Hybrid Fault-Tolerant and Attack-Resilient Cooperative Control in an Offshore Wind Farm

Saeedreza Jadidi, *Member, IEEE*, Hamed Badihi, *Senior Member, IEEE*, and Youmin Zhang*, *Fellow, IEEE*

***Abstract*—Modern wind farms promise increased capacity, sustainability, and efficiency through the integration of information technology with the existing wind energy technologies. However, this integration creates a new category of cyber-physical vulnerabilities stemming from physical faults and/or cyberattacks potentially leading to devastating physical impacts and catastrophic consequences. The large scale and high complexity of a wind farm, in addition to its growing connectivity, control functionality, and wind intermittency and variability make the task of cyber-physical protection particularly challenging. This paper introduces novel approaches for guaranteeing the safety, security, and reliability of a modern wind farm under simultaneous occurrence of faults and attacks using an advanced cyber-physical health monitoring scheme, defined as "intrusion detection and fault diagnosis system", as well as fault-tolerant/attack-resilient control strategies at different levels. The proposed fault-tolerant control strategy is based on adaptive model predictive control at turbine level, enhanced with a control reallocation mechanism at farm level. The attack-resilient control strategy is based on an automatic signal correction (ASC) technique that is applied at network operator level. The effectiveness of the suggested approaches is demonstrated using an offshore wind farm model under wind turbulences, measurement noises, and realistic physical fault and cyberattack scenarios.**

***Index Terms*—Attack-resilient control, control reallocation, cyberattack, fault diagnosis, fault-tolerant control, intrusion detection, model predictive control, wind turbines, wind farm.**

I. Introduction

Energy service providers worldwide are facing grand challenges in meeting the demand of our society in a sustainable and reliable way. Since the last century, the global energy demand has increased significantly, which is expected to continue. With the foreseeable impact of our energy consumption on climate change, it is our responsibility to utilize energy more efficiently with a minimal environmental footprint. This collective goal is driving the global transformation from conventional energy sources of fossil fuels toward renewable energy sources such as wind. Forecasts predict that the penetration of distributed renewable energy resources such as wind farms (WFs) into the existing power grids will increase considerably in the future, leading to a more decentralized electric power infrastructure with numerous cyber-physical assets. On the flip side, this will increase the complexity of the power grid, which will require novel approaches to guarantee *efficient*, *sustainable*, *reliable*, *safe*, and *secure* operation.

With the acceleration of modern WFs development as connected cyber-physical systems (CPSs), protecting these integrated systems against possible *physical faults* and *cyberattacks* becomes critically important. The increasing complexity of WFs' assets especially in offshore regions, harsh environmental loadings, and limited accessibility result in increasing rates of physical faults and failures that make cost-effective and sustainable wind power generation a challenging problem [1]. Also, as wind energy capacity grows in the global power landscape, WFs facilities are becoming more and more vulnerable and at risk due to malicious cyberattacks. For instance, those cyberattacks targeting communication links or cyberattacks related to critical mechanisms in monitoring and control systems [2]. To address the mentioned challenges, effective approaches for fault detection and diagnosis (FDD) and fault-tolerant control (FTC) as well as intrusion detection and diagnosis (IDD) and attack-resilient control (ARC) are necessary to improve the safety and security of WFs [3-7].

After reviewing technical literature and based on a recent comprehensive review papers in [5,6], it appears that most prior publications about health monitoring and fault accommodation in wind turbines (WTs) have investigated the applications of FDD and FTC at individual turbine level (not farm level). However, as will be discussed in this research study, it is easier to deal with some classes of faults (e.g., WT blade erosion and debris accumulation) at farm level. Table I lists the very few references in the technical literature which consider FDD and FTC at farm level. In addition, the design methodologies as well as main objectives of each reference are presented. In the case of power reduction due to blade erosion and debris accumulation, different FDD and FTC strategies based on multi-WT cooperative frameworks are discussed [8,9]. The proposed strategies in [8,9] can only handle mild-level power-loss faults (about 3 percent loss of power) in WTs. It is worth mentioning that these strategies can handle physical faults in WFs with any arbitrary layout without requiring additional information about wind speed or direction. To extend the proposed research works in [8,9] into higher-level power-loss faults (i.e., more that 3 percent), authors in [10] introduce a FTC strategy which is developed based on an integration between model reference

Manuscript received 26 May 2023; revised 10 October 2023; accepted 17 November 2023. Date of publication XX XXXX 20XX; date of current version XX XXXX 20XX. This work was supported by the Natural Sciences and Engineering Research Council of Canada through a Discovery Project Grant, a Seed Fund of Concordia University.

Youmin Zhang (*Corresponding author*) is a Professor at the Department of Mechanical, Industrial and Aerospace Engineering, Concordia University, Montreal, QC, H3G 1M8, Canada (e-mail: youmin.zhang@concordia.ca).

Saeedreza Jadidi is a Postdoctoral Researcher at the Department of Electrical and Computer Engineering, University of Saskatchewan, 57 Campus Drive, Saskatoon, SK, S7N 5A9, Canada (email: lqd573@usask.ca).

Hamed Badihi is an Assistant Professor in Dependable Systems at the Automation Technology and Mechanical Engineering Unit, Faculty of Engineering and Natural Sciences, Tampere University, Tampere, 33720, Finland (email: hamed.badihi@tuni.fi).

Table I Current Research on WFs FDD, FTC, IDD, and ARC

Design Methodologies	Targets and Objectives	References
Interval nonlinear parameter-varying parity equation	Fault diagnosis of a WF	[17]
Adaptive FTC based on barrier Lyapunov function	Active power control during "actuator fault" occurrence	[18]
Particle swarm optimization	Accommodation of "generator fault" effects at WF level	[19]
PI controller, and optimization using the SDR-CGHBO algorithm	FTC for Enhancing WF reliability and optimizing its performance	[20]
FTC based on fuzzy logic at WF level	Accommodation of "mild power loss faults" under "WTs blades erosions and debris accumulation on the blades"	[8,9]
FTC based on adaptive control method at WT level and control reallocation mechanism at WF level	Accommodation of "mild and severe power loss faults" under "erosion, debris accumulation on WT blades"	[10]
Multilayer FTC using a clustering approach	Accommodation of "mild and severe power loss faults" in large-scale WFs	[1]
Fuzzy dynamic modeling and fuzzy adaptive control	IDD and ARC against attacks on "grid frequency" and "WFNO command"	[7]
Bayesian attack graph models	Evaluation of "cyberattacks" on WF SCADA	[15]
Several preventative strategies such as physical security, network segmentation, and system hardening	Mitigation of "cyberattack" for WFs	[11]
Observer-based fuzzy control scheme, using looped-Lyapunov functional and linear matrix inequality (LMI)	ARC for a WF under "sub-synchronous interaction" and "cyberattacks (denial of service (DoS) and deception attacks)"	[21]
Model predictive controller (MPC) for voltage stability in WF	ARC to mitigate the effects of "cyberattacks" on "actuators" and "sensors"	[22]
Observer with adaptive resilient torque controller	ARC against "false data injection" on "rotor speed measurements"	[23]
Observer-based fuzzy control strategy	ARC for WFs against "deception" and "DoS cyberattacks"	[24]

Table II Attack Surface Components in WFs and Their Associated Vulnerabilities

Attack Surface Component	Theoretical / Practical Threat Scenarios	Use Cases
Communication Networks	Vulnerabilities in communication protocols and data encryption methods can lead to unauthorized access and data interception. Distributed Denial of Service (DDoS) attacks can disrupt communication links	Cyberattacks on communication links, Unauthorized access, Data interception, Data tampering, Eavesdropping, Denial of Service (DoS) attacks, Manipulation and spoofing control signals
Control Systems	Weaknesses in control system security can allow attackers to manipulate control commands and spoof signals	Unauthorized control, Data tampering, Data integrity attacks, Manipulation of control commands, Spoofing control signals, False sensor data
Data Transmission	Vulnerable data transmission can lead to data interception and tampering	Intercepting data transmissions, Data tampering
Physical Access Points	Insufficient physical security can result in unauthorized access and equipment tampering	Unauthorized access, Sabotage, Physical tampering, Theft of equipment
WT Systems	Weaknesses in WT systems can allow attackers to manipulate operations and sensor data	Manipulation of WT operations, Unauthorized control, Data tampering, Data integrity attacks, False sensor data
Supervisory Control and Data Acquisition (SCADA)	Vulnerabilities in SCADA systems can lead to unauthorized access and data manipulation	Cyberattacks on SCADA systems, Manipulation of SCADA data, Unauthorized access, Data tampering, Data integrity attacks

adaptive control and control reallocation mechanism (CRM). As a result, in comparison with the proposed strategies in [8,9], the more recent study in [10] can tackle both mild and severe levels of physical faults caused by various intensities of debris accumulation. However, the major challenge facing the proposed strategy in [10] is its effective implementation for large-scale WFs. In fact, when dealing with large WFs, the proposed method in [10] will be computationally expensive due to the high number of modules which are required during the calculations. To overcome this problem, a clustering technique for large WFs is presented in [1] which can facilitate computer programming and improve the effective implementation of the FDD and FTC.

Aside from FDD and FTC, the cybersecurity issues of WFs as well as investigating new technical solutions for these increasingly digitalized infrastructures have attracted more attention in recent years. Table II provides an overview of the attack surface components, their associated theoretical vulnerabilities, practical threat scenarios, and relevant use cases within the context of WF cybersecurity. Traditionally, the cybersecurity of WF's distributed components has been carried out using standard computer security procedures with network and host-based cyber defense (e.g., authentication, data encryption, and firewalls, among others). Yet, it is no secret that highly skilled cyberattacks are still able to bypass these common security procedures and disrupt safe and secure operation of WFs by manipulating control commands and/or monitoring data [2,11]. Indeed, smart cyberattacks in WF's facilities can target industrial control networks, like supervisory control and data acquisition (SCADA) system which is responsible for reliable connection of WTs to higher-level controller (i.e., WF network operator (WFNO)) [7,12,13]. The vulnerabilities of WF SCADA systems are recently studied in [12-15]. Despite the fact that the latest cybersecurity advancements help reduce the exposure of WFs to attacks, these strategies alone are not enough to fully guarantee the operation of WFs in an era of universal online threats. To address this challenging problem, continuous real-time IDD schemes and ARC strategies have been introduced recently to strengthen conventional defense technologies by detecting and diagnosing highly skilled cyberattacks (after their occurrence), and if possible, by responding to their malicious access using mitigation techniques [11,16,23,24]. A categorized list of references on WFs IDD and ARC with the design methodologies is also provided in Table I.

As already discussed, almost all prior research efforts on WFs health monitoring, fault-tolerant, and attack-resilient control only focus on either physical faults or cyberattacks, not cooperatively but independently. The main objective of this study is to address simultaneously both faults and attacks in WFs. The motivation for simultaneously addressing both physical faults and cyberattacks is rooted in several critical considerations. First and foremost, the contemporary threat landscape faced by modern WFs is evolving rapidly, driven by their increased reliance on digital control and communication

systems. This interconnectedness has rendered WFs susceptible to a wide array of risks, including physical faults and cyberattacks. An integrated approach is adopted to provide a holistic solution to ensure the secure and reliable operation of WFs. Furthermore, the decision to address these two types of threats together is driven by a fundamental observation: both physical faults and cyberattacks can lead to a common and detrimental consequence—power loss within a WF. Practical scenarios illustrate that physical faults, such as those affecting WTs, can reduce power generation, while cyberattacks have the capacity to manipulate control signals, resulting in similar power losses. This similarity in outcomes can make it challenging to distinguish between the two based solely on their effects. Therefore, by integrating fault tolerance and attack resilience strategies, the approach effectively manages and mitigates power losses, regardless of their source, thus ensuring the continued safety, security, and reliability of WF operations. Moreover, it is essential to underscore that physical faults and cyberattacks are not isolated issues but can frequently intersect. For example, a cyberattack on a WF's control system can trigger abnormal operations that mimic the effects of physical faults, such as power loss. Consequently, addressing both threats concurrently enables the development of a more robust and adaptive control system, capable of distinguishing genuine physical faults from cyberattack-induced anomalies. The proposed approach in this study seeks to fortify the resilience and adaptability of WF control systems by seamlessly integrating FDD with IDD mechanisms, culminating in the "intrusion detection and fault diagnosis (IDFD) system". This integration empowers WFs to respond effectively to a broad spectrum of anomalies, ensuring consistent and secure power generation. Finally, real-world scenarios often witness the simultaneous occurrence of faults and attacks or their close succession. By addressing both challenges holistically, the approach is well-suited to confront real-world scenarios where these threats may overlap, offering robust protection against a backdrop of evolving and multifaceted threats.

