COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

MULTICENTRALITY ANALYSIS FOR VULNERABILITY ASSESSMENT IN ELECTRICAL DISTRIBUTION NETWORK TOPOLOGY ARCHETYPES

Author: Beatriz Pineda Salcedo

Industrial Director: Ciaran Higgins

Academic Director: Graeme Hawker

Glasgow

August 2025

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Multicentrality analysis for vulnerability assessment in electrical distribution network topology archetypes

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2024/25 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Beatriz Pineda Salcedo Fecha: 13/ 08/ 2025

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Ciaran Higgins

Fdo.: Ciaran Higgins Fecha: 14/ 08/ 2025

EL CODIRECTOR DEL PROYECTO

Fdo.: Graeme Hawker Fecha: 14/ 08/ 2025

MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

MULTICENTRALITY ANALYSIS FOR VULNERABILITY ASSESSMENT IN ELECTRICAL DISTRIBUTION NETWORK TOPOLOGY ARCHETYPES

Author: Beatriz Pineda Salcedo

Academic Director: Graeme Hawker

Industrial Director: Ciaran Higgins

Glasgow

August 2025

ACKNOWLEDGEMENTS

I would like to thank my supervisors, Graeme Hawker and Ciaran Higgins, for their guidance and support throughout the development of this project. Their advice and mentorship have played a key role in supporting the progress of the work. Thank you very much for the time dedicated to my progress and for sharing your knowledge, which has greatly contributed to refining the approach and strengthening the outcomes of this study.

I would also like to thank Connor McGarry, Bruce Stephen and Junyi Lu for the insightful discussions held during the course of this work and for their guidance, which provided valuable perspectives that enriched the project.

To my family, I am deeply grateful for your unconditional support and encouragement throughout this academic journey. In particular, I would like to thank my parents for their constant guidance and care and my grandparents for their unwavering belief in me, all of which have been a true source of strength and motivation.

MULTICENTRALITY ANALYSIS FOR VULNERABILITY ASSESSMENT IN ELECTRICAL DISCTRIBUTION NETWORK TOPOLOGY ARCHETYPES

Autor: Pineda Salcedo, Beatriz
Director: Hawker, Graeme
Entidad Colaboradora: Scottish Power Energy Networks

RESUMEN DEL PROYECTO

En un contexto de creciente complejidad operativa de las redes de distribución eléctrica, se ha llevado a cabo una evaluación del uso del análisis de multicentralidad (MCA) para la identificación de vulnerabilidades en redes de distribución. El trabajo se centra tanto en métricas de centralidad puramente topológicas como en métricas híbridas que incorporan determinadas propiedades eléctricas. Los resultados muestran que las métricas basadas en la centralidad de intermediación (betweenness) tienen una alta correlación con los nudos más críticos de la red. Además, reduce significativamente el tiempo de cálculo frente a métodos tradicionales.

Palabras clave: Análisis de centralidad múltiple, Evaluación de vulnerabilidades, Redes eléctricas de distribución

1. Introducción

Las redes de distribución eléctrica están evolucionando rápidamente para dar respuesta a nuevas necesidades operativas y de planificación debido a factores como la electrificación de la demanda y el rápido crecimiento de la generación distribuida. Estos cambios aumentan la complejidad de la gestión de la red y refuerzan la necesidad, por parte de los operadores de redes de distribución, de garantizar la continuidad del suministro y su resiliencia. Los métodos tradicionales de evaluación de vulnerabilidades, como el análisis de contingencias, ofrecen una alta precisión, pero requieren un esfuerzo computacional muy elevado. Por ello, en muchos casos resultan poco prácticos para su aplicación rutinaria.

Aunque las métricas de centralidad han sido ampliamente estudiadas en la literatura académica, su uso se ha concentrado principalmente en sistemas de prueba estándar IEEE y en redes de transmisión más malladas, en lugar de aplicarse a grandes redes de distribución con topologías radiales o débilmente malladas. Este proyecto aborda este reto mediante la evaluación del potencial del Multi-Centrality Analysis (MCA) como una alternativa rápida y escalable para la identificación de nudos críticos en sistemas de distribución.

2. Definición del proyecto

Se han evaluado tanto métricas de centralidad puramente topológicas como métricas híbridas que incorporan propiedades eléctricas con el fin de determinar su capacidad para identificar los nudos más vulnerables de la red.

El alcance se centra en redes de distribución reales del Reino Unido. Se han analizado cuatro casos de estudio bajo condiciones de máxima demanda, facilitados por Scottish Power Ltd. (en adelante SPEN). Estos casos han sido seleccionados para cubrir un rango

variado de tamaños y configuraciones topológicas que garantice la relevancia práctica de los resultados.

El objetivo principal del proyecto es evaluar la eficacia de las distintas métricas de centralidad para identificar nudos críticos en redes de distribución eléctrica. Asimismo, se busca cuantificar los posibles ahorros computacionales que se pueden lograr mediante el uso de MCA frente a métodos tradicionales y explorar cómo estos resultados podrían aplicarse de forma práctica para apoyar los procesos de planificación y operación en SPEN.

3. Descripción del modelo

Para determinar la efectividad del análisis de multicentralidad en la evaluación de vulnerabilidades en redes de distribución, es fundamental no solo desarrollar el marco MCA, sino también establecer un método de referencia sólido con el cual comparar sus resultados.

El modelo MCA desarrollado calcula métricas de vulnerabilidad tanto puramente topológicas, por ejemplo el grado o la centralidad de intermediación (betweenness), como métricas híbridas que incorporan propiedades eléctricas, tales como las impedancias de línea. Las primeras se obtuvieron mediante la biblioteca NetworkX, mientras que las segundas se calcularon implementando directamente las fórmulas correspondientes. El sistema procesa el grafo de la red, asocia los valores a cada nodo y permite una comparación directa entre métricas de distinta naturaleza.

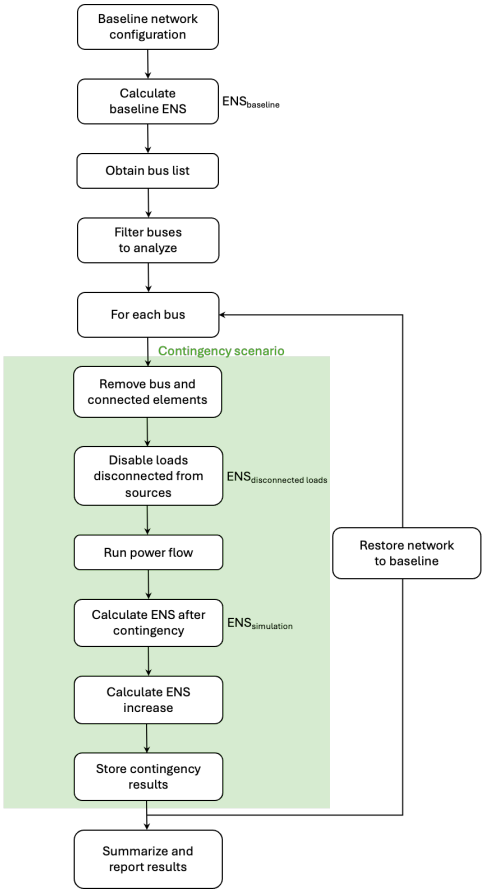

Ilustración 1: Flujo de trabajo del análisis de contingencias utilizado como método de referencia para evaluar la vulnerabilidad de la red.

Para la evaluación comparativa, se realiza un análisis de contingencias utilizando OpenDSS, que simula el impacto de la caída de cada nodo bajo condiciones de máxima demanda. El escenario de demanda se genera con el modelo CREST, que ofrece perfiles residenciales realistas. Se ha seleccionado la ENS como métrica principal para cuantificar el impacto operativo de las contingencias, ya que mide la cantidad de energía que no puede ser entregada a los clientes debido al fallo de nudos individuales durante las simulaciones. La Ilustración 1 representa el flujo de trabajo del análisis de contingencias usado como método de referencia.

4. Resultados

La Ilustración 2 muestra la comparación entre las cinco métricas de centralidad puramente topológicas y los valores de ENS calculados para cada nodo al simular su fallo en la red.

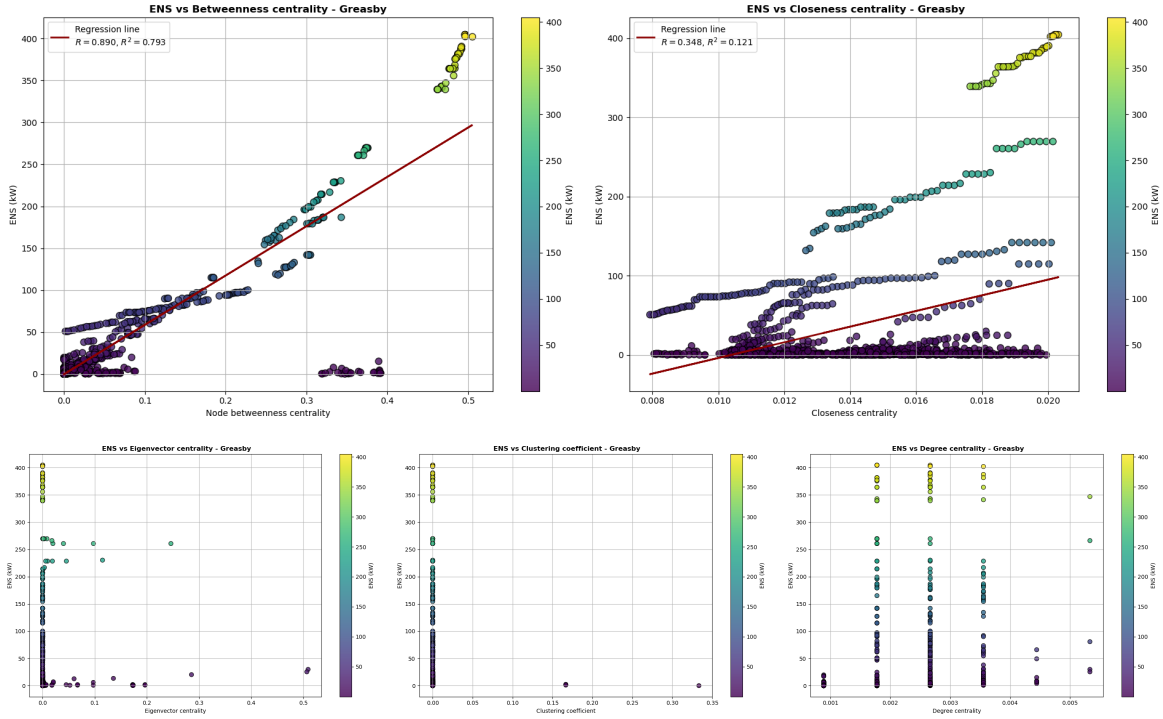

Ilustración 2: Gráficos de dispersión comparativos entre cinco métricas de centralidad puramente topológicas y la ENS para cada nodo

Aunque algunas métricas presentan poca o ninguna correlación con la ENS, las basadas en centralidad de intermediación (betweenness) destacan por su buen alineamiento con el método de referencia. En la Ilustración 3 se aprecia que identifican de manera bastante fiable los nodos más críticos, aunque tiende a sobreestimar algunos con baja criticidad. Además, presenta varios agrupamientos verticales en los gráficos, consecuencia de que la estructura por sí sola no discrimina suficientemente entre nodos.

La centralidad de intermediación híbrida corrige en gran medida estas sobreestimaciones y mejora la precisión al incorporar parámetros eléctricos como las impedancias y otra información asociada a cada nodo. Sobre todo, sobresale en la identificación de los nodos más críticos, localizados en la parte inferior izquierda de la figura, que son la principal prioridad para un DSO, mientras que las desviaciones en nodos menos críticos tienen una relevancia secundaria.

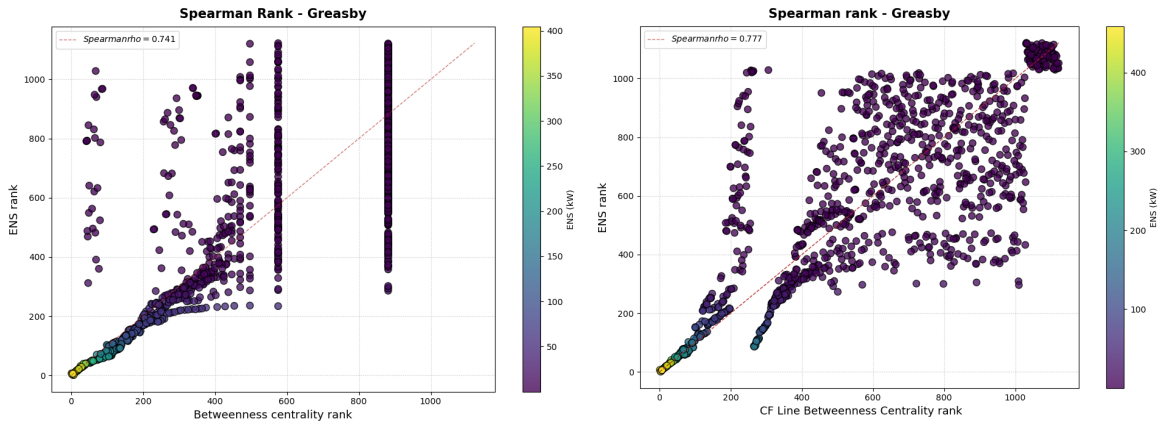

Ilustración 3: Comparación de rangos Spearman entre ambas centralidades de intermediación y la ENS

5. Conclusiones

La metodología desarrollada ha logrado ahorros computacionales significativos en comparación con el análisis de contingencias completo. Esto permite realizar un cribado rápido de vulnerabilidades en la red manteniendo una alta precisión en la identificación de los elementos más críticos.

El análisis comparativo de las métricas de centralidad ha tenido diferencias notables en su efectividad para evaluar la vulnerabilidad en redes de distribución. La centralidad de intermediación (betweenness) ha mostrado un rendimiento sorprendentemente sólido, especialmente considerando que se basa únicamente en información topológica. Por su parte, la centralidad de intermediación híbrida, que integra tanto las propiedades eléctricas como la posición estructural de cada nodo, resultó ser generalmente la métrica más eficaz para identificar nodos vulnerables en todos los casos de estudio.

SPEN podría implementar el MCA como una herramienta de cribado inicial para filtrar y priorizar rápidamente los nodos más críticos de la red, dejando únicamente un subconjunto reducido para su evaluación con estudios más detallados y costosos. Más allá del ahorro de tiempo, este enfoque permitiría responder con mayor rapidez a problemas emergentes en la red y optimizar la priorización de proyectos de refuerzo.

6. Referencias

[1] A. Mittal, J. Hazra, N. Jain, V. Goyal, D. P. Seetharam and Y. Sabharwal, “Real time contingency analysis for power grids,” 2011. Available: https://doi.org/10.1007/978-3-642-23397-5_31.

[2] P. Espinoza-Arriagada, G. A. Ruz and L. Gutierrez-Lagos, “Graph Theory-Based Topological and Nodal Analysis for Identifying Critical Points to Enhance Resilience in Electrical Distribution Systems,” *CIRED 2025 Conference, Paper 686*, Vienna, Austria, Jun. 2025 https://www.researchgate.net/publication/386456331

MULTICENTRALITY ANALYSIS FOR VULNERABILITY ASSESSMENT IN ELECTRICAL DISCTRIBUTION NETWORK TOPOLOGY ARCHETYPES

Author: Pineda Salcedo, Beatriz
Supervisor: Hawker, Graeme
Collaborating Entity: Scottish Power Energy Networks

ABSTRACT

In the context of increasing operational complexity in electrical distribution networks, an evaluation has been conducted on the use of multicentrality analysis (MCA) for identifying network vulnerabilities. The study focuses on both purely topological centrality metrics and hybrid metrics that incorporate specific electrical properties. The results show that metrics based on betweenness centrality exhibit a high correlation with the most critical nodes in the network and that the MCA approach significantly reduces computation time compared to traditional methods.
Keywords: Multiple centrality analysis, Vulnerability assessment, Electrical distribution networks

1. Context and motivation

Electrical distribution networks are rapidly evolving to accommodate the electrification of demand, the rapid growth of distributed generation and Net Zero ambitions. These changes increase the complexity of network operation and emphasize the importance of ensuring resilience and reliable supply for DNOs. Traditional vulnerability assessment methods, such as contingency analysis, provide high accuracy, but are very computationally intensive [1] and often impractical for usual applicability.

While centrality metrics have been widely studied within academic literature, their application has predominantly focused on standard IEEE test systems [2] and more meshed transmission networks rather than on large distribution grids with radial or weakly meshed topologies. This project addresses this challenge by evaluating the potential of MCA as a fast and scalable alternative for identifying critical nodes in distribution systems.

2. Project definition

By evaluating both purely topological and hybrid centrality metrics, the project seeks to determine their ability to identify the most vulnerable nodes. This could provide a basis for faster and more targeted decision making in network operation, maintenance and reinforcement planning.

The scope focuses on real UK distribution networks. 4 case studies, provided by Scottish Power Ltd., are analyzed under peak demand conditions. They have been selected so that they cover a range of sizes and topological configurations, to ensure practical relevance. The main objective is to evaluate how effectively different centrality metrics can identify critical nodes within electrical distribution networks. Also, to quantify the potential computational savings achieved by using MCA compared to traditional approaches and to explore how these findings could be practically applied to support processes at SPEN.

3. Model description

In order to assess the effectiveness of MCA for vulnerability assessment in distribution networks, it is essential not only to develop the MCA framework itself, but also to establish a robust benchmarking method against which its results can be evaluated.

The MCA model developed calculates both topological vulnerability metrics, like degree or betweenness centrality, and hybrid metrics that incorporate electrical properties such as line impedances. The former were obtained with NetworkX and the latter through direct implementation of formulas. The system processes the network graph, associates values with each node and allows for the comparison of metrics of different types.

For benchmarking purposes, contingency analysis is performed using OpenDSS. The benchmark involves simulating the impact of the outage of each node on the network under peak demand conditions. The demand scenario is generated with the CREST demand model, which provides realistic residential load profiles. Illustration 1 illustrates the contingency analysis workflow.

ENS is chosen as the primary metric to quantify the operational impact of these contingencies, as it measures the amount of energy that cannot be delivered to customers due to the outage of individual nodes during the contingency simulations. This metric serves as an intuitive and widely accepted indicator of network vulnerability, enabling a meaningful comparison between the detailed electrical simulation results and the MCA centrality metrics.

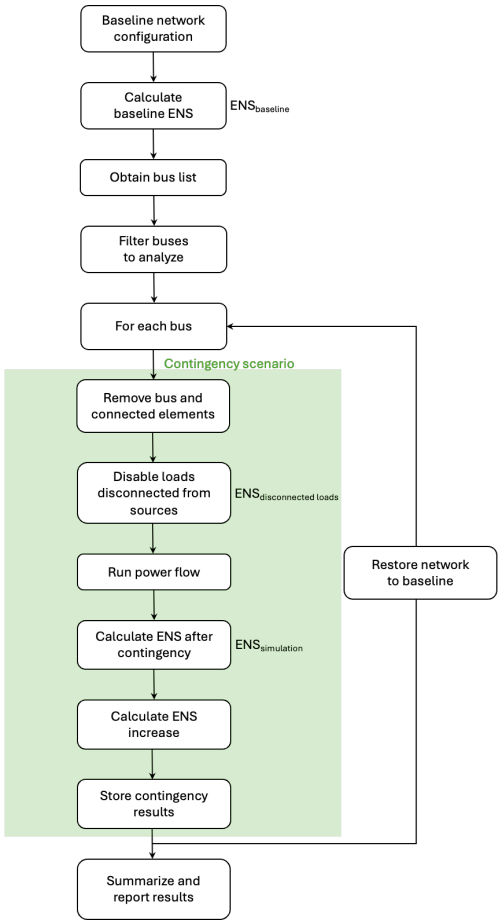

Illustration 1: Contingency analysis workflow for evaluating network vulnerability using ENS

4. Results

Illustration 2 shows comparisons between the five purely topological centrality metrics and the calculated ENS values of the respective node when simulating its failure in the network.

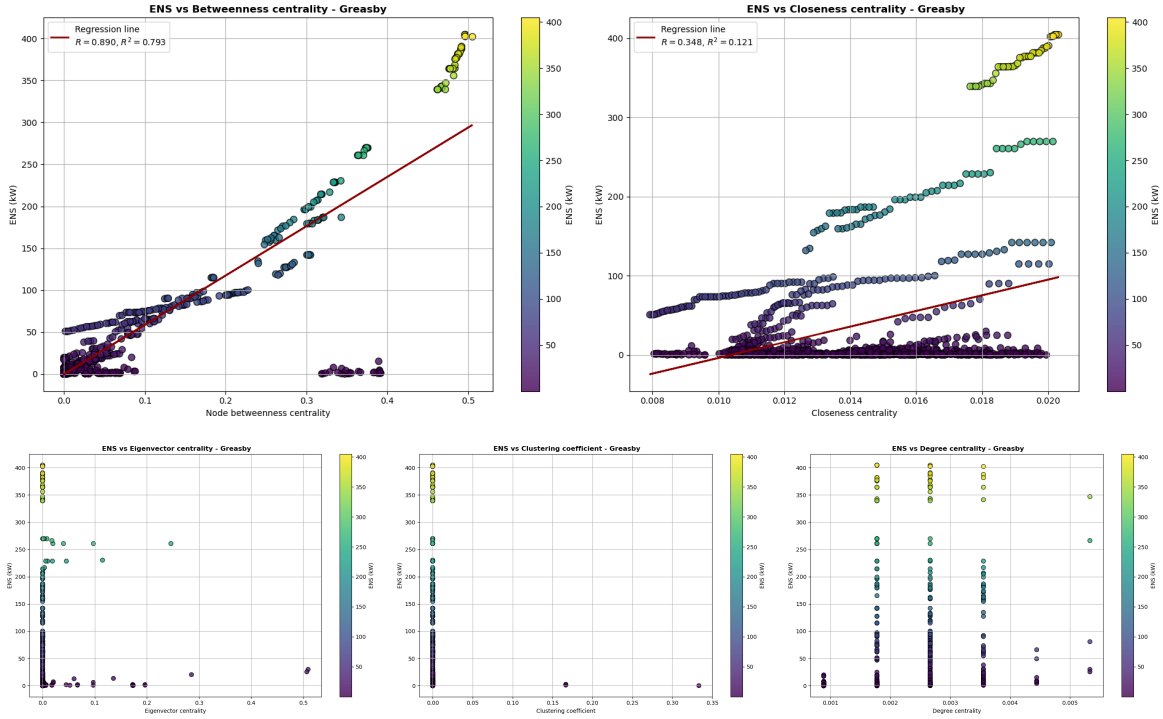

Illustration 2: Comparative scatter plots of five topological centrality metrics against ENS

Although some metrics show little or no correlation with the ENS, those based on betweenness stand out for their good alignment with the benchmark. Topological betweenness offers a reliable screening of the most critical nodes, although it tends to overestimate some lightly critical nodes. It also shows several vertical clusters, due to the fact that structure does not sufficiently discriminate between nodes.

