Measuring and Enabling Transmission Systems Resiliency With Renewable Wind Energy Systems

Tushar, *Member, IEEE*, Z. Nie, *Student Member, IEEE*, A. Srivastava, *Fellow, IEEE*, and S. Basumallik, *Member, IEEE*

***Abstract*—This paper introduces a resiliency quantification approach for transmission power system, that incorporates a de-centralized Remedial Action Scheme (RAS). RAS is designed to alleviate transmission line overloads under high wind conditions. A resiliency metric is computed to quantify the ability of the system to supply power to critical loads in the presence of RAS. First, a de-centralized RAS is designed to curtail excess wind optimally, in order to limit excess power flow on the transmission lines. Next, the effect of RAS operation on the transmission system is quantified using the proposed resiliency metric. The metric is based on system configuration and real-time measurements and incorporates a graph theory-based approach to quantify the redundancy and vulnerabilities of the transmission network. This makes the metric adaptive and flexible to changing grid conditions. The algorithm is fully implemented and validated on a hardware-in-the-loop testbed consisting of a Real-Time Digital Simulator (RTDS), Phasor Measurement Units (PMUs), and Cisco FOG routers with a real-time distributed computing platform for online implementation. The effectiveness of the proposed approach is validated through offline simulations on the IEEE 39 bus system and real-time simulations on an IEEE 14 bus system considering high wind and cyber attack scenarios.**

***Index Terms*—Cyber attack, cyber-physical systems, distributed computing, hardware-in-the-loop, resiliency metric, wind power.**

I. Introduction

CRITICAL electric power system provides vital support to essential national services such as telecommunications, water, natural gas and oil, banking and finance, transportation, government, and emergency services. However, the growing frequency of weather-related and cyber events poses a significant threat to the power grid, risking damage to infrastructure, triggering outages, and undermining national security. As a result, improving grid resiliency has become crucial to minimize downtime and preserve the stability and security of the power supply. The IEEE PES Task Force describes the key enablers of resiliency against "natural threats, accidents, equipment failures, and deliberate physical or cyber-attacks" to include "the capacity to anticipate, absorb, rapidly recover from, adapt to, and learn from such an event", and defines power system resilience as "*the ability to limit the extent, system impact, and duration of degradation in order to sustain critical services following an extraordinary event* [1]."

This paper focuses on enabling and quantifying the transmission resiliency of the power system with the penetration of wind energy systems. The quantification of transmission system resiliency, unlike distribution systems, has several challenges: (1) transmission networks cover a large geographic area and involve multiple transmission lines and substations, making it more complex to assess the overall resiliency of the system. In contrast, power distribution systems are more localized, making it easier to measure resiliency; (2) transmission networks are usually meshed networks as compared to distribution networks which are mostly radial in nature. These networks have multiple sources of power supply that need to be taken into account while estimating the performance of the system; (3) the mesh nature creates redundancy in the network paths, thus, the shortest path from the source is not a characteristic property of critical/priority load; (4) all transmission-level substations mostly have critical loads, thus, a single metric cannot asses the resiliency of all important loads in a transmission network; (5) resiliency in distribution systems focuses on reducing the duration and extent of power outages, as well as quickly restoring power to customers in case of an outage, while transmission system resiliency focuses on bouncing back from major disruptions to the transmission lines, such as damage from natural disasters or cyber-physical attacks; and (6) the resiliency of the transmission system is not limited to the transmission level alone; it needs to be extended and integrated with the distribution systems as well [2]. To address these challenges, this paper proposes a novel method to quantify the transmission resiliency of both *operational* and *infrastructure* indices, that takes into account not only physical power flows but also network configuration and connectivity redundancy. We define a resilient transmission system as "*a system that has an improved ability to supply critical loads at every transmission-level substation under disruptive events.*" This resiliency is quantified relatively and thus a change in the

Manuscript received 18 April 2023; revised 24 July 2023 and 9 October 2023; accepted 24 October 2023. Date of publication 30 October 2023; date of current version 21 March 2024. Paper 2023-TRPG-0291.R2, approved for publication in the IEEE Transactions on Industry Applications by the Towards Resilient Power Grids Integrated with High-Penetrated Renewable Energy Sources: Challenges, Opportunities, Implementation Strategies, and Future Perspectives of the IEEE Industry Applications Society. *(Corresponding author: A. Srivastava.)*

Tushar and Z. Nie were with the Washington State University, Pullman, WA 99164 USA. They are now with the GE Digital, Bothell, WA 98011 USA (e-mail: tushar.wsu@gmail.com; niezj93@gmail.com).

A. Srivastava was with the Washington State University, Pullman, WA 99164 USA. He is now with the West Virginia University, Morgantown, WV 26506-6201 USA (e-mail: anurag.srivastava@mail.wvu.edu).

S. Basumallik is with the West Virginia University, Morgantown, WV 26506-6201 USA (e-mail: sagnik.basumallik@mail.wvu.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIA.2023.3328572.

Digital Object Identifier 10.1109/TIA.2023.3328572

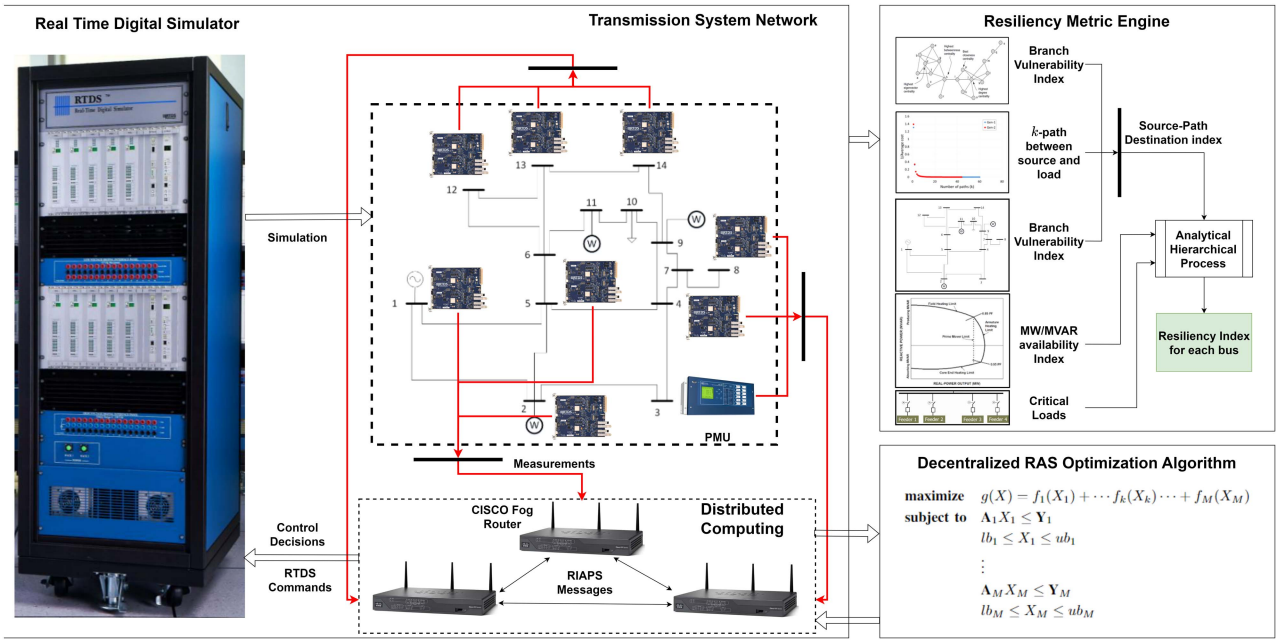


Fig. 1. Overview of the resiliency analysis using decentralized RAS on a real-time hardware-in-the-loop testbed.

resiliency metric is used as an indicator for potential improvements in the existing system.