In summary, this study uses a cyberattack-complemented FDD, defined here as IDFD system integrated with FTC and ARC. In fact, it is possible to upgrade conventional FDD for defending against different types of attacks through appropriate modeling of physical consequences caused by successful and highly skilled attacks, which are usually stealthier and sometimes more catastrophic than physical faults. In more details, this novel strategy includes these major contributions:

1. *Comprehensive Approach to WF Anomalies*: WFs are dynamic and vulnerable systems that face a dual threat of physical faults and cyberattacks. Devising strategies to address these challenges simultaneously is a complex problem. This paper introduces a pioneering approach by integrating intrusion detection and fault diagnosis with cooperative control strategies. It aims at bridging the gap between addressing physical faults and cyber threats, acknowledging the real-world complexity faced by WF operators.
2. *Intrusion Detection and Fault Diagnosis*: This paper describes an IDFD system designed for real-time monitoring of a modern WF. The system aims to detect and identify both physical faults and cyberattacks on the WF. It uses novel algorithms and multiple estimators based on adaptive models and fuzzy logic to approximate the normal power values generated by WTs. This allows for a structured framework that focuses on specific physical faults (such as power loss) and cyberattacks (specifically targeting the WF's reference power command signal). The IDFD system functions independently and provides information for fault accommodation and attack mitigation strategies, as well as cyber-physical monitoring.
3. *Cooperative Fault-Tolerant and Attack-Resilient Strategies*: This paper also discusses the implementation of FTC and ARC strategies at different control levels in a WF. The purpose is to effectively handle physical faults in WTs and mitigate cyberattacks on the WFNO to ensure reliable integration with the external power grid. In the FTC design, an adaptive MPC (AMPC) is employed for each turbine, modifying the demanded active power signal received from the WF controller. Distributed AMPCs can handle mild-level power-loss faults at the WT level. To address severe-level power-loss fault scenarios, a novel CRM strategy is implemented at the farm-level control, specifically in the WF controller. Additionally, the ARC strategy utilizes real-time information from the IDFD system. This information is utilized to activate an automatic signal correction (ASC) for attack mitigation purposes.

To the best of the authors' knowledge, this research study is the first of its kind in the field of cyber-physical protection in WFs. It focuses on simultaneously detecting, isolating, and identifying physical faults and cyberattacks, while also proposing cooperative strategies for fault accommodation and attack mitigation. Notably, the "plug-and-play" capability of the proposed solutions makes them more appealing to the wind industry compared to other approaches that require a complete replacement of the control system from the beginning.

The paper's remaining sections are structured as follows: Section II provides a description of the WF benchmark model. Section III focuses on modeling physical faults, specifically power loss at the turbine level, and the cyberattack, specifically data integrity at the WFNO. Section IV presents a detailed structure of the FTC and ARC strategies, including their major components. Section V presents and discusses the simulation results, while the final conclusions are drawn in Section VI.

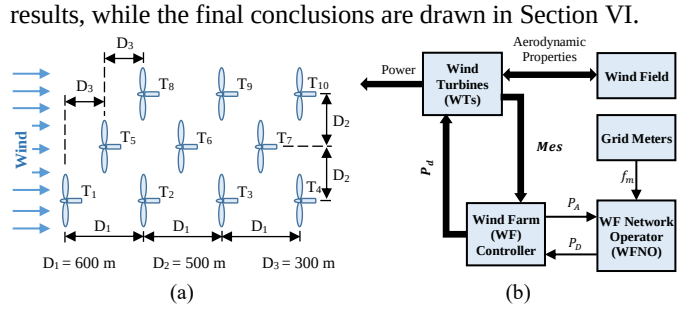

Fig. 1. WF benchmark: (a) considered layout, and (b) block diagram [10].

II. Wind Farm Benchmark

This paper uses a nonlinear simulation benchmark model developed by *SimWindFarm* toolbox, which is designed as part of the "Aeolus FP7 Project" [25]. In this research study, a modern WF is represented by Q that includes N WTs, mathematically: $Q = \{q_i | \, i \in \mathbb{N}, i \leq N\}$ and q_i is the ith WT in

WF Q (i.e., $\mathbb{N}$ is the set of natural numbers). The simulations are conducted in a WF with ten 5-MW offshore WTs with the layout and functional block diagram shown in Fig. 1. The benchmark comprises five major blocks as follows: network operator, WF controller, WTs, wind field, and grid meters.

Network Operator Block or simply WFNO can work in different modes in the benchmark (i.e., absolute active power control, frequency regulation, delta mode, power rate limiter, and balance control) to determine the WF total demanded power P_D from WF Q (i.e., $P_D = \sum_{i=1}^{N} P_{d,q_i}$, where P_{d,q_i} denotes the WT q_i demanded power) [25]. The WFNO in this paper works based on the frequency regulation mode, where a feedback signal from grid meters block (i.e., measured frequency f_m) is used to enable real-time active power control (APC). In this operational mode, the WF plays a role in grid frequency regulation by adjusting the generated power, either increasing or decreasing it as needed. As observed in Eqs. (1) and (2), the WFNO employs a dead-band proportional gain control which is a function of the frequency error f_e to compute P_D at time-step $(k+1)$. This control strategy regulates the frequency to any specified reference value f_r [9].

$$f_e(k) = f_m(k) - f_r \tag{1}$$

$$P_D(k+1) = \begin{cases} P_{min} & f_e(k) \geq c \\ \dfrac{P_{max}+P_{min}}{2} - \dfrac{(P_{max}-P_{min})(f_e(k)-d)}{2(c-d)} & d < f_e(k) < c \\ \dfrac{P_{max}+P_{min}}{2} & -d \leq f_e(k) \leq d \\ \dfrac{P_{max}+P_{min}}{2} - \dfrac{(P_{max}-P_{min})(f_e(k)+d)}{2(c-d)} & -c < f_e(k) < -d \\ P_{max} & f_e(k) \leq -c \end{cases} \tag{2}$$

The predetermined constants c and d in Eq. (2) respectively denote the control-band and the dead-band values where $c > d$. Also, P_{min} and P_{max} are defined as the *minimum* and *maximum* allowable limits for the WF total generated power, respectively.

WF Controller Block is in fact the interface between WFNO and WTs. It computes an estimation of WF total available power P_A and sends it to WFNO. However, the main duty of this controller is active power distribution in which P_D (which is received from WFNO) will be distributed among WTs according to the following equation:

$$P_{d,q_i}(k+1) = P_D(k+1)\frac{P_{a,q_i}(k)}{P_A(k)} \quad , \; q_i \in Q \tag{3}$$

where q_i denotes the ith WT in WF Q, and $P_{d,q_i}(k+1)$ denotes the demanded power from WT q_i in the farm for the next time-step. Moreover, $P_{a,q_i}(k)$ represents the estimated available power in WT q_i (i.e., $P_A = \sum_{i=1}^{N} P_{a,q_i}$) based on [25] as follows:

$$P_{a,q_i}(k) = \frac{\pi}{2}\rho R^2 \, V_{mes,q_i}^3(k) C_{P,max} \tag{4}$$

where ρ, R, $C_{P,max}$, and $V_{mes,q_j}(k)$ are air density, rotor radius, maximum power coefficient, and the measured nacelle wind speed of WT q_i in WF Q, respectively.

WTs Block simulates the real-life dynamics of N WTs in WF Q using the nonlinear dynamic models developed by the U.S. National Renewable Energy Laboratory (NREL) for an offshore 5-MW WT [26]. The primary components of the WT model include Aerodynamics, Drive Train, Tower, Generator, Pitch Actuator, and WT Controller blocks, all of which are thoroughly described in [25]. These models are driven by wind profiles from the wind field block and power set-points from the WF controller. Each WT produces various outputs used by the WF controller and provides the thrust coefficient C_T, which is utilized to calculate wake effects and wind profiles within the wind field block. In this benchmark, WTs generate active power outputs and measurement signals that are utilized by the WF controller. Each WT q_i, governed by the WT control system, acts upon P_{d,q_i} obtained from Eq. (3). The WT control system uses blade pitch angle and generator torque controllers to calculate reference signals for blade-pitch angle β_{r,q_i}, and generator torque τ_{r,q_i}, respectively.

Wind Field Block in the benchmark utilizes an advanced wind field model, which includes both ambient and wake models, to accurately simulate the complex aerodynamic interactions between WTs in the WF. In more detail, this block takes inputs such as wind speed, turbulence, and field dimensions, and it uses the Veers algorithm to create a wind field spectrum following IEC 61400-1 standards [27].

Grid Meters Block estimates the frequency of grid based on the WF's total generated power that is injected into the grid and the demanded power from electrical load at each time step.

III. Considered Physical Faults and Cyberattacks

Due to their significant impact and consequences, this paper specifically examines power loss faults in WTs caused by blade erosion or debris accumulation on the blades due to dirt, ice, etc. Additionally, this study addresses data-integrity cyberattacks on the WFNO, which can be triggered by the compromise of the control command signal P_D, as shown in Fig. 2.

A. Modeling of Power Loss Faults

A decrease in power generation within a WF can occur due to various malfunctions. However, the most common faults that affect the rotor aerodynamics and cause a reduction in the generated output power are erosion and debris accumulation on the blades due to dirt, ice, etc. Specifically, the wind exerts an aerodynamic torque τ_{aer,q_i} on the rotor of WT q_i, which is determined by Eq. (5). This equation takes into account the rotor angular speed ω_{rot,q_i}, wind speed V_{w,q_i}, and the swept area of the WT rotor A [28].

$$\tau_{aer,q_i}(t) = \frac{1}{2\omega_{rot,q_i}(t)}\rho \, A \, V_{w,q_i}^3(t) \, C_p(\beta_{q_i}(t), \lambda_{q_i}(t)) \tag{5}$$

In Eq. (5), power coefficient $C_p(\beta_{q_i}, \lambda_{q_i})$ is a three-dimensional nonlinear function of the tip-speed ratio λ_{q_i} and the blade pitch angle β_{q_i}. The operating condition of a variable-speed WT is determined by λ_{q_i} and β_{q_i}, with the ideal operation occurring at the peak of the C_p for maximum wind energy capture [29]. However, power loss faults such as erosion or debris accumulation on rotor blades can shift the WT's C_p surface downward. As a result, the new peak of shifted C_p surface not only has a lower magnitude, but also different coordinates, resulting in lower energy capture by WT.

In order to model the power loss faults that have been considered, the generated power from WT q_i, which is represented by P_{g,q_i}, can be expressed as follows:

$$P_{g,q_i}(t) = \eta_g \eta_m P_{aer,q_i}(t) \tag{6}$$

where η_g and η_m are the generator and transmission system efficiencies, respectively, and P_{aer,q_i} is the rotor aerodynamic power defined by [28] as:

$$P_{aer,q_i}(t) = \tau_{aer,q_i}(t)\ \omega_{rot,q_i}(t) \tag{7}$$

By substituting Eq. (7) into Eq. (6) and using Eq. (5):

$$P_{g,q_i}(t) = \frac{\eta_g \cdot \eta_m}{2} \rho\ A\ V_{w,q_i}^3(t)\ C_p(\beta_{q_i}(t), \lambda_{q_i}(t)) \tag{8}$$

The above equation shows a direct relationship between the generated power P_{g,q_i} and the power coefficient C_p, which can vary due to the effects of erosion or debris accumulation on blades, as explained earlier. Therefore, modeling the power loss faults can be accomplished by scaling the WT generated power.

B. *Modeling of Data-Integrity Cyberattacks*

Cyberattacks can be considered as fault-like events categorized as data-integrity cyberattacks. These attacks can have adverse impacts on a system, similar to physical faults, and necessitate measures to address them at the control-system level, such as through the use of ARC. However, cyberattacks often have stealthier consequences compared to common physical faults, posing challenges in their detection, identification, and mitigation. The stealth capability of cyberattacks enables attackers to cause significant damage, especially when they possess extensive knowledge about the targeted system. Therefore, it is crucial to effectively retrieve data to counteract the effects of data-integrity cyberattacks.

