

Cyber-physical-aware cascading mitigation in converter-dominated power systems

Hashemi, Sina; Rajkumar, Vetrivel S.; Ștefanov, Alexandru; Panteli, Mathaios

DOI

[10.1016/j.segan.2025.102065](https://doi.org/10.1016/j.segan.2025.102065)

Publication date

2025

Document Version

Final published version

Published in

Sustainable Energy, Grids and Networks

Citation (APA)

Hashemi, S., Rajkumar, V. S., Ștefanov, A., & Panteli, M. (2025). Cyber-physical-aware cascading mitigation in converter-dominated power systems. *Sustainable Energy, Grids and Networks*, 44, Article 102065. <https://doi.org/10.1016/j.segan.2025.102065>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

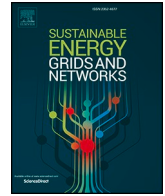
Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

**Green Open Access added to [TU Delft Institutional Repository](#)
as part of the Taverne amendment.**

More information about this copyright law amendment
can be found at <https://www.openaccess.nl>.

Otherwise as indicated in the copyright section:
the publisher is the copyright holder of this work and the
author uses the Dutch legislation to make this work public.



Cyber-physical-aware cascading mitigation in converter-dominated power systems

Sina Hashemi^{a,*}, Vetrivel S. Rajkumar^b, Alexandru Ștefanov^b, Mathaios Panteli^a

^a Department of Electrical and Computer Engineering, University of Cyprus, Cyprus

^b Department of Electrical Sustainable Energy, Delft University of Technology, Delft, the Netherlands

ARTICLE INFO

Keywords:

Cascading failures
DC segmentation
Grid reinforcement
Operational mitigation
Cyber-physical resilience

ABSTRACT

Mitigation strategies to absorb impacts from extreme events that may trigger cascading outages are crucial for modern power systems, particularly given the increasing penetration of power electronics, thereby enhancing system resilience. This paper presents a comprehensive resilience-centered framework that integrates cyber-physical cascading mitigation through network topology reinforcement and operational strategies, specifically DC segmentation and controlled islanding, respectively. The methodology first identifies AC lines at segmentation boundaries (i.e., those that most frequently contribute to system partitioning) and evaluates the benefits of replacing them with VSC-HVDC links through dynamic cascading analysis and quantification, thereby enabling the asynchronous interconnection of segments. This approach helps confine cascading impacts within segments, significantly reducing the risk of widespread blackouts, especially in renewable-rich power grids with a heightened risk of instability. Next, to enhance operational resilience against cascading failures, controlled islanding is implemented within the DC-segmented system undergoing cascade initiation, effectively further confining cascading stress to a limited area around the origin of the initiating events. Tailored to enhance resilience in hybrid AC/DC power grids against cyber and physical cascade triggering events, the method leverages a cyber-anomaly detection technique to identify elements affected by fabricated protection trip commands and measurement replay attacks, distinguishing cyberattacks from physical disturbances. Implemented in the IEEE 39-bus and 118-bus test systems with dynamic cascading failure modeling that fully captures voltage and frequency transients in system response, the method demonstrates improvements of up to 88 % and 97 % in served demand, respectively, highlighting its effectiveness in mitigating cascading impacts and enhancing system resilience.

1. Introduction

Modern power systems, particularly cyber-physical power systems (CPPS) dominated by power-electronics-interfaced technologies and high renewable energy source (RES) penetration, are increasingly vulnerable to cascading failures triggered by cyberattacks and natural hazards. Cyberattacks, in particular, significantly elevate the risk of widespread blackouts, a threat that increases as CPPS become more dependent on digital technologies [1]. Notably, past cyberattacks, such as those on Ukraine's power grid in 2015 and 2016 [1], underscore the critical need for resilience enhancement strategies to defend against such threats. In CPPS, cyberattacks may involve compromising critical communication links, such as those between phasor measurement units

(PMUs) and Phasor Data Concentrators (PDCs), potentially fabricating, altering, or deleting measurement data, which disrupts real-time grid monitoring. Moreover, the manipulation of control signals and protection commands—such as blocking controllers or replaying trip commands—can further destabilize the grid, amplifying vulnerabilities [2]. To mitigate these risks, a combination of infrastructural and operational resilience enhancement strategies should be implemented in the physical layer to localize and contain the impact of cyber-physical incidents. These measures help prevent cascading propagation across the grid, ensuring system resilience even in scenarios where adversaries successfully breach cyber defenses or when severe physical disturbances, such as weather-related events, occur.

DC segmentation is one such infrastructural resilience enhancement

* Corresponding author.

E-mail addresses: hashemi.seyedsina@ucy.ac.cy (S. Hashemi), v.subramaniamrajkumar@tudelft.nl (V.S. Rajkumar), a.i.stefanov@tudelft.nl (A. Ștefanov), panteli.mathaios@ucy.ac.cy (M. Panteli).

<https://doi.org/10.1016/j.segan.2025.102065>

Received 26 March 2025; Received in revised form 10 November 2025; Accepted 13 November 2025

Available online 17 November 2025

2352-4677/© 2025 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

strategy that strengthens the transmission network by dividing large AC grids into smaller, asynchronously operated segments interconnected by HVDC links [3,4]. Enabled by VSC-HVDC technology, it improves power flow controllability, provides voltage and frequency support, offers black-start capability, and enhances grid stability through dynamic insulation and controlled power flow [5]. DC segmentation mitigates electromechanical oscillations [6], enhances transfer capacity and stability [7–9], and prevents overloading. By limiting disturbance propagation and containing initiating events within confined areas, it minimizes cascading outages and prevents widespread propagation, particularly in large synchronous power systems [4]. This significantly reduces blackout risks and strengthens overall grid resilience [10].

Additionally, alongside network reinforcement strategies, power grids must incorporate effective operational mitigation measures—such as controlled load reduction and controlled islanding—to minimize the risk of cascading outages and blackouts during emergencies and extreme operating conditions. As a last-resort strategy in both preventive [11] and corrective control actions [12,13], controlled islanding effectively mitigates cascading failures triggered by cyberattacks, severe weather-related incidents, and technical disturbances. In [14], various controlled islanding methods suitable for online Wide-Area Monitoring, Protection, and Control (WAMPC) applications are evaluated, emphasizing the critical need for a very short computational time to enable effective reactive applicability in near-real-time. Following severe events that trigger cascading failures, power system operators can implement operational mitigation strategies to prevent system collapse, particularly in cases that raise suspicions of cyberattacks. Operational measures such as controlled islanding can isolate affected elements, enabling direct communication between the control center and power plants or substations. This, in turn, facilitates a more thorough investigation of evolving incidents, enhances situational awareness, and supports informed decision-making for effective grid operations [15,16].

Several critical research gaps remain underexplored in the context of infrastructural and operational resilience enhancement strategies within the physical layer—particularly for hybrid AC/DC power grids facing cyber-physical disturbances. Key challenges requiring further investigation include identifying optimal segmentation boundaries to contain cascading failures effectively, evaluating the dynamic performance of DC segmentation in mitigating cascading failures—especially in grids with high penetration of wind generation—and conducting quantitative studies on its benefits in reducing large-scale blackouts and cascading outages in converter-dominated power systems. Beyond infrastructural reinforcement, operational strategies like controlled load reduction and controlled islanding in converter-dominated grids remain under-examined. This paper, for the first time in this domain, bridges these gaps by introducing a hybrid approach that integrates both infrastructural and operational resilience enhancement strategies to mitigate cascading failures triggered by cyber-physical disturbances. The key contributions of the paper are as follows:

- Offering holistic dynamic modelling and quantification of cascading failures, incorporating the influence of converter-interfaced technologies such as WTs and HVDC links, and considering cyber-induced cascading outages.
- Introducing a novel DC segmentation technique for power network reinforcement, enhancing the infrastructure resilience of grids with high penetration of wind generation.
- Developing a cascading-aware operational mitigation strategy for DC-segmented grids, incorporating controlled load reduction and controlled islanding, along with an anomaly detection technique to identify and distinguish cyberattacks and affected elements, thereby improving operational resilience.

The remainder of this paper is organized as follows: Section II presents the proposed methodology for enhancing hybrid infrastructure and operational resilience against cyber-physical disturbances. It primarily

provides a detailed explanation of each resilience enhancement framework. Section III delves into simulation studies and analyses of the results for various scenarios and case studies, comparing the outcomes of no reinforcement strategy, reinforcement strategy alone, and the combined reinforcement and operational mitigation strategies. Finally, Section IV concludes the paper.

2. Cyber-physical resilience enhancement strategy

2.1. Proposed framework and methodology

Fig. 1 illustrates the proposed holistic framework for resilience enhancement against cascading failures. The framework incorporates resilience-oriented measures to mitigate cascading failures through both proactive and reactive strategies. These measures include infrastructural enhancements, such as transmission network topology reinforcement with DC segmentation, and operational improvements, such as controlled load reduction and intentional controlled islanding, to significantly strengthen system resilience against extreme events. Fig. 2 conceptually depicts the resilience trapezoid of a power system before (a) and after (b) segmentation, demonstrating how resilience can be effectively enhanced in DC-segmented power systems as a proactive strategy. By establishing two segments through HVDC links in an asynchronous interconnection manner, disturbances affecting one segment (e.g., Segment 1) do not impact the other (Segment 2), enhancing overall system resilience through network topology reinforcement. This results in a significant reduction in demand-not-served (DNS), where DNS after segmentation (DNS2) is considerably lower than before segmentation (DNS1), i.e., $DNS2 < DNS1$. Comparatively, Fig. 2-(c) illustrates how operational mitigation strategies can further confine the stress of initiating events to a limited area and absorb cascading impacts. This further enhances system resilience by reducing DNS, with DNS3 being significantly lower than DNS2 ($DNS3 < DNS2$). It should be noted that the DNS value is calculated consistently across all cases as the difference between the system load under normal operation, prior to the initiating event(s), and the system load after cascading propagation halts in time-domain simulation studies.

Subsections II-B, II-C, II-D, and II-E provide detailed explanations of the converter-dominated power system setup, the definition of cyber-physical disturbances, the dynamic modeling of cascading failures in converter-dominated power grids, and the identification of affected elements (AEs), respectively. These subsections support the proposed methodology, which facilitates effective solutions for both infrastructure and operational resilience enhancements against cyber-physical cascading failures. This includes the identification of AC lines for DC segmentation as a network topology reinforcement and the identification of boundary lines for controlled islanding as an operational mitigation strategy, both described in detail in Subsection II-F.

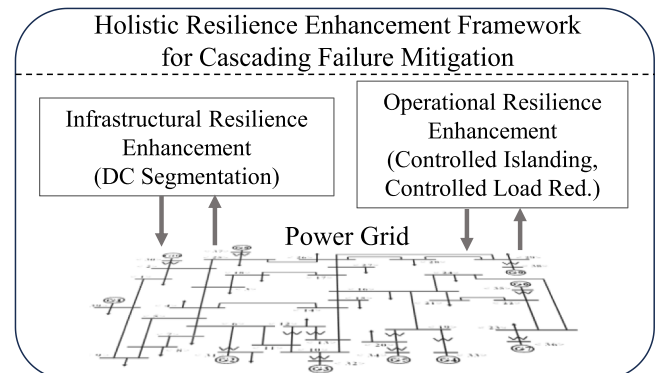


Fig. 1. Proposed holistic framework for resilience enhancement.

