energies

MDPI

Article

Assessing Critical Edges in Cyber-Physical Power Systems Using Complex Network Theory: A Real-World Case Study

Mehdi Doostinia and Davide Falabretti *

Electrical Engineering, Department of Energy, Politecnico di Milano, 20156 Milan, Italy; mehdi.doostinia@polimi.it

* Correspondence: davide.falabretti@polimi.it

Abstract

Cyber-physical power systems (CPPSs) are increasingly vital to the reliable and resilient operation of modern electricity infrastructure. Within these systems, both physical components—such as power substations and lines—and cyber components—such as communication links, mobile base stations, and controllers—are interdependent, making the identification of critical elements essential for improving system robustness. While prior research has largely focused on node-level analysis, this study addresses the underexplored challenge of identifying critical edges using tools from complex network theory. We evaluate edge importance through edge betweenness centrality (EBC) and edge removal analysis (ERA) across a real-world CPPS located in Northeastern Italy. Three network scenarios are analyzed: a directed power network, an undirected power network, and an undirected cyber network. Nearly 10 percent of the important edges, based on the EBC and ERA methods, are discussed. A Pearson correlation is considered to find the correlation between the results of the two methods. The findings can support distribution system operators in prioritizing infrastructure hardening and enhancing resilience against both physical failures and cyber threats.

Keywords: cyber-physical power systems (CPPSs); edge betweenness centrality; edge removal analysis; complex networks; vulnerability assessment; power grid resilience

Academic Editor: Chong Wang

Received: 4 August 2025
Revised: 28 August 2025
Accepted: 5 September 2025
Published: 9 September 2025

Citation: Doostinia, M.; Falabretti, D. Assessing Critical Edges in Cyber-Physical Power Systems Using Complex Network Theory: A Real-World Case Study. *Energies* **2025**, *18*, 4803. https://doi.org/10.3390/en18184803

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

1. Introduction

Over recent decades, the development and integration of essential physical infrastructures—such as electrical grids, transportation frameworks, and communication networks—have been significantly accelerated by technological advancements. Increasingly, these traditionally isolated systems are being coupled with computational intelligence and control functionalities, forming what are now widely known as cyber-physical systems (CPSs). First introduced in the early 2000s, CPSs represent a paradigm shift in how modern infrastructure is designed, monitored, and managed [1].

This convergence between physical operations and digital technologies—driven by the proliferation of sensors, communication protocols, and embedded systems—has transformed key sectors, including energy, healthcare, and mobility [2]. By integrating Information and Communication Technology (ICT) into physical systems, CPSs enable greater automation, real-time monitoring, and decision-making capabilities [3]. Among the most impactful applications of CPSs is in the energy sector, where their principles have given rise to cyber-physical power systems (CPPSs)—an evolution of conventional power grids that incorporates advanced communication, sensing, and control tools [4].

CPPSs are now recognized as a cornerstone of the broader CPS ecosystem and form the technological backbone of modern power distribution systems [5,6]. They support the secure, efficient, and intelligent operation of electrical infrastructure by enabling real-time data exchange between physical devices (e.g., substations, transformers) and cyber entities (e.g., control centers, sensors). With the increasing digitization of the energy grid, ensuring the resilience and reliability of CPPSs against disturbances has become a critical priority. Effective resilience strategies must address not only physical failures—such as equipment faults or natural disasters—but also cyber vulnerabilities, such as data loss or targeted attacks.

A defining feature of CPPSs is the mutual dependence between their power and cyber layers. The ICT components rely on the power infrastructure for energy supply, while the electrical system depends on the cyber layer for command execution, control actions, and system monitoring [7,8]. This interdependence introduces additional complexity, as failures in one layer can propagate to the other, increasing the risk of cascading failures and widespread outages. In this context, enhancing CPPS resilience requires a comprehensive understanding of system vulnerabilities at both the node and edge levels [9,10].

Identifying critical components within these systems is key to pinpointing vulnerabilities and implementing strategies to enhance system robustness, particularly during disruptive events that affect these crucial components. This approach ensures the continued operation of essential services and improves resilience against cascading failures [11].

Although significant research has focused on identifying critical nodes within these networks, comparatively less attention has been paid to the role of edges—such as power lines and communication links—which serve as the conduits of power and information. The failure of a single edge can isolate multiple nodes or disrupt control communication, leading to serious operational consequences.

To evaluate such vulnerabilities, complex network (CN) theory offers a robust modeling framework. CN theory treats infrastructure systems as graphs, where nodes represent system elements (e.g., substations, routers), and edges denote connections (e.g., power lines, fiber links). Complex network (CN) theory is one of the most effective methods to model CPPSs because it captures interdependencies, identifies critical nodes, and assesses vulnerabilities, ultimately improving system resilience [12,13].

Within this framework, centrality metrics are commonly used to rank the importance of network components based on their topological roles [14–16]. Among edge centrality measures, edge betweenness centrality (EBC) has gained prominence. It quantifies the influence of an edge by measuring the number of shortest paths passing through it [17]. High-EBC edges are considered structurally critical because their failure can significantly disrupt the connectivity or operational flow of the system.

To complement EBC, edge removal analysis (ERA) assesses the functional impact of removing an edge. This method evaluates system performance degradation, such as disconnection of nodes or loss of communication paths, when a specific edge fails. Together, EBC and ERA provide both topological and operational perspectives for identifying critical edges in CPPSs.

1.1. Related Works

Some studies have employed physics-based N-1 contingency simulations to identify critical components, where each single line or substation outage is evaluated under defined operating points to assess impacts on power flow, voltage/security margins, and potential cascading effects [18]. While such approaches are valuable, they rely on detailed electrical and protection parameters. In CPPS contexts, the need for credible models of communication latency, control logic, and reliability makes these methods computationally intensive

and data-demanding at scale. In this paper, we position our edge-centric EBC+ERA framework as a complementary, data-light screening stage that rapidly narrows the contingency space, thereby balancing scalability with modeling fidelity in real CPPSs.

Various studies have considered centrality metrics for power systems and CPPSs to identify critical components. The researchers in [19] utilized complex network theory to simulate the interaction between power and ICT infrastructures using a synthetic IEEE 30-bus benchmark system. They evaluated system vulnerability by employing centrality indicators—specifically degree, closeness, and betweenness—to establish a ranking of node significance. Nevertheless, the authors did not evaluate the important edges, just focusing on the nodes, and the study's scope is constrained by its reliance on IEEE-standardized test systems.

In [20], the authors applied betweenness centrality, degree centrality, and clustering coefficients to identify vulnerable nodes within a power grid integrating renewable energy sources. Their analysis focused on the electrical layer of the IEEE 118-bus system, without addressing vulnerabilities in the cyber infrastructure. Additionally, the study did not consider edge vulnerabilities in the case study.

Similarly, [21] examined clustering coefficient, degree centrality, and eigenvector centrality metrics to identify critical nodes in power systems, applying their methodology to the IEEE 5-bus and 57-bus case studies. However, the study neither incorporated a critical node assessment for the ICT layer nor considered the evaluation of edge importance.

In [22], complex network theory was utilized to model and assess the vulnerability of the Nordic transmission grid, identifying important nodes using betweenness, degree, and clustering coefficient. However, the research lacks critical edge analysis and does not consider the important evaluation of the cyber layer.

The study in [23] employed betweenness centrality to identify vulnerable transmission lines in a power grid exposed to wildfire risks, demonstrating BC's effectiveness in pinpointing lines whose failure could isolate entire communities and compromise grid resilience. However, the authors focused solely on the power network and did not evaluate critical edges within the cyber layer.

In [24], the authors used betweenness and closeness centrality metrics along with clustering coefficient to determine the optimal placement of microgrids in a modified IEEE 30-bus case study. However, the study did not include modeling or evaluation of the cyber layer and no consideration of critical edges.

In [25], the researchers applied betweenness centrality to assess the significance of nodes by evaluating the number of shortest paths that traverse each node. Nodes with high BC were identified as essential for maintaining network connectivity, and their failure could severely impact power flow within the real-world isolated distribution grid of Cordova, Alaska. Nonetheless, the study relied exclusively on BC, without exploring alternative centrality measures or incorporating ICT components.