To simulate data-integrity cyberattacks, various attack templates can be used, such as "scaling", "ramp", "pulse", and "random" attacks. In the energy and power systems field, scaling and ramp attacks are more frequently observed, as they enable an intelligent attacker to quickly alter the system's frequency. The attacker's objective is often to decrease the grid frequency and activate under-frequency load shedding strategies [30,31]. This paper focuses specifically on the challenging ramp data-integrity cyberattacks, in Eq. (9). The true measured data $y(t)$ or control command data is gradually manipulated over the period T by adding a ramp function $(\gamma_r t)$ that changes over time. This results in the compromised data being represented as $y_{att}(t)$.

$$y_{att}(t) = \begin{cases} y(t) & t \notin T \\ y(t) + \gamma_r t & t \in T \end{cases}, \quad \gamma_r \in \mathbb{R} \tag{9}$$

As illustrated in Fig. 2, the target of the attack in this study is the WFNO, which is responsible for generating the reference command signal P_D that determines the entire WF's operation. The attacker can manipulate the value of attack parameter $\{\gamma_r\} \in \mathbb{R}$ to execute a stealthy and impactful attack without activating the traditional data-quality alarms in WFNO's control center. The attackers must consider the following criteria:

1. The value of P_D, which represents the total required power output from the WF, should stay within the allowed limits for both its magnitude and rate.
2. The frequency protection schemes should not be activated until the desired impact is fully achieved.

IV. Hybrid Cooperative FTC and ARC Design

The general framework of the IDFD system with integrated FTC/ARC strategies is shown in Fig. 3. In comparison to Fig. 1(b), the WF block diagram has been updated to include three additional blocks: the AMPC, IDFD, and ASC. Furthermore, the default WF controller has been enhanced to a fault-tolerant WF controller that uses the CRM. The combination of these blocks enables them to serve two primary objectives: firstly, to address the effects of power loss faults at both the WT and WF levels, with mild faults handled at the WT level and severe faults at the WF level. Secondly, they also help to mitigate the impact of data integrity attacks targeting the output of the WFNO. In the event of power loss faults, WTs with mild faults can still operate by adjusting the received signal P_{d,q_i} with AMPCs. However, severely faulty WTs require the reallocation of control signals P_{d,q_i}. The WF controller takes into account the available power from both healthy and mildly faulty WTs, generating additional power to compensate for those affected by severe power loss. As for data integrity cyberattacks, the IDFD provides information to the ASC unit, which then applies the appropriate signal correction to counteract the effects of the attack. The detailed structure of the blocks is illustrated in Fig. 4.

A. *Adaptive Model Predictive Controllers*

In the event of mild power loss faults, the AMPCs assume a pivotal role by passively accommodating these effects within the WTs. Notably, this is achieved without the requirement for explicit fault information. This proactive approach effectively eliminates the need for laborious and time-consuming fault detection and identification processes. Furthermore, it serves as a powerful means to mitigate potential uncertainties typically

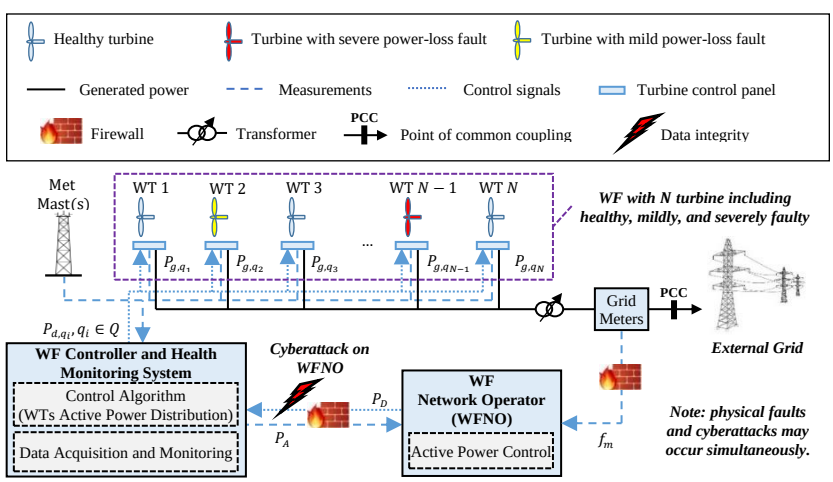

Fig. 2. WF schematic diagram under considered physical faults and cyberattacks (based on [7]).

associated with traditional FDD systems. In practice, mildly faulty WTs are generally capable of operating appropriately, although their reference powers may need to be adjusted or adapted based on the extent of power loss they are experiencing. The "AMPC controllers" block in Figures 3 and 4 includes N controllers, denoted as AMPC 1 to AMPC N, corresponding to the N WTs in WF Q. To explain further, if there is any reduction in the output power generated by WT q_i due to a fault, this will create noticeable errors between the WT's generated power P_{g,q_i} and the demanded power P_{d,q_i}, representing the reference signal from the WF controller. These errors serve as crucial inputs for the AMPCs, allowing them to adjust the demanded power reference vector $P_d = \{P_{d,q_i} | i \in \mathbb{N}, i \leq N\}$ computed by the WF controller. Importantly, the AMPCs do not interfere with the baseline controllers at either the WT level (i.e., blade pitch angle and generator torque controllers) or WF level (i.e., WF controller). Instead, they work in tandem with these controllers by modifying the input of demanded power in WTs based on the aforementioned errors. In other words, the AMPCs are adopted to adapt the reference demanded power vector (i.e., $\hat{P}_d$), which is then transmitted to the WTs and the IDFD system.

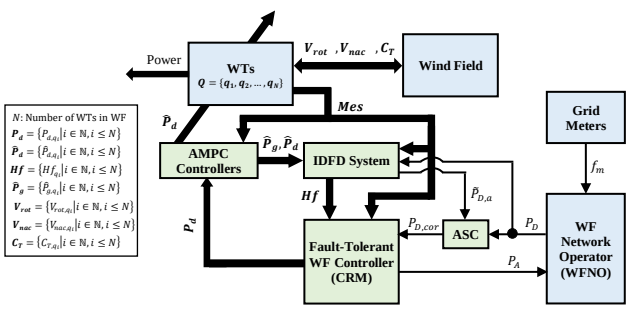

Fig. 3. Framework of the IDFD system with FTC/ARC integration.

In order to effectively handle uncertainties and nonlinearities in WFs, this paper proposes the adoption of AMPCs. The technique involves initially designing a linear MPC for the nominal operating condition. During operation, an AMPC approach is employed to continuously update the prediction model by utilizing a linear parameter varying (LPV) system at each control interval. To achieve this, an offline implementation of an LPV system, consisting of multiple linear plant models, accurately captures the local dynamics of the plant under a wide range of operating conditions. The designed AMPCs utilizes the LPV system to update only the parameters of the model, thereby addressing uncertainties and nonlinearities in WFs effectively.

The initial model is a sampled linear time-invariant (LTI) system that takes as inputs the manipulated variable (MV) signal $u_c(k) = \hat{P}_{d,q_i}$ and vector $u_v(k) = [\tau_{r,q_i}, \omega_{g,q_i}]^T$. Here, τ_{r,q_i} and ω_{g,q_i} (that appropriately represent the dynamic of WT) respectively are the generator reference torque and generator angular speed for WT q_i. The model used as the basis is described as follows:

$$\begin{cases} x_p(k+1) = A_p x_p(k) + B_{p,mv} u_c(k) + B_{p,v} u_v(k) \\ y_p(k) = C_p x_p(k) + D_{p,mv} u_c(k) + D_{p,v} u_v(k) \end{cases} \tag{10}$$

where A_p, $B_{p,mv}$, $B_{p,v}$, C_p, $D_{p,mv}$, and $D_{p,v}$ are state-space matrices. Additionally, $x_p(k)$ and $y_p(k)$ are the state vector and the output (i.e., the estimation of WT generated power), respectively. Using a system identification procedure in [32], the model in Eq. (10) is linearized as a third order system. The general model can be expressed in terms of deviation from the nominal operating condition as follows:

$$\begin{cases} x_p(k+1) = \bar{x}_p(k) + A(k)\left(x_p(k) - \bar{x}_p(k)\right) \\ \quad + B(k)\left(u_t(k) - \bar{u}_t(k)\right) + \Delta\bar{x}_p(k) \\ y_p(k) = \bar{y}_p(k) + C(k)\left(x_p(k) - \bar{x}_p(k)\right) \\ \quad + D(k)(u_t(k) - \bar{u}_t(k)) \end{cases} \tag{11}$$

Here, $u_t(k) = [u_c(k) \quad u_v(k)]^T$ is the combined input vector. The matrices $A(k)$, $B(k)$, $C(k)$, and $D(k)$, and the nominal conditions $\bar{x}_p(k)$, $\Delta\bar{x}_p(k)$, $\bar{u}_t(k)$, and $\bar{y}_p(k)$ are updated using the LPV system; and the output of prediction model (i.e., $y_p(k) = \hat{P}_{g,q_i}$) is sent to the IDFD to determine the health factor of each WT (i.e., Hf_{q_i} in Section IV.B).

Without loss of generality, the discrete affine form of the LPV system, whose dynamics vary as a function of scheduling parameter vector p, can be defined as follows [33]:

$$\begin{cases} x_p(t + \Delta T) = A(p)x_p(t) + B(p)u_t(t) \\ + \left(\bar{x}_p(p) + \Delta\bar{x}_p(p) - A(p)\bar{x}_p(p) - B(p)\bar{u}_t(p)\right) \\ y_p(t) = C(p)x_p(t) + D(p)u_t(t) \\ + \left(\bar{y}_p(p) - C(p)\bar{x}_p(p) - D(p)\bar{u}_t(p)\right) \end{cases} \tag{12}$$

where $A(p)$, $B(p)$, $C(p)$ and $D(p)$ are matrices parametrized by p, and ΔT is the sampling time. Also, $\bar{x}_p(p)$, $\Delta\bar{x}_p(p)$, $\bar{u}_t(p)$, and $\bar{y}_p(p)$ are the offset values at a given parameter p. These matrices and offset values are used to update the mentioned parameters in the general prediction model in Eq. (11). The model in Eq. (12) is represented as an interpolated array of linear state-space models. Several points in the scheduling space are chosen (here, for each $p = (\tau_{r,q_i}, \omega_{g,q_i})$ a range of values is selected), and for each point, a linear approximation of WT dynamics is obtained. More details about the linear interpolation technique are available in [33]. Additionally, since the true states of the plant model are not accessible to the AMPC, a linear time-varying Kalman filter (LTVKF) is implemented.

With the prediction model described in Eq. (11), the control action can be calculated by solving the quadratic programming (QP) problem shown below at each time step [34]:

$$\begin{aligned} J(Z_k) = \sum_{i=0}^{p-1} \Big(& \left(w_{i+1}^{y}\left[y_p(k+i+1|k) - r(k+i+1|k)\right]\right)^2 \\ & + \left(w_i^{u}\left[u_c(k+i|k) - u_{target}(k+i|k)\right]\right)^2 \\ & + \left(w_i^{\Delta u}\left[u_c(k+i|k) - u_c(k+i-1|k)\right]\right)^2 \Big) \\ & + \rho_\varepsilon \varepsilon_k^2 \end{aligned} \tag{13}$$

where k and p are the current time step and the prediction horizon, respectively. The AMPC constraints are bounded by:

$$\begin{aligned} y_{p,min}(i) - \varepsilon_k V_{min}^{y}(i) \leq y_p(k+i+1|k) \\ \leq y_{p,max}(i) - \varepsilon_k V_{max}^{y}(i) \end{aligned} \tag{14}$$

$$\begin{aligned} u_{c,min}(i) - \varepsilon_k V_{min}^{u}(i) \leq u_c(k+i|k) \\ \leq u_{c,max}(i) - \varepsilon_k V_{max}^{u}(i) \end{aligned} \tag{15}$$

$$\begin{aligned} \Delta u_{c,min}(i) - \varepsilon_k V_{min}^{\Delta u}(i) \leq \Delta u_c(k+i|k) \\ \leq \Delta u_{c,max}(i) - \varepsilon_k V_{max}^{\Delta u}(i) \end{aligned} \tag{16}$$

