IDENTIFICACIÓN DE MÉTODOS PARA EVALUAR LA VULNERABILIDAD EN REDES ELÉCTRICAS DE DISTRIBUCIÓN CON INTEGRACIÓN DE GENERACIÓN DISTRIBUIDA.

RANDY JOSÉ AGUSTÍN MONTENEGRO SOCHA

Universidad Santo Tomás
Facultad de Ingeniería Electrónica
Maestría en Ingeniería Electrónica
Bogotá, Colombia
2024

IDENTIFICACIÓN DE MÉTODOS PARA EVALUAR LA VULNERABILIDAD EN REDES ELÉCTRICAS DE DISTRIBUCIÓN CON INTEGRACIÓN DE GENERACIÓN DISTRIBUIDA.

RANDY JOSÉ AGUSTÍN MONTENEGRO SOCHA

Proyecto de grado presentado como requisito para optar al título de:

Magíster en Ingeniería Electrónica.

Director:
Dr. Jaime Vitola Oyaga.
Codirector:
Dr. Billy Vladimir Toro Tovar

Grupo de Investigación MEM
Línea de Investigación:
Fuentes de Energía Renovables y Eficiencia Energética.
Universidad Santo Tomás
Facultad de Ingeniería Electrónica
Maestría en Ingeniería Electrónica
Bogotá, Colombia
2024

Autoridades de la universidad

RECTOR GENERAL

FRAY ÁLVARO JOSÉ ARANGO RESTREPO, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL

FRAY HERNÁN YESID RIVERA ROBERTO, O.P.

VICERRECTOR ACADÉMICO GENERAL

FRAY MAURICIO ANTONIO CORTES GALLEGO, O.P.

SECRETARIO GENERAL

DOCTORA LUZ PATRICIA ROCHA CAICEDO

DECANO DIVISIÓN DE INGENIERÍAS

FRAY JAVIER ANTONIO HINCAPIÉ ARDILA, O.P.

SECRETARIA DE DIVISIÓN

DOCTORA LUZ PATRICIA ROCHA CAICEDO

DECANO FACULTAD DE INGENIERÍA ELECTRÓNICA

PH. D. CARLOS ANDRÉS TORRES PINZÓN

Nota de aceptación

Firma del tutor

Firma del jurado

Firma del jurado

BOGOTÁ D.C. _____ DE 2024

ADVERTENCIA

La Universidad Santo Tomás no se hace responsable de las opiniones y conceptos expresados en el trabajo de grado, solo velará por qué no se publique nada contrario al dogma ni a la moral católica y porque el trabajo no tenga ataques personales y únicamente se vea el anhelo de buscar la verdad científica.

Capítulo III –Art. 46 del Reglamento de la Universidad Santo Tomás.

Dedicatoria

Con el corazón lleno de gratitud, dedico este trabajo a mis padres. A mi padre, cuya ausencia siento profundamente, pero cuyo recuerdo sigue siendo una fuente de inspiración constante y a mi madre que siempre ha estado pendiente de mi con su amor y apoyo.

A mi novia Karina por siempre motivarme a culminar este logro académico.

A mis amigos Jhon Montoya, Santiago Arévalo, Denise Acosta, Mónica Martínez y Gloría Medina por siempre creer en mí y mis capacidades.

Agradecimientos

Al Dr. Carlos Andrés Macana, por compartir generosamente sus conocimientos y experiencias tanto académicas como profesionales.

A los profesores de la facultad, quienes hicieron todo lo posible para ayudarme a alcanzar este logro.

Contenido

Resumen ..... **X**
Abstract ..... **XI**
Lista de Figuras ..... **XII**
Lista de Tablas ..... **XIII**
Glosario ..... **XIV**
1. Introducción **1**
1.1. Planteamiento del Problema 2
1.2. Objetivos 2
1.2.1. Objetivo General 2
1.2.2. Objetivos Específicos 3
1.3. Justificación 3
1.4. Impacto Social 4
2. Estado del Arte **5**
2.1. Métodos para evaluar vulnerabilidad en sistemas de potencia 5
2.2. Nuevas propuestas para evaluar la vulnerabilidad de las redes eléctricas 7
2.3. Métodos para evaluar vulnerabilidad en redes eléctricas de distribución ... 8
2.4. Métodos para evaluar vulnerabilidad en sistemas de distribución con alta penetración de energías renovables. 9
3. Marco Teórico **11**
3.1. Sistemas de transmisión y distribución en Colombia: 11
3.2. Definiciones 12
3.3. Infraestructuras Críticas: 13
3.4. Riesgos del sistema eléctrico: 13
3.5. Modelos generales utilizados para evaluar el riesgo en las infraestructuras críticas: 14
3.6. Modelos para analizar redes eléctricas. 18
4. Diseño Metodológico **20**
4.1. Fases y Metodología 20
4.1.1 Tipo de investigación y enfoque 20
4.1.2 Fases del desarrollo y actividades 20
Actividades: 20
4.2. Cronograma 22

