Multi-Level Frequency Control, Resilience Enhancement and Cyber-Attack Identification in Multi-Area LCC-HVDC Interconnected Networks

Hossien Faraji, Amir Khorsandi, and Seyed Hossein Hosseinian

***Abstract*—The utilization of LCC-HVDC lines is one of the methods for transferring bulk-scale power and interconnecting systems with different frequencies. Various control methods have been previously proposed to manage and control LCC-HVDC systems, but none have provided a multi-level control system capable of operating in multiple areas simultaneously. This article presents a comprehensive and multi-task control system for wide-area HVDC systems. In the proposed control systems, multi-level frequency control is conducted in multi-area LCC-HVDC interconnected grids. Additionally, various control strategies are implemented to enhance the network's resilience during three-phase fault conditions. Furthermore, the proposed control system can detect and distinguish intelligent false data injection (FDI) cyber-attacks. Nonlinear time domain simulations conducted in MATLAB/SIMULINK demonstrate that the proposed method can effectively balance the frequency of weaker areas, enhance network resilience in critical conditions, and identify FDI cyber-attacks.**

***Index Terms*—Multi-area networks, multi-level frequency control, LCC-HVDC, cyber-attack, resilience.**

NOMENCLATURE

I_{dc}	DC Current (A)
I_{dc}^{ref}	Referenced DC current (A)
I_{dc}^{reg}	Regulated DC current (A)
I_{Err}	Error current (A)
I_{Inv}	Inverter triggering current (A)
I_{Rec}	Rectifier triggering current (A)
I_{Li}	load current of area i (A)
IL_{ref}	Referenced load current (A)
P_{dc}	DC Power (W)
P_{ac}	RMS Power (W)
P_{ref}	Referenced generator power (W)
P_{dc}^{ref}	Referenced DC power (W)
PL_{ref}	Referenced load power (W)
P_{Li}	Load power of area i (W)
ΔP_{Gen}	Generator power deviation (W)
ΔP_L	Load power deviation (W)
$\Delta P_{DCi,j}$	DC power deviation between area i and j (W)
ΔP_{DC}^{ref}	Referenced DC power deviation (W)
ΔV	Voltage difference (V)
V_{dc}	DC voltage (V)
V_{dc}^{ref}	Referenced DC voltage (V)
V_{dc}^{reg}	Regulated DC voltage (V)
ω_i	Measured frequency of area i (rad/s)
ω_{ref}	Nominal frequency (rad/s)
$\Delta\omega$	Frequency deviation (rad/s)
h	Conversion gain proportional to inertia
β	Frequency bias
K	Control gain
K_d	Gain proportional to the damping coefficient
T_d	Time constant proportional to damping and inertia
T_{dc}	Time constant proportional to DC links
$T_{i,j}$	Overall time constant of steam turbine and governor
$R_{i,j}$	Droop rate of each of the production units

Received 16 March 2024; revised 29 July 2024 and 13 September 2024; accepted 3 November 2024. Date of publication 6 November 2024; date of current version 21 February 2025. Paper no. TSG-00428-2024. *(Corresponding author: Amir Khorsandi.)*

The authors are with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran 6719773615, Iran (e-mail: hossien.faraji@aut.ac.ir; a_khorsandi@aut.ac.ir; hosseinian@aut.ac.ir).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2024.3492956.

Digital Object Identifier 10.1109/TSG.2024.3492956

I. INTRODUCTION

DUE TO reactive power limitations and the challenges of transmitting AC power over long distances, high voltage direct current (HVDC) proves to be more efficient for large-scale power transmission compared to high voltage alternating current (HVAC) systems [1], [2]. HVDC technology has the capability to transmit large power over long distances with lower losses compared to the conventional AC systems [3]. Furthermore, HVDC facilitates the interconnection of grids with different frequencies, thereby improving the overall stability and reliability of the electric power grid [4].

The essential components of an HVDC system are its converter stations [5]. At the sending end of an HVDC line, an AC/DC converter is utilized to convert the AC voltage into a DC voltage at the transmission level. Conversely, a DC/AC converter is employed at the receiving end to invert the DC voltage into the desired AC network voltage level [6]. HVDC links commonly utilize two main types of converters: line commutated converters (LCCs) and voltage-source converters (VSCs) [7].

LCC-HVDC is a well-established technology for bulk power transmission due to the high voltage and current ratings of thyristors. However, it requires additional components for reactive power compensation and harmonics filtering [8]. LCCs are based on thyristors that require a certain voltage for

commutation [9]. Therefore, a non-zero AC voltage on their AC side is needed to fire the thyristor valves. The converters of stations are controlled by adjusting the firing angle of the thyristors: 0 to 90 degrees for rectifiers and 90 to 180 degrees for inverters [10].

A. Literature Review

In [11], a wide-area coordinated control for an HVDC system has been implemented, but it lacks resilience-boosting strategies and cyber-attack identification capabilities. In [12], a control strategy for LCC-HVDC is presented for emergency conditions using wide area measurement systems in just two areas. However, the strategy does not support each other, and cyber-attack resilience has not been addressed. Additionally, a multi-level frequency control is implemented in [13], and several control strategy aimed at enhancing transient state stability have been implemented in [14]. Nevertheless, none of these strategies extend across multiple areas. In [15] and [16], various control schemes have been investigated to address fault conditions. However, none of these control strategies have been able to effectively distinguish cyber-attacks from fault modes and respond accordingly. In [17], the fault clearing scheme using half-bridge modular multilevel converter technology is investigated. But, the proposed method only studies a single transmission line and does not offer a specific strategy for multi-zone systems. In [18] and [19], various methods for detecting cyber-attacks in HVDC are presented. However, the proposed methods are limited to covering two-zone systems. A security domain layer and decision framework to detect and mitigate the impact of false data injection (FDI) attacks targeting HVDC stations is presented in [20]. In [21], two regions with different operating frequencies are linked by an HVDC transmission line. The control strategies in place manage the frequency and voltage of the system, while also addressing fault conditions and detecting cyber-attacks. Despite these capabilities, it does not operate as a multi-zone and multi-control scheme, nor does it offer a backup strategy for continuous three-phase faults. Article [22] introduces an evaluation method for assessing the resilience of the power system. This method focuses on the system's capacity to support power sources and network topology, with a specific focus on LCC-HVDC systems. However, this method does not address frequency control or include provisions for handling cyber-attacks. In [23], the resilience of LCC-HVDC under hazardous conditions is investigated using a new phase-locked loop. Although the proposed method can provide an accurate phase reference for the DC control system and increase overshoot, its performance in power frequency fluctuations, such as lack of power production and load increase has not been studied. Additionally, it may encounter challenges during cyber-attacks. In [24], the effect of FDI cyber-attacks on converters of LCC-HVDC is investigated. However, this study does not investigate the effect of simultaneous cyber-attacks with frequency fluctuations, nor does it provide a solution to enhance resilience under such conditions. Cyber-attack against wide area control is studied in [25], where the proposed defense strategy can accurately estimate the injected state signal. However, the detection method does not address any significant reduction in the frequency or resilience that may result from these attacks. In [26], a system frequency response model for multi-zone asynchronous grids is developed, deriving frequency constraints using an approximate algorithm and formulating a single commitment model for initial frequency reserve sharing, which facilitates inter-zone power transmission through HVDC. However, the performance of the proposed method under faults remains unknown, and the resilience of the system against FDI cyber-attacks has not been investigated. Paper [27] investigates the automatic generation control (AGC) of a multi-area power system relies on HVDC links, considering the planned partial load in a hydroelectric and thermal power generation unit, resulting in an improved dynamic response of the system. However, the method mentioned does not include any proposed systems for detecting FDI cyber-attacks or addressing fault conditions. In [28], a partitioning method is proposed for the post-event reconstruction of the power grid with LCC-HVDC systems. However, the research does not investigate the improvement of the system's resilience and performance under the conditions of FDI cyber-attacks. The impact of a cyber-attack on an HVDC system is investigated in [29], focusing on FDI attacks. This study examines the effects of FDI on various HVDC control modes, including rectifier-side constant DC current control, supplementary damping control, inverter-side constant DC voltage control, and constant shutdown control based on the basic HVDC control strategy. However, the impact of attacks on power transmission between areas has not been investigated.