To improve transmission resiliency under high wind energy systems, this paper employs Remedial Action Schemes (RAS) that detect abnormal events and take prompt corrective actions to arrest failures. The North American Electric Reliability Corporation (NERC) defines RAS as a scheme "designed to detect predetermined system conditions and automatically take corrective actions that may include, but are not limited to, curtailing or tripping generation or other sources, curtailing or tripping load, or reconfiguring a system" [3]. While RAS improves system resiliency, this paper focuses specifically on making the RAS schemes more resilient to maximize their effectiveness. In conventional approaches, a centralized RAS controller collects data, takes control action, and communicates with network nodes. However, if the centralized node fails due to errors or sophisticated attacks, the operational resiliency and reliability are jeopardized. In contrast, each node in a distributed control architecture is a computing entity and the control decisions are based on the communication among every node in the network. The communication requirements in distributed control are extremely high. To address this challenge, this paper develops a decentralized RAS architecture utilizing a convex mathematical optimization approach, that strikes a balance between centralized and distributed systems, and eliminates single-point failures while maintaining a certain level of coordination and consensus among independent nodes at the system level. The proposed algorithm is solved using a distributed simplex approach on a distributed computing algorithm where computational units constantly communicate with each other to adequately distribute the computational load and coordinate to carry out their shared function. The overall architecture is presented in Fig. 1. The main contributions of this paper are,

1) Proposed a decentralized remedial action scheme for wind generation curtailment to enhance transmission resiliency, especially when centralized schemes fail to converge, for example, under cyber attack scenarios.
2) Assessed the effectiveness of the decentralized remedial action scheme using a resiliency metric under high wind conditions for the first time.
3) Validated the proposed method for an online system on a hardware-in-the-loop platform equipped with real phasor measurement units on a distributed computing platform.

The rest of the paper is organized as follows. Section II provides a brief description of resiliency in the context of transmission systems. Section III discusses the drawbacks of centralized and distributed RAS architectures and introduces the proposed decentralized RAS implementation. Section IV quantifies the resiliency metric. Section V presents the results and discussions, followed by the conclusion in Section VI.

II. Resiliency in Transmission Systems

Research efforts in the past have been largely focused on achieving high levels of reliability in the design of complex power systems. These reliability studies focus on the ability to withstand instability, routine maintenance, and unforeseen events during normal operation [4]. Various reliability indices have been developed to assess the performance of power systems [5]. Despite efforts to achieve high reliability in power systems, there have been instances where it was insufficient to prevent failures, particularly in cases of extreme weather events [6]. Research shows that the number of power outages due to natural disasters is on the rise in recent years [7]. The current reliability metrics are not deemed suitable to assess the performance of the power system under such low-probability

TABLE I
ENABLING POWER SYSTEM RESILIENCY

Resiliency Categories	Subcategories
Operational	Threat detection, integrated defense plan, physical system measure, switching (reconfiguration and resource allocation, islanding), network segmentation, DER, and mobile generators
Planning and development	Resource redundancy, power grid network redundancy, network hardening, system hardening (newer transmission lines, underground cables, backup generators), data analytics (centralized, decentralized, distributed), robust cyber-infrastructure (communication network redundancy, communication network management flexibility, communication architecture), automation, flexibility, adaptability
Computational algorithm and control architecture	Control architecture (centralized, local, distributed, decentralized, hierarchical, hybrid), communication architecture (centralized, federated, peer-to-peer), computational algorithm (local, parallel, distributed), robust mathematical algorithm and robust control (distributed optimization, robust convergence and time guarantee, distributed coordination)

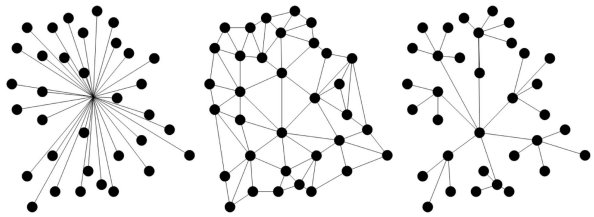
high-impact weather events. Thus, there is a need to shift in focus from preventing failures (reliability) to being able to quickly recover from them (resiliency). A resilient system increases the ability to survive and recover from extreme (low probability, high consequence) events, and fosters flexibility and adaptability while preserving minimum requirements set by the user. For a comprehensive discussion on resilience, we direct the readers to [1], [8].

Several approaches for improving the transmission resiliency under high penetration of wind power have been proposed in the literature. The resiliency is formulated as a transmission line hardening problem in [9] considering uncertain wind power generation and line contingencies. Minimizing load curtailment and cost of operation through generation and renewable energy sources dispatch was suggested in [10]. A resilience index was introduced in [11] considering load priority and wind-affected operational states. Ordered curtailment for large-scale offshore wind power systems under high wind conditions was developed in [12]. Resiliency models considering fragility modeling of components, emergency responses, and restoration can be found in [13], [14], [15].

Table I shows the various approaches towards enabling power system resiliency. *System operational resiliency* plays a central role in safeguarding critical infrastructure. Robust threat detection and an integrated defense plan, merging both cyber and physical security, identify and counter potential risks. Dynamic capabilities such as power system switching, reconfiguration, and controlled islanding ensure localized power supply during emergencies. Network segmentation and network switching compartmentalize the system, minimizing the impact of cyberattacks. Distributed Energy Resources (DER) and mobile generators provide decentralized backup ensuring continuous power supply during emergencies. Resiliency in *system planning and development* ensures longevity and adaptability of critical power grid infrastructure. Resource redundancy ensures that ample backup resources are readily available to mitigate potential shortages while grid network redundancy creates alternative routes for power transmission. Hardening measures include building newer transmission lines, underground cables, and backup generators. While they improve durability, they are usually expensive and may take a longer time. Centralized, decentralized, or distributed data analytics enable real-time monitoring and predictive maintenance. Lastly, a robust cyber-infrastructure with redundant communication networks, flexibility, and automation further safeguards against threats safeguards against advanced threats. Lastly, *computational algorithm and control architecture* enables effective deployment of resilient control strategies. Control architectures include centralized, local, distributed, decentralized, hierarchical, and hybrid models. Various underlying communication infrastructures for seamless data exchange include centralized, federated, and peer-to-peer networks. Computational algorithms, ranging from local and parallel to distributed approaches, optimize system performance. Finally, robust mathematical algorithms and control methods, including distributed optimization, robust convergence with time guarantees, and distributed coordination further enable fast, adaptive response to complex grid resiliency challenges.