5. Resultados y Discusión 23
6. Conclusiones y Trabajos futuros 32
7. Anexos 34
8. Referencias Bibliográficas 37

Resumen

El presente trabajo se enfoca en identificar métodos para evaluar la vulnerabilidad en redes de distribución eléctrica que integran generación distribuida, un aspecto clave en el marco de la transición energética. La incorporación de fuentes de energía renovable, como la solar y la eólica, junto con el aumento de vehículos eléctricos, introduce nuevos desafíos que afectan la estabilidad de estas redes. La revisión del estado del arte busca responder a la necesidad de analizar cómo estos cambios influyen en la resiliencia y robustez de las redes de distribución.

Se realizó una revisión detallada del estado del arte consultando diversas bases de datos académicas, clasificando los métodos existentes según su naturaleza probabilística, determinista o basada en simulación. Uno de los métodos seleccionados fue simulado para evaluar la vulnerabilidad de una red de distribución con generación distribuida.

Se identificaron y clasificaron varios métodos para la evaluación de la vulnerabilidad en redes de distribución con energías renovables, como el método TOPSIS y análisis de redes complejas. Se optó por el método de relación de orden G1 para la simulación, que mostró que ciertos nodos y líneas de la red son más vulnerables debido a inestabilidades de voltaje y sobrecargas.

Este trabajo proporciona un marco metodológico para evaluar la vulnerabilidad en redes de distribución con alta integración de energías renovables. Los resultados subrayan la importancia de combinar enfoques subjetivos y objetivos en la ponderación de los indicadores de vulnerabilidad. La revisión del estado del arte ofrece herramientas valiosas para que los operadores de red (OR) puedan mejorar la planificación y operación de redes más robustas y resilientes frente a fallos y fluctuaciones.

Palabras clave: Vulnerabilidad, Generación Distribuida (GD) y Energías Renovables.

Abstract

The present work focuses on identifying methods to assess vulnerability in electric distribution networks that integrate distributed generation, a key aspect within the framework of the energy transition. The incorporation of renewable energy sources, such as solar and wind, along with the increase in electric vehicles, introduces new challenges that affect the stability of these networks. The state-of-the-art review aims to address the need to analyze how these changes influence the resilience and robustness of distribution networks.

A detailed review of the state-of-the-art was carried out by consulting various academic databases, classifying existing methods based on their probabilistic, deterministic, or simulation-based nature. One of the selected methods was simulated to evaluate the vulnerability of a distribution network with distributed generation.

Several methods for vulnerability assessment in distribution networks with renewable energy sources were identified and classified, such as the TOPSIS method and complex network analysis. The G1 order relation method was chosen for the simulation, which showed that certain nodes and lines in the network are more vulnerable due to voltage instabilities and overloads.

This work provides a methodological framework for evaluating vulnerability in distribution networks with high integration of renewable energy sources. The results highlight the importance of combining subjective and objective approaches in the weighting of vulnerability indicators. The state-of-the-art review offers valuable tools for network operators (OR) to improve the planning and operation of more robust and resilient networks against failures and fluctuations.

Keywords: Vulnerability, Distributed Generation (DG), and Renewable Energy.

