Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Reliability-Gated GRU-Based Secure Control of a Nonlinear Floating Offshore Wind Turbine Under False Data Injection Attacks

Nadir Abbas
Dalian Maritime University
Li-Ying Hao
Dalian Maritime University
Majid Ayoubi
ayoubi.m@ku.edu.af

Kabul University

Article

Keywords: Floating offshore wind turbine, false-data injection attack, secure control, GRU predictor, reliability-gated compensation, cyber-physical systems, nonlinear wind turbine control

Posted Date: September 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10760246/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Reliability-Gated GRU-Based Secure Control of a Nonlinear Floating Offshore Wind Turbine Under False Data Injection Attacks

Nadir Abbas [1,*], Li-Ying Hao [1], Majid Ayoubi [2,*]

[1] *College of Marine Electrical Engineering, Dalian Maritime University, Dalian, China; nadirabbas063@gmail.com, haoliying_0305@163.com*

[2] *Computer Science Faculty Kabul University, Kabul, Afghanistan; Email: ayoubi.m@ku.edu.af*

Abstract

The offshore floating wind turbines are coupled with strong wind-wave disturbances and need to rely on feedback from the sensors for the regulation of rotor speed, monitoring of the platform motion, and power regulation. But the FDI attacks may taint the critical measurements, such as rotor speed, platform pitch and generated power, resulting in poor feedback-dependent control behaviour and inaccurate operational assessment. In this paper, a secure-control framework based on a reliability-gated gated recurrent unit (GRU) is proposed to control a nonlinear model of a floating offshore wind turbine (FOWT) designed based on a reference turbine from the NREL (National Renewable Energy Laboratory) 5-MW reference series. The proposed framework combines a residual based attack detection, GRU based safe sensor prediction, channel-wise reliability assessment and reliability gated compensation prior to the corrected measurements being provided to a baseline Region II/III controller. The proposed reliability gate decreases over-reliance on the weakly predicted channels of the sensors and conservatively corrects the uncertain feedback from the platform-motion channels. A set of false measurements (rotor speed, platform pitch, and generated power biases) is added to the various measurement channels during the time period between 120 and 210 s. The simulation results indicate that the total sensor level RMSE of the reliability-gated GRU compensation is 85.95%, of which the rotor speed error is 85.71%, the platform pitch error is 50.01%, and the generated power is 86.33%. Closed-loop secure-control validation results show that the proposed method can detect the attack with 97.27% accuracy, and the RMSE of the rotor-speed and generated-power decreases by 26.96% compared with the unprotected attacked case with the platform-pitch response being almost unchanged. Reliability gating is also robust and ablator robust to show a good trade-off between sensor recovery, prediction uncertainty, and closed-loop control safety. The results show the capability of reliability-aware learning compensation to recover sensors securely and control rotor speed/power in nonlinear floating wind turbine systems when subject to cyber-physical sensor attacks.

Keywords: Floating offshore wind turbine; false-data injection attack; secure control; GRU predictor; reliability-gated compensation; cyber-physical systems; nonlinear wind turbine control

1. Introduction

The global shift towards low carbon and carbon neutral energy systems has led to an increased deployment of renewable energy technologies, with offshore wind energy being one of the key strategies for large-scale clean electricity generation. Onshore wind power has advantages over offshore wind power in terms of higher wind speed and more persistent wind resources, lower land-use restriction and higher potential capacity factor [1]. However, floating offshore wind turbines (FOWTs) have paved the way for the exploitation of wind energy in deep water, where the fixed-bottom foundation becomes economically and technically infeasible, and therefore have received considerable research and industry interest [2]. Despite the advantages of FOWTs, their operation and control are still difficult due to the strong coupling between the aerodynamic, hydrodynamic, structural and control components of the system. In the closed-loop response of a floating wind turbine, the wind turbulence and wave excitation, the platform surge, the platform pitch, the rotor-speed variation, the generator torque dynamics, blade-pitch actuation, and actuator saturation are all intrinsically coupled [3]. Hence, under unsteady offshore operating conditions, stable rotor-speed regulation, acceptable platform motion and reliable power production can be achieved by having accurate sensor feedback and robust control decisions.

Modern FOWTs are cyber–physical energy systems where physical turbine dynamics are highly coupled with sensing, communication, computation and feedback control. Rotor speed, generator power, blade pitch, generator torque, platform pitch, tower motion, nacelle acceleration, wind information and wave information are some of the measured variables in the supervisory and feedback control loops [4]. These measurements are employed to switch between operating regions, to control the generator torque, to calculate the blade-pitch command, to minimize loading on the structure, and for rated power operation. The main difference between Region II and Region III is that in Region II, the controller is mainly responsible for maximizing energy capture via torque control, while in Region III, collective blade-pitch control is applied to control rotor speed and power around rated values. Thus, falsified measurements can directly affect the control input and potentially result in undesirable closed-loop performance, such as inefficiency, safety, or misleading behavior. In the case of floating turbines, the motion of the platform introduces further coupling between rotor aerodynamics and structural response, and the sensitivity of the sensors to platform motion can lead to significant feedback between the two elements, even when some of the sensors are corrupted to a moderate degree [5, 6].

Therefore, cybersecurity is a crucial issue for wind turbine control and monitoring systems. Supervisory control and data acquisition systems, remote communications links, intelligent monitoring platforms, digital twins and data-driven decision-making tools are becoming a critical part of the life of offshore wind farms. These technologies enhance operational awareness and predictive maintenance, but also introduce the wind energy infrastructure with new attack surfaces. In particular, false-data injection (FDI) attacks are more serious than other types of cyberattacks for feedback-controlled systems [7]. FDI attack: Adversary changes the sensor readings without necessarily disrupting communication and causing obvious hardware issues. The measured signal may seem like a valid signal if the injected bias is carefully designed, but it will still fool the

controller. In the case of a FOWT, the measurements of rotor-speed, platform-pitch, and generated-power could be attacked, which can lead to a misjudgement by the controller of the turbine state operation. A biased rotor speed measurement can lead to premature or suboptimal blade pitch; a corrupted platform-pitch signal can cause incorrect platform-rate damping terms; and a corrupted power signal can mask poor power regulation and/or result in erroneous supervisory decisions [8].

So far, most studies for the control of FOWT have concentrated on physical perturbations and modelling uncertainty, such as turbulent wind, irregular waves, platform motions, actuator constraints, and nonlinear aerodynamics effects [9]. These studies have led to significant progress in the fields of baseline control, gain-scheduled control, model predictive control, sliding-mode control, robust control and data-driven prediction. However, very little efforts have been made to achieve comparatively secure closed loop control of FOWTs under cyber-physical sensor attacks. In many of these situations the controller is assumed to have accurate measurements, and the malicious corruption of sensors is not explicitly taken into account. The assumption limits the use of the offshore wind application, as it is challenging to detect and compensate for corrupted measurements in remote offshore wind operation, due to the distributed sensing, communication delay, extreme environmental conditions, and limited physical access [10].

The data driven learning methods are a potential approach for sensor recovery and attacks compensation since they can learn temporal relations between operational variables. Recurrent neural networks, specifically gated recurrent unit (GRU) and long short-term memory models are suitable for the prediction of nonlinear time-series, as they are able to model temporal dependence in wind turbine measurements [11]. A learned predictor can predict safe sensor readings from the non-attacked operational inputs, and the difference between the predicted and sensed signals can be used to identify abnormal behaviour if a safe or acceptable control is desired. However, it is not always safe to achieve direct neural compensation for closed-loop control. A neural predictor might be correct for some channels (e.g., rotor speed or power) but less accurate for other channels (e.g., platform pitch or platform-rate motion). When all the predicted channels are believed equally, weak predicted channels can cause the compensated measurement vector degradation and add extra closed-loop error [12]. In FOWTs, the platform dynamics are lightly damped and strongly coupled with the aerodynamic loading, which is particularly important for this limitation.For this limitation, it is especially important for FOWTs due to the lightly damped and strongly coupled nature between the platform dynamics and the aerodynamic loading, which is called blade icing on FOWT (BLI) (see also [13]).

In order to tackle this problem, in this paper an FDI-attacked nonlinear reduced-order FOWT model is proposed, and a reliability-gated GRU-based secure control framework is developed. The model is based on the rated scale and baseline control structure of the NREL 5-MW reference turbine [14] and the floating structure is not a certified OC3-Hywind or OC4-DeepCwind type, but rather a generic reduced-order surge–pitch platform type. It involves rotor speed dynamics, aerodynamic torque and thrust, platform surge and pitch motion, blade-pitch and generator-torque actuator dynamics, and Region II/Region III supervisory control [15]. This model is not meant to be a substitute for high fidelity aero-hydro-servo-elastic models like OpenFAST or computational-fluid-dynamics (CFD) solvers. Rather, it offers a cloud computing platform

with a clear nonlinear control framework for testing the closed loop turbine response to sensor attacks and data-driven compensation, as described in [16].

The proposed secure control framework will have four major components. An FDI attack model is introduced to corrupt key measurement signals such as rotor speed, platform pitch, platform pitch rate, generator power, blade pitch and generator torque, first. Secondly, a GRU-based safe sensor predictor is trained to predict values of non-attacked sensors given the operational inputs including wind, wave, control commands, and operating-region information. Third, a residual-based detector, which calculates the difference between the attacked measurements and the GRU prediction, is used to detect abnormal sensor behaviour. Fourth, to determine confidence level of each predicted sensor channel during the compensation process, a channel-wise reliability gate is introduced. If an attack is identified, then the compensated measurement is created as a weighed average of the attacked measurement and the GRU prediction, with the weights determined by the reliability of the measurements. This ensures the controller can leverage on accurate prediction channels from the neural network, while negating the impact of weakly predicted channels [17].

The proposed method is primarily based on the reliability-gated compensation mechanism. The approach does not require the complete replacement of attacked measurements with neural predictions, but instead allocates a gain of reliability for each sensor channel: one for validation prediction error and one for scale of the signal. The channels that have the highest prediction reliability are strongly corrected with the GRU estimate, while the channels with lower prediction reliability are corrected more conservatively. It is also significant for FOWT secure control since the aim is not only to reduce the prediction error at the sensor level, but to also ensure safe closed-loop behaviour. The proposed method is especially suitable for enhancing the rotor-speed and power regulation, and also to avoid introducing any more control degradation from unreliability of the platform-motion compensation. The main contributions of this paper are summarized as follows.

1. An OpenFAST-based secure sensor validation framework is developed for the IEA 15-MW reference wind turbine mounted on the UMaine semi-submersible platform. Unlike reduced-order FOWT validation models, the proposed dataset is generated from coupled aero-hydro-servo-elastic simulations under multiple wind–wave operating conditions, providing a physically meaningful basis for evaluating FDI attack detection and sensor compensation.
2. A physics-informed GRU predictor and residual-based multi-channel FDI detector are developed for FOWT sensor reconstruction. The GRU estimates attack-free generator-speed, platform-pitch, generator-power, blade-pitch, and generator-torque responses using physically meaningful OpenFAST inputs, while the residual detector identifies abnormal sensor deviations caused by FDI attacks.
3. A detector-driven reliability-gated compensation law is proposed to reconstruct corrupted sensor measurements without unnecessary replacement of healthy signals. The gate activates only during detected attacks and applies channel-wise reliability weighting to blend attacked measurements with GRU predictions. The framework achieves 95.78% detection accuracy, 100% recall, 0% missed detection, and

attack-interval RMSE reductions of 81.92%, 93.09%, 32.25%, 84.91%, and 83.75% for generator speed, platform pitch, generator power, blade pitch, and generator torque, respectively.

The remainder of this paper is organized as follows. Section **??** presents the control-oriented nonlinear FOWT model, including aerodynamic loading, rotor-speed dynamics, platform motion, actuator dynamics, and the baseline Region II/Region III controller. Section **??** formulates the false-data injection attack model and defines the attacked sensor channels. Section **??** describes the GRU-based safe sensor prediction framework. Section **??** introduces the residual-based attack detector and the reliability-gated compensation law. Section **??** presents the closed-loop secure control implementation using compensated measurements. Section 4 discusses boundedness and closed-loop safety under bounded prediction and compensation errors. Section 5 describes the simulation setup, attack scenario, and evaluation metrics. Section 6 reports the sensor-level compensation, closed-loop secure-control, robustness, and ablation results. Finally, Section 7 concludes the paper and outlines future work toward validation using high-fidelity FOWT models.

2. Reduced-Order FOWT Model and FDI Attack Formulation

The NREL 5-MW reference turbine serves as a motivation for the development of a reduced-order model of a floating offshore wind turbine (FOWT) that is considered rated scale and baseline control structure for this study. The model is not a certified OpenFAST, OC3-Hywind or OC4-DeepCwind benchmark. Rather it offers a linear-to-nonlinear environment through which to simulate secure feedback compensation when the sensor data is polluted by sensor false-data injection (FDI) attacks.