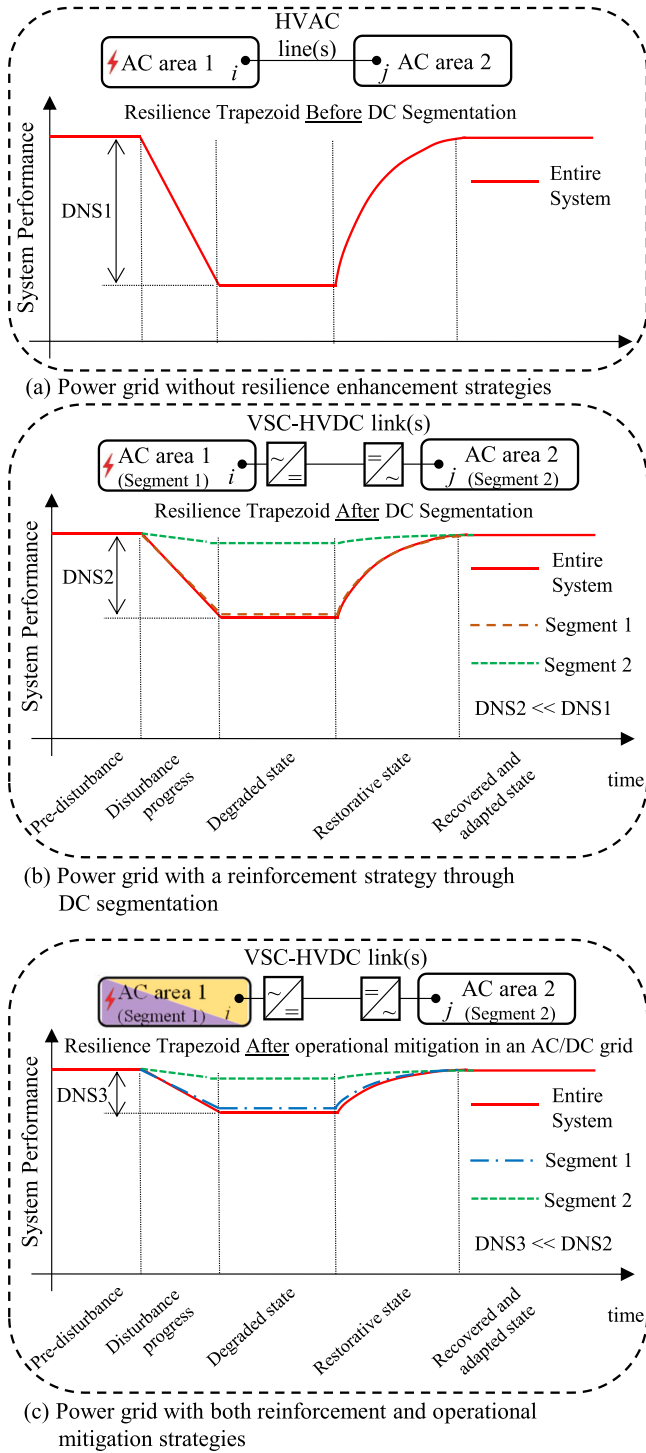


Fig. 2. Conceptual framework of the hybrid resilience enhancement strategy.

2.1.1. Infrastructure resilience via DC segmentation

In essence, system segmentation is influenced by economic considerations, such as HVDC installation costs, and by technical ones, particularly improvements in system dynamic performance. It should be emphasized, however, that the present study focuses specifically on the technical aspects from a dynamic stability assessment perspective, accounting for potential improvements achieved through optimal HVDC sizing and placement configurations. From a stability standpoint, the study assumes that each segment must include at least one synchronous generator and one black-start unit (BSU) to ensure adequate frequency support, voltage regulation, and system restoration capability.

Moreover, depending on the size of the grid and the location of generators and BSUs, the segments may differ. Building on the conceptual framework introduced earlier, Fig. 3 presents the flowchart of the cascading-aware DC segmentation methodology, which divides the power grid into two or more segments using VSC-HVDC links for asynchronous interconnection. This approach ensures distinct dynamics and behaviors for each segment, effectively confining the stress of cascading failures within the segment where the initiating events originate.

The methodology begins by defining a contingency set containing $N-k$ contingencies of network branches. These contingencies are then applied to the system, and a power flow analysis is conducted to compute the edge weights of the power network graph, which are subsequently used in the spectral clustering technique for system partitioning. Each edge weight (w_{ij}), as detailed in Subsection II-F, is defined as the mean of the absolute values of the active power flowing across the transmission line connecting nodes i and j . Next, system partitioning is carried out using the constrained spectral clustering technique, ensuring that each segment contains at least one conventional power plant with blackstart (BS) capability. AC lines at segmentation boundaries are then identified, and this process is repeated for all defined contingencies. The optimal location for DC segmentation is then determined by identifying the lines that most frequently contribute to system partitioning.

2.1.2. Operational resilience via controlled islanding and load reduction

On the other hand, the proposed operational resilience enhancement strategy deploys controlled load reduction and controlled islanding, depending on the grid size and available BS resources that can support the system. Fig. 4 illustrates the flowchart of this operational resilience enhancement strategy. Controlled islanding can be implemented if the grid size allows for the formation of at least two islands (as determined by Eq. (1)) and ensures that each island contains at least one black-start unit (BSU), such as a conventional power plant or a VSC-HVDC link operating in grid-forming (GFM) mode. This methodology begins with defining cyber-physical disturbances (explained in Section II-C). Next, dynamic modeling of power grids, incorporating wind turbines (WTs) and VSC-HVDC systems, is conducted from a cascading failure perspective to capture the interactions and behaviors of protective relays and controllers. Then, based on measurement data from

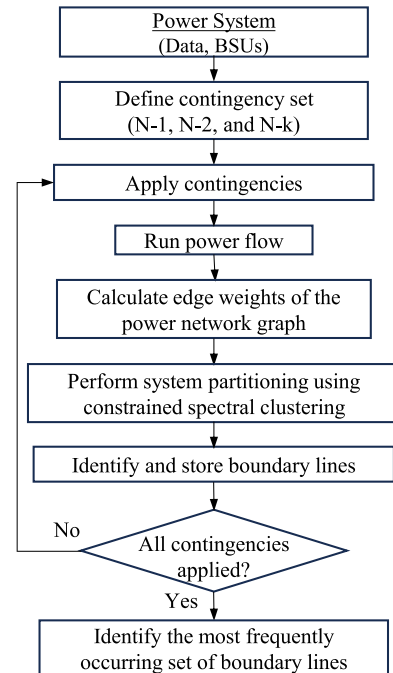


Fig. 3. Flowchart of the proposed method for the power network reinforcement (DC segmentation).

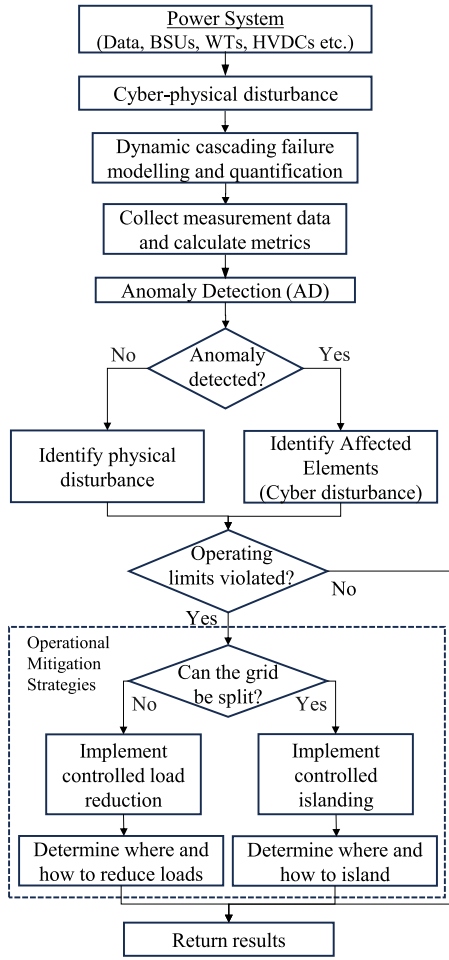


Fig. 4. Flowchart of the proposed method for the operational mitigation strategies (controlled load reduction and controlled islanding).

simulations, an anomaly detection technique is applied to distinguish between disturbances originating from the cyber layer (cyberattacks) and those from the physical layer (technical failures within the power grid).

Eq. (1) is presented as a mathematical relation to determine the number of islands that can be formed in Segment i when operational mitigation against cascading failures, specifically controlled islanding, is required. Specifically, the number of islands in Segment i , $N_{Seg_i}^{isl}$, established through controlled partitioning can be calculated using Eq. (1). This value depends on the number of available Black-Start Units ($N_{Seg_i}^{BSU}$) and the total number of buses in Segment i (N_{Seg_i}). This equation constrains the islanding problem by ensuring that the network being split is sufficiently large, defined as $\lfloor 0.5 \cdot \sqrt{N_{Seg_i}} \rfloor$, which represents the rounded-down value [17], and contains at least one BSU.

$$N_{Seg_i}^{isl} = \min(N_{Seg_i}^{BSU}, \lfloor 0.5 \cdot \sqrt{N_{Seg_i}} \rfloor) \quad (1)$$

Upon detecting an anomaly, the technique identifies power grid elements affected by cyberattacks and mitigates their subsequent cascading impacts through operational mitigation strategies, such as controlled load reduction or controlled islanding, depending on the grid size and available BSUs. These operational mitigation strategies are implemented when power grid operating limits, such as line loading and voltage magnitudes, are violated. Upon operating limit violations, if the grid size and available BSUs allow for at least two islands (Eq. (1)), controlled islanding is implemented. Otherwise, controlled load reduction is applied to resolve the violations, thereby alleviating system stress

and preventing propagation.

2.2. Setup of converter-dominated power systems

The methodology develops models of AC/DC power systems dominated by power electronics converters, suitable for time-domain RMS simulations. This enables accurate representation of dynamic responses at millisecond-level resolution, supporting the analysis of cascading failures that typically unfold over seconds to minutes. It further establishes the setup of converter-interfaced technologies in power systems with high penetration of renewable energy sources (RES), including wind turbines (WTs) modeled as Type-4 (full converters) and HVDC links represented as point-to-point bipolar VSC-HVDC connections, incorporating both selective Grid-Forming (GFM) and Grid-Following (GFL) control strategies. Fig. 5 illustrates the Type-4 WT model, which employs a back-to-back power electronics converter that fully decouples the generator from the grid, enabling active and reactive power controls [18]. The machine-side converter (MSC) regulates generator speed for maximum power point tracking (MPPT), while the grid-side converter (GSC) controls active power and either AC voltage or reactive power, with fault ride-through (FRT) capabilities.

Fig. 6 also illustrates the point-to-point VSC-HVDC link, including converters on both ends along with their respective controllers [19,20]. For this HVDC architecture, one converter operates in GFL mode, regulating the DC link voltage while also controlling either the AC voltage or reactive power (Q) at the point of connection (POC). In contrast, the other converter can operate in either GFL or GFM mode. In GFM mode, the converter supports the voltage and frequency of the AC grid at POC.

