A Cyber Attack Mitigation Scheme for Series Compensated DFIG-Based Wind Parks

Mohsen Ghafouri, *Member, IEEE*, Ulas Karaagac, *Member, IEEE*, Amir Ameli, *Member, IEEE*, Jun Yan, *Member, IEEE*, and Chadi Assi, *Fellow, IEEE*

***Abstract*—Subsynchronous Interaction (SSI) phenomenon is known to be one of the most frequent and severe stability issues of a Wind Park (WP), and can potentially lead to a significant loss of power generation. The broad impacts of this phenomenon on a power grid have made WPs interesting targets for cyber attacks. To initiate the SSI, an adversary can target either the power grid (external attacks) or the cyber system of WPs (internal attacks). This paper proposes a mitigation scheme for attacks that initiate the SSI phenomenon in series compensated doubly-fed induction generator (DFIG)-based WPs. External attacks are addressed by employing a robust static-output-feedback Subsynchronous Damping Controller (SSDC), which is designed based on the insensitive strip region and Linear Matrix Inequality (LMI) techniques. Internal attacks, however, are detected by comparing the estimated and measured converters' currents. Once the compromised measurements are detected, the designed SSDC is restructured to mitigate the attacks. The effectiveness of the proposed method is demonstrated using detailed Electromagnetic Transient (EMT) simulations for both internal and external cyber attacks. Additionally, the performance of the proposed method is corroborated using a real-time co-simulation framework.**

***Index Terms*—Cyber-attacks, doubly-fed induction generator (DFIG), insensitive design region, series capacitor compensation, subsynchronous interaction (SSI), wind park.**

I. Introduction

Wind, as a promising renewable source of energy, has been substantially harvested and integrated into power grids in recent years through the deployment of large-scale Wind Parks (WPs). Despite the undeniable socio-economic impacts of WPs on power grids, they can negatively affect the stability and operation of the network if they are not managed or controlled properly, as evidenced by the UK power outage in 2019 [1], [2] and ERCOT incident in 2009 [3]. Thus, due to the potential broad impacts of WPs on a power grid, they have become interesting targets for cyber attacks. For instance, in March 2019, a cyber attack targeted a WP in Salt Lake City, Utah, U.S., and ceased the operator's control over wind turbines (WTs) totaling 500 megawatts [4], [5]. It was following this incident that the U.S. Department of Energy published a report to emphasize on the necessity of dedicated attention to identify vulnerabilities, raise awareness, and develop strategies to protect wind energy infrastructure against cyber attacks [4].

Subsynchronous Interaction (SSI) phenomenon is known to be one of the most frequent and severe stability issues of a WP [6] that can potentially lead to a significant loss of power generation. As demonstrated in [7], [8] and confirmed by the incidents occurred in U.S. and China [9]–[11], series compensated Doubly-Fed Induction Generator (DFIG)-based WPs are prone to SSI. This phenomenon can be triggered by internal and external cyber attacks as well. An internal cyber attack can be initiated by exploiting the vulnerabilities exist in the communication links or industrial Internet of Things (IoT) devices of a WP's Supervisory Control and Data Acquisition (SCADA) system. For instance, a malware can be used to launch a cyber attack against a WP's industrial control system, similar to Stuxnet malware that targeted the SCADA system of Iranian nuclear facilities in 2010 [12]. On the other hand, an external cyber attack can initiate an SSI phenomenon by targeting neighboring substations' automation systems, similar to the cyber attack that targeted the Ukrainian power network substations in 2015 and 2016 [13]. Therefore, as the previous record of similar cyber attacks proves, SSI attacks are imminent and require proactive security measures.

External cyber attacks can be mitigated by adding a Subsynchronous Damping Controller (SSDC) to the control loops of DFIGs [14]–[23]. SSDCs offered in the literature are designed based on a wide range of techniques, including Linear Quadratic Regulator (LQR) and a full-state feedback observer [15], [16], proportional-integrator (PI) design [17], PI-like design based on an optimal quadratic technique [21], energy-shaping control [22], inertia phase locked loop [23], proportional derivative controller for Rotor Side Converter (RSC) [24], injecting subsynchronous current using a subharmonic voltage source converter [25], injecting currents at the subsynchronous frequency range based on bus voltages and line currents [26], partial feedback linearization [18], two-degree-of-freedom [19], and μ-synthesis [20]. The main techniques and corresponding challenges for the design and implementation of SSDCs are discussed in [27], [28]. Although the majority of these techniques are effective in damping SSI oscillations, they suffer from at least one of the following drawbacks: (i) not being resilient to cyber attacks, (ii) not being robust, i.e., their performance may deteriorate if the operating condition varies, and (iii) being complex in structure. Therefore, there is a need to design an SSDC that addresses all these issues.

On the other hand, as much as a robust SSDC can maintain the stability of a power system during external attacks, it can be a cause of instability during internal ones if it is not cyber-resilient. Since WPs are often of a very high order, which makes the design procedure of their SSDCs formidable, such controllers usually operate centrally based on the aggregated signals received from WTs [28]. As a result, SSDCs are often vulnerable to cyber threats originating from communication links or deployed IoT devices, as discussed above. Even in

the case of having a local SSDC, this controller is also prone to cyber attacks stemming from the IoT device in which the controller is implemented, or the ones that provide the controller with its inputs. These IoT devices can be targeted by malware that exploits the vulnerabilities inside their firmware. Therefore, an SSDC should be equipped with an auxiliary component to detect, identify, and mitigate cyber attacks before they render the system unstable.

Although mitigating SSI-related cyber attacks is crucial for the stable operation of DFIG-based WPs, to the best of the authors' knowledge, this issue has not been addressed to date. There are only a few studies in the literature on the cyber security of wind-based energy systems. However, these studies either analyze the security of WPs [29] or present availability-based attack models for them [30], [31]. Therefore, this paper is the first systematic effort to analyze SSI-related cyber attacks and mitigate them.

To fill the above-mentioned gaps, this paper proposes an attack mitigation strategy for SSI-related internal and external cyber attacks. The external attacks are mitigated by developing a robust SSDC designed based on insensitive strip region and Linear Matrix Inequality (LMI) techniques. The designed static-output-feedback controller has a simple structure, which makes it easy to implement, and is effective over a wide range of operating conditions. An observer-based attack detection, identification, and mitigation technique is also incorporated in the structure of the designed SSDC to address internal cyber attacks. On this basis, the contributions of the paper are summarized below:

- Demonstrating the abilities of internal and external attackers to launch SSI-based cyber attacks, and proving the impacts of such threats on the stability of power grids and WPs.
- Designing a robust static-output-feedback controller to mitigate external cyber attacks.
- Developing an observer-based auxiliary component for the SSDC to detect, identify, and mitigate internal SSI-based cyber attacks.

Although, the solutions proposed in [15], [20], and [28] often damp the SSI oscillations triggered by faults, the proposed method in this current paper differs from them due the following reasons. First, the LQR controllers proposed in [15] and [28] are not robust, i.e., they works only for a limited range of operating points. Thus, they might be ineffective for some external cyber attacks. Second, even though [20] presents a robust controller for damping SSI oscillations, the proposed controller in this current paper outperforms the one proposed in [20] (as shown in Section VI) due to minimizing the impacts of variations in the system operating point on the loci of eigenvalues. Third, internal cyber attacks have been totally ignored in [15], [20], and [28].

The rest of the paper is organized as follows: Section II presents the cyber-physical model of a WP; Section III discusses attack models and scenarios; in section IV the proposed SSDC is designed to address external cyber attacks; Section V addresses internal SSI-based intrusions; EMT simulations and Hardware-in-the-Loop (HIL) verification of the proposed method are presented in Section VI, and finally Section VII concludes the paper.

II. Cyber-Physical Modelling of WPs

The cyber-physical connection of a WP with a series compensated transmission system is depicted in Fig. 1. On the physical side, the WTs are connected to Medium Voltage (MV) feeders through WT transformers. These feeders form the MV collector grid that transmits the power from WTs to the Point of Interconnection (POI), i.e. the High Voltage (HV) transmission grid, through the WP transformer. A two-level control system, WT and WP levels, regulates several system parameters. The details of a typical DFIG-based WP physical model that contains protection, control and hardware (both the electrical and mechanical systems) can be found in [15].

A modern WP has an extensive communication of data between the WP operator and WTs, as well as a monitoring system. The data can be transferred (i) from WT to the SSCD of the WP (WPC), such as voltage, current, power, acceleration, pitch angle; (ii) from WPC to WT, such as voltage tracking reference [15], SSDC output signals [28]; or (iii) between the WP operator and smart grid operator, e.g., power generation, required reactive power. The structural health monitoring, energy management and condition monitoring can be also performed using this transferred data and cyber infrastructure [32]. The existing infrastructures including both wired (LAN network, fiber optic, etc.) and wireless (ZigBee, WiFi, WiMAX, etc.) communication systems are discussed and surveyed in [33]. The details of a WP cyber system are presented in [34] and [35] for a 34-WT and a 80-WT WPs in British Colombia and Denmark, respectively.