The reduced-order state vector is given by

$$\mathbf{x}_k = \begin{bmatrix} x_{s,k} & \dot{x}_{s,k} & \theta_{p,k} & \dot{\theta}_{p,k} & \Omega_{r,k} & \beta_k & T_{g,k} & \Omega_{f,k} \end{bmatrix}^T, \tag{1}$$

where x_s and θ_p are the platform surge and pitch, respectively, Ω_r is the rotor speed, β is the blade pitch angle, T_g is the generator torque, and Ω_f is the filtered signal of the rotor speed. The discrete-time nonlinear plant is represented compactly as

$$\mathbf{x}_{k+1} = \mathbf{x}_k + T_s f\left(\mathbf{x}_k, \mathbf{u}_k, \mathbf{d}_k\right), \tag{2}$$

where T_s is the sampling time, $\mathbf{u}_k = [\beta_{c,k}, T_{g,c,k}]^T$ is the controller-command vector, and $\mathbf{d}_k$ contains wind and equivalent wave-excitation inputs. The nonlinear function $f(\cdot)$ includes rotor-speed dynamics, generic surge–pitch platform dynamics, blade-pitch and generator-torque actuator dynamics, and generated-power calculation.

The measured sensor vector used by the secure-control framework is

$$\mathbf{y}_k = \begin{bmatrix} \Omega_{r,k} & \theta_{p,k} & \dot{\theta}_{p,k} & P_{g,k} & \beta_k & T_{g,k} \end{bmatrix}^T. \tag{3}$$

The standard Region II/Region III wind-turbine control logic is used in the baseline controller. In Region III, the generator torque is maintained approximately at its rated value while in Region II generator torque

is programmed in response to the rotor speed. In compact form,

$$\mathbf{u}_k = \mathcal{K}\left(\mathbf{y}_k, \Omega_{\text{rated}}\right), \tag{4}$$

Note that $\mathcal{K}(\cdot)$ is the baseline Region II/III control law.

In sensor level FDI attacks, the measurement vector is corrupted as shown below.

$$\mathbf{y}_k^a = \mathbf{y}_k + \alpha_k \mathbf{a}_k, \tag{5}$$

The attacked measurement vector is $\mathbf{y}_k^a$, attack signal is $\mathbf{a}_k$, and activation variable is α_k which is binary. In the main simulation case,

$$\alpha_k = \begin{cases} 1, & 120 \text{ s} \leq t_k \leq 210 \text{ s}, \\ 0, & \text{otherwise}. \end{cases} \tag{6}$$

The three channels that respond to the activated attack are rotor speed, platform pitch, and generated power. Hence, the attack vector is represented by

$$\mathbf{a}_k = \begin{bmatrix} a_{\Omega,k} & a_{\theta,k} & 0 & a_{P,k} & 0 & 0 \end{bmatrix}^T. \tag{7}$$

In this paper, the objective is not the high fidelity load prediction of FOWT, but rather the reconstruction and closed loop protection of this load under corrupted sensor measurements, and this compact model formulation is adequate for this objective.

3. Proposed Reliability-Gated GRU Secure-Control Framework

This section introduces an idea of a reliability-gated GRU secure-control framework. The idea is to predict the output response of the FOWT sensor in the absence of attack given a GRU network, then compare the prediction to the received measurement to detect FDI attack, and finally compensate the corrupted feedback with the reliability gains obtained in each channel to account for the attack. The resulting vector of measurements is finally sent to the secure Region II/III controller.

The architecture in Fig. 1 is the framework consists of four main parts: GRU-based safe sensor prediction, residual-based attack detection, reliability-gated compensation, and secure feedback control implementation.

3.1. GRU-Based Safe Sensor Prediction

The GRU predictor is trained on FOWT operation data without attacks. It aims to determine the safe sensor vector from the input sequences used during operation which are not directly affected by the envisaged FDI attack. The predicted sensor vector is written to

$$\hat{\mathbf{y}}_k = \mathcal{N}_{\text{GRU}}\left(\mathbf{Z}_k; \boldsymbol{\Theta}_{\text{G}}^{\star}\right), \tag{8}$$

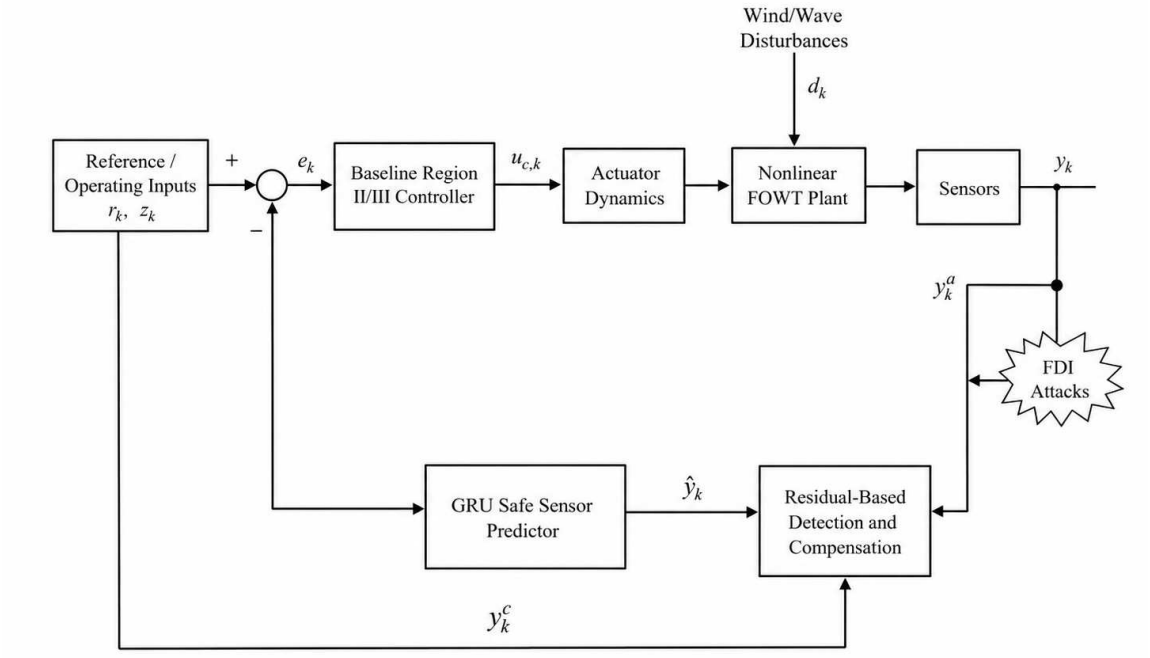


Fig. 1: Control structure of the reliability-gated GRU secure-control scheme for a nonlinear FOWT under FDI attacks.

The prediction of the non-attacked measurement vector $\hat{\mathbf{y}}_k$, the trained GRU network $\mathcal{N}_{\mathrm{GRU}}(\cdot)$, and the optimized GRU parameters $\boldsymbol{\Theta}_{\mathrm{G}}^{\star}$.

The input sequence to the GRU is given by

$$\mathbf{Z}_k = [\mathbf{z}_{k-L+1}, \mathbf{z}_{k-L+2}, \ldots, \mathbf{z}_k], \tag{9}$$

where L is the number of sequences. The operational input vector is chosen to be

$$\mathbf{z}_k = \begin{bmatrix} V_{w,k} & F_{w,k} & M_{w,k} & \beta_{c,k} & T_{g,c,k} & \chi_k \end{bmatrix}^T, \tag{10}$$

In this, $V_{w,k}$ is the wind speed, $F_{w,k}$ and $M_{w,k}$ are equivalent features of the wind-excitation, $\beta_{c,k}$ is the commanded blade pitch, $T_{g,c,k}$ is the commanded generator torque and χ_k is the operating-region indicator. In this reduced order simulation study, $F_{w,k}$ and $M_{w,k}$ are assumed to be the same environmental excitation inputs. In practice, these variables need to be replaced by measured or estimated proxies, such as wave-elevation estimates or platform inertial measurements, or observer-estimated wave loads.

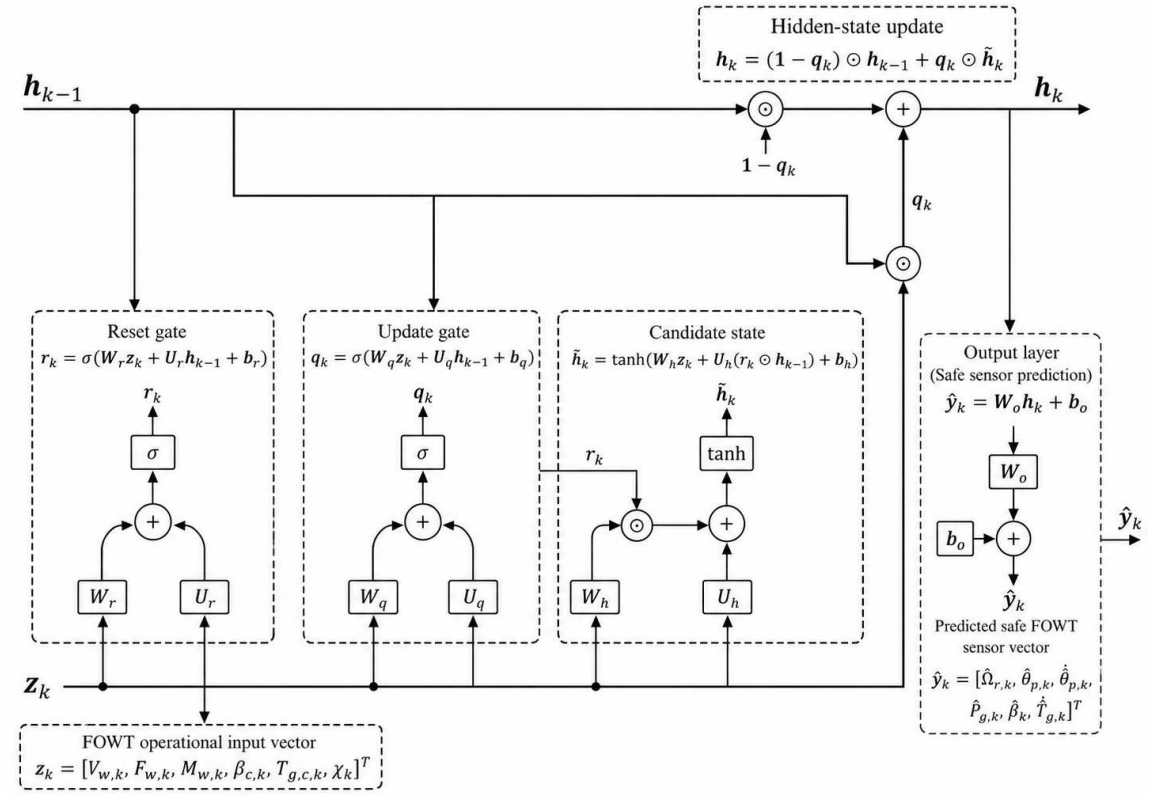


Fig. 2: GRU-based safe sensor predictor used in the proposed FOWT secure-control framework. The operational input vector $\mathbf{z}_k$ is processed through the reset gate, update gate, and candidate-state dynamics to generate the predicted safe sensor vector $\hat{\mathbf{y}}_k$.

For an input vector $\mathbf{z}_k$ and previous hidden state $\mathbf{h}_{k-1}$, the GRU gates are expressed as

$$\mathbf{r}_k = \sigma\left(\mathbf{W}_r \mathbf{z}_k + \mathbf{U}_r \mathbf{h}_{k-1} + \mathbf{b}_r\right), \tag{11}$$

$$\mathbf{q}_k = \sigma\left(\mathbf{W}_q \mathbf{z}_k + \mathbf{U}_q \mathbf{h}_{k-1} + \mathbf{b}_q\right), \tag{12}$$

$$\tilde{\mathbf{h}}_k = \tanh\left(\mathbf{W}_h \mathbf{z}_k + \mathbf{U}_h\left(\mathbf{r}_k \odot \mathbf{h}_{k-1}\right) + \mathbf{b}_h\right), \tag{13}$$

$$\mathbf{h}_k = (\mathbf{1} - \mathbf{q}_k) \odot \mathbf{h}_{k-1} + \mathbf{q}_k \odot \tilde{\mathbf{h}}_k. \tag{14}$$

Here, $\mathbf{r}_k$ is the reset gate, $\mathbf{q}_k$ is the update gate, $\tilde{\mathbf{h}}_k$ is the candidate hidden state, $\sigma(\cdot)$ is the sigmoid function, and $\odot$ denotes element-wise multiplication. The predicted safe sensor vector is obtained using the linear output layer

$$\hat{\mathbf{y}}_k = \mathbf{W}_o \mathbf{h}_k + \mathbf{b}_o. \tag{15}$$

Figure 2 illustrates the GRU-based safe sensor predictor. The GRU is trained offline using non-attacked data, and its weights are kept fixed during online secure-control testing. This prevents the predictor from adapting to corrupted measurements during the attack interval.