However, most existing studies focus on node-level vulnerability assessments, while edge-level evaluations remain relatively underexplored. Yet edge failures—such as a downed power line during a storm or a compromised communication link due to a cyberattack—can be equally disruptive. Furthermore, the majority of prior research focuses solely on the power network, often neglecting the cyber network, or relies exclusively on IEEE benchmark systems, which may not fully reflect the structural and geographical complexities of real-world CPPSs.

1.2. Contributions

Table 1 compares the related works discussed earlier with the approach presented in this paper. While existing studies offer valuable insights, they primarily focus on node

importance evaluation and tend to overlook the critical role of edge analysis. Additionally, many rely on IEEE standard test cases, which fail to capture the complexity of real-world cyber-physical power systems (CPPSs), especially at large scales or when accounting for interdependence with ICT networks. The ICT layer significantly influences system operations but is frequently neglected in favor of analyzing only the power network. Only a few studies have modeled real distribution grids with integrated ICT components. This reveals a clear gap in the literature regarding the analysis of large-scale, interconnected CPPSs.

Table 1. Comparison of related works on CPPS vulnerability analysis using centrality metrics with this paper.

Ref.	Case Study	Real Net.	Power Layer	ICT Layer	Node/Edge Important Evaluation	Limitations
[19]	IEEE 30-bus	–	✓	✓	Node	- Focusing on just IEEE standards and not real case studies. Not considering the important evaluation of edges.
[20]	IEEE 118-bus	–	✓	–	Node	- Focusing on just IEEE standards and not real case studies. Not considering the important evaluation of edges. Focusing on just power layer and ignoring the ICT layer.
[21]	IEEE 5/57-bus	–	✓	–	Node	- Focusing on just IEEE standards and not real case studies. Not considering the important evaluation of edges. Focusing on just power layer and ignoring the ICT layer.
[22]	Nordic grid	✓	✓	–	Node	- Not considering the important evaluation of edges. Focusing on just power layer and ignoring the ICT layer.
[23]	Real grid (wildfire)	✓	✓	–	Edge	- Focusing on just power layer and ignoring the ICT layer.
[24]	Mod. IEEE 30-bus	–	✓	–	Node	- Focusing on just IEEE standards and not real case studies. Not considering the important evaluation of edges. Focusing on just power layer and ignoring the ICT layer.
[25]	Cordova, Alaska	✓	✓	–	Node	- Focusing on just power layer and ignoring the ICT layer.
The presented paper	A real Italian grid	✓	✓	✓	Edge	–

This study fills this gap in the literature by offering a comprehensive edge-level vulnerability analysis of cyber-physical power systems. The key contributions are as follows.

- Edge-centric vulnerability analysis using EBC and ERA methods: The EBC method is used to structurally identify critical edges, while the ERA method identifies functionally critical edges in the CPPS. Together, they offer a more nuanced perspective.
- Integrated multi-layer modeling with real-world data: We model three network configurations—directed power, undirected power, and undirected cyber layers—using detailed geographical and topological data from Northeastern Italy to realistically capture the interdependencies and complexity of actual CPPSs.

- Practical insights for resilience planning: Our results reveal edge-level vulnerabilities across both power and cyber layers, providing actionable insights for distribution system operators (DSOs) to enhance resilience and operational security in large-scale distribution networks.

1.3. Structure of the Paper

The rest of the paper is organized as follows: Section 2 discusses the methodology, including graph modeling for CPPSs, definitions of edge betweenness centrality, and edge removal analysis. Section 3 describes the real-world case study and its graph modeling. Section 4 presents and discusses the simulation results across three scenarios. Finally, Section 5 concludes the study.

2. Methodology

2.1. Graph-Theoretic Modeling of CPPSs

One of the most effective frameworks for modeling and analyzing cyber-physical power systems (CPPSs) is graph theory, a branch of complex network theory [2]. A graph is defined as $G(V, E)$, where $V = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes (e.g., substations or routers), and E is the set of edges representing physical or communication links [26–28].

In this paper, we model the CPPS as two separate graphs: $G_{\text{Power}}(V_P, E_P)$ for the power layer and $G_{\text{Cyber}}(V_C, E_C)$ for the cyber layer. In G_{Power}, the node set $V_P = \{v_{p1}, v_{p2}, \ldots, v_{pn}\}$ represents the power substations, and the edge set E_P corresponds to the power transmission lines. Likewise, in G_{Cyber}, the node set $V_C = \{v_{c1}, v_{c2}, \ldots, v_{cn}\}$ represents communication elements such as routers or controllers, and E_C denotes the communication links connecting these components. This dual-layer modeling enables the independent analysis of each subsystem while capturing their interdependencies.

A general graph modeling of a CPPS is shown in Figure 1, in which the cyber layer, or the ICT network, consists of a control center responsible for overseeing and regulating the power network. This is achieved by collecting real-time feedback signals from various nodes across the system and dispatching appropriate control commands to ensure stable and efficient operation. The intermediate cyber nodes are the mobile base stations (MBSs), which serve as communication relays, enabling data transmission between remote field devices and the control center. The end nodes are the remote terminal units (RTUs), which interface directly with physical equipment in the power substations, gathering sensor data and executing control actions. The ICT links are also modeled without considering latency or packet loss, which simplifies the analysis but captures connectivity and structural dependencies.

On the other hand, the physical power network comprises power substations, which house transformers, switchgear, and protection systems, as well as power lines that provide the electrical connectivity between them. The integration of the cyber and physical layers enables real-time monitoring, adaptive control, fault detection, and self-healing capabilities within the smart grid infrastructure.

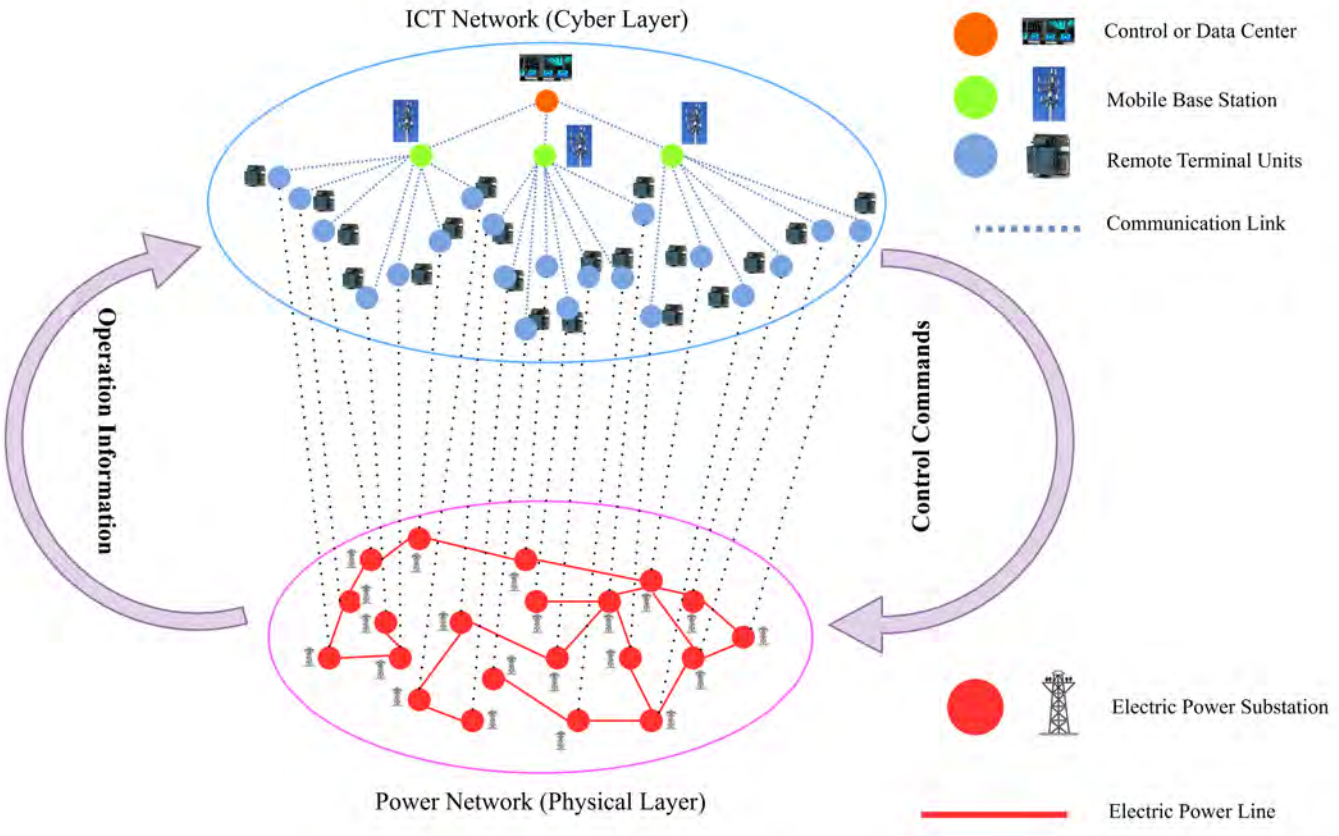

Figure 1. General graph modeling of CPPSs.