Lista de Figuras

Ilustración 1 Ilustración de un sistema de potencia.[28] 12
Ilustración 2 Ejemplo de la interdepencia entre el sistema de energía eléctrica y otras infraestructuras críticas. 13
Ilustración 3 Escenarios de fallas en sistemas de potencia. 14
Ilustración 4 Diferentes métodos para el análisis de vulnerabilidad 18
Ilustración 5 Cronograma de Actividades 22
Ilustración 6 Porcentaje de publicaciones por año de la muestra seleccionada sobre métodos para evaluar la vulnerabilidad en redes de distribución con integración de fuentes renovables. 24
Ilustración 7 CIGRE Networks - Medium voltage distribution network with PV and Wind DER 26
Ilustración 8 Gráfica de barras con el índice de vulnerabilidad de los nodos de la red CIGRE MV 30

Lista de Tablas

Tabla 1 Tabla resumen métodos topológicos 7
Tabla 2 Comparativa métodos evaluación vulnerabilidad en redes de distribución. 9
Tabla 3 Lista artículos sobre evaluación de vulnerabilidad en redes de distribución con integración de generación distribuida. 23
Tabla 4 Categorización métodos evaluación de vulnerabilidad en redes de distribución con integración de generación distribuida. 25
Tabla 5 Tabla resultados simulación. 30
Tabla 6 Personas que intervienen en el proyecto y su rol 36
Tabla 7 Valor licencia 36

Glosario

ABM: Modelado Basado en Agentes (Agent-Based Modeling). Técnica utilizada para simular la interacción de agentes individuales dentro de un sistema, como operadores o componentes de la red, para evaluar cómo sus decisiones afectan el sistema eléctrico en su conjunto.

CNT: Teoría de Redes Complejas (Complex Network Theory). Enfoque que estudia la estructura y dinámica de sistemas interconectados, utilizado para analizar la vulnerabilidad y eficiencia de redes eléctricas.

DG: Generación Distribuida (Distributed Generation). Producción de energía eléctrica a pequeña escala, usualmente cercana al punto de consumo y proveniente de fuentes renovables.

DN: Red de distribución (Distribution Network). Sistema que transporta electricidad desde las subestaciones hasta los usuarios finales, ajustando la tensión para consumo doméstico, comercial o industrial.

EENS: (Energía Esperada No Suministrada). Medida de la cantidad de energía que una red eléctrica no puede entregar a los usuarios debido a fallas o interrupciones.

EV: Vehículos Eléctricos (Electric Vehicles). Vehículos que utilizan motores eléctricos, los cuales imponen nuevos desafíos a las redes de distribución por la carga variable que generan.

HILP: Eventos de Baja Probabilidad y Alto Impacto. Fenómenos raros pero con consecuencias graves para las redes eléctricas, como desastres naturales o ataques deliberados.

MGs: (Microrredes). Pequeñas redes eléctricas locales que pueden operar conectadas al sistema principal o de forma independiente, integrando generación distribuida y almacenamiento de energía.

OR: Operador de red. Entidad encargada de operar, mantener y gestionar la infraestructura eléctrica, asegurando un suministro continuo y seguro de energía.

SIN: Sistema Interconectado Nacional. Es el sistema que interconecta las principales redes de transmisión y distribución de energía en Colombia, cubriendo áreas clave como la región Andina, Caribe y Pacífico.

TSCG: Grafo de Correlación Temporal-Espacial. Modelo que combina características topológicas y operativas para evaluar la vulnerabilidad y propagación de fallas en redes eléctricas.

NOTAS EXPLICATIVAS DEL PRESENTE FORMATO (NO HACE PARTE DEL DOCUMENTO):

El documento está estructurado en las siguientes partes:

- Portada
- Declaración
- Agradecimiento
- Dedicatoria
- Tabla de Contenido
- Preliminares (Resumen, Lista de Figuras, Lista de Tablas y Glosario)
- Introducción
- Estado del Arte
- Marco Teórico
- Diseño Metodológico
- Desarrollo Conceptual
- Resultados y Discusión
- Conclusiones y Trabajos Futuros
- Anexos
- Bibliografía.

En total, desde la portada hasta las conclusiones, el documento debe contar **como máximo con 80 páginas de extensión)**. No existe límites de páginas en los anexos ni bibliografía.

La tabla de Contenido, el Índice de Tablas y el Índice de figuras debe ser generado automáticamente.

A partir de ahora se explicará lo que debe ir en cada sección y su límite máximo de páginas (si aplica).

Todo el documento está escrito en Arial (15 puntos y negrita para nivel 1, 13 puntos y negrita para títulos de otro nivel y 12 puntos para párrafos).

El interlineado entre párrafos es de 1.0 puntos, sin sangría.