3.2. Residual-Based FDI Detection

When operating online, the sensor vector received can be corrupted and is denoted by $\mathbf{y}_k^a$. Its prediction residual is

$$\boldsymbol{\rho}_k = \mathbf{y}_k^a - \hat{\mathbf{y}}_k. \tag{16}$$

The residual is scaled by a diagonal matrix $\mathbf{S}$, to compensate for the different magnitudes of the signals in each channel. The detection index is then calculated as

$$D_k = \left\| \mathbf{S}^{-1} \boldsymbol{\rho}_k \right\|_2 . \tag{17}$$

The binary attack decision is obtained from

$$\delta_k = \begin{cases} 1, & D_k > \rho_{\text{th}}, \\ 0, & D_k \leq \rho_{\text{th}}, \end{cases} \tag{18}$$

where ρ_{th} is the residual threshold obtained from non-attacked validation data. If $\delta_k = 1$ it is considered attacked and the compensation layer is turned on.

3.3. Reliability-Gated Compensation

When some channels have weak predictions, replacing these attacked measurements directly with GRU predictions can be unsafe. Thus, in this paper, a channel-wise reliability gate is introduced. The validation RMSE for the ith sensor channel is given by

$$\epsilon_i = \sqrt{\frac{1}{N_{\text{val}}} \sum_{k=1}^{N_{\text{val}}} \left(y_{i,k} - \hat{y}_{i,k} \right)^2}, \qquad i = 1, 2, \ldots, m. \tag{19}$$

The reliability gain is the following:

$$g_i = \left(1 + \frac{\epsilon_i}{s_i + \epsilon_s} \right)^{-1}, \qquad 0 < g_i \leq 1, \tag{20}$$

The scales of the ith sensor channel are captured by s_i and a small positive constant is chosen as ϵ_s. All of the above are correct.

$$\mathbf{G} = \operatorname{diag}\left(g_1, g_2, \ldots, g_m \right). \tag{21}$$

The compensated sensor vector is then generated as

$$\mathbf{y}_k^c = (1 - \delta_k)\mathbf{y}_k^a + \delta_k \left[(\mathbf{I}_m - \mathbf{G})\, \mathbf{y}_k^a + \mathbf{G}\hat{\mathbf{y}}_k \right]. \tag{22}$$

When no attack is detected, then $\delta_k = 0$ and the measurement received is applied directly to the system. In case of an attack, $\delta_k = 1$ and the received measurement is mixed with the GRU prediction using the

reliability matrix $\mathbf{G}$. Thus, stronger correction is given on channels that are well predicted and conservative correction is given on uncertain channels.

3.4. Ensure Implementation of Feedback Control

The vector of measurements with compensation.

$$\mathbf{y}_k^c = \begin{bmatrix} \Omega_{r,k}^c & \theta_{p,k}^c & \dot{\theta}_{p,k}^c & P_{g,k}^c & \beta_k^c & T_{g,k}^c \end{bmatrix}^T \tag{23}$$

is fed to the secure Region II/III controller. In Region III, the compensated rotor-speed error is defined as

$$e_{\Omega,k}^c = \Omega_{f,k}^c - \Omega_{\text{rated}}, \tag{24}$$

and the safe "Pitch" command is written as

$$\beta_{c,k}^s = \beta_0 + K_{p,\beta} e_{\Omega,k}^c + K_{i,\beta} I_{\Omega,k}^c + K_\theta \alpha_\theta \dot{\theta}_{p,k}^c, \tag{25}$$

The integral of the compensated rotor-speed error $I_{\Omega,k}^c$. Conservative platform rate feedback blending uses the coefficient $\alpha_\theta = 0.25$.

The logic for the generator-torque command is based on the Region II/III logic:

$$T_{g,c,k}^s = \begin{cases} K_{\text{II}} \left(\Omega_{r,k}^c\right)^2, & \text{Region II,} \\ T_{g,\text{rated}}, & \text{Region III.} \end{cases} \tag{26}$$

Lastly, the saturated secure-control command is

$$\mathbf{u}_{c,k}^{s,\text{sat}} = \text{sat}\left(\begin{bmatrix} \beta_{c,k}^s \\ T_{g,c,k}^s \end{bmatrix} \right). \tag{27}$$

The proposed framework doesn't change the fundamental structure of the Region II/III controllers. Instead, it ensures the controller's protection by providing a reliability-gated compensated feedback vector when detected FDI attacks.

The resulting compensated measurement vector $\mathbf{y}_k^c$ is used as the feedback signal in the secure closed-loop controller described in the next section.

3.5. Secure Feedback Control Implementation

The proposed technique does not require the redesign of the baseline wind-turbine controller. Instead, it safeguards the feedback path of the controller by substituting the attacked measurement vector $\mathbf{y}_k^a$, with the compensated measurement vector $\mathbf{y}_k^c$. The compensated feedback vector is:

$$\mathbf{y}_k^c = \begin{bmatrix} \Omega_{r,k}^c & \theta_{p,k}^c & \dot{\theta}_{p,k}^c & P_{g,k}^c & \beta_k^c & T_{g,k}^c \end{bmatrix}^T. \tag{28}$$

Algorithm 1 Reliability-Gated GRU Detection and Compensation

Require: Training/validation data $\mathcal{D}_{\mathrm{tr}}$, $\mathcal{D}_{\mathrm{val}}$, received online measurement $\mathbf{y}_k^a$, GRU input sequence $\mathbf{Z}_k$, scale matrix $\mathbf{S}$, threshold coefficient κ_D

Ensure: Attack decision δ_k, compensated measurement $\mathbf{y}_k^c$, detection index D_k

Offline GRU training and reliability calibration

0: Train the GRU predictor by solving

$$\boldsymbol{\Theta}_G^\star = \arg\min_{\boldsymbol{\Theta}_G} \frac{1}{N_{\mathrm{tr}}} \sum_{k=1}^{N_{\mathrm{tr}}} \left\| \bar{\mathbf{y}}_k - \bar{\hat{\mathbf{y}}}_k \right\|_2^2, \qquad \hat{\mathbf{y}}_k = \mathcal{N}_{\mathrm{GRU}}\left(\mathbf{Z}_k; \boldsymbol{\Theta}_G\right).$$

0: **for** $i = 1, 2, \ldots, m$ **do**

0: Compute the validation prediction error of the ith channel:

$$\epsilon_i = \left(\frac{1}{N_{\mathrm{val}}} \sum_{k=1}^{N_{\mathrm{val}}} \left(y_{i,k} - \hat{y}_{i,k}\right)^2 \right)^{1/2}.$$

0: Compute the channel-wise reliability gain:

$$g_i = \left(1 + \frac{\epsilon_i}{s_i + \epsilon_s}\right)^{-1}, \qquad 0 < g_i \leq 1.$$

0: **end for**

0: Construct the reliability matrix: $\mathbf{G} = \mathrm{diag}\left(g_1, g_2, \ldots, g_m\right)$.

0: Select the detection threshold:

$$\rho_{\mathrm{th}} = \mu_D + \kappa_D \sigma_D, \qquad \mu_D = \mathrm{mean}\left(D_k^{\mathrm{val}}\right), \qquad \sigma_D = \mathrm{std}\left(D_k^{\mathrm{val}}\right).$$

Online residual detection and reliability-gated compensation

0: Predict the safe sensor vector:

$$\hat{\mathbf{y}}_k = \mathcal{N}_{\mathrm{GRU}}\left(\mathbf{Z}_k; \boldsymbol{\Theta}_G^\star\right).$$

0: Compute the detection index:

$$D_k = \left\| \bar{\boldsymbol{\rho}}_k \right\|_2.$$

0: Determine the attack flag using the threshold logic:

$$\delta_k = \begin{cases} 1, & D_k > \rho_{\mathrm{th}}, \\ 0, & D_k \leq \rho_{\mathrm{th}}. \end{cases}$$

0: Compute the reliability-scaled correction term:

$$\Delta \mathbf{y}_k = \delta_k \mathbf{G}\left(\mathbf{y}_k^a - \hat{\mathbf{y}}_k\right).$$

0: Construct the compensated measurement vector:

$$\mathbf{y}_k^c = \mathbf{y}_k^a - \Delta \mathbf{y}_k.$$

0: Equivalently,

$$\mathbf{y}_k^c = \left(1 - \delta_k\right) \mathbf{y}_k^a + \delta_k \left[\left(\mathbf{I}_m - \mathbf{G}\right) \mathbf{y}_k^a + \mathbf{G} \hat{\mathbf{y}}_k\right].$$

0: Supply $\mathbf{y}_k^c$ to the secure Region II/Region III controller. =0

The secure control policy is thus compactly written as

$$\mathbf{u}_{c,k}^{s} = \pi_s\left(\mathbf{y}_k^c\right), \tag{29}$$

where $\pi_s(\cdot)$ refers to the protected Region II/Region III control law.

Rotor-speed filtering during Region III operation is done with the compensated rotor-speed signal:

$$\Omega_{f,k+1}^{c} = \Omega_{f,k}^{c} + T_s \frac{\Omega_{r,k}^{c} - \Omega_{f,k}^{c}}{\tau_f}, \tag{30}$$

and the compensated rotor-speed error is

$$e_{\Omega,k}^{c} = \Omega_{f,k}^{c} - \Omega_{\text{rated}}. \tag{31}$$

The integral state is updated as follows:

$$I_{\Omega,k+1}^{c} = I_{\Omega,k}^{c} + T_s e_{\Omega,k}^{c}. \tag{32}$$

The secure generator-torque command is based on the baseline Region II/Region III logic:

$$T_{g,c,k}^{s} = \begin{cases} K_{\text{II}}\left(\Omega_{r,k}^{c}\right)^2, & \text{Region II,} \\ T_{g,\text{rated}}, & \text{Region III.} \end{cases} \tag{33}$$

The minimum value of blade pitch is maintained in Region II. For Region III, the protected command to control the blade pitch is derived from the compensated rotor speed error and the feedback from the platform pitch rate. The platform-pitch-rate channel is not as reliable as rotor speed or generated power, so a conservative blending factor is used:

$$\dot{\theta}_{p,k}^{s} = \alpha_\theta \dot{\theta}_{p,k}^{c}, \qquad \alpha_\theta = 0.25. \tag{34}$$

Then the last secure Region III pitch command is thrown as

$$\beta_{c,k}^{s} = \beta_0 + K_{p,\beta} e_{\Omega,k}^{c} + K_{i,\beta} I_{\Omega,k}^{c} + K_\theta \alpha_\theta \dot{\theta}_{p,k}^{c}. \tag{35}$$

The resulting secure command is at the actuator level.

$$\mathbf{u}_{c,k}^{s} = \begin{bmatrix} \beta_{c,k}^{s} \\ T_{g,c,k}^{s} \end{bmatrix}. \tag{36}$$

The saturated command vector is indicated as after application of pitch, pitch-rate, torque and torque-rate

limits.

$$\mathbf{u}_{c,k}^{s,\mathrm{sat}} = \mathrm{sat}\left(\mathbf{u}_{c,k}^{s}\right) = \begin{bmatrix} \beta_{c,k}^{s,\mathrm{sat}} \\ T_{g,c,k}^{s,\mathrm{sat}} \end{bmatrix}. \tag{37}$$

The protected closed-loop FOWT dynamics are given by the saturated secure command, which is represented as

$$\mathbf{x}_{k+1}^{s} = \mathbf{x}_{k}^{s} + T_s f\left(\mathbf{x}_{k}^{s}, \mathbf{u}_{c,k}^{s,\mathrm{sat}}, \mathbf{d}_k\right). \tag{38}$$

So the total protected feedback path is given by

$$\mathbf{y}_k \longrightarrow \mathbf{y}_k^a \longrightarrow \hat{\mathbf{y}}_k \longrightarrow \mathbf{y}_k^c \longrightarrow \mathbf{u}_{c,k}^{s,\mathrm{sat}} \longrightarrow \mathbf{x}_{k+1}^{s}. \tag{39}$$

This demonstrates that the proposed method provides a measurement-security layer, i.e., the loop structure of the baseline controller is still maintained, but the influence of the corrupted feedback on pitch and torque commands is decreased.