Inspiring from [30] and [32], the communication infrastructure shown in Fig. 1 is considered in this paper. The WTs communicate with a SCADA server in the control room, where the communication server manages the data transfer. The application server in the control room performs the basic operational functions and the database stores historian data of the system as well as the system logs. A Human Machine Interface (HMI) is also deployed in the control room to receive the necessary commands by the operator and a GPS antenna synchronizes the system and control room. Given that the safe operation of the transmission grid requires communicating data with the WP, a firewall is used to connect the control system of the wide area power system to the operating room of the WP.

The cyber-physical system shown in Fig. 1 can be represented by a linearized state-space model as follows:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u} \\ \mathbf{y} &= \mathbf{C}\mathbf{x} + \mathbf{D}\mathbf{u} \end{aligned} \tag{1}$$

where $\mathbf{x}$, $\mathbf{u}$, and $\mathbf{y}$ denote the vectors of the system states, inputs and outputs, respectively. The matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$ specify the small signal behavior of the linear model. In this model the transmission system and collector grid are modeled by a Thevenin equivalent system. The details of the linearization can be found in [15].

The test system of this paper is shown in Fig. 2. The WP consists of 268 DFIG WTs, each 1.5 MW, and is connected

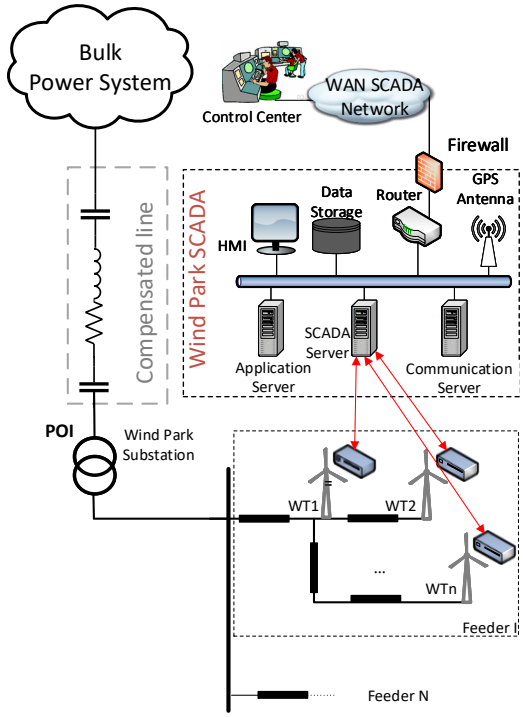

Fig. 1. Single line diagram of simplified system.

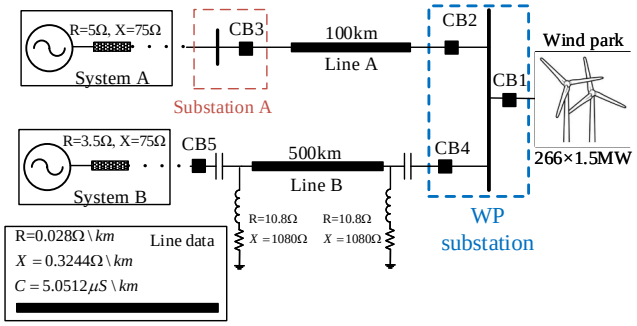

Fig. 2. The case study system

to two 500 kV transmission lines (Lines A and B) with the lengths 100 km and 500 km, respectively. These transmission lines are used to connect the WP to two large power systems, System A and System B, represented with their Thevenin equivalents. Line B is series compensated by two identical capacitor banks located at both ends, and provide a total of 50% compensation level. When Line A is disconnected, it leaves the WP radially connected to the series capacitor compensated line (Line B). Reader should refer to [15] for the details of this test system and its linearized state-space representation.

III. Attack Models and Scenarios

Two different cyber-attack models are presented in this section. An attacker aims to create a subsynchronous instability condition leveraging the WP and the associated power system connected to it. For these attacks, this paper assumes that the system data is already available to the attackers. In practice, the required data can be obtained through various techniques,

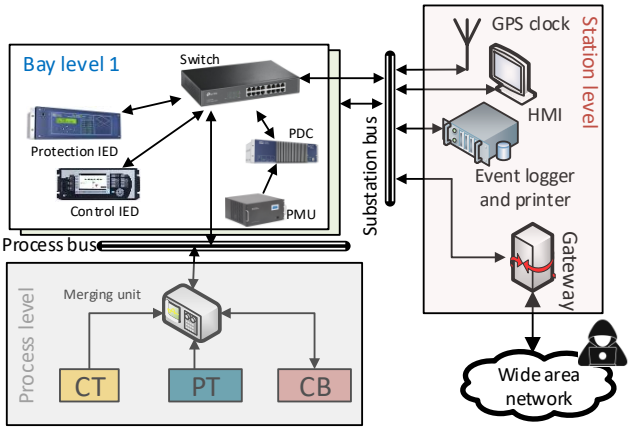

Fig. 3. The considered substation model.

such as by (i) taking advantage of insiders, (ii) compromising a database that contains system data, (iii) performing reconnaissance activities, (iv) eavesdropping a control center communication, or (v) deploying malware [36].

A. External Cyber Attacks

In this scenario, the adversary exploits the vulnerabilities of substation A (Fig. 2) to open CB3 and trip line A. The considered attack model is similar to the one occurred in 2015 and 2016 in the Ukrainian power system. The targeted substation model is demonstrated in Fig. 3 [37]. The adversary can change the status of Circuit Breakers (CBs), e.g., open or close them, using the connections in the cyber parts of the substation. For instance, the adversary can compromise the gateway, take the control of protection IED through substation bus and send the GOOSE trip command to CBs. On the other hand, IED devices of the substation can also be compromised using a malicious malware uploaded to them using patches or by physical access to them. A list of possible cyber attacks against substations and their consequences are detailed in [37], [38].

This paper considers two external cyber attack scenarios:

- Scenario A: The uncompensated line is tripped by an adversary who has compromised substation A. Consequently, the WP is radially connected to the series compensated line, and thus become vulnerable to SSI.
- Scenario B: The adversary compromises the substations of system B and causes a 30% decrease in the equivalent impedance of System B (a hypothetical scenario). Consequent to this attack, the SSI mode damping decreases.

B. Internal Cyber Attacks

The control system of a WP, particularly its SSDC, hugely rely on the availability and integrity of sensor data. In the internal attack model, it is assumed that the WP is equipped with an SSDC that damps SSI oscillations. Fig. 4 depicts the feedback control loop of an SSDC. In this loop, the measurements of WTs are sent to the SSDC through IEC 104 communication links, and the control signals are fed back to the WTs. As Fig. 4 shows, in this attack model the adversary

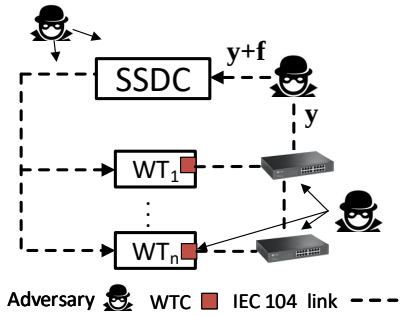

Fig. 4. The scheme of the attack model for internal threats.

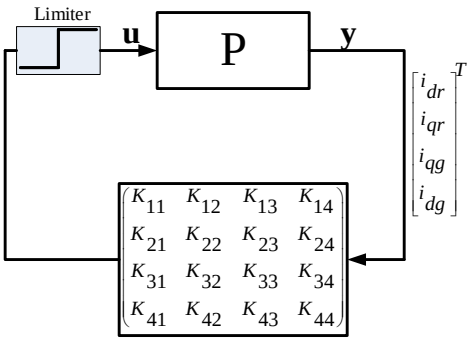

Fig. 5. Control schematic diagram of the closed-loop system.

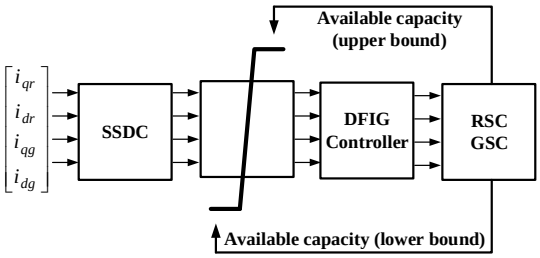

Fig. 6. Implementation of the SSDC within the control system of a DFIG

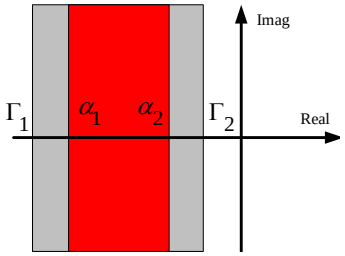

Fig. 7. The strip design regions $H(\Gamma_1, \Gamma_2)$ and $H(\alpha_1, \alpha_2)$

can compromise the communication link using a man-in-the-middle attack that falsifies the data of the WTs, for instance by adding a gain to the input of he SSDC. Additionally, the adversary can deploy malware on the SSDC or communication switches to falsify the data.