B. Discussion of LCC-HVDC Necessity

With the growing trend of energy demand and the need to transfer large amounts of power, the use of HVDC networks is increasing. Currently, extensive HVDC line networks exist worldwide, such as the Western LCC-HVDC link with the length of 422 km with the exchange of 2.2 gigawatts of power between Wales and Scotland [30]. Another example is the Terna Link, which connects Sicily with Sardinia and the Italian peninsula through a pair of underwater cable, enabling the exchange of 1 gigawatt of power between the regions. Furthermore, depending on requirements, multiple connections and areas for such lines may be established. One method for bulk power transmission involves the utilization of modular multilevel converters based on VSC technologies, which are well-suited for handling harmonics. However, when expanding the transmission areas for networks that previously used LCC lines, like the western LCC- HVDC link, expanding other lines with the same type of technology is more cost-effective [31]. Therefore, given the various operational LCC lines globally and the potential expansion of their transmission areas to multiple regions as per the requirements, the presence of wide-area central control systems (WACCS) and new control strategies to control the frequencies between these areas is necessary. Given that WACCS units are susceptible to malicious cyber-attacks, it is crucial to implement cyber-attack detection algorithms that aim to detect FDI attacks on

TABLE I
COMPARISON BETWEEN THE CURRENT PAPER AND PREVIOUS LITERATURE

Ref. No	Multi-area LCC-HVDC interconnected systems	Multi-level frequency control for wide-area through LCC-HVDC lines	Resilience enhancement in wide-area	Cyber-attack detection in wide-area HVDC lines
[11]	Yes	No	No	No
[12]	No	No	Yes	No
[13]	No	Yes	No	No
[14]	No	No	Yes	No
[15]	Yes	No	Yes	No
[16]	No	No	Yes	No
[17]	No	No	Yes	No
[18]	No	No	No	Yes
[19]	No	No	No	Yes
[20]	No	No	Yes	Yes
[21]	No	No	Yes	Yes
[22]	Yes	No	Yes	No
[23]	Yes	No	Yes	No
[24]	Yes	No	No	Yes
[25]	Yes	No	No	Yes
[26]	Yes	Yes	No	No
[27]	No	Yes	No	No
[28]	No	No	Yes	No
[29]	No	No	No	Yes
Current Paper	Yes	Yes	Yes	Yes

the frequency, which try to obtain power from other areas by creating a false demand through fake frequency reduction. Additionally, it is imperative to detect attacks that manipulate the power transmitted between areas. On the other hand, the need of the future is that in case of multiple connections of different power areas, they provide mutual support to each other in the event of three-phase faults in multiple regions.

C. Motivations

According to the review of previous researches, the challenge of frequency control between regions in LCC-HVDC interconnected networks, addressing FDI cyber-attacks on transmission power or attacks by fake power requesters, and improving network resiliency have attracted the attention of researchers. However, none of the previous research has comprehensively covered all these topics. This article introduces a WACCS unit that connects with internal central control systems (CCSs) of multiple areas through telecommunication platforms to address various objectives. These objectives include developing new control strategies for frequency control between areas, identifying FDI cyber-attacks that may occur through fake frequency requests and manipulation of exchanged power, and enhancing network resilience to manage outages caused by three-phase events. A comparison between the current paper and the existing literature is presented in Table I.

D. Contributions and Innovations

This paper presents a model of a wide-area network where a WACCS unit transfers power from stronger to weaker areas through communication with CCSs. Also, the paper presents algorithms designed to detect FDI cyber-attacks and enhance network resilience. The main innovations of this article are listed as follows:

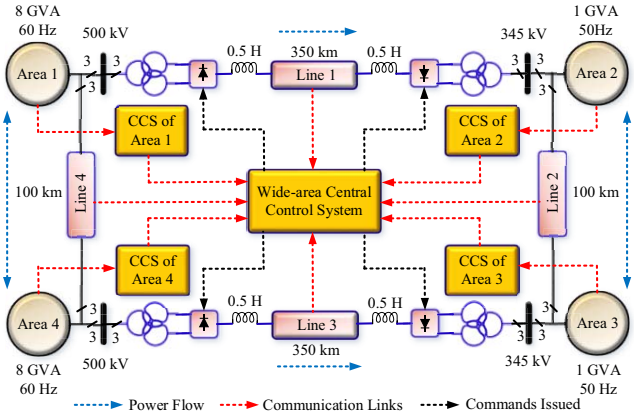

Fig. 1. Outline of the proposed wide-area LCC-HVDC interconnected grids.

- ➢ *Designing a decision-making system for the WACCS based on three proposed control systems: frequency control unit, FDI attack detection, and resilience improvement.*
- ➢ *Implementing multi-level frequency control in multi-area networks through LCC-HVDC interconnected systems.*
- ➢ *Identifying FDI cyber-attacks corresponding to the changes in the power consumption and frequency in the areas and detecting FDI cyber-attacks on DC power systems.*
- ➢ *Enhancing the Resilience of wide-areas by combining several support strategies, including mutual support of LCC-HVDC lines, and between different network areas.*

II. WIDE-AREA LCC-HVDC NETWORKS

The wide-area LCC-HVDC interconnected network under study is shown in Fig. 1. The network consists of four power generating areas with different frequencies, where areas 1 and 4 operate at 60 Hz, and areas 2 and 3 operate at 50 Hz. Areas 1 and 2 are linked through LCC-HVDC transmission line 1, while areas 3 and 4 are connected by LCC-HVDC transmission line 3. Additionally, areas 1 and 4 are connected by AC three-phase line 4, while areas 2 and 3 are connected by line 2. Under normal operation, lines 2 and 4 are open; however, in the event of an emergency, lines 2 and 4 are closed. The generators shown in Fig. 1 represent the aggregate equivalent of all synchronous generators installed in each area. Additionally, for each region, there are time-varying three-phase loads. Each HVDC line is 350 km long with voltage level of 500 kV. The control system sends power from areas 1 and 4 through lines 1 and 3 to stabilize the frequency of areas 2 and 3 in case of frequency drop.

In the network under study, a WACCS has been designed to connect the four areas. It receives information from the CCSs of areas 1 to 4 and sends commands to the converter stations on both sides of lines 1 and 3 based on the specified goals and strategies. The internal decision-making systems of the WACCS unit include frequency control system, detection of FDI cyber-attacks, and resilience improvement strategy.

Signal transmission between the CCSs and the WACCS unit is facilitated through the optical-fiber telecommunication

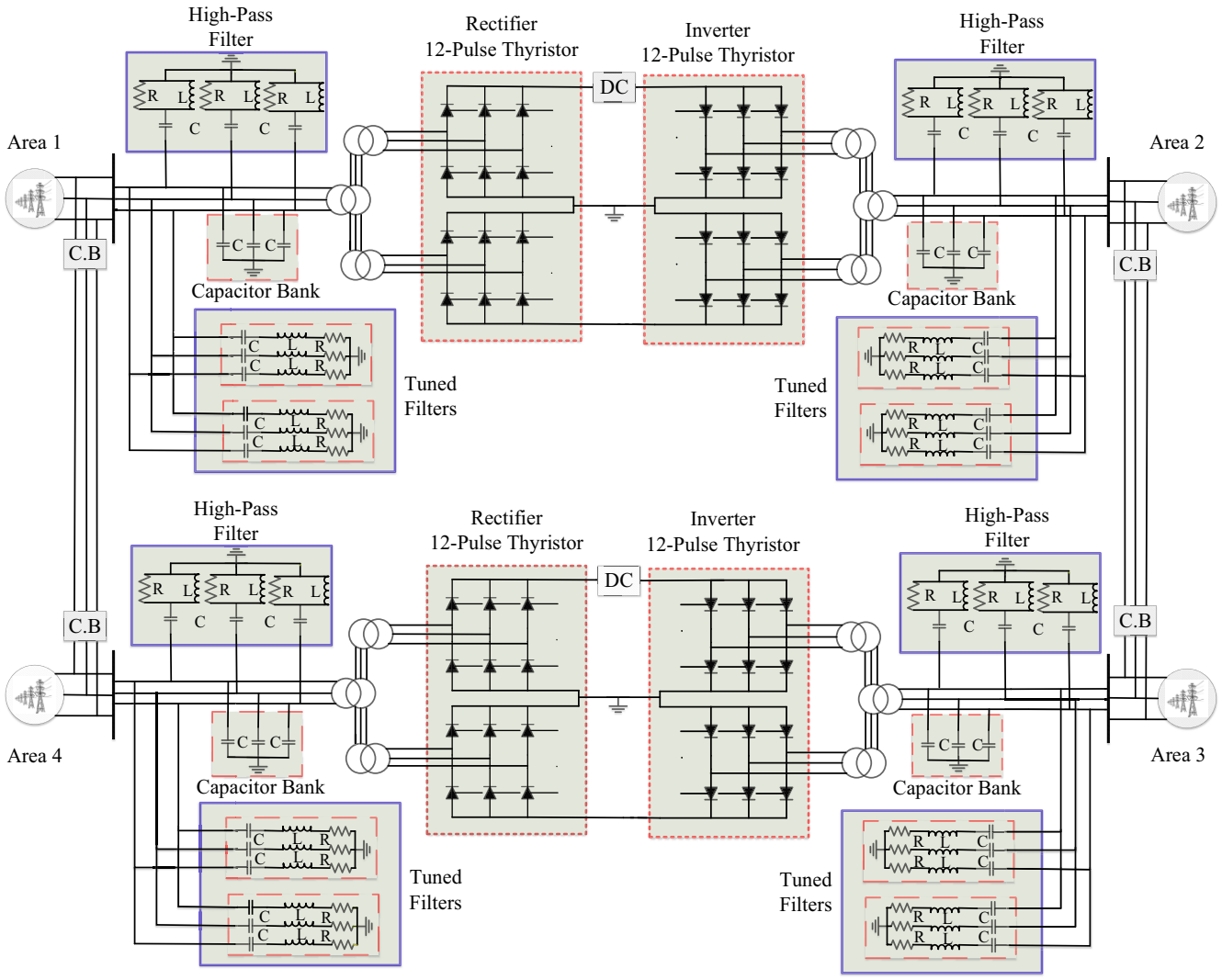

Fig. 2. The detailed model of the network under study.

platform. It is assumed that an attacker has access to the information of CCS in areas 2 and 3, as well as the functional information of the WACCS, and can inject false data into the control loops.