Current-flow betweenness largely corrects these overestimations and improves overall accuracy, as it incorporates electrical parameters like impedances and further node information. Most importantly it excels in identifying the most critical nodes, situated at the bottom left corner, which remains the key priority for a DNO, while deviations in less critical or peripheral nodes are of secondary relevance.

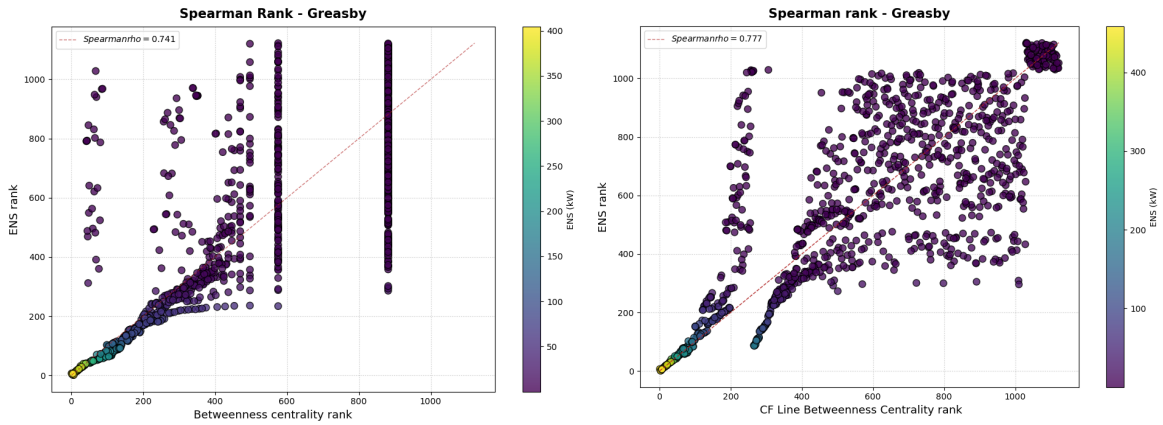

Illustration 3: Spearman rank comparison between topological betweenness and CF line betweenness

5. Conclusions

The methodology achieved significant computational savings compared to full contingency analysis, enabling rapid screening of network vulnerabilities while maintaining high accuracy for the most critical elements.

The comparative analysis of centrality metrics revealed remarkably different levels of effectiveness in assessing vulnerability across different distribution network topologies. Betweenness centrality demonstrated a surprisingly robust performance taking into account it only relied on topological information. Furthermore, the CF line betweenness centrality, which integrates both the electrical properties and the structural position of each node, was generally found to be the most effective metric for identifying vulnerable nodes across all case study networks.

Scottish Power could therefore implement MCA as a first stage screening tool to quickly filter and prioritise the most critical nodes in the network. This allows only a small subset to be passed on to slower or more expensive detailed studies. Beyond the raw time saving, such an approach would enable faster responses to emerging network issues or a better prioritisation of reinforcement projects.

6. References

[1] A. Mittal, J. Hazra, N. Jain, V. Goyal, D. P. Seetharam and Y. Sabharwal, "Real time contingency analysis for power grids," 2011. Available: https://doi.org/10.1007/978-3-642-23397-5_31.

[2] P. Espinoza-Arriagada, G. A. Ruz and L. Gutierrez-Lagos, "Graph Theory-Based Topological and Nodal Analysis for Identifying Critical Points to Enhance Resilience in Electrical Distribution Systems," *CIRED 2025 Conference, Paper 686*, Vienna, Austria, Jun. 2025 https://www.researchgate.net/publication/386456331

Table of contents

List of figures

List of tables

NOMENCLATURE

Relevant nomenclature is listed below in alphabetical order.

- BESS – Battery Energy Storage Systems
- CNMC – National Commission on Markets and Competition
- DER – Distributed Energy Resources
- DNO – Distribution Network Operator
- DSO – Distribution System Operator
- EENS – Expected Energy Non-Served
- EU – European Union
- EPRI – Electric Power Research Institute
- HV – High Voltage
- IEA – International Energy Agency
- LV – Low Voltage
- MCA – Multiple Centrality Analysis
- NREL – US National Renewable Energy Laboratory
- SAIDI – System Average Interruption Duration Index
- SPEN – Scottish Power Energy Networks

Chapter 1. INTRODUCTION

1.1 PROJECT OVERVIEW

In recent years, the resilience of electricity distribution networks has become an increasingly critical concern as the UK electricity system evolves toward greater decentralization and decarbonization. Distribution grids are facing unprecedented challenges from the electrification of heat and transport, the integration of DG and a corresponding increase in network complexity. Ensuring the continued reliability of supply in this changing context requires robust tools for identifying vulnerable elements within the network, to correctly prioritize investments and operational interventions.

Traditional methods for vulnerability assessment are very computationally intensive and may be impractical for large distribution systems. As an alternative, centrality metrics offer a means of rapidly estimating node vulnerability based solely on network structure. However, the actual effectiveness of these metrics in accurately identifying critical nodes within real power distribution grids is not ensured.

This project aims to explore the potential of Multicentrality Analysis (MCA) for vulnerability assessment in electrical distribution networks. Both purely topological and hybrid centrality metrics are included in this study. Several issues exist regarding the practical deployment of such an approach. The goal of this study is to assess whether MCA methods can provide a computationally efficient yet sufficiently accurate alternative for identifying the most critical nodes in electrical distribution networks. Thereby, supporting more informed and timely decision making by DNOs.

1.2 MOTIVATION

The idea for this project originated from a proposal by Scottish Power Energy Networks (SPEN), who identified significant potential for the application of centrality based vulnerability analysis in electrical distribution grids. As distribution networks face increasing complexity, there is a strong need for rapid and efficient tools to support asset management and planning.

SPEN recognized that centrality metrics, widely discussed in academic literature, are starting to be adopted in various sectors. Yet, their application in real world distribution networks remains limited. While most research to date has focused on relatively small, highly interconnected systems such as IEEE test systems or HV transmission grids, SPEN saw an opportunity to extend these techniques to large-scale, radial distribution systems typical of UK networks.

The project was therefore designed to investigate how these centrality metrics and hybrid approaches perform in more realistic distribution grids. This would enable to enhance vulnerability assessment and permit more targeted network reinforcement or reconfiguration strategies. The abundance of existing studies on the topic provided a solid foundation but also highlighted the gap in practical application for DSOs and DNOs. This research seeks to bridge that gap and deliver insights of direct relevance to SPEN and the wider industry.

1.3 OBJECTIVES AND HIGH LEVEL METHODOLOGY

Given the motivation and context outlined above, the following key research questions were formulated to guide this project:

- How well do these metrics predict critical nodes according to the selected criteria? Is there any significant correlation between centrality metrics and node vulnerability?
- How accurately can purely topological centrality metrics identify critical nodes in real UK distribution networks?

- To what extent do hybrid centrality metrics that incorporate electrical properties improve vulnerability assessment compared to topological metrics?
- What are the computational savings achieved by the MCA method when compared to traditional approaches?
- How could MCA be applied in practice by a DNO?

To address these questions, a structured methodology was designed. The approach involved calculating a range of centrality metrics on selected SPEN networks, developing benchmark results from traditional approaches and comparing their ability to identify vulnerable nodes. Computational efficiency was also measured to assess the practical feasibility of the MCA approach at scale. The overall process can be summarised in the following main stages:

1. Conduct a thorough literature review of centrality metrics and vulnerability assessment approaches applied to electrical distribution networks.
2. Define the concept of vulnerability in the context of SPEN's operational and planning needs. Based on this definition, choose a network performance metric that best represents this concept for the purposes of the study.
3. Implement an MCA framework to compute and compare centrality metrics and design a benchmark for vulnerability assessment using the chosen performance metric to evaluate MCA results against it.
4. Analyse and compare the performance of different metrics across distinct network topologies.
5. Evaluate the potential for computational savings and practical applicability of MCA for DNOs.

Chapter 2. BACKGROUND AND LITERATURE REVIEW

Electricity distribution networks are rapidly evolving towards smart grids, driven by the integration of DERs, electric vehicles and advanced metering technologies. This transformation has significantly increased the complexity of these networks, presenting operational and computational challenges for distribution network operators. ScottishPower, the second largest distribution network operator in the UK, is allocating approximately £360 million to the resilience of its network [1]. This investment is part of its RIIO-ED2 regulatory plan, in which many preventive measures have been taken, including asset adaptation or emergency response enhancement.

Electricity supply is an essential service in modern societies. Failures at the LV level usually directly disconnect users. This can not only cause inconvenience for dwellings, but even important economic losses for businesses. It is difficult to measure these social costs, however, many institutions try to estimate the VoLL, which basically quantifies the maximum value that customers are willing to pay in order to avoid an outage and ensure the security of supply [2]. For instance, a Value of Lost Load of £16/kWh was established by Ofgem for RIIO ED1 [3].

With policies setting very demanding targets to achieve the Net Zero transition, significant pressure is put on LV networks. The drive towards electrification of transport and domestic heating, will cause relevant increases in electricity demand, which will stress the electrical infrastructure [4]. Furthermore, DER penetration at the distribution level is also introducing new operational challenges, such as reverse power flows or localized congestions.

In this rapidly evolving context, DNOs face the challenge of conducting an extensive vulnerability assessment across all the networks that they manage, which are also becoming increasingly more complex. However, traditional methods are very computationally intensive when applied to entire distribution systems [5]. Because of that, there is a critical need for computationally efficient methodologies that can rapidly identify the most vulnerable elements in the network without requiring an exhaustive analysis.

Therefore, network planning and vulnerability assessment tools that can efficiently prioritize critical assets and optimize performance are essential to deploy a safe, secure and resilient network.

2.1 VULNERABILITY ASSESSMENT

As already mentioned, the reliable and secure operation of power networks is of paramount importance, as its efficiency and availability have significant economic and societal consequences [6]. It is therefore essential to analyze the vulnerabilities of the power grid, which are usually understood as those elements whose failure can cause relevant consequences for the stability of the system [7]. They are also known as critical points.

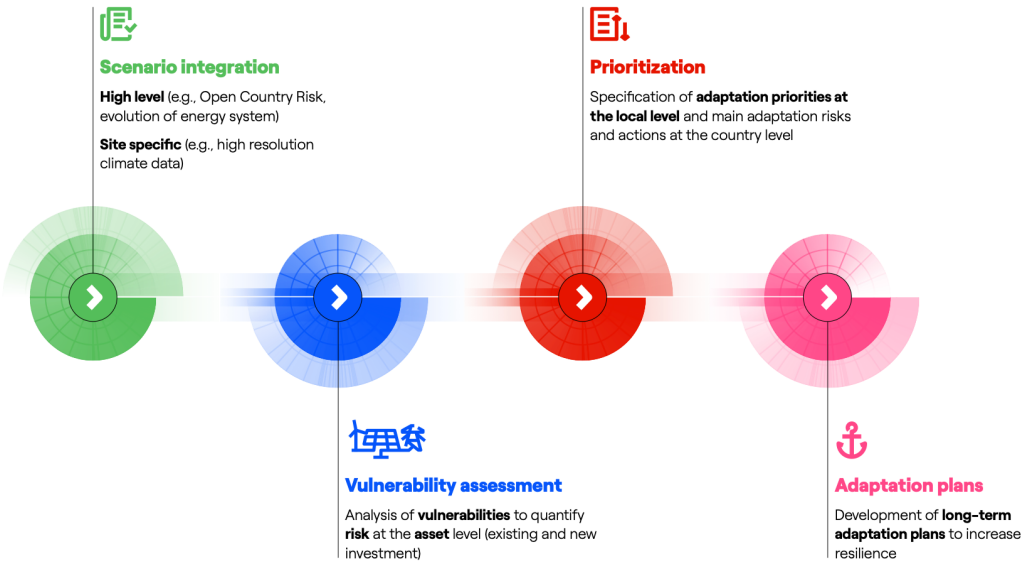

Figure 1. Enel's group strategy and risk management scheme [8]

Utilities use vulnerability frameworks to identify critical infrastructure and prioritize mitigation measures in those assets [9]. Vulnerability Assessment (VA) specifically focuses on determining the susceptibility of the network by analysing its components, their structure and their operational state. By this means, the impact of a failure on system stability or continuity of supply can be quantified and its management can be planned. These failures can be caused by internal disturbances (equipment failures) or external disturbances (extreme weather).

Many companies use it to prioritize investments in assets whose failures causes the greatest impact or optimize network design, by evaluating different topologies (e.g. ring or radial) to reduce vulnerabilities. They also need to comply with regulatory resilience standards imposed by EU directives, OFGEM (UK) or CNMC (Spain).

Large utilities have teams specializing in resilience or risk analysis, where they model networks, simulate contingencies and analyze many data to draw relevant conclusions. For instance, Enel applies a digital vulnerability index to optimize investments [8] and Con Edison models floods and simulates element failures to prevent massive outages [10].

2.2 TRADITIONAL APPROACHES

VA has changed since its beginnings and has adapted to the needs of the electrical era, according to the development of technologies and the characteristics of the grid. Below is an overview of the most widespread methods that have been deployed historically to carry out VA with key points and relevance to this study.

2.2.1 CLASSICAL DETERMINISTIC METHODS

During the 1980s and the 1990s, the electrical sector's main focus was N-1 and N-2 contingency analysis (CA). N-*k* contingency analysis simulates the failure of *k* components to test security of supply and system stability. CA requires running a power flow for each simulated contingency. This is a computationally intensive process, especially in large networks.

Currently, the N-1 security standard is required for European TSOs [11]. It is very computationally demanding for distribution networks and regulation does not state it as mandatory.

Additionally, CA requires iterative power flows through methods such as Newton Raphson or Gauss Seidel. A power flow consists in the calculation of the steady-state values of some parameters of the system. Power flows are very useful to identify overloadings or not desired voltage profiles. There are two types of power flows, AC and DC. The former is more accurate

and calculates active (P) and reactive (Q) power, voltages and angles at each node. However, AC is more complex and more computationally intensive. Alternatively, the latter assumes a flat voltage profile (node voltages at 1 p.u.), negligible losses and small angle differences [12]. Therefore, DC only calculates active power and voltage angles, making it much faster than the AC power flow, although its results are a simplification and less accurate.

The objective of CA is to ensure that system can maintain normal operation under N-*k* conditions. Normally, the safety criterion is that the system remains within certain operating limits after the simulated contingency. Those limits are usually ± 10 % in voltage values [13] and that flows do not exceed the thermal capacity of the conductors [14].

CA is a great method which is still used to this date however, it has several key limitations. It ignores correlations between faults, so it does not capture cascading faults. Apart from that, other factors such as event probability or economic impacts are not considered. Consequently, it needs to be complemented with other approaches to ensure that it contemplates all the desired aspects.

2.2.2 PROBABILISTIC APPROACHES

Introduced between the 1990s and the 2000s, Probabilistic Risk Assessment (PRA) marked a major step forward by incorporating uncertainty into risk models through methods such as:

- Fault Tree Analysis (FTA): Top-down deductive method that models causes of failures using logic gates, AND or OR. It starts with a complex "top event" for instance, a power outage. Then, breaks it down into root causes decomposing each immediate cause into basic causes. Each cause has assigned their respective probabilities based on historical data and the probability of the top event is calculated with the following equations [15].
- Monte Carlo Simulation: Estimates indexes such as SAIDI by simulating the actual process and random behaviour of the system [16]. This method approximates numerical solutions through repeated random sampling, in which it models many aspects of the network such as component states (operational or failed) or random variables (e.g. demand or weather).

This probabilistic era transformed metrics like SAIDI and EENS from descriptive indices to predictive and economic tools. SAIDI passed from simply measuring the average interruption time to a probabilistic indicator through the use of probabilistic distribution and Monte Carlo simulation. In contrast, EENS was linked to economic by multiplying it by the VoLL.

Nevertheless, although these metrics are very helpful, they require complementary analyses due to inherent limitations. SAIDI ignores any kind of social criticality, as one minute of interruption in a hospital has more severe consequences than in a residential area. Similarly, economic assessments via EENS depend on VoLL values. These exhibit significant disparities for instance, between countries even for identical industrial sectors.

Furthermore, there are other practices such as short circuit analyses [17], in which fault currents are simulated to size protective devices and ensure relay coordination, however this is beyond the scope of this project.

2.3 *FUTURE TRENDS AND EMERGING CHALLENGES*

Electrical distribution networks have evolved from passive radial systems to complex active systems with bidirectional flows. Traditionally, distribution networks have always had a hierarchical radial structure. Their design was characterized by radial systems with unidirectional energy flows [18]. Generation, which was heavily centralized, was generated in large plants such as thermal or hydroelectric power stations. Then, transmitted via HV lines to substations, where voltage levels were reduced for distribution to consumers, via MV and LV networks. As can be appreciated in Figure 2, the radial configuration had a feeder or main line that branched out to end consumers.

This model was efficient for predictable and practically static load patterns, as residential demand used to be. This hierarchical topology presented several persistent problems [19], such as voltage drops higher than 10 % at network extremes due to high R/X ratio, thermal overloads and phase imbalances that fostered high losses.

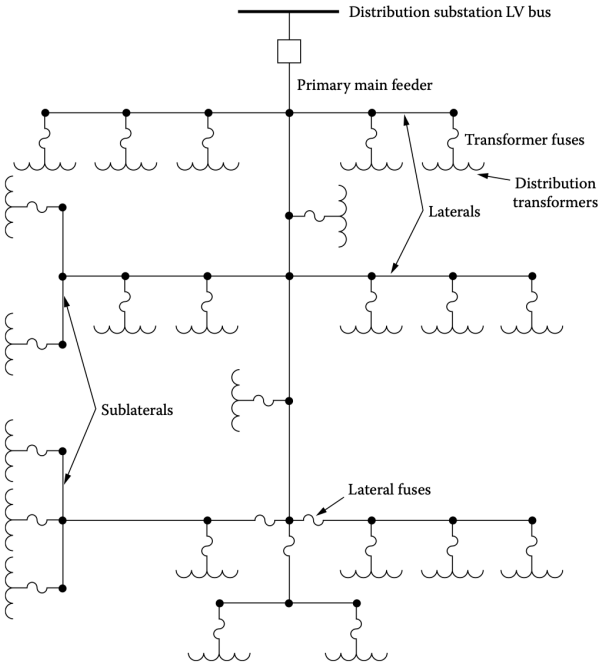

Figure 2. Radial distribution network [18]

Over the course of time distribution grids have gradually progressed to lightly more interconnected networks, although they still conserve a rather radial structure. They have also undergone a significant transformation due to technological advances, decarbonization, digitization and the decentralization of the energy sector [20].

2.3.1 DISTRIBUTED GENERATION AND DISTRIBUTED ENERGY RESOURCES

Distributed Generation (DG) refers to the production of electricity using small scale systems located nearby the end consumer. For example, PV solar panels or small wind turbines. DERs, on the other hand, expand this concept to include not only generation, but also energy storage systems, such as BESS, or EVs.

Recent DER growth stems mainly from government decarbonisation policies. Distributed PVs, heat pumps and EVs account for much of the recent DER expansion. The IEA estimates that 167 GW of distributed PV were added globally from 2019 to 2021, electric car registrations increased 41% in 2020 and almost 180 million heat pumps were used for heating in 2020, as the global stock had increased nearly 10% per year in the previous 5 years [21].

Both concepts challenge the traditional model of centralized generation and long distance transmission, promoting a more decentralized and flexible energy system. These technologies offer significant advantages and can provide some solutions to the challenges faced by the decarbonization of the electrical grid, such as:

- Emissions reduction: Many DERs use renewable sources (e.g. solar, wind), which do not emit greenhouse gases during operation.
- Greater resilience: DERs can operate independently or connected to the grid, serving as a backup during power outages. NREL confirms the reliability of DERs for backup and estimates, for example, that PV systems can maintain critical loads from 1 hour to 2 weeks depending on configuration, storage and demand [22].
- Energy efficiency: By generating close to the point of consumption, transmission losses are reduced. The authors of [23] state that a 2.8% losses reduction could be achieved.

However, DERs also imply a more complex operation and can provoke issues in the management of distribution networks. Reverse flows usually occur in high DER penetration networks, when DER production exceeds local demand, and energy flows from the user to the upstream grid [24]. This is a phenomenon for which many distribution systems are not designed. The flow of energy from DERs to the grid can raise the network's voltage profile, especially under low load conditions, causing overvoltages [25]. Additionally, the presence of DERs can cause traditional overcurrent relays to false tripping or even to fail to detect faults, leading to system disconnection failures and potential safety risks [26].

Nowadays, the objective is that distribution networks are active and intelligent structures that integrate advanced technologies and distributed energy resources (DERs). The following analysis brings on further detail on the aforementioned technologies and their challenges for DNOs and network operation.

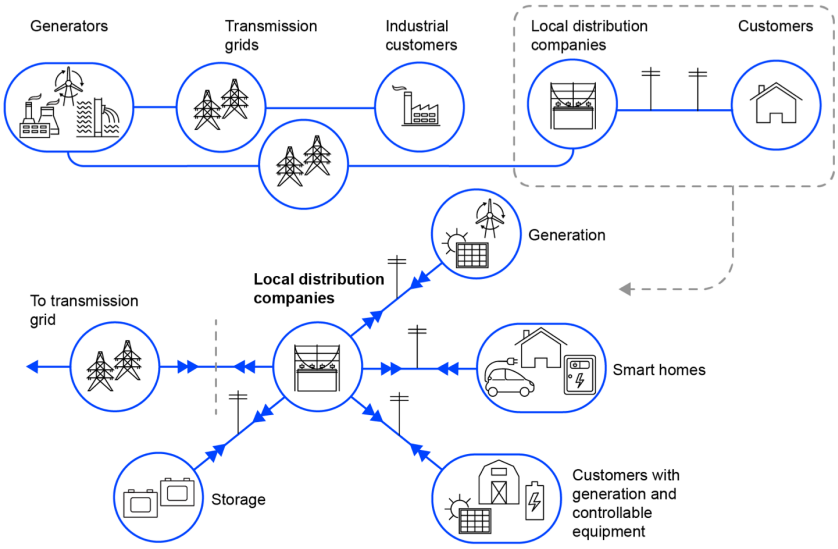

Figure 3: Evolution of the power system architecture [27]

2.3.2 EVs

EVs are cars powered by electric motors, fuelled by rechargeable batteries, which significantly reduce carbon emissions compared to internal combustion vehicles. As per Bloomberg NEF's report, EVs will account for 30% of all new car sales by 2030 [28].

However, the rapid growth and integration of electric vehicles also present significant challenges for electricity distribution networks. The following explores how EVs affect these networks, the challenges they introduce and how they relate to vulnerability assessment.

Network overloading

The rapid increase in the number of electric vehicles can cause the existing distribution networks to overload. A recent study of the California grid, in which more than 5,000 feeders were examined, concludes that 67% of the feeders will be overloaded by 2045 if EV growth continues. This would require a substantial need for infrastructure upgrades, estimated as more than 25 GW of reinforcement, which would cost between $6 billion and $20 billion [29].

Unpredictable peaks and load profiles

Simultaneous charging of EVs, as many consumers follow similar daily routines, can significantly impact the power system. Demand can spike, exceeding the capacity of infrastructure in residential areas. This temporal clustering of charging in the same residential area intensifies the stress on the grid. France expects from 7 to 16 million EVs by 2035, consuming between 40 and 65 TWh annually, reaching 8 GW during peak hours [30].