1. Introducción

En los últimos años se ha visto como se han integrado las fuentes de generación distribuida (DG) y los vehículos eléctricos (EV) a las redes de distribución eléctrica de las grandes ciudades, incrementando la complejidad y vulnerabilidad de estas. Estos avances han aportado beneficios en cuanto a sostenibilidad y diversificación energética, pero también han introducido nuevos desafíos y complejidades que afectan la estabilidad y vulnerabilidad de los sistemas de distribución eléctrica, esto por fenómenos como la generación de energía bidireccional, fluctuaciones de voltaje, la distorsión armónica y las variaciones de carga. Dichos factores aumentan la vulnerabilidad de la red, dificultando su estabilidad y confiabilidad, especialmente ante eventos como catástrofes naturales o ataques deliberados.

Los sistemas de potencia son considerados una infraestructura critica ya que el suministro de energía eléctrica es esencial para la sociedad y su economía porque una falla parcial o total de uno o más de sus componentes puede tener una incidencia negativa en la economía, funciones de gobierno y seguridad nacional.[1]

Por lo tanto, identificar los nodos vulnerables de la red eléctrica de distribución es crucial para evitar fallas en cascada significativas.[2] Un estudio de vulnerabilidad de la red permite determinar cuáles son los componentes más débiles de un sistema de potencia y que pueden llegar a ser reforzados ante un futuro evento tal como una catástrofe natural o un ataque deliberado.

El análisis de vulnerabilidad de las redes de distribución difiere al de las redes de transmisión en muchos aspectos, como función, estructura y estado, por lo que los resultados de investigación existentes sobre la vulnerabilidad de las redes de transmisión no pueden aplicarse directamente a las redes de distribución[3]. Por lo tanto, muchas investigaciones han mejorado los resultados en función de las características estructurales de la red de distribución. [4]

El análisis de vulnerabilidad de las redes de distribución requiere un análisis cuantitativo o cualitativo de los factores internos y externos de la red, utilizando una variedad de indicadores de evaluación. La continua integración de recursos a la red eléctrica de distribución aumenta su complejidad y la incertidumbre de las redes de distribución. Por lo cual es de gran importancia proponer modelos que simplifiquen este proceso de cálculo.[4]

1.1. Planteamiento del Problema

Un estudio de vulnerabilidad o robustez es la herramienta más adecuada para que el operador pueda medir la capacidad de respuesta de la infraestructura ante eventos extremos, cuantificar el rendimiento estructural de todo el esqueleto de la red e identificar los buses más débiles que requieren un refuerzo significativo. [5]

Las redes de distribución eléctrica suelen verse afectadas por sucesos relacionados con el clima, como el hielo, los vientos fuertes, las inundaciones y los rayos que son las causas de alrededor del 78% de las principales interrupciones de energía en el sistema de distribución de energía de EE.UU. [6] Este tipo de fenómenos naturales de baja probabilidad y alto impacto que se han venido incrementando por el cambio climático, muestran cómo se pueden ocasionar cortes de energía en los sistemas de distribución eléctrica desde un punto de vista de la vulnerabilidad de los sistemas eléctricos.

Además, estos grandes apagones podrían aumentar con el cambio hacia la generación distribuida y el aumento de los prosumidores (productores y consumidores de energía), siendo esta otra razón por la cual los sistemas de distribución deben considerarse en riesgo y necesitan un análisis de vulnerabilidad. [7]

Las anteriores razones hacen ver la importancia de contar con métodos para medir la vulnerabilidad en los sistemas de distribución eléctrica para de esta forma poder tomar acciones que conduzcan a mejorar la robustez del sistema de distribución eléctrico que cuenten con generación distribuida (DG) y autos eléctricos (EV) ante eventos como las catástrofes naturales que por efecto del cambio climático cada vez son más frecuentes o en caso de un ataque terrorista deliberado.

En el contexto del planteamiento del problema descrito, la pregunta que guía este trabajo de grado es: ¿Cuáles son los métodos existentes para evaluar la vulnerabilidad de las redes de distribución eléctrica con alta penetración de generación distribuida y cómo pueden ser aplicados para identificar los puntos críticos que requieren intervenciones preventivas, teniendo en cuenta los efectos de fenómenos de baja probabilidad y alto impacto? Este cuestionamiento surge de la necesidad de entender cómo los avances en la integración de fuentes renovables y la distribución de energía influyen en la resiliencia de los sistemas eléctricos, especialmente ante eventos disruptivos, y cómo los operadores de red (OR) pueden anticiparse y mitigar estas vulnerabilidades

1.2. Objetivos

1.2.1. Objetivo General

Identificar los métodos existentes para evaluar la vulnerabilidad de las redes eléctricas de distribución con integración de generación distribuida (DG).