This paper focuses on RAS, a coordinated defense mechanism for system operational resiliency, which provides a coordinated and automated response to situations that jeopardize the resiliency for systems with high wind penetrations. RAS detects and takes predetermined steps to correct abnormal system conditions to improve system integrity and performance. They provide automatic control action with a high impact on the system performance, making the operation of the grid more robust and reliable. The general architecture of RAS is shown in [16]. RAS implementation can be grouped into three approaches: (1) event-based, (2) parameter-based, and (3) response-based [17]. Event-based schemes quickly detect outages/faults and trigger actions like generator/load tripping to mitigate system instability. Parameter-based schemes indirectly detect critical events by measuring power, angles, or other variables. On the other hand, response-based RAS are not hard-coded but are adaptive to changing system conditions [18], and hence are usually better, and is the focus of this paper. Typical time bounds for different RAS operations are several seconds for thermal overload, a few hundred milliseconds for voltage instability, and a few tens of milliseconds for transient instability. The control and computation of RAS can either be centralized, distributed, or decentralized as shown in Fig. 2.

Various RAS approaches have been developed in the literature to improve transmission resiliency. The RAS in [19] is designed to prevent voltage instabilities through generation rescheduling/load shedding and utilizing utility-scale solar resources considering the highest impact on volt/var controls. A deep neural network-based RAS was proposed to optimally change loads to avoid triggering under-frequency and over-frequency relays [20]. RAS leveraging sensitivities between generators and overloaded lines improve resiliency under cyber attacks targeting generators [21]. Strategic locations of thyristor-controlled



(a) Centralized (b) Distributed (c) Decentralized

Fig. 2. Control architectures for RAS.

series capacitors RAS are used to alleviate transmission line congestions caused by false data attacks [22]. A cyber resilient RAS was presented in [18]. While situations of faulty leader nodes were analyzed, situations of cyber-attack scenarios or computation of resiliency metrics were not incorporated in [18]. In the authors' previous paper [23], a RAS is developed to minimize the wind generation curtailment and maintain the transmission line flows at the same time. In [23] a RAS is developed to maximize the wind energy integration without compromising the security and reliability of the power system based on specific utility requirements. Further, a distributed linear state estimation was developed to provide fast and accurate input data for RAS. While distributed computation for the purpose of decentralized state estimation and utilization of RAS to reduce the impact of renewable energy source losses were addressed, enhancing the resilience of the transmission system during periods of stress such as excess wind and cyber attacks that compromise the data inputs to the RAS as well as quantifying resiliency metrics have not been addressed in [23]. A list of RAS that has been used in the industry to maintain stability, acceptable voltage limits, line flows, and arrest cascading failures can be found in [24], [25], [26], [27], [28], [29]. However, in general, there is a lack of extensive assessment of the effectiveness of the decentralized remedial action scheme using a resiliency metric under high wind conditions. In the next section, we introduce our proposed decentralized RAS.

III. Proposed Decentralized RAS

The intermittent and uncertain nature of wind power feeding at different nodes of a power grid may cause frequent violations of the ampacity ratings of the transmission lines, affecting stability. This section focuses on a decentralized RAS for optimal wind curtailment to reduce line overloads for systems with high renewable penetration.

A. Drawbacks of Centralized and Distributed RAS

There are multiple design strategies for RAS - centralized, distributed, and decentralized, as shown in Fig. 2. For centralized control shown in Fig. 2(a), a single controller gets the measurement data from all other nodes in the network, takes control action, and communicates the control signal back to the various nodes. However, centralized architecture becomes largely unsuitable when the centralized node fails, threatening the resiliency and reliability of operations. Fig. 2(b) shows the distributed control scheme architecture. Here, every node is a computing entity and the control decisions are based on the communication among every node in the network. As a result, the communication requirements are extremely high.

TABLE II
Comparison Among Various Control Strategies

Features	Centralized	Distributed	De-centralized
Fault Tolerance	Low	High	Medium
Scalability	Low	High	Medium
Ease of Development	Easy	Hard	Medium
Communication Latency	High	Low	Medium
Resilient to single node failures	Low	High	High

B. Decentralized RAS Architecture

Decentralized architecture, as shown in Fig. 2(c), is a middle ground between centralized and distributed systems, where there is no single-point failure, and nodes operate independently while maintaining a certain level of coordination and consensus. Table II summarizes the features of each type of control architecture. Here, the network is divided into various control areas and there is a control center for each control area. The control nodes in each area obtain the measurements, perform the control algorithm and send back the control decisions to the nodes in the corresponding area. Communication exists between the nodes in an area to its corresponding control center, however, there may be no communication among the nodes within an area. Control centers of various areas can communicate with each other for coordination. In this paper, we focus on the decentralized control approach. The architectures used for computational purposes is identical to Fig. 2(c). The algorithm is mathematically distributed among various computing nodes where each node performs a block of computations, giving better algorithmic and mathematical resiliency.

C. Mathematical Formulation

We develop a decentralized, fast, fault-tolerant RAS designed to be implemented in multiple controllers at electric substations connected to decentralized data sources. The proposed RAS logic performs calculations continually in an optimal layout for data delivery and initiating emergency control actions. The proposed RAS is designed to reduce wind energy curtailment to eliminate thermal overloads on the transmission line. The objective function is formulated as [23],

$$f(X) = \sum_{i=1}^{N} x_i P_i^g \tag{1}$$

where N is the total number of installed wind farms in the system, $x_i \in [0, 1]$ is the curtailment variable and corresponds to wind farms $1..N$, and P_i^g is the power generation of the wind farm i. The curtailment is formulated as the reduction in wind power through the summation over the product of x_i and P_g^i for the N wind power plants. To formulate the constraints, we

consider the DC power flow equations where the total generation and load in the system are related as,

$$P = P^g - P^l = \mathbf{B}\Theta \tag{2}$$

where P is a vector of nodal injections, P^l is the vector of loads, Θ is a vector of θ_i and $\mathbf{B}$ is the matrix with line parameters. To incorporate x_i into the formulation, (2) is converted into a standard linear programming format as,

$$\begin{bmatrix} P_g^1 & \cdots & 0 & -P_1^l \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & P_g^N & -P_N^l \\ 0 & \cdots & 0 & -P_{N+1}^l \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & -P_{N+K}^l \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_N \\ x_{N+1} \end{bmatrix} = \mathbf{B}\Theta \Rightarrow \mathbf{P}X = \mathbf{B}\Theta \tag{3}$$

where $\mathbf{P}$ is a $(N+K)\times(N+1)$ matrix, Θ is a $(N+1)\times 1$ vector, and $x_{N+1}=1$. The vector Θ can be written as,

$$\Theta = \mathbf{B}^{-1}\mathbf{P}X \tag{4}$$

The power flow and their dynamic line ratings are,

$$P_{ij} = B_{ij}(\theta_i - \theta_j) \leq P_{ij}^{\max} \tag{5}$$

where P_{ij} is the active power flow between line $i-j$, $P_{ij}^{\max}$ is the dynamic line rating, B_{ij} is the line parameter and θ_i denote the node i voltage phase angle. Here, (5) can be expanded as,