$$\Delta u_c(k+h|k) = 0 \tag{17}$$

$$\varepsilon_k \geq 0 \tag{18}$$

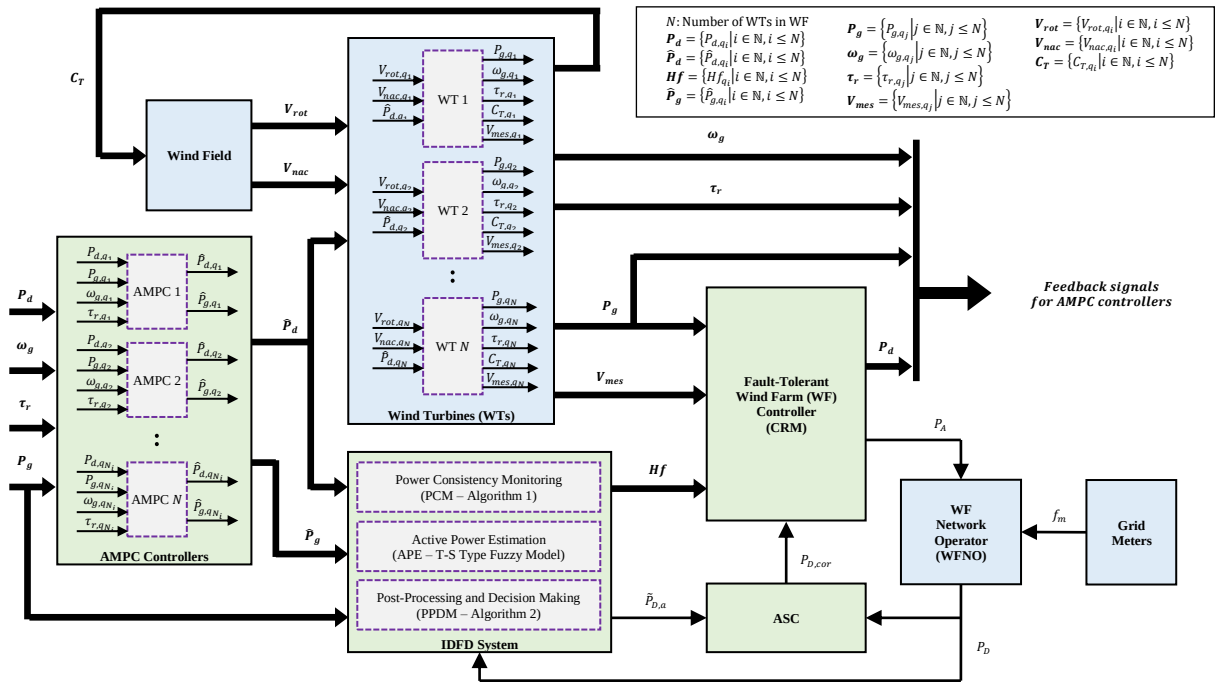

Fig. 4. The detailed structure of hybrid cooperative FTC and ARC strategies with integration into IDFD system.

Table III Parameters and Their Definitions

$y_p(k+i+1\|k)$	Output predicted value at $(i+1)$th prediction horizon step based on available information at time-step k (i.e., $y_p = \hat{P}_{g,q_i}$)
$r(k+i+1\|k)$	Reference value at $(i+1)$th step (i.e., $r = P_{d,q_j}$)
$u_{target}(k+i\|k)$	Target value for MV at the ith step
w_{i+1}^{y}	Tuning weight for output at the $(i+1)$th step
w_i^{u}	Tuning weight for MV at ith step
$w_i^{\Delta u}$	Tuning weight for MV movement at ith step
ε_k	Slack variable for implementing soft constraints
ρ_ε	Constraint violation penalty weight
$\{y_{p,min}(i), y_{p,max}(i)\}$	Lower and the upper bounds for output at ith step
$\{u_{c,min}(i), u_{c,max}(i)\}$	Lower and the upper bounds for MV at ith step
$\{\Delta u_{c,min}(i), \Delta u_{c,max}(i)\}$	Lower and the upper bounds for MV movement at ith step
$V_{min}^{y}, V_{max}^{y}, V_{min}^{u}, V_{max}^{u}, V_{min}^{\Delta u}, V_{max}^{\Delta u}$	Non-negative elements that are identical to the weights in cost function but for constraint softening

with respect to $i = 0, \dots, p-1$, $h = m, \dots, p$, the sequence of $\{\Delta u_c(k|k), \dots, \Delta u_c(k-1+m|k)\}$, and ε_k. It should be noted that m is the control horizon. The QP decision is:

$$Z_k^T = [\Delta u_c(k|k)^T \quad \Delta u_c(k+1|k)^T \quad \dots \quad \Delta u_c(k+m-1|k)^T \quad \varepsilon_k] \quad (19)$$

Finally, the AMPC sets $u_c(k) = u_c(k-1) + \Delta u_c{}^*(k|k)$ in which $\Delta u_c{}^*(k|k)$ represents the first element of the sequence. The QP is solved using the method presented in [35]. Other parameters used in Eqs. (13)-(19) are defined in Table III.

B. IDFD System Design

Fig. 5 depicts the parallel units of the IDFD system: power consistency monitoring (PCM), active power estimation (APE), and post-processing and decision-making (PPDM).

PCM Unit: The PCM unit proposed in Algorithm 1 utilizes predictive models in AMPCs to monitor the real-time consistency of power generated by WTs. In more details, it addresses the physical faults by continuously monitoring the consistency of power production across all WTs. This enables the detection and identification of any inconsistencies in output powers, providing reliable information on faults.

A highly effective approach for monitoring power consistency within a WF is to perform real-time monitoring of power output from each individual WT and from all other WTs in the farm. In Algorithm 1, Line 1 designates two arbitrary turbines within the farm as q_i and q_j, and this algorithm is applied to all q_i and $q_j$within the WF. To accurately monitor power consistency between any two WTs q_i and q_j within WF Q, it is essential to consider not only their generated powers P_{g,q_i} and P_{g,q_j}, but also their power reference signals $\hat{P}_{d,q_i}$ and $\hat{P}_{d,q_j}$ [8]. In Algorithm 1, the generated powers from WTs q_i and q_j are considered consistent when the values of $P_{g_{i,j}}$ and $\hat{P}_{g_{i,j}}$ are approximately equal (or when the residual r in Line 1.4 is almost zero). However, achieving perfect equality between these values is not always possible in practice due to measurement noises and possible uncertainties. To address this issue, a procedure for the inconsistency signature (Lines 1.8-1.10) has been developed based on [1,8]. This procedure enables the calculation of an absolute inconsistency value $I_{i,j}$ between the two WTs. Finally, Algorithm 1 produces two outputs, $ID_{i,j}$ and $IM_{i,j}$, which respectively indicate the occurrence and magnitude of any inconsistencies in the powers between WTs q_i and q_j. When power output is inconsistent between these WTs, the $ID_{i,j}$ and $IM_{i,j}$ signals provide information on the faulty WT as well as the estimated absolute value of power-loss, $|\overline{\Delta P}_{i,j}|$ (as shown in Lines 1.11-1.15).

APE Unit: The APE unit employs Takagi-Sugeno (T-S) type dynamic fuzzy modeling technique, which is a widely used data-driven fuzzy modeling and identification approach [36]. Using

this method, the APE unit creates a model-based estimator that generates nominal estimates of the WF's totally generated power $\hat{P}_G$. The estimator, in Fig. 5, uses carefully selected inputs (i.e., P_D and $\hat{P}_G$) to represent the WF's operating conditions.

Algorithm 1 Power Consistency Monitoring (PCM)

Inputs: $\{\boldsymbol{\hat{P}_{g,q_i}(k)}, \boldsymbol{P_{g,q_i}(k)}, \boldsymbol{\hat{P}_{d,q_i}(k)} \mid \boldsymbol{i} \in \mathbb{N}, \boldsymbol{i} \leq \boldsymbol{N}\}$

$\mathbb{N}$: natural numbers set.

$\boldsymbol{N}$: number of WTs in a WF.

$\boldsymbol{k}$: time-step.

$\boldsymbol{\hat{P}_{g,q_i}(k)}$: AMPC $\boldsymbol{i}$ predictive model output.

$\boldsymbol{P_{g,q_i}(k)}$: generated power of WT $\boldsymbol{q_i}$.

$\boldsymbol{\hat{P}_{d,q_i}(k)}$: manipulated variable (MV) from AMPC $\boldsymbol{i}$.

Outputs: $\{\boldsymbol{ID_{i,j}(k)}, \boldsymbol{IM_{i,j}(k)} \mid \boldsymbol{i,j} \in \mathbb{N}, \boldsymbol{i} < \boldsymbol{N}, \boldsymbol{i} < \boldsymbol{j} \leq \boldsymbol{N}\}$

$\boldsymbol{ID_{i,j}(k)}$: inconsistency detection signal shows the "occurrence" of any inconsistency between the generated powers by WT $\boldsymbol{q_i}$ and $\boldsymbol{q_j}$.

$\boldsymbol{IM_{i,j}(k)}$: inconsistency magnitude signal shows the "value" of any inconsistency between the generated powers by WT $\boldsymbol{q_i}$ and $\boldsymbol{q_j}$.

Constants and Variables:

$\{\boldsymbol{I_{i,j}(k)}, \boldsymbol{r(k)}, \boldsymbol{T_r}, \boldsymbol{T_1(k)}, \boldsymbol{T_2(k)}, \boldsymbol{\overline{\Delta P}_{i,j}(k)}, \boldsymbol{N_w}\}$

$\boldsymbol{I_{i,j}(k)} \in \{\boldsymbol{0}, \boldsymbol{1}\}$: absolute inconsistency signal in which 0 means consistent and 1 inconsistent.

$\boldsymbol{r(k)}$: residual used during procedure.

$\boldsymbol{T_r}$: constant threshold for checking the residual.

$\boldsymbol{T_1(k)}$: and $\boldsymbol{T_2(k)}$ two variables used during the calculations.

$\boldsymbol{\overline{\Delta P}_{i,j}(k)}$: running mean of $\boldsymbol{\Delta P_{i,j}(k)}$.

$\boldsymbol{N_w}$: length of the sliding window.

1. **for** each $\{\boldsymbol{q_i}, \boldsymbol{q_j} \mid \boldsymbol{i,j} \in \mathbb{N}, \boldsymbol{i} < \boldsymbol{N}, \boldsymbol{i} < \boldsymbol{j} \leq \boldsymbol{N}\}$ **do**
   calculate the predicted, demanded, and generated power differences:
   1.1. $\boldsymbol{\hat{P}_{g_{i,j}}(k)} = \boldsymbol{\hat{P}_{g,q_i}(k)} - \boldsymbol{\hat{P}_{g,q_j}(k)}$
   1.2. $\boldsymbol{\hat{P}_{d_{i,j}}(k)} = \boldsymbol{\hat{P}_{d,q_i}(k)} - \boldsymbol{\hat{P}_{d,q_j}(k)}$
   1.3. $\boldsymbol{P_{g_{i,j}}(k)} = \boldsymbol{P_{g,q_i}(k)} - \boldsymbol{P_{g,q_j}(k)}$
   compute the residual:
   1.4. $\boldsymbol{r(k)} = \boldsymbol{P_{g_{i,j}}(k)} - \boldsymbol{\hat{P}_{g_{i,j}}(k)}$
   calculate the power difference between $\boldsymbol{P_{g_{i,j}}(k)}$ and $\boldsymbol{\hat{P}_{d_{i,j}}(k)}$:
   1.5. $\boldsymbol{\Delta P_{i,j}(k)} = \boldsymbol{P_{g_{i,j}}(k)} - \boldsymbol{\hat{P}_{d_{i,j}}(k)}$
   calculate the running mean of the power difference:
   1.6. $\boldsymbol{\overline{\Delta P}_{i,j}(k)} = \frac{\boldsymbol{1}}{\boldsymbol{N_w}} \sum_{\boldsymbol{l=k-N_w+1}}^{\boldsymbol{k}} \boldsymbol{\Delta P_{i,j}(l)}$
   >> Inconsistency Signature Post-Processing <<
   1.7. **if** $|\boldsymbol{r(k)}| < \boldsymbol{T_r}$ **then**
      1.7.1. $\boldsymbol{I_{i,j}(k)} = \boldsymbol{T_1(k)} = \boldsymbol{T_2(k)} = \boldsymbol{0}$
      1.7.2. **if** $\boldsymbol{I_{i,j}(k-1)} \neq \boldsymbol{0}$ and $\boldsymbol{T_2(k-1)} < \boldsymbol{T_{out}}$ **then**
      1.7.3. $\boldsymbol{I_{i,j}(k)} = \boldsymbol{1}$
      1.7.4. $\boldsymbol{T_1(k)} = \boldsymbol{T_1(k-1)}, \boldsymbol{T_2(k)} = \boldsymbol{T_2(k-1)} + \boldsymbol{1}$
      1.7.5. end if
   1.8. **else**
      1.8.1. $\boldsymbol{I_{i,j}(k)} = \boldsymbol{1}, \boldsymbol{T_1(k)} = \boldsymbol{T_1(k-1)}, \boldsymbol{T_2(k)} = \boldsymbol{0}$
      1.8.2. **if** $\boldsymbol{I_{i,j}(k-1)} = \boldsymbol{0}$ and $\boldsymbol{T_2(k-1)} < \boldsymbol{T_{in}}$ **then**
      1.8.3. $\boldsymbol{I_{i,j}(k)} = \boldsymbol{0}$
      1.8.4. $\boldsymbol{T_1(k)} = \boldsymbol{T_1(k-1)} + \boldsymbol{1}, \boldsymbol{T_2(k)} = \boldsymbol{0}$
      1.8.5. end if
   1.9. end if
   >> Inconsistency Analysis and Isolation Procedure <<
   1.10. **if** $\boldsymbol{I_{i,j}(k)} = \boldsymbol{1}$ and $\boldsymbol{\overline{\Delta P}_{i,j}(k)} > \boldsymbol{0}$ **then**
      1.10.1. $\boldsymbol{ID_{i,j}(k)} = \boldsymbol{j}, \ \boldsymbol{IM_{i,j}(k)} = |\boldsymbol{\overline{\Delta P}_{i,j}(k)}|$
   1.11. **else if** $\boldsymbol{I_{i,j}(k)} = \boldsymbol{1}$ and $\boldsymbol{\overline{\Delta P}_{i,j}(k)} < \boldsymbol{0}$ **then**
      1.11.1. $\boldsymbol{ID_{i,j}(k)} = \boldsymbol{i}, \ \boldsymbol{IM_{i,j}(k)} = |\boldsymbol{\overline{\Delta P}_{i,j}(k)}|$
   1.12. **else**
      1.12.1. $\boldsymbol{ID_{i,j}(k)} = \boldsymbol{0}, \ \boldsymbol{IM_{i,j}(k)} = \boldsymbol{0}$
   1.13. end if
2. end for
3. **return** $\{\boldsymbol{ID_{i,j}(k)}, \boldsymbol{IM_{i,j}(k)} \mid \boldsymbol{i,j} \in \mathbb{N}, \boldsymbol{i} < \boldsymbol{N}, \boldsymbol{i} < \boldsymbol{j} \leq \boldsymbol{N}\}$