Fig. 2 illustrates the detailed model of the network under study. In lines 1 and 3, the 12-pulse LCCs consists of two series 6-pulse thyristor bridges, each supplied separately by Y-Y and Y-Δ transformers. Additionally, in each area, a 400 MVAR capacitor bank is utilized to provide the required reactive power. The filters are tuned to eliminate dominant harmonics. The parameters of the network are given in Table II. The parameters of the generators, capacitor banks, and filters are provided in [21].

TABLE II
TEST SYSTEM PARAMETERS: GENERATORS, TRANSFORMERS AND HVDC LINES

	Area 1 and 4		Area 2 and 3	
	Generator	Transformer	Generator	Transformer
Power (GVA)	8	2	1	2
Frequency (Hz)	60	60	50	50
Voltage (kV)	500	500/200/200	345	200/200/345
HVDC Lines				
Length	350 (km)			
Voltage	500 (kV)			
Inductance	0. 71 (mH/km)			
Capacitance	0.29 (μF/km)			
Resistance	0.018 (Ω/km)			

III. PROPOSED CONTROL SYSTEM

The methodology of the proposed WACCS is presented in Fig. 3. The system comprises three control units: the frequency control system, FDI cyber-attack detection system, and resilience improvement unit, all overseen by the WACCS. The proposed frequency control system connects lines 1 and 2, and 3 and 4 when detecting frequency deficits in areas 2 and 3. The FDI identification unit monitors frequency changes caused by load changes, not attacks, and also monitors the power transmitted between the lines to detect an FDI cyber-attack on the transmitted power. Additionally, in the event of a severe voltage drop in areas 2 and 3 due to three-phase faults, the WACCS provides the ability to connect areas 2 and 3 according to the resilience control strategy. In such scenarios, depending on the fault location in area 2 or 3, line 1 is used to support area 3 as well as area 2, and line 3 can also cover area

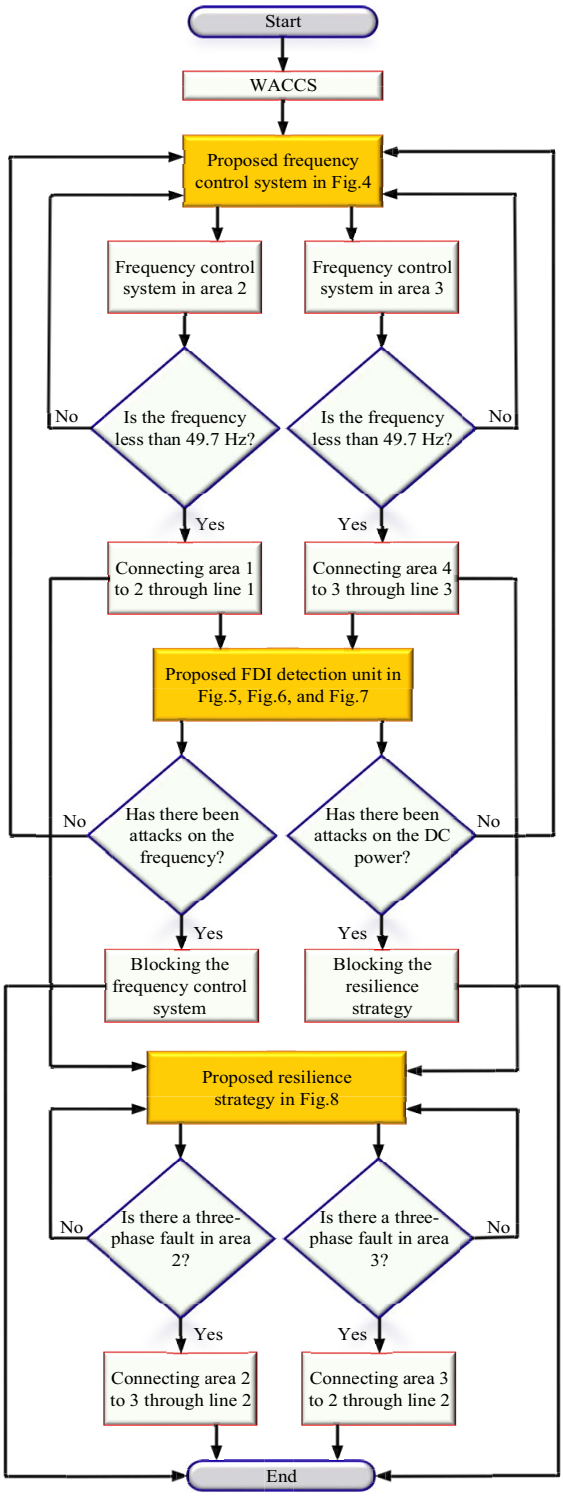

Fig. 3. Methodology of the operation of the proposed control systems: frequency control system, identification of FDI cyber-attacks, and resilience strategy under the supervision of WACCS.

2 in addition to supporting area 3. Therefore, three control units, including the multi-level frequency control unit between multiple areas, the FDI attack detection unit, and the resilience improvement unit in fault conditions, all operate under the WACCS supervision. The operation of each of the proposed control unit will be detailed below.

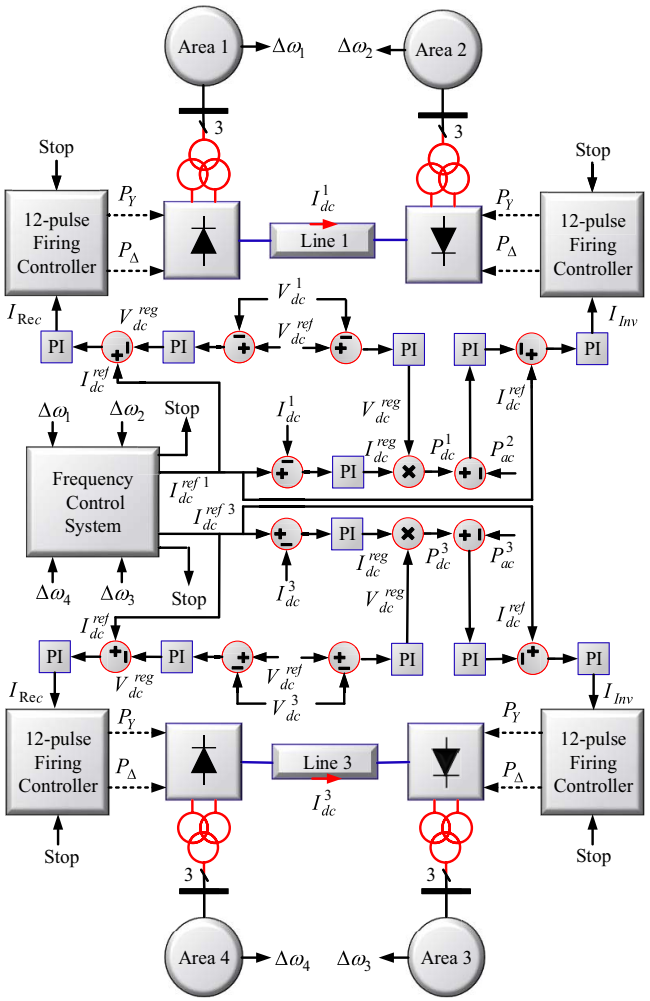

Fig. 4. Proposed control system for multi-level frequency control of areas 2 and 3 by areas 1 and 4 through the DC power transmitted on LCC-HVDC lines 1 and 3.

In this article, it is assumed that the attacker can potentially target both the WACCS and CCS units of areas due to the utilization of measurement units in areas 1 to 4 and communication links between CCSs of areas 1 to 4 with WACCS. The attacker may send a false power request to the control system by manipulating the frequency of areas 2 and 3, as well as adjusting the power transmitted between areas 1 and 2 or 3 and 4. These attacks are highly sophisticated and involve penetrating the control layers and manipulating measurement units or injecting false data into the control layers, which could cause the control systems to malfunction.

A. Proposed Multi-Level Frequency Control System

According to this strategy, the frequency of areas 2 and 3 is regulated by areas 1 and 4, respectively. In this manner, the severe and multi-level changes in frequency of areas 2 and 3 are addressed by generating more active power in areas 1 and 4. The generated active power is transmitted to their designated destinations via DC lines 1 and 3. At the end of the line, the DC power is converted into three-phase power at the corresponding frequency and voltage levels.

