected DC nanogrids is obtained by clustering the different nanogrids in the distribution system to accrue beneficial support to the grid and liquify the down-scale power markets. To efficiently control this interconnected system, the centralized control architecture is not only the simplest solution but also is a global objective aware system. Nonetheless, the centralized control networks require communication links with each nanogrid, which is hard to achieve in the wide-area geographical system as the distribution system. Besides, the large computational and communication burden is required to operate the overall distribution system [5], [84].

In light of the distributed control advantages, the networked control/management systems can work cooperatively to achieve the global control objective in a more reliable

and economical way. In distributed systems, the information is exchanged among the controllers to achieve the agreement on the control objective based on the consensus protocol. This cyber system has low cost, high reliability, less computational burden and requires only neighbor to neighbor communication [71], [79], [105], [127], [128]. In addition, it has been applied successfully in AC/DC microgrid and nanogrid applications [127]–[130]. Although the distributed networked control systems have many advantages, the two-way communication among the connected neighbors is vulnerable to cyber-attacks. Unlike the centralized control system, instead of concerning the security of a single central control unit, the distributed control blocks create multiple weak points, which requires high-cost security solution [131]–[134].

From the networked control system point of view, to control the future interconnected smart grid securely, many different control approaches are established to be security-aware as centralized, decentralized, and distributed control systems. The centralized control archives the best performance and easy to secure but it lacks scalability for further extensions [84]. The application of the distributed control in the small-scale power system has a very close performance as compared to the centralized control but it is more vulnerable to cyber-attacks [135]. Practically, the future applied energy echo systems will witness a complete transition to the distributed applications [129], controllers [136], ledgers [137] and algorithms [138], which impose a protentional security weakness in these distributed systems. Hence, the authors believe the distributed system security challenge should be addressed in future research work.

The cyber system is linked via a heterogeneous network, which uses the TCP/IP internet communication that provides the attacker with the capability to launch an attack. The data integrity attack on the distributed consensus protocol has been studied in the literature [14]–[16], [26], [132]–[134], [139]. In [14], a data integrity attack on the distributed energy management algorithm using local information is studied. The authors showed the importance of addressing renewable energy integration and protecting the distributed management system against possible cyber threats, simultaneously. In large-scale smart grid systems, a resilient distributed energy management technique is introduced in [15]. The developed technique protects the distributed economical dispatch management system against the unexpected attack on a generator. The authors developed a neighbor-watch-defense mechanism to detect, mitigate, isolate the misbehaving generator and update the control law to achieve the required global performance. Although the effectiveness of the developed solution, the detection methodology is very slow in defining the misbehaving generator. Consequently, the isolation and updating processes are made gradually, which provide the attacker with the ability to redesign the attack and deceive the protection system. In [16], an attack-resilient distributed control algorithm is introduced to protect the synchronization of the interconnected inverters. Even though the developed solution successfully protected the system against the attack, the solution is slow and can be affected by the communication graph topology. Therefore, the developed solution cannot satisfy the inverters synchronization and keep the proper voltage profile.

The power system transient stability in a smart grid is compromised by the denial of service attack and the communication latency in [26]. A framework based on the feedback

linearized control is illustrated to protect the system against these attacks, but the suggested framework did not consider the data integrity attack.

Motivated by the fact that the nanogrid is the basic building block of the future constructed smart grids, nanogrids are expected to be exposed to a higher level of cyber threats. Therefore, the nanogrid resiliency and security should receive extra attention. Unlike the previously discussed literature, the interconnected nanogrids control system should be designed by embedding the security solution inside the controllers. This will reduce the cost of cyber system encryption and authentication.

In this chapter, a novel integrated, fast and low-cost secure controller is introduced to achieve a resilient distributed control objective. The developed solution is designed to capture the cyber system dynamical features using the real-time morphological analysis to detect the attack. Unlike the previous techniques, the introduced methodology can discriminate between the normal change in control law (cyber system behavior) and the malicious control agent (attacker behavior). The mathematical morphology method is utilized to discover the change in the features of the transmitted data from the neighbor agents and discard the infected agent from the graph. The cyber system graph adjacency matrix is updated to update the consensus protocol agreement and correct the control system objective.

The developed control system is designed to guarantee proper power-sharing among the interconnected nanogrids while supporting the ancillary service. In addition, the secondary and the tertiary control levels aim at keeping the system voltage profile within the limits during the normal operation and in the presence of cyber-threats.

8.2 Interconnected Nanogrid CPS Description

In this work, the nanogrid system contains household load appliances, renewable PV system, and BSS. The household has local control agent, which dispatches the photovoltaic energy to satisfy the nanogrid load and manage the BSS to wisely charge/discharge according to the customer preference, energy price, and the available renewable power. The two-way communication interface is used between the control agent and the local components to exchange the information and the internal control decisions. In addition, a peer-to-peer connection between each interconnected household cooperatively coordinate the energy dispatch among the nanogrids. The interconnected DC nanogrids system, described as a cyber-physical system, is illustrated in Figure 8.1.

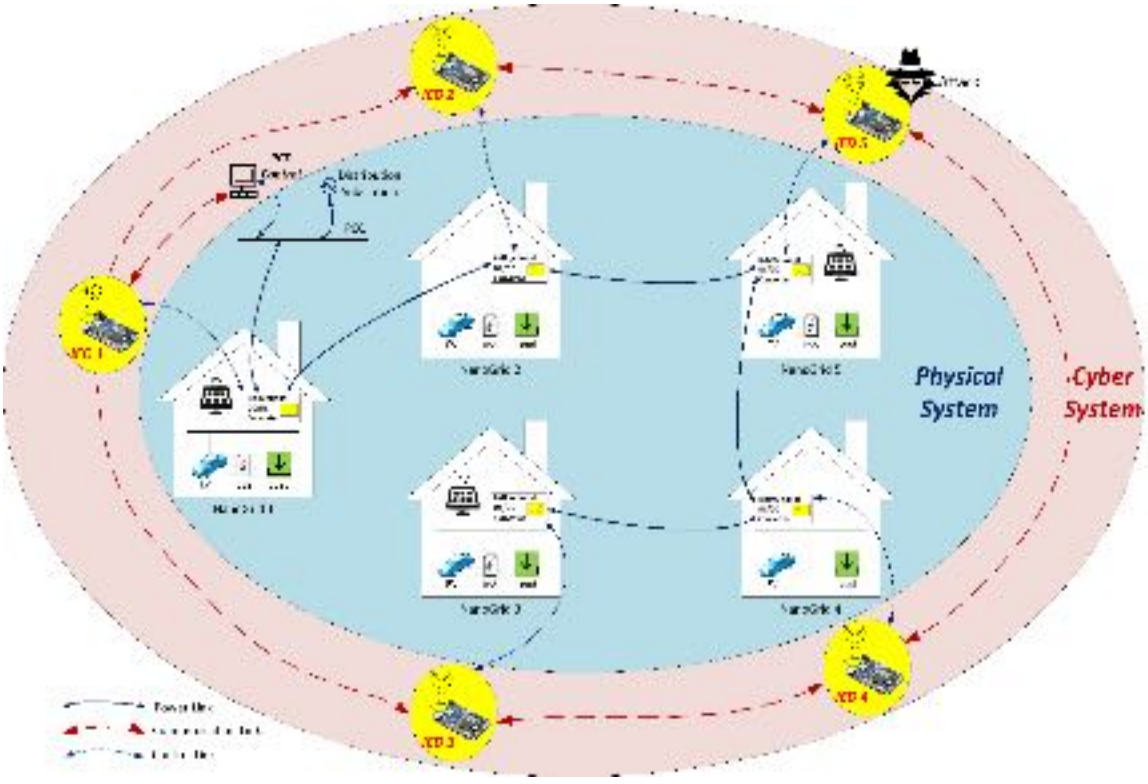


Figure 8.1: Interconnected DC Nanogrid cyber-physical system.

As shown in Figure 8.1, the physical system contains interconnected DC nanogrids. Each nanogrid is represented by a DC bus, which links the nanogrid demand, PV system, BSS and EV charging slot. The bi-directional DC/DC converter is utilized to interconnect each DC nanogrid and its neighbors. The nanogrids interconnection can be flexibly configured to modify the topology of the DC distribution system to reroute the power between nanogrids to achieve certain operation. The overall distributed DC system is connected to the main distribution substation via the point of common coupling (PCC).

The cyber system consists of IED based controllers, which cooperatively control a cluster of nanogrids by controlling the DC/DC coupling converters. The cyber system has a set of peer-to-peer communication links to share the information. The distributed control system utilizes the communication network to achieve certain control law, which is assigned by the PCC control center. In this system, the PCC control center requests certain transmitted power without violating the PCC voltage limits.

The power-sharing of each nanogrid is defined based on the market price and real-time customer preferences. However, if the purpose of the nanogrid operation is equal power sharing, the control agents should supportively achieve the transmitted power set-point sent by the PCC control. Typically, each nanogrid has its own power rating or power availability. To achieve proper equal power-sharing, each nanogrid contributes by a power amount that is proportional to its power rating. Therefore, the PCC defines certain sharing factor and sends to a pre-selected leader control agent. The follower control agents should follow the leader to achieve consensus according to the sharing factor.

In this system, the heterogeneous communication network is highly vulnerable to cyber-attacks due to the low-security level in the distribution system. An attacker can manipulate the data with the neighbors to threaten the overall system control objective or deactivate the system functionalities.

8.3 Interconnected DC Nanogrid Architecture

The considered nanogrid integrates the DERs and loads into a single LVDC bus. The distributed nanogrids are linked via a bi-directional DC/DC converter to a MVDC distribution bus. Figure 8.2 shows the system architecture with the primary, secondary, and tertiary control systems. The nanogrid physical system is modeled as a Thevenin equivalent circuit connected to the tie-converter and coupled with the distribution line. The primary control system contains current and voltage control loops, which drive the converter according to the reference voltage $V_{ngi,ref}$, which is generated from the secondary control system. The secondary control system works to provide a safe local voltage level and maintain the power control objective r_i^*, from the tertiary control level. This level defines the interaction between the interconnected nanogrids cluster and the utility grid for optimizing the energy utilization and providing the ancillary service.

8.3.1 Interconnected DC Nanogrids Physical Dynamics

In light of the power system modeling, the DC distribution system is considered as an interconnected multi-converter system, which has multiple coupled state variables. As shown in Figure 8.2, the system can be modeled in terms of the following differential equations. Suppose a DC system has a single main PCC bus with a voltage V_{dc}, n converters interconnected by segmented two-wire DC distribution lines l.

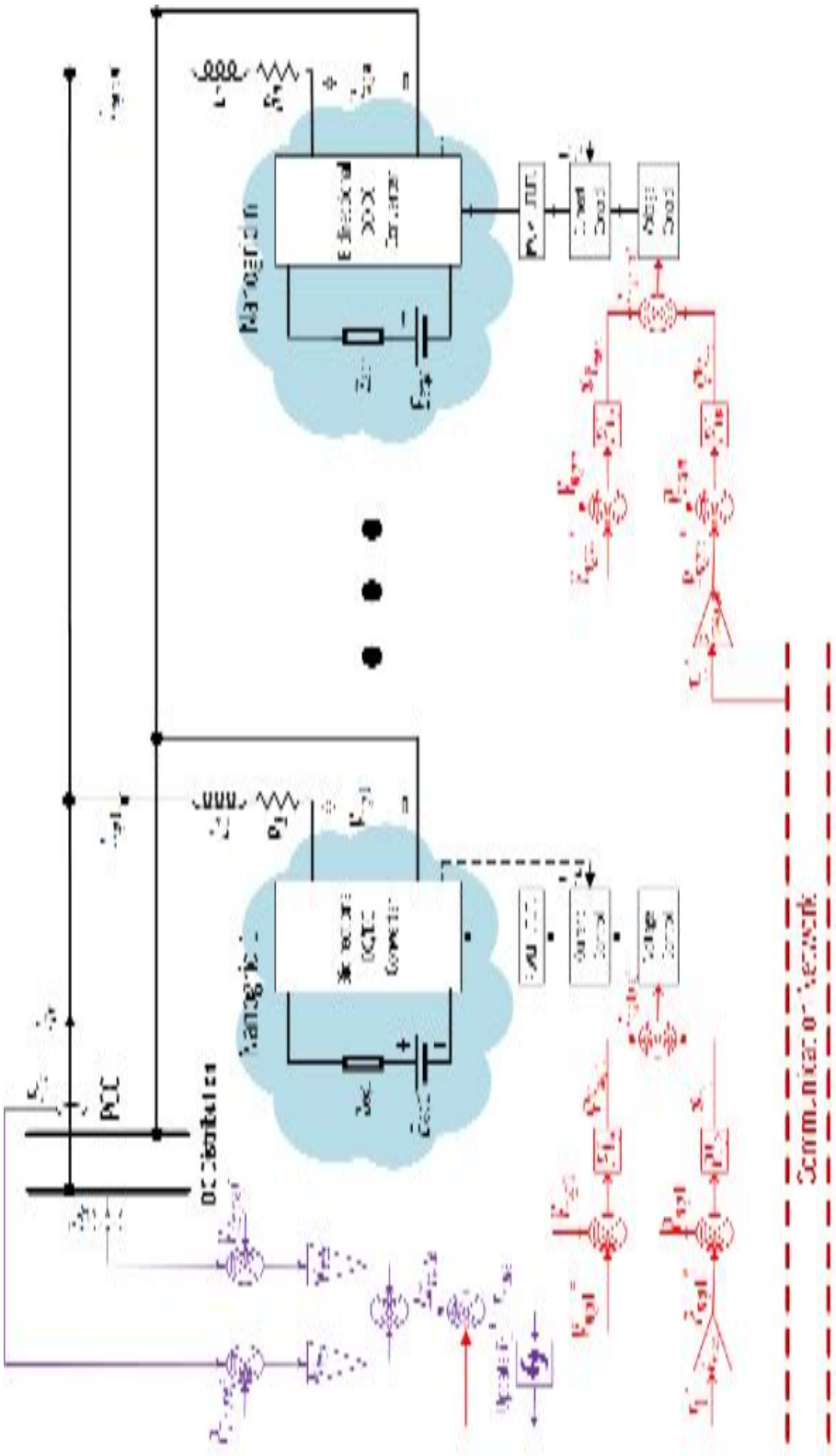


Figure 8.2: Distributed DC Nanogrid architecture.

$$\frac{dV_{dc}}{dt} = \frac{1}{C}\left(I_{Tr} - \sum_{i=1}^{n} I_{ngi}\right) \tag{8.1}$$

$$\frac{dI_{ngi}}{dt} = \frac{1}{L_i}\left(V_{dc} - \Delta V_l - R_i I_{ngi} - V_{ngi}\right) \tag{8.2}$$

$$\frac{dI_l}{dt} = \frac{1}{L_l}(\Delta V_l - R_l I_l) \tag{8.3}$$

$$P_{loss} = \sum_{i=1}^{n} R_i {I_{ngi}}^2 + \sum_{l=1}^{m} R_l {I_l}^2 \tag{8.4}$$

8.3.2 Cyber Communication System Dynamics

The communication cyber system is implemented based on the graph theory and the consensus algorithm works to share the information and averaging among the distributed agents. The consensus agreement problem finds its origins in the computer science area. The main purpose of the consensus protocol is to allow distributed agents to reach an agreement on an average value or a certain quantity of interest by exchanging information. Graph Laplacians matrix describes the underlying communication system based on the graph theory basics.

The communication network between the control agents can be characterized by a directed graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ consists of nodes $\mathcal{V}$ and a set of directed edges $\mathcal{E}$. The graph has adjacency matrix $A = [a_{ij}]$, which represents the interaction between the nodes set and the edges set. The matrix has a dimension $(n + 1) \times (n + 1)$.

$$[A] = \begin{cases} 1 & if \ \ i \longrightarrow j \quad \in \mathcal{E} \\ 0 & otherwise \end{cases} \tag{8.5}$$

In the directed graph, the notation *degree* divided into the *In-degree* and *Out-degree* and the mathematical definition of the *in-neighbors* of node i is represented as $D = diag\{d_{ij}\}$.

According to the consensus protocol, the Laplacian matrix $\mathcal{L}$ is utilized to solve the agreement problem and it can be calculated as follows,

$$\mathcal{L} = D - A. \tag{8.6}$$

In the cooperated multi-agent control system, a certain agent is chosen to be the control node q to ensure the local voting protocol. The node q is called the leader and it represents the node that has a reachable path to all other nodes (followers). Each node has an associated state x_i and it can be represented as the following control law $u_i = \dot{x}_i$.

$$\dot{x}_i = \sum_{j \in n} a_{ij}(x_j - x_i) + b_i(q - x_i) \tag{8.7}$$

$$\dot{\boldsymbol{x}} = -(\boldsymbol{\mathcal{L}} + \boldsymbol{B}).\boldsymbol{x} + \boldsymbol{B}\underline{\boldsymbol{1}}\boldsymbol{q} \tag{8.8}$$

where $B = diag\{b_i\}$ represents the pinning matrix and b_i is the weights of the edge between the leader and the upper control level.

8.3.3 Secondary Control System

The coordination of the DER can be realized through nanogrid, which represent the smallest cell in the power system. While the primary control system provides the voltage stability, the distributed secondary control reacts with the load changes and ESS management to enable aggregated renewable resources integration in the distribution grid. The distributed control objective is developed to track the required reference power that is injected at the PCC and to maintain the voltage of the DC bus. In the secondary control level, the control has two objects; the first one is the local objective $\varphi_{V_{ngi}}$and it keeps the coupling DC/DC bi-directional converter output voltage at a proper value. The second objective φ_{r_i} is a global interconnected nanogrids cluster objective that satisfies the

appropriate relative power sharing among the nanogrids. The essential control variable in the secondary control system is the sharing factor $r_i{}^*$, which is calculated as $r_i{}^* = P_{ngi}/P_{ngi,max}$. As shown in Figure 8.2, the secondary control for an agent i is represented as,

$$V_{ngi,ref} = \varphi_{V_{ngi}} + \varphi_{r_i} \tag{8.9}$$

$$\varphi_{V_{ngi}} = k_p^{V_{ng}}\left(V_{ngi}^* - V_{ngi}\right) + k_I^{V_{ng}} \int \left(V_{ngi}^* - V_{ngi}\right) dt \tag{8.10}$$

$$\varphi_{r_i} = k_p^P\left(r_i^* P_{ngi,max} - P_{ngi}\right) + k_I^P \int \left(r_i^* P_{ngi,max} - P_{ngi}\right) dt \tag{8.11}$$

The sharing factor is calculated at the PCC control center and propagates according to the consensus agreement protocol as follows,

$$\Delta r_{rule} = k_{Ptr}\left(P_{Tr,ref} - P_{Tr}\right) + k_{Vdc}\left(V_{dc,ref} - V_{dc}\right) \tag{8.12}$$

The leader (agent 1) control input is updated by Δr_{rule} and is calculated in another formulation (8.13). As depicted in Figure 8.2, the update block keeps posting the control law according to the leader state feedback and the PCC tertiary controller as follows:

$$r_{rule}^*(k+1) = r_{rule}^*(0) + \Delta r_{rule}(k) \tag{8.13}$$

where $r_{rule}^*(0)$ is the r_{rule}^* initial condition. The followers consequently follow the leader by the communication network dynamics that is discussed previously according to the following auxiliary control input. The following equations are special forms of the general forms in (8.7)-(8.8). In addition, this control input should satisfy the constraints as follows,

$$P_{ngi,min} \le P_{ngi} \le P_{ngi,max}, \sum_i P_{ngi} - P_{loss} = P_{Tr}, \tag{8.14}$$

$$\dot{r}_i = \sum_{j \in n} a_{ij}(r_j - r_i) + b_i(r_{rule} - r_i) \tag{8.15}$$

$$\boldsymbol{u} = -(\boldsymbol{\mathcal{L}} + \boldsymbol{B}).\boldsymbol{r} + \boldsymbol{B}\underline{\boldsymbol{1}} r_{rule} \tag{8.16}$$

8.4 Cyber-Attack Adversarial Model

The communication link in the networked control systems is vulnerable to different cyber-attacks. The attacker can intentionally modify the transmitted data between the distributed control agents, which cause failure in the required control objective. The attacker may also disturb the sensor, actuator, communication link or controller. The threats can be classified into many types, such as the denial of service, replay attack, stealthy attack, etc. Those types are mainly categorized into two adversaries which are: blocking the update of the transmitted data or injecting false data.

The distributed secondary control system is restricted by the regulation of sharing healthy information with neighbors. The following assumptions are made on the adversary attack capabilities:

Assumption 1. An attacker needs only to acquire the local information to launch an attack.

The above assumption shows the ability of an agent, with local information knowledge, to launch an effective attack in the developed distributed control system. Bad data detection technique can be applied in a centralized control system rather than the distributed control system, which makes the distributed control network more disposed to the attackers [140]. The attacker model can analyze the impact of different data injections to cause an infeasible solution for the control objective.

Assumption 2. An attacker who has a knowledge of the control system, consensus protocol, network topology, and power-sharing limits can mislead the controllers by injecting well-studied false data.

This assumption illustrates the influence of an attacker with good knowledge about the overall system dynamics. The control objective can be manipulated to target the optimal power-sharing dispatch for economic benefits and/or technical misbehaving. For instance, certain nanogrid can be attacked to decrease the power drawn from neighbors nanogrids to increase its own sharing factor to gain more financial profits. If the attacker is the owner and needs to maximize his profit, he can tamper physically with the shared power by reducing the output and increasing the sharing factor intentionally. Another manipulation can be done during the normal transient consensus process by launching a replay attack on a certain operating point or replaying a previous period of step-change response.

Assumption 3. The leader agent has a high-security level and the attacker cannot attack the leader.

Practically, the leader agent, which is directly connected to the PCC, should be protected by a higher cost security system using encryption and authentication [15]. In addition, this is the only agent that knows the actual control rule. If the attacker gets access to the leader agent, the entire nanogrids clusters must be disconnected from or stop injecting power to the PCC.

Assumption 4. After isolating the infected agents, the rest of the agents can support the control objective without violating the load balance in a single cluster.

Running a coordinated attack on a single nanogrids cluster can cause severe consequences. The reason is the consensus protocol depends on a cooperative role of all agents to support the control objective. If the attacker gets the reachability to manipulate with a sufficient number of agents at the same time, the isolation procedures can lead to the non-functional cluster.

Figure 8.3 illustrates the block diagram of the consensus protocol dynamics under attack. The block diagram represents the control law in (8.16) under two categories of attacks. In the graph topology, the node dynamics are represented as the summation of weighted neighbor's data r_j. The controlled node (leader) connection can be activated by the diagonal b_i. The cyber-attack is represented by the discrete signal θ_a, which represents data updates blocking. In addition, the input u_a models the false data injection and its effect can be controlled by the gain k_a.

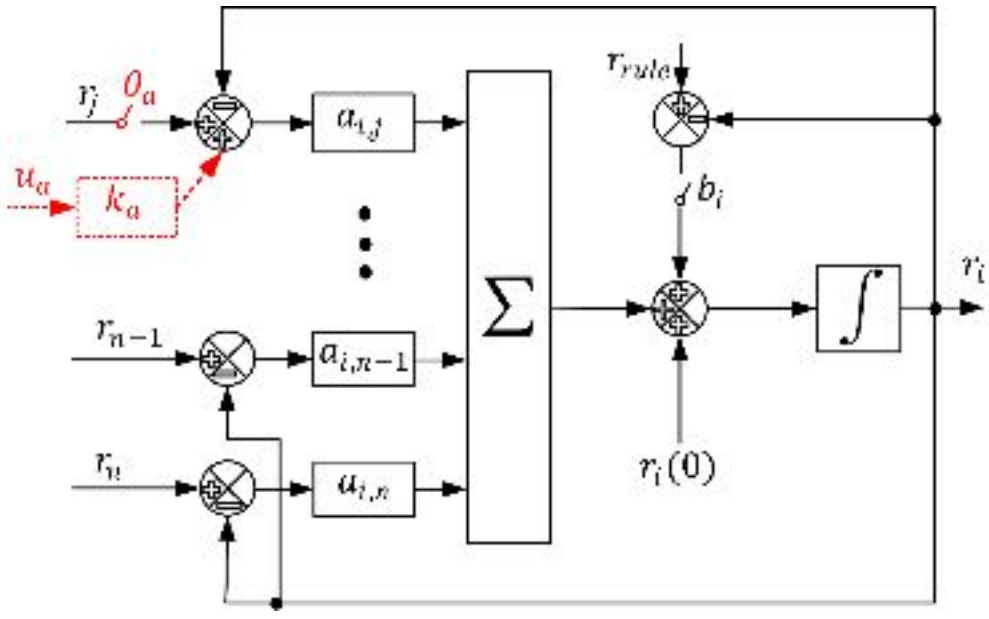


Figure 8.3: Consensus protocol under attack.