2.3. Cyber-physical disturbance definition

This work considers both types of resilience events arising from the cyber layer and the physical layer. For the grid reinforcement (DC segmentation), the study implements a list of full $N - 1$, $N - 2$, 1000 random $N - 3$, and $N - 4$ contingencies. For the operational mitigation strategy, two random scenarios are selected for detailed analysis: one involving cyber disturbances and the other involving physical disturbances. This work formulates the generation of $N - k$ contingencies as physical disturbances (PD) using the Monte Carlo technique, as expressed in Eq. (2).

$$PD = \left\{ O^m | O^m \in \{0, 1\}^N, \sum_{i=1}^N (1 - O_i^m) = k, \underline{k} \leq k \leq \bar{k} \right\}, \quad m = 1, 2, \dots, M \quad (2)$$

where PD represents the set of M outage scenarios, and O^m denotes the m -th outage scenario in the Monte Carlo simulation. N represents the dimension of L , which corresponds to the total number of network branches. This formulation ensures the simultaneous outage of exactly k

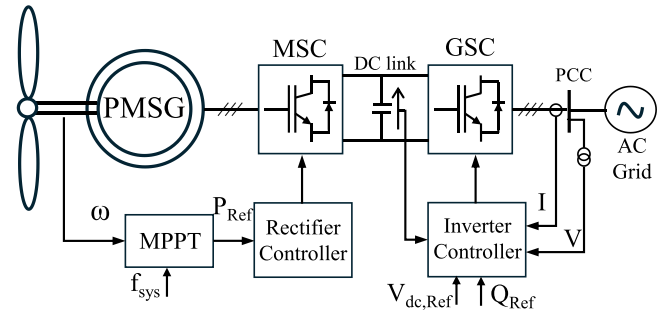


Fig. 5. Type-4 wind turbine generator and its associated controllers.

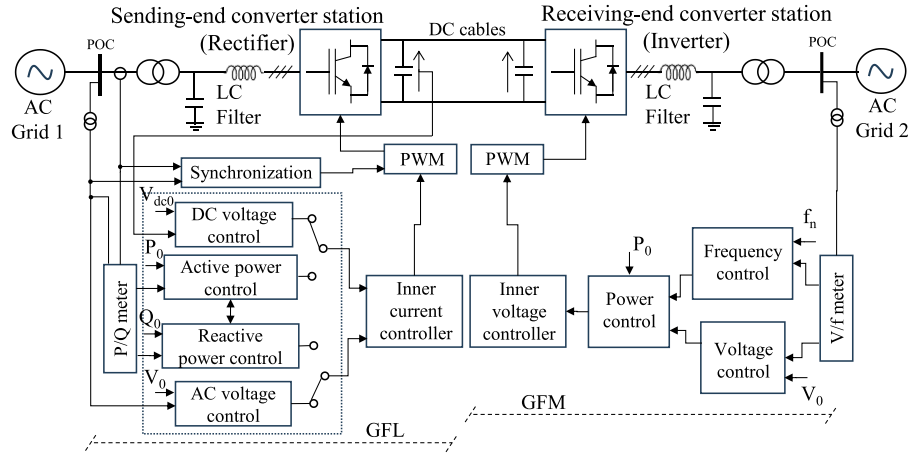


Fig. 6. Point-to-point VSC-HVDC link and its associated controllers.

branches in each scenario, where k ranges between $\underline{k}$ and $\bar{k}$ (3 and 4, respectively, for the network reinforcement in this study). Here, $O^m \in \{0, 1\}^N$ indicates that each outage scenario is represented as an N -dimensional binary vector, where $O_i^m = 0$ denotes an outage of branch i , and $O_i^m = 1$ indicates no outage. M is the total number of Monte Carlo simulations, i.e., the number of outage scenarios to be generated.

Fig. 7 conceptually illustrates vulnerable points in CPPS that adversaries can target to carry out their planned attacks [13]. These vulnerabilities may include compromising communication links between PMUs and PDC, fabricating, altering, or deleting measurement data, and manipulating control signals and protection commands. In this study, two types of cyberattacks, i.e., fabricated trip commands and replay attacks, are considered, targeting protection relays and measurement data, respectively. It is also assumed that network security is compromised and breached by adversaries through gaining necessary access to launch cyberattacks, due to vulnerabilities within the cyber layer. In the attacker model, attack resources limited by the maximum available number are considered due to the attack budget [21]. Different scenarios can be defined using Eq. (3) by varying the maximum number of concurrent attacks ($\bar{R}$) [22]. It can also be assumed that a maximum of $\bar{\gamma}$ generators can be attacked in each scenario. The cyberattack-affected elements are defined randomly, as formulated below:

$$CD = \left\{ O^a | O^a \in \{0, 1\}^N, \sum_{i=1}^N (1 - O_i^a) \leq \bar{R}, \sum_{r \in \Gamma} (1 - O_r^a) \leq \bar{\gamma} \right\}, \quad a = 1, 2, \dots, M \quad (3)$$

where, CD denotes the cyber disturbance as a random integer vector representing cyberattack-affected elements, with values of 0 and 1 indicating affected and not-affected elements, respectively; O^a is a vector including binary numbers corresponding to all transmission lines, transformers, and generators; N represents the dimension of I , which corresponds to the total number network elements, comprising all transmission lines, transformers, and generators, while Γ represents a set of all generators; $\bar{R}$ refers to the maximum number of concurrent attacks.

2.4. Dynamic modelling of cascading failures in converter-dominated power grids

Dynamic modeling of cascading failures is essential for modern power systems integrating emerging converter-interfaced technologies, such as HVDC links and renewable energy sources. This requires leveraging time-domain RMS simulations to capture transients in system voltage and frequency responses during and after disturbances [23]. The choice of RMS simulation in such studies is typically motivated by its ability to provide an optimal balance between computational efficiency and the level of detail needed to assess system-wide dynamic behavior and resilience under a range of high-impact, low-probability (HILP) events [24]. While EMT simulations capture finer device-level transients on microsecond to millisecond timescales, RMS simulations with millisecond-level resolution are more suitable for analyzing cascading failures that typically unfold over seconds to minutes. They offer sufficient temporal resolution to capture the relevant dynamics while maintaining computational efficiency for large-scale systems and extensive scenario analyses [25]. Time-domain RMS studies account for the nonlinear behavior of system components, including synchronous machines, inverter-based resources (IBRs), their controllers, and protection systems. By simulating voltage and frequency responses over time, these studies help identify critical and vulnerable components and areas of the grid, such as generators and transmission corridors with frequent contributions to cascades, relay operations, and load shedding—factors that can intensify cascading failures, ultimately leading to system-wide instability and collapse. The modeling in this work accounts for both GFL and GFM control schemes of HVDC links, WT power control modes, and other controllers for conventional power plants, such as the automatic voltage regulator (AVR) and governor. The protective relays modeled in this dynamic cascading failure study include line

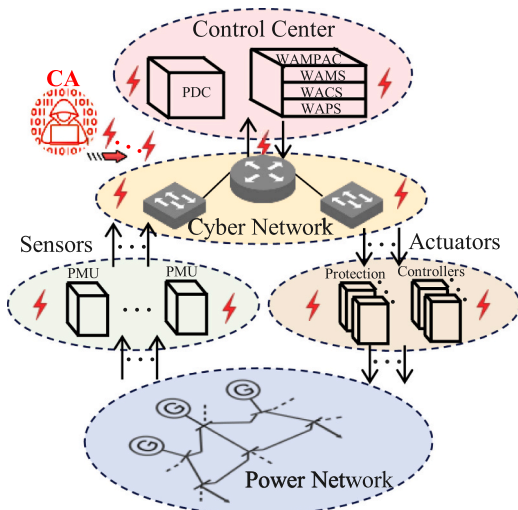


Fig. 7. Vulnerable points to launch cyberattacks on a conceptually represented typical CPPS.

overload protection, over/under-voltage and frequency protective relays, such as underfrequency and undervoltage load shedding relays, as well as over/under-voltage and frequency generator tripping relays [26]. In this work, the entire model, including protective relays and controllers associated with devices such as WTs and VSC-HVDC links, is simulated using built-in DSL and composite models from the DiGSILENT PowerFactory software library.

2.5. Identification of affected elements (AE)

As the proposed methodology is designed for near-real-time applications, the computational burden of the anomaly detection method needs to be low. To this end, the overall methodology employs the Pearson correlation as a data-driven online detection comparison metric for cyberattacks. It is used to measure the strength and direction of a linear relationship between two variables. This anomaly detection (AD) method is nearly instantaneous and effectively locates affected elements by calculating correlations of data within a moving window of PMU measurements [27]. Given that attack resources are limited and only a few elements can be targeted [21], detection of anomalies caused by cyberattacks, including fabricated trip commands and replay attacks, can be achieved by tracing correlations in measurement data. The method distinguishes between data packets originating from an actual fault or disturbance and those fabricated or altered by attackers. As a consequence of the cyberattack, a sudden drop in the correlation value between two successive instants is detected. This drop reflects a low or poor correlation, indicating a loss of a common trend and unison in the system's response at respective measurement points [27]. If the correlation value of a specific measurement compared to that of other neighboring measurements exhibits a distinctive trend, the corresponding element is identified as being attacked. The pseudocodes presented in Algorithm 1 outline the process of identifying affected elements due to cyberattacks. It is worth mentioning that the present studies do not consider security measures in the cyber layer of CPPS.

Algorithm 1. Identification of Affected Elements (AE)

```

- Collect phasor measurement data
- Calculate correlations between each pair of measurements within the moving window
- if a distinctive trend in correlations is detected then
-   if any tripping occurred then
-     Identify the tripped elements with the detected anomaly as Affected Elements (AE)
-     Proceed with the implementation of operational mitigation strategies
-   end if
- end if

```

2.6. Spectral clustering-based system partitioning

The spectral clustering-based technique is employed for both DC segmentation (Section II-A-1), which strengthens network topology using HVDC links, and controlled islanding as an operational mitigation strategy (Section II-A-2). The technique performs a graph cut on an undirected edge-weighted graph representation of the power grid. The edge weight of a power network graph (w_{ji}), as formulated in Eq. (4) [28], is calculated as the mean of the absolute values of the active power across the transmission line connecting nodes i and j . This serves as a dynamic weighting that captures the effects of ongoing changes in actual operating conditions on power flow.

$$w_{ij} = w_{ji} = (|P_{ij}| + |P_{ji}|)/2 \quad (4)$$

Since the objective of system splitting is to confine cascading propagation within a limited area where the initiating events occur, the objective function aims to identify AC transmission lines for splitting while minimizing subsequent power flow disruption. This is achieved by minimizing the summation of the absolute values of the active power flow across the splitting boundary branches, as expressed in (5).

$$\min \left(\sum_{i,j \in \mathcal{S}_B} (|P_{ij}| + |P_{ji}|)/2 \right) \quad (5)$$

Subject to

$$CL = \{(i,j) \mid i,j \in B_{BSU}\} \quad (6)$$

$$ML = \{(i,j) \mid i,j \in [B_{HVDC}, B_{AE}]\} \quad (7)$$

where $\mathcal{S}_B$ is the set of buses at both ends of the splitting boundary branches. B_{BSU} represents the set of buses at BSUs.

In this work, the spectral clustering formulation is refined and enhanced for application in DC segmentation and controlled islanding by introducing two types of pairwise constraints: Must Link (ML) and Cannot Link (CL) [29]. An ML constraint between two vertices ensures that these vertices will belong to the same cluster, while a CL constraint guarantees that the vertices will be assigned to different clusters. In the following subsections, Subsections II-F-1 and II-F-2, these enhancements are detailed for both applications.