Voltage fluctuations, harmonics and supply quality

Massive and rapid charging can cause undervoltages at the ends of the distribution power lines. Uncontrolled charging can also result in power quality problems due to harmonics introduced by electronic chargers [31].

Given these factors, EVs can increase vulnerability causing for example localized overloads, especially in radial networks. Consequently, it is essential to consider peak demand scenarios, such as simultaneous charging in residential areas, to ensure stability.

2.3.3 HEAT PUMP WATER HEATERS (HPWHS)

HPWHs are devices that use electricity to extract heat from the surrounding air and transfer it to domestic water, remarkably reducing energy consumption and associated carbon emissions compared to conventional electric or gas water heaters. According to the IEA, HPWHs can deliver 2 to 4 times more thermal energy than the electrical energy they consume, and global stock is expected to surpass 150 million units by 2030 as governments push for building decarbonisation [32].

While they are primarily designed to provide hot water for residential use, modern HPWHs are recognized as DERs thanks to their operational flexibility and ability to shift demand in response to grid signals [33]. However, the rising deployment of HPWHs also brings new challenges for distribution networks, notably in terms of peak load management, voltage stability and local infrastructure adequacy.

Increased Peak Load and Demand Patterns

Similarly to EVs, the electrification of end use devices can place an additional burden on the grid and peak coincidence is a key risk. HPWHs shift significant domestic heating demand from gas to electricity, increasing peak demand loads, especially during cold periods where hot water use spikes. Studies estimate that high penetration rates of HPWHs (along with other heat pumps) could raise annual electric demand by 35%, and peak loads by up to 70% in strongly electrified scenarios, defying distribution grids previously sized for lower loads [34].

Voltage Issues

When many HPWHs operate at once, especially in rural or older low voltage feeders with limited reserve capacity, voltage sags may occur. Also, load spikes related to HPWH compressor starts and coincident running can foster undervoltages and increase losses at network edges. Sometimes even at relatively modest penetration rates, between 5 and 20%, depending on feeder design [35]. Induction motor-driven compressors in HPWHs can consume reactive power, further increasing current flow and voltage drops.

These combined effects highlight that distribution networks will increasingly be stressed and substantial reinforcement will be necessary to maintain reliable and efficient operation. It is thus essential to assess vulnerability under peak demand scenarios, such as during periods of extreme cold, in order to identify and mitigate weak points in the network.

2.4 ALTERNATIVE METHODS

As detailed in Section 2.3.1, the growth of DERs and the increase of energy demand, mainly caused by the electrification of transport and heating are provoking difficulties in the management of the networks. The electrical grid needs flexibility to be able to adapt to relevant variations in demand and integrate new renewable resources and DG. For instance, high DG penetration in traditionally radial LV networks results in reverse power flows and overvoltages, which cause numerical instability in iterative methods like power flows [36].

These computational issues are forcing utilities to advance and upgrade their vulnerability assessment methods towards faster and more scalable approaches. To address the limitations of traditional methods, utilities and researchers are exploring other faster, non-iterative and scalable approaches.

In response to this increasing complexity within modern distribution networks, the limitations of traditional vulnerability assessment tools have urged both industry and research to develop new, faster and more scalable methods. As distribution grids evolve to accommodate high penetration of DERs, rapid and robust VA becomes even more critical to ensure reliability and resilience.

In this context, several innovative methodologies have emerged, each offering distinct advantages in speed, scalability, and adaptability:

- Machine Learning (ML) and AI-Driven methods: The deployment of advanced metering infrastructure (AMI) and sensors in the electrical network has enabled data driven assessment techniques. Some ML supervised models such as graph attention

neural networks, which integrate real network data and Monte Carlo simulations, are used to train explainable models capable of predicting vulnerabilities [37].

- Graph-based or topological analysis: Use of centrality metrics such as degree, betweenness, and closeness, adjusted or combined in what is called "multicentrality analysis" [38], to quickly identify critical nodes and lines from the perspective of network structure.
- Hybrid methods: They combine physical grid models with topological analysis and classification algorithms, enabling efficient screening of vulnerabilities to focus detailed analyses only on vulnerable parts, achieving a balance between accuracy and speed [39].

Among these, centrality-based approaches are particularly appealing for vulnerability analysis in future grids, since they use purely topological data and scale well as network size and complexity grow. The integration of graph-based and multicentrality approaches presents a promising direction for fast, non-iterative and scalable VA, that could adequately complement those more computationally intensive traditional methodologies. This progression supports the motivation for the multicentrality analysis framework presented in this work.

2.5 MCA

Multiple Centrality Analysis (MCA) is a general mathematical process that can be implemented in any network structure, regardless of what it represents. The main concept is that the centrality of a node within a network is a fundamental trait for understanding its structure and function. However, "being central" [40] can have different meanings. Therefore, a single measure of centrality cannot capture all the important dimensions of the network.

The objective of MCA is to assess the spatial distribution of centrality in geographic systems. This requires the translation of the spatial system into a primal graph [41], where intersections become nodes and streets or connections become edges. Through a set of distinct centrality measures such as betweenness or eigenvector centrality, the graph is analysed.

MCA has shown promise in various domains. Urban design is a very common field, where it was first developed and used to analyse public spaces and pedestrian routes of the University

Campus in Parma [41]. Another example of its versatility is the maritime transport sector, where vulnerable ports in supply chains have been identified by combining multiple centrality metrics using the Borda Count method [42].

However, more limited research exists on this application specifically to electrical distribution networks. Among some of the few examples in electrical networks, Forsberg et al. applied weighted MCA with respect to the transmission line's reactance to evaluate the Nordic transmission network, where 5 out of 12 critical substations were successfully identified [43]. In addition, Hines and Blumsack developed a metric called "electrical centrality" for the IEEE 300-bus network, revealing highly electrically connected hub nodes that were not evident in the topological analysis [44].

Nonetheless, it is important to highlight that distribution networks possess unique structural characteristics very distinct from transmission grids and from IEEE test networks. While the latter are usually highly meshed and display substantial redundancy, distribution networks tend to feature predominantly radial or weakly meshed topologies, as already mentioned in section 2.3. This structural difference could affect the efficacy of centrality metrics for distribution networks.

Despite the fact that the amount of literature applying MCA directly to distribution grids remains limited, there are notable recent contributions bridging this gap. The authors of [7] emphasize how topological metrics enable a first screening of critical elements and how their variation under simulated failures reflects the criticality of that node. However, their results also state that such metrics alone may not capture fully operational vulnerability, especially in the presence of electrical constraints or power flow limitations. In contrast, [38] introduces and validates hybrid centrality metrics, that combine topological information with some electrical parameters, such as line impedances or node characteristics. However, both of this works use IEEE bus systems, but are not tested in actual distribution networks.

These recent methodological developments, together with the aforementioned limitations of traditional vulnerability assessment tools, underscore the motivation for this project. Specifically, there is a need to critically evaluate MCA frameworks to real world distribution

networks, such as those operated by SPEN, that exhibit lightly meshed structures and complex electrical behaviour.

2.5.1 THEORETICAL FRAMEWORK

A network can be represented as a graph $G = (V, E)$, where V is the set of nodes (e.g. buses, substations, loads), also called vertices, and E is the set of edges, illustrated as links between the nodes. A is the adjacency matrix of G, where $A_{ij} = 1$ if there is an edge between nodes i and j [45]. Otherwise, $A_{ij} = 0$.

A graph is the foundation for the systematic application of centrality metrics to quantify structural properties. The metrics presented and discussed below, are precisely those calculated and analysed as part of this project, following the approaches established in the aforementioned literature. These include both the classical topological metrics, such as degree, betweenness and closeness centrality, as well as physically-adapted measures like current-flow centrality, which has been shown to provide deeper insights into the vulnerability and resilience of electrical networks. The explicit definitions, calculation methods, and interpretative context for each metric are presented below.

The first group of metrics considered in this project are the classical topological centrality measures, which evaluate node importance based solely on the structure of the network. These metrics rely purely on the configuration of connections, without any reference to electrical properties of the system.

2.5.1.1 Degree Centrality

Degree Centrality is one of the simplest metrics and it is defined by the number of direct connections a node has. Nodes with high degree act as hubs and are often crucial for local connectivity.

$$DC(i) = \frac{\sum_{j \in V} A_{ij}}{n - 1} \qquad (1)$$

Where A_{ij} represents the connectivity between nodes i and j in the adjacency matrix, A, and n is the total number of nodes in the network.

2.5.1.2 Betweenness Centrality

Betweenness centrality quantifies how often a node appears on the shortest paths between other pairs of nodes:

$$BC(i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \tag{2}$$

Where σ_{st} is the total number of shortest paths from node *s* to node *t*, and $\sigma_{st}(i)$ only includes those paths that pass through node *i*. High betweenness nodes usually act as bridges or bottlenecks and are usually essential for global power flow by measuring how frequently they appear on shortest paths between random pair of nodes.

2.5.1.3 Closeness Centrality

Closeness centrality measures how close a node is to all others, in terms of shortest path lengths:

$$CC(i) = \frac{1}{\sum_{j \in V} d(i,j)} \tag{3}$$

Where $d(i,j)$ is the shortest path distance between nodes *i* and *j*.

2.5.1.4 Eigenvector Centrality

Eigenvector centrality assigns relative scores based on connections to highly connected neighbours:

$$EC(i) = \frac{1}{\lambda} \sum_{j \in V} A_{ij} \cdot EC(j) \tag{4}$$

with λ being the respective eigenvalue of the adjacency matrix, A. Node influence is based on the importance of its neighbours. This metric identifies nodes that are not just locally well connected, but also part of influential subnetworks.

2.5.1.5 Clustering Coefficient

The clustering coefficient is a fundamental metric in network theory that quantifies the degree to which nodes tend to cluster or group together:

$$CC(i) = \frac{2 \cdot T(i)}{DC(i) \cdot (DC(i) - 1)} \quad (5)$$

A high value indicates a strong tendency to form dense communities or groups, while a low value would suggest that the network is dispersed and local clusters rarely form.

Complementing the topological approach, the second family of metrics integrates electrical characteristics into the analysis, providing a more physically relevant understanding of criticality and vulnerability. The mathematical basis of this approach is the weighted Laplacian matrix of the network, which not only includes the connectivity between nodes, but also uses the admittance or the inverse of the impedance of each line as an electrical weight.

The Laplacian matrix, L, is constructed by subtracting the weighted adjacency matrix from the degree matrix. However, in order to correctly analyse electrical transmission, it is necessary to calculate the pseudo-inverse of the Laplacian, L^{+}. It is also called reactance matrix or effective resistance distance (ERD) matrix.

2.5.1.6 Current-flow Closeness Centrality

This metric is based on the concept of ERD between nodes and it measures the mean distance of from a node to the other nodes [38], which is defined as:

$$d_i = \frac{\sum_{k=1}^{n} Z_{ik}}{n} \quad (6)$$

Therefore, the metric is expressed as:

$$CF\ CC_i = \frac{n-1}{\sum_{k=1}^{n} Z_{ik}} \quad (7)$$

A central node for CF CC is a node that is joined to others by the shortest mean ERD. The shorter the total electrical distance, the greater its centrality.

2.5.1.7 Current-flow Line Betweenness Centrality

CF Line BC quantifies the importance of a line in terms of the power flow in each line, based on the shortest resistance paths. To formulate this, it takes into account which nodes are source nodes and which ones are target nodes. In the case of distribution networks, a source node would be a transformer, while a target node is a load. The power flow [38] between a source-target pair *(s,t)* passing through a transmission line *(i,k)* is given by:

$$P_{ik}^{st} = \sum_{k=1}^{n} A_{ik} \cdot |\delta_i^{st} - \delta_k^{st}| = \sum_{k=1}^{n} A_{ik} \cdot |L_{is}^{+} - L_{it}^{+} - L_{ks}^{+} + L_{kt}^{+}| \quad (8)$$

Where $\delta_i^{st} = L_{is}^{+} - L_{it}^{+}$ and $\delta_k^{st} = L_{ks}^{+} - L_{kt}^{+}$ are the phase angle nodes of nodes *i* and *k* with the respective pseudo-inverse of *L*. After simplifying, applying it to every possible source and target pair and normalizing it:

$$CF\ Line\ BC_i = \frac{2 \cdot \sum_{s<t} P_{ik}^{st}}{n \cdot (n-1)} \quad (9)$$

Where n is the total number of nodes in the system. It is a physically coherent way to identify potential "bottlenecks" or overloads. This metric is the only one in this project that evaluates lines, instead of nodes.

Chapter 3. PROJECT MODELLING

In order to assess whether MCA can effectively identify vulnerabilities in distribution networks, a model was designed, which enables the systematic computation of centrality metrics and their validation against an objective performance indicator. This requires not only the implementation of algorithms to calculate both topological and hybrid centralities, but also the construction of a meaningful benchmark to serve as a basis for comparison and evaluation.

Accordingly, this section explains:

- The methodology development process, including design considerations, methodological decisions and iterative improvements made during the research process.
- The final vulnerability assessment framework, detailing the model setup, implemented algorithms for both topological and hybrid centrality measures, testing and validation.
- The design of the benchmark model, including the selection of the operational scenario, metric choices and detailed development.

3.1 FRAMEWORK DEVELOPMENT PROCESS

The development of an effective methodology for assessing network vulnerability through centrality measures involved research and several iterative stages, where different approaches were considered. This section documents the methodological evolution, design decisions and alternative approaches that were considered, but ultimately abandoned in favour of the final framework.

3.1.1 INITIAL DEVELOPMENT AND METHODOLOGICAL EVOLUTION

The project initially began with the hypothesis that purely topological centrality measures would provide sufficient insight into distribution network vulnerability patterns. Hence, early research focused solely on standard graph theory metrics (e.g. degree, closeness or

betweenness). The initial approach was to develop a composite criticality index that would combine multiple centrality metrics into a single indicator. This approach was motivated by existing literature which suggested that different metrics capture complementary aspects of the network structure. For this reason, authors in [46] or [47] proposed that their combination would provide a better performance in vulnerability assessment.

This methodology involved using a weighting scheme to calculate the final index. In this way, each metric is assigned a relative importance and the index could be adjusted to SPEN's distribution network characteristics. Several combination methods were considered, such as equal weighting or entropy weighting methods. However, this composite approach varied between studies, so it proved to be more subjective and network dependent, with different networks probably requiring different weighting schemes.

Furthermore, other findings like [48] or [49] explained that some specific metrics, particularly betweenness centrality, had a great performance in vulnerability assessment. Thus, it was decided to evaluate the centrality measures individually in order to assess the significance and explanatory power of each one. As in much of the existing literature, metrics are often analysed separately rather than in combination.

Additionally, more recent research recognized that topological information alone could be insufficient to capture the nuances of vulnerabilities in electrical networks [48]. So rather than combining multiple topological metrics, hybrid centrality measures were proposed. This was proposed as a way to integrate both structural and electrical network characteristics within a single framework.

Therefore, it was decided to incorporate both types of metrics, purely topological and hybrid, into the analysis. The objective was to evaluate the individual performance and practical relevance of each metric across a range of realistic distribution networks and also, to evaluate whether hybrid centrality measures result in a notable improvement in identifying vulnerable nodes. Ultimately, the study aims to provide a clearer understanding of how effective these metrics truly are at identifying vulnerabilities and whether their level of accuracy justifies their use as a computationally efficient alternative.

3.1.2 SELECTION OF THE BENCHMARK'S VULNERABILITY METRIC

A fundamental prerequisite for developing a substantial benchmark in this project was the clear definition of what constitutes vulnerability in the context of a DNO, such as SPEN, with regards to distribution networks. For a utility, vulnerability is intrinsically linked to the network's ability to reliably supply all customers under both normal operating conditions and during disturbances. Therefore, an objective measure of vulnerability should directly reflect the degree to which customer supply is threatened or interrupted as a consequence of failures, overloads or other adverse scenarios. Establishing such a definition is essential to provide a baseline for assessing, comparing and validating the performance of MCA.

In recent literature, vulnerability and its quantification take different methodological directions. The authors of [38] evaluate it indirectly through the concept of network efficiency, which is computed as the average inverse of the ERD between all node pairs. However, this metric has a has a key limitation in the distribution context, despite its ability to reflect the ease of power transfer across the network. It does not provide direct information on whether specific customers remain supplied after a disturbance.

In [7], vulnerability is assessed directly simulating network operation through a power flow analysis and subsequently monitoring for critical issues such as voltage variations, overloads or other violations of operational limits. This method essentially involves observing whether the removal of certain nodes causes power quality or supply issues somewhere in the system. Nevertheless, this approach typically encompasses qualitative or visual assessments rather than a single, quantitative vulnerability score.

Given these limitations in the literature, it was decided in this project to adopt Energy Not Served (ENS) as the main indicator of vulnerability. ENS quantifies vulnerability through the total amount of energy that fails to be delivered to end users during specific fault scenarios, typically due to disconnection, voltage variation or line saturation. It offers a clear, objective and physically meaningful measure of the extent to which the distribution network fails to fulfil its fundamental purpose, which is supplying electricity to all connected customers.

In this framework, a contingency analysis has been carried out. Each simulated failure disconnects a node of the network, executes a power flow and calculates the ENS produced. When a contingency caused parts from the network to become isolated, each unsupplied demand in every load was calculated and added to the ENS.

This metric enables a direct and quantitative comparison between contingencies, as it assigns a specific ENS value to each node or scenario within the network. Moreover, ENS accurately captures the actual impact of network failures in terms that are directly relevant for utility operators, as it expresses vulnerability as the concrete loss of service experienced by consumers. As such, it offers both technical relevance and operational clarity, enabling an effective validation of MCA and facilitating objective comparisons of vulnerability across different nodes.

3.2 VULNERABILITY ASSESSMENT FRAMEWORK

The MCA model implemented in this project calculates the set of vulnerability metrics introduced in the Theoretical framework, encompassing both purely topological and hybrid centralities.

For the purely topological metrics, such as degree or betweenness centrality, the model uses the network's adjacency structure to quantify the relative importance of nodes and connections based solely on their connectivity patterns. These metrics reveal structural vulnerabilities and provide insight into the network's resilience without incorporating electrical parameters.

Complementing this, the hybrid metrics integrate electrical characteristics by leveraging the weighted Laplacian matrix and its pseudo-inverse. Metrics such as current-flow closeness or current-flow betweenness are computed using electrical weights assigned to network elements, capturing nuances of power flow and resistance that pure topology overlooks.

The MCA computation is performed using a dedicated computational framework that processes the network graph, calculates each metric and associates the results with corresponding nodes.

This enables a direct comparison of vulnerability indicators derived from different theoretical perspectives.

The purely topological centrality metrics were computed using the NetworkX [50] library, which offers a comprehensive set of graph algorithms specifically designed for analysing the structural properties of complex networks. In contrast, the hybrid physically-informed metrics were calculated by directly implementing the mathematical formulas detailed in the Theoretical framework.

To support interpretation of results, network visualizations were developed using Plotly [51], enabling dynamic exploration of the network's topology, node characteristics, and loading patterns. Additionally, static plots illustrating metric distributions, vulnerability rankings, and comparative analyses were created with widely used Python libraries such as Matplotlib [52] and Seaborn [53].

3.2.1 MODEL VALIDATION

The MCA computation code was initially developed and thoroughly tested on the IEEE 30-bus benchmark network. To ensure fidelity with the network model used in the comparative literature, specifically in [7], the exact system data file was downloaded from the Pandapower [54] repository, following the same methodology as the referenced paper. This dataset was then converted into the model's structured format, allowing seamless integration of the network information into the analysis environment.

Applying the complete set of centrality metrics to the IEEE 30-bus system enabled the reproduction of the key results reported in the literature, thereby confirming that the code accurately computes the range of topological centralities. The corresponding table of results from this implementation is presented below in Figure 4. This validation step was essential for building confidence in the reliability of our approach before moving on to analyse the more complex and realistic SPEN distribution networks.

```
================================================================================
CENTRALITY METRICS (Top 3 Nodes)
================================================================================
Degree Centrality          Bus 5 (0.241), Bus 9 (0.207), Bus 11 (0.172)
Betweenness Centrality     Bus 5 (0.435), Bus 9 (0.285), Bus 3 (0.221)
Eigenvector Centrality     Bus 5 (0.520), Bus 9 (0.375), Bus 3 (0.306)
Clustering Coefficient     Bus 7 (1.000), Bus 13 (1.000), Bus 20 (1.000)
```

Figure 4: Centrality metric results computed using the MCA model on the IEEE 30 bus test network

To further validate the model, a power flow simulation was also executed and compared to the one reported in [7]. Figure 5 displays the power flow results generated by our model. While some minor differences were observed, it is worth noting that there are variations in the underlying power flow solvers, the overall results were found to be highly consistent with those obtained in the published work.

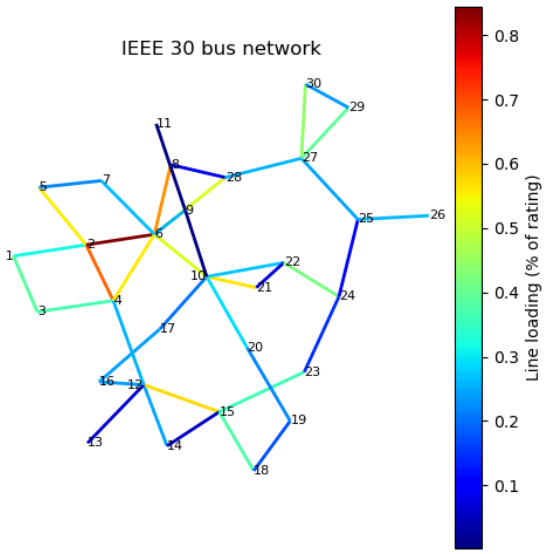

Figure 5: Line loading simulation output for the IEEE 30 bus network

The successful replication of the results in [7] demonstrated that the MCA implementation is consistent, robust, and ready to be deployed for practical vulnerability assessment and comparison with contingency analysis in real-world power distribution systems.

3.3 CASE STUDIES, OPERATIONAL CONDITIONS AND BENCHMARKING APPROACH

This section explains the final implementation of the benchmarking methodology used to validate the effectiveness of centrality measures in identifying network vulnerabilities. Accordingly, network case studies and their characteristics are presented, the operational scenario is defined and the benchmarking procedure is described.

3.3.1 SPEN CASE STUDY NETWORKS

To ensure the robustness and general applicability of the proposed vulnerability assessment framework, 4 distribution networks with diverse topological and operational characteristics were selected as test cases.

Given that centrality measures were originally developed for highly interconnected networks, it was expected that these metrics would perform better in networks with multiple pathways rather than purely radial configurations. Therefore, an effort was made to include some of the most meshed topologies available within typical distribution system constraints.

SPEN provided the information on the case studies and they were chosen based on topological diversity and size. The aim was to test networks representing different structural characteristics, including varying degrees of radiality and meshing levels to test MCA performance across different distribution network archetypes. Also, from small distribution feeders to larger urban networks, to ensure the methodology's applicability across different system scales. All case studies are 230 V LV distribution networks.