This paper considers the following internal cyber attack scenarios:

- Scenario C: In this attack scenario, it is assumed that the adversary has compromised the communication links of the SSDC and performs a false data injection attack. The adversary continuous the attack until a disturbance triggers SSI oscillations in the system. The cyber attack deteriorates the performance of the SSDC during the oscillations caused by the disturbance. The considered disturbance in this scenario is a three-phase metallic fault that occurs at POI side of the uncompensated line (Line A) at t = 1 s. The operating times of CB2 and CB3 are 60 ms and 80 ms, respectively.
- Scenario D: The attack procedure of this scenario is similar to the previous one. However, the disturbance that initiates the SSI oscillations is a three-phase fault that occurs at System B side of the compensated line (Line B) when the uncompensated line (Line A) is out of service. The fault happens at $t = 4$ s with the impedance of $Z = 0.3162,\ \Omega\ (X/R = 3)$ and it is removed at $t = 4.3$ s. This scenario imitates a fault condition inside System B (remote fault) and the extended fault clearing time is due to the operation of backup protection. In fact, this disturbance results in more severe SSI oscillations compared to the previous scenario.

IV. MITIGATING EXTERNAL CYBER ATTACKS BY DESIGNING A ROBUST SSDC

The objective of this section is to design a robust static-output-feedback ($\mathbf{u} = \mathbf{K}\mathbf{y}$) SSDC that mitigates SSI oscillations during external cyber attacks. The necessary and sufficient conditions for the existence of such controllers are described in [39]. The control diagram of the closed-loop system after implementing the proposed SSDC is shown in Fig. 5. As seen in this figure, the SSDC is zero-order and has a simple structure, i.e., it. contains only static gains and limiters, thus it is easy to implement. The limiters attenuate the impact of high-magnitude disturbances on the controller output to avoid saturation of converters. Fig. 6 illustrates the implementation of the SSDC within the control system of a DFIG. As shown in this figure, the SSDC is also limited dynamically to ensure the desired DFIG response during severe voltage sag and swell conditions. In this dynamic scheme, the upper and lower limits are calculated based on the available current capacity at the RSC and Grid Side Converter (GSC) of the DFIG [15]. The following presents the design procedure of an SSDC based on aggregated model of a WP.

Assuming the matrix $\mathbf{E}$ is obtained by adding a small perturbation to matrix $\mathbf{A}$ as

$$\mathbf{E} = \mathbf{A} + \Delta\mathbf{A} \tag{2}$$

where $\mathbf{A}$ and $\Delta\mathbf{A}$ are $n \times n$ real matrices ($\in \mathcal{R}^{n\times n}$). $\Delta\mathbf{A}$ is used to model the variations in the system parameters, e.g., impedance of grid or operating conditions. The maximum Euclidean distance between the eigenvalues of the matrix $\mathbf{E}$ ($\lambda^i_{\mathbf{E}}$) and the ones of $\mathbf{A}$ ($\lambda^i_{\mathbf{A}}$) can be expressed as:

$$S^{\mathbf{E}}_{\mathbf{A}} = \max_{1\le j\le n}\{\min_{1\le j\le n}|\lambda^i_{\mathbf{A}} - \lambda^i_{\mathbf{E}}|\} \tag{3}$$

The main aim here is to ensure that the system poles following the parameter variation remains in the desired region of s-plane. To achieve that, it is paramount to ensure that the neighborhood of eigenvalues calculated using $S^{\mathbf{E}}_{\mathbf{A}}$ is still inside the left half plane. In this regard, the Bauer-Fike theorem

presents an estimation bound for $S_{\mathbf{A}}^{\mathbf{E}}$ [40].

Bauer-Fike Theorem: If $\mathbf{A} \in \mathcal{R}^{n\times n}$ is diagonalizable and matrix $\mathbf{V} \in \mathcal{C}^{n\times n}$ exists such that

$$\mathbf{V}\mathbf{A}\mathbf{V}^{-1} = \Lambda = \text{diag}(\lambda_1, \ldots, \lambda_n) \tag{4}$$

then, $\mathbf{A}$ is referred to as nondefective. In this case, the upper bound of $S_{\mathbf{A}}^{\mathbf{E}}$ can be obtained as:

$$S_{\mathbf{A}}^{\mathbf{E}} \leq K(\mathbf{A})||\Delta\mathbf{A}|| \tag{5}$$

where $||\ ||$ denotes any induced norm and coefficient $K(\mathbf{A})$ can be calculated as:

$$K(\mathbf{A}) = ||\mathbf{V}||_2||\mathbf{V}^{-1}||_2 \tag{6}$$

It is worth mentioning that if $\mathbf{A}$ is a normal matrix (i.e., $\mathbf{A}\mathbf{A}^* = \mathbf{A}^*\mathbf{A}$), then $\mathbf{V}$ can be a unitary matrix i.e., $\mathbf{V}\mathbf{V}^* = \mathbf{I}$ where operator "*" denotes the conjugate transpose of the matrix [40]. Symmetric, orthogonal, and Hermitian matrices are all normal matrices. If $\mathbf{A}$ is a normal matrix and considering L_2-norm in (5), the unity eigenvectors ($||\mathbf{V}||_2 = ||\mathbf{V}^{-1}||_2 = 1$) can be leveraged to calculate $K(\mathbf{A})$ as detailed in [39]. Thus, (5) indicates that the maximum bound for $S_{\mathbf{A}}^{\mathbf{E}}$ is $||\mathbf{A}||_2$, i.e., $S_{\mathbf{A}}^{\mathbf{E}} \leq ||\Delta\mathbf{A}||_2$. As a result, the eigenvalues of $\mathbf{E}$ are restrained in a disk whose radius is $||\Delta\mathbf{A}||_2$ and centered on the corresponded eigenvalue of $\mathbf{A}$. It is also worth mentioning that if matrix $\mathbf{A}$ does not satisfy the conditions of a normal matrix, the radius of the bounding disk can be significantly large due to sensitivity to perturbation.

Eigenvalues of the closed-loop system, i.e., the ones of matrix $(\mathbf{A}+\mathbf{BKC})$, indicates the stability condition of the system. Depending on the system condition, this matrix may not be normal. Thus, the SSDC is designed using the symmetric matrix $\mathbf{A}_C^S$, since it is symmetrical and has similar eigenvalues compared to $(\mathbf{A}+\mathbf{BKC})$. In summary, the design objective is to restrain the eigenvalues of the $\mathbf{A}_C^S$ in a strip region, i.e.,

$$\Gamma_1 < \lambda^i(\mathbf{A}_C^S) < \Gamma_2 \tag{7}$$

where

$$\mathbf{A}_C^S = \frac{(\mathbf{A}+\mathbf{BKC})^T + (\mathbf{A}+\mathbf{BKC})}{2} \tag{8}$$

Since $\mathbf{A}_C^S$ is symmetric, the small perturbations in system parameters will not move the closed-loop eigenvalues out of the desired region. Assuming $\mathbf{K}$ to be the desired SSDC, the condition of equation (9) should always hold [40].

$$\begin{gathered}\Gamma_1 < \alpha_1 \leq \text{Real}(\lambda^i(\mathbf{A}+\mathbf{BKC})) \leq \alpha_2 < \Gamma_2 \\ \alpha_1 = \lambda_{min}(\mathbf{A}_C^S) \\ \alpha_2 = \lambda_{max}(\mathbf{A}_C^S)\end{gathered} \tag{9}$$

It can be observed that eigenvalues of the closed-loop system are confined in the strip regions $H(\Gamma_1, \Gamma_2)$ and $H(\alpha_1, \alpha_2)$, Fig. 7, i.e.,

$$\lambda^i(\mathbf{A}+\mathbf{BKC}) \in H(\alpha_1, \alpha_2) \subset H(\Gamma_1, \Gamma_2) \tag{10}$$

where

$$\begin{aligned}H(\alpha_1, \alpha_2) &= \{s | s \in \mathcal{C}, \alpha_1 \leq \text{Real}(s) \leq \alpha_2\} \\ H(\Gamma_1, \Gamma_2) &= \{s | s \in \mathcal{C}, \Gamma_1 \leq \text{Real}(s) \leq \Gamma_2\}\end{aligned} \tag{11}$$

The solution of the control problem can be transformed into an LMI as:

$$2\Gamma_1 < (\mathbf{A}+\mathbf{BKC})^T + (\mathbf{A}+\mathbf{BKC}) < 2\Gamma_2 < 0 \tag{12}$$

It is worth mentioning that in some practical cases, Γ_1 can be selected as $-\infty$ or a very large number. Then, the minimum of Γ_2, which represents the maximum damping, can be obtained using the following optimization problem:

$$\begin{cases}\min \Gamma_2 \\ \text{s.t.} (\mathbf{A}+\mathbf{BKC})^T + (\mathbf{A}+\mathbf{BKC}) < 2\Gamma_2 < 0\end{cases} \tag{13}$$

The subsynchronous mode frequencies are determined by the transmission system and WP operating conditions, and move almost horizontally in the s-plane. Therefore, confining the eigenvalues in a strip region with minimum Γ_2 ensures the maximum damping. The main advantage of this controller is its robustness against small perturbations in matrix $\mathbf{A}$, which are resulted from small variations in the operating conditions of the power system and WP. This advantage occurs due to confinement of the closed-loop eigenvalues ($\mathbf{A}_C^S$), and consequently the ones of $(\mathbf{A}+\mathbf{BKC})$, in $H(\alpha_1, \alpha_2)$ as shown in Fig. 7. It should be noted that the eigenvalues of ($\mathbf{A}_C^S$) are insensitive to perturbations due to symmetric structure of the matrix.