Fig. 4 shows the schematic of the proposed control system for multi-level frequency control of the network. The central

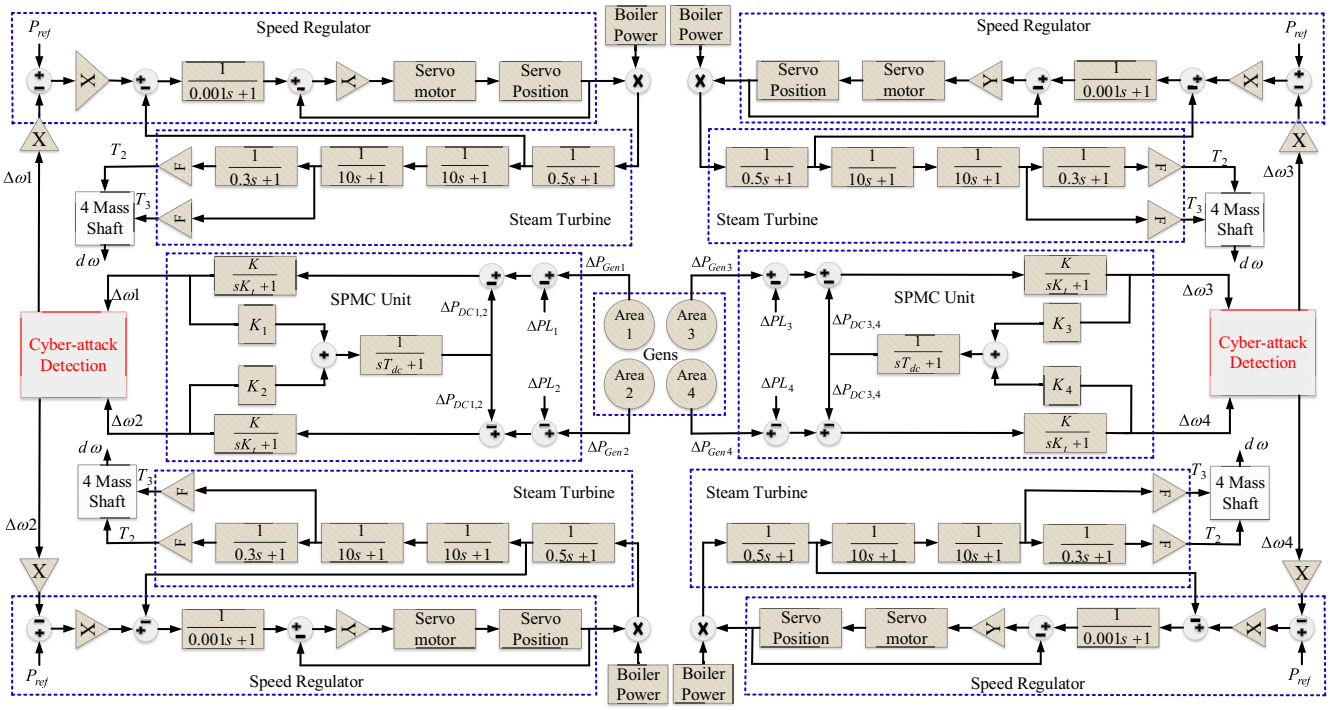

Fig. 5. Proposed control system for identifying FDI cyber-attacks along with complete modeling of steam turbine and governor parts in 4 regions.

frequency control system continuously monitors the frequency deviations of the areas. If the change is non-zero in areas 2 and 3 and the frequency in those areas exceeds the permissible value, a DC reference current is generated by (1). The DC regulated current is calculated using (2), the DC power of the lines is obtained from (3), and the regulated DC voltage is calculated using (4). The transmitted DC power for lines 1 and 3 is compared with the effective power of areas 2 and 3 using (5) to calculate the current error. This current error is then converted into triggering pulses suitable for the inverters on lines 1 and 3 using (6) with a 12-pulse firing controller. Furthermore, the current required to generate suitable firing pulses for the rectifiers at the beginning of lines 1 and 3 is calculated using (7).

$$\begin{cases} \Delta\omega 2 \neq 0 \rightarrow if\ f_2 < 49.7 \rightarrow I_{dc}^{ref1} = 1 \\ \Delta\omega 3 \neq 0 \rightarrow if\ f_3 < 49.7 \rightarrow I_{dc}^{ref3} = 1 \end{cases} \tag{1}$$

$$I_{dc}^{regi} = K_p\left(I_{dc}^{refi} - I_{dc}^{i}\right) + K_I \int \left(I_{dc}^{refi} - I_{dc}^{i}\right) dt \quad \forall i \in Line[1,3] \tag{2}$$

$$P_{dc}^{refi} = V_{dc}^{regi} \times I_{dc}^{regi} \quad \forall i \in Line[1,3] \tag{3}$$

$$V_{dc}^{regi} = K_p\left(V_{dc}^{ref} - V_{dc}^{i}\right) + K_I \int \left(V_{dc}^{ref} - V_{dc}^{i}\right) dt \quad \forall i \in Line[1,3] \tag{4}$$

$$I_{Err}^{i} = K_p\left(P_{dc}^{i} - P_{ac}^{j}\right) + K_I \int \left(P_{dc}^{i} - P_{ac}^{j}\right) dt \quad \forall i \in Line[1,3] \& j \in Area[2,3] \tag{5}$$

$$I_{Inv}^{i} = K_p\left(I_{dc}^{refi} - I_{Err}^{i}\right) + K_I \int \left(I_{dc}^{refi} - I_{Err}^{i}\right) dt \quad \forall i \in Line[1,3] \tag{6}$$

$$I_{\text{Rec}}^{i} = K_p\left(I_{dc}^{refi} - V_{dc}^{regi}\right) + K_I \int \left(I_{dc}^{refi} - V_{dc}^{regi}\right) dt \quad \forall i \in Line[1,3] \tag{7}$$

B. Proposed Control System for FDI Cyber-Attack Identification on Frequency and Load Deviations

This section describes the proposed control system related to steam turbine and governor models of functional areas that identifies smart cyber-attacks in real time, as shown in Fig. 5.

Each region is equipped with combined steam turbine systems, including a speed regulator, steam turbine, and shaft with a maximum of four masses. It should be noted that generator mass is not included in this study. The two masses 2 and 3 are the closest shaft masses to the generator. Therefore, only these masses, providing the output torques T_2 and T_3, are considered in the "compressed" generator model. The steam turbine consists of four stages, each modeled by a first-order transfer function. The first stage represents the steam chest, while the remaining three stages represent reheaters or crossover piping. The boiler pressure is constant at 1.0 pu, and no model is used for the boiler. Additionally, the F fractional index is used to distribute the turbine power among the different shaft stages.

In Fig. 5, the shaft is modeled as a four-mass system, coupled to the mass in the synchronous generator (Gen) model, resulting in a total of five masses. The shaft is characterized by mass inertias denoted as H, damping factors represented by D, and rigidity coefficients indicated as K. The Label X is the permanent droop Rp (pu) and Y is the interest rate. The reference power in each GEN unit is calculated by (8). In the Laplace domain, the frequency deviation of each area can be expressed as (9). Eq. (8) can be rewritten as displayed in (10).

With the HVDC links, the area control error (ACE) signal contains both AC/DC power flows and frequency deviation of each area, and acts as an input for the integral control action, by (11). To model the HVDC link for dynamic analysis in the interconnected system, the concept of the supplementary power modulation controller (SPMC) has been employed [32]. The SPMC is designed as a high-level damping controller aimed at enhancing the performance of power systems during load changes. The inputs of the SPMC consist of frequency deviations in the connected areas. By changing the duty cycles of converters, the SPMC output is used for the HVDC link to generate the desired DC power. This coordinated control strategy is expressed in (12) and (13). To summarize, the system model under the high-level control structure for the two-area sample system (comprising areas 1 and 2 as well as areas 3 and 4) with DC links is presented by (14), where $x(t)$ represents the vector of all state variables and d is the system input of load variations as given in (15). Subsequently, for the purposes of numerical analysis, (15) needs to be discretized. To obtain the analytical solution for discretization, the matrices A and B of the sampled discrete time model with a sampling period T_s must be transformed as shown in (16).

$$P_{ref} = h \times \omega_{ref} \times \frac{d\Delta\omega}{dt} \tag{8}$$

$$\Delta\omega_i(s) = \frac{K_d}{1+sT_{d_i}}\left[\Delta P_{Geni} - \Delta PL_i - \Delta P_{DCi,j}\right] \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{9}$$

$$\Delta P_{i,j}(s) = \frac{1}{1+sT_{i,j}}\left[\frac{\Delta\omega_i}{R_{i,j}\times 2\pi}\right] \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{10}$$

$$ACE_i = \frac{\beta_i}{2\pi}\Delta\omega_i + \Delta P_{DCi,j} \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{11}$$

$$\Delta P_{DC}^{ref} = K_i \times \Delta\omega_i + K_j \times \Delta\omega_j \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{12}$$

$$\Delta P_{DCi,j} = \frac{1}{1+sT_{dc}} \times \Delta P_{DC}^{ref} \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{13}$$

$$\begin{cases} \frac{dx(t)}{dt} = A \times x(t) + B \times d(t) \\ y(t) = C \times x(t) \end{cases} \tag{14}$$

$$\begin{cases} x = \left[\Delta\omega_i \, \Delta\omega_j \ \Delta P_{Geni} \ \Delta P_{Genj} \ \Delta P_{DCi,j}\right]^T \\ d = \left[\Delta PL_i \ \Delta PL_j\right]^T \\ \forall i,j \in Area[1,2] \ or \ Area[4,3] \end{cases} \tag{15}$$

$$\begin{cases} A = e^{A_c \times T_s} \\ B = \int_{t=0}^{T_s} e^{A_c(T_s - t)} \times Bd(t) \end{cases} \tag{16}$$

An identification cyber-attack unit has been designed for areas 1 and 2, and another unit for areas 3 and 4. The frequency deviations are then passed through the cyber-attack detection unit before entering the steam turbine system. These units propose control strategies that identify cyber-attacks occurring in these areas, as well as transmission line attacks.