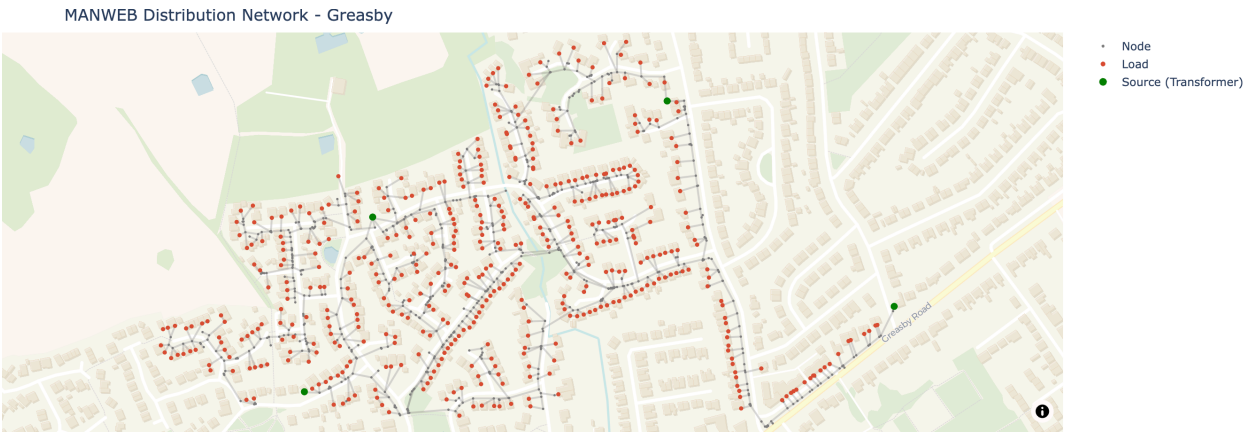

Figure 6: Representation of the Greasby distribution network within SP MANWEB area

The network in Figure 6 is located in Greasby, a village within the Wirral Peninsula, which forms part of the greater Liverpool area. This region is served by SP MANWEB, the regional electricity DNO responsible for Merseyside, North Wales, Cheshire and surrounding areas [55]. The SP MANWEB network is characterised by its meshed operation in urban locations such as Wirral, as can be seen in Figure 6, providing enhanced reliability and capacity for its customers. This distribution network comprises 4 transformers, 1,127 lines and 1,126 nodes, of which 480 are loads. It is one of the biggest networks in the study and has a more complex topology, with multiple feeders and considerably meshed structure for a distribution grid.

Furthermore, the Lanark network in Figure 7 is managed by SP Distribution, which oversees central and southern Scotland. The areas where the project's case studies from SP Distribution belong to are Lanarkshire and Glasgow. It represents a medium distribution network with mainly radial structure, although it has some localized interconnections. The grid features 5 transformers distributed across the network, 847 lines and 847 nodes, of which 356 are loads.

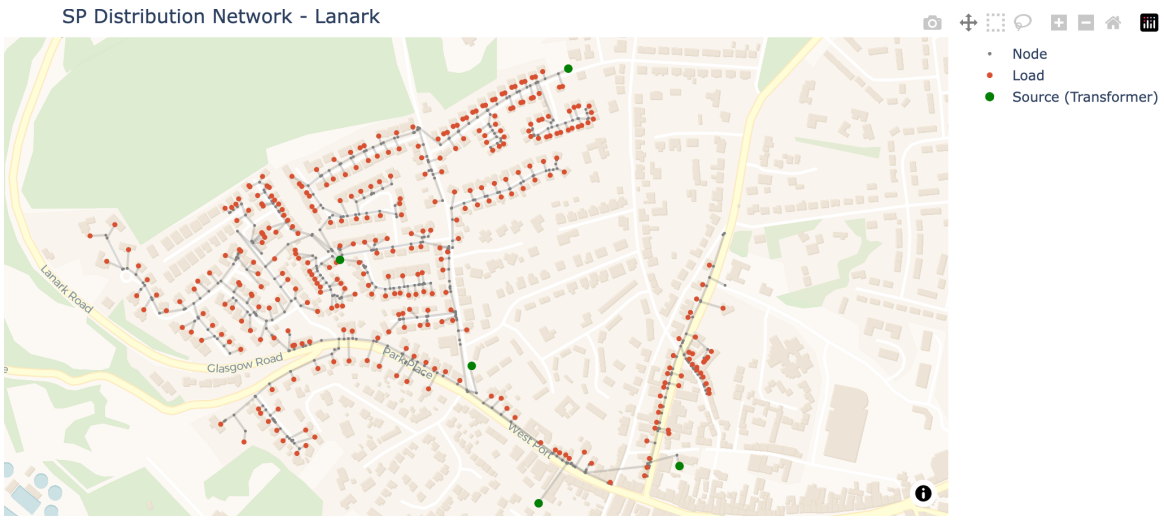

Figure 7: Representation of the Lanark distribution network within SP Distribution area

On the other hand, this Whifflet subnetwork in Glasgow shows a much smaller grid that is solely supplied by one transformer. Figure 8 shows that it has a predominantly radial structure, although it presents a few very valuable interconnections.

This configuration provides interesting insights into vulnerability patterns in less complex systems, where single points of failure can significantly affect customer supply. It has 220 lines and 221 nodes, of which 70 are loads, and it has one transformer.

Figure 8: Representation of the Whifflet distribution network within SP Distribution area

Lastly, the distribution network shown in Figure 9 is also operated by SP MANWEB. As part of the MANWEB area, this grid benefits from its typical characteristics, as it exhibits a lightly more meshed topology. The system has 4 transformers, 1235 lines and nodes, of which 460 are loads. It can be appreciated that it is more radial than Greasby's network, although it still presents some relevant redundancy and meshing.

Figure 9: Representation of the Moreton distribution network within SP MANWEB area

3.3.2 OPERATIONAL SCENARIOS

Distribution network vulnerability is not a static characteristic, so it requires careful analysis of the different operating scenarios that can expose weaknesses in the network. Each scenario can reveal specific vulnerabilities related to network topology, the integration of DERs and new loads such as EVs and heat pumps.

Therefore, two main scenarios were considered, each characterized by different challenges:

- Peak demand: This usually occurs during periods of high simultaneous electricity consumption. For instance, during winter evenings or summer afternoons, when heating, cooling and typical electric loads usually reach their maximum values. Under these conditions, network components tend to operate close to their maximum capacity or their thermal limits resulting in line overloading and supply interruptions.

- Low demand: When customer demand is minimal, networks present very different issues. Voltage problems are very common, for example, overvoltages could also arise due to significant DG penetration.

This project focuses specifically on peak demand scenarios. While this represents a critical operational condition, it should be acknowledged that distribution networks may exhibit different vulnerability patterns under other operational states. Hence, it is important to recognize the limitations of this approach, as other scenarios may introduce additional vulnerabilities that are not fully addressed in this study. However, this case was chosen due to several methodological and practical considerations.

Peak demand scenarios align naturally with the contingency analysis framework. As it is a node-based methodology, this enables to compare the nodes in the network with the centrality metrics from the MCA, which are mainly nodal too. In that way, the failure of each node can be simulated and its impact can be quantified for a later comparison.

On the contrary, in low demand scenarios vulnerabilities are not related to overloads, but rather to control issues, voltage stability or reverse power flows. Under low load conditions, simulating individual node failures loses its meaning, as it is more focused on evaluating load loss or disconnections. Consequently, as vulnerabilities in these scenarios are often related to dynamic problems, such as voltage oscillations or instability in control systems, it is more difficult to quantify them using traditional nodal metrics.

Furthermore, peaks in demand have traditionally represented the most stressful conditions for the grid. Especially with the growing electrification of transportation and heating, which will amplify loads and general demand on LV networks. The results directly support traditional network planning activities such as capacity upgrades, contingency planning and thermal constraint management, which remain core responsibilities for a DNO such as SPEN.

3.3.3 BENCHMARK MODEL IMPLEMENTATION

The project aimed to create a realistic and operationally meaningful benchmark for assessing vulnerability in SPEN's distribution networks. Given that SPEN provided network datasets in the *.dss* format, OpenDSS [56] was chosen for its native compatibility and recognized reliability in electrical network studies. To enhance flexibility and facilitate integration with modern data analysis and visualization tools, the model was implemented using OpenDSSDirect [57] within a Python environment.

This approach made it possible to efficiently process large volumes of power flow results and use additional Python libraries for subsequent processing and graphical representation of outcomes.

A list of the input variables in the benchmark model and a descriptive flowchart are provided in this section for clarity. The detailed functioning of the model will be explained later.

Further details on the execution of contingency scenarios and ENS calculation, as well as the specific use of power flow and data handling, are detailed below.

Power flow analysis

In this project, power flow analysis was employed as a fundamental tool for assessing network performance and identifying vulnerability to thermal overloads in SPEN's distribution network. A workflow was developed through OpenDSSDirect to simulate AC power flows, enabling systematic determination of branch loading throughout the network.

Therefore, to provide a clear view of network stress, the model includes a visualization module that highlights according to a colour map the overloading tendence of the network. This approach closely follows practices seen in [7], where graphical representation of the line loading is used as a main decision tool.

As illustrated in Figure 10, an example grid from a neighbourhood in Glasgow is shown, where the loading of each network element is denoted by colour coding along the branches. This visualisation enables immediate identification of more loaded or heavily used components.

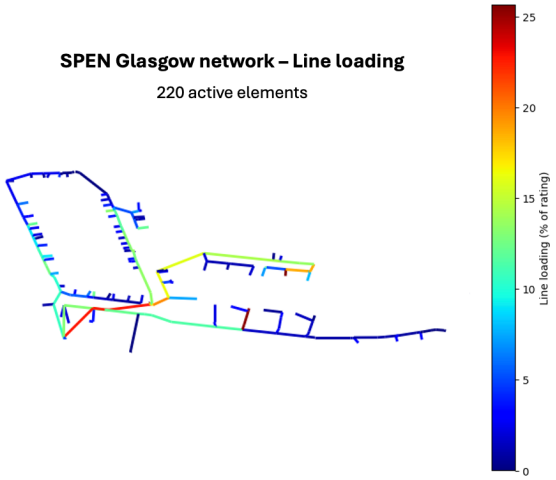

Figure 10: Power flow analysis visualization for a distribution network in Glasgow

It should be noted that the original network data provided by SPEN did not include any customer load information, primarily due to privacy policies and regulatory restrictions on the use of client consumption data. To address this limitation and ensure realistic demand allocation, the CREST demand model [58] was employed to generate demand profiles for 100 distinct dwellings, reflecting diverse residential consumption patterns. The CREST demand tool is an established open-source model developed by the University of Loughborough, specifically designed to produce demand profiles for UK households under a wide range of occupancy and appliance scenarios.

Each dwelling's demand at the time of the system's peak was extracted, in other words, at the hour when the total aggregate demand across all dwellings reached it maximum value. This approach aligns with the project's vulnerability framework, which prioritises the system's performance at peak load as the most critical operational scenario. For the purposes of the benchmark design, the peak demand value from each simulated dwelling was randomly assigned to each load in the network, thereby introducing realistic variation and heterogeneity

into the allocation. For full transparency and reproducibility, the detailed peak demand values used for the 100 simulated dwellings are provided in Appendix .

This method provides a more credible representation of stresses that might be observed during actual peak conditions, compared to uniform load assumptions. Consequently, the resulting power flow simulations and overload visualizations better reflect credible network behaviour under realistic operational conditions, enhancing the robustness and interpretability of the vulnerability assessment in the absence of customer data.

Contingency analysis

To systematically assess the vulnerability of the distribution network under failure conditions, a contingency analysis model was developed also using OpenDSSDirect within Python. The contingency analysis conducted in this project focuses exclusively on single contingencies, where each scenario simulates the outage of a node at a time. This approach, often referred to as an "N-1" analysis, was deliberately chosen both for its practical relevance in distribution network operation and to ensure direct comparability with the results obtained from the MCA.

By isolating the impact of individual element failures, it becomes possible to assign a distinct, quantitative vulnerability value to each node in the network. This is essential, just as MCA produces a centrality score for every node, the single contingency analysis yields a clear metric associated with the loss of each node, that can be directly compared. This methodological consistency supports the core objective of the benchmark framework, which is to enable a robust, node by node comparison between centrality-based values and ENS outcomes derived from simulated outage scenarios.

The core workflow comprises several stages, from data input to demand assignment, network setup and final contingency simulation. The key logic and inputs are summarised below. For transparency and reproducibility, the demand assignments are randomly allocated but can be fixed and recorded for repeated executions.

The flowchart in Figure 11 details the data preparation and initial simulation workflow, illustrating the key steps from network and input data loading and up to the stage where the

model is ready for contingency simulation or power flow analysis. This process ensures all relevant network and demand information is correctly structured prior to conducting any advanced analyses, such as contingency studies.

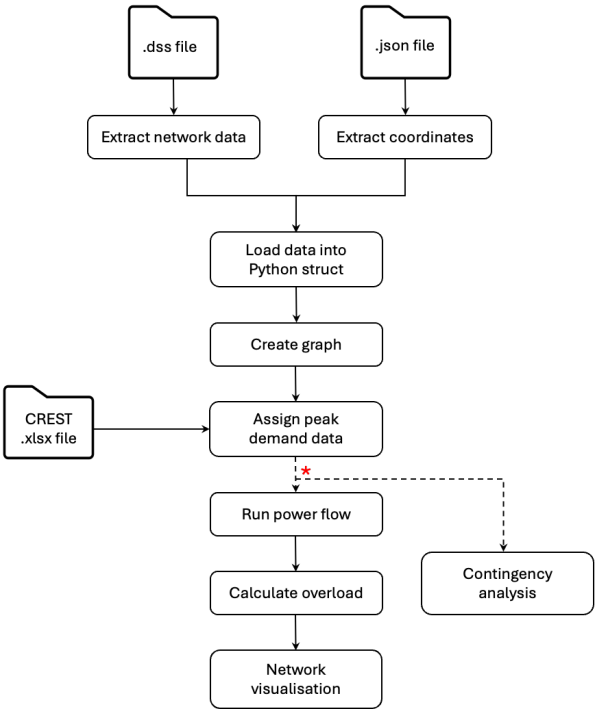

Figure 11: Data preparation and initial simulation workflow

The input data in the model, as illustrated in Figure 11, are summarised in the list below:

- Network topology and parameters: The distribution network is provided in OpenDSS (.dss) format by SPEN, containing real asset and connectivity data, such as line ID, their capacities, resistance and reactance, the buses that they are formed by and their length.
- Coordinates: SPEN also provided in a .json format the geospatial coordinates for each node.
- Demand profiles: A list of peak load values in W for 100 residential dwellings, extracted from CREST, is used as a pool for random assignment to the loads in the network. Each assigned load is paired with a power factor, which has been assumed to be 0.95 by default, to compute VAR values.

In the flowchart, a red asterisk is used to highlight that at that stage there is flexibility in the analysis pathway. The model is at that point fully configured and ready for simulations, which means the user can choose to proceed directly with a conventional power flow analysis of a given scenario, or alternatively, advance to the contingency analysis module described below.

For completeness, Figure 11 depicts the full process including the power flow analysis, illustrating the end-to-end simulation and visualisation of network loading. However, it should be emphasised that the red asterisk denotes a methodological branching point, after which any other process can be undertaken depending on the objectives of the analysis. This framework was mainly used with the objective of executing a contingency analysis to identify which are the most vulnerable nodes in the studied network. Therefore, the decision variable that quantifies and enables the node ordering by criticality is, as already explained earlier, ENS. Below is a more detailed explanation of the full contingency analysis workflow.

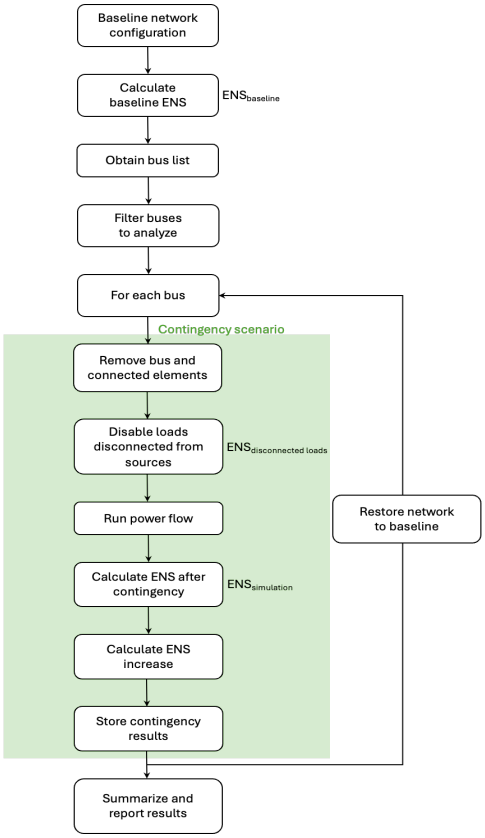

Figure 12: Contingency analysis workflow for evaluating network vulnerability using ENS

Figure 12 facilitates understanding of the analytical workflow for the contingency analysis model, detailing the sequential processes of scenario simulation, power flow computation and ENS calculation. This diagram complements the previous flowchart in Figure 11 by illustrating the systematic steps undertaken to evaluate network vulnerability under single contingency events.

The contingency analysis process is designed to systematically assess the impact of the failure of each node on the overall network performance. Starting from a baseline network configuration, the model calculates the baseline ENS to establish a reference point for subsequent comparisons. Calculating this baseline value is critical, as it reveals whether the initial network state already experiences overloads or other issues that prevent full supply of demand.

Each bus in the network is then iteratively taken out of service along with its connected elements, simulating a realistic contingency scenario. Loads that become electrically isolated from power sources due to these outages are explicitly identified and disabled in the model. The demand of these disabled loads is directly added to the contingency's ENS to ensure the metric accurately reflects all unserved energy. This step is necessary because OpenDSS alone does not automatically account for disconnected loads during contingency analysis. Failure to manually disable these loads often causes power flow non-convergence, leading to unreliable or missing ENS results.

Following each contingency event, a power flow simulation recalculates the network state, allowing for updated computation of the ENS, which quantifies the additional unserved energy caused by the component outage. The difference between the post-contingency ENS and the baseline serves as a direct measure of the vulnerability contribution of the removed element. For clarity, the increase in ENS associated with each contingency is calculated as:

$$ENS_{increase} = ENS_{contingency} - ENS_{baseline} = ENS_{disconnected\ loads} + ENS_{simulation} - ENS_{baseline}$$

After processing each scenario, the system automatically restores the network to its baseline state to ensure independence of analyses. Results from all contingency scenarios are systematically collected, summarized, and prepared for evaluation and comparison against MCA metrics.

Chapter 4. RESULTS AND ANALYSIS

This chapter presents the results and analysis derived from the modelling and simulation framework developed in this project. The outputs of the centrality metrics across the distribution network are examined, providing a comprehensive overview of both purely topological and hybrid centrality measures. These results are compared with the ENS values obtained from the contingency analysis, enabling a direct evaluation of the extent to which MCA can predict the vulnerability of each node to supply disruptions. The aim is to investigate potential correlations and insights into network vulnerability.

The core findings focus on a primary case study for illustrative clarity, while additional scenarios and extended results are documented in Appendix for reference and completeness.

4.1 TOPOLOGICAL METRICS

The main case will analyse the distribution network located in Greasby, which SP MANWEB manages. Further details of each analysed network are given in section 3.3.1.

As observed in Figure 13, most nodes exhibit low degree values, which reflects the limited connectivity that is characteristic of distribution networks. This degree distribution, where average node degree is 2.002, totally suits with the inherently radial and hierarchical structure typical of power distribution networks, where most nodes serve as simple endpoints and only a few act as main feeders or connection hubs.

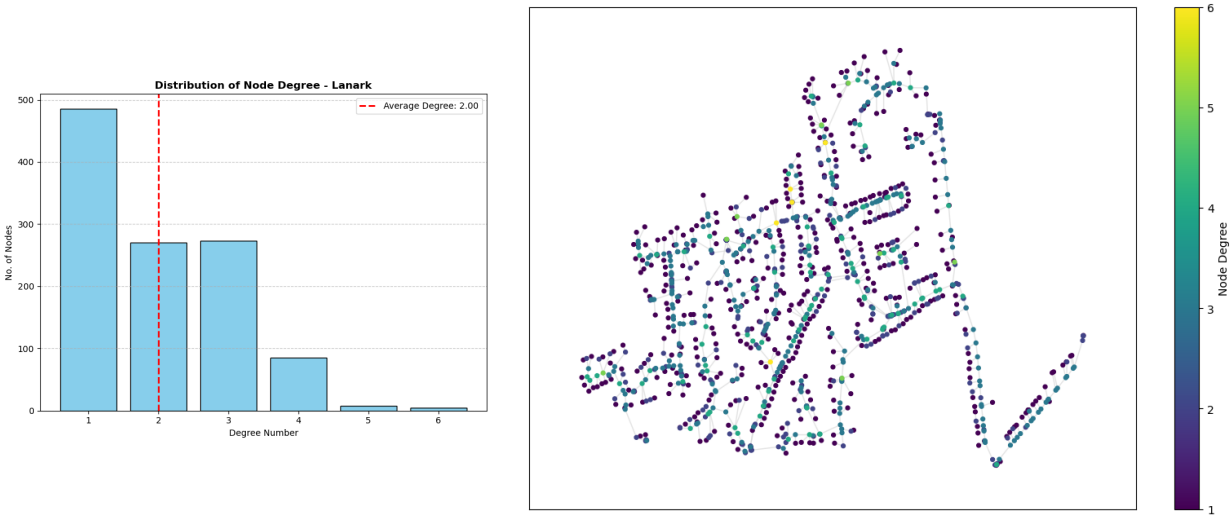

Figure 13: Distribution of node degree in the Greasby distribution network

Figure 14 shows comparisons between the five purely topological centrality metrics and the calculated ENS values of the respective nodes when simulating its failure in the network.

For the clustering coefficient analysis, the scatter plot shows that the vast majority of nodes have clustering coefficient values of zero. Only a small number of nodes have non-zero values and they do not show any meaningful correlation with ENS.

This pattern reflects the inherently radial topology of distribution networks, which implies little local redundancy and high vulnerability to the disconnection of key nodes. This strongly contrasts with the meshed configurations typical of transmission networks. In radial systems, nodes are connected in a tree-like structure where each load point typically has only one path to the source. This fundamentally prevents the formation of triangles, which is what the clustering coefficient equation (5) is based on.

On the other hand, transmission networks have significantly more connections and meshed topologies, which are specifically designed to provide multiple power flow paths and system redundancy. Consequently, these networks have naturally higher clustering coefficients. This leads to diverse values that could serve as meaningful indicators of structural vulnerability and operational flexibility, as proved in the IEEE 30 bus validation.