4. Stability and Boundedness Discussion

The proposed reliability-gated secure-control framework is briefly discussed in this section from a boundedness perspective. The purpose is not to claim that the considered FOWT model is globally asymptotically stable since it is a reduced-order model and nonlinear. Rather, it is desired that the proposed compensation structure preserves control stability of the closed-loop system while maintaining an ultimately bounded response to the protected closed-loop system for standard local stability and bounded-input assumptions, and that the cyber-induced measurement error is bounded.

Let the error between the actual and the predicted values of the GRU be

$$\tilde{\mathbf{y}}_k = \mathbf{y}_k - \hat{\mathbf{y}}_k. \tag{40}$$

The analysis assumes that the prediction error is bounded in the validated operating region:

$$\|\tilde{\mathbf{y}}_k\| \leq \bar{\epsilon}_y, \qquad \forall k, \tag{41}$$

The equality holds if the maximum prediction error within the operating envelope under consideration is equal to $\bar{\epsilon}_y > 0$. The injected attack is also assumed to be bounded:

$$\|\mathbf{a}_k\| \leq \bar{a}, \qquad \forall k. \tag{42}$$

The assumption of the simulation setting is that the GRU is trained and validated in the same reduced order FOWT operating envelope and the attack type considered is a bounded sensor-bias signal.

The reliability-gated compensation law is:

$$\mathbf{y}_k^c = (1-\delta_k)\,\mathbf{y}_k^a + \delta_k\left[(\mathbf{I}_m - \mathbf{G})\,\mathbf{y}_k^a + \mathbf{G}\hat{\mathbf{y}}_k\right], \tag{43}$$

δ_k is detection decision and $\mathbf{G}$ is a diagonal reliability matrix. The compensation error is defined as:

$$\mathbf{e}_{c,k} = \mathbf{y}_k - \mathbf{y}_k^c. \tag{44}$$

If the attack is detected correctly then $\delta_k = 1$ and $\mathbf{y}_k^a = \mathbf{y}_k + \mathbf{a}_k$.

Substituting this relation into Eq. (43) gives

$$\mathbf{e}_{c,k} = -\left(\mathbf{I}_m - \mathbf{G}\right)\mathbf{a}_k + \mathbf{G}\tilde{\mathbf{y}}_k. \tag{45}$$

Therefore,

$$\|\mathbf{e}_{c,k}\| \le \|\mathbf{I}_m - \mathbf{G}\|\,\bar{a} + \|\mathbf{G}\|\,\bar{\epsilon}_y. \tag{46}$$

The primary trade-off of the reliability gate is given in Equation (46). The larger the gain matrix $\mathbf{G}$, the less attack bias it removes, but the more influence it has over the prediction error from the GRU. A smaller gain matrix will lead to a smaller effect of prediction error but to a larger attack bias residual in the compensated signal. The proposed channel-wise reliability design takes into balance these two effects.

The same limits also apply to missed detections and false alarms. If an attack is missed, then $\delta_k = 0$ and $\mathbf{y}_k^c = \mathbf{y}_k^a$, which gives $\|\mathbf{e}_{c,k}\| \le \bar{a}$. If a false alarm occurs, then $\delta_k = 1$ while $\mathbf{y}_k^a = \mathbf{y}_k$, which gives $\|\mathbf{e}_{c,k}\| \le \|\mathbf{G}\|\bar{\epsilon}_y$. So when the attack and prediction errors are bounded, the detection error will not cause the measurement error to be unbounded to reduce compensation performance.

The closed loop FOWT dynamics with protection can be expressed as

$$\mathbf{x}_{k+1}^s = F_s\left(\mathbf{x}_k^s, \mathbf{y}_k - \mathbf{e}_{c,k}, \mathbf{d}_k\right), \tag{47}$$

The vector $\mathbf{d}_k$ represents the environmental disturbance vector. Thus, the compensation error is a second bounded input to the closed loop system. Suppose that the considered operating region of the nominal closed-loop FOWT system is locally ISS bounded and the disturbance is ISS bounded in the considered operating region.

$$\|\mathbf{d}_k\| \le \bar{d}. \tag{48}$$

Then there exist a non-negative constant c_0 and class-$\mathcal{K}$ functions $\gamma_d(\cdot)$ and $\gamma_e(\cdot)$ such that

$$\limsup_{k\to\infty} \|\mathbf{x}_k^s\| \le c_0 + \gamma_d\left(\bar{d}\right) + \gamma_e\left(\bar{e}_c\right), \tag{49}$$

where

$$\bar{e}_c = \|\mathbf{I}_m - \mathbf{G}\|\,\bar{a} + \|\mathbf{G}\|\,\bar{\epsilon}_y. \tag{50}$$

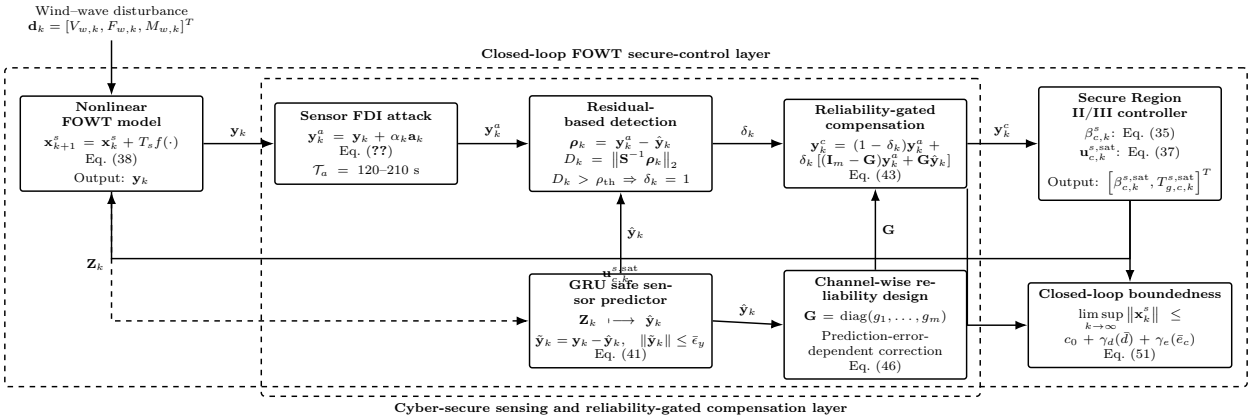


Fig. 3: Equation-supported flow of the proposed reliability-gated GRU secure-control framework.

This substitution of Eq. (50) into Eq. (49) gives

$$\limsup_{k\to\infty} \|\mathbf{x}_k^s\| \le c_0 + \gamma_d\left(\bar{d}\right) + \gamma_e\left(\|\mathbf{I}_m - \mathbf{G}\|\,\bar{a} + \|\mathbf{G}\|\,\bar{\epsilon}_y\right). \tag{51}$$

The result shows that under the conditions that the nominal closed-loop system is locally stable, the wind–wave disturbance is bounded, the FDI attack is bounded and the GRU prediction error is bounded, the protected closed-loop response is ultimately bounded. This analysis backs the proposed framework for using it as a secure compensation layer with reliability awareness. It does not guarantee global asymptotic stability for all wind–wave conditions or for an arbitrary attacking signal.

Before going towards simulation setup, the flow of the proposed control framework is summarized in Fig. 3. The diagram links the main components of the framwork, including the FOWT model, FDI attack model, GRU-based safe sensor prediction, residual detection, reliability-gated compensation, and secure Region II/III control. This flow clarifies how the attacked measurements are detected and corrected before being supplied to the closed-loop controller.

5. Simulation Setup

In this section, the settings for the simulation of the proposed reliability-gated GRU secure-control framework are summarized. The goal is to compare nominal operation, unprotected attacked operation, protected operation with the proposed method and no-gate GRU compensation. The same reduced-order nonlinear FOWT model, trained GRU predictor, residual threshold and reliability matrix are utilized in all main, robustness and ablation cases.

5.1. Simulation Configuration

The summary of the simulation configuration is shown in Table 1. Because this study employs a reduced-order control-oriented model, the table lists the model structure, operating condition, attack setting, and secure-control configuration, not a complete high fidelity aero-hydro-servo-elastic parameter set.

Table 1: Reduced-order FOWT simulation configuration.

Item	Setting	Role in the simulation
Reference turbine scale	NREL 5-MW-inspired	Provides the rated-power scale and baseline control structure.
Model type	Nonlinear reduced-order control-oriented FOWT model	Used for preliminary cyber-secure feedback-control validation.
Floating-platform representation	Generic surge–pitch platform	Captures dominant platform-motion coupling without claiming OC3/OC4/OpenFAST fidelity.
State vector	$[x_s, \dot{x}_s, \theta_p, \dot{\theta}_p, \Omega_r, \beta, T_g, \Omega_f]^T$	Represents platform motion, rotor speed, actuator states, and filtered rotor speed.
Measured output vector	$[\Omega_r, \theta_p, \dot{\theta}_p, P_g, \beta, T_g]^T$	Defines the monitored sensor channels used for detection and compensation.
Control command vector	$[\beta_c, T_{g,c}]^T$	Contains blade-pitch and generator-torque commands.
Environmental inputs	$[V_w, F_w, M_w]^T$	Represents wind speed and equivalent wave-excitation features.
Operating condition	Above-rated Region III dominant operation	Uses generator torque near rated value and blade pitch for rotor-speed regulation.
Simulation duration	900 s	Total nonlinear simulation time.
Main plotted interval	0–300 s	Time window used for the main response figures.
Attack interval	120–210 s	Time interval during which FDI attacks are activated.
Main attacked channels	Rotor speed, platform pitch, generated power	Dominant channels used for secure sensor-recovery validation.
Maximum rotor-speed attack	0.135 rad/s	Corrupts rotor-speed feedback used in pitch regulation.
Maximum platform-pitch attack	2.5°	Corrupts floating-platform pitch measurement.
Maximum generated-power attack	0.470 MW	Corrupts the monitored power response.
Platform-rate blending	$\alpha_\theta = 0.25$	Limits the influence of platform-rate compensation uncertainty.

The predictor GRU is trained with FOWT operation data not contaminated by attacks. In the online test, the weights of the GRU remain constant and the predictor produces a safe estimation of the measurement $\hat{\mathbf{y}}_k$ based on the measurement operational input sequence $\mathbf{Z}_k$. The implementation details of GRU predictor and reliability-gated compensation module are summarized in Table 2.

These reliability gains are evaluated in an offline manner, using non-attacked validation data and then fixed during a secure-control test online. This prevents the use of true attacked-response information in the evaluation and guarantees correction of each sensor channel based on the predictability of the sensors' validation information.

Table 2: GRU training, residual detection, and reliability-gated compensation setup.

Item	Setting	Purpose
Training data source	Non-attacked nonlinear FOWT operation data	Learns safe sensor behaviour without using attacked measurements.
Input sequence	$\mathbf{Z}_k = [\mathbf{z}_{k-L+1}, \ldots, \mathbf{z}_k]$	Provides temporal information to the GRU predictor.
Input feature vector	$[V_{w,k}, F_{w,k}, M_{w,k}, \beta_{c,k}, T_{g,c,k}, \chi_k]^T$	Uses wind, equivalent wave-excitation, command, and operating-region information.
Predicted output vector	$[\hat{\Omega}_{r,k}, \hat{\theta}_{p,k}, \hat{\dot{\theta}}_{p,k}, \hat{P}_{g,k}, \hat{\beta}_k, \hat{T}_{g,k}]^T$	Estimates the non-attacked sensor vector.
Number of output channels	$m = 6$	Matches the monitored measurement vector.
Network type	GRU recurrent predictor with linear output layer	Captures nonlinear temporal dependence in sensor responses.
Training target	Normalized true non-attacked sensor vector	Prevents the predictor from learning corrupted sensor behaviour.
Training loss	Mean-squared prediction error	Optimizes safe sensor prediction accuracy.
Online update	GRU weights fixed after offline training	Prevents online adaptation to corrupted attack data.
Residual signal	$\boldsymbol{\rho}_k = \mathbf{y}_k^a - \hat{\mathbf{y}}_k$	Measures deviation between received and predicted measurements.
Detection index	$D_k = \left\|\mathbf{S}^{-1}\boldsymbol{\rho}_k\right\|_2$	Detects attacks using normalized multi-channel residual magnitude.
Detection threshold	$\rho_{\mathrm{th}} = \mu_D + \kappa_D \sigma_D$	Obtained from non-attacked validation residual statistics.
Reliability gain	$g_i = (1 + \epsilon_i/(s_i + \epsilon_s))^{-1}$	Assigns stronger correction to more reliable prediction channels.
Reliability matrix	$\mathbf{G} = \mathrm{diag}(g_1, \ldots, g_m)$	Implements channel-wise reliability-gated compensation.
Compensation law	Eq. (22)	Blends attacked measurements and GRU predictions during detected attacks.