$$\begin{bmatrix} \cdot \\ \cdot \\ P_{ij} \\ \cdot \end{bmatrix} = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & B_{ij} & -B_{ij} & 0 \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} \begin{bmatrix} \cdot \\ \theta_i \\ \theta_j \\ \cdot \end{bmatrix} \leqslant \begin{bmatrix} \cdot \\ \cdot \\ P_{ij}^{\max} \\ \cdot \end{bmatrix} \tag{6}$$

which can be written as,

$$\mathbf{P}_{ij} = \mathbf{T}\Theta \leq \mathbf{P}_{ij}^{\max} \tag{7}$$

Substituting (4) in (7), we get,

$$\mathbf{P}_{ij} = \mathbf{T}\mathbf{B}^{-1}\mathbf{P}X \leq \mathbf{P}_{ij}^{\max} \Rightarrow \mathbf{A}X \leq \mathbf{Y} \tag{8}$$

For implementing distributed RAS with M distributed actors, the objective function is formulated as,

$$g(X) = f_1(X_1) + \cdots f_k(X_k) \cdots + f_M(X_M) \tag{9}$$

where $f_k(X_k)$ is similar to (1). The optimization problem for decentralized RAS is thus formulated as,

$$\begin{aligned} \textbf{maximize} \quad & g(X) = f_1(X_1) + \cdots f_k(X_k) \cdots + f_M(X_M) \\ \textbf{subjectto} \quad & \mathbf{A}_1 X_1 \leq \mathbf{Y}_1 \\ & lb_1 \leq X_1 \leq ub_1 \\ & \vdots \\ & \mathbf{A}_M X_M \leq \mathbf{Y}_M \\ & lb_M \leq X_M \leq ub_M \end{aligned} \tag{10}$$

where $lb_k = 0$ for each x_k corresponding to a wind farm generator P_k^g, otherwise $lb = 1$ for all load, and $ub = 1$.

D. Implementation on Distributed Platform

A distributed simplex method [30] is used to solve the above linear programming problem. The steps to solve the distributed simplex are as follows - (1) all inequality constraints are converted into equality constraints using non-negative slack variables; (2) the entire power system is divided into M groups; (3) a leader is selected from each group which is responsible for message passing and computation (these leaders gather electrical and wind weather data from sensors within the group to estimate the dynamic line rating and monitor the power system states to detect any transmission line overloads); (4) each group leader observes the same objective function in (10), has knowledge of the total number of constraints in the system and maintains only its local simplex tableau. Given that the objective function is shared among all groups, the final row of every simplex tableau is identical; (5) each group leader exchanges its pivot row and corresponding row indicator with other group leaders; (6) the smallest row indicator is determined and this indicator is used to perform the matrix row operation in all the groups; and (7) iterate till all column indicators are non-negative. According to Theorem 3 [30], the distributed simplex reaches the same optimal solution as the centralized approach since the minimum row pivot obtained in step (6) is the same as the row pivot for each iteration in the centralized approach.

The distributed simplex is programmed on the Resilient Information Architecture Platform for Smart Grid (RIAPS) [31] that supports decentralized computations. The RIAPS platform runs the decentralized RAS by spawning two leaders for each group - a primary and a secondary. This RIAPS platform can detect leader node crashes and automatically switch the processing to the backup leader. The computational load is evenly distributed among all computing nodes, and the overall architecture is designed to be fault tolerant.

IV. Quantification of Resiliency

We quantify the resiliency metric on both *operational* and *infrastructure* indices. The evaluation takes into consideration not only physical power flows but also network configuration and connectivity redundancy. Quantitatively, the resiliency metric comprises of four components:

- Source-Path-Destination (SPD) index
- MW availability index
- MVAR availability index
- Loss of load index

Note that these four components are not necessarily the only factors needed to determine the resiliency of transmission systems. This paper focuses only on providing a general framework to assess transmission resiliency. The different components are explained next.

A. Components of Resiliency Metric

Source-Path-Destination (SPD) index: This index is a topological-structure-based index that includes various factors like multiple transmission paths from source to loads, redundancy in generation sources, multi-circuit transmission lines and vulnerability in transmission lines due to repetitive occurrence

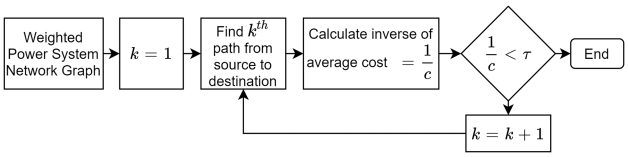


Fig. 3. Flow chart for computation of k-shortest paths.

in all transmission paths. The SPD index is mathematically computed as,

$$\text{SPD index} = \sum_{i=1}^{N_G} \frac{k_i^2}{\text{BVI}_i * \text{HI}_i * (1 + \text{Average cost}_i)} \tag{11}$$

where k_i is the k-number of paths from a source i to a destination, BVI_i is the Branch Vulnerability Index, HI_i is the Hops Index, Average cost_i is computed in terms of electrical distance and N_G is the total number of MW sources. The calculation of k_i, BVI_i and HI_i are described next.

Calculation of k-number of paths from a MW source i to destination substation: One of the major challenges in calculating resiliency is to take into account multiple sources feeding a particular substation. The transmission system is usually a meshed network, thus there exist multiple paths feeding a particular load from various generators. As a result, the shortest path is not a characteristic property in transmission systems. Further, it is computationally very expensive to compute all paths between all generators and a particular substation, thus, k-number of paths are chosen based on the contribution of each path (constituting transmission lines, transformers, etc.) towards the *mean electric distance* between a generator and load substation. Here, the k-shortest paths algorithm [32] is used to calculate the k number of paths between a MW generation source and a destination substation. The determination of k is based on the number of paths that contribute to the average cost between the MW generation source and the destination load substation, considering the impedance of transmission lines as the cost factor c. As the algorithm progresses, it identifies additional paths, and the convergence of the inverse of average impedance to a constant value, less than the tolerance τ, is observed. The process is shown in Fig. 3.

Calculation of Branch Vulnerability Index: The BVI is computed to reflect the vulnerability in the network due to repetitive occurrence of the transmission lines/transformers in the k-number of paths i.e., if a particular transmission line occurs in all k-number of paths between a generator and substation, then this line has a higher impact on the resiliency metric as compared to other transmission lines. This index also takes into account the multi-circuit transmission lines in the system. The BVI is calculated as,

$$\text{BVI}_i = \sum_{N_L} \frac{\frac{n_k}{p}}{k} \tag{12}$$

where n_k is the number of times a branch occurs in k-number of paths between MW source i and the destination substation and p is the number of parallel lines in a multi-circuit transmission line.

Calculation of Hops Index: Hops Index reflects the factor of the number of transmission lines connecting a generator and a substation. The Hops Index for a particular generator to the substation is calculated as follows:

$$\text{HI}_i = \frac{\sum n_{lk}}{k} \tag{13}$$

where n_{lk} is the number of hops (transmission lines, transformer, etc.) in the k^{th} path between MW source i and the destination substation.