2.2. Edge Betweenness Centrality

Edge betweenness centrality (EBC) is a fundamental metric in complex network (CN) theory that quantifies the structural importance of an edge within a graph. Specifically, it measures how frequently an edge appears on the shortest paths between all pairs of nodes. In the context of CPPSs, an edge with high EBC often acts as a communication or power transmission bottleneck—meaning that its failure can critically impair the overall connectivity or operability of the network.

Mathematically, EBC for an edge h is defined as [17]:

$$EBC(h) = \sum_{i \neq j \in V} \frac{\sigma_{ij}(h)}{\sigma_{ij}}, \tag{1}$$

where σ_{ij} denotes the total number of shortest paths between nodes i and j, and $\sigma_{ij}(h)$ represents the number of those paths that pass through edge h.

This metric helps identify transmission lines or communication links whose failure would reroute a large volume of traffic or control signals, increasing the operational burden on alternative paths. As such, EBC is particularly useful in identifying structurally critical edges that might serve as failure points in either the cyber or physical layers of CPPSs.

2.3. Edge Removal Analysis

While centrality metrics like EBC offer topological insights, they may not fully capture the operational consequences of component failures. To address this, edge removal analysis (ERA) evaluates the impact of individual edge failures on the continuity of supply in CPPSs. This analysis is particularly relevant in assessing the functional resilience of the system beyond its structural layout.

In this method, each edge is temporarily removed to simulate a fault or physical disconnection. The resulting topology is then examined to determine how many nodes remain connected to the main power supply. This allows the identification of edges whose failure would isolate a significant portion of the network.

To maintain analytical simplicity and consistency with centrality-based assessments, it is assumed that each node serves an equal number of users. Although this does not capture demand variability, it provides a useful first-order approximation of edge criticality.

The procedure is outlined in Algorithm 1. The process iterates through all edges in the network, allowing for a ranked comparison of their operational significance.

Algorithm 1: Edge Removal Analysis

for each Edge in the network **do**

1. Remove the edge from the network
2. Calculate the number of nodes still supplied
3. Restore the removed edge back into the network
4. Proceed to remove the next edge in the network

This approach complements EBC by providing a functional perspective on network vulnerability. Together, ERA and EBC enable a more holistic identification of critical edges in CPPSs, supporting more informed resilience planning. In other words, in this study, both EBC and ERA are specifically adapted to capture the interdependencies of CPPSs. While EBC traditionally provides a topological measure of edge importance, here it is applied separately on the power and cyber layers to highlight structural bottlenecks in electrical flows and telemetry/command routing, respectively. ERA is then extended beyond a purely topological interpretation by incorporating the functional dependency between layers: a power node is considered operational only if it remains electrically supplied and cyber-reachable. This dual constraint ensures that the evaluation reflects realistic CPPS operation, where a failure in the cyber layer (e.g., loss of control signals) can disable power delivery even if physical connectivity is intact, and vice versa. By considering structural (EBC) and functional (ERA) perspectives under these interdependent rules, the proposed methodology identifies critical edges that cannot be detected by conventional single-layer analysis. This adaptation directly addresses the unique characteristics of CPPSs.

This uniform demand assumption treats each node as serving an identical number of users—a simplification that enables scalable, topology-focused benchmarking of resilience. While real load profiles could alter criticality rankings, this approach provides a foundational vulnerability baseline aligned with DSO outage indices.

To assess edge criticality, this paper focuses on edge betweenness centrality (EBC) and edge disruption impact (ERA) as complementary metrics. EBC captures structural importance by quantifying shortest-path dependencies, while ERA evaluates functional impact on system performance, directly linking to operational resilience indicators. This dual perspective—structural and functional—reflects topological-functional synergy, aligning with CPPS resilience objectives. EBC and ERA were, therefore, selected for their combination of methodological relevance, computational efficiency, and practical applicability.

3. Case Study

The case study presented in this research examines a real-world power distribution network located in Northeastern Italy, which incorporates a realistic ICT layer constructed using publicly accessible data, as depicted in Figure 2. Even if operated radially, this power distribution network features a meshed topology, in line with the methods currently employed by DSOs, aiming to improve reliability and service continuity through mesh

grids that enable counterfeeding. The medium-voltage network is connected to the transmission system via a high-voltage/medium-voltage substation and includes 154 secondary substations (or power nodes) along with 158 power lines. The ICT infrastructure comprises 154 remote terminal units (RTUs), each assigned to a power node, and 14 mobile base stations (MBSs) linked to the central data control facility.

In Figure 2, the power nodes, RTUs, and power lines are represented by red nodes and edges, with each power node being equipped with an RTU. Grid operators use these RTUs to oversee control and protection systems at secondary substations and gather essential measurements and data for the grid's state estimation. The blue nodes represent the mobile base stations (MBSs), which are placed at the center of circles around a 2 km radius and connect to RTUs within these zones. Additionally, extra MBSs are deployed in urban areas to enhance system performance.

Figure 3 illustrates the graph network representation of the CPPS. In this model, each power station or electrical node is represented as a node in the graph, while each power line is depicted as an edge, forming the graph of the power distribution system. For the ICT network, nodes represent the RTUs, MBSs, and the data center, and edges represent the communication links between them, creating the cyber network graph. The nodes are placed based on the exact geographical coordinates (latitude and longitude) of real-world CPPS. The graph shows orange nodes and edges corresponding to the power network, while purple nodes represent the MBSs. Node 29 in the power network graph is the connection point to the high-voltage system (i.e., the primary substation). In the ICT network graph, each MBS connects to nearby RTUs, and the MBSs are interconnected with each other and the data center. The ICT network functions as a bidirectional graph, facilitating the transmission of control signals and receiving feedback for power network monitoring. The electrical connections required to power ICT devices are excluded from this system, making it applicable for short-term power outages, where ICT equipment continues to operate on backup power. In the case study's graph modeling, all edges in both the power and communication networks were considered uniform (unweighted), emphasizing the structural characteristics of vulnerability instead of the dynamic electrical or communication parameters. Nevertheless, the proposed approach remains adaptable and can be expanded to include weighted edges. The system is designed and simulated using the open-source programming language Python 3.11 with NetworkX library.

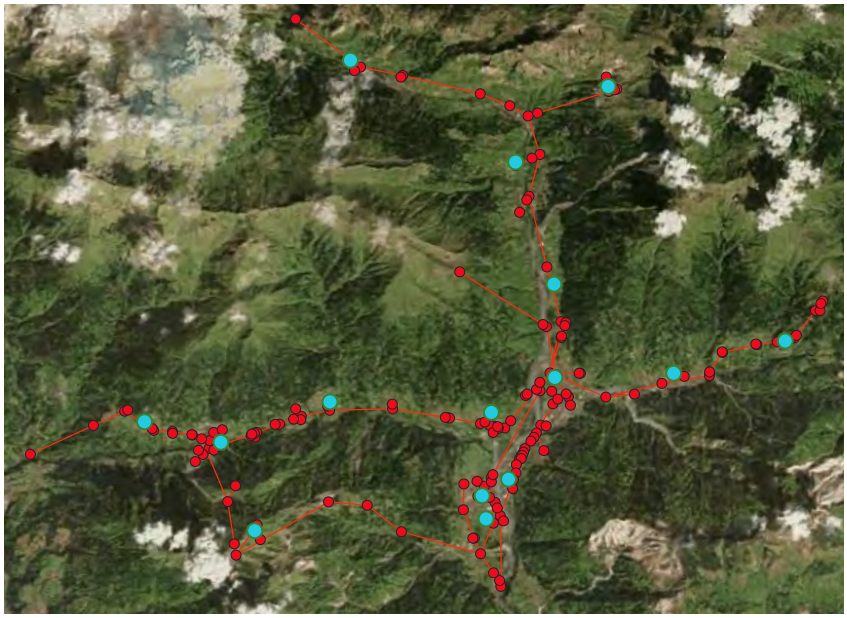

Figure 2. Case study (red nodes are power nodes and RTUs; blue nodes are MBSs).