As shown in the figure, the attack is a malicious external activity, which can compromise the consensus agreement and consequently impose a deficit in the control objective. The controlled consensus is designed to make the node state r_i track the leader q and cooperatively converge to r_{rule}. Let $b_i \neq 0$, then $(\boldsymbol{\mathcal{L}} + \boldsymbol{B})$ is non-singular with positive eigenvalues $\boldsymbol{\lambda}$ and $-(\boldsymbol{\mathcal{L}} + \boldsymbol{B})$ is asymptotically stable. Therefore, the dynamical consensus response can be derived by solving the first-order differential equation (8.16) as follows,

$$\boldsymbol{r(t)} = \boldsymbol{r(0)}.\boldsymbol{e}^{-(\boldsymbol{L}+\boldsymbol{B})\boldsymbol{t}} + r_{rule} \tag{8.17}$$

If a node i is attacked by attack vector $U_a = \theta_a + k_a u_a$ at time t_a, the dynamical feature of the infected node changes by ψ and the new solution with the attack effect is represented as follows,

$$\boldsymbol{r(t)} = \boldsymbol{r(0)}.\boldsymbol{e}^{(-(\boldsymbol{L}+\boldsymbol{B})+\boldsymbol{\psi})\boldsymbol{t}} + r_{rule} + \boldsymbol{U_a(t)} \tag{8.18}$$

It worth mentioning that the infected node change (ψ) affects the nodes differently, which diverge the consensus and lead to a disagreement about the steady state. The effective control input law under attack and its dynamics can be formulated as follows,

$$\widetilde{u_i} = u_i + \theta_a + k_a u_a \tag{8.19}$$

$$\dot{\widetilde{u_i}} = \ddot{r_i} + \dot{\theta_a} + k_a \dot{u_a} \tag{8.20}$$

where the dynamical behavior of the graph topology is defined as $\ddot{r_i} = \dot{u_i}$, the attack dynamical behaviour is represented in terms of $\dot{\theta_a}$ and $\dot{u_a}$. By suppressing the steady-state

fundamental component in the neighbour signal and enhancing the dynamical change, the change in the graph feature (ψ) can be detected. Consequently, the difference between the original graph dynamics and the attacked dynamics can be the key element to detect, identify and mitigate the suspicious agent.

8.5 Morphological Features Based Resilient Distributed Control System

The developed defense model mechanism is based on the ad-hoc network security protocol, which is conceptionally digested as neighbor watching [139]. The cyber-attack detection is based on the distributed observer, which is embedded in each controller and is responsible for analyzing the neighbor's signals to discriminate between the healthy and faulty data.

After detecting and identifying the infected node, the controller can apply the defense mechanism by excluding this node from the graph adjacency matrix. In this case, the developed defense model converts the traditional distributed controller into a security-aware controller. To make the controller aware of the healthy data, each agent must know the features of the graph. In addition, the setting of the false data detection threshold is identified based on the dynamical behavior, which is related to the maximum transmitted power step response.

The attack detection is based on the dynamical relation of the transmitted data, which means that the in-neighbors data at a certain node should always be coherent. Suppose a compromised edge $(i, j) \in \mathcal{E}$ and the attacker modifies r_{ij} to $\widetilde{r_{ij}}$. According to (8.19)-(8.20), the dynamical feature of the neighboring data can be used as a detection condition $\dot{r_{ij}} \neq \dot{\widetilde{r_{ij}}}$. The change in the dynamical feature with time is the key rule of the

discrimination between healthy and malicious data. The following subsection shows the developed technique to capture the change in dynamical features based on the morphological features of the graph algebraic behavior.

8.5.1 Mathematical Morphology

Mathematical morphology is a signal processing technique, which depends on the mathematical set theory to define the shapes. One of the major applications of the MM is image processing. MM can deal with the shape of the signals in the grey-scale.

The MM key advantage is the ability to analyze non-linear signal dynamics without linearization, which increase the accuracy of the extracted features [141]–[143].

The main mathematical operators of the MM are the dilation and the erosion processes. Those two operators extract the signal features via the interaction between the analyzed signal set f and a smaller probing set g, which is called the structuring element. The SE is pre-defined according to prior knowledge of the signal characteristics [144].

There are many shapes of the SE (as line, circle, disc, square etc.). In the application of signal processing, the flat line is utilized. In addition, the line size is selected based on the sampling time and the required degree of the extracted features.

The dilation operation is defined as the expanding of the signal shape by the SE. Conversely, the erosion operator is defined as the shrinking of the proceeded signal by the same SE. Mathematically, the dilation and the erosion operators of the signal f by the SE g that lies in the domains D_f, D_g are formulated as follow,

$$(f \oplus g)(k) = max\left\{f(k+s) + g(s) | (k+s) \in D_f, s \in D_g\right\} \quad (8.21)$$

$$(f \ominus g)(k) = min\left\{f(k+s) + g(s) | (k+s) \in D_f, s \in D_g\right\} \quad (8.22)$$

8.5.2 MM based Cyber-attack detection

The leader state $r^*(k)$ is required to traverse through the directed graph network. Consider an agent j receives the state $r_i(k)$ from a neighbor agent i. The distributed observer in the agent's controller j applies the MM analysis to extract the morphological key feature $\nabla^w_{mmg,i}(k)$ using a flat structuring element (SE) g. The morphological gradient ∇_{mmg} is defined as the arithmetic difference between the dilated and the eroded signal. The morphological gradient can be repeated sequentially in a multi-resolution manner to increase the strength of the extracted features. The multi-resolution morphological gradient in w^{th} level can be formulated as follows,

$$\nabla^w_{mmg} = (f \oplus g)^w - (f \ominus g)^w \quad (8.23)$$

The digital processing implementation of the MMG, which is calculated as stated previously in (8.21)-(8.23) is depicted in Figure 8.4. The distributed observer in this figure applies the minimum and maximum operation on a set of buffed samples to calculate the dilation and erosion operations, respectively.

The real-time difference between those operations represents the first level of MMG. Then, a smaller set of the observed signal is proceeded by the same technique to generate the second level, which represents the dynamical key features of the cyber-system.

As stated by (8.18)-(8.20), the attack can be detected if the extracted dynamics of the transmitted data is changed compared to the normal graph dynamics. Therefore, the attack is detected when the following condition holds.

$$\left|\nabla^{w}_{mmg}\right| \geq \rho \qquad \forall\, t \geq 0, \rho \in \mathbb{R}^{+} \tag{8.24}$$

Due to the nature of the morphological gradient that works to suppress the minor fundamental feature and enhance the key features, the resulted response is very close to zero. Therefore, the threshold ρ is estimated empirically by trial and error. The second resolution level of the morphological gradient $w = 2$ is sufficient to clearly discriminate between the attack dynamics and the maximum change in the transmitted power set point $P_{Tr,ref}$.

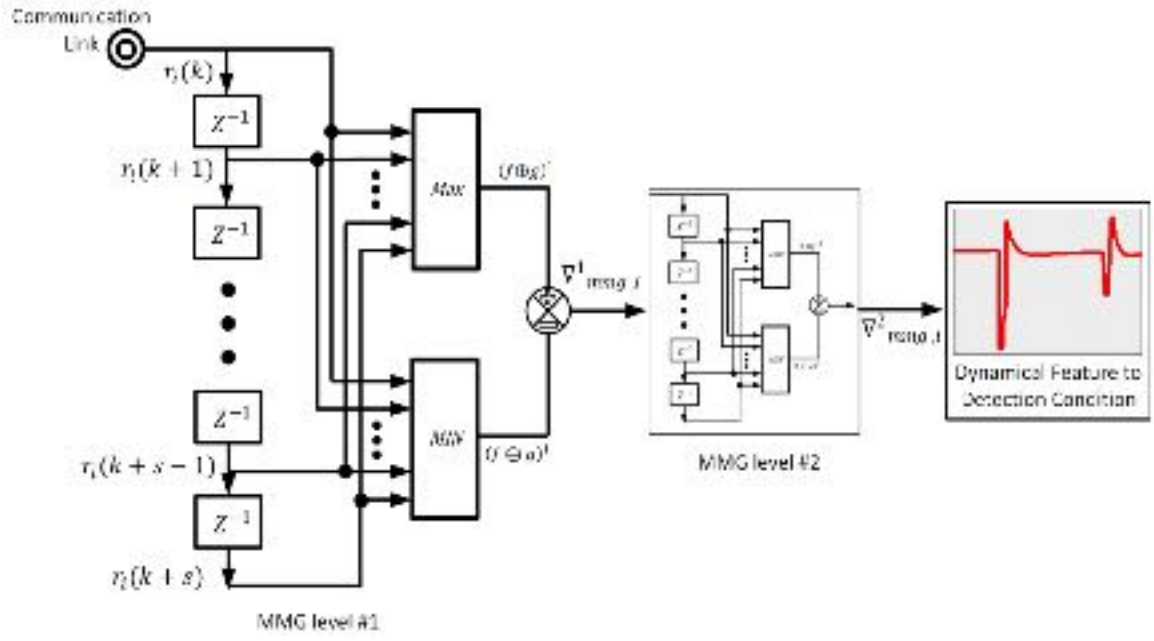


Figure 8.4: Distributed observer based on MM for dynamical feature extraction.

8.5.3 Cyber-attack mitigation

According to the detection decision that is previously discussed, the infected controller is identified, and the mitigation process is started. The mitigation process is done by downsizing the effect of the information coming from the infected agent to entirely exclude it. In this work, the infected agent is excluded from the graph. Let v be the weighting factor of the communication link (i, j), which represents the connectivity strength of the two nodes. Therefore, equation (8.15) can be rewritten as,

$$\dot{r}_i = \sum_{j \in n} v_{ij}.\, a_{ij}\left(r_j - r_i\right) + b_i(r_{rule} - r_i). \tag{8.25}$$

The controller can set the weight v_{ij} of the infected edge by zero if the attack is detected. Figure 8.5 shows the flowchart of the cyber-attack detection and mitigation at j^{th} agent. After the distributed agents start the communication, each agent listens to its neighbor's data r_j. The first and the second morphological gradient are calculated sequentially then, condition (8.24) is checked. When an attack is detected, an alarm flag is triggered, and the suspicious agent is declared. The transmitted information is accepted only to update the node's control law if the attack is not detected. To mitigate the effect of the identified infected agent in the consensus protocol, the malicious node is excluded from the graph. The adjacency matrix A is modified to isolate the effect of the infected node by assigning its weight to zero, $A\{v\} = 0$. Consequently, the Laplacian matrix $\mathcal{L}$ is updated to correct the behavior of the consensus protocol, which mitigates the control objective.

8.6 Results and Discussion

In order to validate the developed secured control system, many scenarios have been implemented. The cyber-physical interconnected nanogrids system model was simulated

using MATLAB/SIMULINK. As shown in Figure 8.1, the tested system contains five nanogrids and they are interconnected as ring DC distribution topology. For a more realistic simulation, each nanogrid is simulated to have a different generation, load, storage levels, which make the maximum transmitted power of the nanogrids are different. In addition, the interconnection segment lengths between every two nanogrids are different.

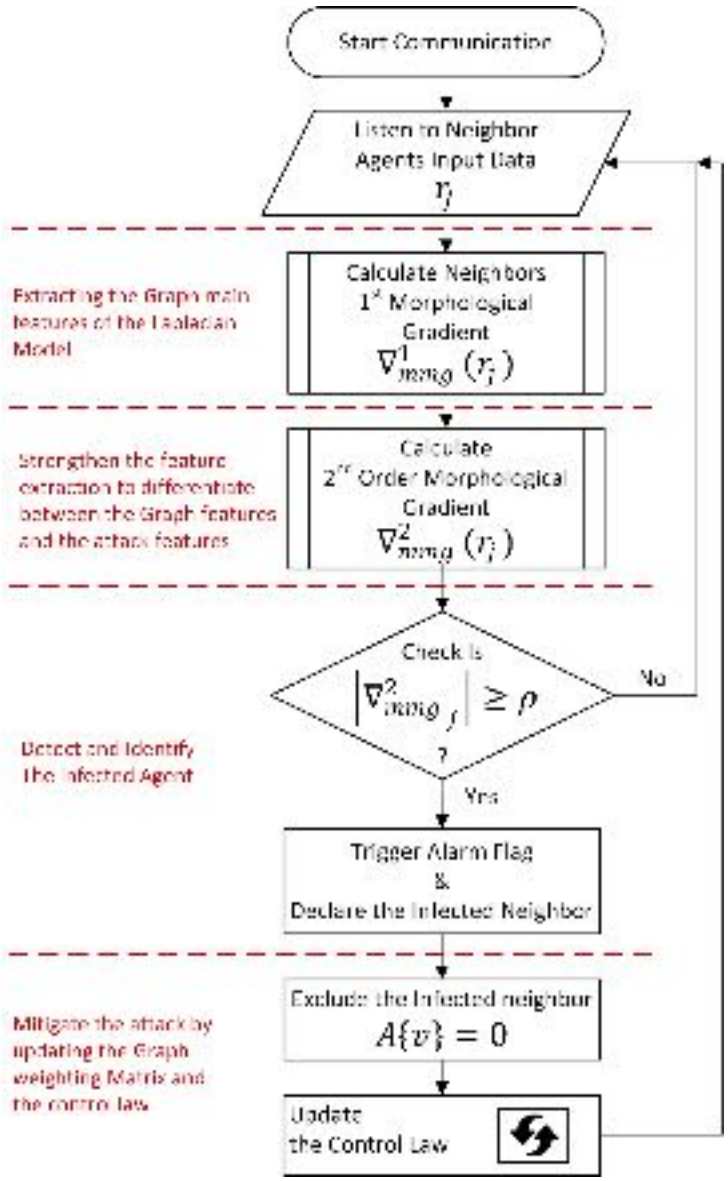


Figure 8.5: Attack detection and mitigation at each agent.

Table 8.1 shows the system parameters and the distributed controller settings. The system has two voltage levels. The LVDC is kept inside the nanogrid itself and the MVDC level is the voltage of the common bus between the nanogrids. The maximum and minimum sharing capabilities are 10 kW and 5 kW, respectively. The value of the threshold is empirically calculated and is set to $\rho = 5$.

Table 8.1: Case Study Parameters

Parameter	Value	Parameter	Value
E_{eq}, V	380	$k_p^{V_{ng}}$	12.4
V_{dc}, V	3000	$k_I^{V_{ng}}$	1.1
$P_{max,1}, W$	10000	k_p^P	2.6
$P_{max,2}, W$	5000	k_I^P	1.05
$P_{max,3}, W$	8000	k_{Ptr}	0.1
$P_{max,4}, W$	7000	k_{Vdc}	1.2
$P_{max,5}, W$	8000	ρ	5.0

The cyber system topology contains five agents; the first agent is the leader and the rest are the followers. Figure 8.6 shows the cyber system topology and its consensus dynamics under step response. As shown, the communication link between the leader (agent 1) and agents 2,3 is unidirectional (from the leader to the followers). The rest of the communication interaction between the followers are bi-directional. The system is subjected to a change in the control input at $t = 5\ s$. The leader adheres to the control input, recording the settling time of 3.9s and the consensus agreement among the followers happens at 16.9s. To validate the cyber-physical mathematical model, the model was compared to the actual implementation response as exemplified in Figure 8.7. The comparison shows the effect of the normal load step change at $t = 1\ s$ and the response is

compared under the existence of an attack at $t = 33\ s$. The overall response a comparable feature, which ensures the mathematical model and validate the implementation.

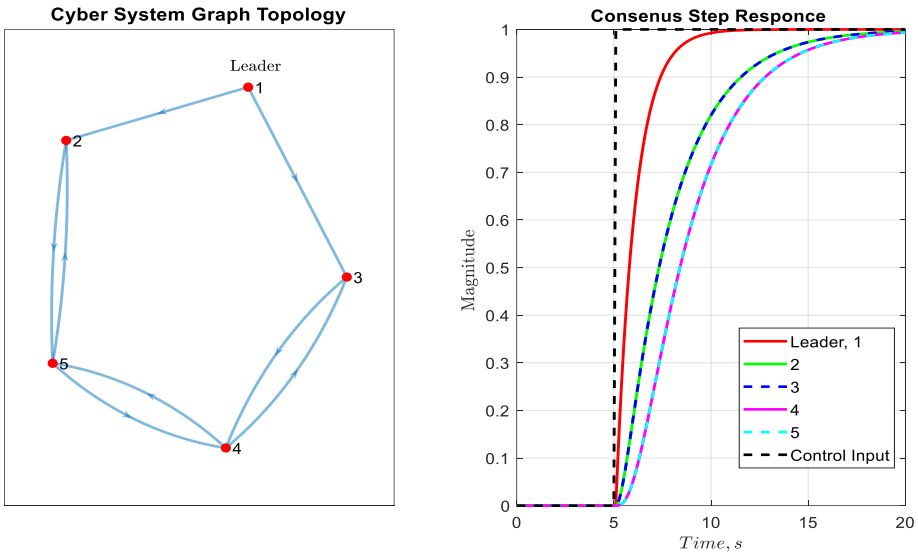


Figure 8.6: Cyber system topology and the consensus dynamical step response.

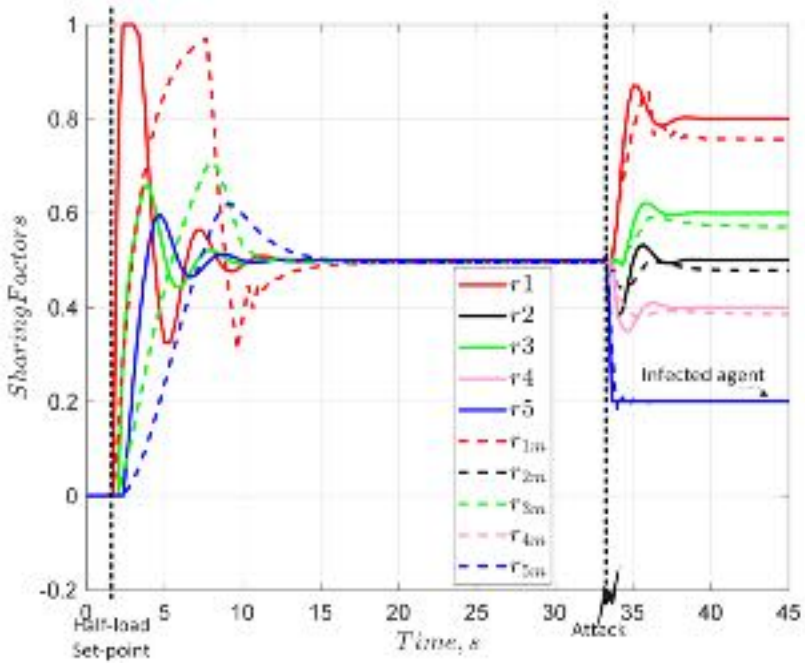


Figure 8.7: A comparison between the actual cyber-physical system implementation and the mathematical model response.

A slight difference in the response is witnessed during the normal step change. The reason is that the practical response of the control system, which drives the physical system is slow. The graph interactions with the attack in both the model and the implementation are very close.

8.6.1 Scenario 1: Replay Attack

In this scenario, all agents have zero initial conditions, and a new set-point of the reference transmitted power is initiated at $t = 1s$. After that, a replay attack on agent 4 has been launched at $t = 3.9\ s$. by replaying the sharing factor at $r_4 = 0.4$ to the end of the simulation. Figure 8.8 shows the response of the cyber system before and after the attack. Three different behaviors of the agents have been captured by the second resolution morphological gradient.

Firstly, the agents tried to follow the leader before the attack between $t = 1\ s$ and $t = 3.8\ s$. In this time slot, the agent's features ∇_{r2} and ∇_{r3} are similar and faster than the rest of the agents because both of them are connected directly to the leader. The slower agents 4 and 5 have almost the same dynamical behavior and have lower MM gradients ∇_{r4} and ∇_{r5}. Then, the second dynamical change happens after the attack between $t = 3.9\ s$ and $t = 10\ s$. On the one hand, agents 2 and 3 have the same interaction with the attack and they behave like the previous time slot.

On the other hand, agents 4 and 5 are significantly different after the attack. As illustrated in Figure 8.8, the feature ∇_{r5} after the attack was similar to the previous time slot of the same agent and it recorded a peak value of $\nabla_{r5} = 0.0005$. In contrast, the attacked agent behavior ∇_{r4} was significantly different than the normal set-point response

and it recorded a peak of $\nabla_{r4} = 74$, which is sufficient to declare that the forth agent is attacked. Finally, the graph's dynamical changes are vanished without reaching consensus.

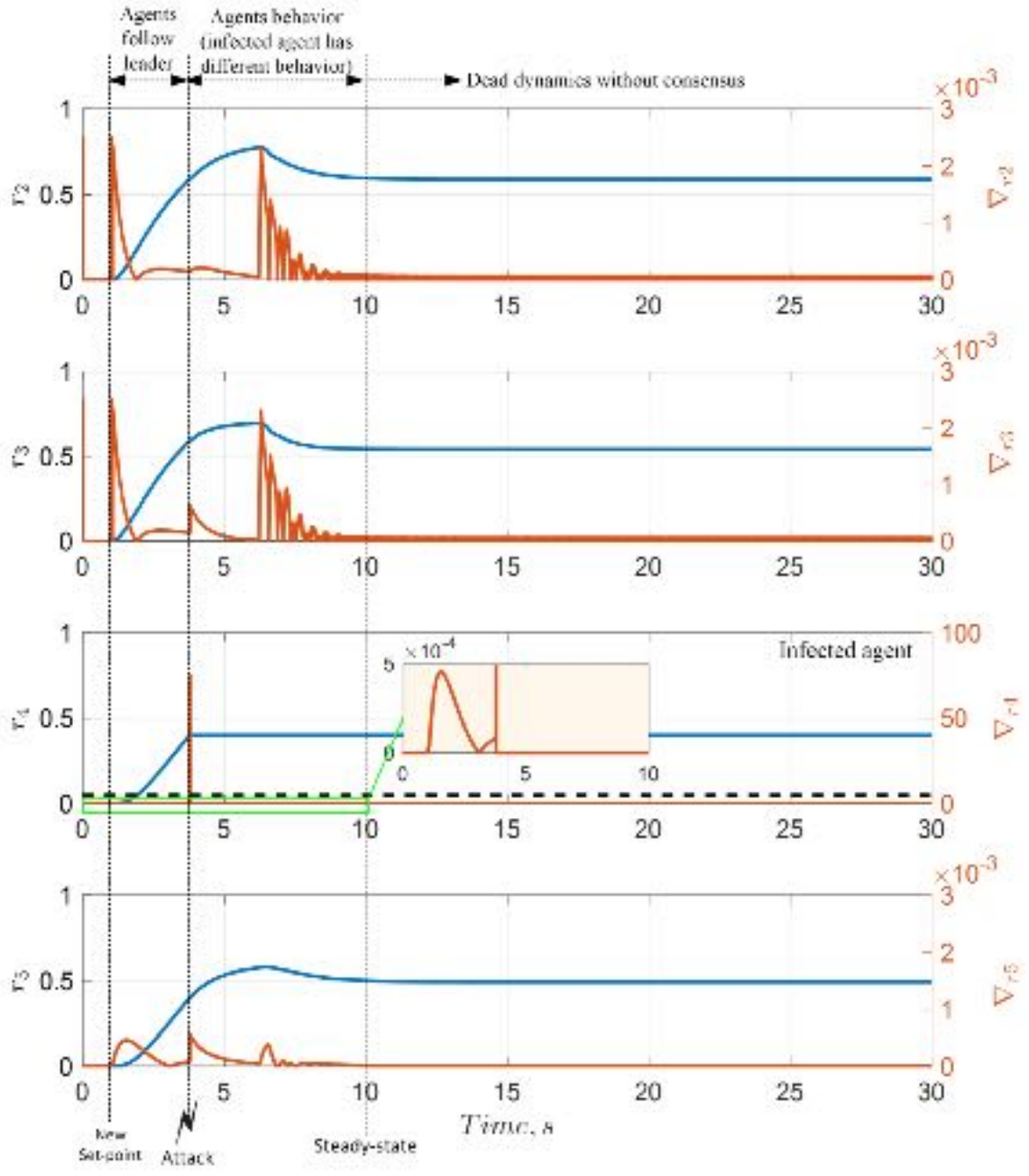


Figure 8.8: Scenario 1: morphological gradient analysis and the attack detection mechanism.

Figure 8.9 illustrates the detailed results of the first scenario. To clearly evaluate the developed method, a comparison between the attack without and with mitigation are depicted on the left and on the right, respectively. At first, the transmitted power of all nanogrids are initialized by zero transferred power. At $t = 1s$, the aggregated refrence transmitted power at PCC is set to $P_{Tr} = 20kW$. Due to the large error signal, the controller updated the control law r_{rule} aggressively to reach unity. The leader agent increases the sharing factor rapidly to follow the control law and the coupling converter follows the controller and increases the leader nanogrid participation. Consequently, the followers follow the leader with a slower response constrained by the graph dynamics. While the distributed controllers cooperatively reach the consensus, agent 4 is attacked and the agreement is disturbed.

As shown on the left-hand side, the control law r_r is changed at $t = 1\ s$. During the transient process, the replay attack is launched by repeating $r_4 = 0.4$ and affects the consensus dynamics. On the one hand, without mitigating the attack, the leader only follows the control rule and the follower reached to different sharing factors at steady-state. Accordingly, different output powers P_{nG} are drawn from the converters to satisfy the total required transmitted power. Without mitigating the attack, the consensus is not accomplished, and the power-sharing objective is not satisfied.

On the other hand, the replay attack with cyber and physical mitigation is simulated. The attack is detected and mitigated by excluding the fourth agent from the cyber system, which corrects the response of the consensus and the agreement has been reached among all agents except the infected one.