The wide-area measurement can be modified as a result of an FDI attack. Therefore, the discrete-time model of the system output under FDI attacks can be described by (17), where Y represents the corrupted output and f represents the

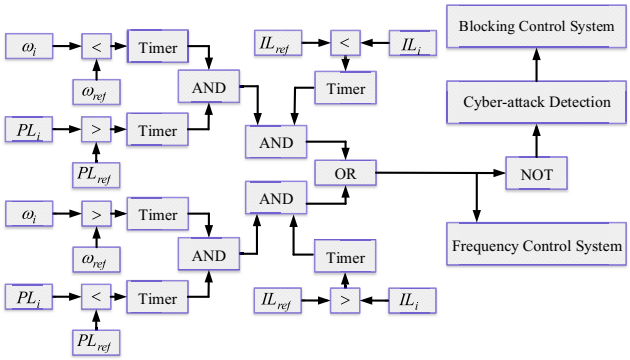

Fig. 6. The proposed method of identifying cyber-attacks on changes in load and frequency of areas.

FDI attacks. Cyber-attacks aimed at changing frequency deviations are modeled by (18) as well as attacks on transmission power between areas by (19).

$$Y_K = c \times x_k + f_k \tag{17}$$

$$ACE_i = \frac{\beta_i}{2\pi}\Delta\omega_i + \Delta P_{DCi,j} + f_{i,j} \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{18}$$

$$\Delta P_{DC}^{ref} = (K_i \times \Delta\omega_i) + \left(K_j \times \Delta\omega_j\right) + \left(K_{i,j} \times f_{i,j}\right) \quad \forall i,j \in Area[1,2] \ or \ Area[4,3] \tag{19}$$

According to the above equations, the attacker, knowing the power exchange control strategy between different areas, manipulates the frequency and load deviation coefficients to deceive the control system and disrupt power exchange. However, the cyber-attack detection unit continuously monitors all system changes using the real-time algorithm shown in Fig. 6, enabling the detection of any potential cyber-attack. The proposed method involves continuously comparing the frequency and load power in each area with their nominal values. The frequency control system will take action when there are conflicting changes in frequency and power levels. For instance, if power increases, the frequency should decrease in that area. If the frequency remains constant or increases when it should decrease, the control system identifies this as an attack and takes measures to prevent further disruption.

The second type of attack can be more sophisticated, with the attacker adeptly altering both the frequency and the load in opposing directions. In response, the proposed method evaluates the load current of the area relative to its nominal value. For instance, if the attacker increases the load power while simultaneously decreasing the frequency, it implies that no additional power is required from another area, as the power and frequency fluctuations within this area are deceptive and the result of a cyber-attack, as described in (17) to (19).

C. Proposed Control System for FDI Cyber-Attack Identification on DC Power Transmission Lines During Fault Conditions

In this study, to improve resilience, the proposed control system is evaluated against the second type of FDI cyber-attack aimed at sabotaging the system. As cyber-attacks are

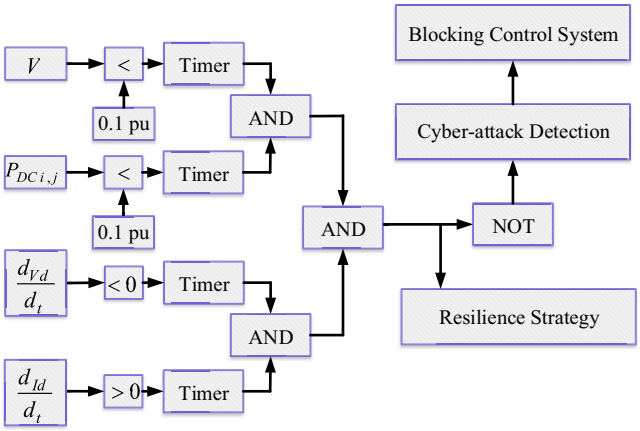

Fig. 7. The proposed method of identifying cyber-attacks on DC Power transmission lines in the condition of three-phase fault on the receiving side.

carried out with sophisticated intent, the attacker is aware that in the event of a three-phase fault occurring in either areas 2 or 3, the control system will isolate the faulted area as well as the DC transmission line of that area and transfer the load of the faulted area to another area to maintain the required power supply. Therefore, the attacker can target the voltage measuring device on the receiving end and the line power measuring device to disrupt the system. The study introduces a real-time method for identifying cyber-attacks designed to falsify the resilience improvement strategy, as depicted in Fig. 7. By using the proposed method, the transmission power between areas 1, 2 and areas 3, 4 is monitored along with three-phase voltage levels in areas 2 and 3. If both the three-phase voltages and the transmitted DC power are less than 0.1 pu, the control system identifies this as a fault and activates the resilience improvement control strategy, provided that the control system generates negative and positive voltage and current changes, respectively. Any other decrease in voltage or power is considered a cyber-attack, leading to disabling of the resilience control system.

D. Proposed Strategy to Improve Resilience in the Weaker Areas 2 and 3

In this section, strategies are proposed for enhancing the resilience of areas 2 and 3 in critical conditions by stronger areas 1 and 4. An example of such critical condition is the occurrence of a three-phase fault on the inverter side of these areas.

Fig. 8 show a flowchart illustrating the functional stages of the proposed resilience improvement strategy. In areas 2 and 3, the control system continuously monitors the three-phase voltage levels. If the three-phase voltages drop below 0.1 pu for more than 0.1 seconds, the resilience improvement strategy is activated. For this purpose, the integral of the time-weighted absolute error (ITAE) is used as a resilience metric, serving as a good performance index in designing controllers [33]. The ITAE index calculates the sum of errors in AC voltage in areas 2 and 3 using (20). In the case of a fault detection, the control system isolates the faulted area and then connects line 2 by closing its two-way connection boards. With this strategy, if

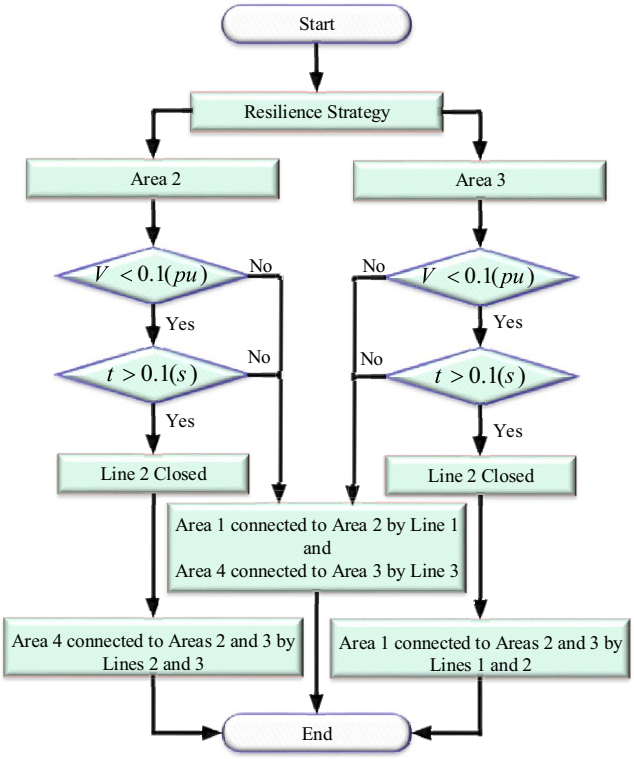

Fig. 8. Proposed control for enhancement of resilience in areas 2 and 3 by load shifting of areas 2 and 3 on each other and mutually supporting lines 1 and 3 from each other in fault conditions.

the fault occurs in area 2, the load of this area shifts to area 3, and both areas are supported by area 4 through lines 2 and 3. Similarly, in the event of a fault in area 3, the load of area 3, along with area 2, is supplied by area 1 through lines 1 and 2. However, under normal operational conditions, area 1 is connected to area 2 through line 1, and area 4 supports area 3 through line 3, and lines 2 and 4 are open. Also, regions 1 and 4 can support each other by closing line 4. In other words, when critical conditions arise in either area 2 or 3, the load of the faulted area can be transferred to the other area by line 2. Accordingly, the load on lines 1 and 3 can be changed with the changes in the area's load. In other words, lines 1 and 3 provide mutual support to each other during these conditions.

$$ITAE = \int_0^\infty t|e(t)|dt = \int_0^\infty t(|\Delta V_{ac}|)dt \tag{20}$$

IV. Simulation Results

The multi-area LCC-HVDC interconnected network of Fig. 1, with the described control strategies, is simulated using MATLAB/Simulink software. The results of this simulation are presented in this section.

A. Multi-Level Frequency Control Between Areas Through HVDC Lines

Step changes in power consumption of area 2 and the resultant changes in frequency of that area, without and with the proposed frequency control system, are presented in Fig. 9.