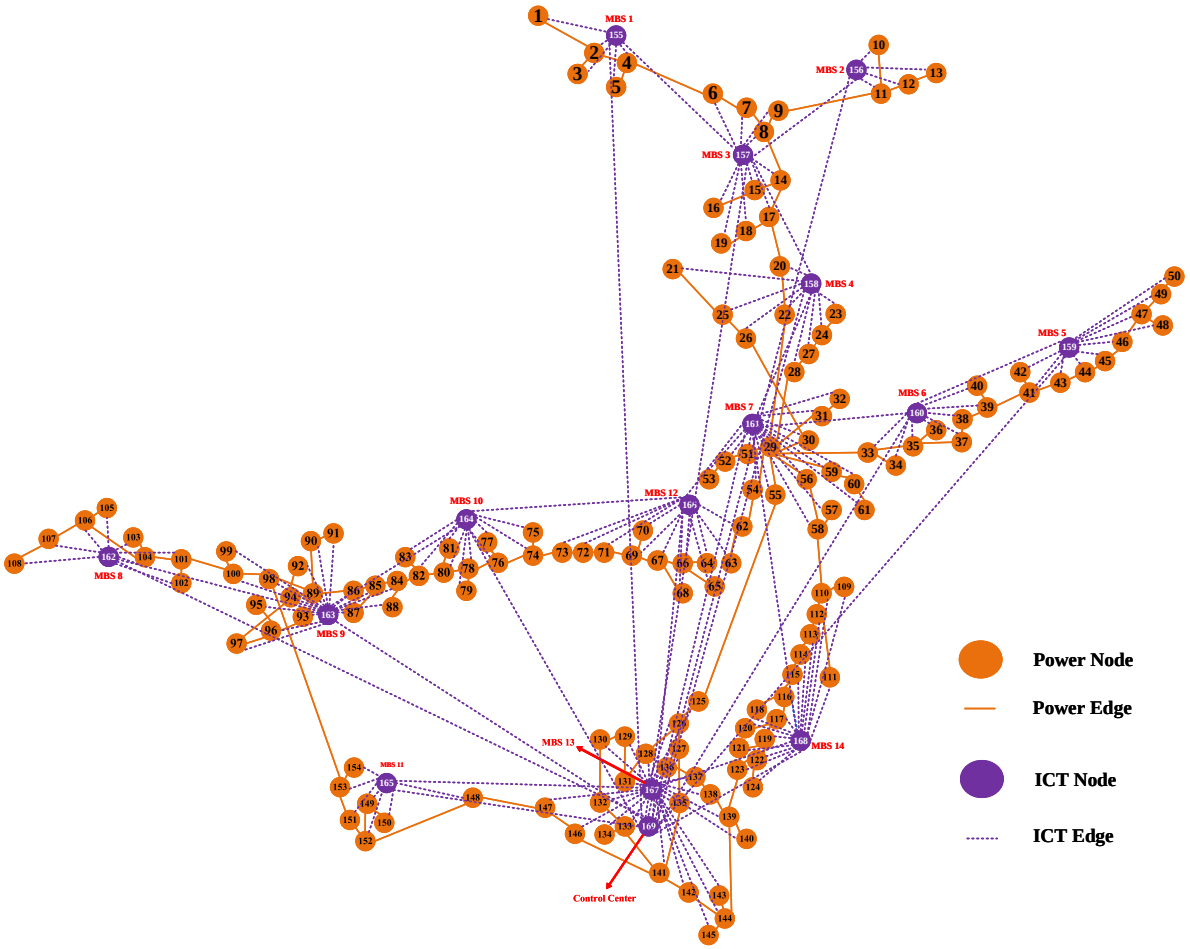

Figure 3. The graph representation of CPPS case study.

4. Simulation Results

In this study, we evaluate three distinct network configurations to reflect different operational modes of the power and ICT infrastructure:

- Undirected power network: In this scenario, all connections are treated as bidirectional, allowing power to flow in both directions. This setup models a more flexible grid where, in the event of faults or abnormal conditions, the DSO can reconfigure the topology to restore service by feeding power from alternative paths. Hence, this scenario represents both standard operation and post-fault reconfiguration via counterfeeding.
- Directed power network: This configuration assumes a unidirectional flow of electricity originating from the primary substation (node 29) and propagating downstream through the network. It mirrors the conventional operation of radial distribution systems, where power is delivered in a top-down manner under normal conditions.
- Undirected ICT (cyber) network: The cyber layer, responsible for monitoring and control, is considered undirected. This reflects its bidirectional communication requirement: operational data must be sent from power nodes to the control center, which in turn issues control commands back to the physical system.

These three configurations were deliberately selected because the choice of directionality (directed vs. undirected) significantly influences the results of network centrality metrics. For example, EBC and ERA values differ in networks depending on whether flow is constrained by edge directionality, as is the case for electric power under normal operation, or whether bidirectional communication or energy redistribution is allowed.

4.1. Undirected Power Network

Figure 4 shows the results for the undirected power network based on the EBC and ERA, and Table 2 shows the top-15 important edges with high ranking for EBC and ERA.

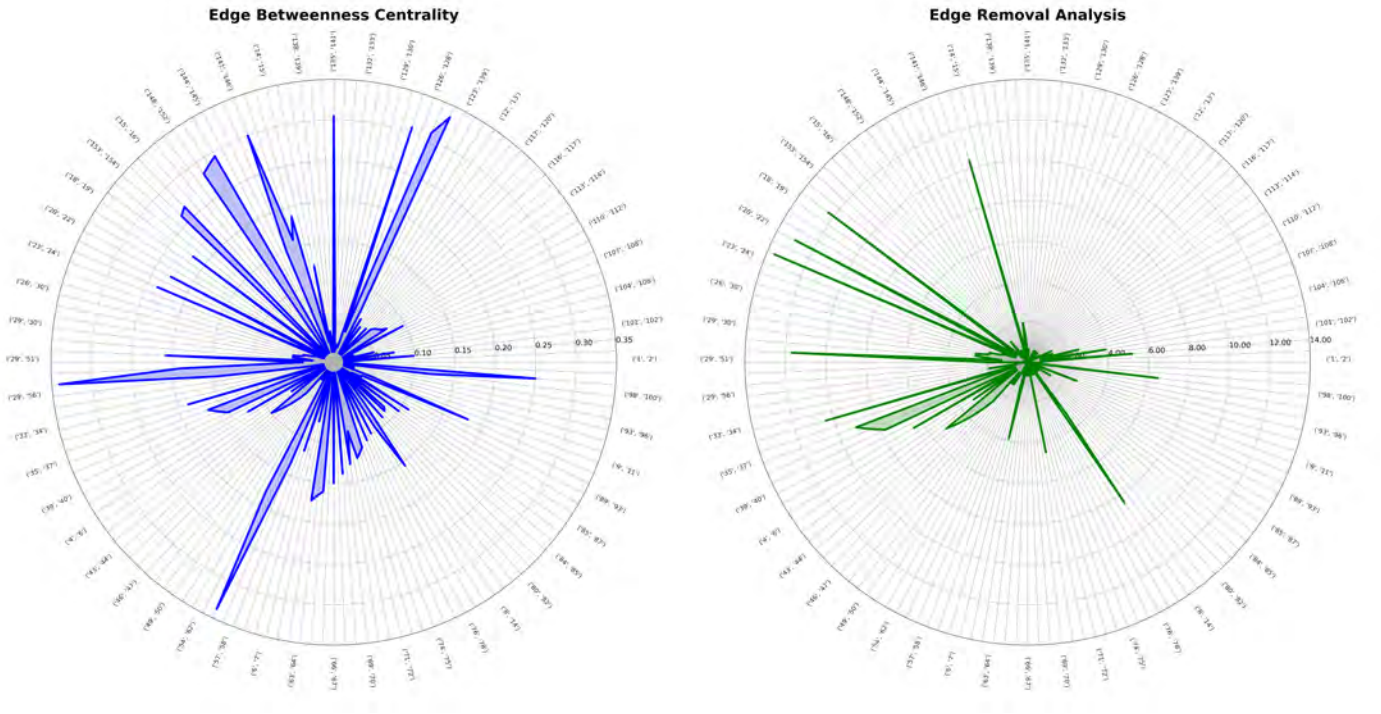

Figure 4. EBC and ERA for the undirected power network.