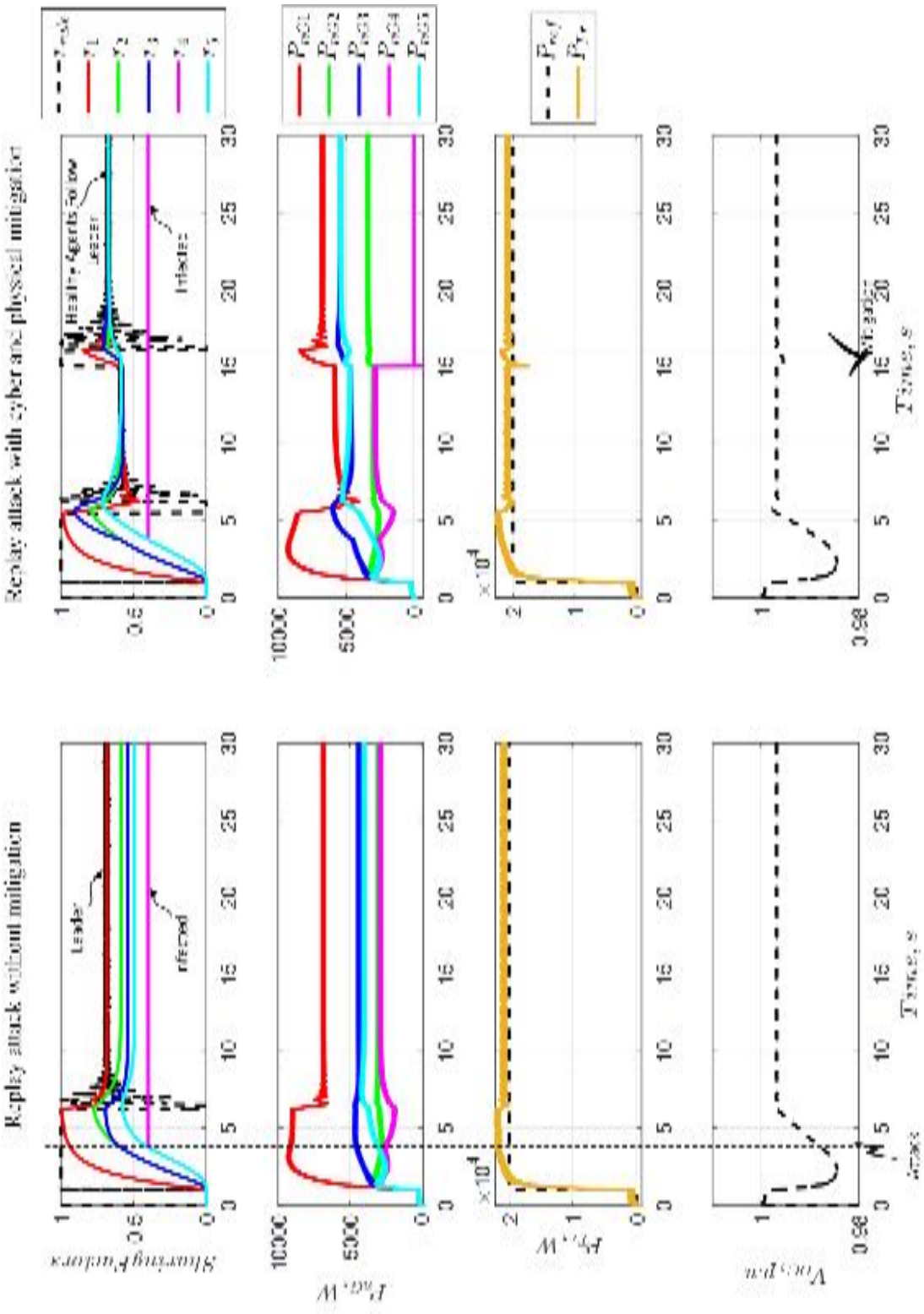


Figure 8.9: Scenario 1: the response with and without attack mitigation.

The infected Nanogrid is still out of control, so the infected nanogrid is isolated from the grid ($P_{nG4} = 0$) and the consensus is automatically updated according to the change in control rule. It can be noted that it takes around 5 seconds to reach the consensus because agent 4 is isolated and it takes a longer time to propagate the updated control law.

8.6.2 Scenario 2: Inception Attack

Similarly, the sharing factors are i initially zeros, and the same reference step change is applied at $t = 1\ s$. The cyber-attack is initiated on agent 2 by setting $r_2 = 0.05$ at $t = 12\ s$ after the consensus on the new reference power. As shown in Figure 8.10, before the attack, all nanogrids follow the leader to satisfy the control rule and the captured features are consistent. Agents 2 and 3 are similar and have comparable gradient values, also agents 4 and 5 are similar and have alike gradient values. The full consensus achieved at $t = 10\ s$ and the agreement is around $r = 0.55$. Then, the attack is launched, and the infected agent has different dynamical behavior. As shown, agents 3, 4 and 5 have almost the same features. It is worth to mention that agents 3 and 4 has a different feature if it is compared to the gradient before and after the attack. That is because of the connectivity path that goes from agent 2 (the infected) to agent 5. Although, the direct connection between agents 2 and 5, the gradient $\nabla_{r2} \gg \nabla_{r5}$, which violates the threshold and accurately helps identify the infected agent.

Figure 8.11 shows the second scenario's sharing factors and transmitted powers before and after mitigating the attack. On the left-hand side, the set-point of the normal load change was applied and the cyber system follow the graph dynamics to reach a consensus according to the leader that follows the control rule r_{rule}.

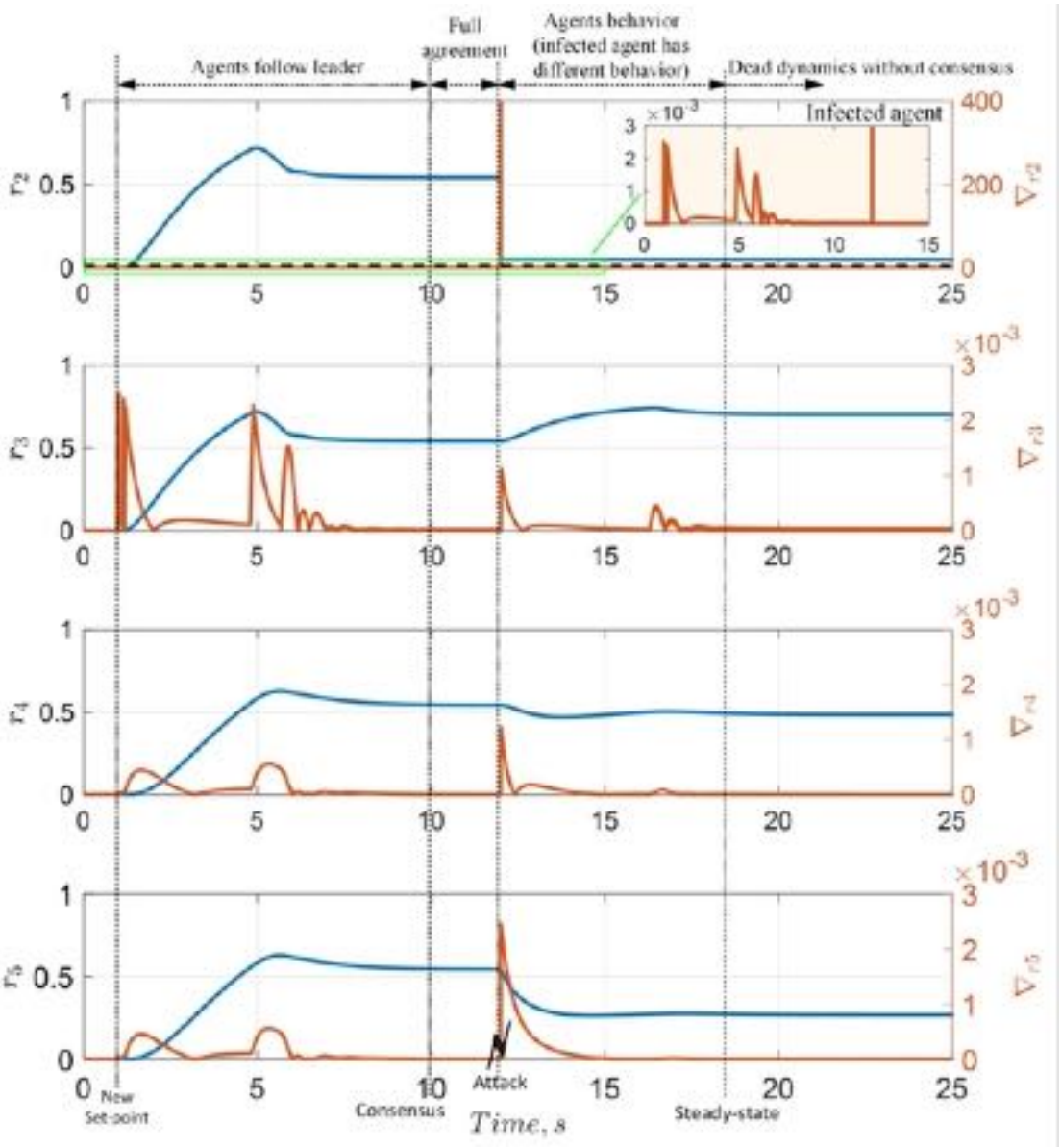


Figure 8.10: Scenario 2: morphological gradient analysis and the attack detection mechanism.

The full agreement is achieved and the DC/DC converters for each Nanogrid tracked the sharing factors according to their maximum limit that is listed in Table 8.1. After the attack, only the leader follows the control rule, while the rest of the agents could not achieve

the consensus. In addition, the leader Nanogrid participated by almost its maximum capability, while the infected one practically did not share. On the right-hand side, the attack is detected, and the mitigation mechanism is activated to isolate the infected agent 2 from the cyber system, which makes the healthy agents follow the leader and accomplishes the agreement. The nanogrid's power sharing conforms the sharing factors decision and the leader power is reduced from 95% to 60%.

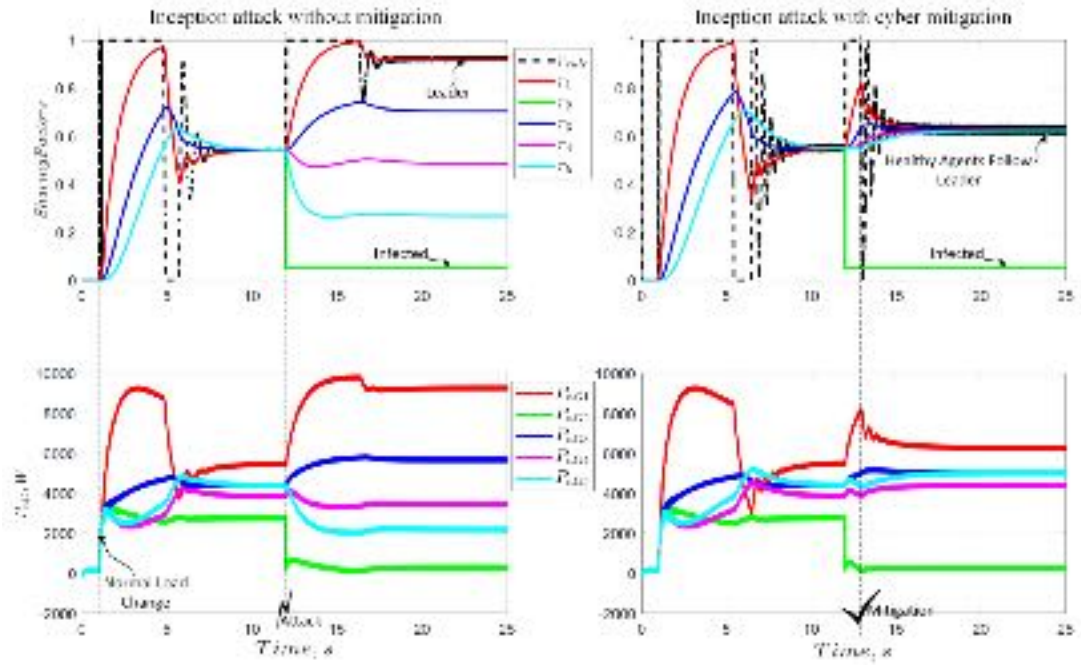


Figure 8.11: Scenario 2: the response with and without attack mitigation.

8.6.3 Scenario 3: Stealthy Attack

Scenario 3 investigates the effectiveness of the developed technique on the stealthy attack. A very slow ramping signal is injected furtively on agent 4 at $t = 12\ s$. As depicted in Figure 8.12, the new set-point application has the same signature for all agents and follows the leader. The consensus is reached at $t = 10\ s$ and the attack is launched after 2 seconds.

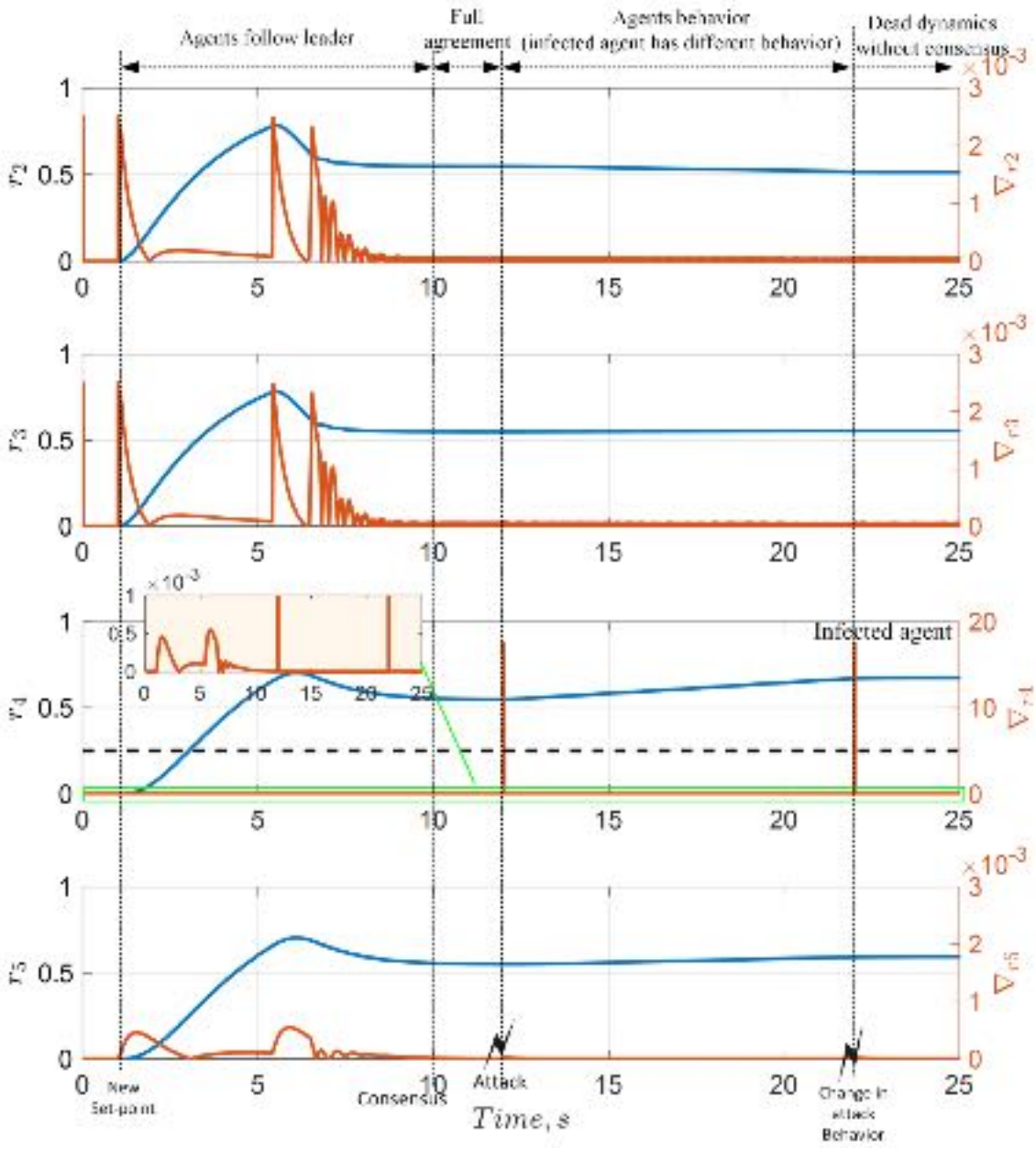


Figure 8.12: Scenario 3: morphological gradient analysis and the attack detection mechanism.

Although the change in the consensus dynamics was very low as compared with normal step-response dynamics, the infected agent 4 is detected and the morphological gradient exceeds the threshold $\nabla_{r4} > \rho$. The rest of the dynamical features recorded almost zero gradients, which easily makes the attack discriminable. In order to ensure the developed

technique accuracy, a change in the attack behavior is applied by changing the ramp slope to zero. The developed detection MM algorithm succeeded to identify the second behavior accurately.

A comparison between the response of the cyber system without mitigation and with mitigation in the third scenario is presented in Figure 8.13. On the left-hand side, the leader follows the control rule after the attack, while the other agents diverged away from the leader and the infected agent follow the injected false ramp data. In contrast, the right-hand side shows the mitigation process by isolating agent 4 from the cyber graph, which achieves the consensus among the heathy agents.

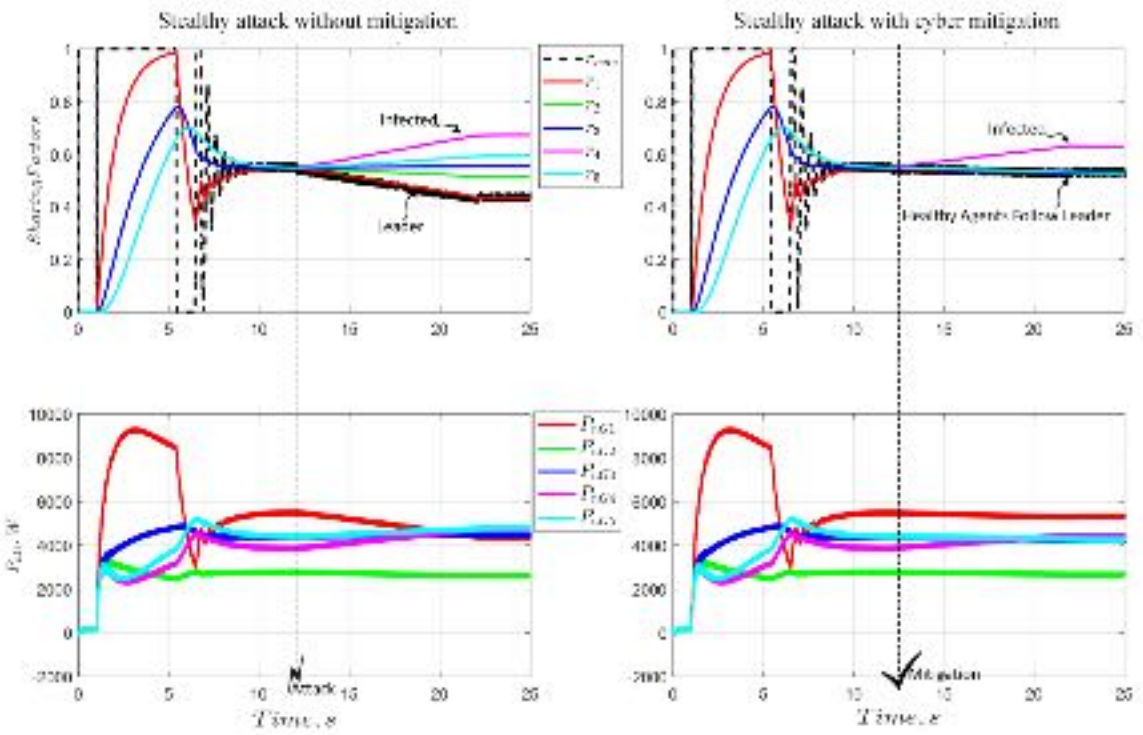


Figure 8.13: Scenario 3: the response with and without attack mitigation.

8.6.4 Scalability Evaluation

To evaluate the scalability of the developed secure distributed control system, a detailed comparison between three different graph topology scales is performed. The scalability of the networked control system is evaluated by the execution time to reach consensus. To reduce the execution time in the large-scale network, more computation and communication capabilities are needed. In the interconnected distributed nanogrids systems, the interactions are usually done by clustering and the number of the nanogrids in a single cluster does not exceed 20 nanogrids/building [145]. Therefore, the topologies under study are selected to be 5 agents,10 agents and 20 agents as shown in Figure 8.14.

The topologies under evaluation have the same formation (ring), sampling time, power set-point and attack type. Firstly, they are subjected to a half-load step change at $t = 1\ s$. After that, an inception attack has been launched at $t = 40\ s$ by holding the infected agent's sharing factors r_5, r_{10} and, r_{20} of the first, the second and the third topologies, respectively. To be able to show the comparison of the same figure, the attack mitigation activation is delayed by 10 seconds. In Figure 8.14(a), the normal load change achieved the consensus after 6.4 seconds of the step change application, while the agreement is accomplished after 9 seconds of the mitigation activation. A very close response has been achieved for the second topology as shown in Figure 8.14(b), which illustrates that the two-consensus process are delayed only 0.6 seconds and 0.5 seconds for the normal change and the mitigation, respectively. By scaling up the number of agents to $n = 20$, as shown in Figure 8.14(c), the full agreement takes 29 seconds with 20 seconds only for mitigating the attack.

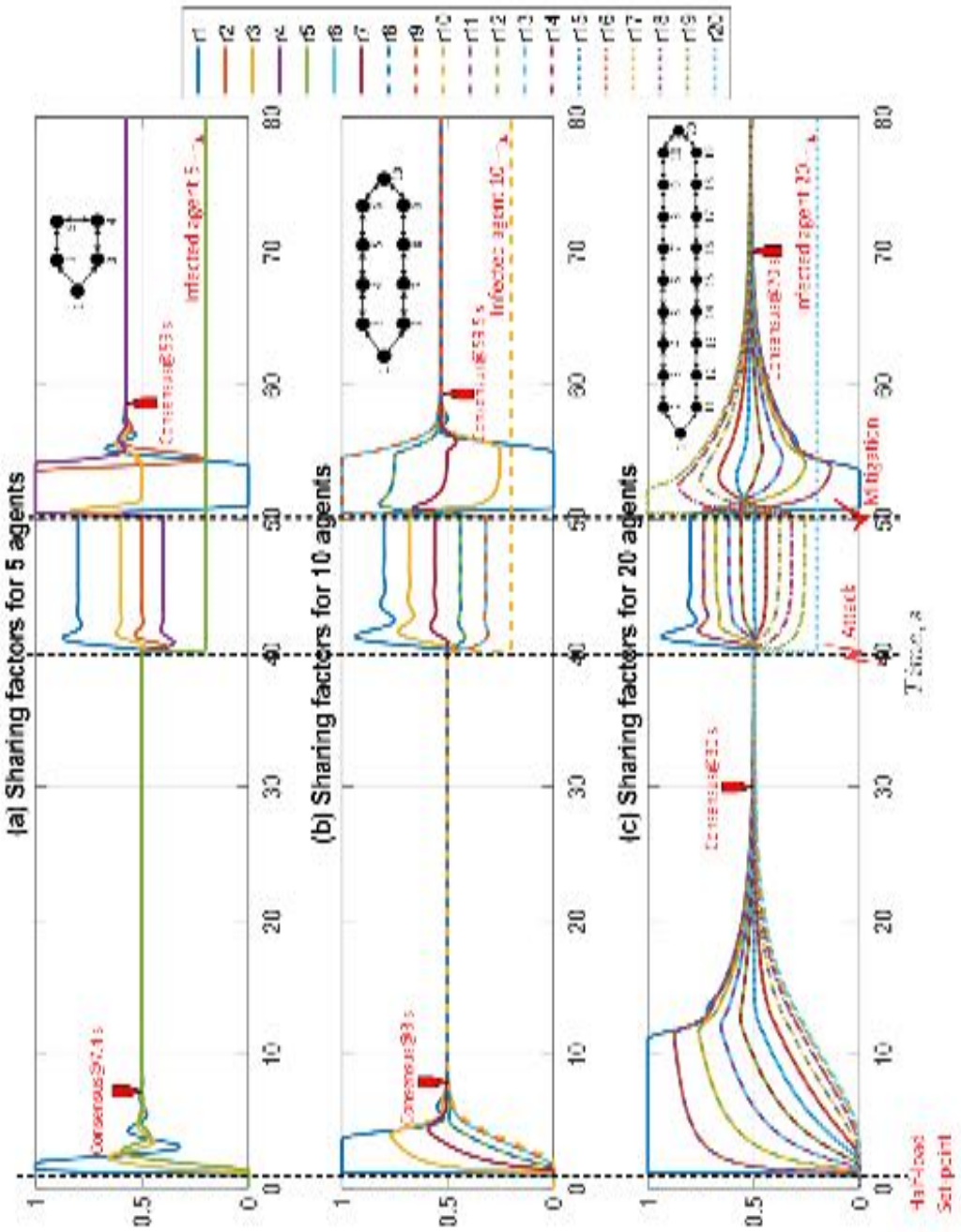


Figure 8.14: Cyber system scalability evaluation under normal load response, attack and attack mitigation.

The half-loading consensus takes a longer time because it starts from zero initial conditions. Practically, the consensus execution time can be defined according to the

application and the control objective. For instance, the secondary control objective requires a few seconds to one minute to update the control objective, which is addressed in this chapter. Therefore, the practical scale of the interconnected nanogrid secondary or even the tertiary control can be implemented successfully using the developed technique.