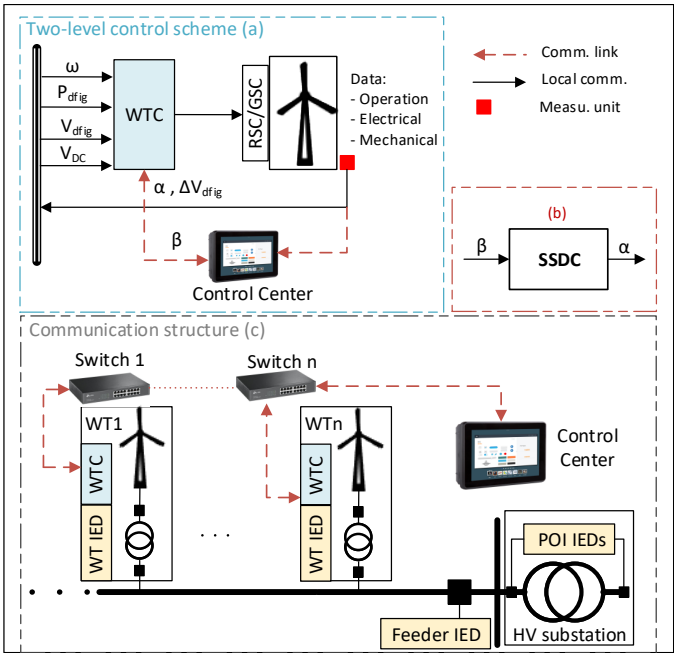

Fig. 8. Schematic diagram of the closed-loop control system.

Fig. 8 illustrates the schematic diagram of the closed-loop control system of a WP after implementing the proposed SSDC. Subfigure (a) illustrates the two-level control scheme of the WP, where β is a vector that contains the measurements of WTs, and α is the SSDC output sent to the WTs. Additionally, subfigures (b) and (c) show the input and output signals of the SSDC and the required communication structure, respectively.

V. DETECTING AND MITIGATING INTERNAL SSI-BASED CYBER ATTACKS

This section proposes an auxiliary component for an SSDC to detect, identify, and mitigate internal SSI-based cyber attacks. The block diagram of the proposed auxiliary component is illustrated in Fig. 9. In the Feature Generation block, which includes the mathematical model of the WP and the power system described in (1), the features of the system, i.e., residues [41], are generated. Residues are defined as the difference between the measured and estimated outputs of the system (i.e., converters' currents in the dq-frame). Since these outputs are also among the system states, a robust state observer, which is designed based on quadratic stability technique, is used to estimate the states of the system. Using the estimated states, the residues are calculated and sent to the Attack Detection block, which compares the system residues with specified thresholds. If any of the residues exceeds its associated threshold, attacks are detected and the Attack Diagnosis block identifies the compromised channels. In the next step, the gain scheduling technique, which is widely used in adaptive control domain [42]–[45], is used to mitigate cyber attacks. Gain scheduling is an approach in which a family of controllers that provides satisfactory control for different conditions is used [46]. Using this technique and based on the compromised channels identified in the previous step, the structure of the SSDC is altered and an appropriate one is activated. This SSDC has been designed previously based on the uncompromised channels. Therefore, to mitigate cyber attacks, $n = 2^G - 1$ (where G is the number of SSDC input signals and is 4 in this study) separate SSDCs must be designed for all possible combinations of input signals. Once a combination of the inputs is compromised, the SSDC that is designed only for the healthy inputs will be used. For example, when GSC d-axis current is compromised, the SSDC that is designed based on the remaining three input signals is selected. It should be noted that, as shown in Section IV, a lower number of inputs is also sufficient for achieving the desired damping over the possible operating range of the WP and power grid. Additionally, an improved attack resiliency can be attained by transferring the data using different communication media as a diversification approach.

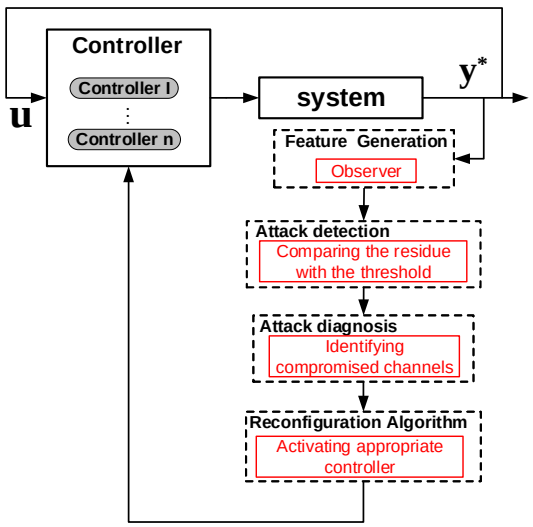

Fig. 9. The block diagram of the proposed attack detection, identification, and mitigation component.

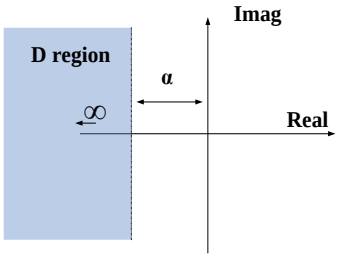

Fig. 10. Predefined D-region.

A. Designing a robust state observer

The family of an uncertain system with interval parametric uncertainty in the impedance of the equivalent power system (i.e., R, X and X_C) can be represented as:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}(\delta)\mathbf{x} + \mathbf{B}\mathbf{u} \\ \mathbf{y} &= \mathbf{C}\mathbf{x} \end{aligned} \tag{14}$$

where δ is an uncertain parameter within a specified range (i.e., $\delta \in [\delta^- \quad \delta^+]$). The dynamic of an observer that estimates the states of (14) is expressed as [36]:

$$\dot{\mathbf{e}} = (\mathbf{A} - \mathbf{L}\mathbf{C})\mathbf{e} \tag{15}$$

where $\mathbf{e} = (\mathbf{x} - \hat{\mathbf{x}})$ is the error signal, $\mathbf{x}$ is the state vector and $\hat{\mathbf{x}}$ is the vector of estimated states. The problem of designing an observer reduces to finding the observer's gain, i.e., $\mathbf{L}$. To this aim, Δ_I is assumed to be the set of all possible edges of the uncertainty space, and is defined as follows:

$$\Delta_I = \{\delta = [\delta_1, \delta_2, \ldots, \delta_k] | \delta_i = \delta_i^- \text{ or } \delta_i^+, i = 1, 2, \ldots, k\} \tag{16}$$

D-region (see Fig. 10), i.e., the desired region for the poles of the observer, is defined by the proper definition of matrices $\mathbf{N}$ and $\mathbf{M}$ in:

$$\mathbf{D} = \mathbf{N} + s\mathbf{M} + \bar{s}\mathbf{M}^T \tag{17}$$

where s is the Laplace variable. The following theorem describes the procedure of observer design based on quadratic stability [40].

Theorem: The problem of finding the observer gain matrix based on the quadratic stability technique reduces to finding the positive-definite matrices $\mathbf{P}$ and $\mathbf{W}$ satisfying the following LMI:

$$\begin{aligned} \mathbf{N} \otimes \mathbf{P} + \mathbf{M}(\mathbf{A}^T(\delta)\mathbf{P}) + \mathbf{M}^T \otimes (\mathbf{P}^T\mathbf{A}(\delta)) + \\ \mathbf{M} \otimes (\mathbf{C}^T\mathbf{W}) + \mathbf{M}^T \otimes (\mathbf{W}^T\mathbf{C}) < 0 \end{aligned} \tag{18}$$

The proof of this theorem can be found in [34]. By choosing the desired D-region to be the shifted left half plane, as shown in Fig. 10, (18) is simplified as follows [40]:

$$\begin{gathered}\mathbf{A}^T(\delta)\mathbf{P}+\mathbf{P}\mathbf{A}(\delta)+\mathbf{C}^T\mathbf{W}+\mathbf{W}^T\mathbf{C}+2\alpha\mathbf{P}<0\\ \mathbf{P}>0\\ \forall\delta\in\Delta_I\\ \mathbf{L}=\mathbf{W}\mathbf{P}^{-1}\end{gathered}\tag{19}$$

where α is the distance between the imaginary axis and D-region. The selected D-region ensures that the damping of the observer poles is higher than a certain value. The optimization problem described by (19) and (16) is solved using the *LMI toolbox* [47] of *MATLAB*.