MW availability index: This index is based on the physical availability of MW sources for critical loads in the system. This index also takes into account the availability of generator resources. For example, a coal or hydro-based generator has a higher availability factor as compared to intermittent solar or wind-based generation. The MW availability index at a substation is calculated as,

$$\text{MWavailability index} = \sum_{i=1}^{N_G} \frac{\text{MW availability}_i \times \text{Generator Availability}_i}{\text{Total MW load}} \tag{14}$$

where N_G is the total number of MW sources. The 'MW availability' is calculated as the difference between MW capacity and the actual MW used in the system. This value is updated in real-time and is based on the measurements obtained from the SCADA/PMU measurements. The 'Generator availability' (GA) is computed based on the reliability analysis of generators [33]. For instance, a coal-based generator may have a GA of 1.0, whereas, a wind-based generator may have a GA of 0.8 due to uncertainty in wind conditions.

MVAR availability index: This index is based on the ability of the system to regulate the voltage at a substation, such that an acceptable voltage profile is maintained at the downstream sub-transmission and distribution level. Reactive power being a local phenomenon, the power system is first separated into several voltage control areas. This voltage control area is computed based on electric distance (based on Jacobian matrix) combined with a hierarchical classification algorithm [34]. Only those sources of reactive power are considered for a particular load bus that are included in its voltage control area. The MVAR availability index at a substation is computed as,

$$\text{MVAR availability index} = \sum_{N_{RR}} \frac{\text{MVAR availability}}{\text{Total MVAR load}} \tag{15}$$

where N_{RR} is the total number of reactive reserves available in the voltage control area of the substation, 'MVAR availability' is calculated as the difference between the MVAR capacity of the available reactive power reserves and the actual amount of MVAR used in the system. This value is also updated in real-time and is based on the measurements obtained from the SCADA/PMU measurements.

Loss of Load index: The calculation of this index takes into account the proportion of critical loads being supplied relative to the total critical load at each substation. The loss of load index

TABLE III
FUNDAMENTAL SCALE USED FOR PAIRWISE MATRIX IN AHP

Intensity of Importance	Definition
1	j and k are equally important
3	j is slightly more important than k
5	j is more important than k
7	j is strongly more important than k
9	j is absolutely more important than k

is computed as,

$$\text{Loss of load index} = \frac{\text{Actual Critical load supplied}}{\text{Total critical load}} \tag{16}$$

B. Combined Resiliency Metric

The above individual resiliency indices are combined together into a single resiliency index (RI) to quantify the resiliency at each transmission-level load substation. This is formulated as a multi-criteria decision-making problem and is solved using the Analytical Hierarchical Process (AHP) method [35]. The AHP process takes into account the different criteria based on the user's objective where the importance of each criterion can be evaluated based on the application in a systematic manner. The scale of importance used in this paper is shown in Table III. The primary importance is on the Loss of Load index (weight = 0.65), followed by the SPD index (weight = 0.25). The MW availability (weight = 0.05) and MVAR availability (weight = 0.05) indices are given relatively lower priority. The wights are chosen in such a manner that the pairwise AHP matrix has a maximum consistency index of 0.1 under varying operating conditions for consistent quantification of results.

V. SIMULATION RESULTS

This section presents the results of the transmission resiliency analysis with RAS. First, we emphasize the significance of employing the RAS scheme to enhance resiliency under excessive wind generation. To illustrate this, we perform offline simulations on a modified IEEE 39 bus system and online simulations on a modified IEEE 14 bus system. Next, we highlight the advantages of utilizing a decentralized RAS approach during online simulations, specifically in the context of a false data injection cyber attack that manipulates measurement values. The effectiveness of the decentralized RAS is demonstrated by its ability to successfully converge, in contrast to the centralized RAS which fails to do so under attack scenarios. The online scenario is run in the RTDS with a real SEL hardware PMU and multiple firmware PMUs. Cisco Fog Routers are used to implement the controller and multiple Fog Virtual Machines (VMs) are used to run the distributed simplex on the RIAPS. All simulations are performed in MATLAB.

A. Offline Analysis

System Setup: A modified IEEE 39 bus system, shown in Fig. 4, is used to evaluate the resiliency for offline analysis. There

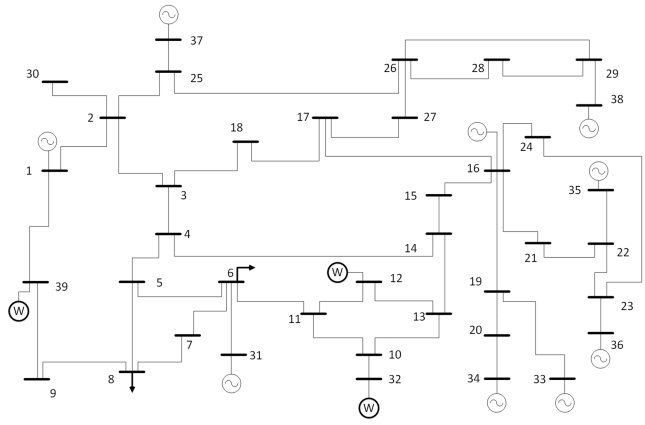


Fig. 4. Modified IEEE 39 bus system with wind generation at buses 12, 32, and 39 and critical loads at buses 6 and 8.

TABLE IV
IEEE 39 BUS WIND GENERATION FOR VARIOUS SCENARIOS

Scenario	Bus 12 (MW)	Bus 32 (MW)	Bus 39 (MW)
Base case	100	650	1000
Excess wind before RAS	200	800	1000
Wind generation after RAS	101.36	800	1000

are three wind generators at buses 12, 32, and 39 with 100 MW, 650 MW, and 1000 MW generation respectively. Further, critical loads are designated at buses 6 and 8. Bus 6 has 80 MW and 20 MVAR and bus 8 has 600 MW and 200 MVAR of load. For this paper, ensuring that critical loads are supplied during disruptive events is of utmost importance from the point of resiliency. Consider the two critical lines: $6-11$ and $13-14$ having a maximum rating of 400 MW and 500 MW respectively. During normal operating conditions (base case), the amount of MW loading on line $6-11$ and $13-14$ are 250 MW and 340 MW respectively.

Loss of resiliency analysis under excess wind conditions: During excessive wind conditions, the amount of wind generation at bus 12 and bus 32 increases to 200 MW and 800 MW respectively. This leads to the overloading of line $6-11$, violating steady-state security protocols and resulting in the tripping of the line. Subsequently, line $13-14$ becomes overloaded and trips. Consequently, a section of the system becomes isolated, causing a divergence in the power flow solution for the remaining portion. In the absence of a resiliency approach, a portion of the critical load on the bus 8 is shed in order to maintain the steady-state stability of the system. This results in a reduction in the system's overall resiliency. This is observed as the resiliency index RI reduces from 1 to 0.874 in Table V and reduces from 1 to 0.715 in Table VI. The loss of critical loads and the resulting prolonged service interruptions amplify the economic and social consequences of the power system, impacting communities, businesses, and essential services.