8.7 Summary

This chapter developed a secured control framework for interconnected nanogrids that represents the basic structure of future smart grids. The developed framework ensures proper coordination among the different nanogrids to ensure a global power objective. The framework also ensures secure operation of the overall system by deploying signal processing technique, graph theory and consensus protocol to make the distributed control system robust against cyber-attacks. The developed algorithm is tested under different attack scenarios, such as the replay attack, inception attack, and stealthy attack. In all cases, the developed framework was able to detect the attacked agent in the system and mitigate the effect of the attack, bringing the system to the normal operation voltage condition and achieving the consensus among the different remaining agents. The developed mathematical morphology based distributed observer gives the ability to the controller to be a security-aware agent via the graph dynamical feature extraction. The developed framework is not expansive since it is a distributed one that does not require high computation and communication burden as centralized. In addition, because of the dependence on the distributed state observer and decision agreement, the developed framework is scalable and reliable, which makes it adequate for future applications.

Chapter 9 Autonomous Decentralized Control for More Resilient Critical Isolated Power Systems

Many critical power systems require a high level of security and resiliency for their decision-making systems. The distributed control system of this critical isolated power system should be designed for the worst case. For instance, if the communication system failed or compromised by a widespread catastrophic attack, the control system should be able to change the control mode autonomously to work without communication. The control objective should depend only on the local measurements and states temporarily until the communication system retrofitted back to normal healthy operation. In this chapter, the shipboard power system is introduced as an example of the critical isolated power system. The shipboard power systems especially the Naval ships have many challenges that are resulted from the loading nature. The control system is this ship should maintain stability. Recently, the shipboard power system design is moving to the Medium Voltage Direct Current (MVDC) power system. However, with the presence of the constant power load (CPL), which behaves as incremental negative resistance, and the presence of heavy pulsed loads (HPL), that consume a massive amount of pulsed power, the voltage stability of the system arises as a critical problem. This problem needs to be addressed appropriately. This work presents a small signal model for a MVDC power system and the design of a model predictive controller that maintains the voltage stability and ensures proper power-sharing among the resources on the ship. Unlike previous works, the small-signal model of the system is embedded inside the controller, which increases the flexibility of the controller to adapt to the different circumstances on the shipboard. The model and the controller are simulated through MATLAB/Simulink and validated using a processor

in the loop. The results showed the ability of the controller to maintain the voltage of the MVDC under different operational circumstances. Also, the controller was able to ensure the adequate operation of the resources and warrant proper power-sharing. The developed control strategy showed the ability to maintain the stability and control objectives even without communication, which can significantly helpful for the critical power systems under catastrophic cyber events.

9.1 Background

With the increasing onboard electrical demand of the maritime ships, adequate system topology and operation became a necessity for the successful operation of future all-electric ships (AES). On-board MVDC power system represents a viable option that can be adopted for future AES [146]–[148]. This is contributed to the different advantages that are developed by the MVDC system such as eliminating the need for a bulky onboard transformer, elimination of synchronization problems, and reducing the risk for systemic disintegration when supplying the emerging pulsed loads [149].

The MVDC system is an interconnected multi-converter network, which uses the power electronic converters to connect the generators, the distributed energy storage system (ESS), and the loads to guarantee a point to point control. However, when multiple converters connected with a feeder that contains a Constant Power Load (CPL) or a High Pulsed Load (HPL), the system becomes vulnerable, and stability issues are expected [150]. The CPL behaves as incremental negative resistance, and the system can easily witness a voltage collapse. CPL and its impact on the stability of a MVDC microgrid under large perturbation were studied in [151]. Unlike [151], the developed technique not only

considers the effect of the HPL alongside the CPL load on the system stability but also deals with the high power density and dynamic operation conditions onboard. The dynamic assessment of the generators and the CPL for a marine MVDC power system was considered in [152]. The authors utilized the small-signal stability analysis to estimate the Source-Load interaction without offering a control or management strategy to stabilize the voltage. Also, they introduced only a closer look at the effect of the CPL and omitted the other types of loads such as the hotel (critical service) load and pulsed loads. In contrast, our developed solution utilizes the small-signal model in the controller to guarantee the stability even with severe conditions.

To maintain the voltage stability, and to keep the proper power-sharing among the distributed ESSs, a droop controller was commonly utilized in the literature. In [153], a cooperative asymmetrical droop controller is used to allow the gensets of a MVDC power system to work in their most efficient operational points, while the hybrid energy storage system was used to absorb the power fluctuations. No pulsed loads were considered, and the power-sharing among storage devices of the same type was not considered as well. One of the main disadvantages of the droop controller in MVDC power systems is the trade-off between the voltage control loop and the current control loop. While the droop characteristics are adjusted to increase the shared current, the voltage of the controlled unit drops and vice-versa. Many research efforts have been made in [154]–[159] to mitigate this problem. Although these methodologies depend on a distributed and communication-based control systems to a consensus on equal power-sharing to increase reliability, the control system resiliency is lower, and it needs more time to follow the global reference

power on the reference current. Also, the dependence on distributed droop control imposes a trade-off between the power-sharing and the voltage drop.

In contrast, our developed solution guarantees proper sharing with slight voltage drop and the non-communication topology of the controller enhance the system resiliency as it is a unique nature of the decentralized control systems. In addition to droop-based controllers, a cascaded control loop scheme is developed in [154], [160] to design the control parameters based on the small-signal stability analysis. However, the developed algorithms focused on the onshore low voltage DC grid. The ship power system, which is the main focus of this paper has a different nature rather than the traditional low voltage DC grids. It has significant non-linear propeller loads and heavy pulsed loads, which require an online control adaption to deal with the different aggressive circumstances. In [161], a hierarchical optimization technique for AES has been used to control the power flow in the presence of pulsed loads. However, the authors studied the issue of managing hybrid energy storage devices; the energy storage generally studied without considering the battery (high energy density) and supercapacitors (high power) different characteristics. Unlike usually dealing with energy storage, the developed management strategy provides the sharing decisions of each storage type according to its features.

From the control architecture perspective, centralized and distributed schemes were applied to control the MVDC systems [162]–[165]. Nevertheless, critical mission-oriented systems like all-electric ship power systems require a resilient architecture, which should be decentralized to decide without extra needed information by the communication as in centralized and distributed architectures. Motivated with the Model Predictive Control

(MPC) which is used to control a process and satisfies the constraints and the model changes, MPC is used in this paper to enhance the controllability of the shipboard power systems [166], [167]. One of the main features of the decentralized control strategy is the resiliency of the system against cyber-attacks or communication failures [168]–[170]. The authors in [171] studied and evaluated different power flow control approaches in the ship power system to reduce the dynamics of the large pulsed load which enhance the flexibility and the computational burden. In [161], the study utilized Pareto Frontier to illustrate the trade-off between the generator control and the energy storage control efforts.

In this chapter, unlike the previous work, instead of initially designing the controller as a conventional PID or droop-based controller using constant stable parameters derived from the small-signal stability analysis, the small-signal modeling is embedded in the controller design. MPC that uses the small-signal model for prediction estimation is developed. The MPC and its optimizer solve the problem to stabilize the voltage and maintain a proper power-sharing policy. The developed controller is adapted online in real-time to support the mission-oriented objectives via defining the mode of operation to enhance the voltage stability during the mission or to maintain the healthy functioning of the storage system during the normal process. Furthermore, the developed strategy is a decentralized one that uses only the local measurements without any communication with the other components of the system [172].

9.2 Shipboard Power System Description

The new shipboard architecture, which mainly depends on electric power, creates a new challenge to increase the ship resiliency. The modern advent of the medium voltage

switch components establishes the ability to electrify the ship to be all-electric. The modernization of the ship to be all-electric gives the ability to reduce the weight of the onboard electrical components so that the AES can be flexibly operated and fulfil its critical missions. The system under study is an actual notional ship power system architecture according to IEEE Standard 1709-2010.

The load nature in the ship power system is significantly different when it is compared with the terrestrial power system, especially with the new advent of electric-based weapons and aircraft launching systems. The ship loading can be classified into three categories: propulsion loads, mission loads and service loads. As shown in Figure 9.1, the MVDC ship power system contains the three loading types. The propulsion load represents the majority of the power capacity by about 80% of the total loading. In addition, the mission loads such as railgun, laser-weapon, and electromagnetic aircraft launching system, which represent the pulsed loads. The pulsed load is a short-time power demand, and it can significantly exceed the total capacity of the main generation system during the missions. Finally, the constant impedance load emulates the service/hotel loads. The ship power system gets its energy from the main synchronous generators, which are derived by gas turbines and then coupled with the MVDC bus via passive rectifiers. For the onboard pulsed loads, the supercapacitors and batteries can adequately supply the surge power demand of the pulsed loads, given that proper power management is adopted.

Supercapacitors can support significant power for a short period, and the batteries can help lower power for longer durations. The energy storage system (ESS) are interlinked with the MVDC bus via DC/DC converters.

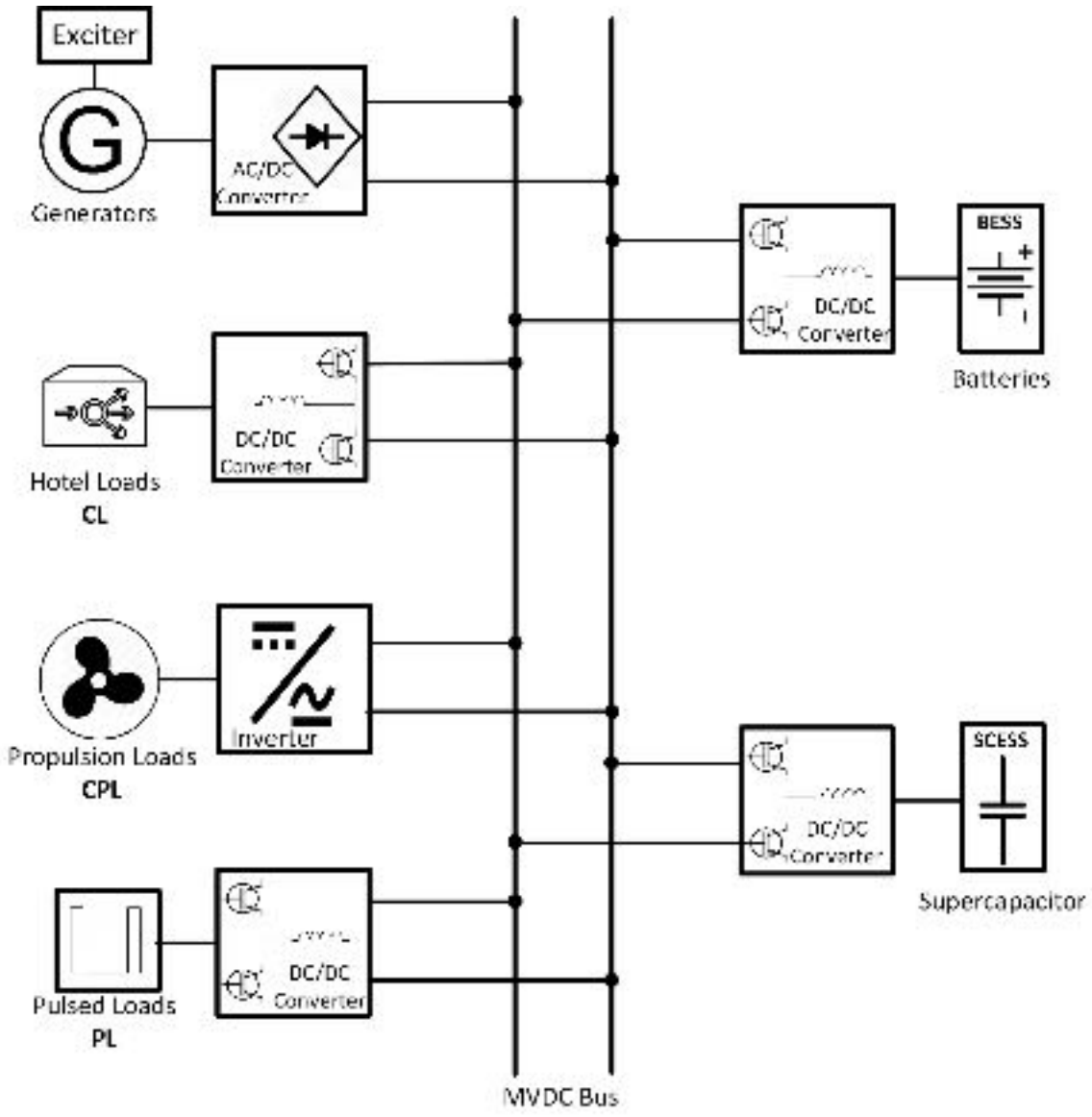


Figure 9.1: MVDC ship power system.

9.3 MVDC System Small-Signal Modelling

MVDC system requires a proper representation of the DC transient behavior of the system to understand the system response under different loading conditions. The inherent nature of the ESS and their power conversion system are inherently non-linear systems. The interaction of the dynamic load changes of ship missions' HPL and the nature of the

propellers' CPL significantly affect the MVDC voltage stability. Due to the non-linear behavior of the MVDC system, the control system is designed based on the small-signal modeling around the equilibrium operating point. Figure 9.2 depicts the typical equivalent circuit of the shipboard power system.

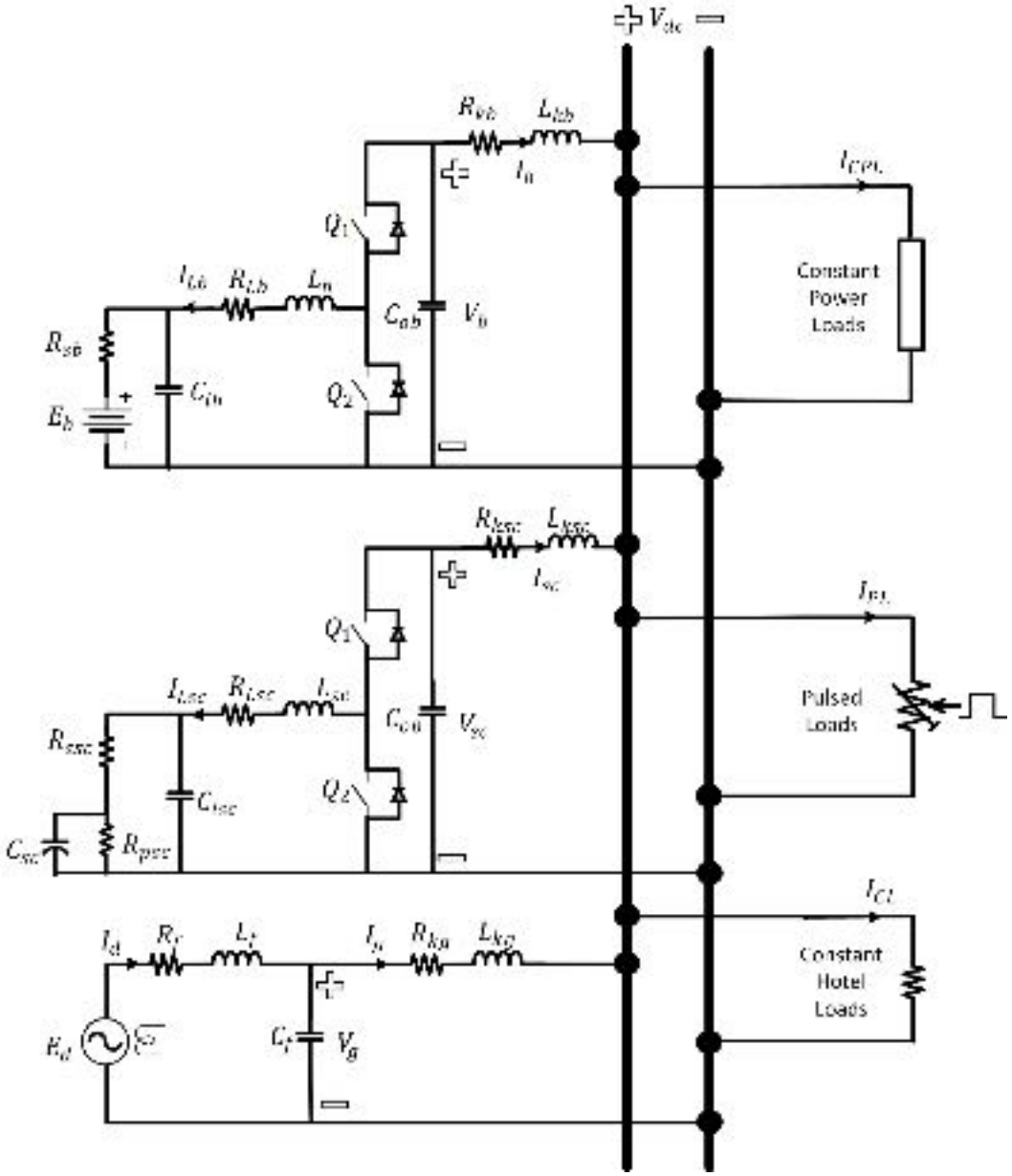


Figure 9.2: System equivalent circuit for MVDC shipboard modeling.

The equivalent circuit is used to design the controllers to capture the system dynamics accurately and is represented using the average model to reduce the computational burden.

Let a MVDC system to have a single main bus with a voltage V_{dc}, n ESS units, g generators and m loads. Each second-order non-linear modelling of an energy unit or load can be decoupled into a large-signal linear state-space modelling and small-signal modelling around the equilibrium point. Consider the system has a non-linear set of dynamics denote f, β and ξ is the dynamics functions of state x and the time t and the non-linear state-space model is written as follows,

$$\dot{x}(t) = f(x,t) + \beta(x,t).u(t) \tag{9.1}$$

$$y(t) = \xi(x,t) \tag{9.2}$$

The previous non-linear state-space system is decoupled to large-signal and small-signal model as follows,

$$\dot{x}(t) = A.x(t) + B.u(t) \tag{9.3}$$

$$y(t) = C.x(t) \tag{9.4}$$

$$\dot{\delta x}(t) = A.\delta x(t) + B^{\delta}.\delta u(t) \tag{9.5}$$

$$\delta y(t) = C.\delta x(t) \tag{9.6}$$

where $x(t), u(t)$ and $y(t)$ are the states, inputs and outputs of the system large-signal model and has parameters A, B and C.

The small-signal model has a change in state, change in inputs, and change in outputs, $\delta x(t), \delta u(t)$ and $\delta y(t)$, respectively. To linearize the non-linear model around the

operating point, A and C still the same as the large-signal model, but B changes according to the linearization process to be B^{δ}. In order to enhance the prediction horizon of the high-bandwidth controller without a large computational burden, the developed model is simplified from the detailed model to the average model. The following sections show the detailed state-space representation of the small-signal model for each energy unit.

9.3.1 Energy Storage System

Generally, for any storage system, power conversion/conditioning is vital to interlink and control the ESS and the MVDC bus. The energy storage units charge/ discharge according to the different loading conditions. Therefore, adequate modeling is required. The main components of the ship power system as a generator, battery storage, supercapacitor storage, constant power load, pulsed load, and MVDC bus are represented to design the controller according to MVDC ship power system IEEE standard. The model focuses on the energy storage systems and their interlinking DC/DC converters alongside the constant power load and pulsed load. The generator model is represented to restrict the interaction with the very high ramping loads by delaying the response time to let the ESSs compensate for the fast load dynamics. It is commonly known in the multiple zone ship power system that the ESSs in one zone serve the pulsed loads within this zone and it does not interact with the other zones.

9.3.1.1 Battery Energy Storage System (BESS) Model

The BESS model consists of three stages: the battery model, the DC/DC converter model and the DC filter model. The equivalent circuit of the battery storage module is illustrated in Figure 9.2, and the mathematical small-signal-state-space representation is

formulated as (9.7)-(9.10). The BESS state vector is δx_b, input vector δu_b and the its major parameters are A_b and B_b^{δ}. The battery storage system can supply power for the steady state low ramping load changes.

$$\delta x_b = [\delta I_{Lb} \quad \delta V_{ib} \quad \delta V_b \quad \delta I_b \quad \delta SOC_b]^T \tag{9.7}$$

$$\delta u_b = [\delta D_b \quad \delta V_{dc}]^T \tag{9.8}$$

$$A_b = \begin{bmatrix} \frac{-R_{Lb}}{L_b} & \frac{-1}{L_b} & \frac{D_b}{L_b} & 0 & 0 \\ \frac{1}{C_{ib}} & \frac{-1}{R_b C_{ib}} & 0 & 0 & 0 \\ \frac{-D_b}{C_{ob}} & 0 & 0 & \frac{1}{C_{ob}} & 0 \\ 0 & 0 & \frac{-1}{L_{kb}} & \frac{-R_{kb}}{L_{kb}} & 0 \\ 0 & 0 & 0 & \frac{1}{Q_b} & 0 \end{bmatrix} \tag{9.9}$$

$$B_b^{\delta} = \begin{bmatrix} \frac{\bar{V}_b}{L_b} & 0 & \frac{-\bar{I}_{Lb}}{C_{ob}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{L_{kb}} & 0 \end{bmatrix}^T \tag{9.10}$$

9.3.1.2 Supercapacitor Energy Storage System (SCESS) Model

The supercapacitor is adopted and naturally designed for high power sudden load changes, which has very high ramping rates. The supercapacitor is represented by an upper capacitance capacitor with an internal series and parallel resistors. Also, as shown in Figure 9.2, the supercapacitor is connected to the MVDC via DC/DC converter. The converter can control the magnitude and the rate of charge/discharge according to the load changes.

The SCESS state vector is δx_{sc}, input vector δu_{sc} and its major parameters are A_{sc} and B_{sc}^{δ}. The mathematical small-signal-state-space representation of the SCESS is depicted in relations (9.11)-(9.14).

$$\delta x_{sc} = [\delta H_{sc} \quad \delta I_{Lsc} \quad \delta V_{isc} \quad \delta V_{sc} \quad \delta I_{sc} \quad \delta SOC_{sc}]^T \tag{9.11}$$

$$\delta u_{sc} = [\delta D_{sc} \quad \delta V_{dc}]^T \tag{9.12}$$

$$A_{sc} = \begin{bmatrix} \frac{-(R_{psc}+R_{ssc})}{R_{psc}R_{ssc}C_{sc}} & 0 & \frac{1}{R_{ssc}C_{sc}} & 0 & 0 & 0 \\ 0 & \frac{-R_{Lsc}}{L_{sc}} & \frac{-1}{L_{sc}} & \frac{D_{sc}}{L_{sc}} & 0 & 0 \\ \frac{1}{R_{ssc}C_{isc}} & \frac{1}{C_{isc}} & \frac{-1}{R_{ssc}C_{isc}} & 0 & 0 & 0 \\ 0 & \frac{-D_{sc}}{C_{osc}} & 0 & 0 & \frac{1}{C_{osc}} & 0 \\ 0 & 0 & 0 & \frac{-1}{L_{ksc}} & \frac{-R_{ksc}}{L_{ksc}} & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{Q_{sc}} & 0 \end{bmatrix} \tag{9.13}$$

$$B_{sc}^{\delta} = \begin{bmatrix} \frac{\bar{V}_{sc}}{L_{sc}} & 0 & \frac{-\bar{I}_{Lsc}}{C_{osc}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{L_{ksc}} & 0 \end{bmatrix}^T \tag{9.14}$$

9.3.2 Generation System Model

The generation system includes gas-driven turbines and synchronous generators. The generator control system is a low bandwidth control as compared to the onboard energy storage systems. Because of the load nature of the ship power system, the control systems of the generators, such as the turbine governors and the exciters, have a low impact on the control decision during the ship mission mode, when high and sudden changes in the load occur. In the light of the high voltage control dynamics, the speed governor control is neglected in the modeling process [163], as it has a low bandwidth control decision. The rest of the generation system, which has a considerable effect as the exciter, the generator, the passive diode rectifier, and the filter is modeled in the linear state-space form as illustrated in relations (9.15)-(9.18).

$$\delta x_g = [\delta E_d \quad \delta I_d \quad \delta V_g \quad \delta I_g]^T \tag{9.15}$$

$$\delta u_g = [\delta \psi_f \quad \delta V_{dc}]^T \tag{9.16}$$

$$A_g = \begin{bmatrix} \frac{1}{\tau_e} & 0 & 0 & 0 \\ \frac{1}{L_f} & \frac{-R_f}{L_f} & \frac{-1}{L_f} & 0 \\ 0 & \frac{1}{C_f} & 0 & \frac{-1}{C_f} \\ 0 & 0 & \frac{1}{L_{kg}} & \frac{-R_{kg}}{L_{kg}} \end{bmatrix} \tag{9.17}$$

$$B_g = \begin{bmatrix} \frac{1}{\tau_e} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{L_{kg}} \end{bmatrix}^T \tag{9.18}$$

9.3.3 Loading Model

As discussed previously, the onboard types are CPL, HPL and constant impedance. According to the equivalent circuit in Figure 9.2, the loads are simplified for modeling using state-space representation. The CPL current depends on the load power rating and the voltage of the MVDC bus and can be represented as in (9.19).

$$I_{CPL} = \frac{P_{CPL}}{V_{dc}} = f(V_{dc}) \tag{9.19}$$

The CPL has non-linear characteristics and to design a controller based on its model behavior; it should be linearized as follows,

$$f(V_{dc}) = \left(\frac{df(V_{dc})}{dV_{dc}}\right)^0 . \delta V_{dc}(t) \tag{9.20}$$

$$I_{CPL} = \frac{1}{-R^0_{CPL}} . \delta V_{dc}(t) \tag{9.21}$$

where $R^0_{CPL} = \bar{V}_{dc}/-P^0_{CPL}$, which is calculated using the steady-state values to linearize the constant power load around the equilibrium operating point. On the other hand, the pulsed

load and the constant impedance load depend only on the power profile and the load impedance, respectively. The representation can be written as,

$$I_{PL} = \frac{P_{PL}}{V_{dc}} \tag{9.22}$$

$$I_{CL} = \frac{V_{dc}}{R_{CL}} \tag{9.23}$$

9.3.4 MVDC Bus Model

The state-space representation of the MVDC bus (DC-link) is mainly obtained using the Kirchhoff current law. All generation units, storage units and loads are connected to the MVDC bus. Algebraically, the change in voltage on the bus depends on the algebraic summation of the injected and absorbed power. In this model, the dc link voltage is modeled as a state, and the inputs are the currents. The small-signal modeling of the MVDC bus is written as,

$$\delta x_{link} = [\delta V_{dc}] \tag{9.24}$$

$$\delta u_{link} = [\delta I_b \quad \delta I_{sc} \quad \delta I_g \quad \delta I_{PL} \quad \delta I_{CL}]^T \tag{9.25}$$

$$A_{link} = \left[\frac{-1}{C_{link}R_{CL}} + \frac{1}{C_{link}R^0_{CPL}}\right] \tag{9.26}$$

$$B_{link} = \left[\frac{-1}{C_{link}} \quad \frac{-1}{C_{link}} \quad \frac{1}{C_{link}} \quad \frac{-1}{C_{link}} \quad \frac{-1}{C_{link}}\right] \tag{9.27}$$

Notably, as in the previous relations, the change in voltage, which is modeled as a disturbance in the resources, is represented here as a state and is affected by the change in load currents. The designed controller should inject the required current to balance the loading and stabilize the voltage. The following part shows how the controller and the management process is created based on the previous model to achieve the required performance in a decentralized manner.