Table 2. Fifteen edges with the highest EBC and ERA for undirected power network.

Edge (EBC)	EBC Value	Edge (ERA)	ERA Value (%)
(‘29’, ‘55’)	0.340	(‘22’, ‘29’)	13.636
(‘55’, ‘125’)	0.337	(‘20’, ‘22’)	12.987
(‘125’, ‘126’)	0.335	(‘17’, ‘20’)	12.337
(‘126’, ‘127’)	0.308	(‘29’, ‘33’)	11.688
(‘127’, ‘135’)	0.306	(‘14’, ‘17’)	10.389
(‘135’, ‘141’)	0.304	(‘33’, ‘35’)	10.389
(‘141’, ‘146’)	0.299	(‘35’, ‘37’)	8.441
(‘146’, ‘147’)	0.294	(‘37’, ‘38’)	8.441
(‘147’, ‘148’)	0.288	(‘8’, ‘14’)	7.792
(‘148’, ‘152’)	0.283	(‘38’, ‘39’)	6.493
(‘151’, ‘152’)	0.266	(‘39’, ‘41’)	6.493
(‘151’, ‘153’)	0.261	(‘98’, ‘100’)	5.194
(‘98’, ‘153’)	0.250	(‘100’, ‘101’)	0.019
(‘22’, ‘29’)	0.237	(‘41’, ‘43’)	5.194
(‘20’, ‘22’)	0.227	(‘43’, ‘44’)	4.545

The results for EBC indicate that edge (‘29’, ‘55’), which is the edge from node 29 to node 55, holds the highest centrality value in the undirected power network, making it the most critical conduit for potential power flow. This is expected, as node 29 represents the main substation, and this edge connects it to the downstream network. Following this, the edge (‘55’, ‘125’) is identified as the second most important. This is also expected, as it lies directly after the (‘29’, ‘55’) edge in the downstream path from the primary substation, transmitting power from the central region to a broader section of the network. The high EBC values of these two edges suggest that many of the shortest paths between node pairs

pass through them, underscoring their structural importance. Similarly, other edges—from ('125', '126') to ('20', '22')—also exhibit high EBC values, as shown in Table 2. These edges serve as critical links between major parts of the network, facilitating connectivity and efficient power distribution. In contrast, edges such as ('99', '100'), ('95', '96'), ('85', '87'), and several others have lower betweenness centrality values. This is because they are located on peripheral branches or at the ends of radial segments, making them structurally less central to the overall network connectivity.

The results for the ERA indicate that edge ('22', '29') is the most important in the undirected power network. This is because its removal leads to a performance reduction of 13.63%, as it disconnects 21 nodes that belong to a critical radial section of the network. Another crucial edge is ('20', '22'), whose removal results in a performance drop of 12.98%. According to Table 2, other significant edges, such as those ranging from ('17', '20') to ('43', '44'), are also considered critical within the undirected power network. However, many edges, such as ('98', '153') and ('94', '97'), are not deemed important based on ERA. This is because they are located in meshed portions of the network, where redundant paths maintain connectivity; as a result, their removal does not disconnect nodes or cause a noticeable decline in network performance.

To compare the relationship between EBC and ERA in the undirected power network, Pearson correlation was applied according to Figure 5, yielding a value of 0.22, which indicates a low linear association between structural centrality and functional impact. This means that edges identified as structurally central (via EBC) do not necessarily correspond to edges whose removal leads to the greatest degradation in system performance (via ERA). For instance, high-EBC edges such as ('29','55') and ('55','125'), listed in Table 2, lie on many shortest paths and act as structural bridges between network clusters. Their removal increases path lengths but rarely causes immediate disconnections because of mesh redundancies. By contrast, the most critical ERA edges include ('22','29') with ERA = 13.6% and ('20','22') with ERA = 12.98%, along with other radial feeders whose failure isolates downstream nodes (e.g., 21 nodes disconnected). These edges are not necessarily topologically central but are functionally indispensable for maintaining connectivity. The divergence arises because EBC emphasizes global efficiency, whereas ERA captures local connectivity loss, and in meshed power networks, redundant paths decouple structural importance from functional criticality.

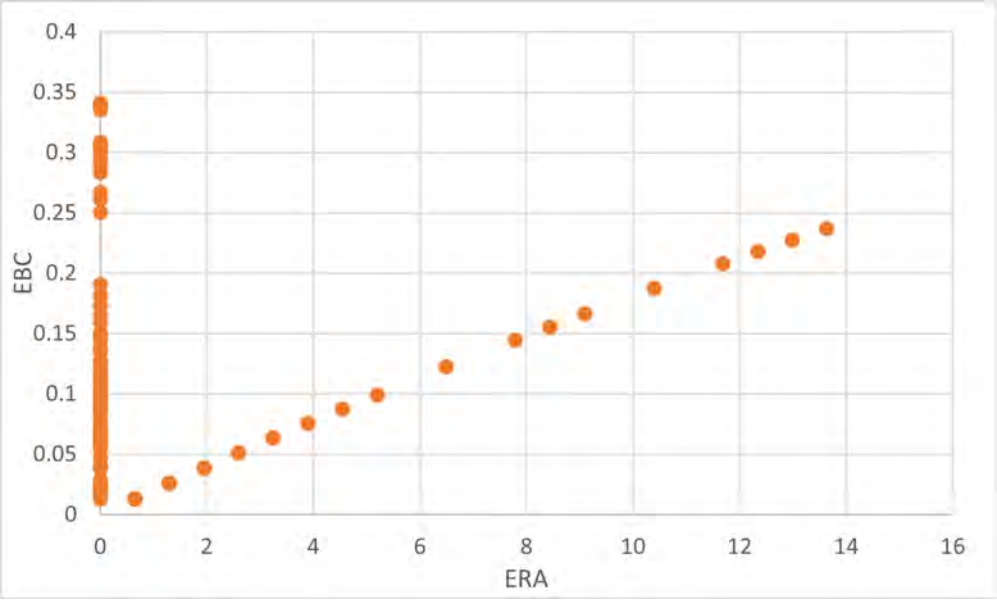

Figure 5. Pearson correlation between EBC and ERA for the undirected power network.

4.2. Directed Power Network

The results for the directed power network based on the EBC and ERA are shown in Figure 6, and the top-15 high-ranking edges are shown in Table 3.