Improving resiliency with RAS: In order to enhance the resiliency of the system under excessive wind conditions, we implement a centralized RAS that considers both the generation

TABLE V
RESILIENCY INDICES AT BUS 6 FOR MODIFIED IEEE 39 BUS SYSTEM FOR OFFLINE ANALYSIS

Scenario	SPD index	MW Availability Index	MVAR Availability Index	Loss of load Index	Resiliency Index (RI)
Base case	43.179	0.646	1.088	1	1.000
Excess wind without RAS	17.881	0.589	1.397	1	0.874
Excess wind with RAS	43.179	0.656	1.016	1	1.000

TABLE VI
RESILIENCY INDICES AT BUS 8 FOR MODIFIED IEEE 39 BUS SYSTEM FOR OFFLINE ANALYSIS

Scenario	SPD index	MW Availability Index	MVAR Availability Index	Loss of load Index	Resiliency Index (RI)
Base case	47.728	0.646	1.088	1	1.000
Excess wind without RAS	12.511	0.589	1.397	0.806	0.715
Excess wind with RAS	47.728	0.656	1.016	1	1.000

TABLE VII
IEEE 14 BUS WIND GENERATION FOR VARIOUS SCENARIOS

Scenario	Bus 2 (MW)	Bus 9 (MW)	Bus 11 (MW)
Base case	40	60	60
Excess wind before RAS	40	90	90
Wind generation after RAS	40	90	64.27

from wind turbines and the flow of power through transmission lines. The RAS is triggered when an excessive loading on line $6-11$ is detected. The centralized RAS algorithm is then activated to mitigate the situation by reducing the amount of generation at bus 12 to 101.36 MW, as shown in Table IV, ensuring a safer and more stable operating condition. By dynamically adjusting the generation output and reducing line flow in response to the observed loading conditions, RAS plays a vital role in enhancing transmission system resiliency and preventing subsequent outages. The resiliency index at bus 6 improves from 0.874 to 1 as shown in Table V and at bus 8 from 0.715 to 1 as shown in Table VI.

B. Online Analysis

System Setup: In order to simulate the physical and communication aspects of a power system in real-time, a cyber-physical hardware-in-the-loop testbed was built with RTDS. A modified IEEE 14 bus system, shown in Fig. 5, is developed to evaluate the resiliency for online analysis. The IEEE 14 bus system is modified such that there are three wind generators at buses $2, 9$, and 11 with 40 MW, 60 MW, and 60 MW generation respectively, shown in Table VII. Further, a critical load is designated at bus 10 consisting of 29.5 MW and 16.6 MVAR. A total of 9 PMUs are installed in the system to obtain real-time measurements which are sent to the controllers. Out of the 9 PMUs, one is an SEL hardware PMU while the rest are GTNET-PMU firmware

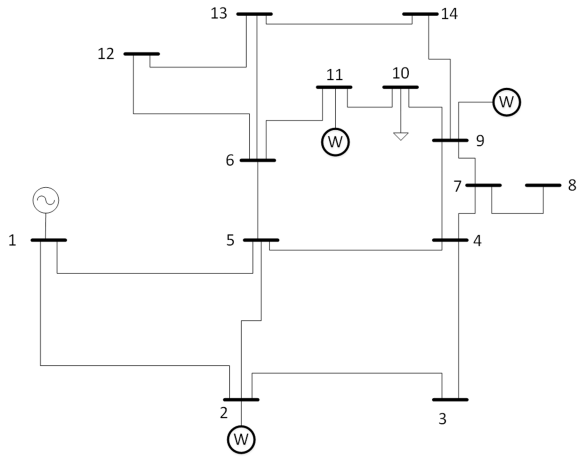


Fig. 5. Modified IEEE 14 bus system with wind generation at buses $2, 9$, and 11 and a critical load at bus 10.

PMUs. The controller in the testbed is implemented using Cisco Fog Routers. Each controller connects to 3 of these PMUs from which it reads and parses C37.118 packets. The setup uses 3 Fog VMs which run RIAPS to carry out the control functions. These VMs run distributed algorithms and coordinate with each other to function as a single control system. The connectivity between the Fog routers, RTDS, and PMUs is established using Ethernet cables. Control commands are sent back to RTDS as text strings over its `ListenOnPort` interface using standard TCP Sockets.

Loss of resiliency analysis under excess wind conditions: Under conditions of excessive wind generation, the MW output from the generators located at buses 9 and 11 increases to 90 MW. This substantial increase in generation causes an overload on the line $6-11$. In a typical scenario, this overload condition would trigger a system operating limit violation, leading to the tripping of the line $6-11$. The tripping of $6-11$

TABLE VIII
RESILIENCY INDICES AT BUS 10 FOR MODIFIED IEEE 14 BUS SYSTEM FOR ONLINE ANALYSIS

Scenario	SPD index	MW Availability Index	MVAR Availability Index	Loss of load Index	Resiliency Index (RI)
Base case	12.462	0.826	2.6579	1	1.000
Excess wind without RAS	7.643	0.911	2.316	1	0.915
Excess wind with RAS	12.462	0.891	2.680	1	1.000

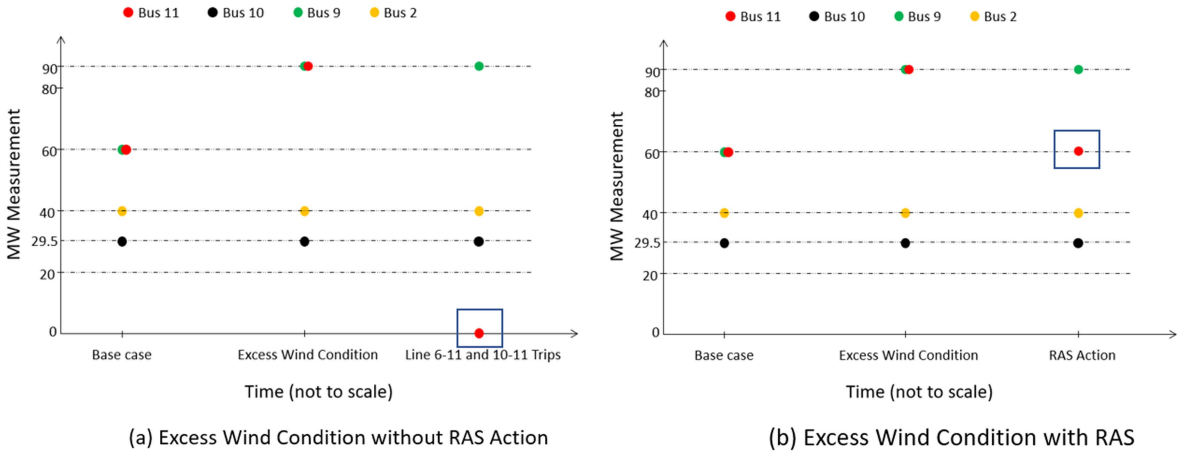


Fig. 6. Excess wind condition without and with RAS action.

adversely affects the overall resiliency of the power system, as seen in Table VIII, where the RI of bus 10 reduces from 1 to 0.915.