A nonlinear system with multiple inputs and a single output, represented by $u \in U \subset \mathbb{R}^m$ for m inputs and $y \in Y \subset \mathbb{R}$ for

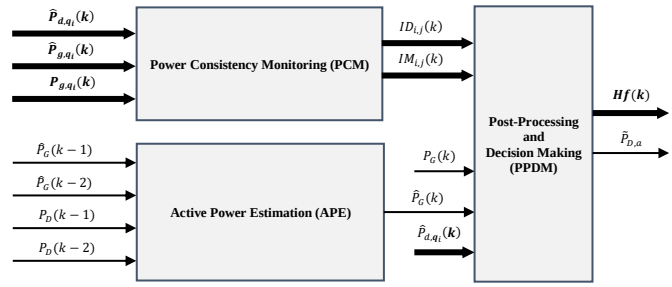

Fig. 5. Intrusion detection and fault diagnosis (IDFD) system.

one output, can be mathematically described as a multi-input single-output (MISO) system, expressed by:

$$y(k+1) = F\big(\phi(k)\big) + \varepsilon \tag{20}$$

$$\phi(k) = \big[y(k), \dots, y(k-n_y+1), u_i(k), \dots, u_i(k-n_{u,i}+1)\big] \quad i = 1, 2, 3, \dots, m \tag{21}$$

where F is a function that is used for approximation, while ε represents the modeling error. Additionally, the integers $n_{u,i}$ and n_y are related to the order of the system. F can be obtained as:

$Rule_{j\text{th}}(j = 1, 2, 3, \dots, M)$:

$$\begin{gathered} \boldsymbol{If}\ y(k)\ is\ \mathcal{A}_{j,1}\ \boldsymbol{and} \dots y(k-n_y+1)\ is\ \mathcal{A}_{j,n_y}\ \boldsymbol{and} \\ u_1(k)\ is\ \mathcal{B}_{j,1,1}\ \boldsymbol{and} \dots u_1(k-n_{u,1}+1)\ is\ \mathcal{B}_{j,1,n_{u,1}}\ \boldsymbol{and} \dots \\ u_m(k) is\ \mathcal{B}_{j,m,1}\ \boldsymbol{and} \dots u_m(k-n_{u,m}+1)\ is\ \mathcal{B}_{j,m,n_{u,m}}\ \boldsymbol{then} \\ \hat{y}_j(k+1) = \sum_{l=1}^{n_y} a_{j,l}\, y(k-l+1) \\ + \sum_{i=1}^{m} \sum_{l=1}^{n_{u,i}} b_{j,i,l}\, u_i(k-l+1) + c_j \end{gathered} \tag{22}$$

The antecedent membership functions are denoted by $\mathcal{A}$ and $\mathcal{B}$, while the rule consequent part is represented by $\hat{y}_j$, which is a linear function of parameters a, b, and c. The rule contributions (i.e., $\hat{y}_j$ with $j = 1,2, \dots, M$) are combined using a weighted average in Eq. (23) to calculate the aggregated output of the model. Here, μ_j represents the membership function that indicates the degree to which the jth rule is satisfied.

$$\hat{y}(k+1) = \frac{\sum_{j=1}^{M} \mu_j(\boldsymbol{\phi}(k)) \hat{y}_j(k+1)}{\sum_{j=1}^{M} \mu_j(\boldsymbol{\phi}(k))} \tag{23}$$

PPDM Unit: The first part of the PPDM unit described in Algorithm 2 is responsible for determining the health status of each WT, based on the relevant signals $ID_{i,j}$. The decision is made by a simple logic, where if at least one of the signals detects a WT (i.e., q_i or q_j based on the value of $ID_{i,j}$) as faulty, then that WT is considered faulty, and its power-loss (i.e., $\hat{\mathcal{P}}_{q_i}$ or $\hat{\mathcal{P}}_{q_j}$) is estimated as the maximum power-loss using relevant $IM_{i,j}$. As per the given information, the decision-making logic used by Algorithm 2 is based on three rules: $Rule$ 1 for WT q_1 (Lines 2-3), $Rule\ Z$ for any WT q_Z with ($Z \in \mathbb{N}$ and $1 < Z < N$) (Lines 4-5), and $Rule\ N$ for WT q_N (Lines 6-7). After applying the rules, the health factor Hf_{q_i} for each WT is calculated using the equation in Line 8.1. In the second part of Algorithm 2, the residual signal r_D is computed in Line 11, and a threshold test technique (described in Lines 12-19) is used to determine the value of $\tilde{P}_{D,a}$, that is employed by the ASC.

C. Fault-Tolerant WF Controller

The fault-tolerant WF controller outlined in Algorithm 3 dynamically adjusts its configuration based on the health factor

Hf_{q_i} of each WT. While the AMPCs at the WT level efficiently handle mild faults, severe faults in any WT result in a proportional decrease in the health factor. This decline in health factor acts as a trigger for the WF controller to initiate a reallocation of control signals P_{d,q_i}. Consequently, healthier WTs within the farm, equipped with unused power, increase their energy production to compensate for the severely faulty WTs. It is noteworthy that prior CRM strategies, as demonstrated in earlier works (e.g., [1] and [10]), employed binary health factors (i.e., $Hf_{q_i}(k) = \{0,1\}$) for switching between normal and reallocation modes. However, to eliminate issues associated with abrupt switching, Algorithm 3 adopts a continuous health factor approach (i.e., $Hf_{q_i}(k) \in [0,1]$), as generated by Algorithm 2 in Line 7.1. This ensures a smoother transition between control modes while optimizing WF performance.

Algorithm 2 Post-Processing and Decision Making (PPDM)

Inputs: $\{\{ID_{i,j}(k), IM_{i,j}(k) |\ i,j \in \mathbb{N}, i < N, i < j \le N\}, \widehat{P}_G(k), P_G(k), \widehat{P}_{d,q_i}(k-1)\}$
$ID_{i,j}(k)$: inconsistency detection from PCM unit.
$IM_{i,j}(k)$: inconsistency magnitude from PCM unit.
$\widehat{P}_G(k)$: generated power estimation from APE unit.
$P_G(k)$: actual WF total generated power.
$\widehat{P}_{d,q_i}(k-1)$: AMPC i manipulated variable (MV) at time-step $k-1$.

Outputs: $\{\{Hf_{q_i}(k) |\ q_i \in Q\}, \widetilde{P}_{D,a}(k)\}$
$Hf_{q_i}(k) \in [0,1]$: health factor of WT q_i that will be used by WF controller for reallocation (i.e., CRM).
$\widetilde{P}_{D,a}(k)$: malicious (cyberattack) data estimates of $P_D(k)$ that will be used by ASC unit.

Constants and Variables: $\{\widehat{\mathcal{P}}_{q_i}(k), Q_f, r_D(k), T_D, C_n\}$
$\widehat{\mathcal{P}}_{q_i}(k)$: power loss in WT q_i.
Q_f: set of faulty WTs in a WF.
$r_D(k)$: residual used during the calculations.
T_D: user-defined thresholds for r_D.
C_n: counter with zero initial value.

>> Physical Faults Detection and Identification Procedure <<

1. **if** $(ID_{1,2} = 1)$ ***or*** $(ID_{1,3} = 1)$ ***or*** ... ***or*** $(ID_{1,N} = 1)$ **then**
   1.1. $q_1 \in Q_f$
   1.2. $\widehat{\mathcal{P}}_{q_1}(k) = max\{IM_{1,2}, IM_{1,3}, IM_{1,4}, \dots, IM_{1,N}\}$
2. end if
3. **for** each $\{q_z \in Q |\ z \in \mathbb{N}, 1 < z < N\}$ **do**
   3.1. **if** $(ID_{1,z} = z)$ ***or*** ... ***or*** $(ID_{z-1,z} = z)$ ***or*** $(ID_{z,z+1} = z)$ ***or*** ... ***or*** $(ID_{z,N} = z)$ **then**
      3.1.1. $q_z \in Q_f$
      3.1.2. $\widehat{\mathcal{P}}_{q_z}(k) = max\{IM_{1,z}, \dots, IM_{z-1,z}, IM_{z,z+1}, \dots, IM_{z,N}\}$
   3.2. end if
4. end for
5. **if** $(ID_{1,N} = N)$ ***or*** ... ***or*** $(ID_{N-2,N} = N)$ ***or*** $(ID_{N-1,N} = N)$ **then**
   5.1. $q_N \in Q_f$
   5.2. $\widehat{\mathcal{P}}_{q_N}(k) = max\{IM_{1,N}, \dots, IM_{N-2,N}, IM_{N-1,N}\}$
6. end if
   calculate the health factor:
7. **for** each $q_i \in Q$ **do**
   7.1. $Hf_{q_i}(k) = \frac{\widehat{\mathcal{P}}_{q_i}(k)}{\widehat{P}_{d,q_i}(k-1)}$
8. end for
   compute the residual:
9. $r_D(k) = P_G(k) + \sum_{i=1}^{N} \widehat{\mathcal{P}}_{q_i}(k) - \widehat{P}_G(k)$

>> Cyberattack Detection and Identification Procedure <<

10. **if** $r_D(k) \le T_D$ **then**
    10.1. "No Cyberattack is Detected" and $\widetilde{P}_{D,a}(k) = 0$
11. **else "**store $r_D(k)$ for the next 3 time-steps"
12. end if
13. **for** each $j \in \mathbb{N}, j \le 4$ **do**
    13.1. **if** $r_D(k+j-1) > T_D$ **then** $C_n = C_n + 1$
    13.2. end if
14. end for
15. **if** $C_n = 4$ **then**
    15.1. "Cyberattack is Detected" and $\widetilde{P}_{D,a}(k) = r_D(k)$
16. **else**
    16.1. "No Cyberattack is Detected" and $\widetilde{P}_{D,a}(k) = 0$
17. end if
18. **return** $\{\{Hf_{q_i}(k) |\ q_i \in Q\}, \widetilde{P}_{D,a}(k)\}$

Algorithm 3 Control Reallocation Mechanism (CRM)

Inputs: $\{P_D(k), P_{g,q_i}(k), V_{mes,q_i}(k), Hf_{q_i}(k) |\ i \in \mathbb{N}, i \le N\}$
$P_D(k)$: WF total demanded power.
$P_{g,q_i}(k)$: generated power of WT q_i.
$V_{mes,q_i}(k)$: measured nacelle wind speed of WT q_i.
$Hf_{q_i}(k) \in [0,1]$: health factor for WT q_i from IDFD system.