The load power changes from 200 MW to 600 MW, from 600 MW to 1.3 GW and from 1.3 GW to 200 MW at times

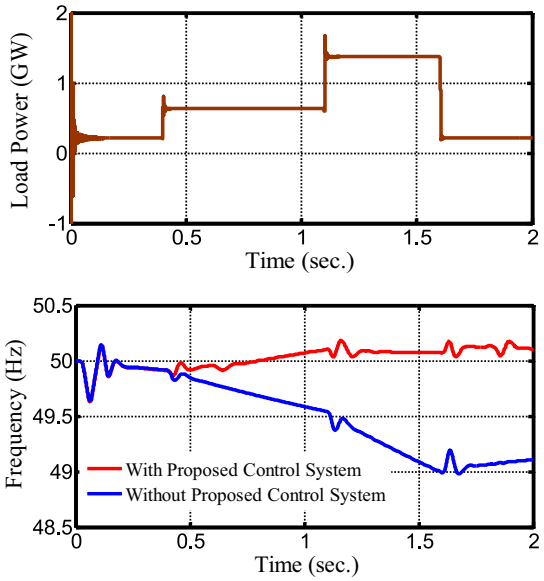

Fig. 9. Changes in power consumption of area 2 and resulting changes in the frequency without and with the proposed control system.

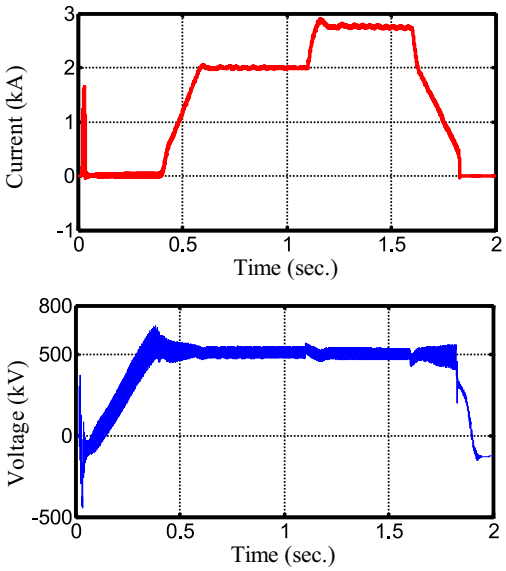

Fig. 10. Variations of LCC-HVDC line 1 current with its fixed voltage during frequency control of area 2 by taking power from area 1.

0.4, 1.1 and 1.6 seconds, respectively. According to Fig. 9, without the proposed frequency control system, a sudden load increase leads to a severe drop in frequency, reaching as low as 49 Hz. Even with a load reduction from 1.3 GW to 200 MW at 1.6 seconds, the frequency does not return quickly to 50 Hz. In contrast, when the frequency control system, presented in Fig. 4, is used, frequency control is achieved by absorbing active power from area 1 through LCC-HVDC line 1. As the load is increased at 0.4 and 1.1 seconds, the frequency remains within the nominal range, and after reducing the load at 1.6 second, the active power absorption function of line 1 is terminated, and the frequency remains at 50 Hz.

Fig. 10 illustrates the current and voltage of line 1 during the frequency control process from 0.4 to 1.1 seconds. Due to

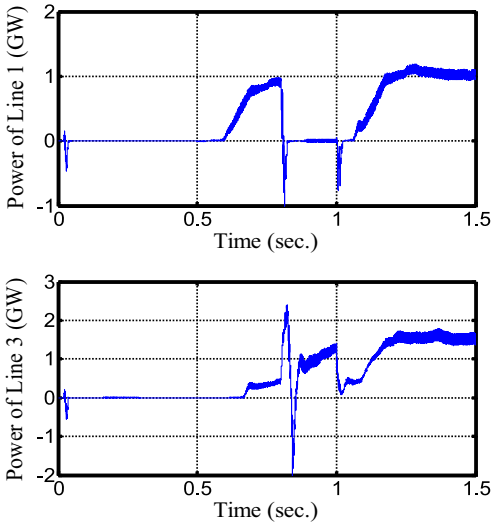

Fig. 11. Changes in power transmitted from lines 1 and 3 due to the occurrence of faults in area 2 and load changes in areas 2 and 3.

the operation of the proposed control system, the power transfers from area 1 to area 2 to compensate for the frequency of area 2, leading to changes in the current of DC line 1 according to the required power changes. From 0 to 0.4 seconds, the current is at zero due to the control system being inactive. Subsequently, in the first step (from 0.4 to 1.1 seconds), the operation of the control system has led to an increase in DC current up to about 2 kA. In the second step, from 1.1 to 1.6 seconds, the current has increased to 2.9 kA. Finally, in the third step, from 1.6 second onwards, since area 2 no longer required power from area 1, the transmitted DC current decreases gradually, reaching zero at 1.8 seconds. In all stages, the DC line voltage has been fixed at 500 kV. In essence, this indicate that the control system has provided the required power changes of area 2 through area 1 in several different steps, achieved by varying the DC current at a constant DC voltage.

B. Wide-Area Resilience Improvement

Fig. 11 shows the network resiliency improvement during a fault condition. Under normal condition, the load of area 2 increases, resulting in the power transfer of 900 MW through line 1 at 0.6 seconds. In area 3, due to load increase at 0.6 seconds, 300 MW of power is transmitted through line 3. At 0.8 seconds, a fault occurs at the power receiving station in area 2, and is cleared at 1 second. According to the strategy presented in Fig. 8, since the fault duration is more than 0.1 seconds and the voltage of the receiving side is zero, the control system has activated the resiliency improvement strategy. Consequently, the pre-fault power, originally transmitted through line 1, has been directed to line 3 following the occurrence of the fault. Therefore, the power of line 1 is reduced to zero from 0.8 to 1 second, and the power of line 3 has increased from 300 MW to 1.2 GW. After the fault is cleared at 1 second, control system is returned to its normal state, resulting in an increase in the transmitted power of line 1 up to 1 GW due to an increase in the load of area 2. Also,

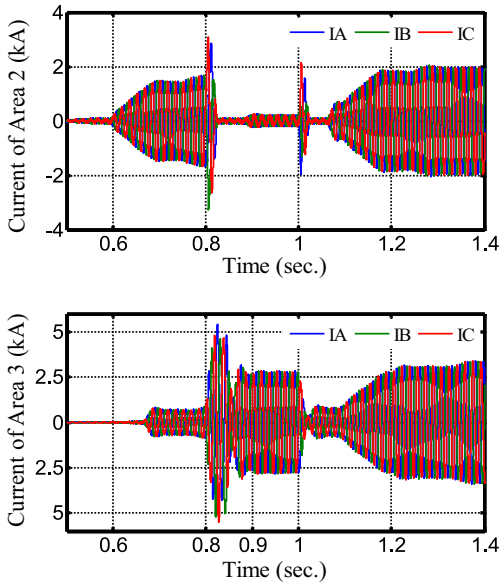

Fig. 12. Three-phase currents of areas 2 and 3 in the event of fault in area 2 and transfer of load to area 3 during time of the fault.

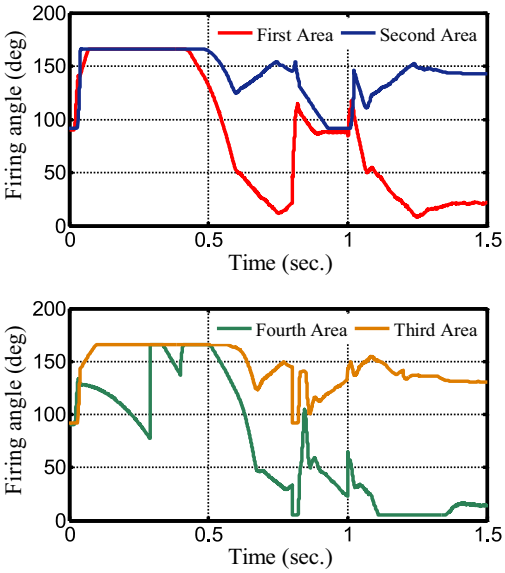

Fig. 13. Changes in the firing angles of the 12-pulse converters of the rectifier and inverter stations installed on lines 1 and 3 in the event of the fault and interruption of power transmission through line 1.

the transmitted power through line 3 has reached 1.5 GW at 1.2 seconds and 1.4 GW at 1.3 second, due to load changes in area 3.

The three-phase currents in areas 2 and 3 are shown in Fig. 12 in the event of a three-phase fault in area 2.

In Fig. 12, Before the fault, the currents in both areas are proportional to their loads. At 0.8 seconds, the fault occurs, causing line 1 to be isolated and the load of area 2 to be supplied through area 3 and line 2. The currents of each area return to the normal conditions after fault clearance at 1 second. Fig. 13 shows the firing angles of 12-pulse converters for the four zones. In regions 1 and 2, with the start of the power transmission process through line 1, the firing angle of the rectifier station in area 1 decreases to less than 90 degrees, while the firing angle of the inverter station in area 2 increases to more than 90 degrees. At 0.8 seconds, upon the occurrence of a fault, the firing angles of both mentioned stations are stabilized at 90 degrees, resulting in the shutdown of both stations and the interruption of power transmission through line 1. The firing angle of the station in area 4 (rectifier station) consistently remains less than 90 degrees, whereas that of the station in area 3 (inverter station) consistently stays greater than 90 degrees.

C. Detection of Cyber-Attacks on Load and Frequency Changes

As previously discussed, the FDI on the ACE parameter can lead to deviations in the rotor speed and, as a result, changes in the frequency within that region. Consequently, the frequency control system may redirect power from another area to the affected area if the attack goes undetected. This can result in a false interpretation due to frequency attacks.