5.2. Compared Cases and Robustness Settings

Four cases are considered. When there is no attack, the measurement vector $\mathbf{y}_k$ is sent to the controller and no attack is applied. The unprotected attacked case is when the FDI attack is applied and the controller receives $\mathbf{y}_k^a$ directly. For the protected case, the proposed residual-detection and reliability-gated GRU compensation module provides $\mathbf{y}_k^c$ to the controller. During detected attacks, the received measurement is completely replaced by GRU prediction in the no-gate ablation case:

$$\mathbf{y}_k^{c,\mathrm{NG}} = (1 - \delta_k)\, \mathbf{y}_k^a + \delta_k \hat{\mathbf{y}}_k. \tag{52}$$

Table 3: Attack and noise scaling factors used in robustness validation.

Scenario	**Attack scale** γ_a	**Noise scale** γ_n
1	0.5	0.0
2	0.5	0.5
3	0.5	1.0
4	1.0	0.0
5	1.0	0.5
6	1.0	1.0
7	1.5	0.0
8	1.5	0.5
9	1.5	1.0

The no-gate case is for checking if there is a need for channel-wise reliability gating for balancing rotor speed/power correction and platform motion preservation.

The main FDI attack is repeated for robustness validation in a variety of attack and noise levels:

$$\mathbf{y}_k^a = \mathbf{y}_k + \alpha_k \gamma_a \mathbf{a}_k + \gamma_n \boldsymbol{\nu}_k, \tag{53}$$

The measurement-noise scaling factor and the measurement-noise vector are γ_n and $\boldsymbol{\nu}_k$, respectively. The robustness scenarios evaluated are summarized in Table 8.

5.3. Evaluation Metrics

The RMSE is used to evaluate sensor-level recovery and closed-loop performance:

$$\mathrm{RMSE}(q) = \sqrt{\frac{1}{N_e} \sum_{k \in \mathcal{K}_e} \left(q_k - q_k^{\mathrm{ref}}\right)^2}, \tag{54}$$

where $\mathcal{K}_e$ is the evaluation index set and N_e is the number of evaluated samples. The percentage RMSE reduction is computed as

$$\mathrm{Reduction} = \frac{\mathrm{RMSE}_{\mathrm{unprotected}} - \mathrm{RMSE}_{\mathrm{protected}}}{\mathrm{RMSE}_{\mathrm{unprotected}}} \times 100\%. \tag{55}$$

In the case of sensor level evaluation, the attacked and compensated measurements are compared to the true non-attacked measurements. When using closed loop evaluation, the unprotected and protected responses are compared to the closed loop response in the absence of attack.

The detection accuracy is calculated as

$$\mathrm{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%, \tag{56}$$

In which TP is the number of true positives, TN the number of true negatives, FP the number of false

positives, and FN the number of false negatives. The reported results are the RMSE reduction at the sensor level, the RMSE reduction in the closed loop, the detection accuracy, the robustness performance, and the comparison of the ablation at the no-gate position.

6. Results and Discussion

The results of the simulation of the proposed secure control framework based on reliability gating has been presented in this section. The results are presented in seven parts. The baseline nonlinear FOWT response is first evaluated to check the model behaviour for control purposes. Second, the effect of false-data injection attacks on key measurement channels is analysed. Third, the performance of the GRU prediction and reliability-gated compensation for the sensor level is presented. Fourth, the closed-loop secure-control performance is compared with nominal and unprotected attacked cases. Fifth, robustness with various attack and noise levels is tested. Sixth, an ablation study is performed to study the role of the reliability gate. Finally, the main drawbacks of the present validation are discussed.

6.1. Baseline Nonlinear FOWT Response

Cyber-attack and cyber-protection simulations were performed for the nonlinear control-oriented FOWT model, with the nominal (unattacked) case simulated first to establish a nominal reference response for the attacked case later. The baseline simulation serves to double check the turbine behaviour of the reduced-order model is bounded under the chosen wind–wave excitation and the controller is working in the desired above-rated regime. Under this operating mode, the generator torque is approximately equal to the rated value and the collective blade pitch controls the rotor speed and the power production.

Figure 4 presents the baseline nonlinear response. Due to the presence of aerodynamic and platform-coupled disturbances, a bounded operating envelope, and oscillations around the rated value of the rotor speed trajectory is seen. The platform-pitch response is also bounded, implying that the platform-pitch motion is dynamically coupled with the turbine response but does not cause the instability. The blade-pitch actuator follows the commanded pitch signal and the generator torque stays almost constant at the rated torque level. The generated power fluctuates around the rated power due to wind speed variation and rotor speed oscillation and the operating-region indicator confirms that the turbine operates in Region III throughout the plotted baseline interval.

The following is a summary of the main baseline operating metrics, see Table 4. The rotor speed varies from 1.139956 rad/s to 1.448160 rad/s, while the maximum platform pitch reaches 12.244594°. The operating fraction for Region III is 1.0000 and the generated power is mean 5.086613 MW. The values show that the simulation setting is at rated power and is appropriate for an analysis of the impact of the false data injection attack at the sensor level on rotor-speed and power regulation.

This reference response is taken as a baseline and is used as a nominal reference response for the rest of the results. In the next phase, false-data injection attacks are added to the selected feedback channels

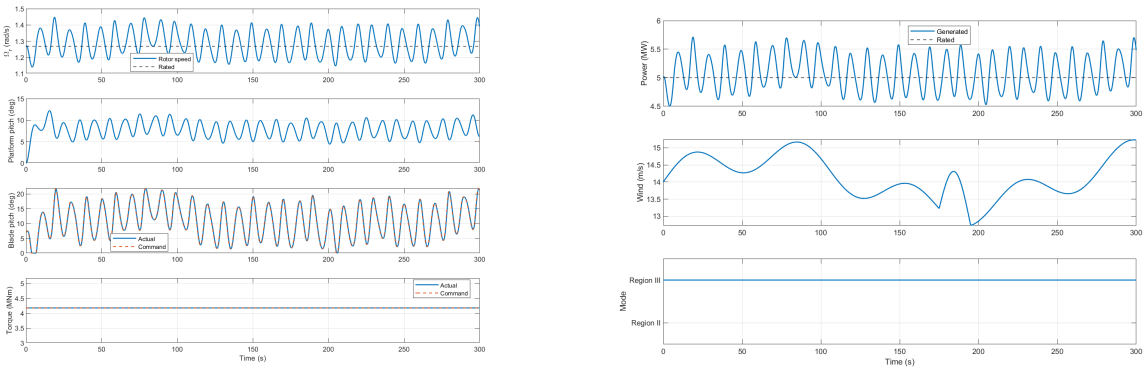


Fig. 4: Baseline nonlinear FOWT response under above-rated operation before introducing false-data injection attacks. The response confirms bounded rotor-speed, platform-motion, actuator, generated-power, and Region III operating behaviour.

Table 4: Baseline nonlinear FOWT operating metrics.

Metric	**Value**
Minimum rotor speed	1.139956 rad/s
Maximum rotor speed	1.448160 rad/s
Maximum platform pitch	12.244594°
Mean generated power	5.086613 MW
Region III operating fraction	1.0000

and the feedback response that has been attacked is compared with this nominal reference to measure the degradation of the feedback response due to falsified measurements.

6.2. Effect of False-Data Injection Attacks

The baseline response was set nominally and then false data was injected into selected sensor feedback channels for the period.

$$\mathcal{T}_a = [120, 210] \text{ s}. \tag{57}$$

The measurement vector received during this time period was generated as

$$\mathbf{y}_k^a = \mathbf{y}_k + \alpha_k \mathbf{a}_k, \tag{58}$$

In which $\mathbf{y}_k$ is the vector of true measurements without attacked data, $\mathbf{a}_k$ is the vector of data injected by the attacker, and α_k is a binary variable that indicates whether the attacked data is present in the measurements.

The attack channels that are dominant are rotor speed, platform pitch and generated power. The maximum injected biases are given in Table 5 for the corresponding configuration. Rotor-Speed bias is

Table 5: FDI attack configuration used in the main simulation scenario.

Attacked channel	Maximum injected bias	Unit
Rotor speed, $a_{\Omega,k}$	0.135	rad/s
Platform pitch, $a_{\theta,k}$	2.5	degree
Generated power, $a_{P,k}$	0.470	MW

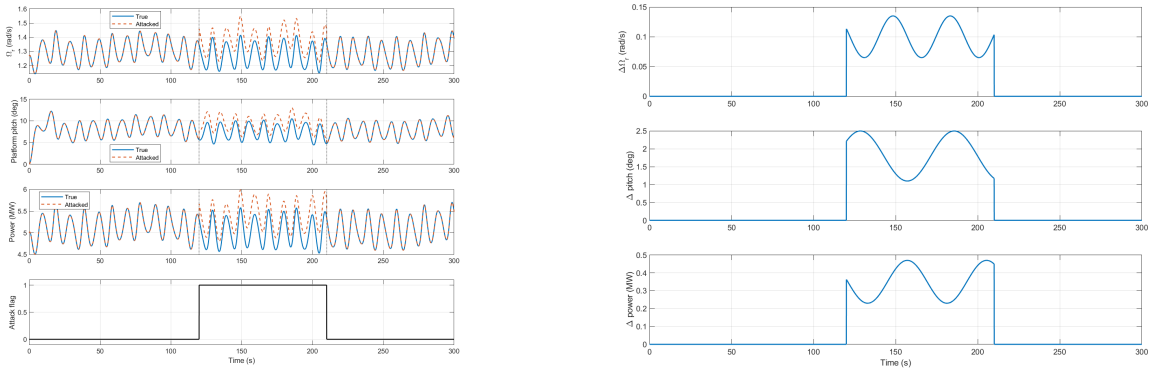


Fig. 5: FDI attack scenario applied to the FOWT sensor feedback channels. The attack is activated during 120–210 s and corrupts the rotor-speed, platform-pitch, and generated-power measurements.

important since the rotor-speed feedback is directly used in region III pitch control. The platform-pitch bias introduces errors into the measured floating-platform motion, and the generated-power bias introduces errors into the electrical response of the turbine. As a result the rotor-speed and platform-motion attacks are mainly related to feedback-dependent control behaviour, while the generated-power attack has a primary impact on monitoring, performance assessment and compensation evaluation. Combined, these attacks result in a cyber-physical mis-match between the actual turbine response and the available signal vector in the secure-control framework.

Figure 5 shows the resulting attacked sensor signals and the injected attack profiles. In Fig. 5a, the attacked measurements deviate from the true measurements only during the activated attack interval. Outside this interval, the attacked and true signals coincide because $\alpha_k = 0$. Figure 5b confirms that the injected biases are bounded and time-localized, with nonzero attack components applied to the rotor-speed, platform-pitch, and generated-power channels.

The separation of the true signal and the attacked signal shows that the controller can receive a feedback that is physically inconsistent to the actual state of the turbine. This is particularly true for the rotor-speed and generated-power channels, which are closely related to the rated-speed regulation and the power-performance assessment. Thus the secure-control framework needs to serve two purposes: (1) identify the attack interval and (2) obtain a reliable compensated measurement vector for subsequent safe controller operation during a corrupted feedback attack.

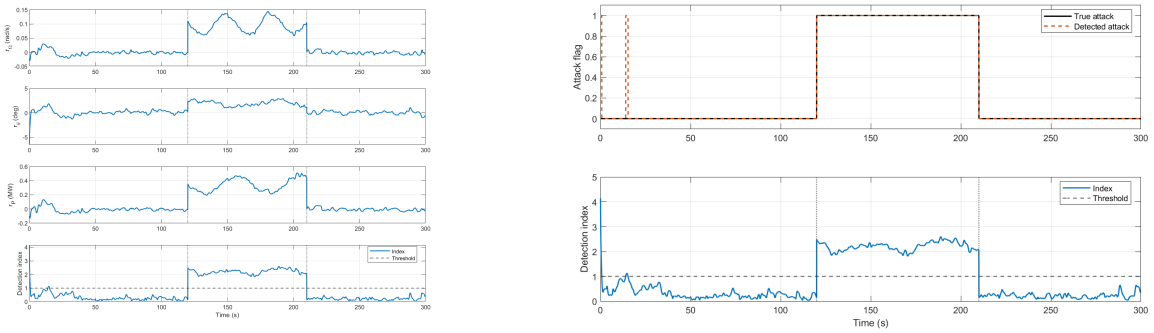


Fig. 6: Residual-based FDI attack detection using the GRU-predicted safe sensor vector. The detection index increases during the attack interval, and the resulting binary detection flag closely follows the true attack activation signal.