2.6.1. Identification of AC lines for DC segmentation as network topology reinforcement

According to the flowchart in Fig. 3, the set of AC lines that frequently contribute to system partitioning is identified after applying a list of contingencies generated by Eq. (2), as described in Section II-C. These AC lines are then replaced with VSC-HVDC links, effectively DC-segmenting the grid. This results in asynchronous interconnections between segments and dynamically isolates the behavior and response of system segments, preventing a complete blackout by confining the impacts of cascading failures to the segment where the initiating events occur. The constraints of spectral clustering, specifically the CL

constraint, for DC segmentation ensure that each individual segment has at least one BSU, typically provided by synchronous generators. This facilitates system restoration in the event of blackouts, thereby enhancing resilience in system recovery. The number and location of BSUs are determined by system operators or planners, based on the number of segments that need to be formed. Therefore, the spectral clustering-based DC segmentation is constrained by CL, as shown in Eq. (6). In this case, for DC segmentation, $\mathcal{S}_B$ in Eq. (5) represents the set of buses at both ends of the splitting boundary branches while accounting for the entire system. Moreover, the ML constraint can be null and is therefore excluded in this case.

Considering that other AC transmission lines remain unchanged, particularly those connected to HVDC POCs, the rated capacity of HVDC interconnectors, in MVA, is then formulated as follows:

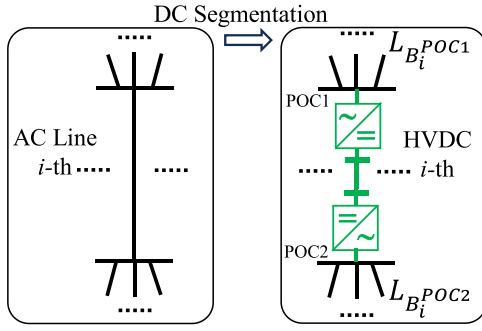


Fig. 8. Typical illustration of an AC line replacement with an HVDC interconnector for the implementation of DC segmentation.

$$MVA_{HVDC_i}^{Rated} = \min \left(\sum_{l \in L_{B_i^{POC1}}} MVA_{L_i}^{Rated}, \sum_{l \in L_{B_i^{POC2}}} MVA_{L_i}^{Rated} \right)$$

where

$$L_{B_i^{POC1}} = \{l \mid \text{Line connects to } B_i^{POC1}, B_i^{POC1} \in \mathcal{S}_B\}$$

$$L_{B_i^{POC2}} = \{l \mid \text{Line connects to } B_i^{POC2}, B_i^{POC2} \in \mathcal{S}_B\} \quad (8)$$

B_i^{POC1} and B_i^{POC2} represent the ending buses or the points of connection for the i -th HVDC link. $L_{B_i^{POC1}}$ and $L_{B_i^{POC2}}$ represent the sets of AC lines connected to the i -th HVDC POCs at B_i^{POC1} and B_i^{POC2} , respectively. $MVA_{HVDC_i}^{Rated}$ denotes the rated capacity of the i -th HVDC link, calculated as the minimum of the summation of the rated capacities of other AC lines, $MVA_{L_i}^{Rated}$, connected to its POCs.

According to Eq. (8) and as illustrated in Fig. 8, when an AC line is replaced with an HVDC interconnector for DC segmentation, the capacity of HVDC links is determined based on the capacity of other lines connected to their POCs. This is because, if no changes apply to other parts of the system topology, including AC lines, the new hybrid AC/DC grid architecture—such as DC-segmented grids—must not degrade system performance, particularly by overloading other AC transmission lines.

2.6.2. Identification of boundary lines for controlled islanding as an operational mitigative action

According to the methodology presented in Section II-A, the spectral clustering-based controlled islanding is implemented as an operational mitigation strategy to further absorb cascading impacts from cyber-physical events, generated using Eq. (3). To this end, the constrained spectral clustering is applied in the segment where initiating events occur, provided that Eq. (1), which relates to the number of islands based on the number of buses and BSUs, results in a value greater than 1. Otherwise, controlled load reduction is implemented to relieve stress, such as line overloading, and to prevent cascading propagation. The constraints in the controlled islanding problem, specifically CL, encompass units and GFM-VSC-HVDCs that provide BS capability. This ensures that BS services are assigned to all islands, facilitating the restoration process for islands that may experience generation outages and blackouts. In this case, for controlled islanding, $\mathcal{S}_B$ in Eq. (5) comprises buses at both ends of the splitting boundary branches while considering only the segment where controlled islanding is required. Additionally, the ML constraint includes buses at both ends of HVDC interconnectors (B_{HVDC}) to ensure that HVDC links remain connected during controlled islanding. It also includes buses at both ends of affected elements (B_{AE}), specifically branches, to prevent those branches impacted by a replay attack from opening or becoming boundary elements, ensuring they remain enclosed within an island, as formulated in

Eq. (7). This is because power system operators cannot rely on measurement data following events that raise suspicions of cyberattacks. Instead, they can initiate mitigation strategies, such as controlled islanding around the affected elements. This helps prevent system collapse due to the spread of a severe cascading blackout while enabling direct communication between the control center and power plants or substations.

3. Results and discussion

3.1. System setup and scenario definition

The test system used in this study to demonstrate the effectiveness of the proposed methodology is the IEEE 39-bus system with a peak demand of 6195 MW. WTs, modeled as Type 4 (full-converter), account for 60 % of the total system generation and are located at Buses 30, 31, 36, 37, and 38. Considering wind turbines (WTs) as renewable energy sources in this study is due to their prominence among the most significant power electronics-interfaced technologies in modern large-scale grids. This choice is further motivated by real-world relevance in the GB and EU interconnected power systems, particularly in the North Continental countries, wind generation accounts for a substantial share of renewable energy integration and provides a practical case for illustrating the proposed methodology [30]. Moreover, HVDC links are modeled using point-to-point bipolar DC topologies, incorporating both selective GFL- and GFM-VSC functionalities. These links provide power control, voltage and frequency support, as well as black-start capabilities for DC-segmented grids with high WT penetration. Two synchronous generators, located at Bus 32 and Bus 39, are assumed to be black-start units (BSUs), in addition to VSC-HVDCs operating in GFM control mode, which also provide black-start capabilities. This setup enables system restoration during blackouts, thereby enhancing system resilience in terms of recovery and restoration. Converters of HVDC links connected to a segment of the grid with higher penetration of WTs are operated in GFM control mode to provide additional voltage and frequency support. However, the control scheme can be adjusted to provide BS services for parts of the system without any BSUs experiencing a blackout. The simulation of protective relays and controllers associated with devices in the test system, including WTs and VSC-HVDC links with GFL or GFM control functionality, is performed using built-in DSL and composite models from the DiGSILENT PowerFactory software library. Notably, Tables A1 and A2 in the Appendix present the control parameters for the HVDC systems and Type-4 WTs, respectively.

In this study, the peak load condition is used as the operating point, which subjects the system to a stressed state, particularly under contingencies. Furthermore, by incorporating multiple outage scenarios (e.g., transmission line outages under peak load), the analysis inherently accounts for a wide range of certain topological variations in system segmentation, including $N - 1$, $N - 2$, random $N - 3$, and $N - 4$ contingencies. For the network reinforcement strategy, the study applies a list of full $N - 1$, $N - 2$, 1000 random $N - 3$, and $N - 4$ contingencies of lines using Eq. (2), with $\bar{k}$ and $\bar{k}$ set to 3 and 4, respectively. For the operational mitigation strategy, the paper then conducts scenario-based studies to analyze the detailed dynamic responses of system voltage and frequency throughout the various stages of cascading failures—from initiation and propagation to eventual stabilization when the cascade halts. Two scenarios are defined and analyzed in this study to assess the cyber-physical resilience of the test power system: one involving concurrent technical failures and the other accounting for a cyberattack. The first scenario is generated using Eq. (2), with random selection emphasizing spatially correlated events resulting from critical component failures or weather-related disturbances. The second scenario, a cyberattack, is generated using Eq. (3) with $\bar{R} = 3$, targeting multiple elements in the system. These disturbances are applied to the test system at 2 s of the simulation. The scenarios are detailed as follows:

- Scenario 1 (Sc1): WT7 at Bus 36, generating 728 MW, along with Line 1–39 and Line 4–5, carrying 448.3 MW and 175.7 MW, respectively, are tripped, representing concurrent component failures in the physical layer, i.e., the power grid.
- Scenario 2 (Sc2): Line 6–11 and Transformer 6–31 are subjected to trip command attacks. Simultaneously, a replay attack is launched at Bus 6 to manipulate measurement data.

3.2. Affected elements' identification

As described in Section II-A-2, the elements affected by a cyberattack are first identified before the operational mitigation strategy is implemented. This identification involves calculating the correlation between time-series voltage signals within a moving window. Subsequently, the identified affected elements, which show distinct correlation trends compared to neighboring buses, are considered for the controlled islanding problem if a cascade is triggered. This effectively surrounds the identified affected elements with an islanded area, providing an opportunity for improved situational awareness of the power grid. This is essential as the system operator cannot rely on the measurement data and availability status of the targeted element. Therefore, by containing them within a limited area—either through DC segmentation or controlled operational strategies—the potential impacts of cascading failures are mitigated, providing more time for the implementation of appropriate security countermeasures.

Fig. 9 depicts the time-series bus voltages of the IEEE 39-bus system under line outage disturbances at 2 s of simulation. It compares the bus voltage measurements under a disturbance, shown in Fig. 9-(a), with the data manipulated by a replay attack on Bus 6, as illustrated in Fig. 9-(b). Fig. 10 shows how a distinctive trend in correlations can be identified by comparing the measurements during a disturbance, depicted in Fig. 10-(a), with the manipulated data, shown in Fig. 10-(b). As observed in Figs. 9-(a) and 10-(a), following a disturbance, all measurement data in the case of disturbance occurrence exhibit changes, and the corresponding correlations for neighboring buses follow nearly identical trends. This indicates that any bus losing correlations with other neighboring buses and exhibiting a distinctive trend, as illustrated in Fig. 10-(b), is identified as being anomalous. Similarly, in the case of fabricated trip commands, if no transients are detected from grid measurements but an element is tripped, it signifies an anomaly.

In this study, 100 test scenarios are used to evaluate the anomaly detection algorithm, consisting of 10 scenarios with anomalies and 90 scenarios without anomalies. The test results reveal that 11 scenarios are positive, with 9 scenarios classified as true positives (TP) and 2 as false positives (FP). Additionally, 89 scenarios are negative, with 88 scenarios classified as true negatives (TN) and 1 as false negative (FN). The evaluation metrics are then calculated as follows: TPR is 90 %, FPR is

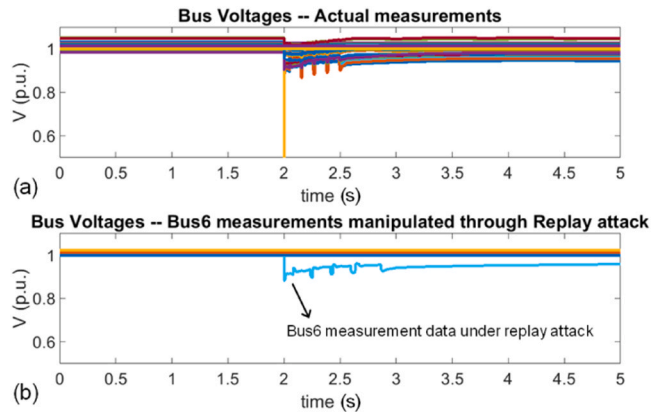


Fig. 9. Comparing the manipulated measurement data for bus voltages with the actual data.