1.2.2. Objetivos Específicos

- Revisar en la bibliografía los modelos y métodos para evaluar la vulnerabilidad de redes eléctricas de distribución con integración de generación distribuida.
- Categorizar los métodos existentes para la evaluación de vulnerabilidad en redes eléctricas de distribución, identificando sus ventajas y limitaciones en escenarios con integración de generación distribuida.
- Simular uno de los métodos existentes para evaluar la vulnerabilidad de las redes de distribución eléctricas que tienen integración de generación distribuida.

1.3. Justificación

En el escenario actual de transición energética en donde se busca usar fuentes de energía renovables y de baja emisión de carbono, cada vez es más común el uso de elementos tales como lo son los paneles solares y estaciones de carga para vehículos eléctricos en las redes de distribución eléctrica (DN).

Los análisis de vulnerabilidad de las redes eléctricas son de gran importancia para los operadores de red (OR) a la hora de desarrollar estrategias que permitan una rápida intervención en redes eléctricas con alta penetración de generación distribuida y vehículos eléctricos para minimizar el impacto causado por fallos en el sistema eléctrico debido a ataques malintencionados al mismo o por catástrofes naturales los cuales provocan una falta de atención a la carga. Por lo cual es fundamental implementar medidas que reduzcan la severidad de los fallos en los sistemas eléctricos debido a la vulnerabilidad inherente de las redes eléctricas de distribución (DN). [8]

El efecto de la alta penetración de las energías renovables en la confiabilidad y vulnerabilidad de los sistemas eléctricos interconectados es un nuevo campo de investigación, que requiere proponer marcos metodológicos integrados para estudiar diferentes atributos interrelacionados de ambos conceptos.[9]

Tener métodos que permitan medir la vulnerabilidad de un sistema de distribución eléctrica con alta penetración de generación distribuida y vehículos eléctricos, permitirán tomar decisiones en cuanto que estrategias tomar para robustecer la red ante eventos tales como huracanes, incendios, inundaciones, terremotos, los cuales se agrupan dentro de los eventos de baja probabilidad y alto impacto (LPHI) que pueden afectar el funcionamiento de la red eléctrica.[10]

1.4. Impacto Social

El trabajo de grado presentado en este documento se centra en la revisión del estado del arte y en un ejercicio de vigilancia tecnológica y prospectiva sobre la evaluación y medición de la vulnerabilidad en redes de distribución con alta penetración de energías renovables. Este enfoque es clave dentro del contexto de la transición energética, ya que los sistemas eléctricos deben enfrentar el desafío de integrar eficientemente fuentes de energía limpias, distribuidas y renovables, manteniendo al mismo tiempo la estabilidad y seguridad operativa.

El trabajo, centrado en el análisis bibliográfico y la vigilancia tecnológica, no solo identifica los enfoques más avanzados para evaluar la vulnerabilidad de las redes, sino que también anticipa las tendencias futuras en tecnologías de redes eléctricas de distribución y su integración con las fuentes de energía renovables. Esta investigación establece una base sólida para futuras investigaciones y desarrollos que contribuyan a la transición energética y al desarrollo de redes eléctricas de distribución más robustas.

Para la comunidad de la Universidad Santo Tomás, este proyecto abre importantes oportunidades. Los estudiantes interesados en el área energética podrán realizar trabajos de investigación que los relacione con empresas del sector eléctrico, fortaleciendo su formación académica y profesional. Además, la universidad, a través de asesorías y consultorías, podría colaborar con instituciones públicas y privadas en la implementación de soluciones que optimicen la gestión energética y refuercen la resiliencia de las redes eléctricas. Este proceso beneficiará a numerosos profesionales y estudiantes, generando un impacto positivo tanto en la educación energética como en el desarrollo de la infraestructura eléctrica en Colombia.