Outputs: $\{\{P_{d,q_i}(k+1) |\ q_i \in Q\}, P_A(k)\}$
$Q = \{q_i |\ i \in \mathbb{N}, i \le N\}$: set of WTs in a WF.
$P_{d,q_i}(k+1)$: demanded power from WT q_i for the next time-step.
$P_A(k)$: WF total available power that will be send to WFNO.

Constants and Variables:
$\{P_{rated,q_i}, \rho, R, C_{Pmax}, P_{d,q_i}(k), P_{a,q_i}(k), P_{m,q_i}(k), P_{u,q_i}(k), P_M(k), P_U(k)\}$
P_{rated,q_i}: rated power of WT q_i.
ρ: air density.
R: rotor radius.
C_{Pmax}: maximum power coefficient.
$P_{d,q_i}(k)$: demanded power for WT q_i.
$P_{a,q_i}(k)$: available power of WT q_i.
$P_{m,q_i}(k)$: missed power of WT q_i.
$P_{u,q_i}(k)$: unused power of WT q_i.
$P_M(k)$: WF total missed power.
$P_U(k)$: WF total unused available power.

1. **for** each $q_i \in Q$ **do**
   calculate the available, missed, and unused power of each WT:
   1.1. $P_{a,q_i}(k) = min\left\{P_{rated,q_i}, \frac{\pi}{2}\rho R^2 V_{mes,q_i}(k)^3 C_{Pmax}\right\}$
   1.2. $P_{m,q_i}(k) = P_{d,q_i}(k) - P_{g,q_i}(k)$
   1.3. $P_{u,q_i}(k) = P_{a,q_i}(k) - P_{g,q_i}(k)$
2. end for
   calculate the total available, missed, and unused power in WF:
3. $P_A(k) = \sum_{i=1}^{N} P_{a,q_i}(k)$
4. $P_M(k) = \sum_{i=1}^{N} P_{m,q_i}(k)$
5. $P_U(k) = \sum_{i=1}^{N} P_{u,q_i}(k)$

>> Control Reallocation Procedure <<

6. **for** each $q_i \in Q$ **do**
   6.1. $P_{d,q_i}(k+1) = \left(P_D(k)\frac{P_{a,q_i}(k)}{P_A(k)} + P_M(k)\frac{P_{u,q_i}(k)}{P_U(k)}\right).Hf_{q_i}(k)$
7. end for
8. **return** $P_A(k)$ **and** $\{P_{d,q_i}(k+1) |\ q_i \in Q\}$

D. ASC Strategy for Attack Mitigation

The ARC unit receives data regarding potential cyberattacks from the IDFD system and executes signal correction procedures utilizing the data provided by $\widetilde{P}_{D,a}$ (as generated by Algorithm 2). The ARC assesses the necessity of signal correction by examining the sign of the malicious data estimated by the IDFD and subsequently applies either signal addition or subtraction as required. In fact, the corrected demanded power signal $P_{D,cor}$ is determined as follows:

$$P_{D,cor}(k) = P_D(k) + \widetilde{P}_{D,a} \tag{24}$$

This approach has a key advantage: it preserves the original settings of the baseline controllers. It means the control system stays secure, making changes only when absolutely necessary. As a result, the WFNO corrects its output only when it is

Table IV Controllers Structure and Deployment Overview

AMPCs	Design a linear MPC model for nominal operating conditions. During operation, employ an AMPC approach to update the model. Utilize an LPV for continuous model updates at each time step. Implement an offline LPV system with multiple linear plant models capturing local dynamics under various operating conditions. AMPCs use the LPV to dynamically update model parameters. Effective handling of uncertainties and nonlinearities in WF. Continuous estimation of generated power for each WT. Transmit power estimates to the IDFD system for determining the health factor of each WT.
CRM	AMPCs at the WT level handle mild faults, but severe faults trigger reallocation of control signals. Healthier WTs produce more power to compensate for severely faulty WTs. Uses continuous health factors, avoiding switching problems. Calculate available, missed, and unused power for WTs and WF. Update demanded power vector based on powers and health factors.
ASC	Receives information about cyberattacks from the IDFD system. Utilizes malicious data estimates for signal correction. Determines the necessity of signal correction based on the sign of malicious data estimated by the IDFD. Applies addition or subtraction of signals as required.

crucial, ensuring the WF remains stable and secure. Table IV provides a comprehensive overview of the control structure and deployment process for AMPCs, CRM, and ASC.

V. Simulation Results

To evaluate the effectiveness of the proposed fault-tolerant/ attack-resilient solutions, three scenarios have been conducted. Each scenario was simulated for 1,000 seconds under realistic wind conditions (mean wind speed of 15 m/s) using the WF benchmark described in Section II. It is worth noting that the selection of fault and attack parameters was a deliberate process aimed at creating realistic scenarios. Fault parameters were chosen based on their nature, while attack parameters were intentionally designed to challenge the detection capabilities of IDFD system due to the stealthiness and subtlety often associated with cyberattacks. This approach allowed the adaptability and effectiveness of the cooperative controllers and IDFD system to be evaluated under varying threat conditions, with a focus on highlighting the distinctions between faults and cyberattacks in WFs. Also, the timelines for faulty WTs and cyberattack in the considered scenarios are as follows:

Mild Power Loss ($\leq 10\%$) (Scenarios 1, 2, and 3)

T_2 during [800,1000] s	T_3 during [450,1000] s
T_4 during [125,300] s	T_7 during [350,1000] s
T_8 during [100,1000] s	T_{10} during [700,1000] s

Severe Power Loss ($> 10\%$) (Scenarios 2 and 3)	**Data Integrity Cyberattack (Scenario 3)**
T_1 during [200,1000] s	P_D during [350,1000] s

A. Scenario 1: Physical Faults (Only Mild Power Loss)

In the first scenario, where mild power loss faults occur in the mentioned WTs, the AMPCs, as discussed in Section IV.A, prove to be sufficient for accommodating the adverse effects of these faults in a passive manner, without requiring any intervention at the WT and WF level controllers.

Figure 6 provides a visual representation of the generated power by the faulty WTs in comparison to normal (fault/attack-free) operation, with and without the FTC. In Fig. 6, distinct lines are employed to depict various operational scenarios. Green lines represent normal (fault/attack-free) operation, red lines denote operation during physical faults in the absence of FTC, and blue lines represent operation during physical faults with FTC (specifically, AMPCs). Notably, the blue lines, which correspond to faulty operation with FTC, closely follow the green lines representing fault/attack-free operation. This visual evidence underscores the effectiveness of the proposed AMPCs in adeptly managing power loss, ensuring that the mildly faulty WT continues to generate power efficiently and reliably, even in challenging operational conditions.

B. Scenario 2: Physical Faults (Mild and Severe Power Loss)

In the second scenario, a severe fault in T_1 leads to a complete loss of power generation, resulting in zero power output after 700 s. The designed FTC strategies, specifically the AMPCs and the CRM, are employed to address the effects of partial or total power loss. According to Algorithm 3, the CRM at the WF level is responsible for mitigating severe power loss faults, while the AMPCs at the WT level passively manage the impacts of mild-level faults.

Figure 7 provides insight into several key WF characteristics, including the power responses of faulty WTs, grid frequency, total power generation within the farm, and the WFNO's output. In this figure, the green, red, and blue lines mean the same as in Fig. 6, but the black lines are added which represent faulty operation with full FTC (both AMPCs and CRM). Figure 7(a) specifically illustrates the power generation responses of the faulty WTs. The overlapping black lines tracking the green ones highlight the effectiveness of the proposed solutions in efficiently managing and accommodating the impacts of physical faults in the WTs. Notably, slight discrepancies between the black and green lines between the 200 s and 700 s in Fig. 7(a) stem from the severe power loss occurred in T_1. It is worth noting that despite utilizing the same settings, such as wind profiles and electrical loads, for both scenarios, there are differences in power generation from the same WTs. These differences arise from variations in the value of Hf_{q_1} and the available unused power in T_2 to T_{10}, which necessitate an increase in power demand from those WTs to compensate for the lost power in T_1.

In Fig. 7, other critical characteristics of the WF are also depicted to provide insights into its behavior under different conditions. These characteristics include the grid frequency f_m, the total power generated by the WF P_G, and the total power demanded, which corresponds to the output of the WFNO denoted as P_D. Notably, the figure reveals the adverse impacts of a fault occurring in T_1, where severe power loss triggers noticeable deviations in both the grid frequency and WFNO's output. These deviations underscore the adverse consequences of faults on the WF's performance. However, by implementing the recommended FTC, as depicted by the black lines in Fig. 7(b), the WF demonstrates a remarkable ability to mitigate the impacts of mild and severe faults at both the individual WT and entire WF levels. The slight variations observed in the black line of Fig. 7(c) are associated with moments when mild fault activities start or end, or during abrupt wind speed disturbances. Furthermore, Fig. 7(d) reveals a critical insight: the WF, when operating under faulty conditions without the benefit of FTC (illustrated by the red line), is required to supply a greater amount of power compared to when FTC strategies are employed.

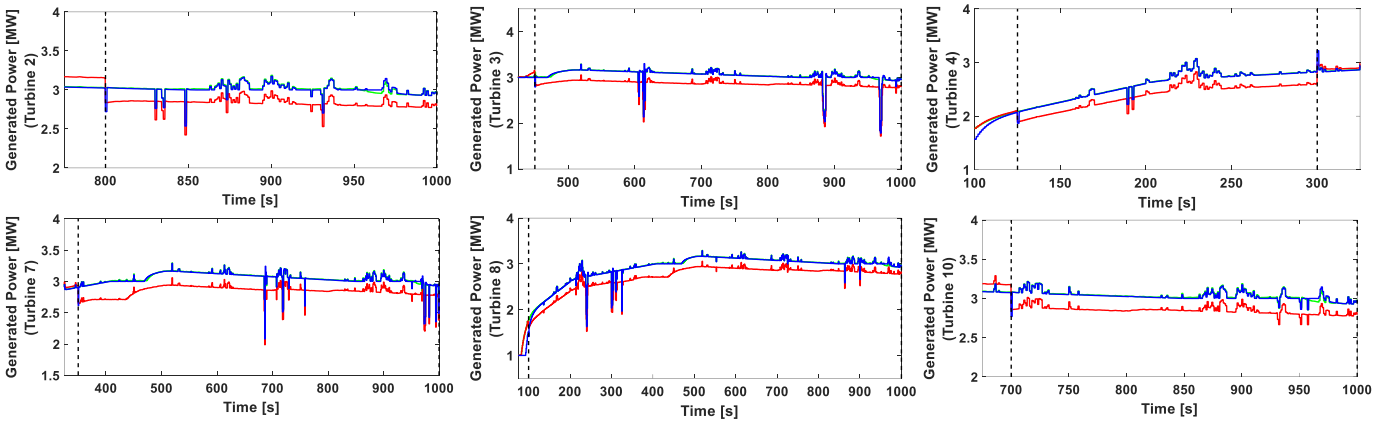

Fig. 6. Power responses in the faulty WTs in Scenario 1.

Note: In this figure, green lines represent normal (fault/attack-free) operation, red lines represent operation under physical faults without FTC, and blue lines represent operation under physical faults with FTC (AMPCs only).