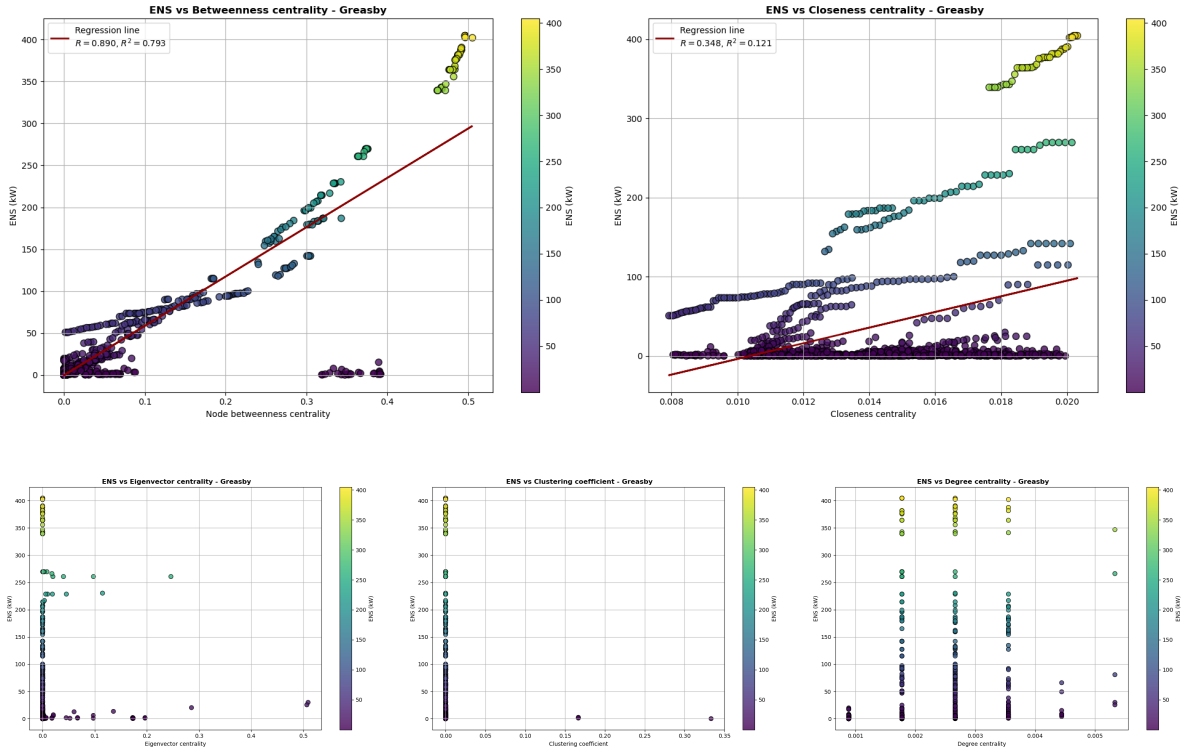

Figure 14: Comparative scatter plots of five topological centrality metrics against ENS in the Greasby network

Eigenvector centrality also reveals another fundamental limitation when applied to distribution networks. It can be appreciated that most nodes are grouped near zero, with only a few nodes displaying higher values. However, these nodes with values different to zero, do not show any meaningful correlation with ENS outcomes.

This tendency to null values stems from several factors typical of large distribution networks. In general, network size plays a crucial role in centrality metrics. Specifically in eigenvector centrality, it tends to decrease its robustness with increasing network size [59]. For this type of distribution networks, where there are hundreds or even thousands of components, this relation could lead to many centrality values becoming insignificantly small.

Additionally, eigenvector centrality of a node strongly depends on being connected to other important nodes, as mentioned in equation (4). Therefore, in large and disperse networks with a low average degree, the probability of a node being peripheral increases, which fosters the appearance of small eigenvalues.

Moreover, the degree centrality plot presents vertical bands, which reflect the fact that node degree values are discrete. Nodes with the same degree value create these distinctive vertical lines on the plot, because degree centrality is determined by dividing the node's total number of connections by the number of nodes in the network minus one.

There is not a clear correlation with ENS, although it is worth mentioning that every node with degree 1 has very low ENS. This stands to reason, as loads will typically always have degree one and when disconnected, they only affect one customer. However, on the whole, nodes exhibit a broad range of ENS values regardless of their degree, suggesting there is no significant relationship.

This discrepancy between ENS and degree centrality makes sense, because for example a node that serves low-demand areas, may have a high degree centrality due to its numerous connections but, it will only make a small contribution to system vulnerability. Nevertheless, if a node is connected to high-demand clients or is near a transformer, nodes with lower degree centrality can produce a sizable amount of ENS, proving that structural connectivity is not enough to assess distribution system vulnerabilities.

Finally, it is worth looking more closely at both betweenness and closeness centrality since they both show at least some predictive potential for finding vulnerable nodes. A distinct positive trend can be seen in the betweenness plot, as nodes with higher betweenness centrality typically have bigger ENS values.

In comparison, more noise can be appreciated in the analysis for closeness centrality. A significant number of nodes with high closeness scores cause little ENS when they fail, despite the fact that many other high closeness nodes correlate with heightened ENS. This suggests that closeness may occasionally overestimate criticality for well connected, but low demand nodes.

Figure 14 shows that betweenness centrality has a more robust linear correlation with ENS, indicated by a coefficient of determination of 0.793. Whereas closeness centrality has a notably lower R^2 of 0.121, which is due to the overestimation mentioned earlier that causes many nodes to be considered as topologically relevant, but do not correspond with a high ENS.

This outstanding performance of betweenness centrality suggests that the concept of intermediary importance, or more simply nodes that lie on shortest paths between other node pairs, translates meaningfully to operational vulnerability. Hence, further study has concentrated on the correlation of betweenness centrality and network vulnerability.

A Spearman rank correlation was carried out in order to provide a more nuanced evaluation than linear correlation. By using the ranking of the values of two variables instead of their actual magnitudes, the Spearman ranking compares how good the order is, not focusing so much linearity, but on if the nodes are consistently ordered. In that way, Spearman correlation can reveal whether nodes identified as most critical by betweenness centrality are also those that yield the highest ENS.

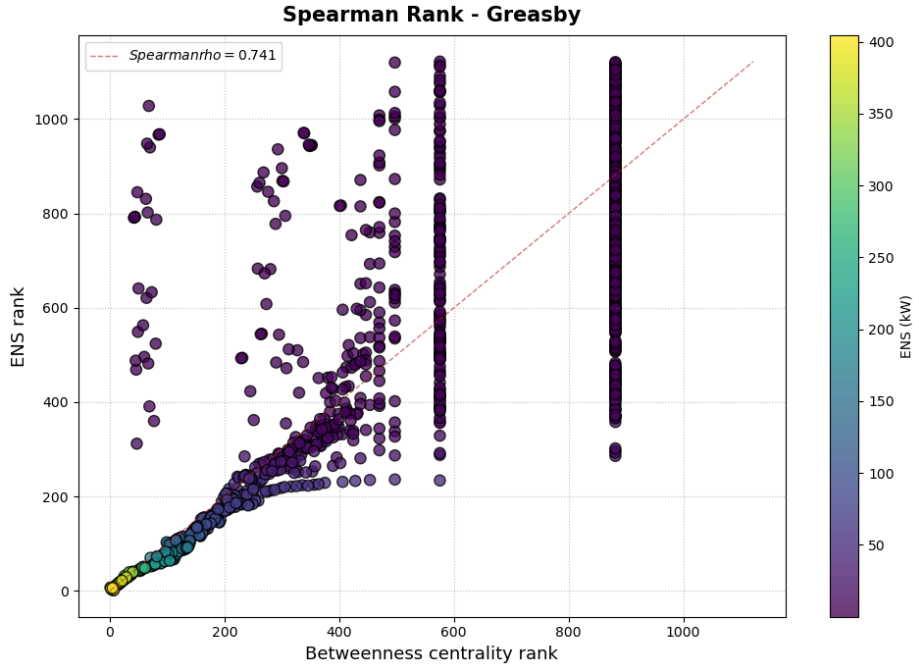

Figure 15: Spearman rank correlation plot comparing node rankings by betweenness centrality and ENS in the Greasby network

It can be appreciated that the most significant nodes congregate along the diagonal, which shows that the metric is able to reflect the actual criticality of the node. A Spearman's ρ score of 0.741 demonstrates a significant correlation between betweenness centrality and ENS, regarding their order. This indicates that nodes identified as critical by betweenness centrality generally correspond with those that yield higher ENS when eliminated. Thereby, validating its efficacy as a vulnerability indicator in distribution networks.

However, a thorough examination of Figure 15 reveals that betweenness centrality overestimates the criticality of a sizable group of nodes. Notably, many other nodes attain high betweenness rankings, yet they are associated with lower ENS ranks. This appears as a large number of dots dispersed well above the diagonal. Additionally, two vertical bands at the right side of the plot can be observed, which happen due to the fact that the network is very large and not so interconnected. This causes nodes with less structural relevance to not be differentiated by betweenness, resulting in the metric assigning all of them the same value.

To gain a clearer understanding of this overestimation phenomenon, we have highlighted the most critical nodes and the overestimated nodes directly on the network plot. This visualization in Figure 16 allows to spatially examine whether there is a structural basis for the overestimation by betweenness centrality. From this, it appears that some of the nodes identified as overestimated correspond to key connecting lines or main streets. In that way, structurally, they represent important links and redundancy within the network topology.

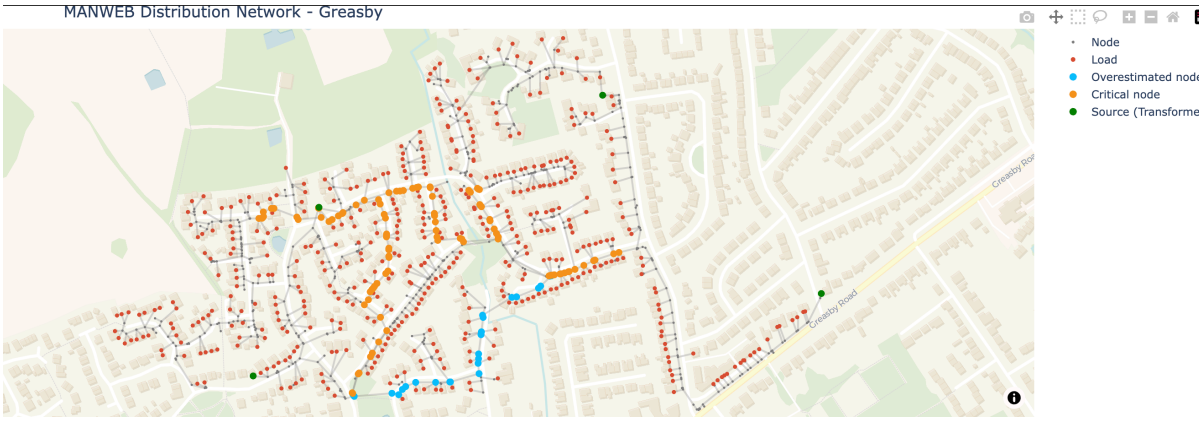

Figure 16: Highlighted Whifflet's network representation showing critical nodes and overestimated nodes

But, despite this structural significance, these connections may not be as electrically essential in terms of maintaining customer supply. In other words, while these nodes serve important topological roles by linking different areas, their failure does not necessarily translate into large scale supply interruptions reflected by the ENS metric. This divergence shows a fundamental limitation of purely topological metrics like betweenness centrality in distribution networks. They capture structural importance, but do not fully reflect the electrical operational impact of node failures.

These drawbacks highlight the need for a more sophisticated vulnerability assessment. Although betweenness centrality has shown impressive results in identifying electrically vulnerable nodes, as all critical nodes are identified correctly. Nonetheless, examining hybrid centrality metrics could enhance those results, as they incorporate electrical data into the model.

4.2 HYBRID METRICS

Current-flow (CF) centrality metrics are a class of hybrid centrality indicators that incorporate electrical properties of the network. As already mentioned in the Theoretical framework section, these hybrid formulations provide a more physically grounded view of structural vulnerability. They are therefore expected to produce results that outperform the purely topological centralities. The first hybrid centrality analysed is CF closeness centrality, which adds line impedances into the original concept of the topological metric.

The behaviour of the relation in Figure 17 is very similar to the closeness centrality plot in Figure 14. Although they both look alike, CF closeness has improved the coefficient of determination from 0.121 to 0.187. However, this overall gain remains limited compared to expectations.

This modest increase in the R^2 suggests that impedance information alone may not be enough for the relation to improve significantly. One possible explanation is that in distribution networks lines could have similar characteristics. Therefore, the difference in impedance values is not enough for the weighted methodology to provide more accurate results.

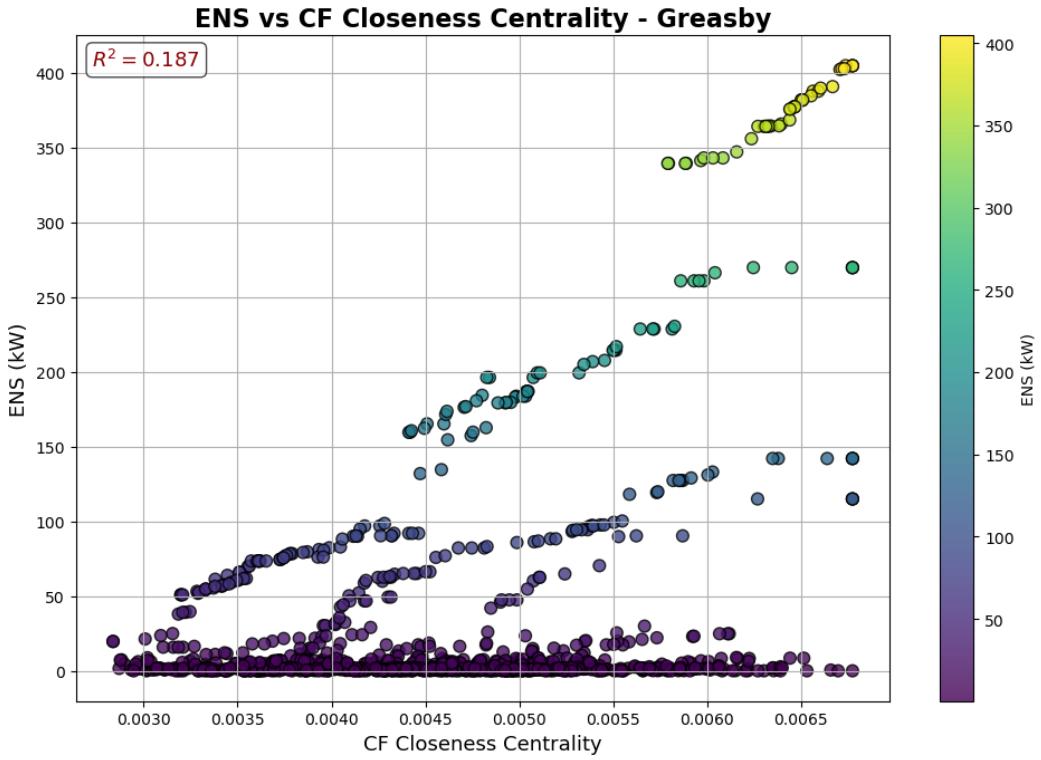

Figure 17: Scatter plot of ENS against current-flow closeness centrality in the Greasby network

Although this type of behaviour represents the general trend across the analysed networks, there is an exception for Whifflet's network where the improvement is considerably more notable. It can be appreciated in Figure 33 that there is a more visible relation between ENS and the metric, with not so many nodes being incorrectly overestimated and the R^2 is 0.547. Figure 34 shows that it has in effect a very strong correlation, with a Spearman's ρ of 0.745.

Nevertheless, it is worth mentioning that topological betweenness for Whifflet's distribution network has a coefficient of determination $R^2 = 0.876$ and a Spearman's ρ of 0.860. So, there is general improvement in this network regarding the correlation between vulnerability and centrality metrics. This outstanding performance may be partly explained by the smaller size and lower complexity of this network compared to the others in the study. With fewer nodes and less topological diversity, the relation between electrical distance and node criticality remains cleaner. Therefore, there are less paths or redundancies that introduce noise into the correlation like in larger networks and the metric is able to reflect more clearly the most vulnerable nodes of the network.

CF line betweenness was studied next. Figure 18 shows the centrality values directly mapped in Greasby's distribution network following a colour scale. This metric takes into account which nodes are generators or loads, as it calculates a centrality value for every possible generator and load pair, which are also referred to as source and target pair in equation (9).

It can be appreciated how the lines located close to source nodes, usually score a much higher value than other end lines. It is also worth noting how lines that serve as main connectors between different areas are consistently assigned high values, such as the yellow-coloured line that goes until the connection with the bottom part of the network. When compared to where real critical nodes are located in Figure 16, there is evidence that the metric captures very satisfactorily the vulnerabilities in the electric grid.

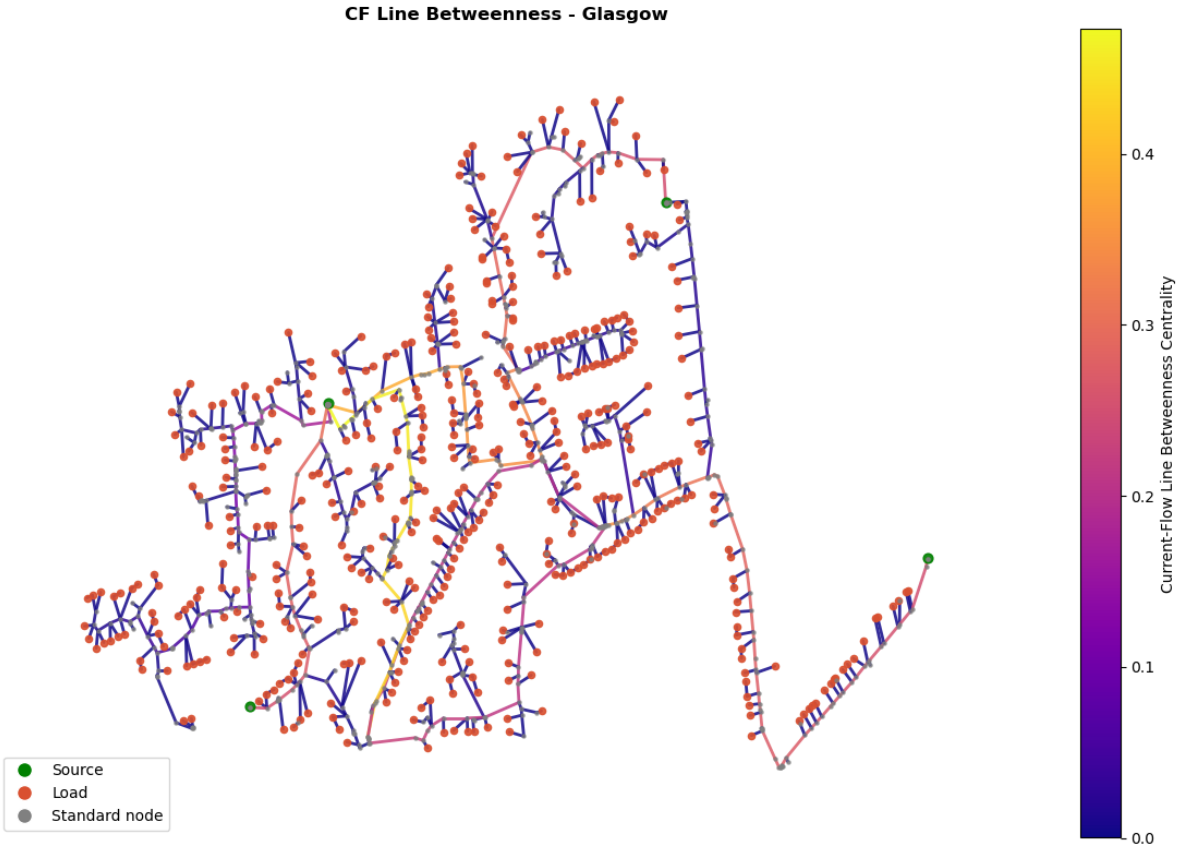

Figure 18: Visualization of current-flow line betweenness centrality values in the Greasby network

Given that CF line betweenness is, by nature, a metric defined for lines and the authors of [38] did not provide an equivalent node metric, it has been necessary to convert values into a node-based version. To accomplish this, the values of all adjacent lines to each node were summed and assigned to that node as its aggregated score. This methodology enables the comparison of this metric with other nodal scores and with the ENS benchmark.

The resulting scatter plot in Figure 19 shows a coefficient of determination of 0.699, which is lower than the purely topological betweenness metric, that had an R^2 of 0.793. However, nodes with higher CF betweenness score tend to have a higher ENS value, which indicates that this metric is good at assessing electrical vulnerability. Although there is an outlier group located towards the bottom right, which means that the metric overestimates vulnerability, it has not been assigned values as large as those of the truly most vulnerable nodes. Thus, even if the plot is slightly deviated, the metric seems to distinguish well among the most critical nodes. Therefore, a Spearman rank was also conducted to confirm this assumption.

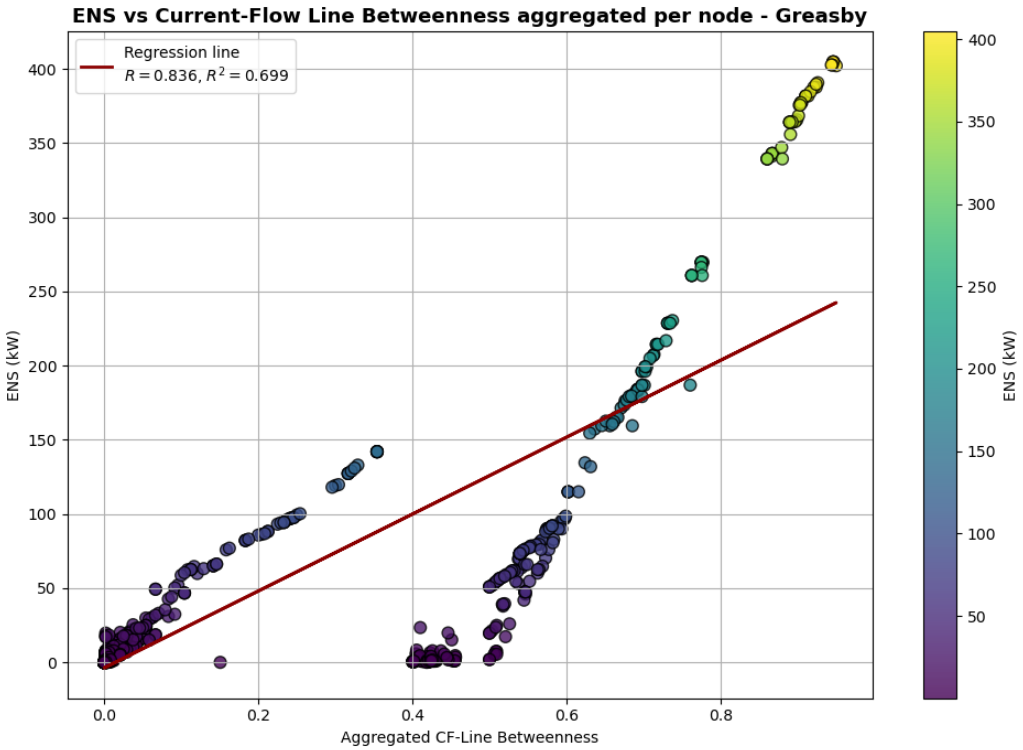

Figure 19: Scatter plot of ENS against current-flow line betweenness centrality in the Greasby network

In effect, Figure 20 shows excellent results at the identification of the most vulnerable nodes in the network. No nodes have been overestimated and compared to the most critical ones, in other words, the metric has not assigned similar values to electrically not so vulnerable nodes, as occurred with betweenness centrality in Figure 15.