2. Estado del Arte

Los sistemas eléctricos son muy importantes para suplir las necesidades de la población en general, tanto a nivel doméstico, industrial, comercial, salud y seguridad; sin embargo, estos sistemas son propensos a sufrir algún tipo de vulnerabilidad, ya sea por desastres naturales, por acción humana (actos vandálicos o terroristas, accidentes) y aspectos técnicos (fallas de equipos e interrupciones no planificadas).[8]

La alta penetración de fuentes renovables como la solar y eólica en los sistemas eléctricos genera nuevos desafíos técnicos debido a su intermitencia, lo cual introduce variabilidad y riesgos de cortes no planificados, afectando la fiabilidad del sistema eléctrico. Al conectar redes que combinan generación distribuida y convencional, se mejora la flexibilidad y el uso eficiente de los recursos. Sin embargo, estas interconexiones aumentan la vulnerabilidad porque una falla en una parte de la red puede propagarse y comprometer la estabilidad general del sistema. Por lo tanto, para garantizar un sistema sólido y seguro, es fundamental realizar evaluaciones de confiabilidad y vulnerabilidad.[9]

Medir la vulnerabilidad es un factor clave en la evaluación del riesgo para infraestructuras críticas. La vulnerabilidad se refiere a los estados inherentes del sistema que pueden ser explotados para causar daño, como aspectos físicos, técnicos, organizacionales y culturales. Al comprender estas vulnerabilidades, es posible anticipar cómo un sistema podría verse afectado por amenazas y cómo respondería a diferentes ataques o desastres, permitiendo a los operadores de red (OR) tomar decisiones informadas, facilitando la implementación de medidas efectivas de prevención y mitigación de riesgos, lo cual es una herramienta clave para fortalecer la seguridad y la resiliencia de los sistemas críticos.[11]

2.1. Métodos para evaluar vulnerabilidad en sistemas de potencia

Los investigadores han desarrollado diversos métodos para evaluar la vulnerabilidad de los sistemas de potencia. A continuación, se van a dar conocer los más relevantes.

2.1.1 Métodos topológicos (Análisis de redes complejas)

Los métodos fundamentados en la teoría de redes complejas (CNT) se han utilizado ampliamente para evaluar la vulnerabilidad operativa de las redes eléctricas. Autores como Wei et Al. [12] usan la teoría de las redes complejas (CNT) para evaluar la vulnerabilidad operativa de las redes eléctricas, la investigación hecha por ellos se orienta en identificar ramas críticas a través de un grafo de correlación temporal-espacial (TSCG) que combina características topológicas, físicas y operativas. Se proponen dos métricas, la capacidad de impacto y la susceptibilidad,

basadas en la entropía simétrica, para evaluar la propagación de fallas y su impacto en la red.

Fu et al. [13] proponen un modelo de redes multicapa para analizar la importancia de los componentes y su interdependencia en sistemas interconectados, teniendo en cuenta las propiedades físicas de las redes de transmisión y distribución. Los autores se centran en las métricas topológicas tradicionales usadas en la teoría de redes complejas tales como la centralidad de grado, la de intermediación (betweenness) y la de cercanía (closeness), aplicándolas a redes multicapa. Estos métodos facilitan la identificación de componentes críticos que son esenciales para la interacción entre las distintas capas de la red, lo que es esencial para la recuperación de infraestructuras críticas después de una interrupción.

Saleh et Al. [14] propone un enfoque novedoso para la ubicación de microrredes (MGs) basado en el análisis de centralidad, el concepto físico del centro de masa y el modelo de redes de entrega controlada (CDG), que considera la gestión en tiempo real de la energía en redes de distribución.

En uno de los más recientes trabajos sobre el uso de las redes complejas Tahirovic et al. [15] desarrollan una métrica de centralidad de flujo rebalanceado, que extiende los métodos tradicionales al incorporar la capacidad de las redes eléctricas de adaptarse a topologías cambiantes. La metodología que proponen basada en redes complejas permite identificar componentes críticos en la red, proporcionando una herramienta más robusta y flexible para la evaluación de la vulnerabilidad, especialmente en redes eléctricas adaptativas en donde los flujos y la estructura pueden cambiar.

Wu et al. [16], mediante el análisis de redes "small-world", como la red eléctrica de la India y modelos IEEE, identifican nodos y líneas críticas cuya falla puede desencadenar apagones a gran escala. Un aporte adicional es el uso de redes ponderadas, donde los pesos de las conexiones entre nodos representan impedancias y otros factores eléctricos relevantes para la transmisión de energía.