Improving resiliency with RAS: In order to enhance the system's resiliency in the face of excessive wind conditions, a centralized Remedial Action Scheme (RAS) is implemented. This proactive measure reduces the power output of the generator 11 from its peak of 90 MW to 64.27 MW, shown in Fig. 6, ensuring that the line $6-11$ operates within its designed limits. By preventing the line trip, the overall resiliency of the power system is preserved, as seen in Table VIII with RI $= 1$, thereby minimizing potential disruptions and improving the system's ability to withstand adverse conditions.

Loss of resiliency analysis under false data injection attack: A false data injection attack is a malicious attack where an adversary intentionally alters or injects fabricated data into a system [36], [37]. These attacks compromise the integrity of critical power processes, leading to erroneous decisions and potentially catastrophic consequences. An attack is simulated using a malicious actor who tampers with the input to the RAS application and changes the power generation values of one of the wind power generators. The original power generation value at bus 11 is 90 MW, which eventually leads to a potential line overload. However, the malicious attacker intercepts and modifies this value, changing it to 60 MW, which is then sent as input to the RAS. Consequently, the centralized RAS optimization problem fails to converge, as seen in Table IX, preventing the activation of remedial action. As a result, line $6-11$ trips, leading to a disruption in the system operations.

TABLE IX
RAS UNDER CYBER ATTACK FOR IEEE 14 BUS

Scenario	Bus 2 (MW)	Bus 9 (MW)	Bus 11 (MW)
Base case	40	90	60 (false data)
Centralized RAS	Did not converge		
De-centralized RAS	14.52	20.52	60 (false data)

Improving resiliency with decentralized RAS: To mitigate the issue of non-convergence of the centralized RAS, we employ the decentralized RAS algorithm. The decentralized RAS takes as input all the required data including the potential falsified measurement values. It is seen that the overload condition is detected and a curtailment value is found, as seen in Table IX. The results are shown in Fig. 7. While the curtailment value obtained through the decentralized RAS algorithm is notably lower than the optimal curtailment value derived under normal conditions with the centralized, it serves the purpose of mitigating the overload situation and preventing the tripping of line $6-11$ under adverse scenarios induced by malicious data injection attacks. This adaptive response highlights the resilience and effectiveness of the decentralized RAS algorithm.

C. Discussions

This section aims to analyze the results and provides insights into the implications, limitations, and future directions of the study. Despite yielding suboptimal results when correct data

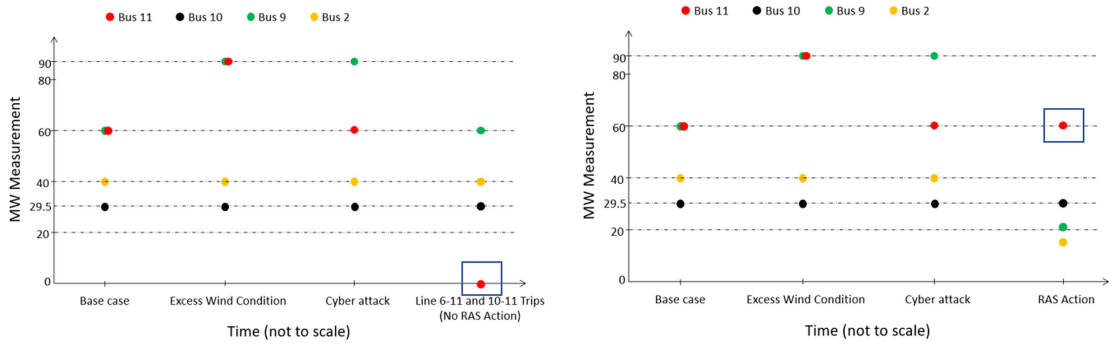


Fig. 7. Centralizedand de-centralized RAS with cyber attack.

is unavailable compared to centralized approaches, decentralized optimization provides usable solutions by leveraging local information and decision-making, offering scalability, robustness, and adaptability in complex systems, making it a viable alternative when a centralized approach may be impractical for real-world applications. It is noted that we only employ the decentralized RAS under cases of false data injection attacks when a subset of correct measurement is not accessible or due to the loss of a subset of sensor data; however, in offline and excess wind scenarios, we opt for the centralized method due to its higher optimality in decision-making with reduced message passing and considering the industry's familiarity with centralized RAS schemes. Our decentralization approach underscores the imperative of transitioning from centralized approaches to enhance the resilience of existing RAS in mitigating security violations. It is also assumed here that high wind and extreme weather scenarios have led to physical system violations such as overload while the underlying sensor data is intact. While it is unlikely that both the sensor and the system will be simultaneously down, if such a scenario occurs, power system operators would face significant challenges and experience extremely limited capabilities. We implement a decentralized RAS using convex optimization techniques to handle situations where data/measurements from one group of sensors are unavailable, while other groups can still compute a possible sub-optimal RAS solution even with incomplete data. Additionally, while excess wind power may temporarily raise the system frequency and trigger over-frequency protection, this paper considers that the multi-step frequency control with the governor, automatic generation control, and dispatch operates at the system level in large interconnected systems, and low and medium voltage systems may lack visibility at that level. Conversely, overloads are local, highlighting the necessity of establishing a RAS scheme to mitigate steady-state security violations. Lastly, it is noted that this paper does not take into account the recovery time from a contingency. The exclusion of the time factor in our resiliency metric computation is a deliberate choice to prioritize the computation of the resiliency metric in real-time and propose control actions that can immediately enhance system resiliency and mitigate risks. In future studies, we look to further expand our resiliency metric by considering transient, dynamic, and long-term security time frames.

VI. Conclusion

There is a growing interest among both system operators and wind power producers in wind curtailment as a solution to the transmission overload problems and reliability concerns caused by increased wind penetration. In this paper, we present a novel metric that takes into account the resiliency of power transmission systems under conditions of wind curtailment. The proposed resiliency metric relies on system configuration and real-time measurements and adapts to changing system conditions. For optimal wind curtailment, we develop a decentralized remedial action scheme. The proposed decentralized RAS scheme is validated on a cyber-physical test bed consisting of a real-time digital simulator, phasor measurement units, and distributed controllers. It is observed that the proposed decentralized architecture outperforms centralized architectures in finding optimal wind curtailment decisions when measurements are falsified under sophisticated cyber attacks. In the future, we will consider a detailed qualitative and quantitative analysis of the proposed resiliency metric on various other complex special protection schemes like intentional islanding to minimize renewable resource curtailment, as well as consider system recovery under different time frames.