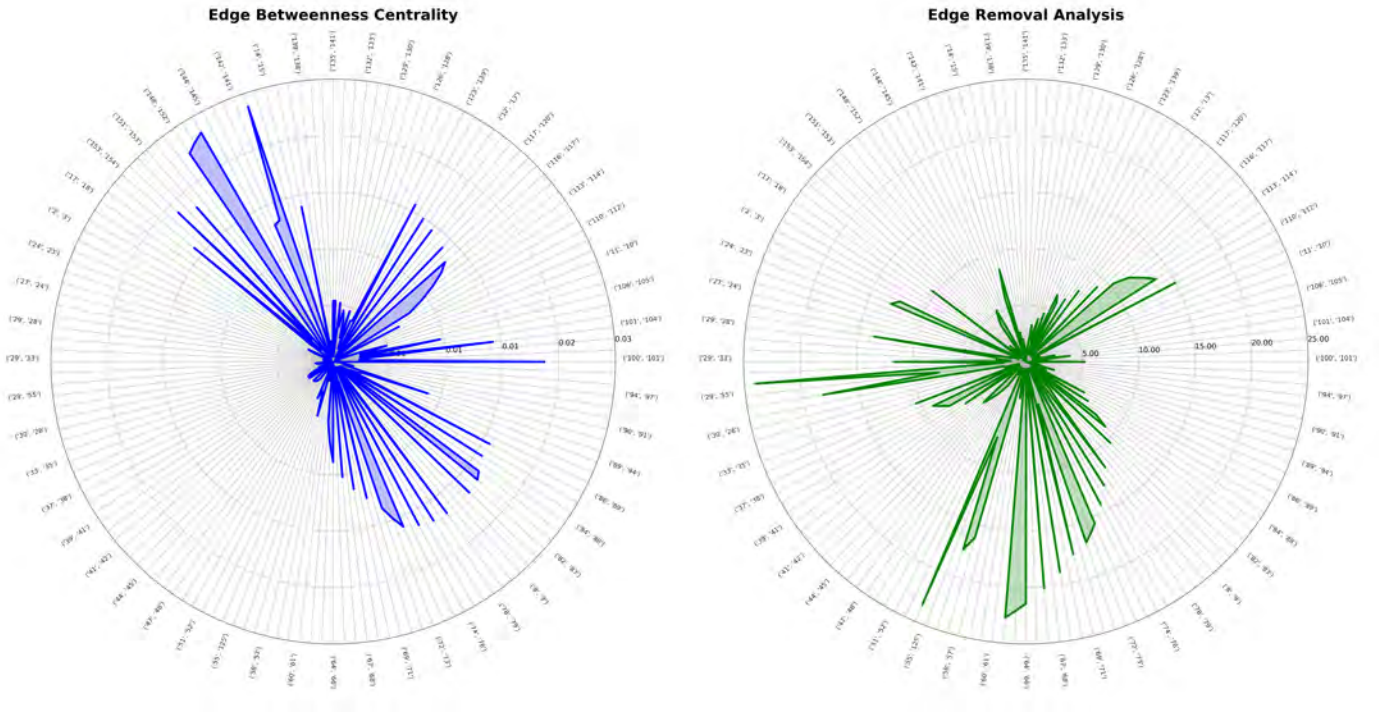

Figure 6. EBC and ERA for the directed power network.

Table 3. Fifteen edges with the highest EBC and ERA for directed power network.

Edge (EBC)	EBC Value	Edge (ERA)	ERA Value (%)
(‘141’, ‘146’)	0.0237	(‘29’, ‘54’)	24.025
(‘146’, ‘147’)	0.0233	(‘54’, ‘62’)	23.37
(‘147’, ‘148’)	0.0229	(‘62’, ‘63’)	22.72
(‘148’, ‘152’)	0.0223	(‘63’, ‘64’)	22.07
(‘152’, ‘151’)	0.0190	(‘64’, ‘66’)	21.42
(‘100’, ‘101’)	0.0186	(‘66’, ‘67’)	20.12
(‘151’, ‘153’)	0.0182	(‘67’, ‘69’)	18.83
(‘78’, ‘80’)	0.0167	(‘29’, ‘56’)	18.18
(‘80’, ‘82’)	0.0167	(‘56’, ‘58’)	17.53
(‘76’, ‘78’)	0.0166	(‘69’, ‘71’)	17.53
(‘82’, ‘84’)	0.0165	(‘71’, ‘72’)	16.88
(‘74’, ‘76’)	0.0163	(‘58’, ‘110’)	16.23
(‘84’, ‘85’)	0.0161	(‘72’, ‘73’)	16.23
(‘153’, ‘98’)	0.0158	(‘73’, ‘74’)	15.58
(‘73’, ‘74’)	0.0158	(‘110’, ‘112’)	14.93

In the directed power network, the results based on edge betweenness centrality (EBC) reveal that edges (‘141’, ‘146’), (‘146’, ‘147’), (‘147’, ‘148’), and (‘148’, ‘152’) possess the highest centrality values, with only marginal differences among them. These edges are of particular importance as they serve as critical conduits or bridges within the power network, enabling efficient power flow between distinct substructures. Their elevated centrality scores underscore their topological significance in maintaining connectivity and robustness across the network. Additional edges, ranging from (‘152’, ‘151’) to (‘73’, ‘74’), also exhibit substantial EBC values, indicating that they too play essential roles in

preserving the structural integrity of the system. In contrast, many other edges, such as (‘2’, ‘1’) and (‘12’, ‘13’), demonstrate very low EBC values. These edges are situated at the periphery of the network—often at the terminal ends of radial structures—and do not facilitate interconnections between major components. Consequently, they are considered topologically insignificant, as their removal would have minimal impact on the overall flow and cohesion of the power system.

On the other hand, edge removal analysis demonstrates that edge (‘29’, ‘54’) is the critical edge in the directed power network. Its removal reduces the performance of the power network by 24.025%, as it disconnects 37 nodes in the power network. The second important edge is edge (‘54’, ‘62’), whose removal reduces the performance of the power network by 23.37%. The other critical edges are (‘62’, ‘63’) to (‘110’, ‘112’) according to Table 3. However, many edges, such as (‘133’, ‘141’), are not very important according to the ERA because their removal does not disconnect any node as a user in the directed power network.

On the other hand, the results from the ERA highlight a different practical dimension of importance within the directed power network. Edge (‘29’, ‘54’) emerges as the most critical, as its removal leads to a substantial performance degradation of 24.025%, resulting in the disconnection of 37 nodes from the network. This clearly underscores its pivotal role in maintaining the network’s functional connectivity. Following closely are edges (‘54’, ‘62’) and (‘62’, ‘63’), whose removals cause performance reductions of 23.37% and 22.72%, respectively. These edges, along with others listed in Table 3 spanning down to (‘110’, ‘112’), constitute the backbone of operational continuity in the system. They are instrumental in ensuring that users remain connected to the core of the power infrastructure. In contrast, certain edges, such as (‘133’, ‘141’), are deemed functionally insignificant according to the ERA results. Their removal has negligible or no effect on network connectivity, as they do not result in the disconnection of any downstream nodes. These findings reflect that while some edges are structurally central, only a subset are critical in terms of user-level service continuity, emphasizing the value of ERA as a functional complement to purely topological measures like EBC.

Figure 7 shows the Pearson correlation between EBC and ERA in the directed power network, with a coefficient of 0.37. This moderate correlation suggests a partial alignment between edges that are structurally central and those that are functionally critical, although many edges still rank high in only one of the two measures. The increase compared to the undirected case arises because directionality constraints amplify the overlap between structural centrality and functional impact, making certain edges both topologically central and operationally indispensable. For example, high-EBC edges such as (‘141’,‘146’) and (‘146’,‘147’) more frequently coincide with critical ERA edges. Nevertheless, the persistence of discrepancies highlights that EBC alone cannot fully capture operational importance, reinforcing the need to integrate both topological and functional perspectives when assessing vulnerabilities in directed power networks.

4.3. Undirected Cyber Network

Figure 8 shows the results for the undirected cyber network for EBC and ERA, and Table 4 shows the top-15 edges with high rankings.

The EBC results indicate that edge (‘167’, ‘169’) holds the highest centrality value in the undirected network, making it the most structurally critical connection. Closely following is edge (‘163’, ‘169’), which also exhibits a high centrality score, reflecting its importance in maintaining overall connectivity. Additional key edges, ranging from (‘168’, ‘169’) to (‘156’, ‘169’), are also identified as significant, as shown in Table 4. These edges serve as essential

bridges within the cyber network, facilitating the flow of information between otherwise disconnected or weakly connected regions of the system.

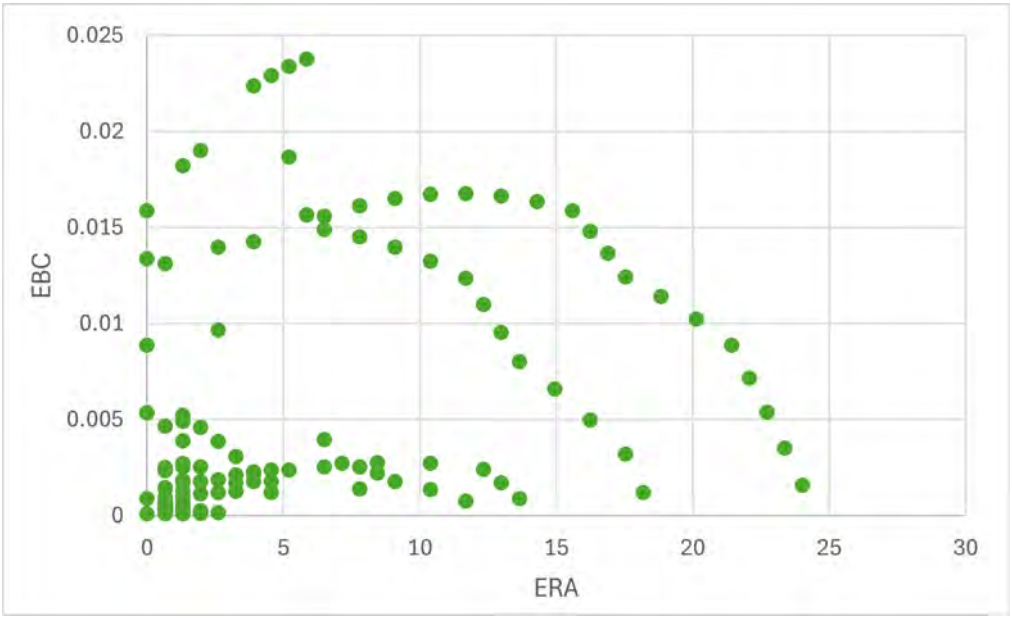

Figure 7. Pearson correlation between EBC and ERA for the directed power network.