6.3. Sensor-Level GRU Prediction and Reliability-Gated Compensation

The non-attacked operation data of the turbines was used for training the GRU predictor, and then the safe sensor vector was estimated during the attacked operation, using the trained GRU predictor online. The residual detector performed the comparison of received attacked measurement vector $\mathbf{y}_k^a$ with the GRU-predicted safe vector $\hat{\mathbf{y}}_k$ at every sampling time. The residual signal was calculated as

$$\boldsymbol{\rho}_k = \mathbf{y}_k^a - \hat{\mathbf{y}}_k, \tag{59}$$

The binary attack decision δ_k was determined by using and the corresponding normalized detection index.

Figure 6 shows the detection behaviour obtained from the residual-based detector. The detected detection index distinctly rises in the FDI interval and the detected attack flag is very close to the true attack-activation signal. This is the case because the prediction error of the GRU is not large enough to cause problems in normal operation, but the injected attack causes a large enough prediction error to leave a residual in the corrupted interval.

In case of an attack, the corrected measurement vector $\mathbf{y}_k^c$ is created by the reliability-gated compensation law:

$$\mathbf{y}_k^c = (1 - \delta_k)\, \mathbf{y}_k^a + \delta_k \left[(\mathbf{I}_m - \mathbf{G})\, \mathbf{y}_k^a + \mathbf{G}\hat{\mathbf{y}}_k \right], \tag{60}$$

where δ_k is the attack decision and $\mathbf{G}$ is the channel-wise reliability matrix. This formulation does not require a direct full replacement of all damaged channels with the neural prediction. Rather, each channel has been corrected based upon its validation reliability.

The results of GRU prediction and compensation are shown in Figure 7. The GRU-predicted trajectories are in accordance with the major non-attacked sensor trends, particularly those of rotor speed and generated power. In the attack interval, the compensated measurements bring the corrupted signals around to be closer to corresponding true measurements. The corrections are greatest for rotor speed and generated power, and

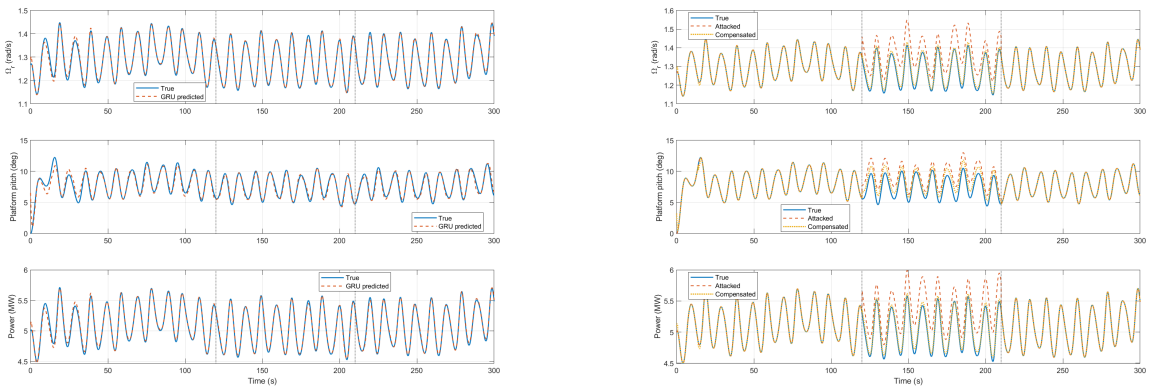


Fig. 7: GRU-based safe sensor prediction and reliability-gated compensation. The predictor estimates non-attacked sensor behaviour, while the compensated measurements move the corrupted feedback signals closer to the true turbine response during the FDI attack interval.

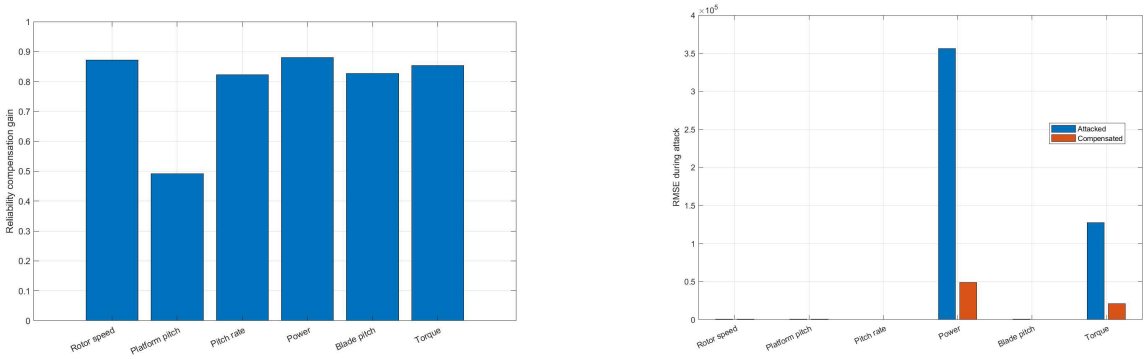


Fig. 8: Reliability-gated sensor compensation performance. The reliability gains limit the influence of weaker prediction channels, while the RMSE comparison confirms substantial sensor-level improvement for the attacked feedback signals.

less but positive for platform pitch. The behaviour is expected, as the effects of wave excitation and nonlinear floating-body dynamics are more pronounced in the case of the platform motion and it is more difficult to predict than the rotor-speed and the power signals.

The reliability-gain design and the corresponding sensor-level error reduction is depicted in Fig. 8. The reliability gains are used for strengthening the correction for channels which had better predictions by the GRU and weakening the correction for channels in which the prediction uncertainty was higher. This is important for closed-loop use, as an off-target neural replacement will result in extra feedback error even if an attack is detected.

Table 6 shows a summary of the sensor-level reduction in RMSE for the reliability-gated GRU compensation. The overall RMSE reduction at the sensor level is 85.95% with the proposed method. The RMSE for

Table 6: Sensor-level RMSE reduction using reliability-gated GRU compensation.

Signal	**RMSE reduction**
Rotor speed	85.71%
Platform pitch	50.01%
Generated power	86.33%
Total sensor-level reduction	85.95%

rotor-speed at the channel level is decreased by 85.71%, the RMSE for platform-pitch at the channel level is decreased by 50.01% and the RMSE for generated-power at the channel level is decreased by 86.33%.

The obtained results show that the GRU predictor gives some useful safe measurements for attacked feedback channels. But the climb rate in compensation improvement for platform pitch confirms that the quality of prediction is not the same for all channels of the sensor. Thus, it is important to have a reliability gate to ensure that the attack rejection robustness is taken into account with the prediction uncertainty before feeding the corrected measurement vector into the closed-loop controller.

6.4. Closed-Loop Secure Control Performance

The proposed reliability based compensation module was then subsequently added to the closed-loop FOWT controller. The comparison was done for three cases: nominal (no attack), unprotected (attacked), and protected (reliability-gated GRU compensation). The controller was given the true measurement vector $\mathbf{y}_k$ in the nominal case. Attacked case: In the unprotected case, the corrupted measurement vector $\mathbf{y}_k^a$ was directly sent to the controller. In the protected case, the compensated measurement vector $\mathbf{y}_k^c$ was obtained from the proposed detection and compensation method.

The compensated rotor-speed signal was relied upon to update the filtered rotor-speed feedback and to compute the protected speed-regulation error to ensure secure Region III operation:

$$e_{\Omega,k}^c = \Omega_{f,k}^c - \Omega_{\text{rated}}. \tag{61}$$

Then the protected blade pitch command was calculated as

$$\beta_{c,k}^s = \beta_0 + K_{p,\beta} e_{\Omega,k}^c + K_{i,\beta} I_{\Omega,k}^c + K_\theta \alpha_\theta \dot{\theta}_{p,k}^c, \tag{62}$$

The platform rate blending coefficient, α_θ, is 0.25, which is a conservative value. This coefficient restricts the effect of the platform-rate prediction error on the pitch-control loop without losing the effect of the platform-motion information on the secure control command.

Figure 9 displays the closed-loop secure-control response during the main FDI attack scenario. As seen in Fig. 9a, the unprotected attacked case exhibits some deviation from the nominal trajectory for the attack interval while the protected response more closely tracks the nominal trajectory. The same pattern is observed in the response when the measurement vector is corrupted by the generated power in

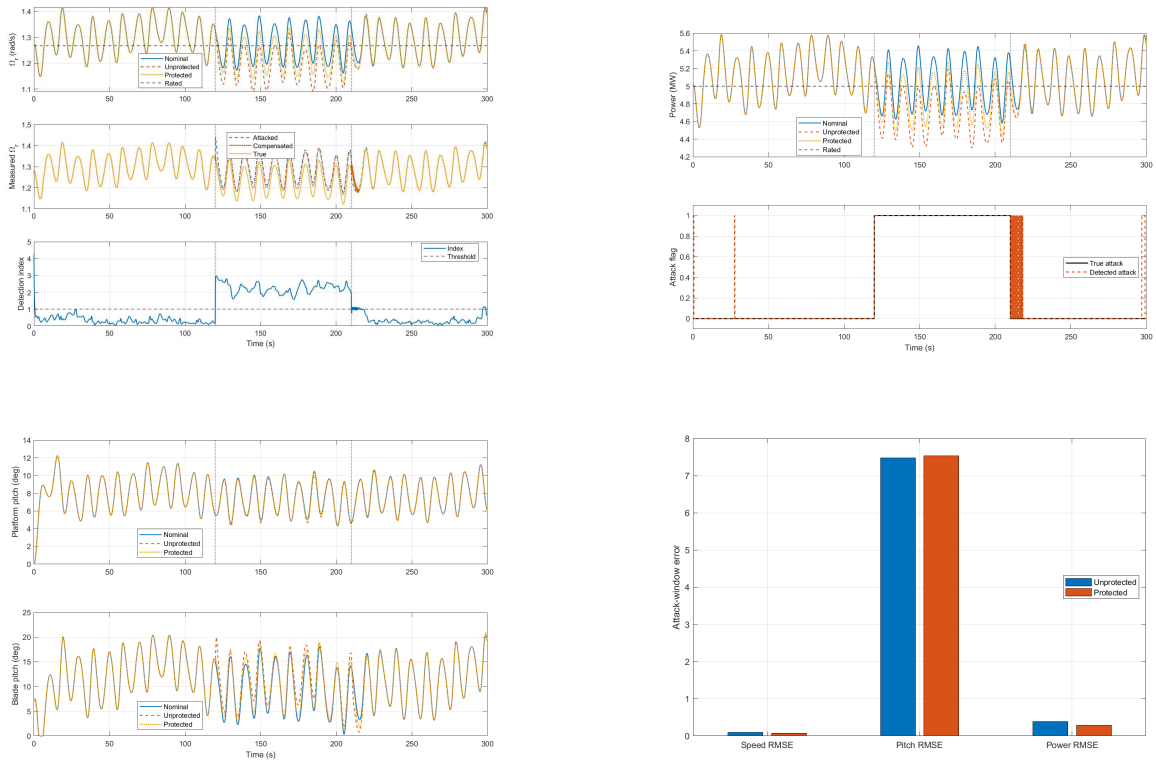


Fig. 9: Closed-loop secure-control performance under FDI attack. The proposed reliability-gated GRU compensation improves rotor-speed and generated-power regulation relative to the unprotected attacked case while maintaining a conservative platform-pitch response.

Fig. 9b, verifying that correcting the corrupted measurement vector yields an improved apparent rated-power response and closed-loop behaviour with regard to rotor-speed regulation. As illustrated in the same figure, the detection signal is being detected during the attacked interval, thereby confirming that the compensation layer is activated during the attacked interval. As seen in Figure 9c, the platform-pitch and blade-pitch responses are kept bounded when operating under protection. The closed loop error comparison in Fig. 9d also shows that the proposed secure compensation layer has the ability to reduce the dominating rotor-speed and power regulation errors compared to unprotected attacked case.

The quantitative closed-loop metrics are summarized in Table 7: For the detection module based on residuals, it has an accuracy of 97.27%, meaning that most of the attacked samples were correctly detected. The method proposed in this paper improved the RMSE of the rotor speed and the RMSE of the generated power compared to the unprotected attacked case by 26.96% and 26.96% respectively. The compensated feedback shows that the attack on the FDI decreases the primary rated operation outputs, which confirms that the compensated feedback improves these two outputs.

The platform-pitch RMSE reduction is around -0.86%. This value should be taken with a pinch of salt. It is not a sign of platform instability or of unsafe platform behaviour. Rather, it is the protected

Table 7: Closed-loop secure-control performance under the main FDI attack scenario.