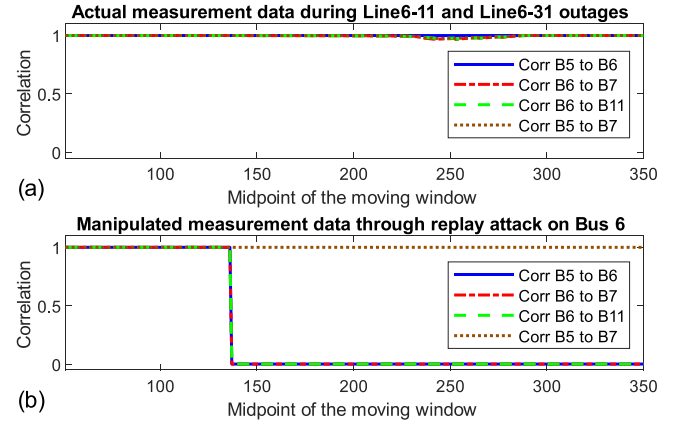


Fig. 10. Comparing the correlations between each pair of voltages for Bus 6 that are under replay attack with those of its neighboring buses.

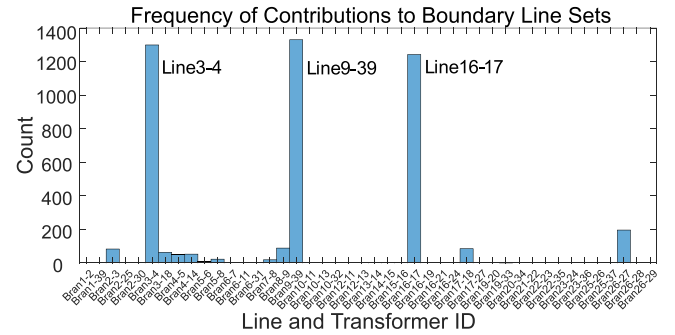


Fig. 11. Candidate AC boundary lines for DC-based segmentation.

2.2 %, TNR is 97.8 %, and FNR is 10 %. These values indicate the satisfactory performance of the algorithm, as the high TPR and TNR values, along with the low FPR and FNR values, demonstrate its effectiveness.

3.3. DC segmentation of the test system

According to the approach detailed in Section II-A and Section II-F-1, the complete set of N-1 and N-2 contingencies, along with 1000 random N-3 and N-4 contingencies of network branches generated using Monte Carlo simulations, are applied to the test system. Following this, system partitioning is performed for each individual contingency using the constrained spectral clustering technique, and the process is extended to all contingencies. The lines that most frequently contribute to the system partitioning as boundary lines are then identified. Fig. 11 presents the results of this analysis, identifying Line 3–4, Line 9–39, and Line 16–17 as the lines that most frequently contribute to the system partitioning. These lines are subsequently replaced with VSC-HVDC links, providing asynchronous interconnection between the two segments of the test system, thereby enabling distinct voltage and frequency response for segments. As shown in Fig. 11, other transmission lines also contribute to system segmentation under various stressed topological conditions. However, these lines have a less frequent contribution and are therefore not selected. Consequently, as mentioned earlier, Lines 3–4, 9–39, and 16–17 are chosen. It is worth noting that during the DC segmentation process, while identifying boundary lines and segments, the method ensures that each segment contains at least one synchronous generator (from Bus 32 and Bus 39) providing black-start (BS) capability. This is in addition to the BS capability provided by VSC-HVDC links operating in the GFM control Mode. Fig. 12 visualizes the results of the DC-segmented test system, where Lines 3–4, 9–39, and 16–17 are replaced with three point-to-point VSC-HVDC interconnectors, thereby

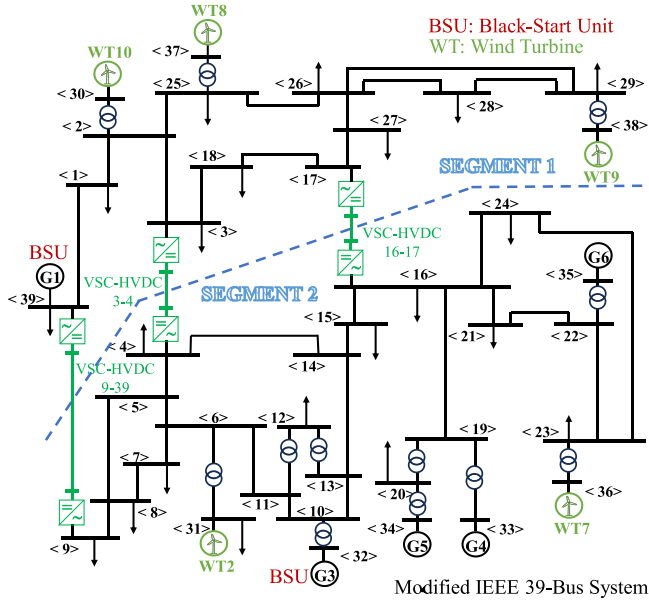


Fig. 12. IEEE 39-bus system after DC-segmentation.

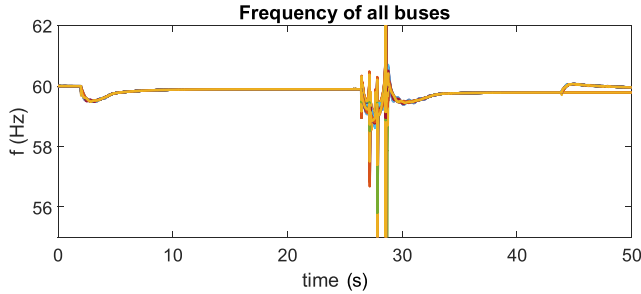


Fig. 13. Frequency response of all buses under Scenario 1 without the reinforcement strategy.

ensuring that each segment contains at least one BSU. The rated capacity of the HVDC links interconnecting Buses 9–39, 3–4, and 16–17, as described in Eq. (8), is 900 MVA, 500 MVA, and 600 MVA, respectively.

3.4. Case study applications

The study begins with Scenario 1, providing a detailed analysis of how cascading failures initiate and propagate across the system, followed by their mitigation through DC segmentation and the implementation of operational strategies. Scenario 2 is then examined in a similar manner, with both scenarios aiming to demonstrate how the system's resilience is enhanced in response to cyber-physical events.

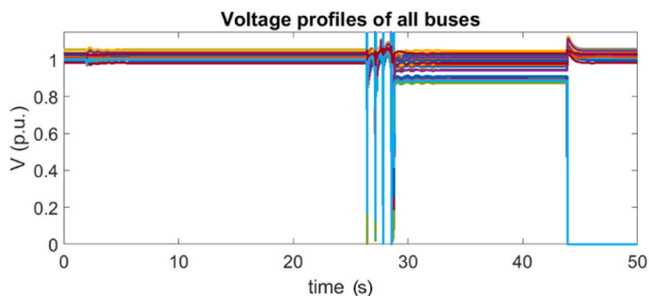


Fig. 14. Voltage profiles under Scenario 1 without the reinforcement strategy.

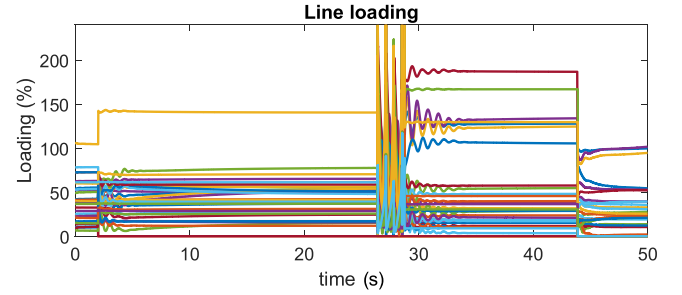


Fig. 15. Line loading under Scenario 1 without the reinforcement strategy.

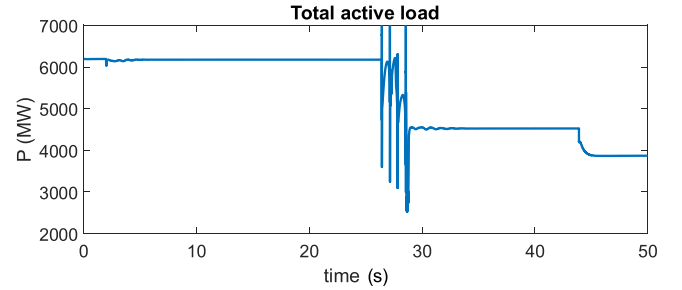


Fig. 16. System load under Scenario 1 without the reinforcement strategy.

3.4.1. Scenario 1

This scenario, Sc1, is analyzed in detail under three different cases: (i) without a reinforcement strategy, (ii) with a reinforcement strategy through DC segmentation, and (iii) with both reinforcement and operational mitigation strategies, as comprehensively described below.

• Without Reinforcement Strategy:

The test system is analyzed without the reinforcement strategy under Scenario 1. Figs. 13–16 illustrate the system's response to the disturbances in Scenario 1, capturing the dynamics of frequency, voltage, line loading, and total load, respectively, throughout the cascade initiation and propagation phases. After the occurrence of the initiating events at

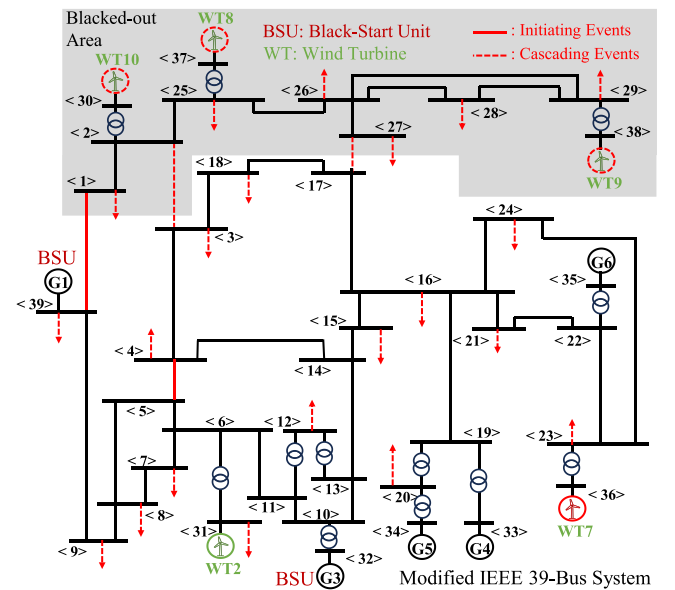


Fig. 17. Visualization of cascading propagation across the test system for Scenario 1 without the reinforcement strategy.

2 s, Line 2–3 becomes overloaded, triggering its overcurrent relay to trip at 26.4 s (see Fig. 15). This event escalates cascading failures, further aggravated by significant frequency and voltage deviations. During the transient period from 27.2 to 27.75 s, 1671 MW of load is shed across the system by protective relays for system stabilization. Subsequently, WTs at Buses 30, 37, and 38 are disconnected by their undervoltage relays at 28.8 s (see Fig. 14). At 43.9 s, Line 17–27 trips due to overloading, leading to system isolation and a partial blackout, while the remaining system stabilizes. As shown in Fig. 16, the total system load remains at 3869 MW, with 2326 MW of load shedding. Fig. 17 depicts the impacts of cascading propagation on the test system, illustrating both the initiating events and the resulting cascading failures. The portion of the system affected by the blackout is also highlighted in gray.