B. Differentiating between cyber attacks and disturbance

Similar to cyber attacks, power system transients (e.g., due to the occurrence and clearance of electrical fault) may also result in an abrupt change in the residues. A successful discrimination between these two types of events is achieved through an averaging process and selection of a proper threshold (η). Low averaging frequency result in smooth residue and consequently late attack detection. High averaging frequency results in fast detection as it updates the residue quickly, but false attack detection can be expected. EMT simulations demonstrate that a wide range of averaging frequency can provide desired SSDC performance.

VI. Performance Evaluation

Simulations are performed using EMTP [48] and the generic WP model in [49], [50]. Given that the switching frequency of converters is much higher than the subsynchronous resonance frequency, the very fast dynamics of converter switchings do not impact the subsynchronous resonance behavior of the system. Thus, DFIG converters are represented by their average value models. Simulation time step is 50 μs. The following subsections evaluate the performance of the proposed method for internal and external cyber attacks using EMT simulations and a real-time co-simulation framework.

A. Mitigating External Cyber Attacks

This subsection first evaluates the robustness of the proposed SSDC for different operating conditions, and then assesses its effectiveness in Scenarios A and B.

1) Robustness of the proposed SSDC: This subsection verifies the robustness of the proposed SSDC under various operating conditions. To this aim, the following three cases are defined: (i) wind speed changes between 0.6 to 0.8 p.u., where the base value for computing wind speed in p.u. is the maximum possible operating speed of wind turbines (11.24 m/s) [49], [50]; (ii) reactive power generation of the WP varies between 0 to 0.2 p.u.; and (iii) the number of in-service WTs is reduced by 25% and 50%. In all cases, a three-phase metallic fault happens at POI of the WP at $t = 1.2$ s. Thus, when the CBs of Line A open at $t = 1.26$ s to clear the fault, the WP becomes radially connected to the series compensated line and the SSI oscillations are triggered. Figs. 11-13 present the generated active and reactive power components of the WP associated with the defined three cases. As these figures show, the proposed SSDC successfully damps the SSI oscillations in different operating conditions. Such a result was expected, since the SSDC is designed based on robust control techniques that handle the operational uncertainties of WPs. However, if the controller does not operate properly, the oscillations grow and the system moves toward instability.

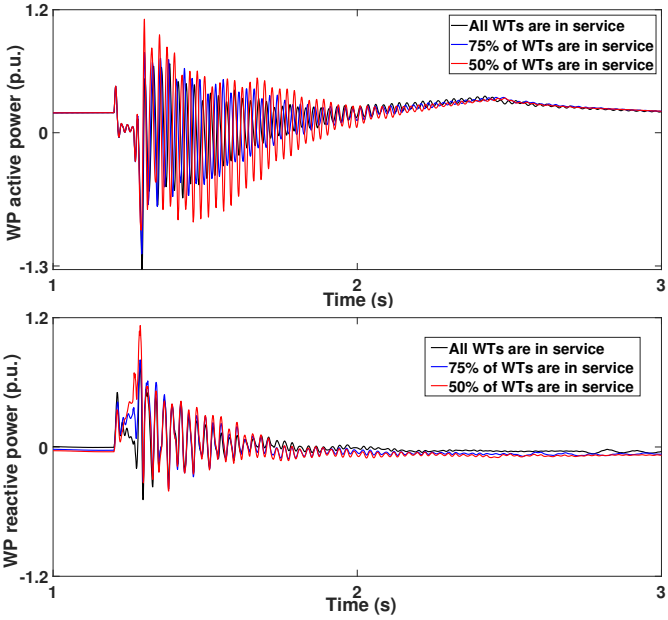

Fig. 11. WP active and reactive power components when 100%, 75%, and 50% of WTs are in service.

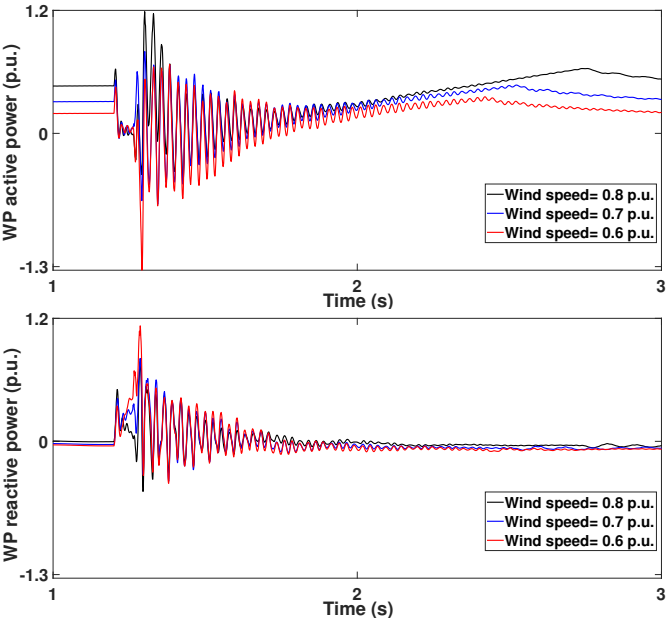

Fig. 12. WP active and reactive power components for 0.6 p.u., 0.7 p.u., and 0.8 p.u. wind speeds.

Additionally, the proposed SSDC is compared with the robust μ-controller presented in [20]. To this aim, both controllers are tested following the fault described above, and the results are presented in Fig. 14. As this figure shows, the proposed SSDC outperforms μ-controller in terms of provided damping.

2) Mitigating cyber attacks in Scenarios A and B: Fig. 15 and Fig. 16 show the WP active power outputs following

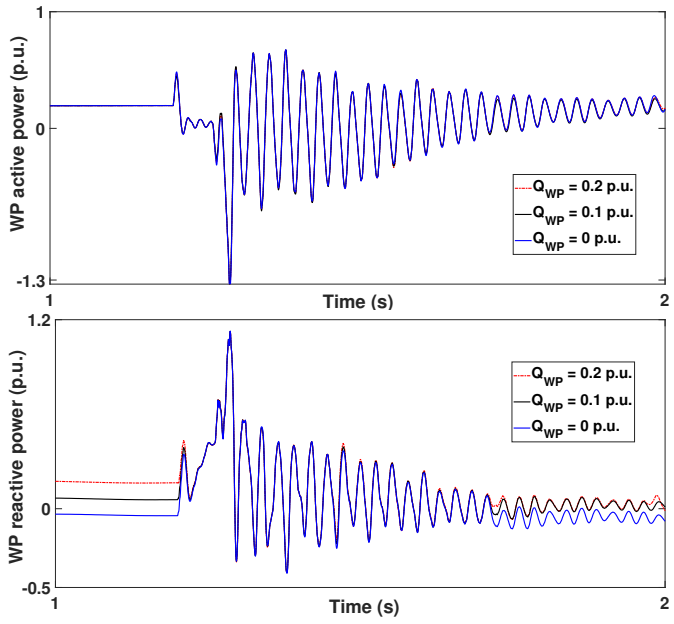

Fig. 13. WP power components for 0.2 p.u., 0.1 p.u., and 0 p.u. generation of reactive power.

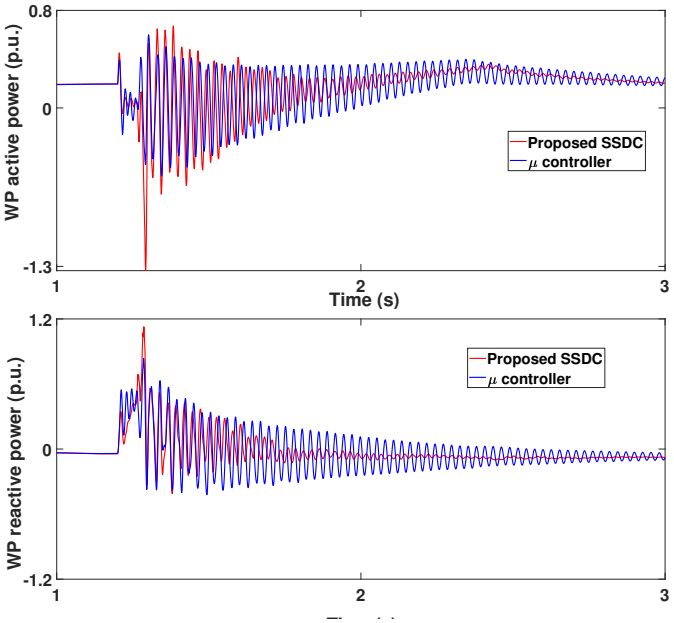

Fig. 14. The comparison between the performance of the proposed SSDC and the controller presented in [20].