9.4 Energy Storage Management Strategy

Traditional management techniques suffer from the conflict between the voltage control loop for the voltage stabilization and the current control loop of power-sharing. This conflict degrades the voltage performance of the system. The main objectives of the developed management strategy are to provide the proper voltage stability performance and the optimal power-sharing among the resources, with an adequate trade-off between the voltage and current control perspective.

The ESSs are controlled to interact with the heavy loading conditions, such as pulsed loads with fast response, to stabilize the voltage before the system voltage collapse. The developed controller manipulates the ESS's interlinking DC/DC converters via the Pulse Width Modulation (PWM) to control the magnitude and the rate of the injected or absorbed power by the ESS.

To increase the resiliency of the MVDC system and support the survivability of the ship, a decentralized control strategy was developed. The introduced methodology provides an isolated controller for each storage unit, and the control action mainly depends on the local measurement without any communication with the other components in the system.

The operation of the different type of ESSs is working independently, i.e., the battery and supercapacitor have different operation logic based on the ramping load features as shown in Figure 9.3. The figure shows a flowchart, which defines the battery operation logic. Firstly, the bus voltage, converter inductor current and battery's output current is measured. Then, the battery activation signal depends on the output voltage of the Low

Pass Filter (LPF), which enforce the battery to work only with slow changes of voltage. After that, the absolute difference in the voltage is compared with the threshold. This threshold is set to a small value of 0.1% of the nominal voltage value to ensure unforeseen changes compensation. Then, the activation signal φ_b is multiplied by the current sharing weighting factor that depends on the state of charge value to formulate the current reference weighting factor ω_{ib}. The MPC controller define the charging/discharging autonomously, by tracking the reference of the change in voltage $\delta v_{b,ref}$, which is set to zero and given weight $\omega_{vb} = 1$. The weighting factor of the voltage reference tracking is set to unity because the voltage stability of MVDC system is critically important as compared to the current sharing. Therefore, when the change in voltage deviates from zero in a negative direction, the batteries discharge and if it grows positively, the charging decision is taken.

On the other hand, after reading the MVDC bus voltage, the High Pass Filter (HPF) is used to capture the high transient dynamics in voltage to activate the supercapacitor. The flowchart on the right-hand side shows the logic operation of the supercapacitor. The supercapacitor working signal φ_{sc} is set to high when the absolute value of the change in voltage $|\Delta\delta V_{dc}| \geq 1\%$ of the nominal voltage. This threshold is selected to be larger than a battery to ensure that the supercapacitor does not interact with the long-term noises, which embedded in the filtered signal. The activation signal is held for 100ms only then reset to zeros. This due to the purpose of the supercapacitor, which supports significant-high power for short time. Therefore, in the case of serving the pulsed load, the supercapacitor provides the power at the starting of the pulse then, the battery continues the operation. As discussed before, the MPC controller autonomously decides of

charging/discharging by tracking the zero-division reference. The sharing currents between the supercapacitors are defined based on the weighting factor ω_{isc}, which is estimated based on the state of charge condition.

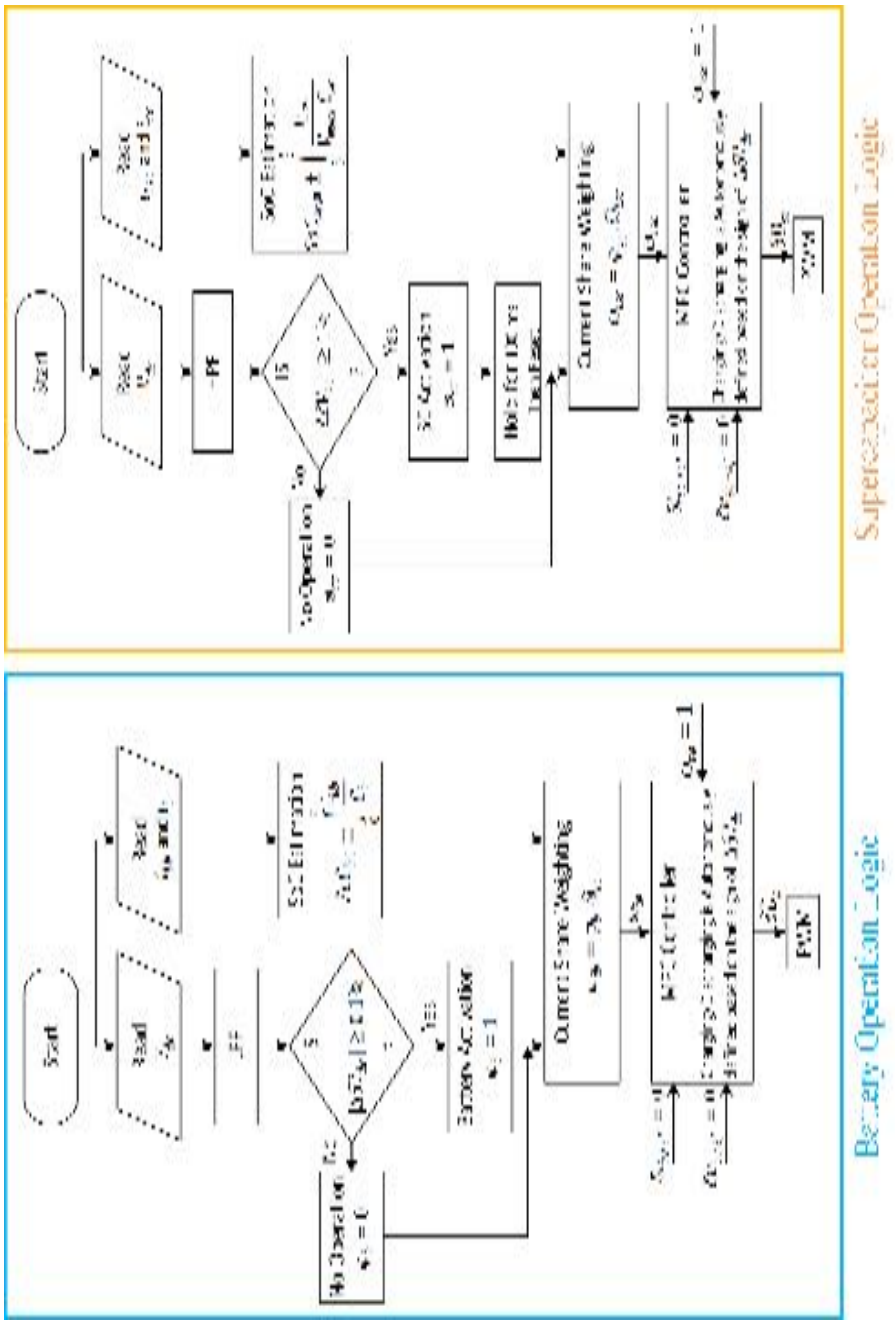


Figure 9.3: Energy Storage Operation Logic.

Figure 9.4 shows the developed storage management strategy. The presented technique has the same structure for the control system of the different storage units, but different settings and initialization.

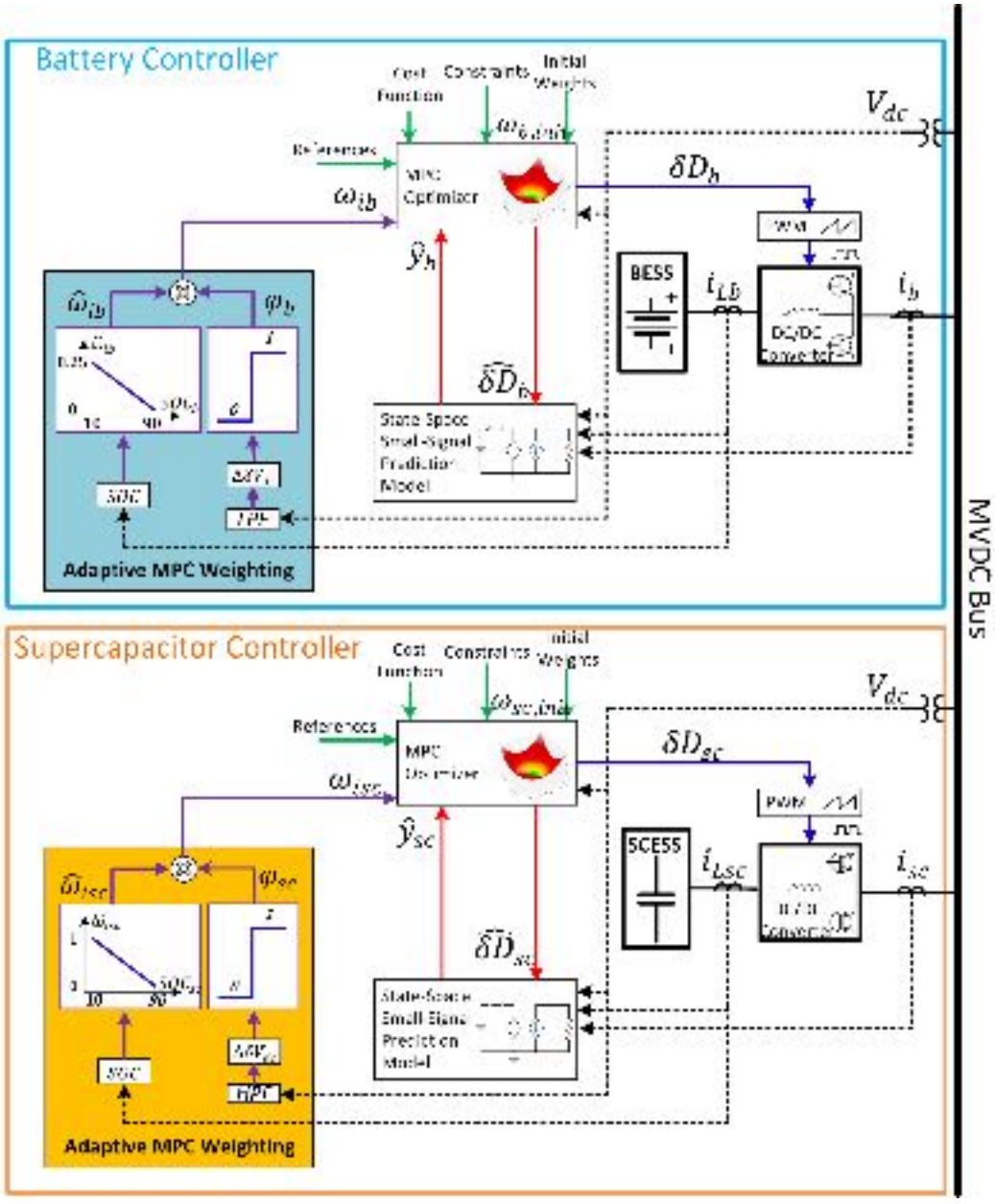


Figure 9.4: Energy storage management strategy.

The approach consists of two main parts: the model predictive control (MPC) and the adaptive MPC weighting algorithm. The following subsections illustrate the description of the two parts.

9.4.1 Model Predictive Controller

The key reason for using the MPC in this strategy is summarized in its ability to optimize the control process to provide a balance between the voltage and the current loops designs. In addition, it can deal with unexpected sudden changes in the onboard loading without violating the system constraints.

Usually, the MPC is designed based on the large-signal state-space modeling in the majority of control problems. In this work, the small-signal model, which as previously described is used to design the MPC.

The reason behind the use of small-signal modeling is the highly non-linearity of the system. The sources of non-linearity are not only the DC/DC converter control, but also the high CPL load that imposes severe instability problems; especially with the interlinking inverter of the propulsion system [25]. Traditionally, the droop control and power-sharing management require stability analysis to cope with the trade-off between the current and voltage control loops, which is not practical for sudden changes.

MPC solve the control problem using the state-space representation of the small-signal modeling to predict the system behavior under the constant power load and provide the corrective action to enhance the robustness under the sudden changes of the HPL.

As shown in Figure 9.4, for both battery and supercapacitor controllers, the MPC has an objective to track the references by manipulating the values of change in duty ratio δD_b and δD_{sc}. The controller is initialized by setting the cost function, constraints and the initial weighting factors $\omega_{b,init}$ and $\omega_{sc,init}$. Then, according to the previously discussed operation logic, the voltage, current references, and weighting factors is defined by observing the MVDC voltage and storage systems currents. Finally, the MPC uses the small-signal state-space model to predict the future output $\hat{y}_b$ and $\hat{y}_{sc}$ and adjusts the input duty ratios based on the corrected model manipulated inputs $\delta\widehat{D}_b$ and $\delta\widehat{D}_{sc}$. The final optimized values of duty ratio are fed to the PWM, which derive the DC/DC converters.

Mathematically, the general formulation of the MPC optimization problem is defined to maintain the voltage profile by minimizing the deviation from 1 p.u. and minimize the storage share to increase the healthy operation of the storage units, without violating the MVDC bus stability. In general, form, consider S is the storage type (battery or supercapacitor). Equation (9.28) shows the general structure of the objective function for a particular storage unit where p and k is the prediction and control horizon of the MPC. The objective function is subjected to the constraints of the small-signal predictive model and the output/input limitations.

The key advantage of the developed small-signal model predictive control can be understood by observing that the reference values of the controller are zero. Therefore, there is no conflict between the two control perspectives, and the controller autonomously optimizes the manipulated input for optimal performance. Also, the MPC finds the solution

that minimizes the voltage deviation with a lower change in the ESSs states, which enhance the healthy operation of the hybrid storage system.

Assume that the MPC state weights are normalized in the range of a maximum value of unity and a minimum amount of zero. The high priority of the voltage support is provided by setting its weight ω_{vs} to unity. From the current control perspective, the weighting of the current change $\omega_{is}$is adapted according to the required share percentage, state-of-charge (SOC) and the mode of operation. The following subsection describes the main concept of the weighting adaption algorithm.

$$\begin{aligned} Min\ J_s &= \sum_{i=1}^{p} \omega_{iv}.\delta V_s(k+i|k) + \omega_{is}.\delta I_s(k+i|k) \\ s.t. \quad & ESS\ model \\ & V_s^{min} \le V_s \le V_s^{max} \\ & I_s^{min} \le I_s \le I_s^{max} \\ & I_{Ls}^{min} \le I_{Ls} \le I_{Ls}^{max} \\ & D_s^{min} \le D_s \le D_s^{max} \\ & SOC_s^{min} \le SOC_s \le SOC_s^{max} \end{aligned} \tag{9.28}$$

9.4.2 Adaptive MPC Weighting

The primary objective of taking the SOC of the storage unit into consideration is to achieve the proper power-sharing between the storage units and to define when the storage can interact with the change in the voltage. The value of the weighting/penalty is determined using the multiplication of two factors. The first one, which establishes the share percentage is $\widehat{\omega}_{is}$. The second factor φ_s is the storage insertion/removal factor, which is a discrete value and it is defined according to the rate of change of the filtered measured voltage.

The output power of specific storage is manipulated according to its SOC to guarantee the healthy operation of the BESSs and SCESSs by preventing under-discharge or over-charge problems. The MPC objective function penalizes the tracking error for the storage output voltage and the output current to ensure the voltage regulation objectives and the shared current reference. When the current tracking error penalty $\widehat{\omega}_{is}$ is zero and the voltage error is unity, the MPC generates the manipulated variable to support the voltage without caring about the output current (minimize the voltage deviation). If the output current penalty $0 < \widehat{\omega}_{is} \leq \omega_{is}^{max}$, and the voltage weighting still unity the MPC gives the required control action to support the voltage, but it will take the current reference of the storage into consideration to satisfy a certain sharing percentage according to the state of charge. The following relation is used to calculate the required current penalty for a certain SOC. The constant values of z and c are defined offline according to the modelling of both the batteries and the supercapacitors.

$$\widehat{\omega}_{is} = f(SOC_s) = z.SOC_s + c \tag{9.29}$$

As discussed before, the supercapacitor should interact only with the aggressive rate of change of voltage during the ramping of the pulsed load. After that, the battery can share during the steady-state operation or with the low ramping changes. The second factor φ_s is a discrete value that changes between 0 and 1 according to a predefined threshold of the gradient of the change of the voltage $\Delta\delta V_{dc}$, which is calculated using the filtered measured voltage.

In order to let the supercapacitor interact with high transients, the High-Pass-Filter (HPF) is used to capture the fast ramping. On the other hand, the battery should react with

the low changes only, so the battery is activated based on the Low-Pass-Filter output (LPF). The following relation describes the discrete factor identification. The final value of the current weighting is calculated as follows.

$$\varphi_s = \begin{cases} 1 & if\ \ \Delta\delta V_{dc} \geq TH \\ 0 & otherwise \end{cases} \tag{9.30}$$

$$\omega_{is} = \widehat{\omega}_{is}.\varphi_s \tag{9.31}$$

9.5 Results and Discussion

To validate the developed management strategy, different loading scenarios are implemented. The MVDC system model is simulated using MATLAB/SIMULINK. The controllers are designed using MATLAB/SIMULINK and are performed on an external STM32 board-based processor in the loop. Table 9.1 shows the system ratings and initial conditions. The system is initially stable, and the MVDC bus voltage is assumed to be one p.u. (5000 V). In order to evaluate the developed technique response, the depicted results in this section are compared with the conventional PI controllers. It is worth mentioning that the conventional PI in this comparison is intended to give a reference that the reader is familiar with. As shown in Table 9.1, the system under study has two generators, two BESSs, two SCESSs, and three different load types. The CPL and Constant Impedance Load (CL) represent about 75% and 20% of the total installed main generation capacity, respectively. Table 9.2 shows the typical model parameters, which are used in the model and the MPC implementation.

The PL has a steady-state rating of 1500 A during one second, and it may be increased to 2000 A during the transient. The initial conditions are assumed to be around the full loading of the generators, and the ESSs is not active with zero current initially. Bat.1 is

almost fully charged and Bat.2 has a low SOC. Both supercapacitors (SC.1 and SC.2) have sufficient SOC at the initial state for the pulsed load.

Table 9.1: Ship system ratings and initial conditions

Unit	Rating, A	Initial Conditions, A
Gen.1	7000	6400
Gen.2	7000	7000
Bat.1	1500	0 @ 80% SOC
Bat.2	1500	0 @ 35% SOC
SC.1	2200	0 @ 65% SOC
SC.2	2200	0 @ 85% SOC
CPL	12000	11100
CL	3000	2300
PL	1500	0

Table 9.2: MVDC circuit Parameters

E_b	931 V	R_{LSC}	0.010 Ω
C_{ib}	1500 μF	L_{SC}	1.288 mH
R_{Lb}	0.017 Ω	C_{oSC}	3500 μF
L_b	2 mH	L_{kSC}	20 μH
C_{ob}	3700 μF	E_d	4.16 kV
L_{kb}	20 μH	C_f	105 mF
C_{SC}	500 F	R_f	0.05 Ω
C_{iSC}	1500 μF	L_f	0.101 mH

The constant factors of the linear relation between the weighting $\widehat{\omega}_{is}$ and the SOC is initialized offline according to the case study parameters. The constants z and c are set to be -0.031 and 0.281 for the BESSs, respectively. For the SCESSs, they are set by -0.0125 and 1.125.

In this case study, the conventional primary droop control and secondary PI control is used to compare their performance with the developed small-signal model predictive control. Figure 9.5 shows the conventional control scheme. The inner control loop of the current and voltage droop is utilized as a primary control to control the storage output voltage. On the other hand, the secondary control loop is used to impose an offset compensation for the voltage as a correction for equal current sharing control. The primary control parameters are chosen as $kp_{vs} = 19, ki_{vs} = 10$, $R_{droop} = 1.25\Omega$. The secondary control loop is initially chosen as $kp_{vdc} = 1, ki_{vdc} = 20, kp_{Is} = 0.03, ki_{vs} = 0.13$. The secondary control parameters are scheduled dynamically to compare the conventional and the developed technique in the same conditions.

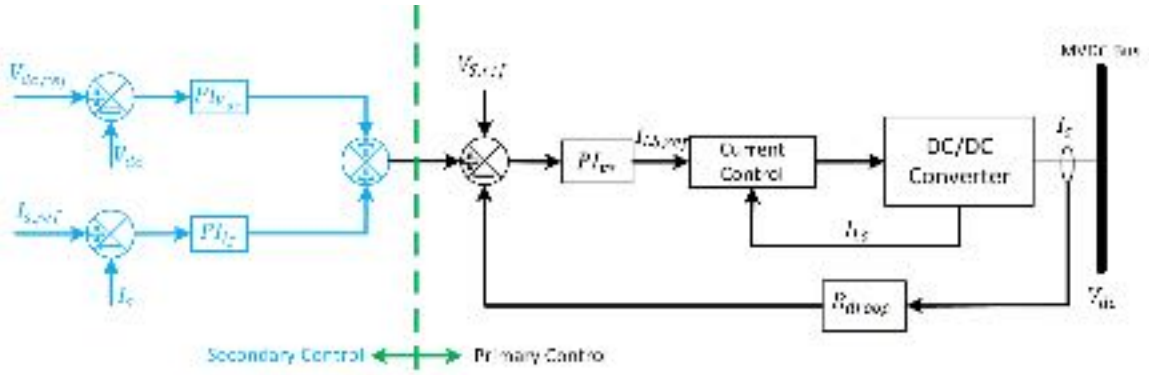


Figure 9.5: conventional control scheme of ESSs.

In this case study, our battery and supercapacitors controllers are designed with a sampling frequency of 0.5kHz and 2kHz, respectively. The developed MPC controller is designed by setting the prediction horizon window to 10 samples and the control horizon window to 1 sample. The simulation study and the processor in the loop implementation sampling frequency are 10kHz. In order to distribute the change in load compensation cooperatively, the LPF and the HPF are paired with a cutting frequency 125 rad/sec. These

chosen frequencies are adopted to adjust the battery and supercapacitor insertion time autonomously. Also, the HPF has another role in filtering the measurement error, which is usually static noise.

9.5.1 Scenario 1: Normal Operation

Starting with the previously mentioned initial conditions, Figure 9.6 illustrates a slow dynamic CPL change in loading and its effect on the MVDC bus after the reaction of the generation system and storage units` sharing. The studied system is exposed to a positive and negative change in the CPL load δI_{load} with the low ramping rate. A comparison between the voltage changes δV_{dc} and the change in generator sharing current δI_{Gen} of the developed SSMPC and the conventional PI is shown. Both voltage responses are good during normal changes.

Although the conventional PI has a better voltage response than the developed technique, the generator sharing is larger for the developed SSMPC, which keeps the healthy operation of the ESSs by reducing their sharing. The sharing of the storage units should increase, only when it is needed. The rest of the changes in the loading current is compensated with the BESSs because the generators become almost near to the full loading.

In this case, as shown in Table 9.1, one battery has 80% initial SOC while the other battery has 35%. The ability of the controller to stabilize the voltage and maintain a proper current contribution based on the available state of charge is also tested. Figure 9.6 depicts also the change in shared current and SOC of the two BESSs under this scenario.