- With Reinforcement Strategy Only (Without Operational Mitigation Strategies):

For this part of the study, the test system is similarly analyzed under Scenario 1, with the transmission network reinforced through DC segmentation, as performed in Section III-C, to demonstrate how the resilience of the DC-segmented grid can be enhanced. Figs. 18–22 illustrate the response of the DC-segmented system to the disturbances in Scenario 1. Following the initiating events at 2 s, Line 2–3 becomes overloaded, causing its overcurrent relay to operate at 21.8 s (see Fig. 20). The converters of two HVDC links at Bus 17 and Bus 3 are tripped by their DC link protective relays at 21.85 s, causing them to fail in providing voltage and frequency support at their points of connection (POC). Fig. 21 shows the HVDCs' power flow at both-end buses. As shown in Fig. 21, the only HVDC link that remains connected at both end buses is the one between Bus 9 and Bus 39, continuously providing voltage and frequency support throughout the entire cascading failure process. This is then followed by the outage of WTs at Buses 30, 37, and 38 due to the operation of their undervoltage relays at 22 s (see Figs. 18 and 19). Immediately after the outages of these WTs, the loads in Segment 1 at Buses 1, 3, 18, 25, 26, 27, 28, and 29 are shed. Fig. 22 illustrates the total system load along with the individual segment loads. As shown, a total load shedding of 1731 MW occurs in Segment 1, while no load shedding is implemented in Segment 2. This is primarily due to the higher robustness of Segment 2, which contains four synchronous generators and two WTs, whereas Segment 1 has only one synchronous generator and three WTs.

Fig. 23 shows the impacts of cascading failures on each segment, illustrating the initiating events and the subsequent cascading failures. As highlighted in this figure, the only segment affected by cascading failures is Segment 1. Comparing the voltage and frequency responses of the two segments, the VSC-HVDC links in asynchronous interconnection result in distinct behavior of the segments. While Segment 1 experiences a blackout, highlighted in gray, Segment 2 remains unaffected, demonstrating the effectiveness of the interconnection in containing the cascading failures.

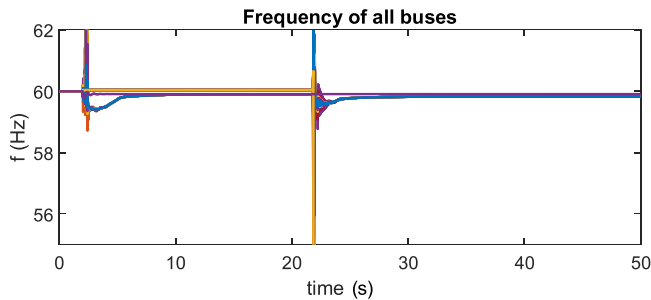


Fig. 18. Frequency response of all buses under Scenario 1 with the reinforcement strategy, specifically DC segmentation.

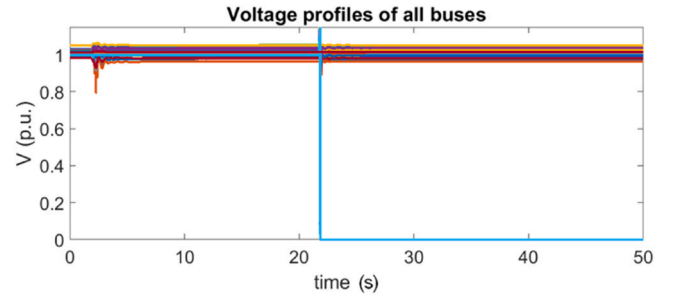


Fig. 19. Voltage profiles under Scenario 1 with the reinforcement strategy.

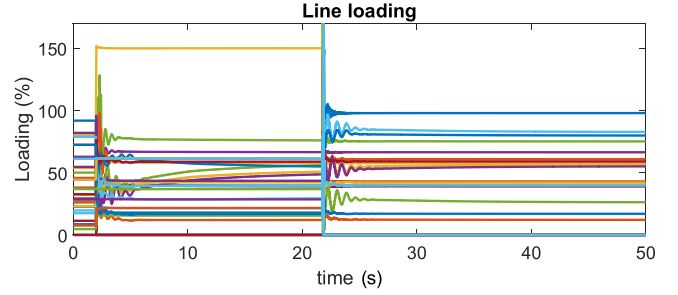


Fig. 20. Line loading under Scenario 1 with the reinforcement strategy.

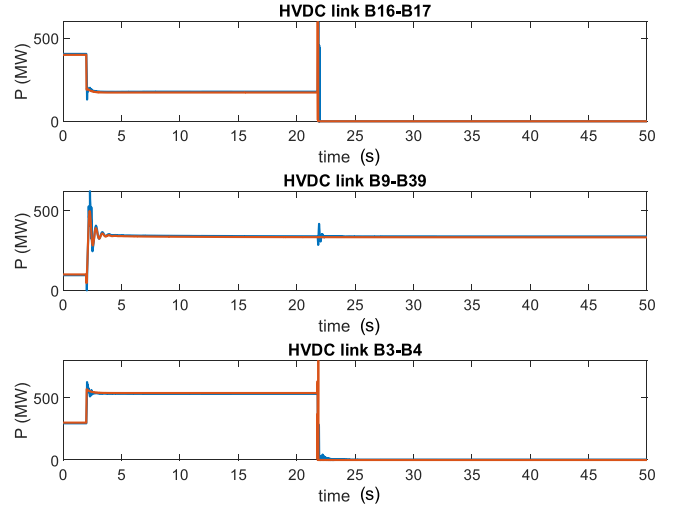


Fig. 21. HVDCs' power flow under Scenario 1 with the reinforcement strategy.

- With both reinforcement and operational mitigation strategies:

This analysis complements the previous one, i.e., "With Reinforcement Strategy Only (Without Operational Mitigation Strategies)", where controlled load reduction is implemented to alleviate AC line overloading, thus preventing the further spread of cascading failures to other parts of the system. To this end, in order to alleviate the overloading of Line 2–3, the loads at Bus 3 and Bus 4 are reduced in a controlled manner, resulting in a total reduction of 461 MW. Figs. 24–28 illustrate the response of the DC-segmented system to the disturbances in Scenario 1, with the implementation of the operational mitigation strategy, specifically controlled load shedding. As a result of the operational mitigation strategy, the impact of cascading failures is significantly reduced, with both segments remaining stabilized (see Figs. 24 and 25), and the HVDC links staying connected (see Fig. 27). Fig. 26 also shows how the loading of Line 2–3 is reduced, while all other lines operate within their rated capacity. Fig. 28 shows the total system load and also compares the

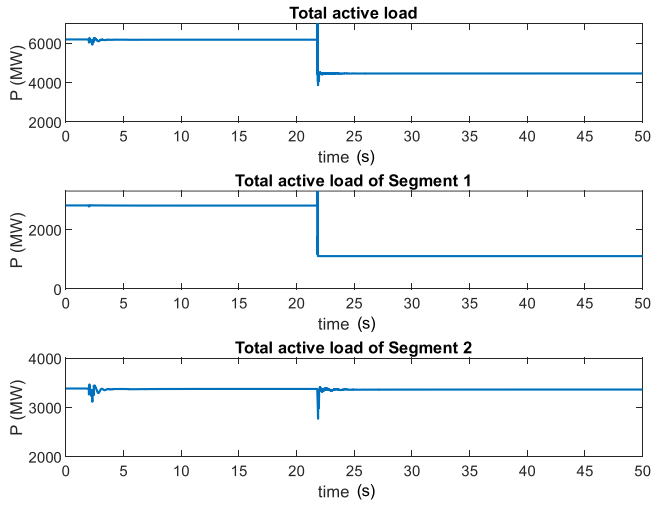


Fig. 22. System load under Scenario 1 with the reinforcement strategy.

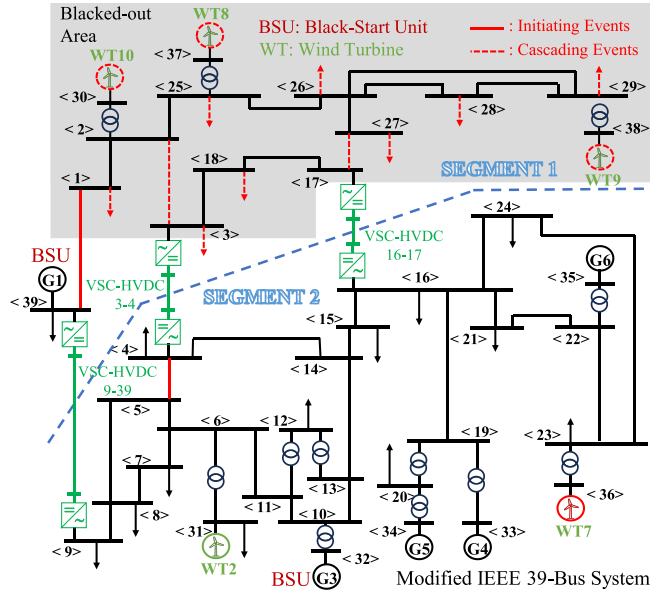


Fig. 23. IEEE 39-bus system after DC-segmentation under Scenario 1.

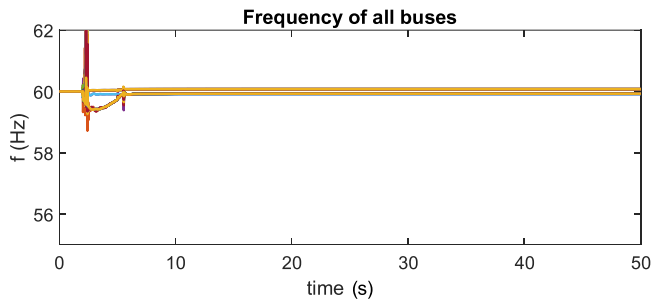


Fig. 24. Frequency response of all buses under Scenario 1 with both reinforcement and operational mitigation strategies.

load of both segments.

Moreover, Fig. 29 provides a comparison of system load amongst different cases, highlighting the influence of reinforcement and operational mitigation strategies under Scenario 1. As shown, DC segmentation improves overall system performance by reducing the lost load by

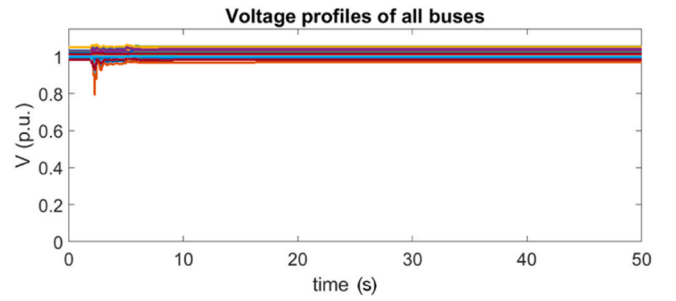


Fig. 25. Voltage profiles under Scenario 1 with both reinforcement and operational mitigation strategies.