the external cyber attacks described in Scenarios A and B, respectively. In both scenarios, the wind speed (V) is 0.6 pu, which is the lowest permissible wind speed for WTs. It should be noted that lower wind speed results in more severe subsynchronous oscillations. As these figures show, in both scenarios, the system becomes unstable following the attacks when the WP is not equipped with the proposed SSDC. Thus, Fig. 15 and Fig. 16 clearly demonstrate the effectiveness of the proposed SSDC against external cyber attacks. It should be emphasized that, SSDCs are typically designed to achieve a desired damping for a wide range of operating conditions for the power grid and WP. Therefore, the considered external

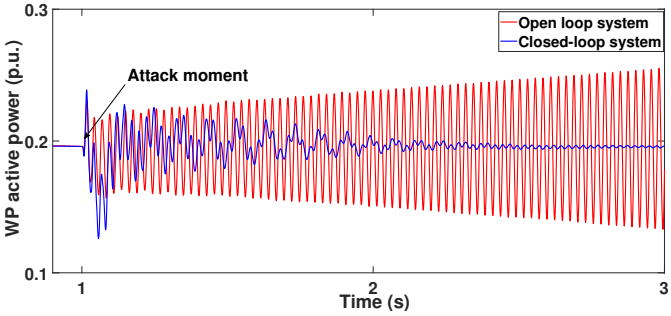

Fig. 15. WP active power output following an attack to Substation A that trips the circuit breaker CB3 (Scenario A).

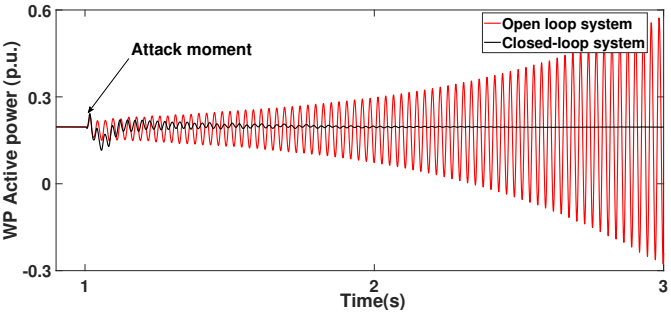

Fig. 16. WP active power output following an attack to System B substations that results a 30% reduction in equivalent impedance of System B (Scenario B).

cyber attacks are not expected to cause an SSI problem if the WP is equipped with a well-designed SSDC.

B. Mitigating Internal Cyber Attack

The system responses to internal cyber attacks described in Scenarios C and D are presented in Fig. 17 and Fig. 18, respectively. In both scenarios, the attacker adds a 30% gain to the q-axis GSC current measurement (i_{qg}) in both scenarios and waits until the disturbances described in these scenarios occur (at $t = 1$ s and $t = 4$ s in Scenarios C and D, respectively). The lowest permissible wind speed is considered in both scenarios. As these figures show, in the absence of the proposed auxiliary component, the attacks deteriorate the performance of the SSDC and give rise to sustained oscillations. However, the proposed auxiliary component removes the compromised channel (i_{qg}) from the feedback loop and activates the SSDC that has been designed based on the other three input signals, i.e., d-axis GSC current (i_{dg}), and d- and q-axis RSC currents (i_{dr} and i_{qr}, respectively). Therefore, the proposed method mitigates the cyber attacks and the oscillations are effectively damped.

The threshold $\eta = 0.09$ and averaging frequency is 20 Hz in the proposed auxiliary component. Fig. 19 represents the residue signal following the attack for different averaging frequencies. Low averaging frequency fully eliminates the adverse effects of the short lived large electrical system transients that occurs following severe disturbances. However, it is at the expense of late attack detection. It should be noted that, averaging frequency selection is not a challenge as a wide range of averaging frequency provides acceptable response

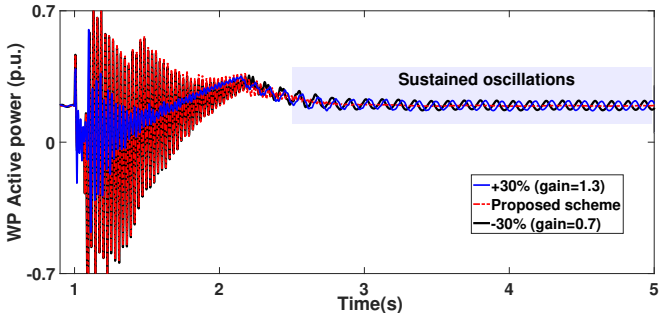

Fig. 17. WP active power output in Scenario C (30% gain change in SSDC q-axis GSC current input at 0.5s).

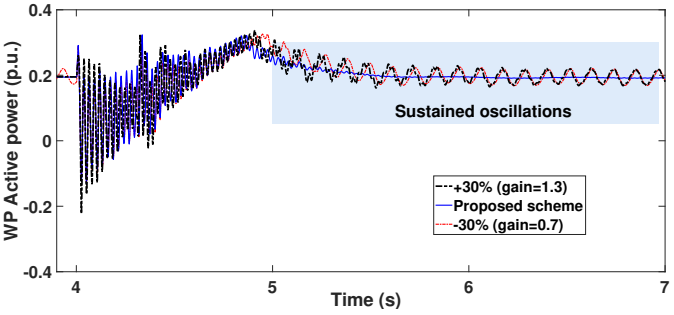

Fig. 18. WP active power output in Scenario D (30% gain change in SSDC q-axis GSC current input at 3s).

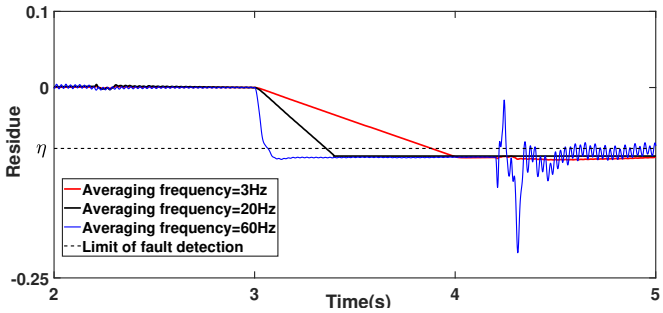

Fig. 19. The residue following 30% gain change in q-axis GSC current.

time and desired immunity against sudden residue variations due to electrical system transients.

To further investigate the performance of the proposed method, a new Scenario E that combines Scenarios C and D is considered in this section. The attack in Scenario C adds a %30 gain to q-axis GSC current and the attack in Scenario D does the same to d-axis GSC current. Fig. 20 presents the active power and voltage at WP's POI in Scenario E. This figure also illustrates the attack detection and SSDC activation instants following the second attack. The SSDC activated after the first attack is designed based on i_{dg}, i_{qr}, and i_{dr} (the other input, i.e., i_{qg} is isolated due to the first attack). The second SSDC is activated after the second attack, and it uses i_{qr} and i_{dr} (i.e., only the RSC current measurements, as i_{dg} is also isolated due to the second attack). As seen in Fig. 20, the transition from the first SSDC to the second one is very smooth, without noticeable transients. The presented waveforms confirm the effectiveness of the proposed SSDC and the auxiliary component. It should be noted that the voltage at the POI is not as large as the previous fault

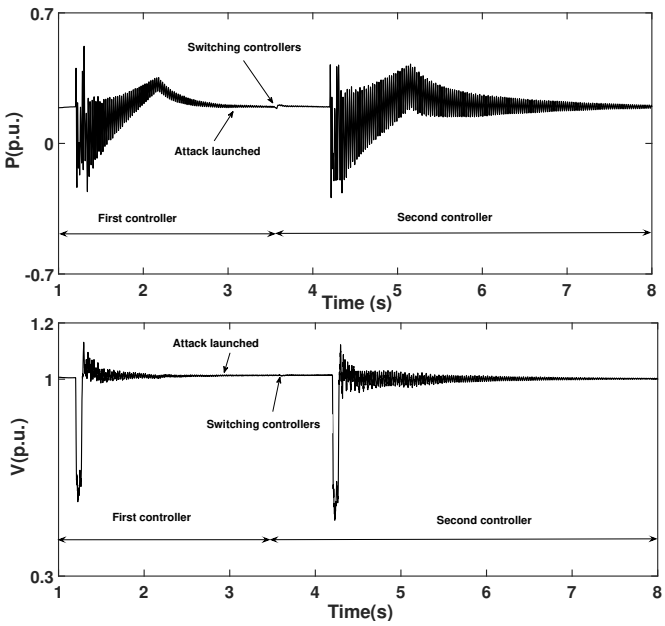

Fig. 20. WP active power output and voltage at POI in Scenario E.