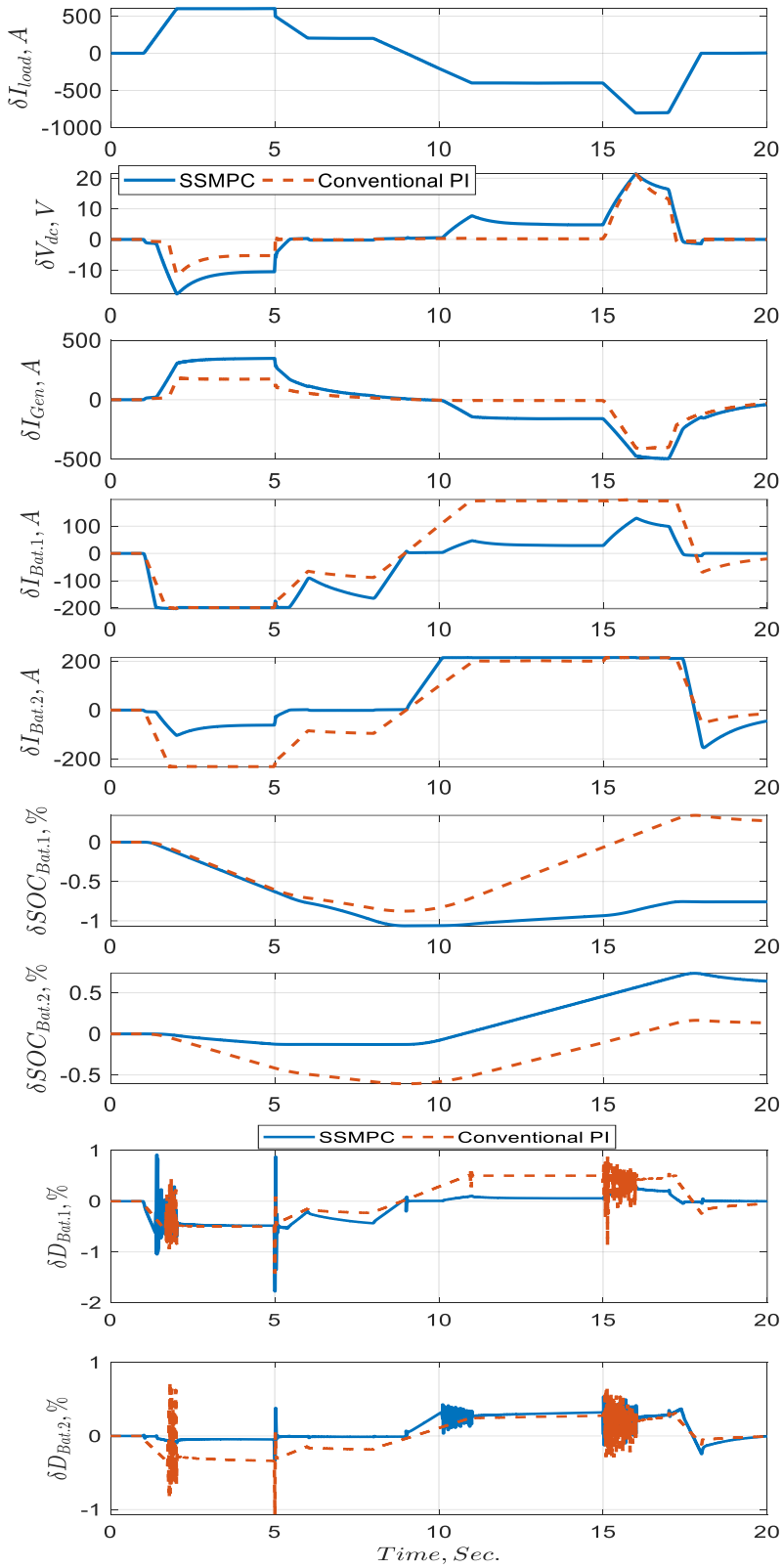


Figure 9.6: Scenario 1: normal operation.

The developed controller reveals that the injected current by Bat.1 is larger than the Bat.2 during the positive change in load while the absorbed power by Bat.2 is larger than the Bat.2 during the negative change. On the other hand, the conventional PI controller fails to adopt the current sharing based on the available state of charge. As shown, it derives the batteries to equally share the current change, which degrades the health of the two batteries. Figure 9.6 also shows Bat.1 that discharges faster than Bat.2 before t=9 Sec. After that, the charging rate of Bat.2 is higher. The changes in the switching duty of the two BESSs $\delta D_{Bat.1}$ and $\delta D_{Bat.2}$ are depicted. The figure shows a comparison between the generated set-points of the switching duty using the developed and the conventional controllers. The two controllers are designed with the same constraints to accurately justify the comparison. The SCESSs does not participate in this scenario, because the change in the load is not abrupt and the batteries can handle it. The advantages of taking the SOC into consideration ensures the ability of the developed controller to maintain the voltage stability, and properly share the change in the load among the distributed storage according to their SOC.

9.5.2 Scenario 2: Mission Operation

As shown in Figure 9.7, In this scenario, a mission is launched, the speed of the propellers (CPL) is slightly increased, and at t=12 Sec. a series of pulsed load (as railgun) is operated. Due to the CPL presence, the application of the conventional controller causes current oscillation and voltage collapse, which should initiate a trip signal for the system. In this scenario, it is assumed that the protection system is deactivated to show the difference between the conventional and the developed controllers.

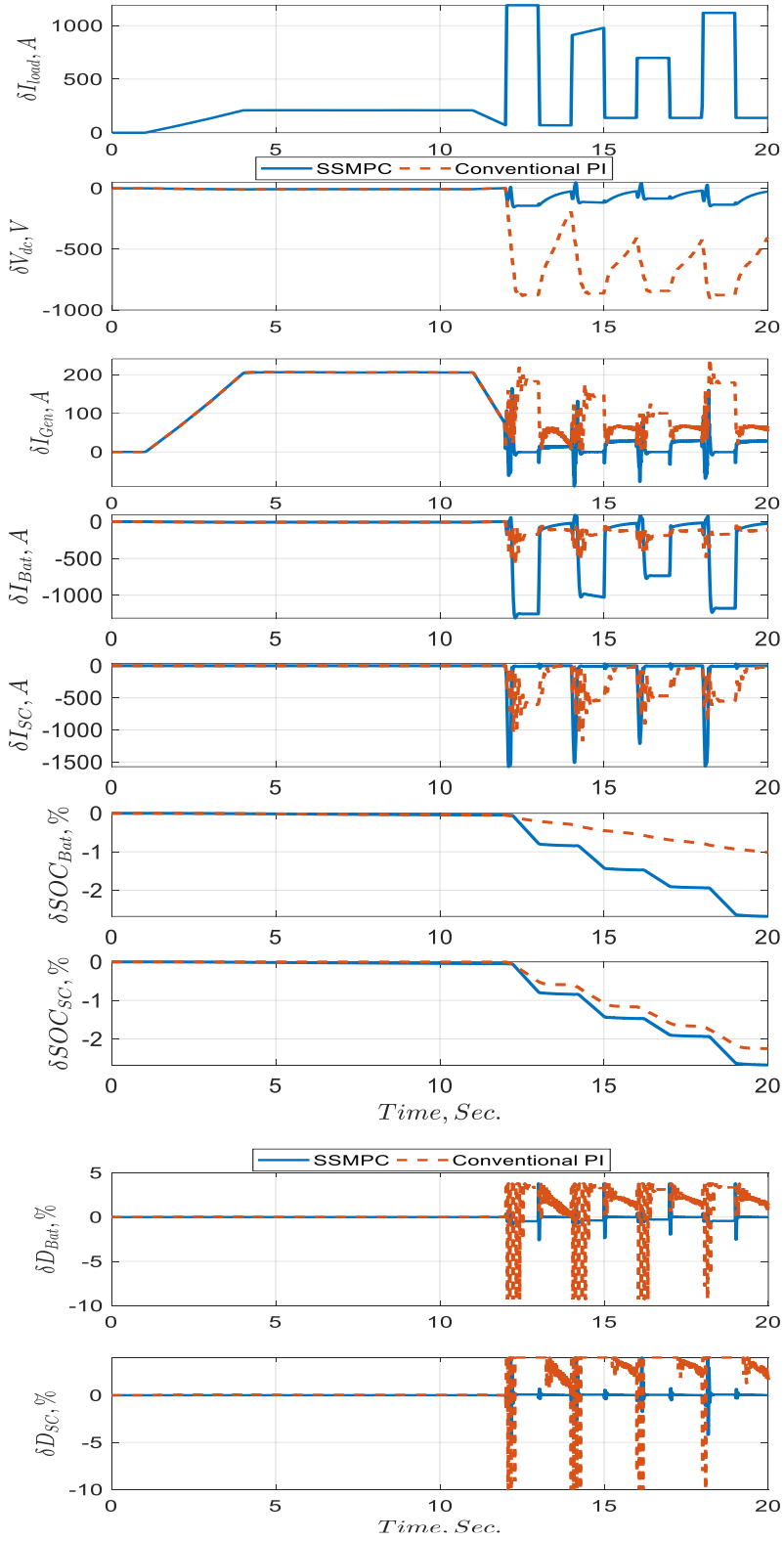


Figure 9.7: Scenario 2: mission operation

As illustrated, the voltage response before launching the pulsed load is approximately identical for both the developed and conventional techniques. After that, the significant load change causes a voltage collapse for the system when using the conventional PI controller. On the other hand, the MPC successfully controlled the system to stabilize the voltage with a drop of less than 3% in voltage. Figure 9.7 shows an identical generator sharing for both controllers before the pulsed load initiation. However, a careful look at the δI_{Gen} after 12 Sec., shows that the developed controller minimizes the generator current changes because it should not be engaged in the pulsed load changes. Nonetheless, the conventional controller fails to guide the generator output current, which causes current oscillation and voltage collapse. Unlike the conventional PI controller, the developed controller wisely manages the batteries and the supercapacitors insertion/removal. The supercapacitors inject the current during the ramping of the pulsed load. After that, the batteries inject the rest of the pulsed load current.

The amount of the injected currents is controlled to stabilize the voltage and consider the SOC of the ESSs. In contrast, the PI controller fails to control the ESSs and drive the systems away from stability. The batteries and the supercapacitors SOC comparison is shown in the same figure. It can be understood that the ESSs are fully utilized during the pulsed load and no transaction is recorded during the normal load change. Finally, Figure 9.7 displays the change in the switching duty of the DC/DC converters for both controllers and both storage types. Unlike the developed controller, the change in the switching duty cycle reached the maximum limits when the conventional controller is used, which show that the traditional controller fails to stabilize the system.

Since the MPC controller design depends mainly on the model, a sensitivity analysis has been done to illustrate the effect of the model parameters error on the controller design. Figure 8 shows the second scenario case study (no model error) and the impact of the error in the battery and supercapacitor converter's inductance. The inductance error range is tested between -50% to 100% of the actual inductance. In addition, the supercapacitor output filter error is tested by -90% of the actual value. Figure 9.8 shows the controller's model parameters error has a slight effect on the response of the results. The control features still the same even with a significant error in a parameter as the inductance.

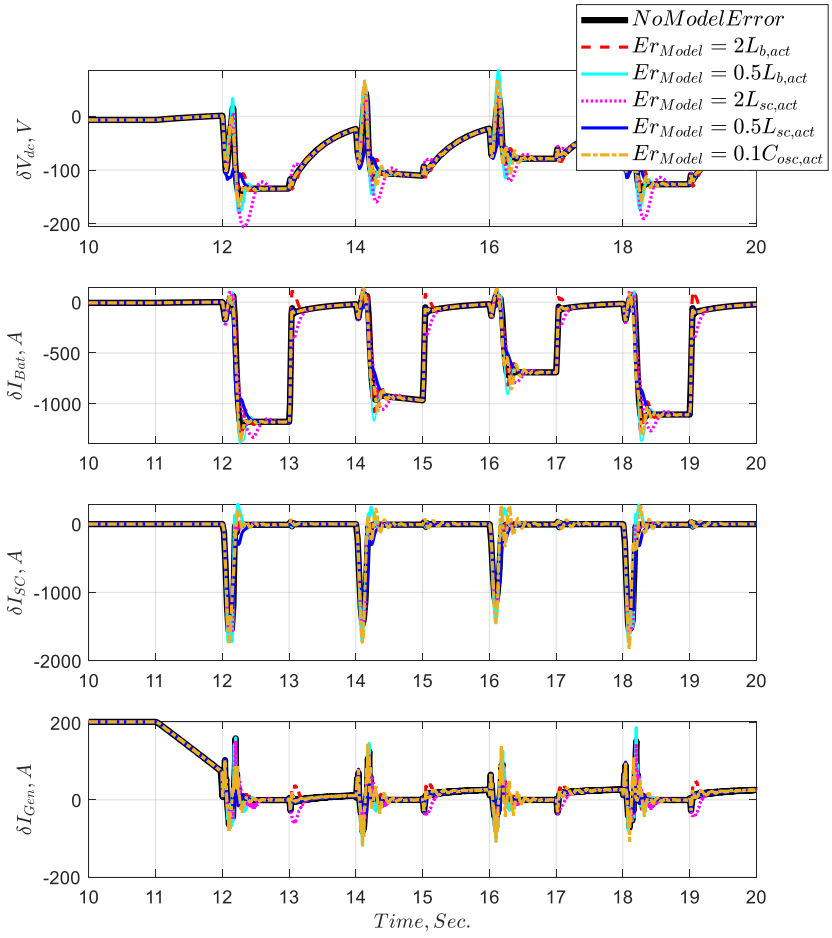


Figure 9.8: Sensitivity analysis for different model errors for scenario 2.

Under another condition, the MPC controller is tested with highly imposed noisy measurement. The voltage measurements of battery and supercapacitor controllers are injected with Gaussian noise as shown in Figure 9.9. As shown, the two controllers are equipped with paired LPF and HPF, which can easily isolate the high-frequency noise. The figure depicts a slight difference in the response as compared with the base case of the second scenario. For the supercapacitor operation logic, the 100ms hold is deactivated here in this test to clearly show the effect of the noise on the response.

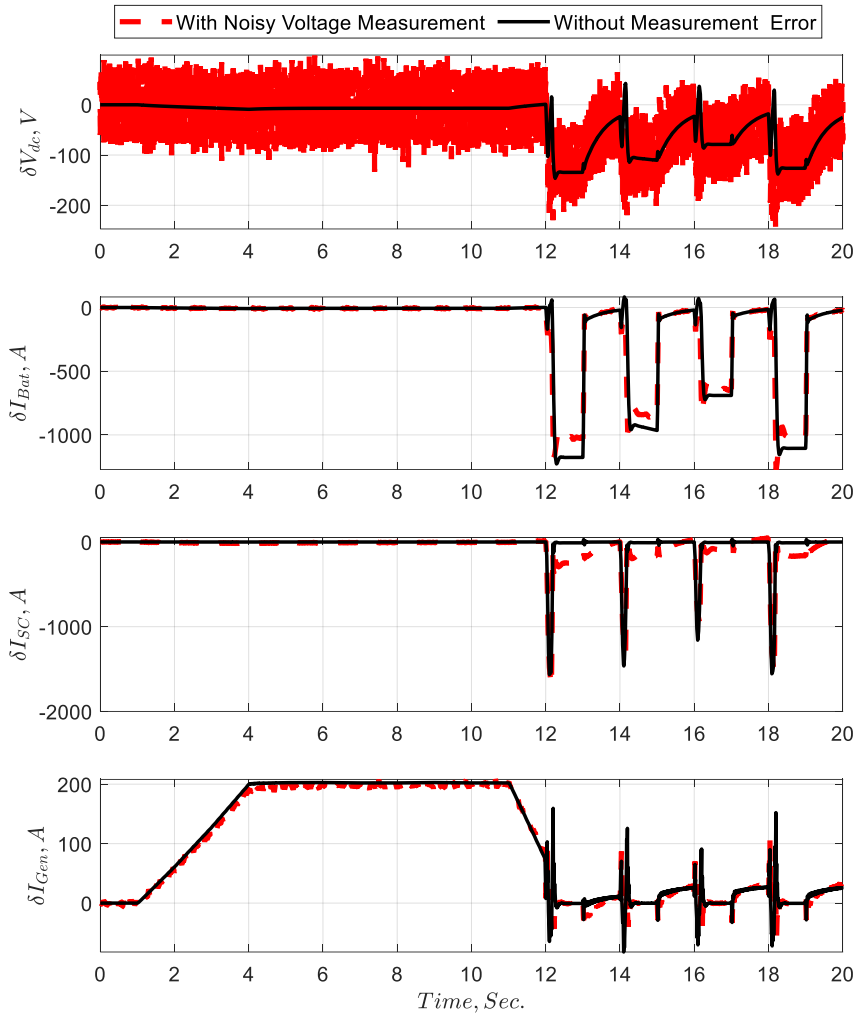


Figure 9.9: Sensitivity analysis for noisy voltage measurement error in scenario 2.

9.6 Processor in the Loop (PIL) Validation

To validate the feasibility of the controller implementation in the real-time application. The developed controllers are implemented through Processor in the loop using STM32F407 Discovery high-performance microcontroller while the MVDC system power models are on the MATLAB/SIMULINK. The board has an *ARM® Cortex-M4* 32-bit processor, 192-Kbyte RAM, up to 168 MHz frequency, 1-Mbyte flash memory, USB ST-LINK embedded debug tool. The board is supported by MATLAB/SIMULINK interconnection through the STMicroelectronics Embedded Coder. Figure 9.10 shows the PIL validation implementation. The batteries and supercapacitors controllers are implemented on the embedded system board while the rest of the model and the generator's controller is simulated in the MATLAB/SIMULINK environment. For each storage type, the C++ code of the operation logic and the MPC algorithms are generated by the embedded coder and sent to the board.

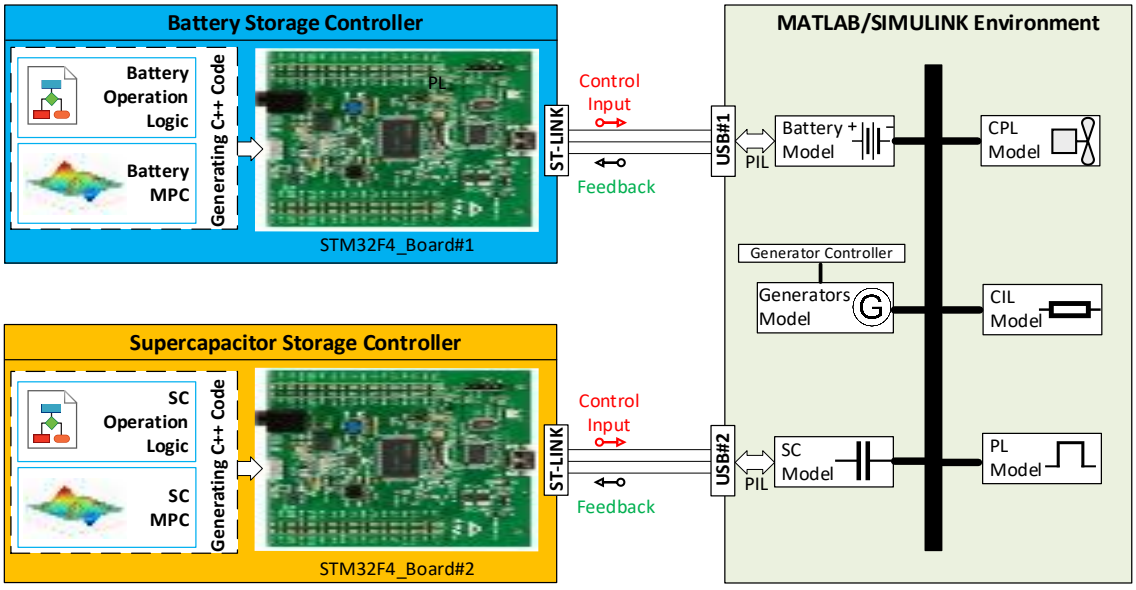


Figure 9.10: PIL controller's validation.

The control input instruction and the actual model feedback data transfers via the ST-LINK through the USB connection. In real-time, the two microcontrollers interact with the simulation process to satisfy the control law concerning each system model state. A comparison between the simulated controller's performance and the PIL-based controller for the second scenario is illustrated in Figure 9.11. The results show that PIL is successfully like the simulated controller behavior, which ensures the validity of the developed controller in the real-time application.

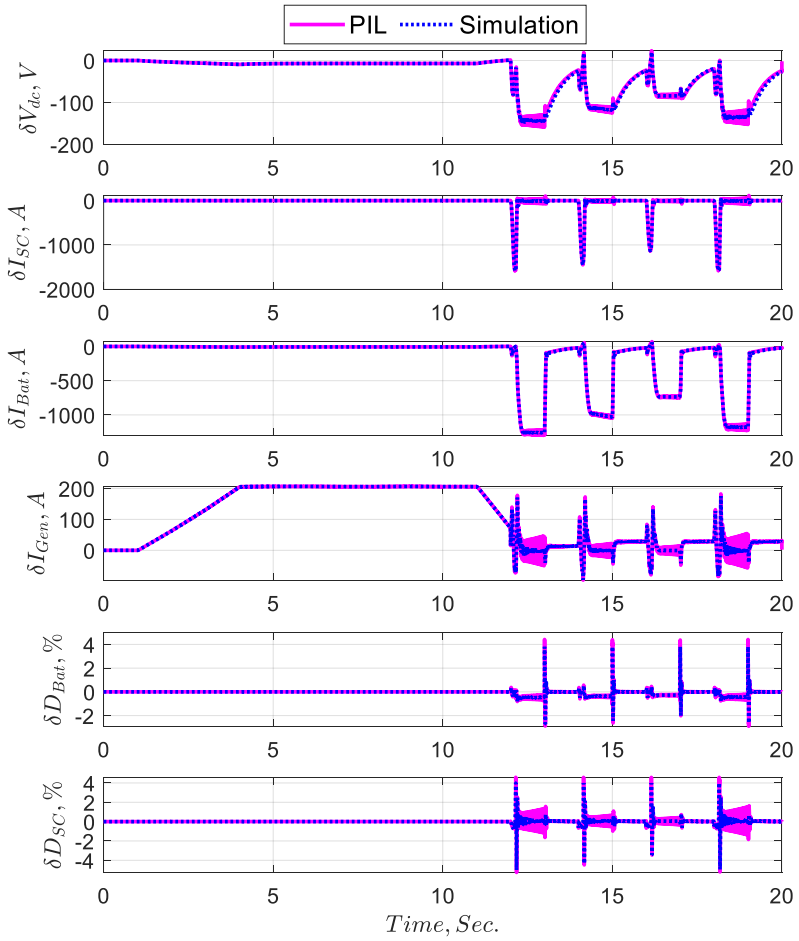


Figure 9.11: Scenario 2 validation by the PIL-based controller compared to the controller simulation.

9.7 Summary

This chapter developed a small signal modeling-based model predictive control to maintain the stability of the MVDC shipboard power system. The model includes the different types of loads ranging from the constant and pulsed loads to the regular hotel loads. Also, small-signal modeling of the generators and energy storage devices is considered. The MPC and its optimizer solve the problem to stabilize the voltage and maintain the sharing policy. The controller works in a decentralized way, which makes it robust as it depends only on the local measurement, especially for critical applications as shipboard power systems. The results show the superior performance of the controller under different loading conditions, where the controller can maintain the voltage stability and warrant the adequate operation of the storage devices.

Chapter 10 Conclusions and Recommendations for Future Work

10.1 Conclusions

This dissertation developed multiple defense lines for the smart grids against the cyberattacks on the networked control systems. The online data-informed model philosophy is utilized to give the energy cyber-physical system security awareness. These data-informed models are designed to be as the digital twin for not only the physical system but also for the cyber systems and their interactions. The developed methodologies provided an integrated solution to enhance the distributed microgrids/nanogrids security, resiliency, and reliability.

In the light of the centralized system architecture abilities, the centric oversight is aided with the digital twin to provide the security and the optimal control/optimization guidance to the distributed control layer. Then, a question has been asked (What if the communication between the centric layer and the distributed layer is failed or compromised?). Therefore, the distributed control layer is supported by adding a distributed security observer that watch the cyber system behavior to detect, identify and isolate the attack.

To guarantee a comprehensive resilient operation, the dissertation developed a decentralized autonomous control design that depends only on the local information without communication to respond to cyberattacks if the communication infrastructure is completely compromised. These solutions are not only enhanced the energy cyber system security but also strictly introduced stable control, optimal decision making and high robustness against uncertainty.

Unlike the current trend of applying the DT for the device level, the DT foundations for the unified cyber-physical system is developed. The emerging technologies in the energy sector as the internet of things, cloud computing, network-aware communication middleware and data-driven model are leveraged to transform the model usage from the study into life decision-making. A novel basis for the cyber-physical system digital twin definitions and mathematical formulation are introduced as the DT shadow, DT model, DT constructor and the DT playground. Also, the overall system architecture energy CPS digital twin is described to put a comprehensive vision for the DT future applications in the smart cities.

Since the dynamic model is a key element in the digital twin design, the CPS twin dynamic modelling structure and formulation are introduced. The DT model should be carefully designed to not only support the DT application/solution but also to has a simple structure, fast to run, require less information from the CPS layers and has a low computational burden.

Besides the theoretical foundations, the practical implementation of the digital twin is developed by introducing the CPS digital twin playground platform. This implementation illustrated how the energy CPS thing is provisioned, registered, and accessed on the cloud, which the hosting environment of the DT playground. Also, the building blocks of the platform as the DT constructor engine and the DT playground environment are created.

To validate the effectiveness of the CPS DT solution, it has been applied to guide the distributed energy management system to the optimal operation even during the uncertainty that is resulted from the high share of renewable energy penetration. The model predictive

control is designed based on the DT life clone to guarantee the global optimality agreement among the distributed coordination managers of the interconnected power system area. The centric oversight model is designed to be an aggregated model, which reduces the system complexity and reduce the dependence on heavy data from the CPS layer. This solution minimized the operation cost, maximized the profits, minimized the load shedding, and maximized renewable utilization.