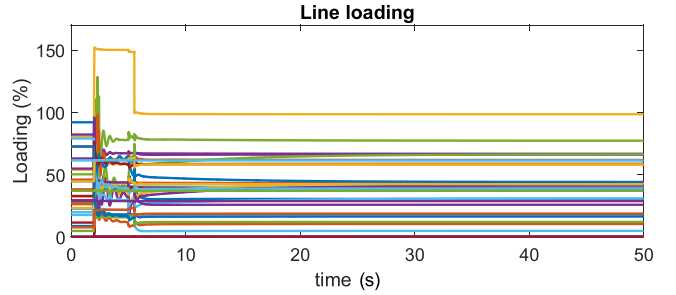


Fig. 26. Line loading under Scenario 1 with both reinforcement and operational mitigation strategies.

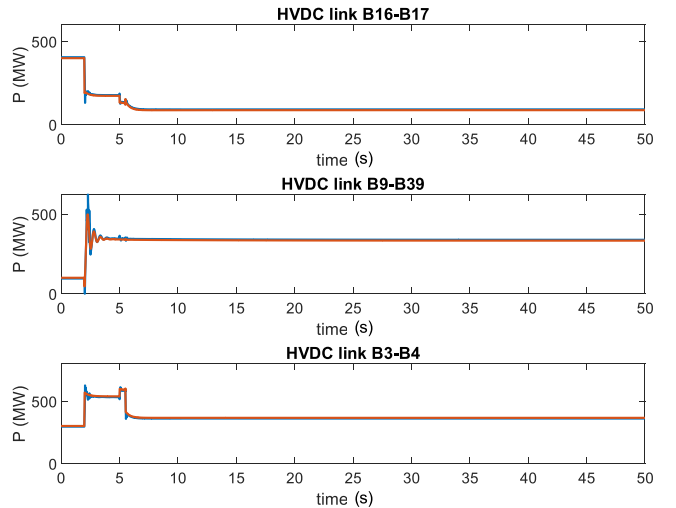


Fig. 27. HVDCs' power flow under Scenario 1 with both reinforcement and operational mitigation strategies.

595.1 MW (9.6 %), from 3869.2 to 4464.3 MW. On the other hand, with the implementation of controlled load reduction in addition to DC segmentation, the total lost load is further reduced by 1864.5 MW (30 %), from 3869.2 to 5733.7 MW. This implies that the impact of cascading failures is confined to a limited area through the implementation of DC segmentation, and can be further mitigated by controlled load reduction, which helps alleviate line overloading and stabilize the system.

3.4.2. Scenario 2

For this scenario, the same analysis as in Scenario 1 is conducted. The initiating events involve the outage of Line 6–11 and Transformer 6–31 at 2 s due to cyberattacks targeting Bus 6. However, the mitigation strategy here is based on controlled islanding rather than controlled load reduction, as the size of the grid where the initiating events originate, i.

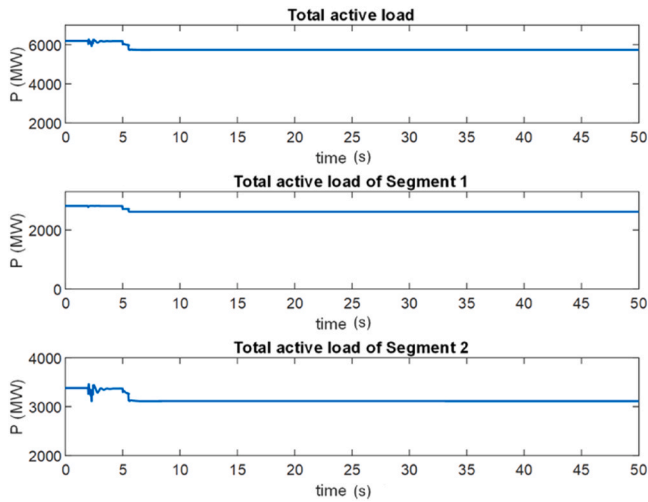


Fig. 28. System load under Scenario 1 with both reinforcement and operational mitigation strategies.

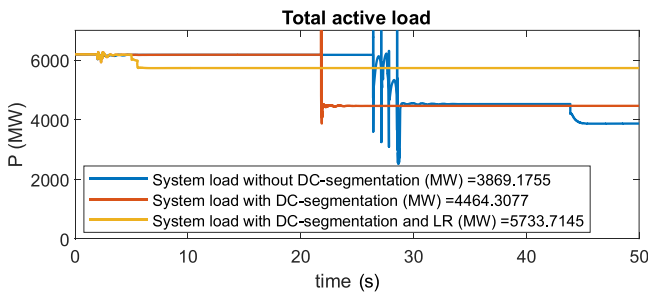


Fig. 29. Comparison of system load under Scenario 1, with and without reinforcement and mitigation strategies.

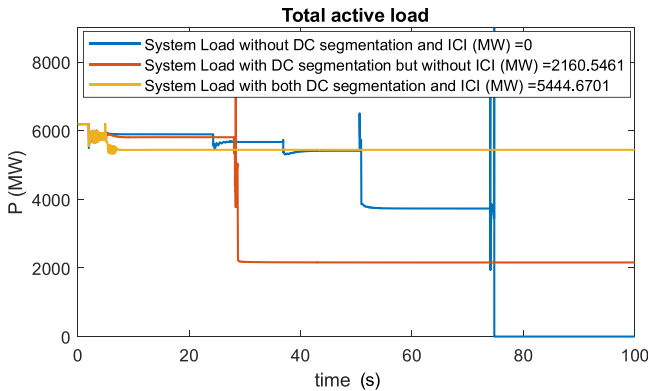


Fig. 30. Comparison of system load under Scenario 2, with and without reinforcement and mitigation strategies.

e., Segment 2, makes the islanding strategy feasible to implement. Fig. 30 shows the system load under Scenario 2 with and without reinforcement and operational mitigation strategies. The system load without reinforcement and operational mitigation strategies is zero, indicating a complete and system-wide blackout. In contrast, after implementing DC segmentation as a reinforcement strategy, the system load reaches 2160.5 MW—a 35 % improvement—following the cessation of cascading failures and system stabilization. On the other hand, when an operational strategy, specifically controlled islanding (CI), is implemented, it further enhances the process of cascade containment and absorption, resulting in the system load reaching 5444.7 MW—an

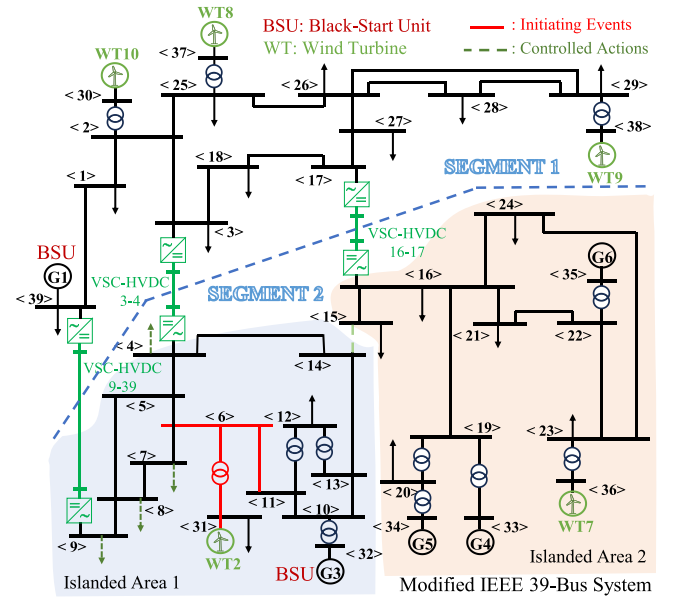


Fig. 31. IEEE 39-bus system after DC segmentation and implementing controlled islanding under Scenario 2.

Table 1
Summary of the results.

Scenario ID		Sc1	Sc2
System's served load in MW	Without DC Segmentation	3869.2	0
	With DC Segmentation but without operational mitigation	4464.3	2160.5
	With both DC Segmentation and operational mitigation	5733.7	5444.7
		[30.0]	[87.9]

88 % improvement.

It is worth noting that in this scenario, Scenario 2, the cascade initiates in Segment 2 and spreads to other parts of the system in the absence of reinforcement and operational mitigation strategies. To prevent cascading propagation, Segment 2 is divided into two islands by opening Line 14–15 as the boundary line, effectively confining the initiating events within a limited area. Additionally, a controlled load

IEEE 118-bus system with DC segmentation and controlled islanding

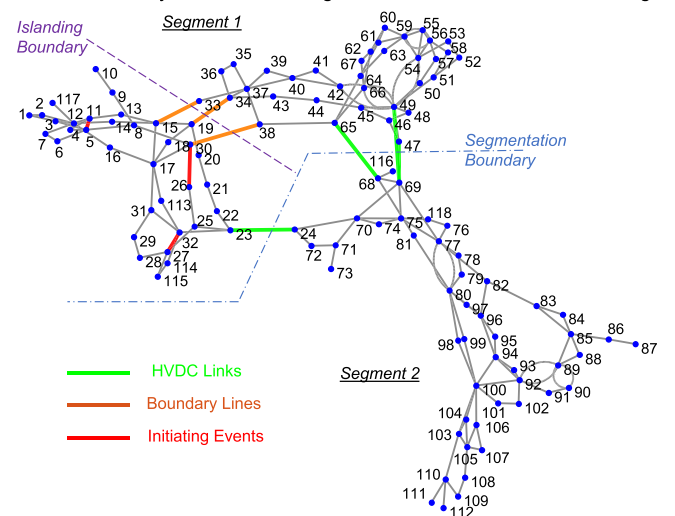


Fig. 32. The IEEE-118 bus system with HVDC links and boundary lines highlighted.

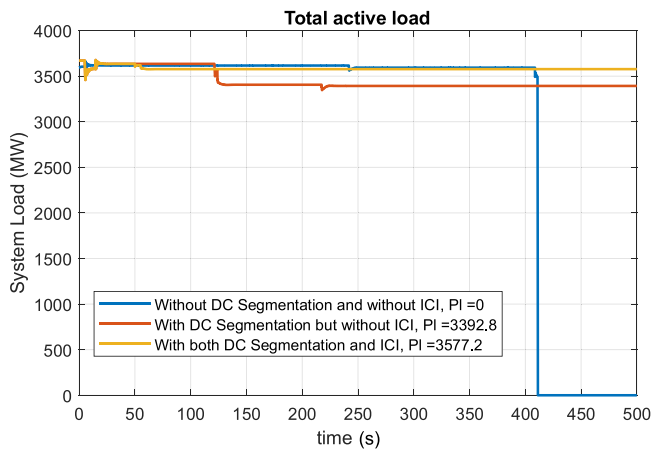


Fig. 33. Quantification and comparison of cascading impacts in the IEEE 118-bus system, with and without the proposed resilience enhancement strategy.

reduction of 750.3 MW from Buses 4, 7, 8, and 9 is implemented in Islanded Area 1 to alleviate line overloading and stabilize the island by maintaining a balance between load and generation. Fig. 31 illustrates how the operational mitigation strategy, controlled islanding in this case, is implemented to halt the spread of cascading failures. This operational strategy complements the absorption of cascading impacts in relation to the reinforcement strategy (i.e., DC segmentation) and significantly enhances cascade mitigation, thereby improving overall system resilience.

Table 1 presents a comparative summary of the results for the scenarios and case studies already analyzed, highlighting the effectiveness of the proposed resilience enhancement strategy, which improves the system's served load by up to 88 %.