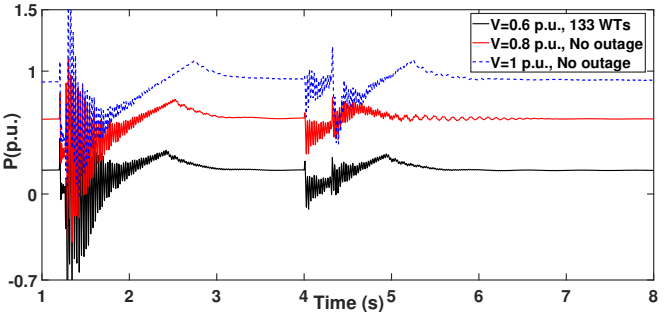

Fig. 21. WP active power output in Scenario E for different wind speed and WT outage scenarios.

scenario during the fault due to following reasons: (i) the fault impedance is non-zero, (ii) the locations of the fault and the POI are far from each other, i.e., the fault is distant, and (iii) WTs are equipped with fault ride-through (FRT) function and inject reactive currents for voltage support.

Additionally, this section evaluates the proposed method for operation conditions other than the one considered in the design procedure (the most vulnerable to SSI). To this aim, Scenario E is repeated when (i) $V = 0.6$ p.u. and 133 WTs are in service, (ii) $V = 0.8$ p.u. and all WTs are in service, and (iii) $V = 1$ p.u. and all WTs are in service. Fig. 21 shows the active power of the WP during the above cases. As this figure shows, in all cases the cyber attacks are successfully mitigated and the oscillations are effectively damped.

C. Real-time co-simulation framework

The under-study system is modeled in a co-simulation framework to validate the effectiveness of the proposed control schemes. To this aim, a HYPERSIM Digital Real-Time Simulator (DRTS) is integrated into a larger co-simulation platform, which interconnects the DRTS with the SSDC through an HIL framework over a network managed by OpenStack. In this platform, the WP and power grid are modeled in the DRTS,

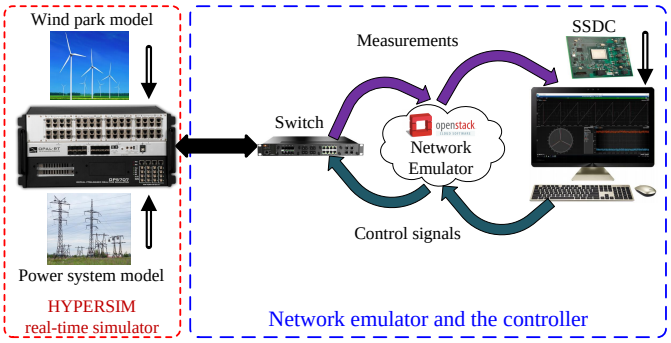

Fig. 22. The developed co-simulation framework.

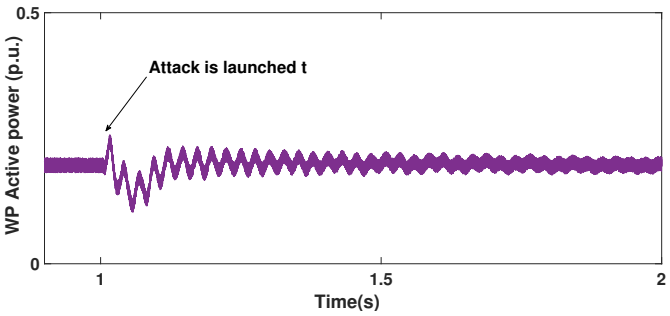

Fig. 23. The active power generation of WP in the attack Scenario B.

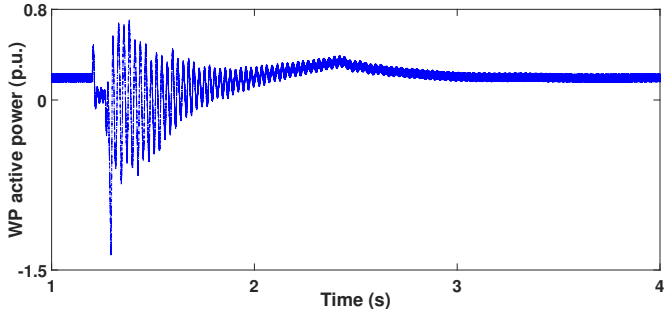

Fig. 24. The active power generation of WP in Scenario C.

and the communication system is emulated by OpenStack. Similar to the EMT simulations, the SSDC receives WT currents in dq-axis over the communication network, and produces the control signals, which are added to the inner loops of the RSC and GSC. Fig. 22 shows the developed co-simulation framework.

To demonstrate the performance of the system using the developed co-simulation framework, first, Scenarios B and C (for $V = 0.6$ p.u. and 50% of WTs in-service) are carried out again. The results are demonstrated in Fig. 23 and Fig. 24. Comparing these figures with Fig. 16 and Fig. 17 reveals that real-time co-simulation testing of the proposed method yields the same results as obtained for Scenarios B in C in previous subsections.

In addition, this subsection defines two new scenarios, i.e., F and G. In both scenarios, which are similar to Scenario E, the attacker adds a 40% gain to d- and q-axis currents of the RSC. In Scenarios F and G, 100% and 50% of the WTs are in service, respectively. Fig. 25 and Fig. 26 show the active and reactive power components of the WP in these

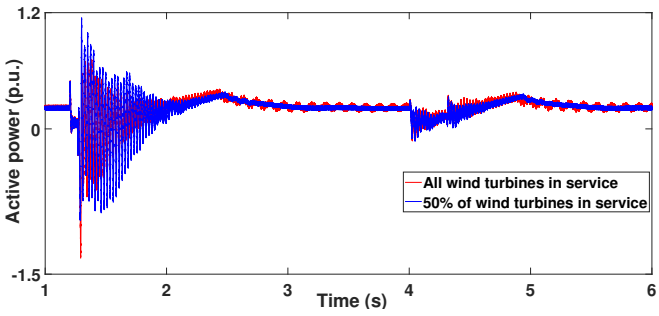

Fig. 25. The active power generation of the WP during Scenarios F and G.

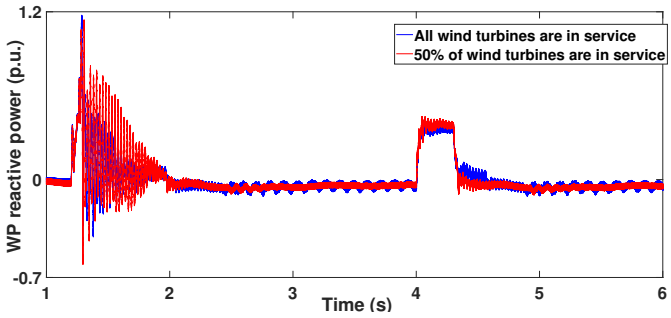

Fig. 26. The reactive power generation of the WP during Scenarios F and G.

scenarios. As the results of this section prove, the auxiliary component mitigates the cyber attacks, and the proposed SSDC successfully damps the oscillations.

VII. Conclusion

This paper proposed an attack mitigation technique for both internal and external SSI-related cyber attacks. External attacks were mitigated by using a robust static-output-feedback SSDC. Internal SSI-related cyber attacks, however, were mitigated by augmenting the SSDC with an auxiliary component that detects, identifies, and mitigates threats. The EMT simulations and real-time co-simulations demonstrated that by implementing the proposed method, including the SSDC and its auxiliary components, both types of cyber attacks are mitigated and resultant oscillations are effectively damped. Additionally, it was shown that the proposed SSDC is robust for different operating conditions. The other advantages of the proposed method include simplicity of the SSDC (zero order structure) and easy implementation (due to the availability of SSDCs' inputs in WTs and often in WPs' SCADA, and the existence of required communication links).

Similar to many other cyber-security improvements, the proposed method comes at the cost of increasing the computation complexity of the WP control system and affecting the SSDC's reliability. However, thanks to the state-of-the-art processing technologies and robust observer design methods, the improved cyber-security of SSDCs overshadows the incurred costs.

VIII. Acknowledgement

This work was partially supported by Concordia Institute for Information Systems Engineering (CIISE) through Start-up Fund under Grant V01325, and also partially supported by

the Department of Electrical Engineering at The Hong Kong Polytechnic University through the Start-up Fund Research Project under Grant 1-ZVLU.

REFERENCES

[1] "Technical report on the events of 9 august 2019," *National Grid ESO*, 2019. [Online]. Available: https://www.nationalgrideso.com/document/152346/download

[2] K. F. Forbes and E. M. Zampelli, "Accuracy of wind energy forecasts in great britain and prospects for improvement," *Utilities Policy*, vol. 67, p. 101111, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957178720301053

[3] M. Sahni, B. Badrzadeh, D. Muthumuni, Y. Cheng, H. Yin, S. . Huang, and Y. Zhou, "Sub-synchronous interaction in wind power plants- part ii: An ERCOT case study," in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–9.

[4] "Roadmap for wind cybersecurity." [Online]. Available: https://www.osti.gov/biblio/1647705

[5] "Eenews, first-of-a-kind u.s. grid cyberattack hit wind, solar." [Online]. Available: https://www.eenews.net/assets/2019/10/31/document_ew_03.pdf

[6] R. N. Damas, Y. Son, M. Yoon, S. Y. Kim, and S. Choi, "Subsynchronous oscillation and advanced analysis: A review," *IEEE Access*, vol. 8, pp. 224 020–224 032, 2020.