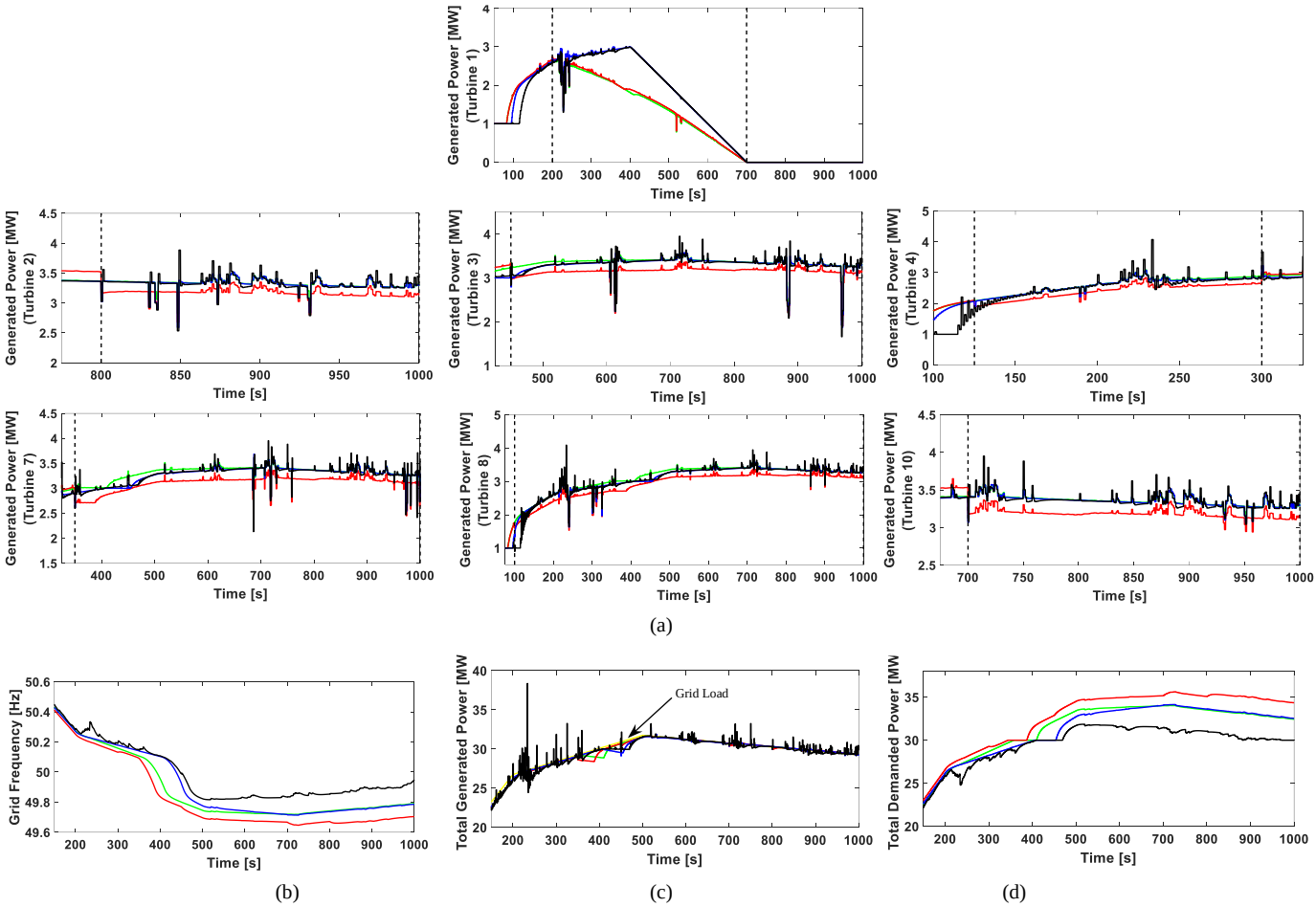

Fig. 7. WF characteristics in Scenario 2: (a) faulty WTs' power responses, (b) frequency, (c) WF generated power, and (d) WFNO's output.

Note: In this figure, green lines represent normal (fault/attack-free) operation, red lines represent operation under physical faults without FTC, blue lines represent operation under physical faults with FTC (AMPCs only), and black lines represent operation under physical faults with full FTC (AMPCs and CRM).

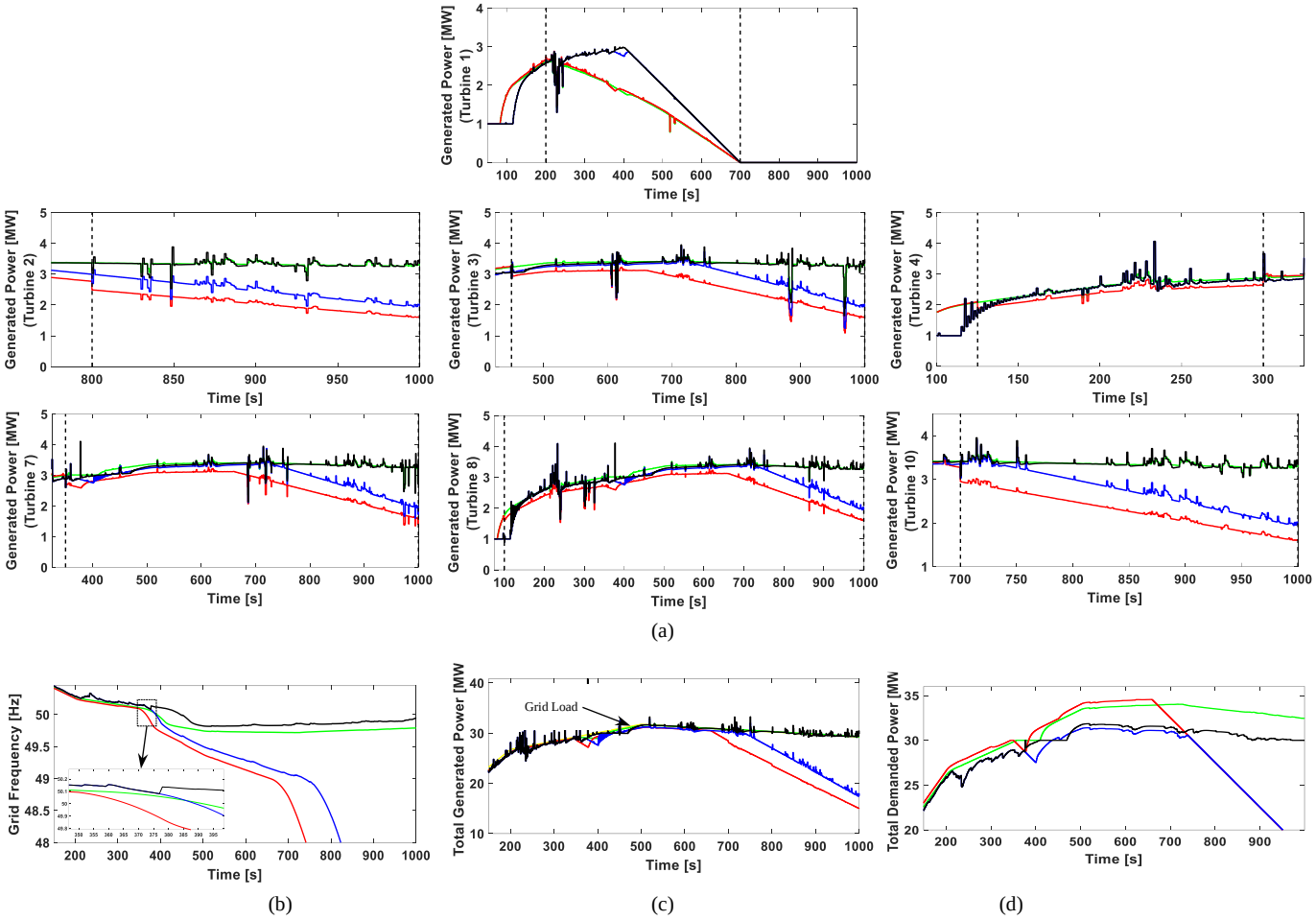

Fig. 8. WF characteristics in Scenario 3: (a) faulty WTs power responses, (b) frequency, (c) WF generated power, and (d) received total demanded power.

Note: In this figure, green lines represent normal (fault/attack-free) operation, red lines represent operation under physical faults and cyberattack without FTC and ARC, blue lines represent operation under physical faults and cyberattack only with full FTC (AMPCs and CRM), and black lines represent operation under physical fault and cyberattack with full FTC and ARC (AMPCs, CRM, and ASC).

Table V Simulation Results for Different Parameters

	Mild Power Loss	Severe Power Loss	Attack Parameter (γ_r)	RMSE (%)	Attack Detection ($t_d[s]$)
Scenario 1	3% in T_2, T_3, T_4, T_7, T_8, and T_{10}	-	-	0.221	-
	3% in T_2, T_3, T_4, and 7% in T_7, T_8, and T_{10}	-	-	0.228	-
	7% in T_2, T_3, T_4, T_7, T_8, and T_{10}	-	-	0.235	-
Scenario 2	3% in T_2, T_3, T_4, T_7, T_8, and T_{10}	100% in T_1	-	0.283	-
	3% in T_2, T_3, T_4, and 7% in T_7, T_8, and T_{10}	70% in T_1	-	0.279	-
	7% in T_2, T_3, T_4, T_7, T_8, and T_{10}	50% in T_1	-	0.273	-
Scenario 3	3% in T_2, T_3, T_4, T_7, T_8, and T_{10}	100% in T_1	-0.5×10^5	0.313	376
	3% in T_2, T_3, T_4, and 7% in T_7, T_8, and T_{10}	70% in T_1	-0.7×10^5	0.308	364
	7% in T_2, T_3, T_4, T_7, T_8, and T_{10}	50% in T_1	-0.9×10^5	0.316	358

Additionally, the blue lines in Fig. 7 show faulty operation with only AMPCs. As anticipated, while the utilization of AMPCs contributes to an enhancement in grid frequency, it is not as effective as the combined use of full FTC (both AMPCs and CRM).

C. *Scenario 3: Both Physical Faults and Cyberattacks*

In the third scenario, in addition to the physical faults in Scenario 2, ramp attack template in Subsection III.B is used. The ramp attack can lead to severe damages if not detected and mitigated in a timely manner. Figure 8 shows some of the WF

characteristics including faulty WTs power responses, grid frequency, WF total generated power, and received total demanded power. In this figure, green lines depict normal operation without any faults or attacks, red lines represent operation affected by faults and attacks in the absence of FTC and ARC, blue lines illustrate operation under the influence of faults and attacks with the full implementation of FTC, including AMPCs and CRM, and lastly, black lines indicate operation during faults and attacks with complete FTC and ARC integration, involving AMPCs, CRM, and ASC. In more detail, Fig. 8(a) shows the WTs' generated powers under the cyber-physical anomalies with and without FTC and ARC. As can be seen, in the absence of FTC and ARC, the generated powers in the WTs (i.e., the red lines) suddenly decrease after about 650 s. After this moment, the baseline APC is not sufficient anymore to control the system appropriately. This is caused by the absolute value of the frequency error f_e in Eq. (1), which increases due to the cyberattack, and saturates P_D at its maximum value P_{max}. It is worth noting that although the FTC slightly improves the WF operation under this scenario (see the blue lines), it is not able to completely mitigate the cyberattack impacts, and the saturation of P_D happens again (this time after about 740 s).

As discussed in Section IV, the IDFD system provides $\tilde{P}_{D,a}$ (in addition to Hf_{q_i}) that is the online estimate of the attack-related malicious data whenever an attack is detected. According to the obtained results, the IDFD system can effectively detect and identify the cyberattack within seconds after its occurrence (i.e., the attack is detected at $t_d = 376$ s) and before the actual grid frequency hits the threshold value of 49.2 Hz at 572 s. From Fig. 8(b), it is observed that the responsive mitigation of cyberattacks using ASC is successful since the frequency is maintained near the normal operation case (see the black lines). Moreover, Figs. 8(c) and 8(d) illustrate the WF generated power P_G and corrected demanded power $P_{D,cor}$, respectively.

Finally, to demonstrate the effectiveness of the proposed cooperative controllers in the three mentioned scenarios, extensive simulation studies were conducted under various levels of physical faults and cyberattack parameters. The timelines for physical faults and cyberattack are considered the same as before. The results are presented in Table V. In this table, root-mean-squared-percentage error (RMSPE), with respect to WF generated power, is used to measure the performance difference between the proposed FTC and ARC under fault and/or attack conditions and the baseline controller during normal operation. Furthermore, the table displays the attack detection times from the IDFD system. As can be seen, all simulations clearly show the successful performance of the cooperative FTC and ARC (i.e., AMPCs, CRM, and ASC) in handling both the physical faults and cyberattacks.

VI. Conclusions and Future Works

To address the growing threat of cyberattacks in addition to physical faults against wind farms (WFs), this paper proposes a novel intrusion detection and fault diagnosis (IDFD) system along with a hybrid cooperative fault-tolerant control (FTC) and attack-resilient control (ARC) design. The IDFD system continuously monitors in real-time to detect and identify physical faults (i.e., power loss due to blade erosion or debris accumulation on wind turbine (WT) blades) and cyberattacks (i.e., data integrity attacks targeting the WF network operator (WFNO)). To handle the impacts of mild physical faults, adaptive model predictive controllers (AMPCs) are employed at the WT level. For severe physical faults, the FTC uses a control reallocation mechanism (CRM) at the WF level. Additionally, the ARC responsively addresses the impacts of detected cyberattacks on the safe and secure regulation of active power from the WF using an automatic signal correction (ASC) technique. All simulations based on an advanced WF benchmark demonstrate the effectiveness of the IDFD as well as the FTC and ARC, offering an efficient solution adaptable to a variety of physical faults and cyberattacks.