Fig. 14 illustrates frequency deviations resulting from cyber-attacks and the injection of false information aimed at misleading the frequency control system. From 0 to 0.4 seconds, area 3 is in normal conditions without an attack. From 0.4 to 1.1 seconds, a cyber-attack occurs in area 3 with no frequency control system in place. Consequently, since the compensating power is not received from area 4, the mechanical torque between the generator and the low-pressure (LP) turbine decreases by 0.2 and 0.3 pu at 0.5 and 1 seconds, respectively. In other words, the attacker aims to demonstrate an increase in the system load and a decrease in the torque. Since the proposed control system is inactive in this period, this decrease in torque results in a sharp decrease in the frequency of area 3. When the proposed frequency control system is activated and the system faces such an attack in area 3, since massive power is injected into area 3 through area 4, the mechanical torque in region 3 increases, in contrast to the previous situation. Therefore, it can be concluded that whether the proposed frequency control is present or absent, cyber-attacks on ACE can lead to incorrect operation of the control system, resulting in an increase or decrease in frequency in the referred area.

According to Fig. 15, the control system successfully detects a cyber-attack aimed at manipulating the frequency at 0.42 seconds. Subsequently, the frequency control systems within the affected areas block power transmission through line 3. In this case, the control system notices the attack by checking the load of area 3 and its stability at 220 MW. This observation is important, as any changes in the mechanical torque (as shown in Fig. 14) should correspond to an increasing trend in the load within this area.

In another scenario in Fig. 15, the attacker has strategically targeted the parameter and power metering of area 3 and has also manipulated the mechanical torque with a negative trend. The voltage and current of the loads in area 3 have been monitored, and no noticeable changes has been observed. Therefore, the cyber-attack detection control system identified it as a cyber-attack, issuing an attack alarm at 0.42 seconds.

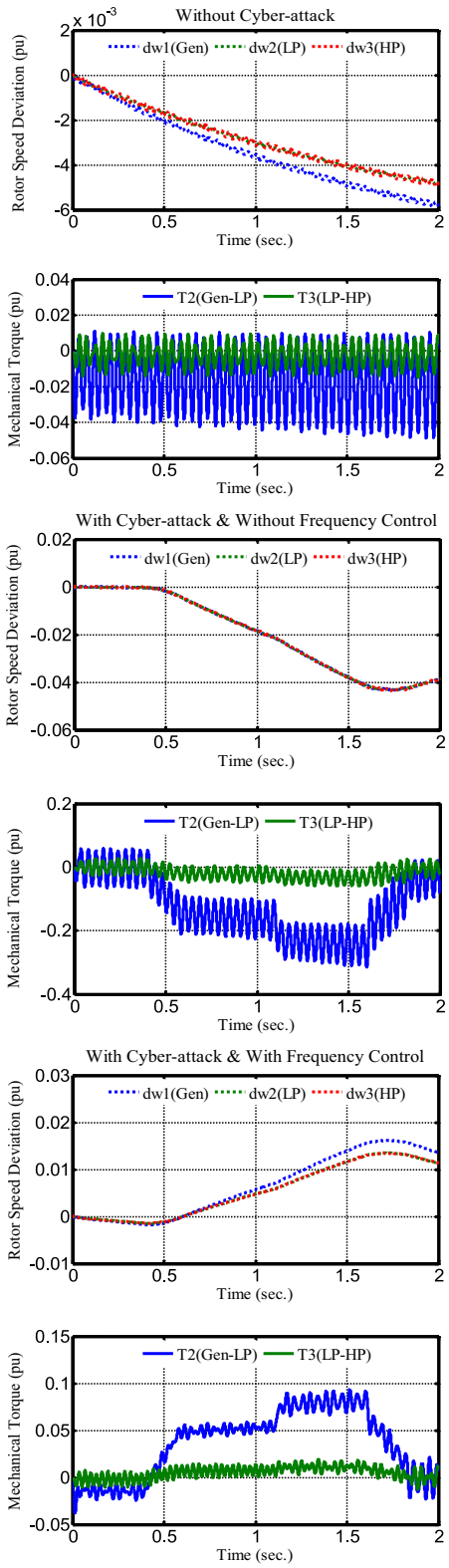

Fig. 14. Rotor speed deviation with mechanical torque fluctuations of the generator of region 3 in normal conditions and cyber-attack conditions without/with proposed frequency control system.

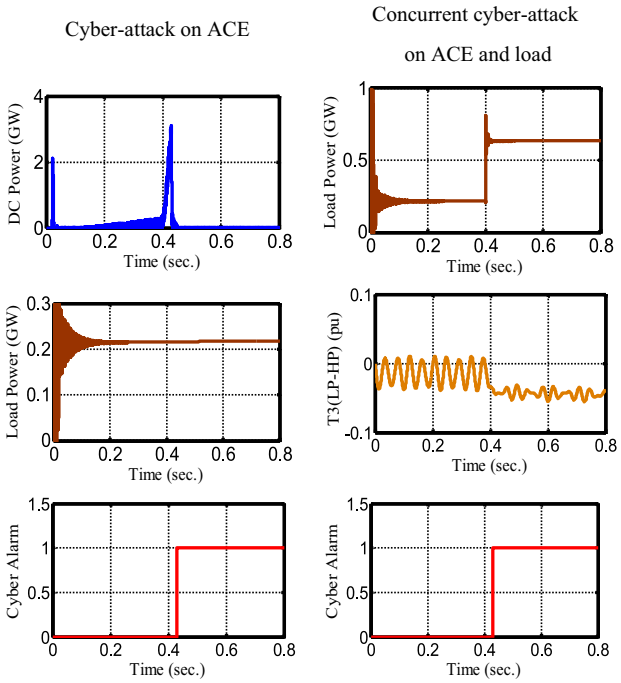

Fig. 15. Cyber-attacks occurred in area 3 with the aim of changing frequency of this area and causing frequency control system malfunction.

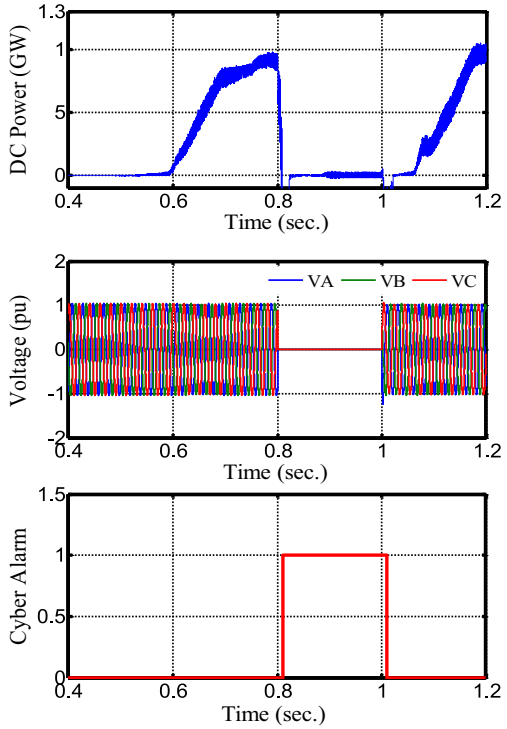

Fig. 16. Simultaneous cyber-attack on the power of transmission line 1 and the three-phase voltages of area 2.

D. Detection of Cyber-Attacks on DC Power Transmission Lines During Fault Conditions

In Fig. 16, a FDI cyber-attack has been initiated with the intention of preventing the transmission of power through line 1. As a result of this attack, both the power measuring devices on line 1 and the three-phase voltage on the inverter side are set to zero from 0.8 seconds to 1 second. Therefore, this creates an opportunity for the false activation of the resilience control system.

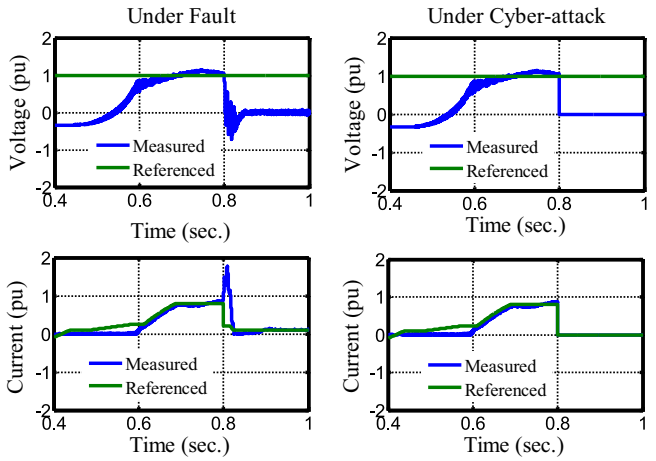

Fig. 17. Measured DC voltage and current changes in fault and cyber-attack conditions to create an algorithm to identify and differentiate between cyber-attacks and faults.

According to Fig. 17, a cyber-attack has been detected based on the pattern of DC voltage and current changes compared to the reference values during fault conditions. It is important to note that if the changes indicate a cyber-attack, the measured DC voltage and current will not show positive changes for current and negative changes for voltage within 0.8 seconds of the fault. When the fault occurs at 0.8 seconds, the measured voltage and current both go to zero, with more negative and positive ramps than their reference values, respectively. However, during a cyber-attack, this condition does not occur, and both the measured voltage and current simultaneously reach zero at 0.8 seconds with the reference values.