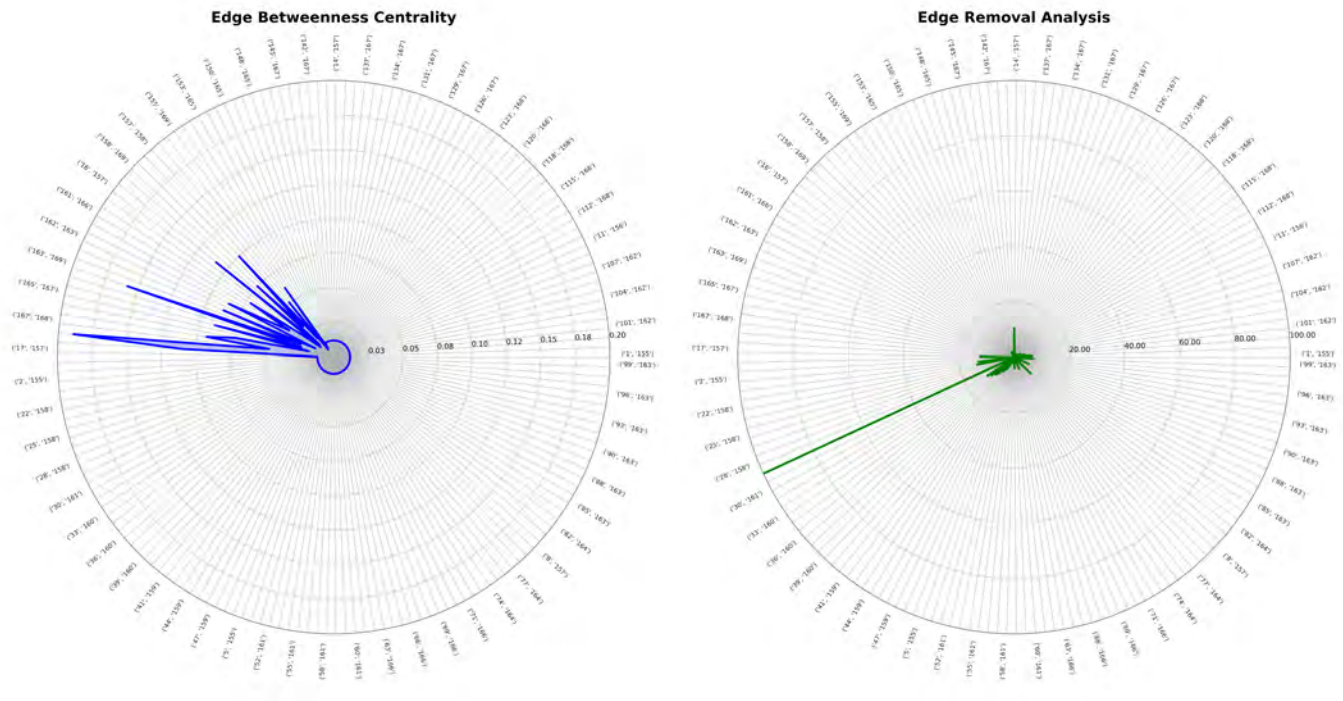

Figure 8. EBC and ERA for the cyber network.

In contrast, ERA identifies edge ('29', '161') as the most critical in the cyber network. Its removal leads to a 100% performance loss in the power network, as it triggers the failure of node 29, which cascades to all other connected power nodes. This makes it the single most vital edge in the system. The second most impactful edge is ('22', '158'), whose removal causes a 13.63% drop in network performance. Other important edges, ranging from ('20', '158') to ('89', '163'), are also functionally significant, as listed in Table 4. In contrast, many other edges exhibit minimal or no impact on performance, as their removal does not disconnect any users within the cyber network, as illustrated in Figure 8.

Figure 9 shows the correlation between EBC and ERA for the undirected ICT network, which is approximately zero, indicating virtually no linear relationship between structural centrality and functional importance. In other words, edges that are topologically central are not necessarily critical to network performance, and vice versa. This divergence is particularly striking in the cyber layer: high-EBC edges such as ('167','169') with EBC = 0.189 connect the control center to MBS 13, but multiple parallel paths make their removal inconsequential for overall connectivity. By contrast, ERA identifies edge ('29','161') (ERA = 100%) as critical, since it is the sole link between the control center (node 29) and the critical power node, whose failure cascades across all dependent nodes despite its low EBC value. This outcome reflects the star-like topology of the cyber layer, where single points of failure (SPoFs) dominate operational risk. Consequently, topological centrality does not equate to functional criticality: low-EBC edges without redundancy (e.g., ('29','161')) dominate ERA, while high-EBC hub interlinks appear resilient due to path redundancy. These findings highlight that relying solely on EBC can severely underestimate risks in ICT networks and reinforce the importance of integrating both topological and functional metrics in edge vulnerability assessment.

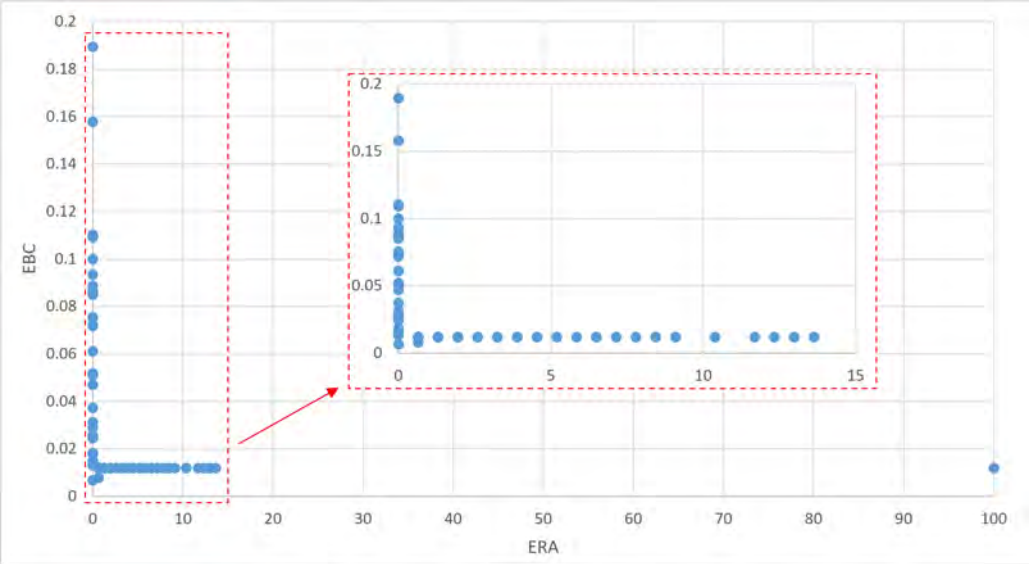

Figure 9. Pearson correlation between EBC and ERA for the undirected cyber network.

Table 4. Fifteen edges with the highest EBC and ERA for cyber network.

Edge (EBC)	EBC Value	Edge (ERA)	ERA Value (%)
('167', '169')	0.189	('29', '161')	100
('163', '169')	0.157	('22', '158')	13.63
('168', '169')	0.110	('20', '158')	12.98
('159', '169')	0.109	('17', '157')	12.33
('157', '169')	0.099	('33', '160')	11.68
('166', '169')	0.093	('14', '157')	10.38
('164', '169')	0.088	('35', '160')	10.38
('162', '169')	0.086	('37', '160')	9.090
('161', '169')	0.085	('38', '160')	8.44
('158', '169')	0.075	('8', '157')	8.44
('165', '169')	0.072	('39', '160')	7.79
('160', '169')	0.071	('98', '163')	7.14
('155', '169')	0.061	('100', '163')	6.49
('161', '168')	0.051	('41', '159')	6.49
('156', '169')	0.051	('89', '163')	5.84

5. Conclusions

In this paper, a real cyber-physical power distribution network in Northeastern Italy was modeled using complex network theory and analyzed with both edge betweenness centrality (structural criticality) and edge removal analysis (functional impact). The results across three scenarios—the undirected power network, the directed power network, and the undirected ICT network—demonstrated that purely topological measures often underestimate the functional importance of certain edges, thereby confirming the added value of ERA for resilience assessment.