References

[1] A. M. Stanković et al., "Methods for analysis and quantification of power system resilience," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4774–4787, Sep. 2023.
[2] S. Chanda and A. K. Srivastava, "Defining and enabling resiliency of electric distribution systems with multiple microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2859–2868, Nov. 2016.
[3] North American Electric Reliability Corporation (NERC), Project 2010-05.2. Special Protection Systems, "Remedial action scheme - definition development background and frequently asked questions," 2014. [Online]. Available: https://www.nerc.com/pa/Stand/Prjct201005_2SpclPrtctnSstmPhs2/FAQ_RAS_Definition_0604_final.pdf
[4] North American Transmission Forum, "Transmission system resiliency - an overview," Tech. Rep. 1042, Sep. 2017.
[5] R. Allan, "Power system reliability assessment—A conceptual and historical review," *Rel. Eng. Syst. Saf.*, vol. 46, no. 1, pp. 3–13, 1994.
[6] N. Yodo, P. Wang, and M. Rafi, "Enabling resilience of complex engineered systems using control theory," *IEEE Trans. Rel.*, vol. 67, no. 1, pp. 53–65, Mar. 2018.
[7] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1604–1613, Mar. 2016.

[8] N. Bhusal, M. Abdelmalak, M. Kamruzzaman, and M. Benidris, "Power system resilience: Current practices, challenges, and future directions," *IEEE Access*, vol. 8, pp. 18064–18086, 2020.
[9] A. Bagheri, C. Zhao, F. Qiu, and J. Wang, "Resilient transmission hardening planning in a high renewable penetration era," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 873–882, Mar. 2019.
[10] M. Abdelmalak and M. Benidris, "Proactive generation redispatch to enhance power system resilience during hurricanes considering unavailability of renewable energy sources," *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 3044–3053, May/Jun. 2022.
[11] H. Sabouhi, A. Doroudi, M. Fotuhi-Firuzabad, and M. Bashiri, "Electrical power system resilience assessment: A comprehensive approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2643–2652, Jun. 2020.
[12] Q. Wang, Z. Yu, R. Ye, Z. Lin, and Y. Tang, "An ordered curtailment strategy for offshore wind power under extreme weather conditions considering the resilience of the grid," *IEEE Access*, vol. 7, pp. 54824–54833, 2019.
[13] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power system resilience to extreme weather: Fragility modeling, probabilistic impact assessment, and adaptation measures," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3747–3757, Sep. 2017.
[14] E. B. Watson and A. H. Etemadi, "Modeling electrical grid resilience under hurricane wind conditions with increased solar and wind power generation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 929–937, Mar. 2020.
[15] Y. Yang, W. Tang, Y. Liu, Y. Xin, and Q. Wu, "Quantitative resilience assessment for power transmission systems under typhoon weather," *IEEE Access*, vol. 6, pp. 40747–40756, 2018.
[16] S. Basumallik, S. Eftekharnejad, and B. K. Johnson, "The impact of false data injection attacks against remedial action schemes," *Int. J. Elect. Power Energy Syst.*, vol. 123, 2020, Art. no. 106225.
[17] Western Electric Coordinating Council, "Remedial action scheme design guide," 2006. [Online]. Available: https://www.wecc.org/Reliability/RWG%20RAS%20Design%20Guide%20_%20Final.pdf
[18] V. V. G. Krishnan, R. Liu, A. Askerman, A. Srivastava, D. Bakken, and P. Panciatici, "Resilient cyber infrastructure for the minimum wind curtailment remedial control scheme," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, 2017, pp. 1–7.
[19] H. Khoshkhoo, S. Yari, A. Pouryekta, V. K. Ramachandaramurthy, and J. M. Guerrero, "A remedial action scheme to prevent mid/long-term voltage instabilities," *IEEE Syst. J.*, vol. 15, no. 1, pp. 923–934, Mar. 2021.
[20] Y. Zhao et al., "Deep learning-based adaptive remedial action scheme with security margin for renewable-dominated power grids," *Energies*, vol. 14, no. 20, 2021, Art. no. 6563.
[21] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 2, no. 4, pp. 188–197, 2017.
[22] E. Naderi, S. Pazouki, and A. Asrari, "A remedial action scheme against false data injection cyberattacks in smart transmission systems: Application of thyristor-controlled series capacitor (TCSC)," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2297–2309, Apr. 2022.
[23] R. Liu, A.K. Srivastava, D. E. Bakken, A. Askerman, and P. Panciatici, "Decentralized state estimation and remedial control action for minimum wind curtailment using distributed computing platform," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5915–5926, Nov./Dec. 2017.
[24] P. Agarwal and C. Kumar, "Validation and tuning of remedial action schemes in Indian grid operations using synchrophasor technology," in *Power System Grid Operation Using Synchrophasor Technology*. Berlin, Germany: Springer, 2018, pp. 385–401.
[25] K. Baskin, M. Thompson, and L. Lawhead, "Design and testing of a system to classify faults for a generation-shedding RAS," in *Proc. IEEE 62nd Annu. Conf. Protective Relay Engineers*, 2009, pp. 140–149.
[26] M. Vaughan, R. Schloss, S. Manson, S. Raghupathula, and T. Maier, "Idaho power RAS: A dynamic remedial action case study," in *Proc. 64th Annu. Georgia Tech Protective Relaying Conf.*, 2010.
[27] J. Malcón, N. Yedrzejewski, A. Balasubramanian, R. Syed, and S. Raghupathula, "Implementing a country-wide modular remedial action scheme in Uruguay," in *Proc. Western Protective Relay Conf.*, 2015, pp. 20–22.
[28] S. C. Pai and J. Sun, "BCTC's experience towards a smarter grid - increasing limits and reliability with centralized intelligence remedial action schemes," in *Proc. IEEE Canada Electric Power Conf.*, 2008, pp. 1–7.
[29] J. Wen, W. H. E. Liu, P. L. Arons, and S. K. Pandey, "Evolution pathway towards wide area monitoring and protection—A real-world implementation of centralized RAS system," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1506–1513, May 2014.
[30] H. Dutta and H. Kargupta, "Distributed linear programming and resource management for data mining in distributed environments," in *Proc. IEEE Int. Conf. Data Mining Workshops*, 2008, pp. 543–552.
[31] S. Eisele, I. Mardari, A. Dubey, and G. Karsai, "RIAPS: Resilient information architecture platform for decentralized smart systems," in *Proc. IEEE 20th Int. Symp. Real-Time Distrib. Comput.*, 2017, pp. 125–132.
[32] J. Y. Yen, "An algorithm for finding shortest routes from all source nodes to a given destination in general networks," *Quart. Appl. Math.*, vol. 27, no. 4, pp. 526–530, 1970.
[33] J.-H. Kim and J.-B. Park, "Generators availability modeling considering planned maintenance outage and demand clustering," in *Proc. Power Eng. Soc. Gen. Meeting*, 2006, p. 7.
[34] P. Lagonotte, J. Sabonnadiere, J.-Y. Leost, and J.-P. Paul, "Structural analysis of the electrical system: Application to secondary voltage control in France," *IEEE Trans. Power Syst.*, vol. 4, no. 2, pp. 479–486, May 1989.
[35] R. Saaty, "The analytic hierarchy process—What it is and how it is used," *Math. Modelling*, vol. 9, no. 3, pp. 161–176, 1987.
[36] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
[37] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Elect. Power Energy Syst.*, vol. 107, pp. 690–702, 2019.