To expand the DT based smart grid management capabilities and enhance the intelligence of the decision-making process, both the optimization problem and the DT model are supported by an online functionality to be self-adaptive with the changes in the power system status. The Analytical hierarchical process is used to autonomously adapt the DT model and the problem formulation to change the operation modes, which include maximum profit mode, contingency mode, and all-out renewable utilization mode. Due to the high uncertainty of the high share of renewable resources as solar and wind energy, the developed technique is introduced to balance a multi-objective optimization problem. Also, it considers the conventional resource physical competences as the minimum output limitations, the ramping rate capabilities, and cycling abilities.

Extra proof for the DT effectiveness of introducing out of the box solutions, the DT playground is used to build an application that watches the distributed control system cyber layer agents and authenticate the control decisions. The DT environment is reconfigured to host the security auditing solution on the cloud. Preselected distributed control agents and the networked sensors are provisioned on the cloud virtual space in the shadow to provide parallel Luenberger observer-based digital clones to authenticate the suspected activity that

is primarily flagged by the distributed control layer. Then, a logic conflict algorithm is used to compare the digital clones residues in real-time to discover the attacked control agent or sensor and then update the shadow states to inform the cyber system and guide the system toward the safe operation. This solution can provide security awareness to the cyber layer even with multi-coordinated attacks, which can include false data injection attacks and denial of service attacks.

For any reason, if the centralized layer (cloud virtual space) is not available, the distributed control layer should be able to respond to the cyberattacks. For this reason, a dynamical feature-based methodology is introduced to be implemented on each agent to discover the attack. This method depends on the change of the cyber graph dynamical feature and the consensus control features due to the cyberattack. An image processing tool named Mathematical Morphology is utilized to extract the dynamical feature from the agent's neighbor signals and compare it with the healthy dynamics. This method was able to detect, identify and mitigate the cyberattack on interconnected nanogrids.

As the last defense line, an autonomous decentralized control method is developed to work independently without remote information in case of a full communication failure. This method is applied for a critical isolated power system (Naval shipboard power system) because this kind of power systems failure is not an option. The small-signal model predictive control is used to grantee voltage stability, proper power-sharing among the generators, battery energy storage and supercapacitor energy storage. Even with the threat of losing the voltage stability by mixing the constant power load and the pulsed load

onboard, the non-communication-based control system was able to satisfy the control objective. This methodology is verified by the processor in the loop validation.

10.2 Recommendations for Future Work

This dissertation introduced the fundamental foundations of the Digital Twin design, implementation and developed many applications/solutions that exploit the DT playground. It covered many challenges to open avenues for future applications that can utilize the digital twin for the cyber-physical systems. Also, due to the special need for future multidisciplinary applications, it is recommended that the following topics be expanded by others:

- For the critical time applications, the synchronization between the CPS and the DT on the cloud should be studied. Many issues as edge-to-cloud communication latency, the data alignment for the online models and event synchronization should be studied for certain types of applications.
- A practical methodology for selecting the provisioned states from the CPS into the cloud is uncharged to scientifically performed by formulated optimization problem that can minimize the provisioned IoT devices and maximize the observability according to the applications.
- The deep-learning models should be built and integrated with the physical-based models to unleash the unlimited abilities of the DT in smart cities.
- Finding more realistic solutions for the power system restoration and reconfiguration during both the healthy state and during an emergency by depending on the DT What-IF analysis.

List of References

[1] J. Kabouris and F. D. Kanellos, “Impacts of Large-Scale Wind Penetration on Designing and Operation of Electric Power Systems,” *IEEE Trans. Sustain. Energy*, vol. 1, no. 2, pp. 107–114, Jul. 2010, doi: 10.1109/TSTE.2010.2050348.

[2] M. H. J. Bollen and F. Hassan, *Integration of Distributed Generation in the Power System*. John Wiley & Sons, 2011.

[3] S. Li and Y. Zheng, *Distributed Model Predictive Control for Plant-Wide Systems*. John Wiley & Sons, 2016.

[4] J. C. Vasquez, J. M. Guerrero, J. Miret, M. Castilla, and L. G. de Vicuña, “Hierarchical Control of Intelligent Microgrids,” *IEEE Ind. Electron. Mag.*, vol. 4, no. 4, pp. 23–29, Dec. 2010, doi: 10.1109/MIE.2010.938720.

[5] Z. Cheng, J. Duan, and M. Chow, “To Centralize or to Distribute: That Is the Question: A Comparison of Advanced Microgrid Management Systems,” *IEEE Ind. Electron. Mag.*, vol. 12, no. 1, pp. 6–24, Mar. 2018, doi: 10.1109/MIE.2018.2789926.

[6] F. Guo, C. Wen, J. Mao, G. Li, and Y.-D. Song, “A distributed hierarchical algorithm for multi-cluster constrained optimization,” *Automatica*, vol. 77, pp. 230–238, Mar. 2017, doi: 10.1016/j.automatica.2016.11.029.

[7] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, “Distributed Cooperative Control of DC Microgrids,” *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015, doi: 10.1109/TPEL.2014.2324579.

[8] S. S. Kia, B. V. Scoy, J. Cortes, R. A. Freeman, K. M. Lynch, and S. Martinez, “Tutorial on Dynamic Average Consensus: The Problem, Its Applications, and the Algorithms,” *IEEE Control Syst. Mag.*, vol. 39, no. 3, pp. 40–72, Jun. 2019, doi: 10.1109/MCS.2019.2900783.

[9] H. Yoo, T. Nguyen, and H. Kim, “Consensus-Based Distributed Coordination Control of Hybrid AC/DC Microgrids,” *IEEE Trans. Sustain. Energy*, vol. 11, no. 2, pp. 629–639, Apr. 2020, doi: 10.1109/TSTE.2019.2899119.

[10] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things," *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017, doi: 10.1109/MPEL.2017.2761422.

[11] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov. 2016, doi: 10.1109/TSG.2016.2542111.

[12] J. Duan and M. Chow, "A Resilient Consensus-Based Distributed Energy Management Algorithm Against Data Integrity Attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729–4740, Sep. 2019, doi: 10.1109/TSG.2018.2867106.

[13] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A Framework for Attack-Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration," *Proc. IEEE*, vol. 106, no. 1, pp. 113–128, Jan. 2018, doi: 10.1109/JPROC.2017.2725482.

[14] J. Duan and M. Chow, "A Novel Data Integrity Attack on Consensus-Based Distributed Energy Management Algorithm Using Local Information," *IEEE Trans. Ind. Inform.*, vol. 15, no. 3, pp. 1544–1553, Mar. 2019, doi: 10.1109/TII.2018.2851248.

[15] W. Zeng, Y. Zhang, and M. Chow, "Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 208–216, Feb. 2017, doi: 10.1109/TII.2015.2496228.

[16] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in Networked Microgrids Under Attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018, doi: 10.1109/TSG.2017.2721382.

[17] H. Zou, S. Mao, Y. Wang, F. Zhang, X. Chen, and L. Cheng, "A Survey of Energy Management in Interconnected Multi-Microgrids," *IEEE Access*, vol. 7, pp. 72158–72169, 2019, doi: 10.1109/ACCESS.2019.2920008.

[18] Y. Han, K. Zhang, H. Li, E. A. A. Coelho, and J. M. Guerrero, "MAS-Based Distributed Coordinated Control and Optimization in Microgrid and Microgrid

Clusters: A Comprehensive Overview," *IEEE Trans. Power Electron.*, vol. 33, no. 8, pp. 6488–6508, Aug. 2018, doi: 10.1109/TPEL.2017.2761438.

[19] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked Microgrids for Enhancing the Power System Resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1289–1310, Jul. 2017, doi: 10.1109/JPROC.2017.2685558.

[20] M. N. Alam, S. Chakrabarti, and A. Ghosh, "Networked Microgrids: State-of-the-Art and Future Perspectives," *IEEE Trans. Ind. Inform.*, vol. 15, no. 3, pp. 1238–1250, Mar. 2019, doi: 10.1109/TII.2018.2881540.

[21] M. H. Cintuglu, T. Youssef, and O. A. Mohammed, "Development and Application of a Real-Time Testbed for Multiagent System Interoperability: A Case Study on Hierarchical Microgrid Control," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1759–1768, May 2018, doi: 10.1109/TSG.2016.2599265.

[22] M. Pajic *et al.*, "Towards synthesis of platform-aware attack-resilient control systems: extended abstract," in *Proceedings of the 2nd ACM international conference on High confidence networked systems - HiCoNS '13*, Philadelphia, Pennsylvania, USA, 2013, p. 75, doi: 10.1145/2461446.2461457.

[23] V. Narayanan and S. Jagannathan, "Distributed adaptive optimal regulation of uncertain large-scale interconnected systems using hybrid Q-learning approach," *IET Control Theory Amp Appl.*, vol. 10, no. 12, pp. 1448–1457, Aug. 2016, doi: 10.1049/iet-cta.2015.0943.

[24] Y. Tang, S. Tasnim, N. Pissinou, S. S. Iyengar, and A. Shahid, "Reputation-Aware Data Fusion and Malicious Participant Detection in Mobile Crowdsensing," in *2018 IEEE International Conference on Big Data (Big Data)*, Dec. 2018, pp. 4820–4828, doi: 10.1109/BigData.2018.8622335.

[25] M. Cebe and K. Akkaya, "Efficient certificate revocation management schemes for IoT-based advanced metering infrastructures in smart cities," *Ad Hoc Netw.*, vol. 92, p. 101801, Sep. 2019, doi: 10.1016/j.adhoc.2018.10.027.

[26] A. Farraj, E. Hammad, and D. Kundur, "A Cyber-Physical Control Framework for Transient Stability in Smart Grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, Mar. 2018, doi: 10.1109/TSG.2016.2581588.

[27] S. L. Brunton and J. N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*. Cambridge University Press, 2019.

[28] B. Cheng, J. Zhang, G. P. Hancke, S. Karnouskos, and A. W. Colombo, "Industrial Cyberphysical Systems: Realizing Cloud-Based Big Data Infrastructures," *IEEE Ind. Electron. Mag.*, vol. 12, no. 1, pp. 25–35, Mar. 2018, doi: 10.1109/MIE.2017.2788850.

[29] J. Poon, P. Jain, I. C. Konstantakopoulos, C. Spanos, S. K. Panda, and S. R. Sanders, "Model-Based Fault Detection and Identification for Switching Power Converters," *IEEE Trans. Power Electron.*, vol. 32, no. 2, pp. 1419–1430, Feb. 2017, doi: 10.1109/TPEL.2016.2541342.

[30] Y. He, J. Guo, and X. Zheng, "From Surveillance to Digital Twin: Challenges and Recent Advances of Signal Processing for Industrial Internet of Things," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 120–129, Sep. 2018, doi: 10.1109/MSP.2018.2842228.

[31] K. M. Alam and A. E. Saddik, "C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems," *IEEE Access*, vol. 5, pp. 2050–2062, 2017, doi: 10.1109/ACCESS.2017.2657006.

[32] H. Laaki, Y. Miche, and K. Tammi, "Prototyping a Digital Twin for Real Time Remote Control Over Mobile Networks: Application of Remote Surgery," *IEEE Access*, vol. 7, pp. 20325–20336, 2019, doi: 10.1109/ACCESS.2019.2897018.

[33] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital Twin in Industry: State-of-the-Art," *IEEE Trans. Ind. Inform.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019, doi: 10.1109/TII.2018.2873186.

[34] A. Canedo, "Industrial IoT lifecycle via digital twins," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, New York, NY, USA, Oct. 2016, p. 1, doi: 10.1145/2968456.2974007.

[35] Y. Xu, Y. Sun, X. Liu, and Y. Zheng, "A Digital-Twin-Assisted Fault Diagnosis Using Deep Transfer Learning," *IEEE Access*, vol. 7, pp. 19990–19999, 2019, doi: 10.1109/ACCESS.2018.2890566.

[36] “Getting started with AWS IoT Core - AWS IoT Core.” https://docs.aws.amazon.com/iot/latest/developerguide/iot-gs.html (accessed Jan. 13, 2021).

[37] B. N. Silva, M. Khan, and K. Han, “Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities,” *Sustain. Cities Soc.*, vol. 38, pp. 697–713, Apr. 2018, doi: 10.1016/j.scs.2018.01.053.

[38] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, “Smart cities: Advances in research—An information systems perspective,” *Int. J. Inf. Manag.*, vol. 47, pp. 88–100, Aug. 2019, doi: 10.1016/j.ijinfomgt.2019.01.004.

[39] P. A. Østergaard and P. C. Maestosi, “Tools, technologies and systems integration for the Smart and Sustainable Cities to come,” *Int. J. Sustain. Energy Plan. Manag.*, vol. 24, Oct. 2019, doi: 10.5278/ijsepm.3405.

[40] B. P. Bhattarai *et al.*, “Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions,” *IET Smart Grid*, vol. 2, no. 2, pp. 141–154, Feb. 2019, doi: 10.1049/iet-stg.2018.0261.

[41] C. Anderton, “Challenges and Benefits of Implementing a Digital Twin in Composites Manufacturing,” p. 13.

[42] “IoT platforms for the Mining Industry: An Overview - Inżynieria Mineralna - Tom R. 21, nr 1 (2019) - BazTech - Yadda.” http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-598fed15-b1cc-4a34-a7d2-ed2db91d1f5d (accessed Jan. 16, 2021).

[43] M. de Sousa, “The Beremiz PLC: Adding Support for Industrial Communication Protocols,” in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2019, pp. 232–239, doi: 10.1109/ETFA.2019.8869526.

[44] E. Glaessgen and D. Stargel, “The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles,” in *53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, American Institute of Aeronautics and Astronautics.

[45] Ó. Gonzales-Zurita, J.-M. Clairand, E. Peñalvo-López, and G. Escrivá-Escrivá, "Review on Multi-Objective Control Strategies for Distributed Generation on Inverter-Based Microgrids," *Energies*, vol. 13, no. 13, Art. no. 13, Jan. 2020, doi: 10.3390/en13133483.

[46] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015, doi: 10.1016/j.mfglet.2014.12.001.

[47] J. Holler, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, *Internet of Things*. Academic Press, 2014.

[48] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328.

[49] M. Hussein, A. I. Galal, E. Abd-Elrahman, and M. Zorkany, "Internet of Things (IoT) Platform for Multi-Topic Messaging," *Energies*, vol. 13, no. 13, Art. no. 13, Jan. 2020, doi: 10.3390/en13133346.

[50] M. Shakeri *et al.*, "An Autonomous Home Energy Management System Using Dynamic Priority Strategy in Conventional Homes," *Energies*, vol. 13, no. 13, Art. no. 13, Jan. 2020, doi: 10.3390/en13133312.

[51] J. Oh, "IoT-Based Smart Plug for Residential Energy Conservation: An Empirical Study Based on 15 Months' Monitoring," *Energies*, vol. 13, no. 15, Art. no. 15, Jan. 2020, doi: 10.3390/en13154035.

[52] A. Tsipis, A. Papamichail, I. Angelis, G. Koufoudakis, G. Tsoumanis, and K. Oikonomou, "An Alertness-Adjustable Cloud/Fog IoT Solution for Timely Environmental Monitoring Based on Wildfire Risk Forecasting," *Energies*, vol. 13, no. 14, Art. no. 14, Jan. 2020, doi: 10.3390/en13143693.

[53] I. Machorro-Cano, G. Alor-Hernández, M. A. Paredes-Valverde, L. Rodríguez-Mazahua, J. L. Sánchez-Cervantes, and J. O. Olmedo-Aguirre, "HEMS-IoT: A Big Data and Machine Learning-Based Smart Home System for Energy Saving," *Energies*, vol. 13, no. 5, Art. no. 5, Jan. 2020, doi: 10.3390/en13051097.

[54] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, “Internet of Things (IoT) and the Energy Sector,” *Energies*, vol. 13, no. 2, Art. no. 2, Jan. 2020, doi: 10.3390/en13020494.

[55] K. Vatanparvar and M. A. Al Faruque, “Control-as-a-Service in Cyber-Physical Energy Systems over Fog Computing,” in *Fog Computing in the Internet of Things: Intelligence at the Edge*, A. M. Rahmani, P. Liljeberg, J.-S. Preden, and A. Jantsch, Eds. Cham: Springer International Publishing, 2018, pp. 123–144.

[56] K. Josifovska, E. Yigitbas, and G. Engels, “Reference Framework for Digital Twins within Cyber-Physical Systems,” in *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, May 2019, pp. 25–31, doi: 10.1109/SEsCPS.2019.00012.

[57] C. Gehrmann and M. Gunnarsson, “A Digital Twin Based Industrial Automation and Control System Security Architecture,” *IEEE Trans. Ind. Inform.*, vol. 16, no. 1, pp. 669–680, Jan. 2020, doi: 10.1109/TII.2019.2938885.

[58] A. J. Calderón Godoy and I. Pérez, “Design and Implementation of Smart Micro-Grid and Its Digital Replica: First Steps:,” in *Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics*, Prague, Czech Republic, 2019, pp. 715–721, doi: 10.5220/0007923707150721.

[59] S. Sahoo and S. Mishra, “An Adaptive Event-Triggered Communication-Based Distributed Secondary Control for DC Microgrids,” *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, Nov. 2018, doi: 10.1109/TSG.2017.2717936.

[60] N. M. Dehkordi and S. Z. Moussavi, “Distributed Resilient Adaptive Control of Islanded Microgrids Under Sensor/Actuator Faults,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2699–2708, May 2020, doi: 10.1109/TSG.2019.2960205.

[61] Y. Liu, H. B. Gooi, Y. Li, H. Xin, and J. Ye, “A Secure Distributed Transactive Energy Management Scheme for Multiple Interconnected Microgrids Considering Misbehaviors,” *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5975–5986, Nov. 2019, doi: 10.1109/TSG.2019.2895229.

[62] M. Kriegleder, “A Correction to Algorithm A2 in ‘Asynchronous Distributed Averaging on Communication Networks,’” *IEEEACM Trans. Netw.*, vol. 22, no. 6, pp. 2026–2027, Dec. 2014, doi: 10.1109/TNET.2013.2292800.

[63] “Raspberry Pi Documentation.” https://www.raspberrypi.org/documentation/ (accessed Jan. 18, 2021).

[64] “Documentation | Data Distribution Service (DDS) Community RTI Connext Users.” https://community.rti.com/documentation (accessed Jan. 18, 2021).

[65] “AWS IoT Core - Developer Guide,” p. 1013.

[66] D. Halamay, M. Antonishen, K. Lajoie, A. Bostrom, and T. K. A. Brekken, “Improving Wind Farm Dispatchability Using Model Predictive Control for Optimal Operation of Grid-Scale Energy Storage,” *Energies*, vol. 7, no. 9, Art. no. 9, Sep. 2014, doi: 10.3390/en7095847.

[67] P. A. Jonas and D. A. Ulbig, “Predictive power dispatch for 100% renewable electricity scenarios using power nodes modeling framework,” 2011.

[68] M. Vrakopoulou, “Optimal decision making for secure and economic operation of power systems under uncertainty,” ETH Zurich, 2013.

[69] L. Park, Y. Jang, S. Cho, and J. Kim, “Residential Demand Response for Renewable Energy Resources in Smart Grid Systems,” *IEEE Trans. Ind. Inform.*, vol. 13, no. 6, pp. 3165–3173, Dec. 2017, doi: 10.1109/TII.2017.2704282.

[70] J. Shen and A. Khaligh, “Design and Real-Time Controller Implementation for a Battery-Ultracapacitor Hybrid Energy Storage System,” *IEEE Trans. Ind. Inform.*, vol. 12, no. 5, pp. 1910–1918, Oct. 2016, doi: 10.1109/TII.2016.2575798.

[71] R. Scattolini, “Architectures for distributed and hierarchical Model Predictive Control – A review,” *J. Process Control*, vol. 19, no. 5, pp. 723–731, May 2009, doi: 10.1016/j.jprocont.2009.02.003.

[72] Z. Hashemi, A. Ramezani, and M. P. Moghaddam, “Energy hub management by using decentralized robust model predictive control,” in *2016 4th International Conference on Control, Instrumentation, and Automation (ICCIA)*, Jan. 2016, pp. 105–110, doi: 10.1109/ICCIAutom.2016.7483144.

[73] A. J. del Real, A. Arce, and C. Bordons, “Combined environmental and economic dispatch of smart grids using distributed model predictive control,” *Int. J. Electr.*

Power Energy Syst., vol. 54, pp. 65–76, Jan. 2014, doi: 10.1016/j.ijepes.2013.06.035.

[74] S. Salinas, M. Li, P. Li, and Y. Fu, "Dynamic Energy Management for the Smart Grid With Distributed Energy Resources," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 2139–2151, Dec. 2013, doi: 10.1109/TSG.2013.2265556.

[75] Y. Xu, W. Zhang, and W. Liu, "Distributed Dynamic Programming-Based Approach for Economic Dispatch in Smart Grids," *IEEE Trans. Ind. Inform.*, vol. 11, no. 1, pp. 166–175, Feb. 2015, doi: 10.1109/TII.2014.2378691.

[76] W. Zhang, Y. Ma, W. Liu, S. J. Ranade, and Y. Luo, "Distributed Optimal Active Power Dispatch Under Constraints for Smart Grids," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5084–5094, Jun. 2017, doi: 10.1109/TIE.2016.2617821.

[77] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Decentralized Cloud-SDN Architecture in Smart Grid: A Dynamic Pricing Model," *IEEE Trans. Ind. Inform.*, vol. 14, no. 3, pp. 1220–1231, Mar. 2018, doi: 10.1109/TII.2017.2742147.

[78] B. T. Stewart, A. N. Venkat, J. B. Rawlings, S. J. Wright, and G. Pannocchia, "Cooperative distributed model predictive control," *Syst. Control Lett.*, vol. 59, no. 8, pp. 460–469, Aug. 2010, doi: 10.1016/j.sysconle.2010.06.005.

[79] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright, "Distributed MPC Strategies With Application to Power System Automatic Generation Control," *IEEE Trans. Control Syst. Technol.*, vol. 16, no. 6, pp. 1192–1206, Nov. 2008, doi: 10.1109/TCST.2008.919414.

[80] A. J. del Real, A. Arce, and C. Bordons, "An Integrated Framework for Distributed Model Predictive Control of Large-Scale Power Networks," *IEEE Trans. Ind. Inform.*, vol. 10, no. 1, pp. 197–209, Feb. 2014, doi: 10.1109/TII.2013.2273877.

[81] Y. Zhang and S. Li, "Networked model predictive control based on neighbourhood optimization for serially connected large-scale processes," *J. Process Control*, vol. 17, no. 1, pp. 37–50, Jan. 2007, doi: 10.1016/j.jprocont.2006.08.009.

[82] "Distributed Model Predictive Control of Nonlinear Systems Based on Price-Driven Coordination | Industrial & Engineering Chemistry Research." https://pubs.acs.org/doi/abs/10.1021/acs.iecr.6b01862 (accessed Jan. 22, 2021).

[83] V. Loia, V. Terzija, A. Vaccaro, and P. Wall, “An Affine-Arithmetic-Based Consensus Protocol for Smart-Grid Computing in the Presence of Data Uncertainties,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 5, pp. 2973–2982, May 2015, doi: 10.1109/TIE.2014.2363046.

[84] D. Wang, M. Glavic, and L. Wehenkel, “Comparison of centralized, distributed and hierarchical model predictive control schemes for electromechanical oscillations damping in large-scale power systems,” *Int. J. Electr. Power Energy Syst.*, vol. 58, pp. 32–41, Jun. 2014, doi: 10.1016/j.ijepes.2014.01.007.

[85] B. T. Stewart, J. B. Rawlings, and S. J. Wright, “Hierarchical cooperative distributed model predictive control,” in *Proceedings of the 2010 American Control Conference*, Jun. 2010, pp. 3963–3968, doi: 10.1109/ACC.2010.5530634.

[86] J. Hu, J. Cao, and T. Yong, “Multi-level dispatch control architecture for power systems with demand-side resources,” *IET Gener. Transm. Amp Distrib.*, vol. 9, no. 16, pp. 2799–2810, Dec. 2015, doi: 10.1049/iet-gtd.2015.0232.

[87] H. Sildir, Y. Arkun, B. Cakal, D. Gokce, and E. Kuzu, “Plant-wide hierarchical optimization and control of an industrial hydrocracking process,” *J. Process Control*, vol. 23, no. 9, pp. 1229–1240, Oct. 2013, doi: 10.1016/j.jprocont.2013.07.007.

[88] X. Kong, X. Liu, and K. Y. Lee, “An Effective Nonlinear Multivariable HMPC for USC Power Plant Incorporating NFN-Based Modeling,” *IEEE Trans. Ind. Inform.*, vol. 12, no. 2, pp. 555–566, Apr. 2016, doi: 10.1109/TII.2016.2520579.

[89] M. Manbachi *et al.*, “Real-Time Co-Simulation Platform for Smart Grid Volt-VAR Optimization Using IEC 61850,” *IEEE Trans. Ind. Inform.*, vol. 12, no. 4, pp. 1392–1402, Aug. 2016, doi: 10.1109/TII.2016.2569586.

[90] T. A. Youssef, M. E. Hariri, A. T. Elsayed, and O. A. Mohammed, “A DDS-Based Energy Management Framework for Small Microgrid Operation and Control,” *IEEE Trans. Ind. Inform.*, vol. 14, no. 3, pp. 958–968, Mar. 2018, doi: 10.1109/TII.2017.2756619.

[91] “Generation.” http://www.ercot.com/gridinfo/generation (accessed Jan. 22, 2021).