Beyond methodological contributions, the findings provide actionable insights for distribution system operators. Identified critical edges can inform infrastructure hardening priorities, support dynamic reconfiguration through RTU-controlled switching, and guide risk-based monitoring by integrating ERA/EBC rankings into SCADA systems. Moreover, resource allocation strategies can be improved by focusing on edges where functional vulnerability outweighs structural centrality.

Although empirical validation with real failure data remains constrained by confidentiality, the proposed framework is reproducible, adaptable to different case studies, and can be extended through collaborations with utilities or synthetic failure injection. Overall, this work establishes an edge-centric, operationally relevant methodology for strengthening the resilience of interdependent cyber-physical power systems against high-impact, low-probability disruptions.

For future work, we plan to extend our analysis by incorporating additional edge centrality metrics and by exploring group centrality measures in larger-scale case studies, such as those involving capital city infrastructures. We also aim to integrate node dynamics and to address voltage- and power-related issues in order to better capture real-world operational constraints. In addition, we will develop more detailed simulations by assigning the exact number of users to each power node based on data provided by the DSO, by incorporating voltage and power flow constraints from realistic series data, and by considering the load profiles modeling. These enhancements will enable a more comprehensive and practical evaluation of cyber-physical power systems.

Author Contributions: Conceptualization, M.D.; data curation, M.D.; investigation, M.D.; methodology, M.D.; project administration, D.F.; software, M.D.; supervision, D.F.; validation, D.F.; visualization, M.D.; writing—original draft, M.D.; writing—review and editing, D.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy restrictions.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Xia, Y.; Small, M.; Wu, J. Introduction to focus issue: Complex network approaches to cyber-physical systems. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*. [CrossRef]
2. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
3. Akbarzadeh, A.; Katsikas, S.K. Dependency-based security risk assessment for cyber-physical systems. *Int. J. Inf. Secur.* **2023**, *22*, 563–578. [CrossRef]
4. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412. [CrossRef]

5. Yohanandhan, R.V.; Elavarasan, R.M.; Pugazhendhi, R.; Premkumar, M.; Mihet-Popa, L.; Terzija, V. A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–I: Background on CPPS and necessity of CPPS testbeds. *Int. J. Electr. Power Energy Syst.* **2022**, *136*, 107718. [CrossRef]
6. Amani, A.M.; Jalili, M. Power grids as complex networks: Resilience and reliability analysis. *IEEE Access* **2021**, *9*, 119010–119031. [CrossRef]
7. Jimada-Ojuolape, B.; Teh, J. Impact of the integration of information and communication technology on power system reliability: A review. *IEEE Access* **2020**, *8*, 24600–24615. [CrossRef]
8. Mohamed, A.A.A. On the rising interdependency between the power grid, ICT network, and E-mobility: Modeling and analysis. *Energies* **2019**, *12*, 1874. [CrossRef]
9. Liu, X.; Chen, B.; Chen, C.; Jin, D. Electric power grid resilience with interdependencies between power and communication networks–a review. *IET Smart Grid* **2020**, *3*, 182–193. [CrossRef]
10. Liu, F.; Xie, G.; Zhao, Z. Importance evaluation of power network nodes based on community division and characteristics of coupled network. *Electr. Power Syst. Res.* **2022**, *209*, 108015. [CrossRef]
11. Li, J.; Lin, Y.; Su, Q. Identifying critical nodes of cyber–physical power systems based on improved adaptive differential evolution. *Electr. Power Syst. Res.* **2024**, *229*, 110112. [CrossRef]
12. Amani, A.M.; Gaeini, N.; Jalili, M.; Yu, X. Which generation unit should be selected as control leader in secondary frequency control of microgrids? *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 393–402. [CrossRef]
13. Li, Y.; Ge, Y.; Xu, T.; Zhu, M.; He, Z. Controllability evaluation of complex networks in cyber–physical power systems via critical nodes and edges. *Int. J. Electr. Power Energy Syst.* **2024**, *155*, 109625. [CrossRef]
14. Narimani, M.R.; Huang, H.; Umunnakwe, A.; Mao, Z.; Sahu, A.; Zonouz, S.; Davis, K. Generalized contingency analysis based on graph theory and line outage distribution factor. *IEEE Syst. J.* **2021**, *16*, 626–636. [CrossRef]
15. Doostinia, M.; Falabretti, D.; Verticale, G.; Bolouki, S. Node Centrality Evaluation Based on Complex Network Theory: A Real Case Study for an Integrated Power Distribution and ICT System. In Proceedings of the 2024 AEIT International Annual Conference (AEIT), Trento, Italy, 25–27 September 2024; pp. 1–6.
16. Doostinia, M.; Falabretti, D.; Verticale, G.; Bolouki, S. Critical Node Identification for Cyber–Physical Power Distribution Systems Based on Complex Network Theory: A Real Case Study. *Energies* **2025**, *18*, 2937. [CrossRef]
17. Cuzzocrea, A.; Papadimitriou, A.; Katsaros, D.; Manolopoulos, Y. Edge betweenness centrality: A novel algorithm for QoS-based topology control over wireless sensor networks. *J. Netw. Comput. Appl.* **2012**, *35*, 1210–1217. [CrossRef]
18. Zhang, S.; Zhang, X.; Zhang, R.; Gu, W.; Cao, G. N-1 evaluation of integrated electricity and gas system considering cyber-physical interdependence. *IEEE Trans. Smart Grid* **2025**, *16*, 3728–3742. [CrossRef]
19. Milanović, J.V.; Zhu, W. Modeling of interconnected critical infrastructure systems using complex network theory. *IEEE Trans. Smart Grid* **2017**, *9*, 4637–4648. [CrossRef]
20. Hu, F.; Chen, L.; Chen, J. Robustness evaluation of complex power grids containing renewable energy. *Int. J. Electr. Power Energy Syst.* **2021**, *132*, 107187. [CrossRef]
21. Adebayo, I.; Sun, Y. New approaches for the identification of influential and critical nodes in an electric grid. *Arch. Electr. Eng.* **2022**, *2022*, 671–686. [CrossRef]
22. Forsberg, S.; Thomas, K.; Bergkvist, M. Power grid vulnerability analysis using complex network theory: A topological study of the Nordic transmission grid. *Phys. A Stat. Mech. Its Appl.* **2023**, *626*, 129072. [CrossRef]
23. Jones, C.B.; Bresloff, C.J.; Darbali-Zamora, R. Electric grid vulnerability analysis to identify communities prone to wildfires. *IEEE Access* **2023**, *11*, 35630–35638. [CrossRef]
24. Saleh, M.; Esa, Y.; Mohamed, A. Applications of complex network analysis in electric power systems. *Energies* **2018**, *11*, 1381. [CrossRef]
25. Kandaperumal, G.; Pandey, S.; Srivastava, A. AWR: Anticipate, withstand, and recover resilience metric for operational and planning decision support in electric distribution system. *IEEE Trans. Smart Grid* **2021**, *13*, 179–190. [CrossRef]
26. Doostinia, M.; Beheshti, M.T.; Alavi, S.A.; Guerrero, J.M. Distributed event-triggered average consensus control strategy with fractional-order local controllers for DC microgrids. *Electr. Power Syst. Res.* **2022**, *207*, 107791. [CrossRef]
27. Doostinia, M.; Beheshti, M.T.H.; Alavi, S.A. A distributed control strategy with fractional order PI controller for DC microgrid. In Proceedings of the 2019 Smart Grid Conference (SGC), Tehran, Iran, 18–19 December 2019; pp. 1–6.
28. Doostinia, M.; Beheshti, M.T.; Alavi, S.A.; Guerrero, J.M. Distributed control strategy for DC microgrids based on average consensus and fractional-order local controllers. *IET Smart Grid* **2021**, *4*, 549–560. [CrossRef]