Furthermore, the study is extended by applying the proposed resilience enhancement strategy to the IEEE 118-bus test system, which operates at a peak load of 3668 MW, thereby enabling an assessment of its applicability and effectiveness in a larger and more complex network. Fig. 32 illustrates the results, where the initiating events—line outages at 5–11, 26–30, and 27–32—are highlighted in red. The placement of HVDC links between bus pairs 23–24, 47–69, 49–69, and 65–68, highlighted in green, partitions the system into two DC-segmented areas. In addition, the boundary for controlled islanding in Segment 1, established by opening lines 15–33, 19–34, and 30–38, is highlighted in orange. Fig. 33 shows the time-domain simulation results for resilience quantification, expressed in terms of the total supplied system load (MW). The figure compares the cascading failure impacts in the IEEE 118-bus system under three cases: (i) without DC segmentation and intentional controlled islanding (ICI), (ii) with DC segmentation only, and (iii) with both DC segmentation and ICI implemented. The corresponding supplied load values are 0 MW, 3392.8 MW, and 3577.2 MW, respectively, demonstrating up to a 97.5 % improvement when both DC segmentation and ICI are implemented.

4. Conclusion

The paper introduces a novel resilience-oriented methodology to

enhance power grid resilience against cascading failures induced by cyber-physical events, such as fabricated protection trip commands, measurement replay attacks, and other technical disturbances in the power grid. The methodology integrates power network topology reinforcement and operational mitigation strategies to reduce the risk of widespread cascading outages in converter-dominated power grids with high penetration of wind generation. It leverages dynamic cascading failure modeling to fully capture cascade mechanisms involving system controllers and protective relays, particularly those related to converter-interfaced technologies like wind generation and HVDC links. The methodology also employs a cyber-anomaly detection technique to identify cyberattacks and affected elements while also distinguishing cyber-based disturbances from the power grid's technical disturbances. The studies are conducted for different scenarios and case studies leading to distinct cascading impacts, comparing the effects of power network topology reinforcement (DC segmentation) and operational mitigation strategies (controlled load reduction or controlled islanding). The results demonstrate that the proposed method improves the served demand by up to 88 % and 97 % for the IEEE 39-bus and 118-bus test systems, respectively, highlighting its effectiveness in mitigating cascading impacts and enhancing overall system resilience. Notably, future work will extend this study by considering a broader generation mix, including photovoltaic (PV) sources, to further enhance the applicability of the proposed methodology. In addition, the integration of a hybrid RMS–EMT co-simulation framework into cascading failure modeling and analysis for AC/DC power grids, enabling efficient device-level to system-level investigations of transient phenomena on micro-second timescales in large IBR-dominated grids, will also be explored.

CRediT authorship contribution statement

Sina Hashemi: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Data curation, Conceptualization. **Rajkumar Vetrivel S:** Writing – review & editing, Validation, Methodology. **Alexandru Ștefanov:** Writing – review & editing, Validation, Investigation. **Mathaios Panteli:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Investigation, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was funded by the Horizon Europe program through the projects “HVDC-based Grid Architectures for Reliable and Resilient WideSprEad Hybrid AC/DC Transmission Systems” (HVDC-WISE) (Grant Agreement No. 101075424) and “Pan-European Interoperable AC-DC Hybrid Electricity Networks” (HYNET) (Grant Agreement No. 101172757).

Appendix

Tables A1 and A2 provide the control parameters for the HVDC systems and Type-4 WTs, respectively [31,32].

Table A1
HVDC control parameters

Parameter	Value
AC voltage reference (V_0)	1.01 p.u.
AC voltage droop gain (K_v)	5 % p.u.
DC voltage reference (V_{dc0})	1 p.u.
DC voltage droop gain (K_{dc})	2 % p.u.
Frequency droop gain (K_f)	5 % Hz/p.u.
Frequency reference (f_n)	60 Hz

Table A2
WT Type-4 control parameters

Parameter	Value
Maximum active current ramp rate (dipmax)	1.5 Ibse/s
Voltage scaling factor for FRT current (K_{qv})	2.0 Ib/U _b
Voltage dip threshold for P control (U _{dip})	0.85 pu
Voltage threshold for UVRT detection in Q control (U _{dip})	0.9 pu
Voltage threshold for OVRT detection in Q control (U _{grise})	1.1 pu
Over-voltage protection trip threshold (U _{over})	1.4 pu
Under-voltage protection trip threshold (U _{under})	0.8 pu
Over-frequency protection trip threshold (f _{over})	1.04 pu
Under-frequency protection trip threshold (f _{under})	0.94 pu

Data availability

Data will be made available on request.

References

- [1] V.S. Rajkumar, A. Stefanov, A. Presekal, P. Palensky, J.L.R. Torres, Cyber attacks on power grids: causes and propagation of cascading failures (no. September), IEEE Access 11 (2023) 103154–103176.
- [2] S. Vahidi, et al., Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: a survey on challenges and opportunities, IEEE Commun. Surv. Tutor. 25 (2) (2023) 1294–1335.
- [3] C. Luo, L. Liang, X. Bai, Review of HVDC systems for enhancing resilience after extreme natural events (vol), J. Eng. 2021 (11) (2021) 653–664.
- [4] D. Gomila, B.A. Carreras, J.M. Reynolds-Barredo, P. Colet, O. Gomis-Bellmunt, Analysis of the blackout risk reduction when segmenting large power systems using lines with controllable power flow, no. June 2022, Int. J. Electr. Power Energy Syst. 148 (2023) 108947.
- [5] M. Callaviik, Grid resilience by power electronics: use subtransmission HVDC interties for novel emergency power control of split networks [Expert View, IEEE Power Electron. Mag. 5 (1) (2018) 54–56.
- [6] M. Robin, J. Renedo, J.C. Gonzalez-Torres, A. Garcia-Cerrada, A. Benchaib, P. Garcia-Gonzalez, An algorithm for DC segmentation of AC power systems to mitigate electromechanical oscillations, IEEE Access 11 (2023) 64651–64667.
- [7] J. Renedo, A. Garcia-Cerrada, L. Rouco, Active power control strategies for transient stability enhancement of AC/DC grids with VSC-HVDC multi-terminal systems, IEEE Trans. Power Syst. 31 (6) (2016) 4595–4604.
- [8] M. Robin, et al., Addressing intra-area oscillations and frequency stability after DC segmentation of a large AC power system, Int. J. Electr. Power Energy Syst. 165 (2025) 1–11.
- [9] S. Pirooz Azad, R. Iravani, J.E. Tate, Stability enhancement of a DC-segmented AC power system, IEEE Trans. Power Deliv. 30 (2) (2015) 737–745.
- [10] G.J.C. Santos, P.R. da Silva Jota, HVDC grid segmentation analysis for blackouts reduction, J. Power Energy Eng. 05 (03) (2017) 36–48.
- [11] Z. Wang, Z. Wang, A novel preventive islanding scheme of power system under extreme typhoon events, no. September 2022, Int. J. Electr. Power Energy Syst. 147 (2023) 108857.
- [12] S. Ranjbar, “Online estimation of controlled islanding time intervals using dynamic state trajectories through cascading failures from WAMS data,” Electr. Power Syst. Res., vol. 214, no. PA, p. 108890, 2023.
- [13] S. Hashemi, M. Panteli, V.S. Rajkumar, A. Stefanov, Operational mitigation of cyberattack-induced cascading failures in power systems, 2024 Int. Conf. Smart Energy Syst. Technol. Driv. Adv. Futur. Electr. SEST 2024 Proc. (2024) 1–6.
- [14] L. Ding, Y. Guo, P. Wall, Performance and suitability assessment of controlled islanding methods for online WAMPAC application, Int. J. Electr. Power Energy Syst. 84 (2017) 252–260.
- [15] U.S. Department of Energy, “Developing and demonstrating tools to monitor and control the grid with advanced analysis, visualization, and situational awareness tools,” 2012. [Online]. Available: [https://www.energy.gov/sites/prod/files/Advanced Applications Development Program Factsheet.pdf?utm_source=](https://www.energy.gov/sites/prod/files/Advanced%20Applications%20Development%20Program%20Factsheet.pdf?utm_source=)
- [16] S. Danifar, F. Aminifar, H. Lesani, Optimal controlled-islanding with AC power flow constraints: A benders-decomposition approach, no. August 2022, Electr. Power Syst. Res. 216 (2023) 108970.
- [17] X. Mao, W. Zhu, L. Wu, B. Zhou, Comparative study on methods for computing electrical distance, no. February 2020, Int. J. Electr. Power Energy Syst. 130 (2021) 106923.
- [18] B.A. Bastiani, R.V. de Oliveira, Frequency dynamics of power systems with inertial response support from wind generation, Energies 16 (14) (2023) 1–21.
- [19] L.A.M. Lima, E.H. Watanabe, Hybrid control scheme for VSC presenting both grid-forming and grid-following capabilities, IEEE Trans. Power Deliv. 37 (6) (2022) 4570–4581.
- [20] B. Bahrani, et al., Grid-forming inverter-based resource research landscape: understanding the key assets for renewable-rich power systems, IEEE Power Energy Mag. 22 (2) (2024) 18–29.
- [21] J. Sakhnini, H. Karimipour, A. Dehghantanha, R.M. Parizi, Physical layer attack identification and localization in cyber-physical grid: an ensemble deep learning based approach, Phys. Commun. 47 (2021) 101394.
- [22] K. Lai, et al., A robust energy storage system siting strategy considering physical attacks to transmission lines, 2018 North Am. Power Symp. NAPS 2018 (2018) 1–6.
- [23] Y. Dai, M. Panteli, and R. Preece, “Python Scripting for DiGSILENT PowerFactory: Enhancing Dynamic Modelling of Cascading Failures,” 2021.
- [24] Y. Dai, M. Noebels, M. Panteli, R. Preece (no. Irep), 11th Bulk Power Syst. Dyn. Control Symp. (IREP 2022) (2022) 1–10.
- [25] OPAL-RT, “RMS vs EMT simulation for IBRs explained for power system engineers,” 2025. (<https://www.opal-rt.com/blog/rms-vs-emt-simulation-for-ibrs-explained-power-system-engineers/>).
- [26] S. Hashemi, M. Asprou, L. Hadjidemetriou, M. Panteli, Quantifying and mitigating cascading impacts in hvdc-interconnected power grids, IEEE Access 13 (2025) 154491–154507.
- [27] K. Chatterjee, S.A. Khaparde, Data-driven online detection of replay attacks on wide-area measurement systems, 2018 20th Natl. Power Syst. Conf. NPSC 2018 (2018) 1–6.
- [28] A. Esmailian, M. Kezunovic, Prevention of power grid blackouts using intentional islanding scheme, IEEE Trans. Ind. Appl. 53 (1) (2017) 622–629.
- [29] X. Wang, B. Qian, I. Davidson, On constrained spectral clustering and its applications, Data Min. Knowl. Discov. 28 (1) (2014) 1–30.
- [30] Eurostat, “Share of electricity from renewables falls in early 2025,” Eurostat News article, 2025. (<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250619-2>) (accessed Sep. 9, 2025).
- [31] DiGSILENT GmbH, PowerFactory 2023 Technical Reference, Gomaringen, Germany, 2023.
- [32] P. Sorensen, B. Andresen, J. Fortmann, P. Pourbeik, Modular structure of wind turbine models in IEC 61400-27-1, IEEE Power Energy Soc. Gen. Meet. (2013) 1–5.