Future research can expand upon this hybrid approach by addressing other common physical faults observed in WFs, such as issues like misaligned blades due to improper installation or variations in drivetrain damping. Additionally, researchers can investigate various types of cyberattacks, including those targeting control and monitoring systems at both the WF dispatch control and individual WT levels. Furthermore, future research directions can delve into the integration of these aspects to develop a more comprehensive WF management solution. This expanded approach would encompass the mitigation of mechanical damages and the consideration of broader impacts resulting from physical faults and/or cyberattacks. This holistic strategy holds the potential to significantly enhance the overall resilience and performance of WFs.

References

[1] S. Jadidi, H. Badihi, and Y.M. Zhang, "Fault-Tolerant Cooperative Control of Large-Scale Wind Farms and Wind Farm Clusters," *Energies*, vol. 14, no. 21, p. 7436, 2021.

[2] A. Sanghvi, B. Naughton, C. Glenn, J. Gentle, J. Johnson, J. Stoddard, et al., *Roadmap for Wind Cybersecurity*, The U.S. Department of Energy, Energy Efficiency and Renewable Energy (EERE), Wind Energy Technologies Office (WETO), 2020.

[3] W. Duo, M. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," *IEEE/CAA J. of Auto. Sinica*, vol. 9, no. 5, pp. 784-800, 2022.

[4] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure Control of Multiagent Systems against Malicious Attacks: A Brief Survey," *IEEE Trans. on Ind. Informatics*, vol. 18, no. 6, pp. 3595-3608, 2022.

[5] H. Badihi, Y.M. Zhang, B. Jiang, P. Pillay and S. Rakheja, "A Comprehensive Review on Signal-Based and Model-Based Condition Monitoring of Wind Turbines: Fault Diagnosis and Lifetime Prognosis," *Proc. of the IEEE*, vol. 110, no. 6, pp. 754-806, 2022.

[6] A. Fekih, H. Habibi, and S. Simani, "Fault Diagnosis and Fault Tolerant Control of Wind Turbines: An Overview," *Energies*, vol. 15, no. 19, p. 7186, 2022.

[7] H. Badihi, S. Jadidi, Z. Yu, Y.M. Zhang and N. Lu, "Smart Cyber-Attack Diagnosis and Mitigation in a Wind Farm Network Operator," *IEEE Trans. on Ind. Informatics*, vol. 19, pp. 9468-9478 2023.

[8] H. Badihi, Y.M. Zhang, and H. Hong, "Fault-Tolerant Cooperative Control in an Offshore Wind Farm using Model-Free and Model-Based Fault Detection and Diagnosis Approaches," *Appl. Energy*, vol. 201, pp. 284-307, 2017.

[9] H. Badihi, Y.M. Zhang, P. Pillay, and S. Rakheja, "Application of FMRAC to Fault-Tolerant Cooperative Control of a Wind Farm with Decreased Power Generation due to Blade Erosion/Debris Build-Up," *Int. J. Adapt. Cont. Sig. Process*, vol. 32, pp. 628-645, 2018.

[10] H. Badihi, S. Jadidi, Y.M. Zhang, P. Pillay, and S. Rakheja, "Fault-Tolerant Cooperative Control in a Wind Farm using Adaptive Control Reconfiguration and Control Reallocation," *IEEE Trans. Sustain. Energy*, vol. 11, pp. 2119-2129, 2019.

[11] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation," *Int. J. of Critical Infra. Protection*, vol. 17, pp. 3-14, 2017.

[12] T. Cruz, et al., "A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems," *IEEE Trans. on Ind. Informatics*, vol. 12, no. 6, pp. 2236-2246, 2016.

[13] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C. Liu, "Cyberattack to Cyber-Physical Model of Wind Farm SCADA," *Proc. of the 44th Ann. Conf. of the IEEE Ind. Elect. Society*, pp. 4929-4934, 2018.

[14] J. Yan, C. Liu, and M. Govindarasu, "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis," *Proc. of the 2011 IEEE/PES Power Syst. Conf. and Expo.*, pp. 1-6, 2011.

[15] Y. Zhang, Y. Xiang, and L. Wang, "Power System Reliability Assessment Incorporating Cyber Attacks against Wind Farm Energy Management Systems," *IEEE Trans. on Smart Grid*, vol. 8, pp. 2343-2357, 2017.

[16] S. Axelsson, *Intrusion Detection Systems: A Survey and Taxonomy*, Dept. Computer Engineering, Chalmers Univ. Technol., 2000.

[17] J. Blesa, P. Jiménez, D. Rotondo, et al., "An Interval NLPV Parity Equations Approach for Fault Detection and Isolation of a Wind Farm," *IEEE Trans. Ind. Elect.*, vol. 62, pp. 3794-3805, 2015.

[18] D. Li, P. Li, W. Cai, Y. Song, and H. Chen, "Adaptive Fault-Tolerant Control of Wind Turbines with Guaranteed Transient Performance Considering Active Power Control of Wind Farms," *IEEE Trans. Ind. Elect.*, vol. 65, pp. 3275-3285, 2018.

[19] K. Ma, J. Zhu, M. Soltani, A. Hajizadeh, and Z. Chen, "Optimal Power Dispatch of an Offshore Wind Farm under Generator Fault," *Appl. Sci.*, vol. 9, pp. 1184, 2019.

[20] A.K. Patil and A.G. Thosar, "Fault-Tolerant Wind Energy Controlling System Using PI Controller with HBO Algorithm," *Journal of The Institution of Engineers (India): Series C*, vol. 1, 2023.

[21] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif, and K. Plataniotis, "Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation Under Cyber Attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3188-3202, 2022.

[22] Z. Li, M. Wang, Y. Yan, D. Qi, Z. Xu, J. Zhang, and Z. Wang, "A Tube Model Predictive Control Based Cyber Attack-Resilient Optimal Voltage Control Strategy in Wind Farms," *CSEE Journal of Power and Energy Systems*, 2023.

[23] S. Zhao, Q. Yang, P. Cheng, R. Deng, and J. Xia, "Adaptive Resilient Control for Variable-Speed Wind Turbines against False Data Injection Attacks," *IEEE Trans. on Sustain. Energy*, vol. 13, no. 2, pp. 971-985, 2022.

[24] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif and K. Plataniotis, "Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation under Cyber Attacks," *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 3188-3202, 2022.

[25] M. Soltani, T. Knudsen, and T. Bak, "Modeling and Simulation of Offshore Wind Farms for Farm Level Control," *Proc. of the Europ. Offshore Wind Conf. and Exhibit. (EOW)*, Stockholm, Sweden, 2009.

[26] J. Jonkman, S. Butterfield, W. Musial, and G. Scott, *Definition of a 5 MW Reference Wind Turbine for Offshore System Development*, National Renewable Energy Laboratory: Golden, CO, USA, 2009.

[27] P.S. Veers, "Three-Dimensional Wind Simulation," *Sandia National Labs.*, Albuquerque, NM (USA), 1988.

[28] L.Y. Pao and K.E. Johnson, "Control of Wind Turbines: Approaches, Challenges, and Recent Developments," *IEEE Cont. Syst. Mag.*, vol. 31, no. 2, pp. 44-62, 2011.

[29] Y. Mousavi, *Optimal and Robust Fault Tolerant Control of Wind Turbines Working under Sensor, Actuator, and System Faults*, School of Computing, Engineering and Built Environment, Glasgow Caledonian Univ., 2023.

[30] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," *IEEE Trans. on Smart Grid*, vol. 5, pp. 580-591, 2014.

[31] H. He and J. Yan, "Cyber-Physical Attacks and Defences in the Smart Grid: A Survey," *IET C.-Ph. Sys.: Theo. & App.*, vol. 1, pp. 13-27, 2016.

[32] S. Jadidi, H. Badihi, and Y.M. Zhang, "Passive Fault-Tolerant Control Strategies for Power Converter in a Hybrid Microgrid," *Energies*, vol. 13, p. 5625, 2020.

[33] R. Tóth, H.S. Abbas, and H. Werner, "On the State-Space Realization of LPV Input-Output Models: Practical Approaches," *IEEE Trans. on Cont. Sys. Tech.*, vol. 20, no. 1, pp.139-153, 2011.

[34] A. Bemporad, N. Ricker, and J.G. Owen, "Model Predictive Control—New Tools for Design and Evaluation," *Am. Cont. Conf.*, vol. 6, pp. 5622–5627, 2004.

[35] A. Bemporad, N. Ricker, and M. Morari, "Model Predictive Control Toolbox for MATLAB: User's Guide," *The MathWorks, Inc.*, 2014.

[36] T. Takagi and M. Sugeno, "Fuzzy Identification of Systems and Its Applications to Modeling and Control," *IEEE Trans. on Syst., Man, and Cyb.*, vol. 15, pp. 116-132, 1985.

Saeedreza Jadidi (Member, IEEE) holds a B.S. degree in computer engineering and an M.S. degree in mechatronics and control systems engineering. He earned his Ph.D. in mechanical engineering from Concordia University, Montréal, QC, Canada, and currently serves as a postdoctoral researcher at the University of Saskatchewan. Dr. Jadidi's current research focuses on several key areas, including condition monitoring, diagnostics, and prognostics in cyber-physical systems. Additionally, he specializes in fault-tolerant and attack-resilient control. His work extends to specific application domains with a particular emphasis on smart grids, mechatronic and robotic systems, as well as renewable energy systems.

Hamed Badihi (Senior Member, IEEE) earned his Ph.D. in mechanical engineering from Concordia University, Montréal, QC, Canada, in 2016. Following that, he held the position of Horizon Postdoctoral Fellow at Concordia University for two years. Previously, he served as an Associate Professor at the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China. Dr. Badihi currently holds the position of Assistant Professor in Dependable Automation Systems at the Automation Technology and Mechanical Engineering Unit, Faculty of Engineering and Natural Sciences, Tampere University, Tampere, Finland. His impactful research in wind energy applications has resulted in over 50 publications in leading journals and international conference proceedings. Notably, he is the first author of the paper titled "A Comprehensive Review on Signal-Based and Model-Based Condition Monitoring of Wind Turbines: Fault Diagnosis and Lifetime Prognosis," published in the prestigious PROCEEDINGS OF THE IEEE. Dr. Badihi's research interests encompass all facets of condition monitoring, fault diagnosis and prognosis, as well as fault-tolerant and attack-resilient control in cyber-physical renewable energy systems. Specific areas of focus include wind turbines and wind farms, solar photovoltaic systems, microgrids, and smart grids. Currently, Dr. Badihi holds editorial roles and serves as a Guest Editor for several journals. Moreover, he actively contributes as a member of the technical/program committees for various international conferences.

Youmin Zhang (Fellow, IEEE) earned his B.S., M.S., and Ph.D. degrees in automatic control from the Department of Automatic Control, Northwestern Polytechnical University, Xi'an, China, in 1983, 1986, and 1995, respectively. Currently, he holds the position of Professor at the Department of Mechanical, Industrial, and Aerospace Engineering, Concordia University, Canada. Dr. Zhang's research interests lie in the domains of monitoring, diagnosis, physical fault/cyber-attack-tolerant/resilient control, as well as guidance, navigation, and control of unmanned systems and smart grids. These areas find applications in contexts such as forest fires and smart cities within the framework of cyber-physical systems (CPSs), complemented by remote sensing techniques. His prolific career includes the publication of 8 books and over 600 journal and conference papers, many of which are highly cited. Dr. Zhang is a registered Professional Engineer in Ontario, Canada, a Fellow of the Canadian Society of Mechanical Engineering (CSME), and a member of the Technical Committee for several scientific societies. Dr. Zhang has held various editorial roles, including Editor-in-Chief and Editorial (Advisory) Board Member for several journals. He is also a Member of the Board of Governors and Representatives for *Journal of Intelligent & Robotic Systems*, Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS - II: EXPRESS BRIEFS, *IET Cyber-systems and Robotics*, *Unmanned Systems*, *Security and Safety*. Moreover, he serves as the Deputy Editor-in-Chief of *Guidance, Navigation and Control*. Dr. Zhang has played key roles such as (Honorary) General Chair and Program Chair in several conferences related to unmanned systems, renewable energy, and smart cities.