V. Conclusion

In this article, multi areas with varying frequencies and powers connected with LCC-HVDC lines was studied. In the network under study, areas 1 and 4, with 8 GVA/60 Hz each, are linked to areas 2 and 3, which operate at 1 GVA/50 Hz each, via lines 1 and 3. Furthermore, power exchange occurs between areas 1 and 4, as well as between areas 2 and 3, utilizing three-phase lines. The entire wide-area was controlled by a central frequency control system, which was responsible for adjusting and stabilizing the frequency of the weaker areas in case of an increase in load. If area 2 encountered a frequency change, area 1 would support it by sending power through line 1. Similar interconnections and support mechanisms existed between areas 3 and 4. Using the proposed frequency control system the multi-level frequency control was achieved.

Moreover, utilizing the resilience strategy of the entire network significantly contributed to the system's ability to operate effectively during three-phase fault conditions. This strategy ultimately led to an increase in the system's overall resilience. Furthermore, the implementation of algorithms and methods aimed at identifying FDI cyber-attacks, specifically targeting frequency control systems, played a crucial role in not only detecting potential sabotage attempts but also in enhancing the resilience of these systems.

As attractive suggestions for future research, it is feasible to consider the development of hybrid algorithms for operating the multi-level frequency control system proposed in this article for long-term frequency events simultaneously with the operation of frequency control systems in areas 1 to 4 to address short-term frequency events. Additionally, it would be compelling and significant to introduce a hybrid flexibility resilience enhancement strategy that addresses both three-phase faults and DC faults.

References

[1] Y. Li, H. Xiao, and X. Duan, "Theoretical parameter design method of SFCL for concurrent commutation failure inhibition in SFCL-segmented multi-infeed LCC-HVDC systems," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 1741–1757, May 2020.

[2] H. Xiao, Y. Li, and X. Sun, "Strength evaluation of multi-infeed LCC-HVDC systems based on the virtual impedance concept," *IEEE Trans. Power Syst.*, vol. 35, no. 4, pp. 2863–2875, Jul. 2020.

[3] E. Pierri, O. Binder, N. G. A. Hemdan, and M. Kurrat, "Challenges and opportunities for a European HVDC grid," *Renew. Sustain. Energy Rev.*, vol. 70, pp. 427–456, Apr. 2017.

[4] P. Bakas et al., "Review of hybrid multilevel converter topologies utilizing thyristors for HVDC applications," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 174–190, Jan. 2021.

[5] X. Li, C. Liu, and Y. Lou, "Start-up and recovery method with LCC–HVDC systems participation during AC/DC system black-starts," *IET Gener., Transm. Distrib.*, vol. 14, vol. 3, pp. 362–367, 2020.

[6] H. Xiao, K. Sun, J. Pan, Y. Li, and Y. Liu, "Review of hybrid HVDC systems combining line communicated converter and voltage source converter," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106713.

[7] A. Alassi, S. Bañales, O. Ellabban, G. Adam, and C. MacIver, "HVDC transmission: Technology review, market trends and future outlook," *Renew. Sustain. Energy Rev.*, vol. 112, pp. 530–554, Sep. 2019.

[8] P. Sun, H. R. Wickramasinghe, and G. Konstantinou, "Hybrid LCC-AAC HVDC transmission system," *Electr. Power Syst. Res.*, vol. 192, Mar. 2021, Art. no. 106910.

[9] Y. Xue and X. P. Zhang, "Reactive power and AC voltage control of LCC HVDC system with controllable capacitors," *IEEE Trans. Power Syst.*, vol. 32, no. 1, pp. 753–764, Jan. 2017.

[10] B. Hu, T. Niu, F. Li, K. Xie, W. Li, and H. Jin, "Dynamic var reserve assessment in multi-infeed LCC-HVDC networks," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 68–80, Jan. 2021.

[11] P. Gupta, A. Pal, and V. Vittal, "Coordinated wide-area control of multiple controllers in a power system embedded with HVDC lines," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 648–658, Jan. 2021.

[12] Y. Zhao, C. Liu, G. Li, and U. Annakkage, "Design of LCC HVDC wide-area emergency power support control based on adaptive dynamic surface control," *IET Gener., Transm. Distrib.*, vol. 11, no. 13, pp. 3236–3245, 2017.

[13] D. H. Kwon, Y. J. Kim, and O. Gomis-Bellmunt, "Optimal DC voltage and current control of an LCC HVDC system to improve real-time frequency regulation in rectifier- and inverter-side grids," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4539–4553, Nov. 2020.

[14] Y. Li, D. Shu, J. Hu, Z. Yan, Y. Zhou, and H. Wang, "A multi-area Thevenin equivalent based multi-rate co-simulation for control design of practical LCC HVDC system," *Int. J. Electr. Power Energy Syst.*, vol. 115, Feb. 2020, Art. no. 105479.

[15] A. Mojallal, S. Lotfifard, and S. M. Azimi, "Fault resilient multi-terminal HVDC systems using distributed corrective power dispatch," *IET Gener., Transm. Distrib.*, vol. 13, no. 19, pp. 4391–4399, 2019.

[16] J. Song, Y. Li, and Y. Zhang, "Fault steady-state analysis method for the AC system with LCC-HVDC infeed," *Electr. Power Syst. Res.*, vol. 192, Mar. 2021, Art. no. 106994.

[17] N. M. Haleem, A. D. Rajapakse, A. M. Gole, and I. T. Fernando, "Investigation of fault ride-through capability of hybrid VSC-LCC multi-terminal HVDC transmission systems," *IEEE Trans. Power Del.*, vol. 34, no. 1, pp. 241–250, Feb. 2019.

[18] T. Ding et al., "Quantifying cyber attacks on industrial MMC-HVDC control system using structured pseudospectrum," *IEEE Trans. Power Electron.*, vol. 36, no. 5, pp. 4915–4920, May 2021.

[19] S. Hopkins, E. Kalaimannan, and C. S. John, "Cyber resilience using state estimation updates based on cyber attack matrix classification," in *Proc. IEEE Kansas Power Energy Conf. (KPEC)*, 2020, pp. 1–6.
[20] B. Chen, S. I. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 592–602, Jan. 2021.
[21] R. Hemmati and H. Faraji, "Multifunctional scheme for frequency/voltage/stability control in HVDC line under concurrent cyber-attacks and faults," *IET Gener., Transm. Distrib.*, vol. 16, no. 7, pp. 1334–1348, 2022.
[22] C. Liao et al., "A resilience evaluation method considering power source ability and network topology of power systems," *IEEE Syst. J.*, vol. 17, no. 3, pp. 3527–3538, Sep. 2023.
[23] J. Wang, Y. Gong, C. Fu, Z. Wen, and Q. Wu, "A novel phase-locked loop for mitigating the subsequent commutation failures of LCC-HVDC systems," *IEEE Trans. Power Del.*, vol. 36, no. 3, pp. 1756–1767, Jun. 2021.
[24] Q. Jiang, B. Li, T. Liu, F. Blaabjerg, and P. Wang, "Study of cyber attack's impact on LCC-HVDC system with false data injection," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3220–3231, Jul. 2023.
[25] Z. Wang and S. Bu, "Design and defense of modal resonance-oriented cyber-attack against wide-area damping control," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2164–2178, Mar. 2024.
[26] Y. He, H. Zhong, G. Ruan, B. Zhou, S. Lu, and Y. Zhuo, "Multi-area asynchronous grid operation with frequency reserve sharing," *IEEE Trans. Power Syst.*, vol. 39, no. 6, pp. 7203–7215, Nov. 2024.
[27] S. Bhagat, L. Saikia, and N. Ram Babu, "Application of an optimal tilt controller in a partial loading schedule of multi-area power system considering HVDC link and virtual inertia," *ISA Trans.*, vol. 146, pp. 437–450, Mar. 2024.
[28] C. Yang, T. Cheng, S. Li, X. Gu, and L. Yang, "A novel partitioning method for the power grid restoration considering the support of multiple LCC-HVDC systems," *Energy Rep.*, vol. 9, pp. 1104–1112, Dec. 2023.
[29] A. Devnath, M. A. Rahman, and M. S. Rana, "Impact analysis of cyber-attack on MMC–HVDC control system with countermeasures," *Int. J. Dyn. Control*, vol. 12, pp. 1952–1962, Jun. 2024.
[30] M. Gul, N. Tai, W. Huang, H. Nadeem, M. Ahmad, and M. Yu, "Technical and economic assessment of VSC-HVDC transmission model: A case study of south-western region in Pakistan," *Electronics*, vol. 8, no. 11, p. 1305, 2019.
[31] O. Saadeh, B. Sba, and Z. Dalala, "Power system analysis of moving from HVAC to HVDC in the presence of renewable energy resources," *J. Electr. Comput. Eng.*, vol. 2023, pp. 1–19, Aug. 2023.
[32] J. C. Gonzalez-Torres, G. Damm, V. Costan, A. Benchaib, and F. Lamnabhi-Lagarrigue, "A novel distributed supplementary control of multi-terminal VSC-HVDC grids for rotor angle stability enhancement of AC/DC systems," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 623–634, Jan. 2021.
[33] R. Hemmati, H. Faraji, and N. Y. Beigvand, "Multilevel and advanced control scheme for multimicrogrid under healthy-faulty and islanded-connected conditions," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2639–2647, Jun. 2022.