Metric	Value
Detection accuracy	97.27%
Rotor-speed RMSE reduction	26.96%
Generated-power RMSE reduction	26.96%
Platform-pitch RMSE reduction	$\approx -0.86\%$

platform-pitch RMSE that is slightly larger than the unprotected attacked case in this specific metric. The platform-pitch response is bounded and the conservative blending coefficient will not allow using the weaker channel for platform motion prediction. So, the primary closed-loop advantage of the proposed method is the regulation of the rotor speed, generated power and the platform-pitch response is almost maintained.

Closed-loop results indicate that the ultimate goal is not a measurement that is compensated at the sensor, but a measurement that will improve the response of the controlled turbine. The proposed reliability-gated GRU framework meets this criterion by mitigating the degradation caused by attacks in the rotor-speed and power channels while maintaining the accuracy of platform-motion feedback channels, which are less sensitive to attack and hence are less prone to needing excessive neural correction.

6.5. Robustness Validation

The robust control was tested in the secure control framework with various levels of attacks and noise. For each case of robustness, the attacked measurement vector was chosen as

$$\mathbf{y}_k^a = \mathbf{y}_k + \alpha_k \gamma_a \mathbf{a}_k + \gamma_n \boldsymbol{\nu}_k, \tag{63}$$

where γ_a is the attack scaling factor, γ_n is the measurement-noise factor, and $\boldsymbol{\nu}_k$ is a measurement-noise vector. This formulation assesses the effectiveness of the proposed secure-control framework when the size of the attack is different from the main FDI scenario, or when the noise is different from the main FDI scenario.

Figure 10 summarizes the robustness results. The residual-based detector's detection accuracy is high regardless of perturbation cases, as illustrated in Fig. 10a. The related closed-loop RMSE reductions of rotor speed, generated power and platform pitch are illustrated in figure 10b. Under the attack and noise conditions considered, the reduction in rotor speed and generated power are still positive, and thus it is concluded that the controller under protection still decreases the major cyber-induced performance degradation.

The robustness validation is done for the nine attack–noise combinations given in Table 8. The attack scaling factor γ_a scales the injected FDI attack magnitude and the noise scaling factor γ_n scales the magnitude of the measurement-noise. The main nominal attack magnitude, without extra measurement noise scaling is scenario 4.

The average detection accuracy was 95.07% for all cases of robustness tested. The mean RMSE reduction for the rotor-speed was 24.10% and the mean RMSE reduction for the generated-power was 24.10%. The

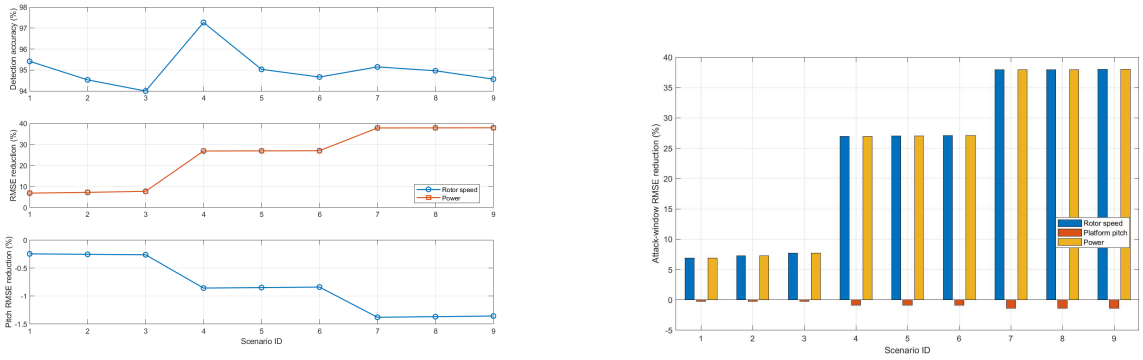


Fig. 10: Robustness validation of the proposed secure-control framework under varying attack and measurement-noise levels. The proposed method maintains useful detection accuracy and positive rotor-speed and generated-power RMSE reduction across perturbed scenarios.

Table 8: Attack and noise scaling factors used in the robustness validation.

Scenario ID	**Attack scale γ_a**	**Noise scale γ_n**
1	0.5	0.0
2	0.5	0.5
3	0.5	1.0
4	1.0	0.0
5	1.0	0.5
6	1.0	1.0
7	1.5	0.0
8	1.5	0.5
9	1.5	1.0

Table 9: Mean robustness performance under different attack and noise levels.

Metric	**Mean value**
Detection accuracy	95.07%
Rotor-speed RMSE reduction	24.10%
Generated-power RMSE reduction	24.10%
Platform-pitch RMSE reduction	$\approx -0.82\%$

mean difference in the RMSE reduction from the platform-pitch was around -0.82%. The above values are concisely presented in Table 9.

The robustness results demonstrate that the suggested technique does not depend on a specific attack magnitude and a specific measurement-noise condition. The average performance is slightly lower than that achieved in the main attack scenario, but the protected controller enhances rotor-speed and generated-power regulation compared to the scenario with the controller being attacked. The response at the platform-pitch is close to the same value, consistent with the conservative design of the platform-pitch based on reliability

gating. The proposed structure should therefore be understood as a safe sensor-compensation and rotor-speed/power-control technique, but not as a platform-load-reduction controller.

6.6. Ablation Study: Effect of Reliability Gating

An ablation study was performed to assess the contribution of the reliability gate in the proposed secure-control framework. The reliability-gated GRU compensation was compared with a no-gate GRU compensation strategy. For the no-gate case, the attacked measurement was completely replaced by the GRU prediction when an attack was detected:

$$\mathbf{y}_k^{c,\mathrm{NG}} = (1 - \delta_k)\, \mathbf{y}_k^a + \delta_k \hat{\mathbf{y}}_k. \tag{64}$$

On the other hand, the proposed reliability-gated method employs

$$\mathbf{y}_k^c = (1 - \delta_k)\, \mathbf{y}_k^a + \delta_k \left[(\mathbf{I}_m - \mathbf{G})\, \mathbf{y}_k^a + \mathbf{G}\hat{\mathbf{y}}_k \right]. \tag{65}$$

The difference between Eq. (64) and Eq. (65) is important for closed-loop operation. The no-gate method uses the entire neural replacement, while the proposed method uses the attacked measurement and GRU prediction with a factor that is determined by the channel-wise reliability matrix $\mathbf{G}$.

Figure 11 shows the closed loop compensation results between no-gate and reliability-gated compensation approaches. Figs. 11a and 11b illustrate the rotor speed response for both the GRU-based strategies versus the unprotected attacked case, demonstrating that both strategies reduce the deviation from the original signal due to the attack. As can be seen from the power response of Fig. 11b, neural compensation results in a more robust control of power during the attack interval. When prediction reliability is less (as is the case in Fig. 11c), however, direct full replacement can lead to more pronounced deviations in the behaviour of the platform-pitch axis. This trade-off is summarized in the RMSE comparison in Fig. 11d: The no-gate strategy may be more aggressive in terms of rotor-speed and power correction, while the reliability-gated strategy offers a more conservative, more balanced closed-loop response.

The results of the ablation demonstrate that replacement of all neural tissue is not necessarily the best closed-loop option. The no-gate GRU can yield more powerful speed and power correction, but also leads to the risk of prediction-error-driven feedback in weaker channels. This effect is most applicable to the variables related to platform motion as platform pitch is highly influenced by wave excitation and nonlinear floating-body dynamics. As such, the reliability-gated approach deliberately does not apply the same amount of correction to every channel that is measured.

Table 10 summarizes the qualitative conclusion of the ablation study. The no-gate GRU strategy is more aggressive since it completely replaces the attacked feedback with the predicted feedback at the time of detection of attacks. The proposed reliability-gated approach is more conservative since the compensation strength is modulated based on the prediction reliability of channels.

This is confirmation of the primary goal of the proposed design (reliability gating). In closed loop control

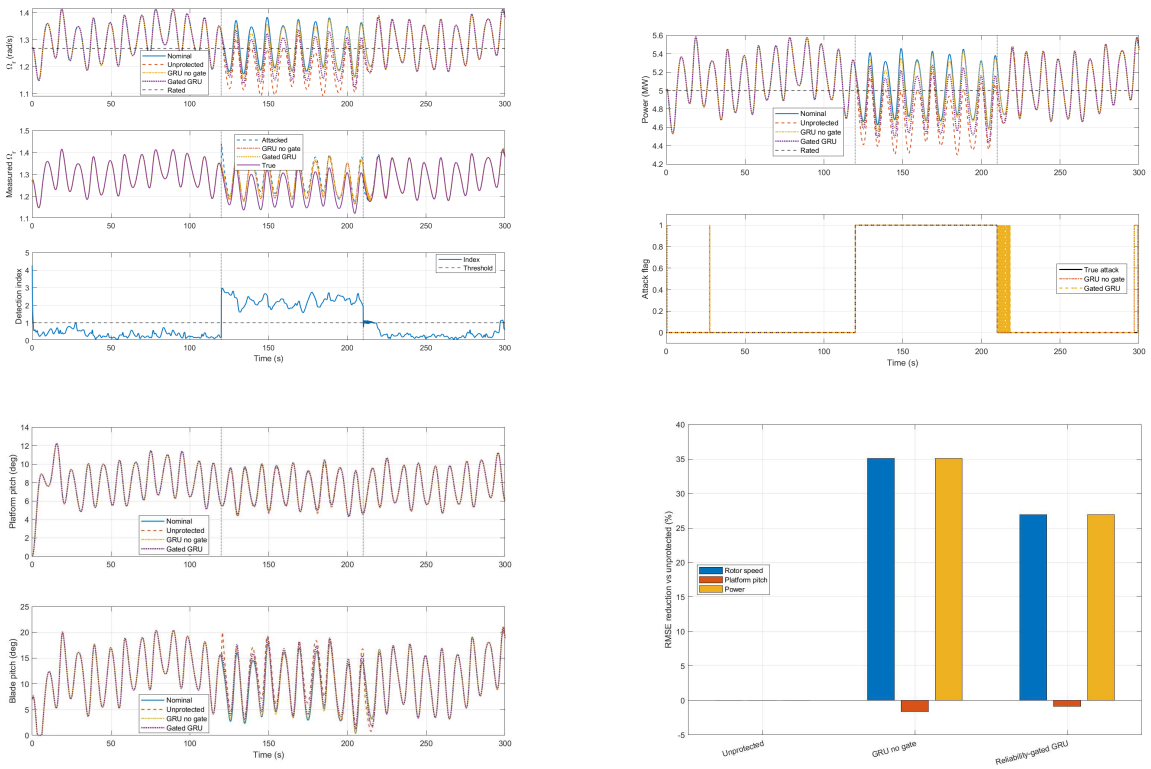


Fig. 11: Ablation study comparing no-gate GRU compensation and reliability-gated GRU compensation. The no-gate strategy gives more aggressive neural replacement, while the proposed reliability-gated method provides a more balanced closed-loop response when prediction reliability differs across channels.

Table 10: Ablation comparison between no-gate GRU and reliability-gated GRU compensation.

Method	**Observed behaviour**
No-gate GRU compensation	Stronger rotor-speed and power correction, but larger risk of platform-pitch degradation due to full replacement of all detected channels.
Reliability-gated GRU compensation	More balanced compensation; improves rotor-speed and power regulation while reducing the negative influence of weak platform-motion prediction channels.

with a secure sensor, the closed loop response may not be the most secure if the sensor level prediction with the best correction is used for all the channels. An effective way to trade off the neural correction with the uncertainty of the prediction of the channel motion, which reduces the rotor-speed and power fluctuation,

without over-reliance on less reliable platform-motion predictions, is the reliability gate.

6.7. Discussion

The full results demonstrate the effectiveness of the proposed reliability-gated GRU secure-control framework at the sensor compensation level and the closed loop control level. The method significantly reduces the attacked vs the true measurement error at the sensor level at 85.95% reduction. The best improvements in the sensor level are for rotor speed and generated power, both of which achieve reductions in RMSE of 85.71% and 86.33% respectively. In addition, platform-pitch sensor error is also reduced by 50.01% (lower than the rotor-speed and power channels due to greater platform motion sensitivity to wave excitation and floating-body dynamics).

At the closed loop level, the framework proposed in this paper enhances the turbine response against FDI attack by providing compensated feedback signals to the secure controller. For the main attack scenario, the reliability-gated GRU compensation decreases the RMSE of rotor-speed and generated-power by 26.96% and 26.96% relative to the unprotected attacked case, respectively. The above reductions attest to the fact that the sensor-level correction is not only numerically effective but also helpful for rated-speed and rated-power regulation in closed-loop. In the main attack case, the detection accuracy of the residual-based detector is 97.27% which suggests that the information in the residual signal from the GRU can provide reliable identification for the attacked interval.