[92] K. W. Cheung and R. Rios-Zalapa, “Smart dispatch for large grid operations with integrated renewable resources,” in *ISGT 2011*, Jan. 2011, pp. 1–7, doi: 10.1109/ISGT.2011.5759143.

[93] K. Heussen, S. Koch, A. Ulbig, and G. Andersson, “Unified System-Level Modeling of Intermittent Renewable Energy Sources and Energy Storage for Power System Operation,” *IEEE Syst. J.*, vol. 6, no. 1, pp. 140–151, Mar. 2012, doi: 10.1109/JSYST.2011.2163020.

[94] Y. Zong, D. Kullmann, A. Thavlov, O. Gehrke, and H. W. Bindner, “Application of Model Predictive Control for Active Load Management in a Distributed Power System With High Wind Penetration,” *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 1055–1062, Jun. 2012, doi: 10.1109/TSG.2011.2177282.

[95] S. Salinas, M. Li, and P. Li, “Multi-Objective Optimal Energy Consumption Scheduling in Smart Grids,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 341–348, Mar. 2013, doi: 10.1109/TSG.2012.2214068.

[96] D. Zhu and G. Hug, “Decomposed Stochastic Model Predictive Control for Optimal Dispatch of Storage and Generation,” *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 2044–2053, Jul. 2014, doi: 10.1109/TSG.2014.2321762.

[97] F. Guo, C. Wen, J. Mao, and Y. Song, “Distributed Economic Dispatch for Smart Grids With Random Wind Power,” *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1572–1583, May 2016, doi: 10.1109/TSG.2015.2434831.

[98] Q. Jiang, M. Xue, and G. Geng, “Energy Management of Microgrid in Grid-Connected and Stand-Alone Modes,” *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3380–3389, Aug. 2013, doi: 10.1109/TPWRS.2013.2244104.

[99] M. Elsied, A. Oukaour, H. Gualous, and R. Hassan, “Energy management and optimization in microgrid system based on green energy,” *Energy*, vol. 84, pp. 139–151, May 2015, doi: 10.1016/j.energy.2015.02.108.

[100] H. Ye and Y. Liu, “Design of model predictive controllers for adaptive damping of inter-area oscillations,” *Int. J. Electr. Power Energy Syst.*, vol. 45, no. 1, pp. 509–518, Feb. 2013, doi: 10.1016/j.ijepes.2012.09.023.

[101] P. D. Christofides, R. Scattolini, D. Muñoz de la Peña, and J. Liu, "Distributed model predictive control: A tutorial review and future research directions," *Comput. Chem. Eng.*, vol. 51, pp. 21–41, Apr. 2013, doi: 10.1016/j.compchemeng.2012.05.011.

[102] A. Bemporad, M. Morari, and N. L. Ricker, "Model Predictive Control Toolbox™ User's Guide," MathWorks, Working Paper, 2004. Accessed: Jan. 25, 2021. [Online]. Available: http://eprints.imtlucca.it/628/.

[103] A. A. S. Shetaya, R. El-Azab, A. Amin, and O. H. Abdalla, "Flexibility Measurement of Power System Generation for Real-Time Applications Using Analytical Hierarchy Process," in *2018 IEEE Green Technologies Conference (GreenTech)*, Apr. 2018, pp. 7–14, doi: 10.1109/GreenTech.2018.00011.

[104] R. D. Zimmerman and C. E. Murillo-Sanchez, "Matpower 6.0 User's Manual," p. 205.

[105] A. Saad, T. Youssef, A. T. Elsayed, A. Amin, O. H. Abdalla, and O. Mohammed, "Data-Centric Hierarchical Distributed Model Predictive Control for Smart Grid Energy Management," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4086–4098, Jul. 2019, doi: 10.1109/TII.2018.2883911.

[106] R. Moghaddass, O. A. Mohammed, E. Skordilis, and S. Asfour, "Smart Control of Fleets of Electric Vehicles in Smart and Connected Communities," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6883–6897, Nov. 2019, doi: 10.1109/TSG.2019.2913587.

[107] M. H. Y. Moghaddam and A. Leon-Garcia, "A fog-based internet of energy architecture for transactive energy management systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1055–1069, Apr. 2018, doi: 10.1109/JIOT.2018.2805899.

[108] D. W. Cearley, B. Burke, S. Searle, and M. J. Walker, "Top 10 Strategic Technology Trends for 2018," p. 24.

[109] M. M. Shabestary and Y. A. I. Mohamed, "Autonomous Coordinated Control Scheme for Cooperative Asymmetric Low-Voltage Ride-Through and Grid Support in Active Distribution Networks With Multiple DG Units," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2125–2139, May 2020, doi: 10.1109/TSG.2019.2948131.

[110] A. A. Saad, S. Faddel, and O. Mohammed, “A secured distributed control system for future interconnected smart grids,” *Appl. Energy*, vol. 243, pp. 57–70, Jun. 2019, doi: 10.1016/j.apenergy.2019.03.185.

[111] M. Yazdanian and A. Mehrizi-Sani, “Distributed Control Techniques in Microgrids,” *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2901–2909, Nov. 2014, doi: 10.1109/TSG.2014.2337838.

[112] H. Zhang, S. Kim, Q. Sun, and J. Zhou, “Distributed Adaptive Virtual Impedance Control for Accurate Reactive Power Sharing Based on Consensus Control in Microgrids,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1749–1761, Jul. 2017, doi: 10.1109/TSG.2015.2506760.

[113] X. Wu *et al.*, “A Two-Layer Distributed Cooperative Control Method for Islanded Networked Microgrid Systems,” *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 942–957, Mar. 2020, doi: 10.1109/TSG.2019.2928330.

[114] L. Yang, Y. Zhao, C. Wang, P. Gao, and J. Hao, “Resilience-Oriented Hierarchical Service Restoration in Distribution System Considering Microgrids,” *IEEE Access*, vol. 7, pp. 152729–152743, 2019, doi: 10.1109/ACCESS.2019.2948372.

[115] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, “Detection and Mitigation of Data Manipulation Attacks in AC Microgrids,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020, doi: 10.1109/TSG.2019.2958014.

[116] R. Deng, P. Zhuang, and H. Liang, “CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid,” *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017, doi: 10.1109/TSG.2017.2702125.

[117] Y. Kim, V. Kolesnikov, and M. Thottan, “Resilient End-to-End Message Protection for Cyber-Physical System Communications,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2478–2487, Jul. 2018, doi: 10.1109/TSG.2016.2613545.

[118] D. Zhang, L. Liu, and G. Feng, “Consensus of Heterogeneous Linear Multiagent Systems Subject to Aperiodic Sampled-Data and DoS Attack,” *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019, doi: 10.1109/TCYB.2018.2806387.

[119] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and Sensitivity Study of Consensus Algorithm-Based Distributed Hierarchical Control for DC Microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016, doi: 10.1109/TSG.2015.2422714.

[120] F. Wei, Z. Wan, and H. He, "Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020, doi: 10.1109/TSG.2019.2956161.

[121] G. Bachelor, E. Brusa, D. Ferretto, and A. Mitschke, "Model-Based Design of Complex Aeronautical Systems Through Digital Twin and Thread Concepts," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1568–1579, Jun. 2020, doi: 10.1109/JSYST.2019.2925627.

[122] B. D. Schutter, "Minimal state-space realization in linear system theory: an overview," *J. Comput. Appl. Math.*, vol. 121, no. 1, pp. 331–354, Sep. 2000, doi: 10.1016/S0377-0427(00)00341-1.

[123] W. Chen, W. Chen, M. Saif, M. Li, and H. Wu, "Simultaneous Fault Isolation and Estimation of Lithium-Ion Batteries via Synthesized Design of Luenberger and Learning Observers," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 1, pp. 290–298, Jan. 2014, doi: 10.1109/TCST.2013.2239296.

[124] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, "AC-microgrids versus DC-microgrids with distributed energy resources: A review," *Renew. Sustain. Energy Rev.*, vol. 24, pp. 387–405, Aug. 2013, doi: 10.1016/j.rser.2013.03.067.

[125] E. O'Shaughnessy, D. Cutler, K. Ardani, and R. Margolis, "Solar plus: A review of the end-user economics of solar PV integration with storage and load control in residential buildings," *Appl. Energy*, vol. 228, pp. 2165–2175, Oct. 2018, doi: 10.1016/j.apenergy.2018.07.048.

[126] D. Burmester, R. Rayudu, W. Seah, and D. Akinyele, "A review of nanogrid topologies and technologies," *Renew. Sustain. Energy Rev.*, vol. 67, pp. 760–775, Jan. 2017, doi: 10.1016/j.rser.2016.09.073.

[127] A. M. Shotorbani, B. Mohammadi-Ivatloo, L. Wang, S. Ghassem-Zadeh, and S. H. Hosseini, "Distributed secondary control of battery energy storage systems in a

stand-alone microgrid," *IET Gener. Transm. Amp Distrib.*, vol. 12, no. 17, pp. 3944–3953, Jul. 2018, doi: 10.1049/iet-gtd.2018.0105.

[128] J. Schonbergerschonberger, R. Duke, and S. D. Round, "DC-Bus Signaling: A Distributed Control Strategy for a Hybrid Renewable Nanogrid," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1453–1460, Oct. 2006, doi: 10.1109/TIE.2006.882012.

[129] Y. Li, P. Zhang, and M. Yue, "Networked microgrid stability through distributed formal analysis," *Appl. Energy*, vol. 228, pp. 279–288, Oct. 2018, doi: 10.1016/j.apenergy.2018.06.038.

[130] S. Sahoo, D. Pullaguram, S. Mishra, J. Wu, and N. Senroy, "A containment based distributed finite-time controller for bounded voltage regulation & proportionate current sharing in DC microgrids," *Appl. Energy*, vol. 228, pp. 2526–2538, Oct. 2018, doi: 10.1016/j.apenergy.2018.06.081.

[131] A. I. Stasiuk, R. V. Hryshchuk, and L. L. Goncharova, "A Mathematical Cybersecurity Model of a Computer Network for the Control of Power Supply of Traction Substations," *Cybern. Syst. Anal.*, vol. 53, no. 3, pp. 476–484, May 2017, doi: 10.1007/s10559-017-9949-z.

[132] D. Tellbach and Y.-F. Li, "Cyber-Attacks on Smart Meters in Household Nanogrid: Modeling, Simulation and Analysis," *Energies*, vol. 11, no. 2, Art. no. 2, Feb. 2018, doi: 10.3390/en11020316.

[133] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Appl. Energy*, vol. 235, pp. 204–218, Feb. 2019, doi: 10.1016/j.apenergy.2018.10.077.

[134] L. Ren *et al.*, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Appl. Energy*, vol. 210, pp. 1251–1265, Jan. 2018, doi: 10.1016/j.apenergy.2017.06.006.

[135] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed Control Systems for Small-Scale Power Networks: Using Multiagent Cooperative Control Theory," *IEEE Control Syst. Mag.*, vol. 34, no. 6, pp. 56–77, Dec. 2014, doi: 10.1109/MCS.2014.2350571.

[136] M. F. Roslan, M. A. Hannan, P. J. Ker, and M. N. Uddin, “Microgrid control methods toward achieving sustainable energy management,” *Appl. Energy*, vol. 240, pp. 583–607, Apr. 2019, doi: 10.1016/j.apenergy.2019.02.070.

[137] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, “Energy Demand Side Management within micro-grid networks enhanced by blockchain,” *Appl. Energy*, vol. 228, pp. 1385–1398, Oct. 2018, doi: 10.1016/j.apenergy.2018.07.012.

[138] G. Liu, T. Jiang, T. B. Ollis, X. Zhang, and K. Tomsovic, “Distributed energy management for community microgrids considering network operational constraints and building thermal dynamics,” *Appl. Energy*, vol. 239, pp. 83–95, Apr. 2019, doi: 10.1016/j.apenergy.2019.01.210.

[139] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, “Heterogeneous ad hoc networks: Architectures, advances and challenges,” *Ad Hoc Netw.*, vol. 55, pp. 143–152, Feb. 2017, doi: 10.1016/j.adhoc.2016.11.001.

[140] M. Jin, J. Lavaei, and K. H. Johansson, “Power Grid AC-Based State Estimation: Vulnerability Analysis Against Cyber Attacks,” *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 1784–1799, May 2019, doi: 10.1109/TAC.2018.2852774.

[141] P. Soille, *Morphological Image Analysis: Principles and Applications*, 2nd ed. Berlin, Heidelberg: Springer-Verlag, 2003.

[142] A. Baug, N. R. Choudhury, R. Ghosh, S. Dalai, and B. Chatterjee, “Identification of single and multiple partial discharge sources by optical method using mathematical morphology aided sparse representation classifier,” *IEEE Trans. Dielectr. Electr. Insul.*, vol. 24, no. 6, pp. 3703–3712, Dec. 2017, doi: 10.1109/TDEI.2017.006398.

[143] Q. H. Wu, Z. Lu, and T. Ji, *Protective Relaying of Power Systems Using Mathematical Morphology*. Springer Science & Business Media, 2009.

[144] A. A. Saad, M. F. El-Naggar, and E. H. Shehab_Eldin, “Modeling and testing of multi-resolution morphological gradient distance relay algorithm,” *Energy Procedia*, vol. 14, pp. 271–279, Jan. 2012, doi: 10.1016/j.egypro.2011.12.929.

[145] “Secure Distributed Control in Networked Control Systems | ADAC.” https://research.ece.ncsu.edu/adac/secure-distributed-control-in-networked-control-systems/ (accessed Jan. 29, 2021).

[146] "IEEE Recommended Practice for 1 kV to 35 kV Medium-Voltage DC Power Systems on Ships," *IEEE Std 1709-2010*, pp. 1–54, Nov. 2010, doi: 10.1109/IEEESTD.2010.5623440.

[147] F. Balsamo, C. Capasso, and O. Veneri, "Performance evaluation of an all-electric waterbus supplied by hybrid energy storage systems," in *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, Jun. 2018, pp. 620–625, doi: 10.1109/SPEEDAM.2018.8445248.

[148] F. Balsamo, C. Capasso, G. Miccione, and O. Veneri, "Hybrid Storage System Control Strategy for All-Electric Powered Ships," *Energy Procedia*, vol. 126, pp. 1083–1090, Sep. 2017, doi: 10.1016/j.egypro.2017.08.242.

[149] Z. Jin, G. Sulligoi, R. Cuzner, L. Meng, J. C. Vasquez, and J. M. Guerrero, "Next-Generation Shipboard DC Power System: Introduction Smart Grid and dc Microgrid Technologies into Maritime Electrical Netowrks," *IEEE Electrification Mag.*, vol. 4, no. 2, pp. 45–57, Jun. 2016, doi: 10.1109/MELE.2016.2544203.

[150] V. Arcidiacono, A. Monti, and G. Sulligoi, "Generation control system for improving design and stability of medium-voltage DC power systems on ships," *IET Electr. Syst. Transp.*, vol. 2, no. 3, pp. 158–167, Sep. 2012, doi: 10.1049/iet-est.2011.0016.

[151] M. Cupelli, A. Monti, E. D. Din, and G. Sulligoi, "Case study of voltage control for MVDC microgrids with constant power loads - Comparison between centralized and decentralized control strategies," in *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, Apr. 2016, pp. 1–6, doi: 10.1109/MELCON.2016.7495331.

[152] U. Javaid, F. D. Freijedo, D. Dujic, and W. van der Merwe, "Dynamic Assessment of Source–Load Interactions in Marine MVDC Distribution," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 4372–4381, Jun. 2017, doi: 10.1109/TIE.2017.2674597.

[153] Z. Jin, L. Meng, J. C. Vasquez, and J. M. Guerrero, "Frequency-division power sharing and hierarchical control design for DC shipboard microgrids with hybrid energy storage systems," in *2017 IEEE Applied Power Electronics Conference and Exposition (APEC)*, Mar. 2017, pp. 3661–3668, doi: 10.1109/APEC.2017.7931224.

[154] X. Lu, J. M. Guerrero, K. Sun, and J. C. Vasquez, "An Improved Droop Control Method for DC Microgrids Based on Low Bandwidth Communication With DC Bus Voltage Restoration and Enhanced Current Sharing Accuracy," *IEEE Trans. Power Electron.*, vol. 29, no. 4, pp. 1800–1812, Apr. 2014, doi: 10.1109/TPEL.2013.2266419.

[155] S. Anand, B. G. Fernandes, and J. Guerrero, "Distributed Control to Ensure Proportional Load Sharing and Improve Voltage Regulation in Low-Voltage DC Microgrids," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1900–1913, Apr. 2013, doi: 10.1109/TPEL.2012.2215055.

[156] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed Secondary Control for Islanded Microgrids—A Novel Approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb. 2014, doi: 10.1109/TPEL.2013.2259506.

[157] J. Fleer and P. Stenzel, "Impact analysis of different operation strategies for battery energy storage systems providing primary control reserve," *J. Energy Storage*, vol. 8, pp. 320–338, Nov. 2016, doi: 10.1016/j.est.2016.02.003.

[158] F. Gao, S. Bozhko, G. Asher, P. Wheeler, and C. Patel, "An Improved Voltage Compensation Approach in a Droop-Controlled DC Power System for the More Electric Aircraft," *IEEE Trans. Power Electron.*, vol. 31, no. 10, pp. 7369–7383, Oct. 2016, doi: 10.1109/TPEL.2015.2510285.

[159] P. Bhowmik, S. Chandak, and P. K. Rout, "State of charge and state of power management among the energy storage systems by the fuzzy tuned dynamic exponent and the dynamic PI controller," *J. Energy Storage*, vol. 19, pp. 348–363, Oct. 2018, doi: 10.1016/j.est.2018.08.004.

[160] S. Anand and B. G. Fernandes, "Reduced-Order Model and Stability Analysis of Low-Voltage DC Microgrid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 11, pp. 5040–5049, Nov. 2013, doi: 10.1109/TIE.2012.2227902.

[161] J. Neely, L. Rashkin, M. Cook, D. Wilson, and S. Glover, "Evaluation of power flow control for an all-electric warship power system with pulsed load applications," in *2016 IEEE Applied Power Electronics Conference and Exposition (APEC)*, Mar. 2016, pp. 3537–3544, doi: 10.1109/APEC.2016.7468377.

[162] Y. Li, L. He, F. Liu, C. Li, Y. Cao, and M. Shahidehpour, “Flexible Voltage Control Strategy Considering Distributed Energy Storages for DC Distribution Network,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 163–172, Jan. 2019, doi: 10.1109/TSG.2017.2734166.

[163] Z. Jin, L. Meng, J. M. Guerrero, and R. Han, “Hierarchical Control Design for a Shipboard Power System With DC Distribution and Energy Storage Aboard Future More-Electric Ships,” *IEEE Trans. Ind. Inform.*, vol. 14, no. 2, pp. 703–714, Feb. 2018, doi: 10.1109/TII.2017.2772343.

[164] O. Palizban and K. Kauhaniemi, “Energy storage systems in modern grids—Matrix of technologies and applications,” *J. Energy Storage*, vol. 6, pp. 248–259, May 2016, doi: 10.1016/j.est.2016.02.001.

[165] T. Bocklisch, “Hybrid Energy Storage Systems for Renewable Energy Applications,” *Energy Procedia*, vol. 73, pp. 103–111, Jun. 2015, doi: 10.1016/j.egypro.2015.07.582.

[166] Y. Zhang, R. Wang, T. Zhang, Y. Liu, and B. Guo, “Model predictive control-based operation management for a residential microgrid with considering forecast uncertainties and demand response strategies,” *IET Gener. Transm. Amp Distrib.*, vol. 10, no. 10, pp. 2367–2378, Jul. 2016, doi: 10.1049/iet-gtd.2015.1127.

[167] A. H. González, J. L. Marchetti, and D. Odloak, “Robust model predictive control with zone control,” *IET Control Theory Amp Appl.*, vol. 3, no. 1, pp. 121–135, Jan. 2009, doi: 10.1049/iet-cta:20070211.

[168] J. Chen and Q. Zhu, “Resilient and decentralized control of multi-level cooperative mobile networks to maintain connectivity under adversarial environment,” in *2016 IEEE 55th Conference on Decision and Control (CDC)*, Dec. 2016, pp. 5183–5188, doi: 10.1109/CDC.2016.7799062.

[169] S. Al-Takrouri, A. V. Savkin, and V. G. Agelidis, “A decentralized control algorithm based on the DC power flow model for avoiding cascaded failures in power networks,” in *2013 9th Asian Control Conference (ASCC)*, Jun. 2013, pp. 1–6, doi: 10.1109/ASCC.2013.6606056.

[170] O. Palizban and K. Kauhaniemi, “Distributed cooperative control of battery energy storage system in AC microgrid applications,” *J. Energy Storage*, vol. 3, pp. 43–51, Oct. 2015, doi: 10.1016/j.est.2015.08.005.

[171] M. Cupelli *et al.*, “Power Flow Control and Network Stability in an All-Electric Ship,” *Proc. IEEE*, vol. 103, no. 12, pp. 2355–2380, Dec. 2015, doi: 10.1109/JPROC.2015.2496789.

[172] A. A. Saad, S. Faddel, T. Youssef, and O. Mohammed, “Small-signal model predictive control based resilient energy storage management strategy for all electric ship MVDC voltage stabilization,” *J. Energy Storage*, vol. 21, pp. 370–382, Feb. 2019, doi: 10.1016/j.est.2018.12.009.

VITA

AHMED ALY SAAD AHMED

1985	Born, Cairo, Egypt
2002-2007	B.Sc., Electrical Engineering, Helwan University, Cairo, Egypt
2008-2009	Electrical Engineer, Egyptian Electricity Holding Company, Cairo, Egypt
2008-2012	M.Sc., Electrical Engineering, Helwan University, Cairo, Egypt
2009-2017	Teaching Assistant and Research Engineer, Helwan University, Cairo, Egypt
2018-2021	Graduate Research Assistant and Doctoral Candidate, Florida International University, Miami, Florida, USA

SELECTED PUBLICATIONS AND PRESENTATIONS

[J-1] Ahmed A. Saad; Faddel, S.; Mohammed, O. IoT-Based Digital Twin for Energy Cyber-Physical Systems: Design and Implementation. *Energies* 2020, 13, 4762.

[J-2] H. H. Eldeeb, A. Berzoy, Ahmed A. Saad, H. Zhao and O. A. Mohammed," Differential Mathematical Morphological Based On-line Diagnosis of Stator Inter-Turn Failures in Direct Torque Control Drive Systems," in IEEE Transactions on Industry Applications, doi: 10.1109/TIA.2020.3019779.

[J-3] Ahmed A. Saad, S. Faddel, T. Youssef and O. Mohammed," On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks," in IEEE Transactions on Smart Grid, doi: 10.1109/TSG.2020.3000958.

[J-4] S. Faddel, Ahmed A. Saad, M. E. Hariri and O. A. Mohammed, "Coordination of Hybrid Energy Storage for Ship Power Systems With Pulsed Loads," in IEEE Transactions on Industry Applications, vol. 56, no. 2, pp. 1136-1145, March-April 2020, doi: 10.1109/TIA.2019.2958293.

[J-5] Ebrahim, A.F.; Ahmed A. Saad; Mohammed, O. Smart Integration of a DC Microgrid: Enhancing the Power Quality Management of the Neighborhood Low-Voltage Distribution Network. Inventions 2019, 4, 25.

[J-6] Ahmed A. Saad, Samy Faddel, and Osama Mohammed. ”A secured distributed control system for future interconnected smart grids.” Applied Energy 243 (2019): 57-70.

[J-7] S. Faddel, Ahmed A. Saad, T. Youssef and O. Mohammed, ”Decentralized Control Algorithm for the Hybrid Energy Storage of Shipboard Power System,” in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 8, no. 1, pp. 720-731, March 2020, doi: 10.1109/JESTPE.2019.2899287.

[J-8] Ahmed A. Saad, Samy Faddel, Tarek Youssef, and Osama Mohammed. ”Small-signal model predictive control based resilient energy storage management strategy for all electric ship MVDC voltage stabilization.” Journal of Energy Storage 21 (2019): 370-382.

[J-9] Ahmed A. Saad, T. Youssef, A. T. Elsayed, A. Amin, O. H. Abdalla and O. Mohammed, ”Data-Centric Hierarchical Distributed Model Predictive Control for Smart Grid Energy Management,” in IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4086-4098, July 2019, doi: 10.1109/TII.2018.2883911.

[J-10] M. M. Eissa, W. M. Fayek, M. M. A. Hadhoud, M. M. Elmesalawy and A. A. Saad Shetaya, ”Frequency/voltage wide-area measurements over transmission control protocol/internet protocol communication network for generator trip identification concerning missed data,” in IET Generation, Transmission & Distribution, vol. 8, no. 2, pp. 290-300, February 2014, doi: 10.1049/iet-gtd.2013.0207.

[P-1] Ahmed A. Saad, and Osama Mohammed. ”Energy Cyber-Physical System Digital Twin Playground.” *U.S. Patent* October, 2020. [Filled]

[P-2] Ahmed A. Saad, Samy Gamal Faddel Mohamed, and Osama Mohammed. ”Systems and methods for providing security in power systems.” *U.S. Patent* 10,686,810, issued June 16, 2020. [Awarded]

[P-3] Eldeeb, Hassan H., Alberto Berzoy, Ahmed A. Saad, and Osama Mohammed. ”Condition monitoring and fault detection in induction motors.” *U.S. Patent* 10,686,394, issued June 16, 2020. [Awarded]