[7] L. Fan, C. Zhu, Z. Miao, and M. Hu, "Modal analysis of a DFIG-based wind farm interfaced with a series compensated network," *IEEE Transactions on Energy Conversion*, vol. 26, no. 4, pp. 1010–1020, 2011.

[8] A. Ostadi, A. Yazdani, and R. K. Varma, "Modeling and stability analysis of a DFIG-based wind-power generator interfaced with a series-compensated line," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1504–1514, 2009.

[9] J. Adams, V. A. Pappu, and A. Dixit, "ERCOT experience screening for sub-synchronous control interaction in the vicinity of series capacitor banks," in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–5.

[10] I. ABB, "ERCOT crez reactive power compensation study," *IEEE Transactions on Power Delivery*, pp. 1–62, 2010.

[11] H. Liu, X. Xie, C. Zhang, Y. Li, H. Liu, and Y. Hu, "Quantitative SSR analysis of series-compensated DFIG-based wind farms using aggregated RLC circuit model," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 474–483, 2017.

[12] A. Nourian and S. Madnick, "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 2–13, 2018.

[13] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[14] U. Karaagac, S. O. Faried, J. Mahseredjian, and A. Edris, "Coordinated control of wind energy conversion systems for mitigating subsynchronous interaction in DFIG-based wind farms," *IEEE Transactions on Smart Grid*, vol. 5, no. 5, pp. 2440–2449, 2014.

[15] M. Ghafouri, U. Karaagac, H. Karimi, S. Jensen, J. Mahseredjian, and S. O. Faried, "An LQR controller for damping of subsynchronous interaction in DFIG-based wind farms," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4934–4942, 2017.

[16] H. A. Mohammadpour and E. Santi, "Optimal adaptive sub-synchronous resonance damping controller for a series-compensated doubly-fed induction generator-based wind farm," *IET Renewable Power Generation*, vol. 9, no. 6, pp. 669–681, 2015.

[17] C. Zhu, L. Fan, and M. Hu, "Control and analysis of DFIG-based wind turbines in a series compensated network for SSR damping," in *IEEE PES General Meeting*, 2010, pp. 1–6.

[18] M. A. Chowdhury, M. A. Mahmud, W. Shen, and H. R. Pota, "Nonlinear controller design for series-compensated DFIG-based wind farms to mitigate subsynchronous control interaction," *IEEE Transactions on Energy Conversion*, vol. 32, no. 2, pp. 707–719, 2017.

[19] P. Huang, M. S. El Moursi, W. Xiao, and J. L. Kirtley, "Subsynchronous resonance mitigation for series-compensated DFIG-based wind farm by using two-degree-of-freedom control strategy," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1442–1454, 2015.

[20] M. Ghafouri, U. Karaagac, H. Karimi, and J. Mahseredjian, "Robust subsynchronous interaction damping controller for DFIG-based wind farms," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 6, pp. 1663–1674, 2019.

[21] A. E. Leon, S. Amodeo, and J. M. Mauricio, "Enhanced compensation filter to mitigate subsynchronous oscillations in series-compensated DFIG-based wind farms," *IEEE Transactions on Power Delivery*, pp. 1–1, 2021.

[22] P. Li, J. Wang, L. Xiong, S. Huang, M. Ma, and Z. Wang, "Energy-shaping controller for DFIG-based wind farm to mitigate subsynchronous control interaction," *IEEE Transactions on Power Systems*, pp. 1–1, 2020.

[23] G. Li, Y. Chen, A. Luo, and Y. Wang, "An inertia phase locked loop for suppressing sub-synchronous resonance of renewable energy generation system under weak grid," *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[24] J. Shair, X. Xie, Y. Li, and V. Terzija, "Hardware-in-the-loop and field validation of a rotor-side subsynchronous damping controller for a series compensated DFIG system," *IEEE Transactions on Power Delivery*, vol. 36, no. 2, pp. 698–709, 2021.

[25] X. Zhang, X. Xie, H. Liu, and Y. Li, "Robust subsynchronous damping control to stabilise ssr in series-compensated wind power systems," *IET Generation, Transmission & Distribution*, vol. 13, no. 3, pp. 337–344, 2018.

[26] X. Zhang, X. Xie, J. Shair, H. Liu, Y. Li, and Y. Li, "A grid-side subsynchronous damping controller to mitigate unstable SSCI and its hardware-in-the-loop tests," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 3, pp. 1548–1558, 2020.

[27] J. Shair, X. Xie, and G. Yan, "Mitigating subsynchronous control interaction in wind power systems: Existing techniques and open challenges," *Renewable and Sustainable Energy Reviews*, vol. 108, pp. 330–346, 2019.

[28] M. Ghafouri, U. Karaagac, J. Mahseredjian, and H. Karimi, "SSCI damping controller design for series-compensated DFIG-based wind parks considering implementation challenges," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2644–2653, 2019.

[29] X. Liu, L. Che, K. Gao, and Z. Li, "Power system intra-interval operational security under false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 4997–5008, 2020.

[30] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2343–2357, 2017.

[31] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Y. Dong, "Application of functional modelling for monitoring of WTG in a cyber-physical environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 1, pp. 79–87, 2019.

[32] M. A. Ahmed, A. M. Eltamaly, M. A. Alotaibi, A. I. Alolah, and Y. Kim, "Wireless network architecture for cyber physical wind energy system," *IEEE Access*, vol. 8, pp. 40 180–40 197, 2020.

[33] B. K. Singh, J. Coulter, M. A. G. Sayani, S. M. Sami, M. Khalid, and K. E. Tepe, "Survey on communication architectures for wind energy integration with the smart grid," *International Journal of Environmental Studies*, vol. 70, no. 5, pp. 765–776, 2013.

[34] F. R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication systems for grid integration of renewable energy resources," *IEEE Network*, vol. 25, no. 5, pp. 22–29, 2011.

[35] J. R. Kristoffersen and P. Christiansen, "Horns rev offshore windfarm: its main controller and remote control system," *Wind Engineering*, vol. 27, no. 5, pp. 351–359, 2003.

[36] C. Wang, C.-W. Ten, and Y. Hou, "Inference of compromised synchrophasor units within substation control networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5831–5842, 2017.

[37] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang, and M. Debbabi, "Modeling supply chain attacks in IEC 61850 substations," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–6.

[38] A. Elgargouri and M. Elmusrati, "Analysis of cyber-attacks on IEC 61850 networks," in *2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT)*. IEEE, 2017, pp. 1–4.

[39] Yong-Yan Cao, You-Xian Sun, and Wei-Jie Mao, "A new necessary and sufficient condition for static output feedback stabilizability and comments on stabilization via static output feedback," *IEEE Transactions on Automatic Control*, vol. 43, no. 8, pp. 1110–1111, 1998.

[40] G.-R. Duan and H.-H. Yu, *LMIs in control systems: analysis, design and applications*. CRC press, 2013.

[41] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, no. 2, pp. 229–252, 2008.

[42] H. Jafarnejadsani and J. Pieper, "Gain-scheduled ℓ_1-optimal control of variable-speed-variable-pitch wind turbines," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 1, pp. 372–379, 2015.

[43] L. Ruttledge and D. Flynn, "Emulated inertial response from wind turbines: Gain scheduling and resource coordination," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3747–3755, 2016.

[44] T. L. Van, T. H. Nguyen, and D. Lee, "Advanced pitch angle control based on fuzzy logic for variable-speed wind turbine systems," *IEEE Transactions on Energy Conversion*, vol. 30, no. 2, pp. 578–587, 2015.

[45] H. Wang, J. Yang, Z. Chen, W. Ge, Y. Li, Y. Ma, J. Dong, M. O. Okoye, and L. Yang, "Analysis and suppression for frequency oscillation in a wind-diesel system," *IEEE Access*, vol. 7, pp. 22 818–22 828, 2019.

[46] V. VanDoren, *Techniques for adaptive control*. Elsevier, 2002.

[47] D.-W. Gu, P. Petkov, and M. M. Konstantinov, *Robust control design with MATLAB®*. Springer Science & Business Media, 2005.

[48] J. Mahseredjian, S. Dennetière, L. Dubé, B. Khodabakhchian, and L. Gérin-Lajoie, "On a new approach for the simulation of transients in power systems," *Electric Power Systems Research*, vol. 77, no. 11, pp. 1514–1520, 2007.

[49] U. Karaagac, H. Saad, J. Peralta, and J. Mahseredjian, "Doubly-fed induction generator based wind park models in EMTP-RV," *Polytechnique Montréal Electrical Engineering Res. Rep.*, 2015.

[50] A. Haddadi, I. Kocar, T. Kauffmann, U. Karaagac, E. Farantatos, and J. Mahseredjian, "Field validation of generic wind park models using fault records," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 4, pp. 826–836, 2019.