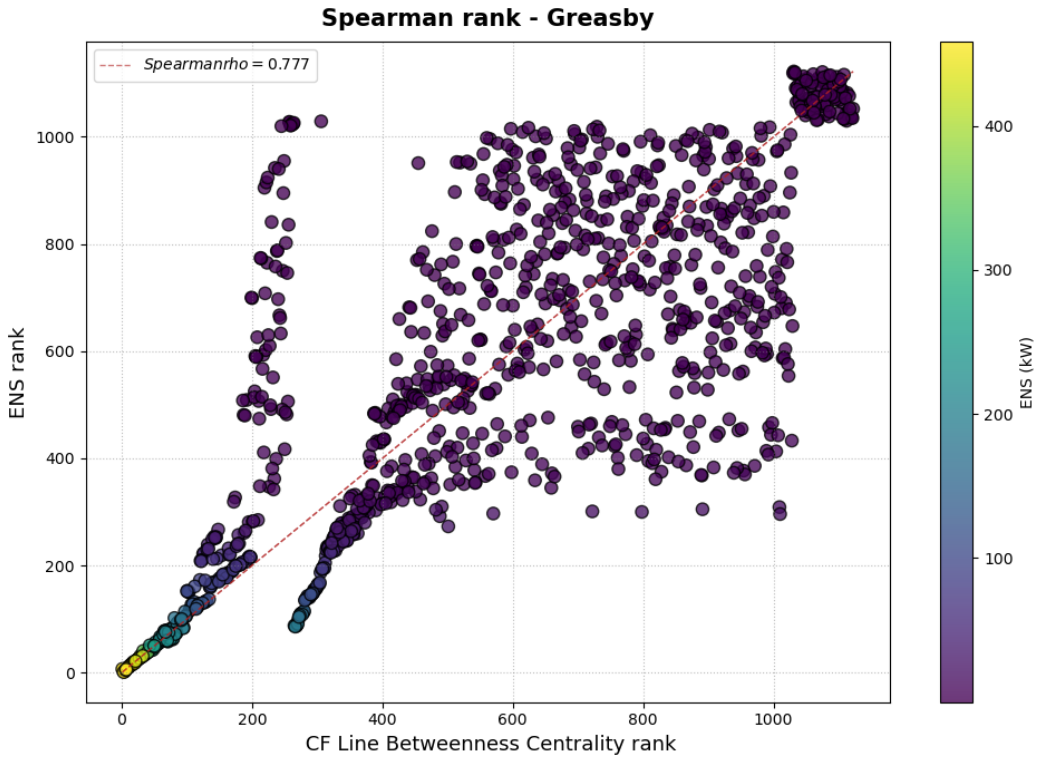

Figure 20: Spearman rank correlation plot comparing node rankings by CF line betweenness centrality and ENS in the Greasby network

Furthermore, as criticality decreases, nodes start to disperse above and below the diagonal and accuracy worsens. However, the vertical bands that appeared in Figure 15 are not present in this plot. This means that this metric is also able to distinguish between not so critical nodes, although it is clearly much better at assessing the most critical nodes in the network.

The Spearman's ρ has improved from 0.741 in the purely topological betweenness centrality to 0.777 in this metric. Most importantly, all critical nodes are correctly identified, and there is no overestimation of non-critical nodes relative to truly vulnerable ones.

As already mentioned, it is logical that results become more imprecise as vulnerability decreases, as in distribution networks it is difficult to differentiate between peripheral lines, where most loads are connected to. Nevertheless, CF line betweenness performs excellently for the most vulnerable nodes in the distribution grid, which is a great achievement. This strong performance demonstrates its potential as an effective screening tool for distribution network vulnerability assessment.

4.3 COMPUTATIONAL EFFICIENCY AND PRACTICAL APPLICATIONS

The table below summarizes the computation times required for both traditional contingency analysis and the proposed MCA method, including the hybrid metrics, across the four distribution networks analysed in this study.

Table 1: Computation time comparison between traditional approach and MCA

Distribution network	Contingency Analysis (s)	MCA (s)	Speed-up factor
Greasby	95.5	7	13.64
Moreton	103.2	6.1	16.92
Glasgow	3.7	0.2	18.5
Lanark	43.9	2.7	16.26

Across all cases, MCA delivers substantial computational savings compared to conventional contingency analysis. For example, in the Moreton and Greasby networks, traditional analysis required over 1.5 minutes per run, while MCA completed the equivalent assessment in no more than 7 and 6 seconds, respectively. This represents a speed-up factor of approximately 16 times or even more in some cases.

From the case studies, it is observed that each distribution network typically includes multiple transformers. For a network the size of SPEN, with approximately 30,000 substations [60] and 159,084 stored files corresponding to LV distribution circuits, the potential computational savings are considerable. They were estimated using the processing times measured for the Greasby network as a reference case:

$$1 - \frac{7}{95.5} = 0.927$$

This corresponds to an estimated computational saving of around 92% compared with conducting a full contingency analysis.

Such computational efficiency directly benefits DNOs when screening large scale distribution areas. If the entire SPEN network, covering thousands of feeders, were to be analysed using traditional methods, the cumulative computation time could run into many hours or even days, becoming a bottleneck for planning and real-time decision-making. By contrast, MCA reduces this to a few seconds per network.

This method could be used as a first stage screening tool to quickly filter and prioritise the most critical nodes in the network. The time saved could then be invested in carrying out more detailed and accurate analyses on this reduced set of priority nodes, ensuring that engineering and computational resources are focused where they deliver the greatest value.

Chapter 5. CONCLUSIONS

The project conducted a comprehensive review of the state of the art of different vulnerability assessment approaches, as well as centrality metrics applied to electrical distribution networks. In which both purely topological indicators and more recent hybrid formulations that incorporate electrical properties were covered. The open source OpenDSS was used to perform the contingency analysis benchmark, while NetworkX python library was employed to calculate most of the centrality metrics. The objective was to evaluate how effectively the MCA approach, based on these metrics, can identify vulnerabilities in electrical distribution networks.

4 real UK distribution network models were selected as case studies, representing a range of sizes and meshing levels, and simulated under peak demand conditions using a contingency analysis approach. Both topological and hybrid metrics were evaluated individually to assess their effectiveness in identifying critical nodes. The methodology achieved significant computational savings compared to full contingency analysis, enabling rapid screening of network vulnerabilities while maintaining high accuracy for the most critical elements.

The comparative analysis of centrality metrics reveals remarkably different levels of effectiveness in assessing vulnerability across different distribution network topologies. Betweenness centrality demonstrated a surprisingly robust performance taking into account it only relied on topological information. However, it tended to overestimate the criticality of certain nodes, giving similar values to genuinely vulnerable and less vulnerable nodes. Nevertheless, this metric has proved useful results as a rapid screening tool to identify a subset of potentially critical nodes. In this way, allowing DNOs to focus more detailed computational resources and further studies on this reduced set.

Other standard topological metrics showed more limited applicability. Clustering coefficient and eigenvector centrality both provided insufficient discrimination between nodes in all the analysed networks. This reflects the fact that distribution grids, by their nature, have a low level of local clustering and tend to be weakly connected. These metrics fail to capture meaningful

differences in node vulnerability, as they need a level of meshing and a considerable number of interconnections that are not typical in distribution systems. Degree centrality is a potentially informative metric that can serve as a global indication of network connectivity. However, it showed no clear relationship with vulnerability to supply interruptions. This is logical as the number of direct connections does not equate to operational criticality.

However, it is worth noting that in MV networks, which tend to be more meshed and have a greater degree of interconnection, metrics such as clustering coefficient and eigenvector centrality could prove more promising. The increased complexity and redundancy in these networks provide a richer topological structure where these metrics can better differentiate node importance and vulnerability.

Hybrid current-flow centrality metrics usually outperformed their purely topological counterparts. The CF line betweenness centrality, which integrates both the electrical properties and the structural position of each node, was generally found to be the most effective metric for identifying vulnerable nodes across all case study networks.

However, it is worth noting that both betweenness-based metrics, the best topological and the best hybrid approach, delivered very strong results in identifying the most critical nodes. Ultimately, this is the primary concern for operational planning. While the detailed ranking for less critical or more peripheral nodes may show greater dispersion, this is of secondary importance for practical applications.

The metric could be employed as a first filter to rapidly identify the subset of nodes that need more detailed analysis. This would allow DNOs to focus computational resources and further studies on these most critical elements. Therefore, a new approach with a two stage methodology could be developed, where CF line betweenness could provide an initial ranking and more sophisticated and computationally expensive analysis techniques would be then applied to the identified critical nodes.

In conclusion, the study demonstrates that while some standard centrality measures offer only limited insight in the context of real distribution networks, betweenness-based approaches can

identify the most vulnerable parts of the grid. Especially when extended into hybrid formulations, where line impedances are included.

Scottish Power could therefore implement MCA as a routine screening tool across the entire network. In this way, critical nodes can be identified for investment purposes or robustness planning in minutes. This would allow only a small subset to be passed on to slower or more expensive detailed studies. Beyond the raw time saving, such an approach would enable faster responses to emerging network issues or a better prioritisation of reinforcement projects.

Chapter 6. FUTURE WORK

The main improvement that could be made to this project's analysis would be to include more operational scenarios to better capture the variability and complexity of modern distribution networks. Due to time constraints, the study focused primarily on peak demand conditions without considering other important scenarios such as low demand periods, which can significantly affect network vulnerability patterns. Incorporating scenarios with varying load levels, especially low demand combined with high or moderate DG penetration, would allow assessment of how the metrics perform under other conditions.

Additionally, including variations in network configuration, such as different switching states or the presence of energy storage, could provide deeper insights into the robustness of MCA vulnerability assessments. Evaluating the influence of distributed generation on vulnerabilities is particularly important as DG alters power flows, potentially reducing the effectiveness of purely topological metrics and increasing the value of hybrid metrics.

In this project, ENS was used as the vulnerability benchmark for evaluating the effectiveness of different centrality metrics in identifying critical nodes. While ENS is a widely accepted and intuitive indicator for assessing the operational impact of node failures under peak demand conditions, other vulnerability metrics could offer additional or complementary insights. For example, loss of load probability or number of affected customers, especially when considering different network priorities or regulatory requirements. Therefore, it could also be valuable to investigate how centrality metrics correlate with other alternative vulnerability measures.

Moreover, in low demand scenarios or high DG penetration, ENS does not capture the relevant vulnerabilities. In such cases, specific indicators reflecting issues like voltage deviations, reverse power flows, or local generation curtailment are more appropriate.

Another valuable extension of this work would be to apply the analysis to MV networks, as their more meshed and interconnected structure could enhance the performance of certain purely topological metrics, such as clustering coefficient and eigenvector centrality. In such

networks, the richer connectivity and higher level of redundancy provide a topology in which these metrics may better capture meaningful differences in node criticality.

Regarding potential future work, a promising direction would be to use the betweenness-based centrality metrics, which were identified in this study as having the strongest correlation with network vulnerability, to give network reconfiguration or reinforcement proposals. A future project could develop an optimization framework that proposes new network configurations or identifies strategic locations for reinforcement based on these metrics. Such an approach would use the most effective centrality metrics to suggest topology changes or new line investments aimed at improving overall network resilience and reliability. This would build on the current work by moving from vulnerability assessment to actionable network design recommendations.

Chapter 7. BIBLIOGRAPHY

[1] SP Energy Networks, "Distribution Annual Performance Report 2023/24," 2024. [Online]. Available: https://www.spenergynetworks.co.uk/userfiles/file/SP__Energy_Networks_Distribution_Annual_Performance_Report_2023-24.pdf. [Accessed 6 July 2025].

[2] C. Ambes and S. Crampes, "The Value of Lost Load," Florence School of Regulation, 18 June 2018. [Online]. Available: https://fsr.eui.eu/the-value-of-lost-load/. [Accessed 25 July 2025].

[3] Electricity North West Ltd., "The Value of Lost Load," Manchester, UK, Nov. 2020.

[4] National Energy System Operator, "Future Energy Scenarios (FES)," 2025. [Online]. Available: https://www.neso.energy/publications/future-energy-scenarios-fes. [Accessed 6 July 2025].

[5] A. Mittal, J. Hazra, N. Jain, V. Goyal, D. P. Seetharam and Y. Sabharwal, "Real time contingency analysis for power grids," 2011. [Online]. Available: https://doi.org/10.1007/978-3-642-23397-5_31. [Accessed 1 August 2025].

[6] A. B. M. Nasiruzzaman, H. R. Pota and F. R. Islam, "Method, impact and rank similarity of modified centrality measures of power grid to identify critical components," in *11th International Conference on Environment and Electrical Engineering*, Venice, Italy, 2012.

[7] P. Espinoza-Arriagada, G. A. Ruz and L. Gutierrez-Lagos, "Graph Theory-Based Topological and Nodal Analysis for Identifying Critical Points to Enhance Resilience in Electrical Distribution Systems," in *CIRED 2025 Conference, Paper 686*, Vienna, Austria, Jun. 2025.

[8] Enel, "Integrated Annual Report 2022," April 2023. [Online]. Available: https://www.enel.com/content/dam/enel-com/documenti/investitori/informazioni-finanziarie/2022/annuali/en/integrated-annual-report_2022.pdf. [Accessed 25 July 2025].

[9] Electric Power Research Institute, "EPRI," 20 October 2023. [Online]. Available: https://www.epri.com/research/products/000000003002026315. [Accessed 25 July 2025].

[10] Consolidated Edison, Inc., "Company ESG Update," June 2021. [Online]. Available: https://investor.conedison.com/static-files/108ae9e7-84bb-408e-bdca-8539ecd18e49. [Accessed 25 July 2025].

[11] Union for the Coordination of Transmission of Electricity (UCTE), "Operation Handbook – Policy 3: Operational Security," March 2009. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_3_final.pdf. [Accessed 25 July 2025].

[12] J. J. Grainger and W. D. Stevenson, Power System Analysis, McGraw-Hill, 1994.

[13] IEEE Power and Energy Society, "IEEE Recommended Practice for Monitoring Electric Power Quality," August 2019. [Online]. Available: https://standards.ieee.org/ieee/1159/6124/. [Accessed 26 July 2025].

[14] IEC Technical Committee 73, "IEC 60909-3," March 2009. [Online]. Available: https://webstore.iec.ch/en/publication/3890. [Accessed 26 July 2025].

[15] IEC Technical Committee 56, "Fault Tree Analysis (FTA)," 26 December 2006. [Online]. Available: https://webstore.iec.ch/en/publication/4311. [Accessed 2025 July].

[16] R. Allan and R. Billinton, "Probabilistic Assessment of Power Systems," February 2000. [Online]. Available: https://home.engineering.iastate.edu/~jdm/ee653/BasicConcept_ReliabilityEvaluation.pdf. [Accessed 26 July 2025].

[17] D. M. El-Hassanin, S. S. Kaddah and M. M. El-Saadawi, "Short Circuit Analysis of Power Distribution Network Including Distributed Generations," *Port-Said Engineering Research Journal,* vol. 17, no. 1, pp. 122-130, 2013.

[18] T. Gonen, "Electric Power Distribution Engineering," 2014. [Online]. Available: https://students.aiu.edu/submissions/profiles/resources/onlineBook/Z7e5T7_Electric_Power_Distribution_Engineering-_Third_Edition.pdf. [Accessed 27 July 2025].

[19] IEEE Industry Applications Society, "IEEE Recommended Practice for Electric Power Distribution for Industrial Plants," 1994. [Online]. [Accessed 27 July 2025].

[20] H. Farhangi, "The path of the smart grid," March 2009. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5357331. [Accessed 27 July 2025].

[21] D. Kim, B. Reidenbach, B. Motherway and V. Rozite, "International Energy Agency," May 2022. [Online]. Available: https://www.iea.org/reports/unlocking-the-potential-of-distributed-energy-resources. [Accessed 28 July 2025].

[22] J. Marqusee and A. Stringer, "Distributed Energy Resource (DER) Reliability for Backup Electric Power Systems," 2023. [Online]. Available: https://doi.org/10.2172/1964053. [Accessed 27 July 2025].

[23] D. Pudjianto, P. Djapic, G. Strbac, E. T. van Schalkwyk and B. Stojkovska, "DER reactive services and distribution network losses," 2020. [Online]. Available: https://digital-library.theiet.org/doi/full/10.1049/oap-cired.2021.0111. [Accessed 27 July 2025].

[24] I. B. Majeed and N. I. Nwulu, "Impact of Reverse Power Flow on Distributed Transformers in a Solar-Photovoltaic-Integrated Low-Voltage Network," December 2022. [Online]. Available: https://www.mdpi.com/1996-1073/15/23/9238. [Accessed 27 July 2025].

[25] A. M. Howlader, S. Sadoyama, L. R. Roose and Y. Chen, "Active power control to mitigate voltage and frequency deviations for the smart grid using smart PV inverters," February 2020. [Online]. Available: https://doi.org/10.1016/j.apenergy.2019.114000. [Accessed 27 July 2025].

[26] M. Meskin, A. Domijan and I. Grinberg, "Impact of distributed generation on the protection systems of distribution networks: analysis and remedies – review paper," 13 November 2020. [Online]. Available: https://doi.org/10.1049/iet-gtd.2019.1652. [Accessed 27 July 2025].

[27] International Energy Agency, "Unlocking the Potential of Distributed Energy Resources," May 2022. [Online]. Available: https://www.iea.org/reports/unlocking-the-potential-of-distributed-energy-resources. [Accessed 28 July 2025].

[28] Bloomberg NEF, "Electric Vehicle Outlook 2025," May 2025. [Online]. Available: https://about.bnef.com/insights/clean-transport/electric-vehicle-outlook/#key-numbers. [Accessed 28 July 2025].

[29] Y. Li and A. Jenn, "Impact of electric vehicle charging demand on power distribution grid congestion," April 2024. [Online]. Available: https://doi.org/10.1073/pnas.2317599121. [Accessed 28 July 2025].

[30] D. Sebilleau and M. Tiguercha, "L'impact de l'intégration des véhicules électriques dans le réseau électrique," 7 April 2021. [Online]. Available: https://www.trialog.com/fr/impact-vehicules-reseau/. [Accessed 28 July 2025].

[31] R. Ibrahim, I. Gaber and N. Zakzouk, "Analysis of multidimensional impacts of electric vehicles penetration in distribution networks," 13 November 2024. [Online]. Available: https://doi.org/10.1038/s41598-024-77662-6. [Accessed 28 July 2025].

[32] International Energy Agency (IEA), "Heating – Energy System: Buildings," July 2023. [Online]. Available: https://www.iea.org/energy-system/buildings/heating. [Accessed 28 July 2025].

[33] K. Fenaughty, D. Parker, J. Butzbaugh and C. Colon, "Detailed Evaluation of Electric Demand Load Shifting Potential of Heat Pump Water Heaters in a Hot Humid Climate," February 2024. [Online]. Available: https://www.doi.org/10.1080/23744731.2023.2261808. [Accessed 28 July 2025].

[34] T. L. Lee, "Implications of Heating Electrification on Distribution Networks and Distributed Energy Resources," May 2022. [Online]. Available: https://hdl.handle.net/1721.1/144976. [Accessed 28 July 2025].

[35] E. a. I. S. Department for Business, "Heat Pump Ready Programme: Background on Innovation Needs," December 2021. [Online]. Available:

https://assets.publishing.service.gov.uk/media/66d1f4bdd107658faec7e42c/heat-pump-ready-background-innovation-needs.pdf. [Accessed 28 July 2025].

[36] S. Jeong, J. Kim and S. Lee, "A Study on Volt-Watt Mode of Smart Inverter to Prevent Voltage Rise with High Penetration of PV System," February 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8973860. [Accessed July 2025].

[37] W. Liu, T. Zhang, C. Lin, K. Li and R. Wang, "Graph Attention Networks Unleashed: A Fast and Explainable Vulnerability Assessment Framework for Microgrids," March 2025. [Online]. Available: https://arxiv.org/html/2503.00786v1. [Accessed 29 July 2025].

[38] S. Maity and P. Panigrahi, "Vulnerability and Efficiency Assessment of Complex Power Grids Using Current-Flow Line Centralities," April 2024. [Online]. Available: https://arxiv.org/pdf/2404.10005. [Accessed 29 July 2025].

[39] Y. Alrowaili, N. Saxena and P. Burnap, "Towards Developing an Asset-Criticality Identification Framework in Smart Grids," September 2024. [Online]. Available: https://orca.cardiff.ac.uk/id/eprint/171133/1/2024217970.pdf. [Accessed 29 July 2025].

[40] S. Porta, P. Crucitti and V. Latora, "Centrality measures in spatial networks of urban streets," *Phys. Rev. E,* vol. 73, no. 3, April 2006.

[41] S. Porta, P. Crucitti and V. Latora, "Multiple centrality assessment in Parma: a network analysis of paths and open spaces," *Urban Design International,* vol. 13, no. 1, 2008.

[42] J. Li, X. Wang and T. Zhang, "Sequence-based centrality measures in maritime transportation networks," *IET Intell. Transp. Syst.,* vol. 14, pp. 2042-2051, 2020.

[43] S. Forsberg, K. Thomas and M. Bergkvist, "Power grid vulnerability analysis using complex network theory: A topological study of the Nordic transmission grid," *Physica A: Statistical Mechanics and its Applications,* vol. 626, 2023.

[44] P. Hines and S. Blumsack, "A Centrality Measure for Electrical Networks," *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008),* pp. pp. 185-185, 2008.

[45] L. Liu, N. Du and D. Sheng, "Security-centric node identification in complex networks," May 2025. [Online]. Available: https://doi.org/10.1038/s41598-025-00360-4. [Accessed 30 July 2025].

[46] M. M. Rahman, A. S. Akash, H. Pirim, C. Le, T. Q. Le and O. P. Yadav, "Enhancing electrical network vulnerability assessment with machine learning and deep learning techniques," June 2024. [Online]. Available: https://orb.binghamton.edu/nejcs/vol6/iss1/2. [Accessed 2 August 2025].

[47] Z. Yang, H. Min, J. Zhao, X. Dong, F. Yang, C. Wang and N. Zhang, "Vulnerability analysis of power grid structure based on complex network theory," January 2025. [Online]. Available: https://doi.org/10.3389/fenrg.2024.1498678. [Accessed 1 August 2025].

[48] F. Gutierrez, E. Barocio, F. Uribe and P. Zuniga, "Vulnerability analysis of power grids using modified centrality measures," 25 February 2013. [Online]. Available: http://dx.doi.org/10.1155/2013/135731. [Accessed 1 August 2025].

[49] J. Dias, A. N. Montanari and E. E. N. Macau, "Power-grid vulnerability and its relation with network structure," March 2023. [Online]. Available: https://doi.org/10.1063/5.0137919. [Accessed 1 August 2025].

[50] "NetworkX – Python Package for Complex Network Analysis," [Online]. Available: https://networkx.org. [Accessed 30 July 2025].