The overall results summary is presented in figure 12. The summary agrees with the four observations made: sensor-level compensation greatly mitigates the corruption of measurements, closed-loop protection enhances the regulation of rotor-speed and generated-power, the ablation study confirms the need for reliability gating, and channel-wise reliability gains offer a practical way to limit the impact of weaker prediction channels.

Finally, the robustness study shows that the proposed framework is not restricted to a particular magnitude of the attack or a particular level of noise. The mean detection accuracy is 95.07% over the evaluated robustness cases and the mean reduction of the RMSE of rotor-speed and generated-power are 24.10% and 24.10% respectively. While these values are slightly lower than what is achieved in the main attack scenario, the results illustrate that the protected controller is still able to deliver useful cyber-resilient regulation when attacked under perturbed attack and measurement-noise conditions.

Another important limitation is shown in the results. The current framework does not directly bring the primary benefit of platform-pitch improvement. The reliability-gated GRU does not significantly lower the platform-pitch sensor error at the measurement level but the platform-pitch error with the closed-loop RMSE is about the same and is slightly decreased in the tested cases. In particular, the platform-pitch RMSE reduction is around -0.86% for the main attack scenario and around -0.82% for the robustness study. This is not closed-loop instability, but rather that the protected platform-pitch response is slightly different than the unprotected attacked response for the selected metric.

The behaviour is physically plausible, as the dynamics of the platform-pitch are determined by coupled

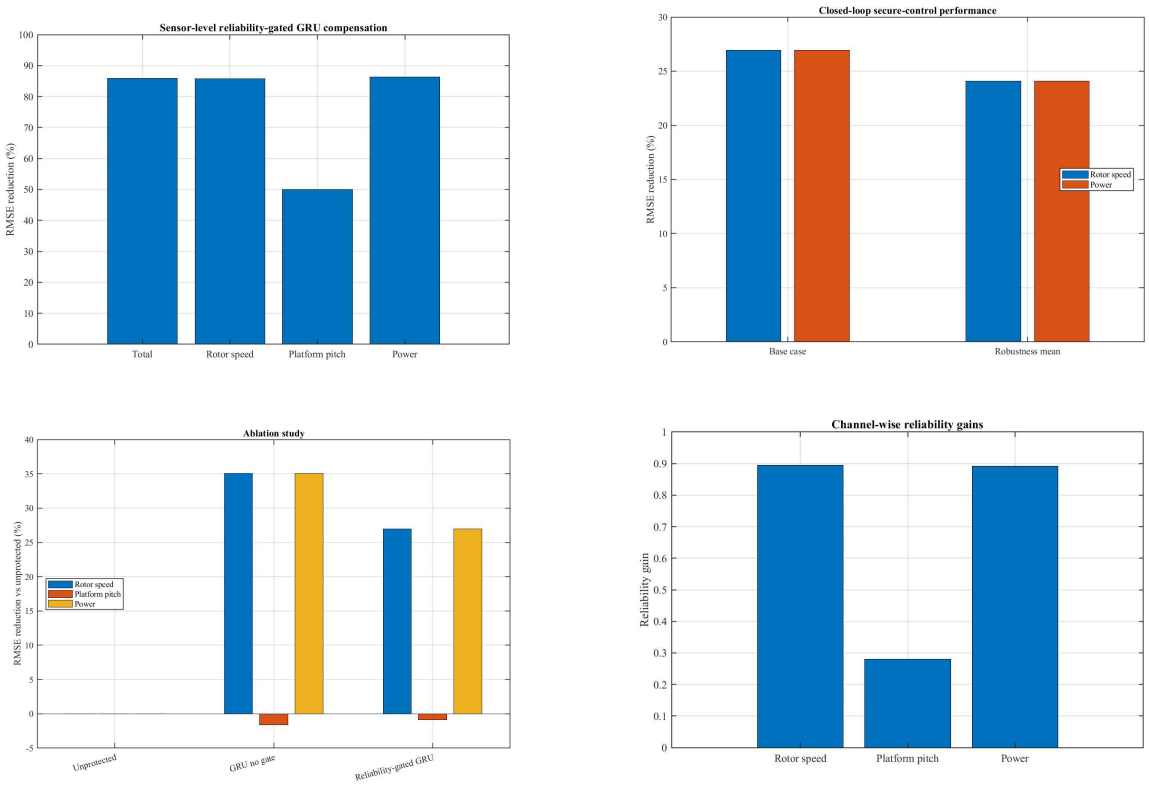


Fig. 12: Graphical summary of the proposed reliability-gated GRU secure-control framework. The results summarize sensor-level compensation, closed-loop secure-control performance, ablation behaviour, and channel-wise reliability-gain design.

aerodynamic thrust and wave-induced excitation, hydrodynamic response, and floating-body motion. These dynamics are less straightforward to accurately reconstruct from the selected operational input sequence than, e.g., the rotor speed or the generated power. As such, the proposed approach is to be considered a sensor-recovery and rotor-speed/power control mechanism, rather than a platform-load-reduction or platform-motion-suppression controller. The reason for the need of reliability gating is clarified by the ablation study. A no-gate GRU compensation strategy completely substitutes the attacked measurements with the neural predictions during attacked periods. This can generate higher correction for channels, which are well predicted, such as rotor speed and generated power. But, replacement is also possible to create prediction error in weaker channels, particularly platform-motion related feedback. The structure proposed here to tackle this problem is the reliability-gated structure, where channel-wise correction gains are assigned. The more reliable the prediction channel, the more it is corrected, and the more conservative the more uncertain prediction channel.

The proposed reliability gated GRU framework offers a practical and feasible compromise between attack rejection and prediction uncertainty. It enables secure reconstruction of feedback; boosts the performance of rotor-speed and generated-power regulation under FDI attacks; provides adequate robustness for different

attack and noise intensities; and reduces the reliance on weak neural prediction channels. These properties can make the method a good front layer of security to the learning-assisted FOWT operation in the floating case, where the bounded sensor attacks are considered.

6.8. Limitations and Future Validation

There are certain limitations in the present study. The FOWT model is a reduced-order nonlinear control-oriented model, inspired by the NREL 5-MW reference turbine. It represents the principle dynamics required for preliminary secure control validation but it is not a complete aero-hydro-servo-elastic model. Second, the proposed approach has not yet been tested on high fidelity tools like OpenFAST, OpenFOAM or experimental FOWT platforms. Third, the current work concentrates on FDI attacks at the sensor side and does not consider currently FDI attacks at the actuator side, communication delay, coordinated multi-channel attacks and wind-farm level cyberattacks.

Another drawback is that the primary benefit that has been shown in the present framework is not platform-pitch load reduction. The reliability-gated GRU does not significantly change the platform-pitch sensor recovery RMSE in closed loop, but it does improve the reliability of the sensor recovery. Hence, the method is more of a sensor-compensation, rotor-speed/power regulation system in a secure manner.

Future work will test the proposed reliability-gated GRU secure-control strategy in a high-fidelity FOWT model, such as OC3-Hywind or OC4-DeepCwind in OpenFAST. Further research should include wind fields and turbulent wind fields, irregular sea states, realistic sensor noise, actuator faults, communication delays, coordinated cyber attacks, and load-based metrics such as tower-base bending moment, blade-root bending moment, platform-pitch fatigue load, and mooring-line tension.

7. Conclusion

This paper presented a reliability-gated GRU-based secure control framework for a control-oriented nonlinear floating offshore wind turbine under false-data injection attacks. The proposed method combines residual-based attack detection, GRU-based safe sensor prediction, channel-wise reliability evaluation, and reliability-gated measurement compensation. The compensated measurements are supplied to the baseline Region II/Region III controller to reduce the influence of corrupted sensor feedback on closed-loop turbine operation.

Simulation results showed that the proposed method effectively improves sensor recovery and closed-loop regulation under multi-channel FDI attacks. At the sensor level, the reliability-gated GRU achieved a total RMSE reduction of 85.95%, with reductions of 85.71% for rotor speed, 50.01% for platform pitch, and 86.33% for generated power. In closed-loop validation, the method achieved 97.27% detection accuracy and reduced rotor-speed and generated-power RMSE by 26.96% compared with the unprotected attacked case. Robustness and ablation studies further confirmed that reliability gating provides a balanced compensation mechanism by improving reliable channels while limiting the negative influence of weak prediction channels. The results demonstrate the potential of reliability-aware learning-based compensation for secure floating

wind turbine control under sensor attacks. Future work will extend the validation to high-fidelity FOWT models, such as OC3-Hywind or OC4-DeepCwind in OpenFAST, and will consider broader wind–wave conditions, communication delays, actuator-side attacks, coordinated cyberattacks, and load-aware secure control objectives.

Data Availability Statement

The data and simulation outputs generated and/or analysed during the current study are available from the corresponding author upon reasonable request. The main numerical results and performance metrics supporting the findings of this study are included in the article.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] K. Cheikh, E. M. Boudi, Multi-objective optimization of federated predictive maintenance under energy, bandwidth, and latency constraints in remote wind farms, Discover Applied Sciences (2026).

[2] H. Ren, Z. Tian, L. Han, S. Meng, Y. Yang, Adaptive pitch control for power stabilization of floating offshore wind turbines, Renewable Energy (2026) 125392.

[3] W. Zhao, J. Wang, W. Huang, M. Zhou, J. Cao, Y. Li, Revealing deep-far offshore wind potential through an integrated resource assessment and priority zoning framework: A case from china's adjacent seas, Applied Energy 413 (2026) 127790.

[4] S. Chilakala, A. Mallepudi, N. Chutturu, Digital twins in action: Real-time monitoring and performance optimization for floating platforms, in: Offshore Technology Conference, OTC, 2026, p. D041S049R007.

[5] H. Xiong, G. Chen, H. Ren, H. Li, Broad-learning-system-based model-free adaptive predictive control for nonlinear mass under dos attacks, IEEE/CAA Journal of Automatica Sinica 12 (2) (2025) 381–393.

[6] R. Das, A. Werth, T. Morris, A convolutional neural network-lstm based physical sensor anomaly detector for interdependent scada controllers, AI, Computer Science and Robotics Technology 4 (2025).

[7] L.-Y. Hao, L.-F. Liu, H. Liu, Data-driven secure control for umvs against false data injection attacks using glu-gru, IEEE Transactions on ReliabilityEarly access/accepted version (2026). doi:10.1109/TR.2026.3702051.

[8] P. Zhu, S. Jin, X. Bu, Z. Hou, C. Yin, Model-free adaptive control for a class of mimo nonlinear cyberphysical systems under false data injection attacks, IEEE Transactions on Control of Network Systems 10 (1) (2023) 467–478.

[9] E. Branlard, J. Jonkman, C. S. D. Brown, J. Zhang, A digital twin solution for floating offshore wind turbines validated using a full-scale prototype, Wind Energy Science 9 (1) (2024) 1–24.

[10] I. E. Taze, M. Hoda, P. Maddaloni, I. Miquelez, S. Eftekhar Azam, A review of digital twinning applications for floating offshore wind turbines: Insights, innovations, and implementation, Energies 18 (13) (2025) 3369.

[11] E. A. OLAJUYIN, P. K. OLULOPE, E. T. FASINA, O. S. ADEOYE, A. M. ADEBIMPE, B. O. OLAJIGA, T. AKINYEDE, Gated recurrent unit (gru)-based predictive model for reliability index prediction and power outages prediction., Annals of the Faculty of Engineering Hunedoara-International Journal of Engineering 24 (1) (2026) 21.

[12] J. Sathyaraj, V. Sankardoss, A comparative study on rnn-lstm-gru ensemble model for short-term wind speed prediction, IEEE Open Journal of the Industrial Electronics Society (2026).

[13] X. Cheng, F. Shi, Y. Liu, X. Liu, L. Huang, Wind turbine blade icing detection: A federated learning approach, Energy 254 (2022) 124441.

[14] F. Papi, A. Bianchini, Technical challenges in floating offshore wind turbine upscaling: A critical analysis based on the nrel 5 mw and iea 15 mw reference turbines, Renewable and Sustainable Energy Reviews 162 (2022) 112489.

[15] B. Xie, Y. Wang, Y. Cai, Z.-L. Ouyang, C. Zhu, G. Tan, H. Sun, Y. Chen, Computational analysis of tandem floating wind turbines under coupled pitch surge motion comparing nrel 5 mw and iea 22 mw, Scientific Reports 15 (1) (2025) 41381.

[16] Y. Zhou, R. Deng, Q. Jiang, H. Liu, S. Zhao, Idat: An impact-driven adaptive threshold for detecting false data injection attacks on wind turbines, IEEE Transactions on Smart Grid (2026).

[17] N. M. Abdi, Deep reinforcement learning based moving target defense for mitigating false data injection attacks in power grids, Master's thesis, Hamad Bin Khalifa University (Qatar) (2024).