[51] "Plotly – Interactive Data Visualization and Dash App Framework," [Online]. Available: https://plotly.com. [Accessed 30 July 2025].

[52] "Matplotlib – Comprehensive Python Library for Static, Animated, and Interactive Visualizations," [Online]. Available: https://matplotlib.org. [Accessed 30 July 2025].

[53] "Seaborn – Statistical Data Visualization Library for Python," [Online]. Available: https://seaborn.pydata.org. [Accessed 30 July 2025].

[54] "pandapower – Open-Source Python Tool for Automated Power System Modeling and Analysis," [Online]. Available: https://www.pandapower.org. [Accessed 30 July 2025].

[55] SP Energy Networks, "SP Manweb Network Development Plan 2024 – Parts 1 and 2: Main Report," May 2024. [Online]. Available: https://www.spenergynetworks.co.uk/userfiles/file/SP_Energy_Networks_2024_Network_Development_Plan_-_SP_Manweb_Parts_1and2_-_Main_Report.pdf. [Accessed 5 August 2025].

[56] Electric Power Research Institute (EPRI), "OpenDSS – Open Distribution System Simulator," [Online]. Available: https://www.epri.com/pages/sa/opendss. [Accessed 1 August 2025].

[57] DSS-Extensions, "Python interface for OpenDSS," [Online]. Available: https://dss-extensions.org/OpenDSSDirect.py/index.html. [Accessed 1 August 2025].

[58] E. McKenna, M. Thomson and J. Barton, "CREST Demand Model," 2015. [Online]. Available: https://doi.org/10.17028/rd.lboro.2001129.v8. [Accessed 7 July 2025].

[59] C. Martin and P. Niemeyer, "On the impact of network size and average degree on the robustness of centrality measures," 2021. [Online]. Available: https://doi.org/10.1017/nws.2020.37. [Accessed 1 August 2025].

[60] SP Energy Networks, "Our Distribution Network Overview," [Online]. Available: https://www.spenergynetworks.co.uk/pages/our_distribution_network.aspx. [Accessed 7 August 2025].

APPENDIX I: SDGS CONTRIBUTION

While the primary focus of this project is technical, its outcomes are broadly aligned with several SDGs. By improving the efficiency, resilience, and flexibility of power distribution systems, the approach explored in this study can facilitate the integration of renewable generation, support reliable energy access, and encourage smarter infrastructure investment. These impacts, although indirect, contribute towards global sustainability objectives by enabling electricity networks to operate more efficiently and adapt to future decarbonisation challenges:

Table 2: Relevant SDGs and this project contribution

SDG	*Project contribution*
7 - Affordable and Clean Energy	Enhances the resilience and efficiency of grids, supporting energy access and seamless integration of renewable generation.
9 - Industry, Innovation and Infrastructure	Encourages the adoption of advanced analytical tools for smarter, more sustainable network management and investment planning.
11 - Sustainable Cities and Communities	Enhances electricity supply reliability in urban and rural areas, supporting community resilience and service continuity.

APPENDIX II: PEAK DEMAND DATA

Table 3: CREST generated peak demand data

Dwelling	*Demand (W)*
1	*3696*
2	*503*
3	*2368*
4	*744*
5	*617*
6	*51*
7	*4085*
8	*1376*
9	*920*
10	*1013*
11	*458*
12	*1022*
13	*724*
14	*818*
15	*973*
16	*430*
17	*74*
18	*57*
19	*1334*
20	*575*
21	*75*
22	*61*
23	*395*
24	*2333*
25	*505*
26	*397*

Dwelling	Demand (W)
27	*593*
28	*262*
29	*309*
30	*2787*
31	782
32	1006
33	3180
34	3685
35	964
36	2777
37	298
38	65
39	515
40	247
41	3125
42	706
43	806
44	563
45	280
46	77
47	185
48	950
49	168
50	452
51	3646
52	886

Dwelling	Demand (W)
53	1034
54	9988
55	462
56	887
57	2854
58	230
59	844
60	61
61	524
62	385
63	77
64	788
65	217
66	3292
67	843
68	774
69	322
70	1041
71	388
72	2727
73	377
74	719
75	585
76	830
77	2555
78	544
79	576
80	912
81	71
82	481
83	743

Dwelling	Demand (W)
84	847
85	546
86	931
87	639
88	412
89	274
90	60
91	402
92	452
93	781
94	197
95	683
96	741
97	71
98	267
99	926
100	63

APPENDIX III: SUPPLEMENTARY PLOTS AND RESULTS FOR ALL CASE STUDY NETWORKS

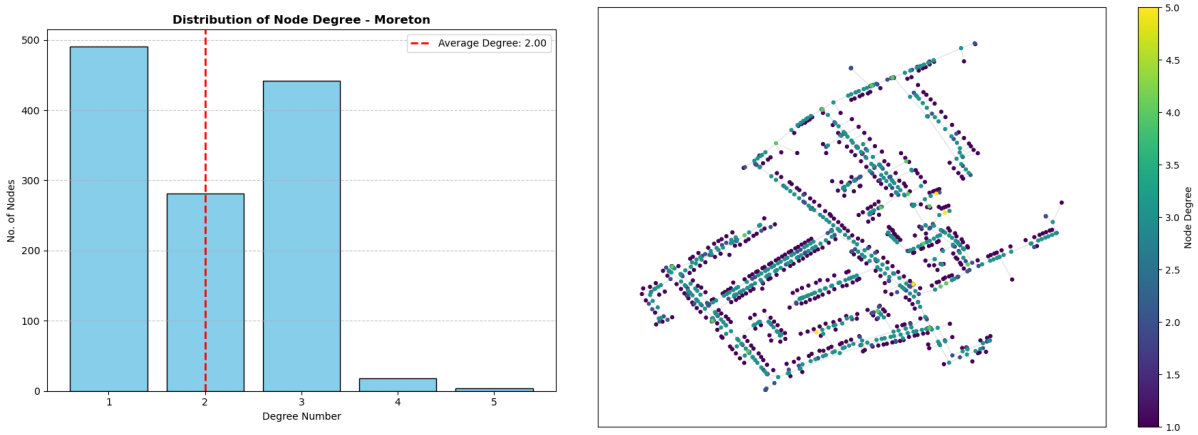

Figure 21: Distribution of node degree in the Moreton distribution network

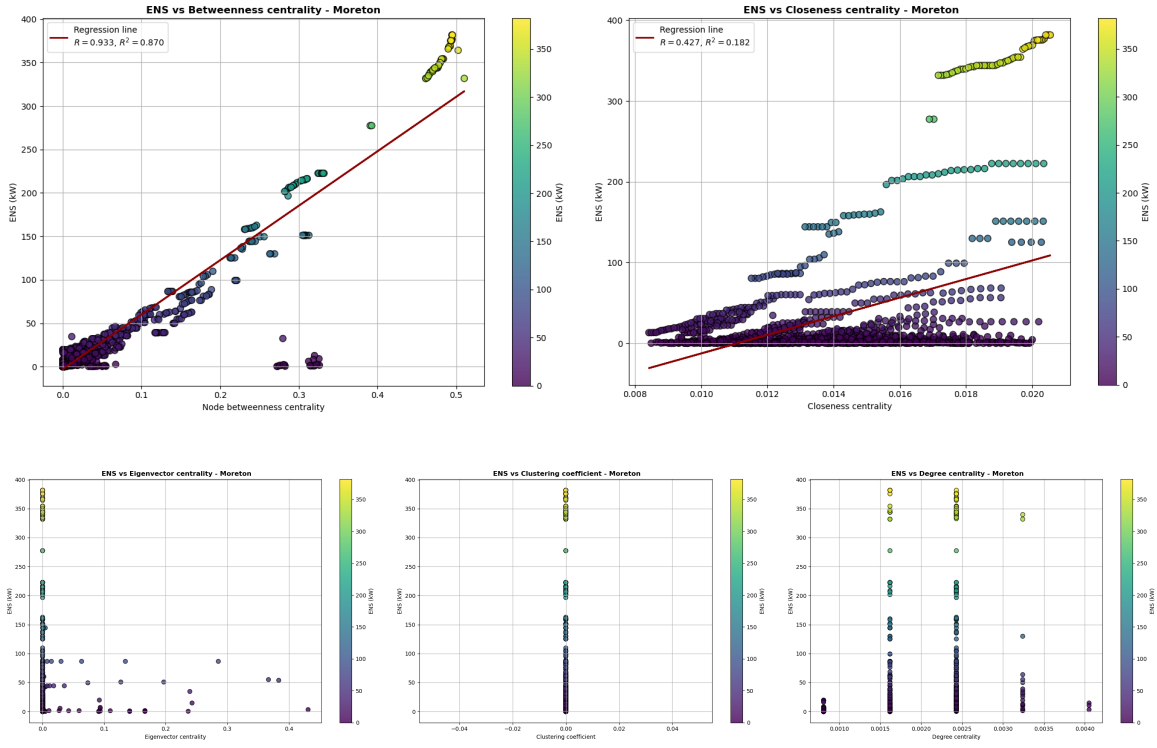

Figure 22: Comparative scatter plots of five topological centrality metrics against ENS in the Moreton network

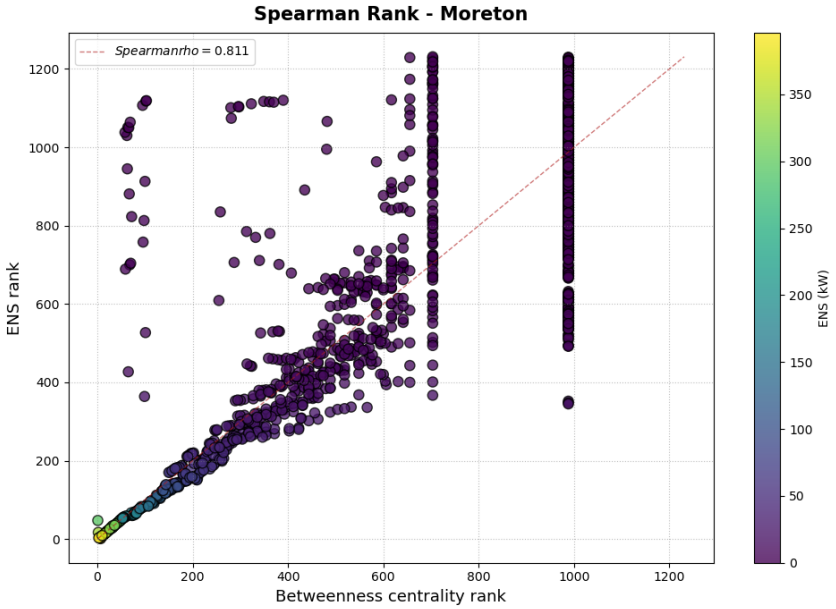

Figure 23: Spearman rank correlation plot comparing node rankings by betweenness centrality and ENS in the Moreton network

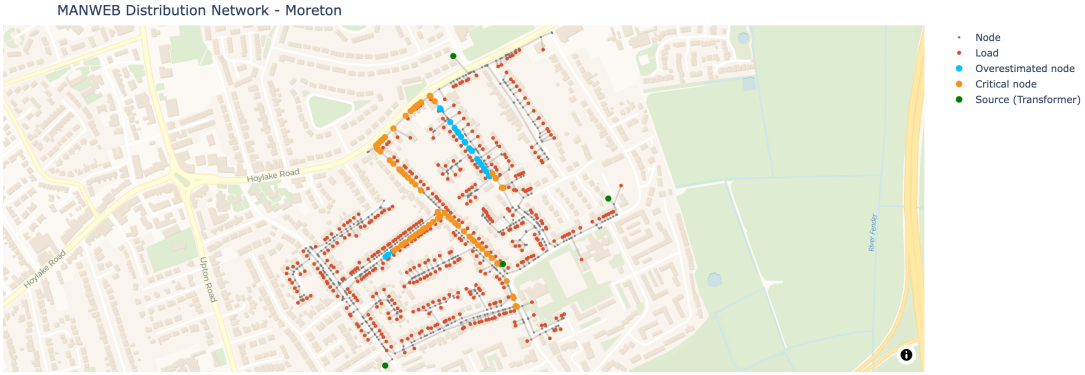

Figure 24: Moreton's network representation showing critical nodes and overestimated nodes

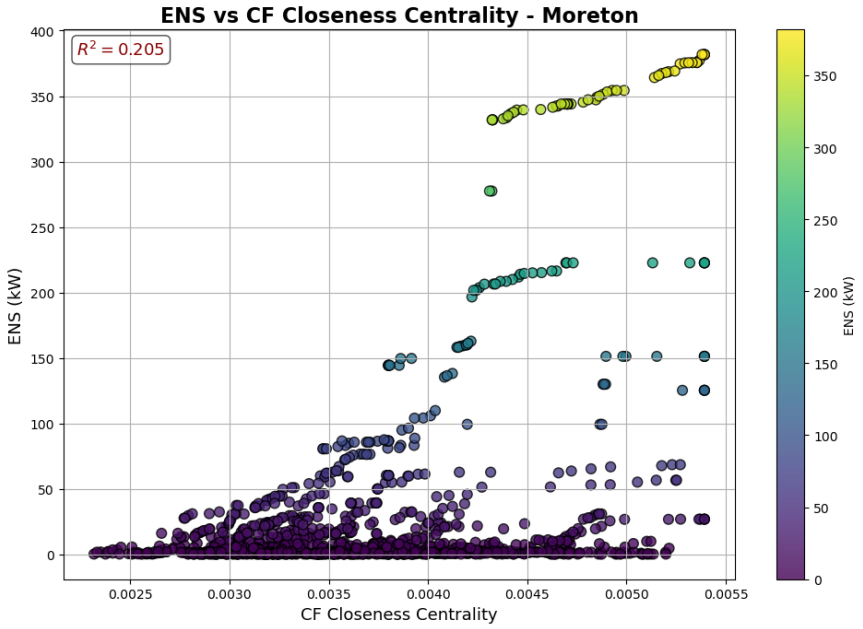

Figure 25: Scatter plot of ENS against current-flow closeness centrality in the Moreton network

Figure 26: Visualization of current-flow line betweenness centrality values in the Moreton network

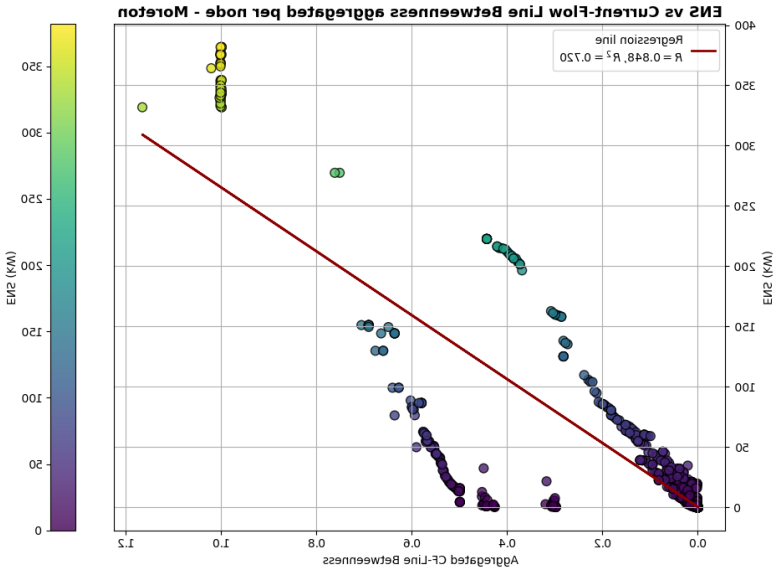

Figure 27: Scatter plot of ENS against current-flow line betweenness centrality in the Moreton network

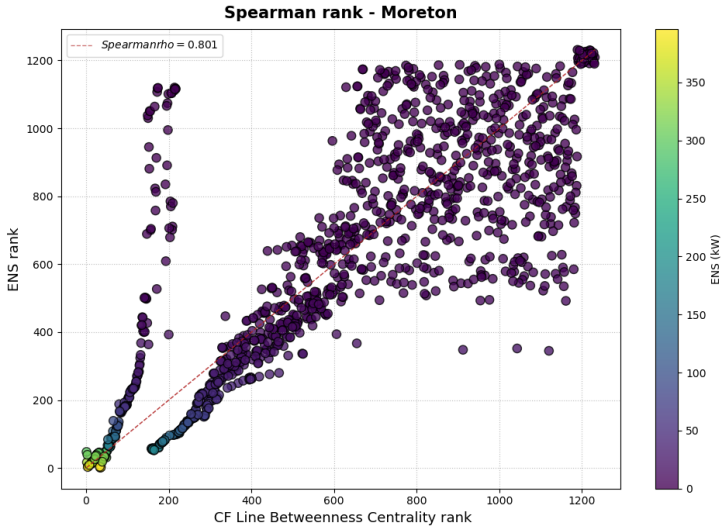

Figure 28: Spearman rank correlation plot comparing node rankings by CF line betweenness centrality and ENS in the Moreton network

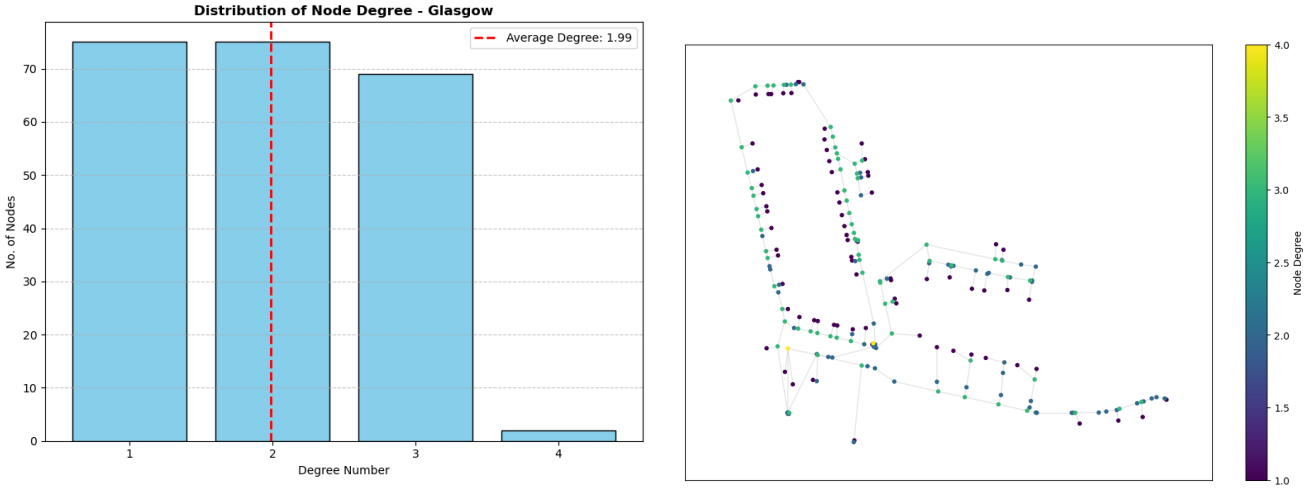

Figure 29: Distribution of node degree in the Whifflet distribution network

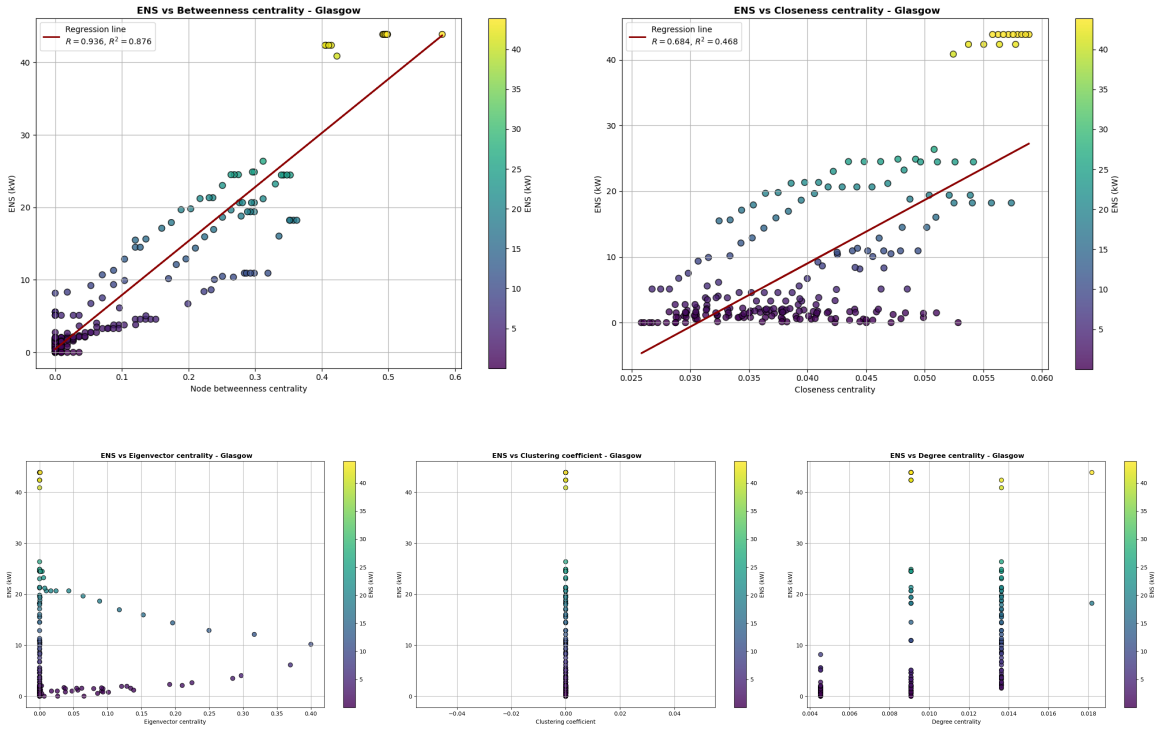

Figure 30: Comparative scatter plots of five topological centrality metrics against ENS in the Whifflet network

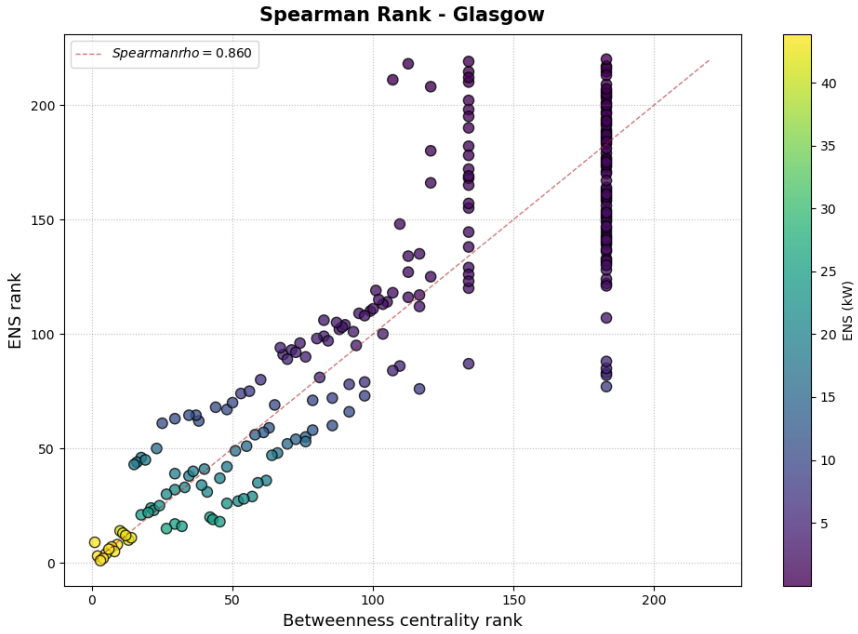

Figure 31: Spearman rank correlation plot comparing node rankings by betweenness centrality and ENS in the Whifflet network

Figure 32: Highlighted Whifflet's network representation showing critical nodes and overestimated nodes

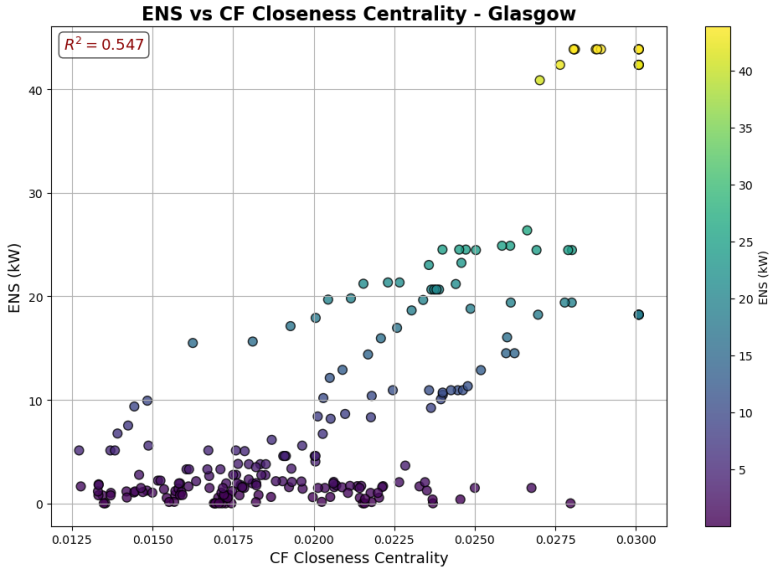

Figure 33: Scatter plot of ENS against current-flow closeness centrality in the Whifflet network

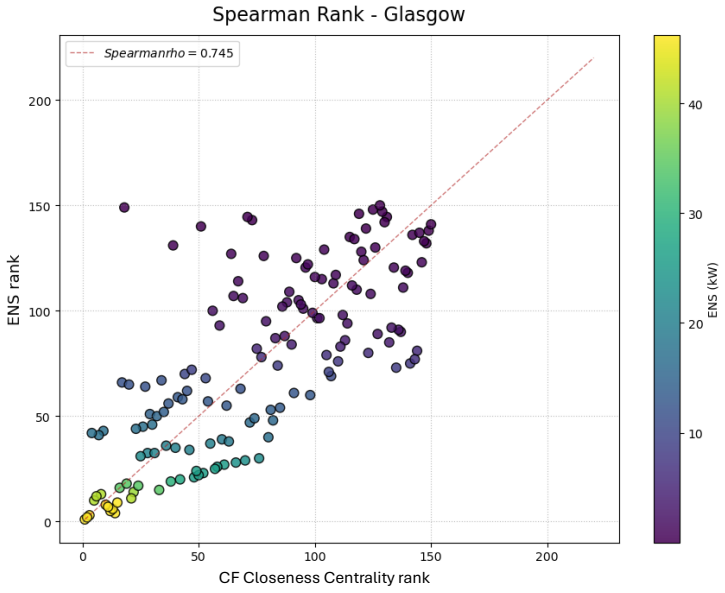

Figure 34: Spearman rank correlation plot comparing node rankings by CF closeness centrality and ENS in the Whifflet network

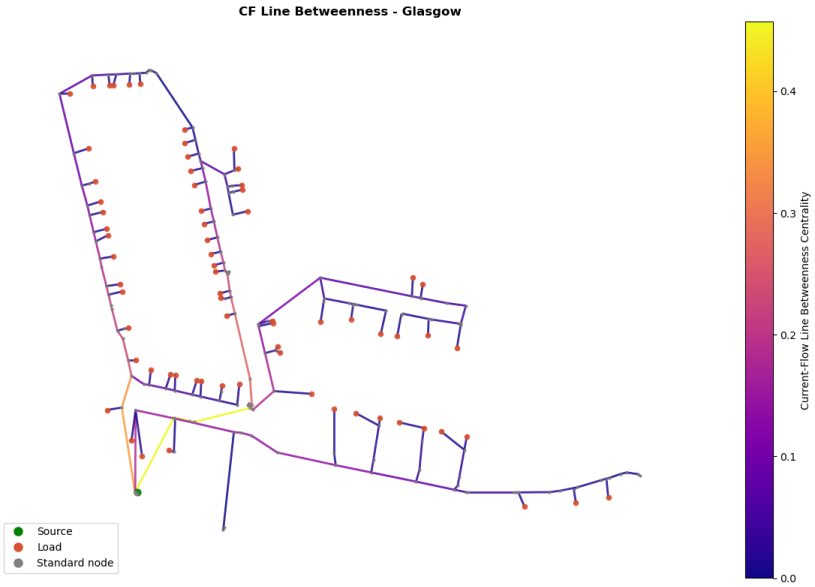

Figure 35: Visualization of current-flow line betweenness centrality values in the Whifflet network

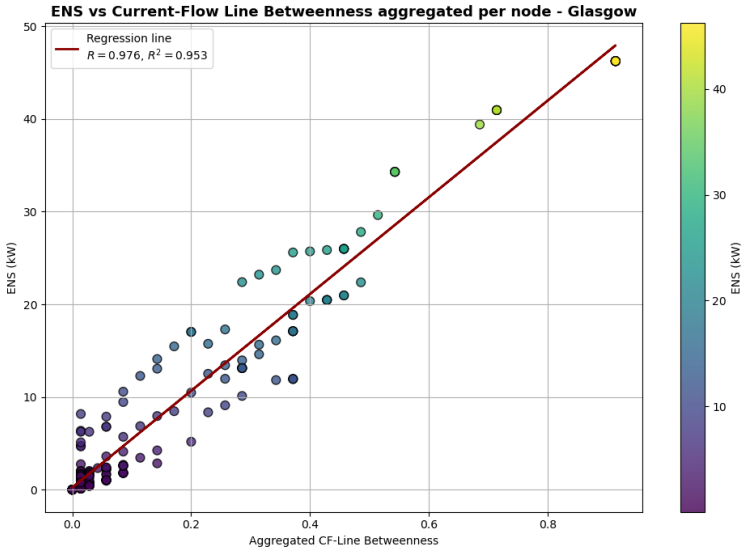

Figure 36: Scatter plot of ENS against current-flow line betweenness centrality in the Whifflet network

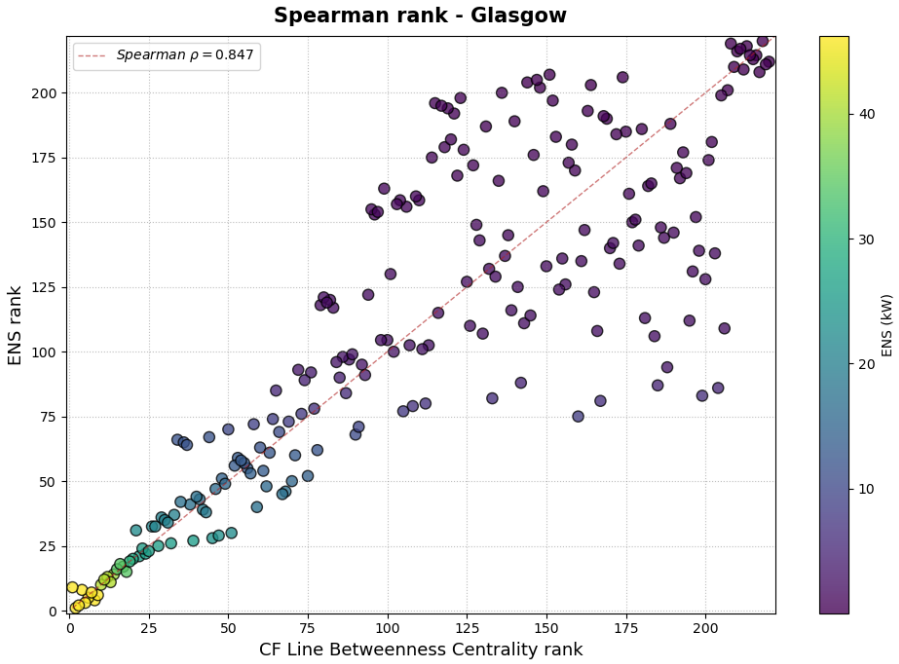

Figure 37: Spearman rank correlation plot comparing node rankings by CF line betweenness centrality and ENS in the Whifflet network

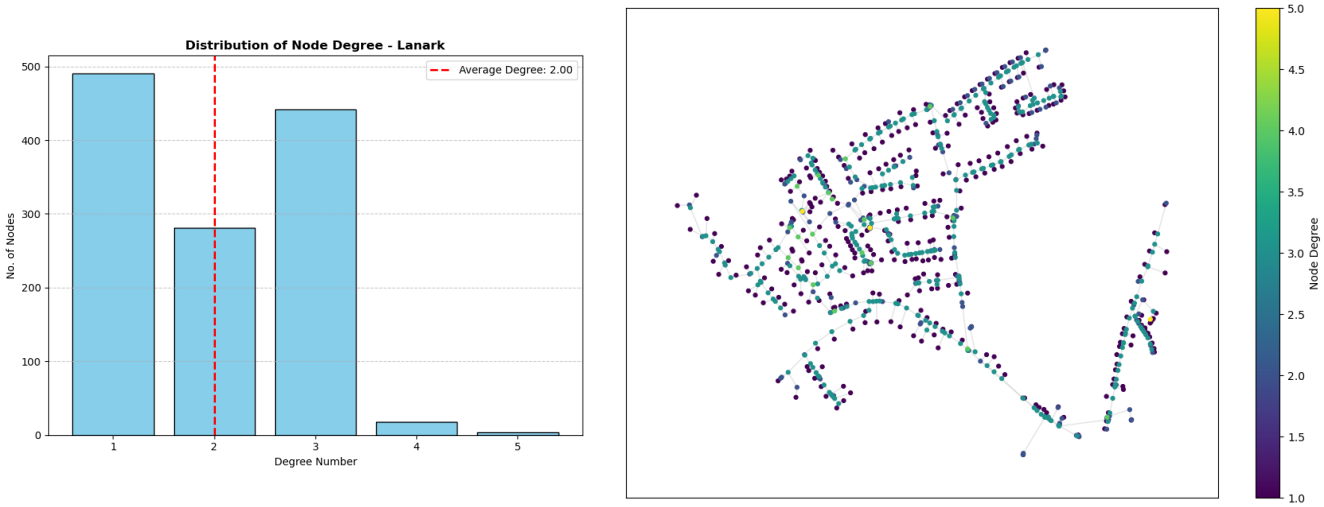

Figure 38: Distribution of node degree in the Lanark distribution network

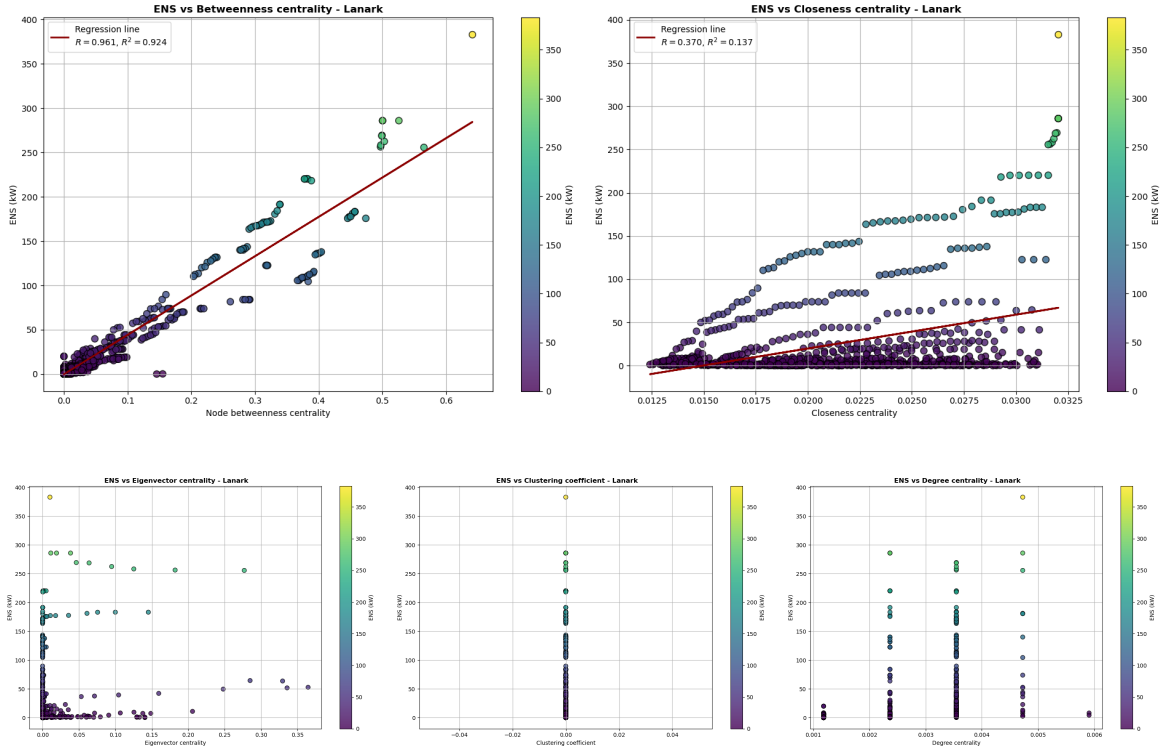

Figure 39: Comparative scatter plots of five topological centrality metrics against ENS in the Lanark network

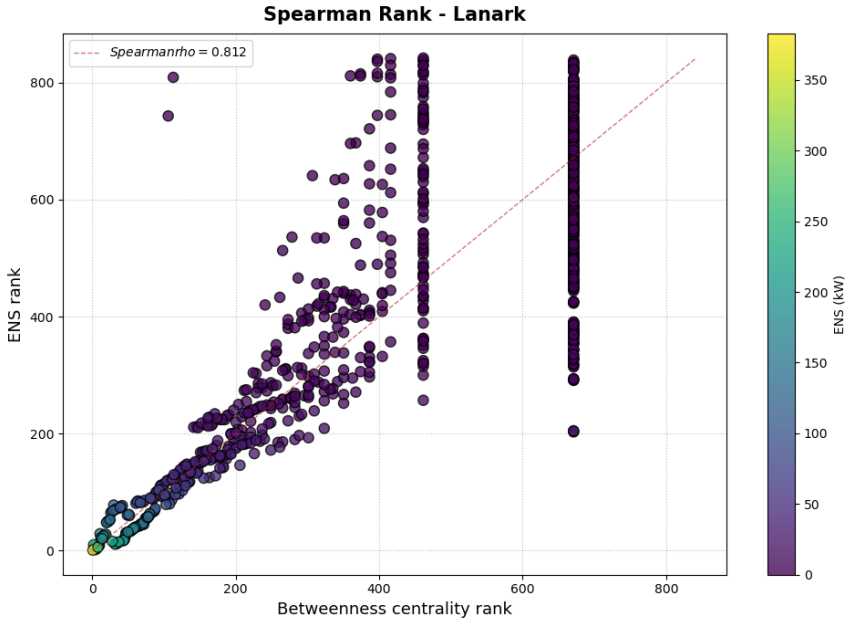

Figure 40: Spearman rank correlation plot comparing node rankings by betweenness centrality and ENS in the Lanark network

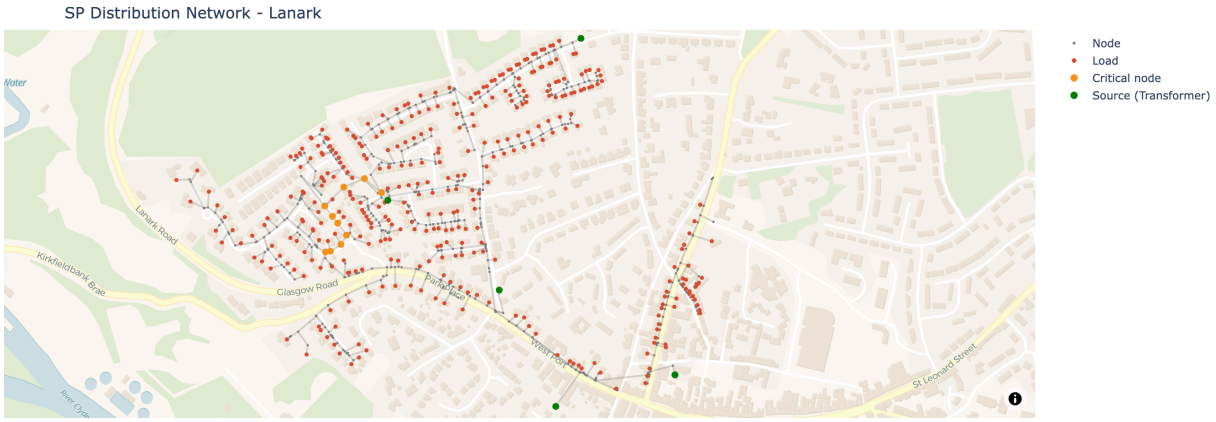

Figure 41: Highlighted Lanark's network representation showing critical nodes and overestimated nodes

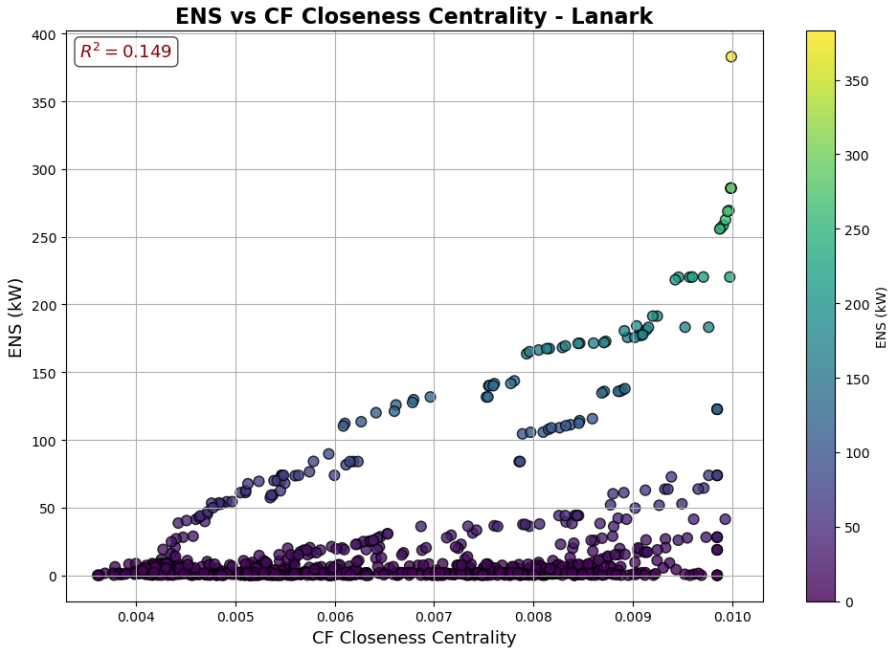

Figure 42: Scatter plot of ENS against current-flow closeness centrality in the Lanark network

Figure 43: Visualization of current-flow line betweenness centrality values in the Lanark network

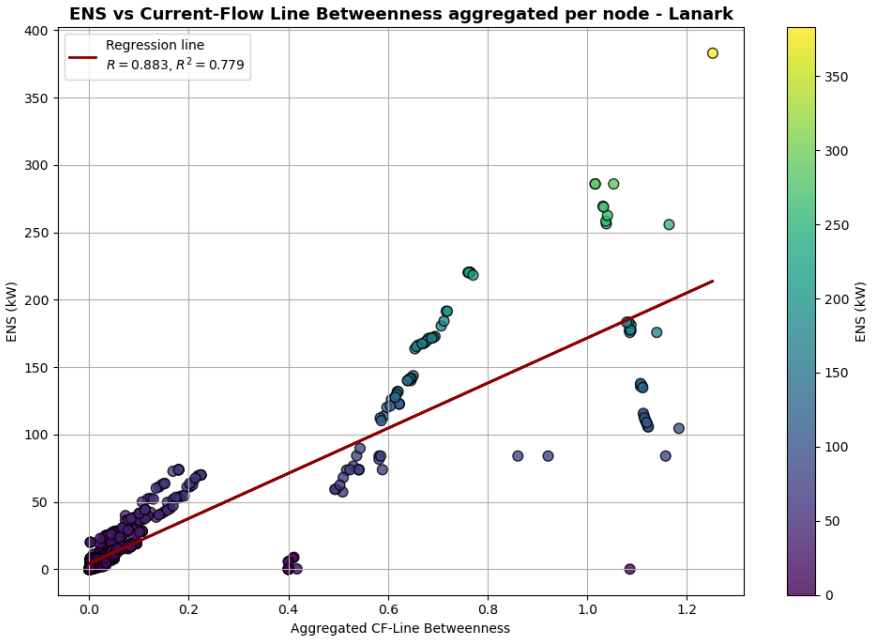

Figure 44: Scatter plot of ENS against current-flow line betweenness centrality in the Lanark network

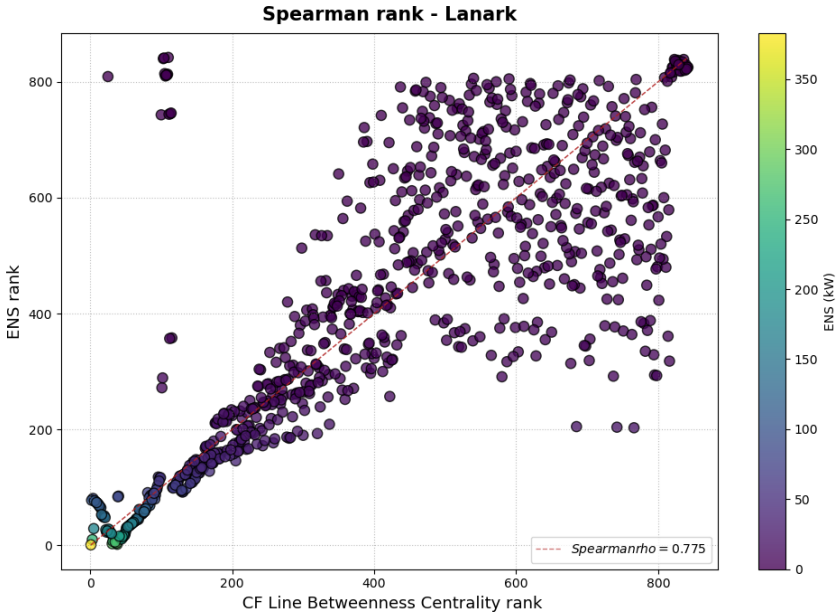

Figure 45: Spearman rank correlation plot comparing node rankings by CF line betweenness centrality and ENS in the Lanark network