En Forsberg et al. [17] evalúan la robustez estructural de la red de transmisión nórdica y hacen un aporte a la medición de la vulnerabilidad en redes eléctricas al combinar la teoría de redes complejas con parámetros eléctricos, con este enfoque hibrido logran identificar los nodos clave en las redes de transmisión y está en línea con los estudios de los operadores de red (OR), lo que lo convierte en una herramienta valiosa para optimizar la planificación y la resiliencia frente a eventos de alta magnitud y baja probabilidad (HILP).
El modelo de fallos en enlaces es usado en Tamhane et Al. [18] para medir la vulnerabilidad de la red eléctrica, este simula la desconexión de líneas de transmisión clave y evalúa cómo la redistribución de carga genera sobrecargas y fallas en cascada. Las fallas en enlaces entre generadores son las más críticas, mientras que las fallas en dead-ends tienden a ser locales y no impactan significativamente a la red en su conjunto.

En el trabajo de Wan et al. [19] presenta una propuesta innovadora que se centra en el uso de redes neuronales gráficas, combinado con la teoría de redes complejas y el uso de la centralidad de autovectores como métrica de vulnerabilidad, ofreciendo un método más eficiente y preciso para identificar nodos críticos en las redes eléctricas. Este trabajo proporciona una herramienta práctica para la gestión y operación de los sistemas eléctricos. Además, este enfoque que se centra en atacar los enlaces supone un avance importante en comparación con los métodos tradicionales enfocados en los nodos, y tiene aplicaciones prácticas para mejorar la resiliencia de las redes eléctricas ante fallos o ataques.

Año	Título artículo	Referencia	Red de prueba	Medida de centralidad usada	Modelo de red	Métricas de eficiencia	Red ponderada o no ponderada	Modelo empleado para evaluar ataques
2018	Applications of Complex Network Analysis in Electric Power Systems	[14]	Red IEEE de 30 nodos	Centralidad de cercanía, intermediación	Red no dirigida.	Resiliencia, Factor de rendimiento, Reducción de pérdidas	Ponderada	Vulnerabilidad ante ataques dirigidos
2019	Electrical Network Operational Vulnerability Evaluation Based on Small-World and Scale-Free Properties	[20]	Sistema IEEE de 39 nodos, Sistema IEEE de 118 nodos, Red Francesa	Grado, Intermediación (Betweenness), Grado de Entrada (In-Degree), Grado de Salida (Out-Degree)	Small-World, Scale-Free	Simulación de flujo de carga y pérdida de carga	Ponderada	Evaluación de vulnerabilidad con entropía simétrica para ataques específicos
2022	Component Importance and Interdependence Analysis for Transmission, Distribution and Communication Systems	[13]	Illinois Regional Transmission, Distribution, and Communication Systems	Cross-Closeness, Cross-Betweenness	Red de capas múltiples	Eficiencia, Caída de eficiencia de nodos	Ponderada	Simulación.
2021	A Complex Network Approach to Power System Vulnerability Analysis based on Rebalance Based Flow Centrality	[15]	IEEE 30, 57, 118-bus	Centralidad de flujo basada en reequilibrio	Red de flujo Laplaciano	Demanda suplida, tiempo de cálculo	No ponderada	Ataques en componentes críticos con centralidad de flujo
2023	Structure and stability of the Indian power transmission network	[18]	Red de transmisión de la India	Centralidad de grado	Red de transmisión	Lf/Lt para fallas de enlaces	Ponderada	Análisis de fallos en enlaces con nodos de alto grado
2023	Research on vulnerability assessment method of electric power network based on graph neural	[19]	IEEE 2383, case1354, case6515	Centralidad de autovector	Red de aprendizaje profundo	Precisión en nodos vulnerables	Ponderada	Redes neuronales gráficas para identificar nodos vulnerables
2018	Power grid vulnerability analysis using complex network	[17]	Nordic490	Centralidades combinadas (grado, cercanía, betweenness)	Red simplificada	Comparación cualitativa	Ponderada y no ponderada	Ataques dirigidos con centralidades
2018	Structural Vulnerability of Complex Networks Under Multiple Edge-Based Attacks	[16]	Red eléctrica italiana, ER, SF, WS	Centralidad de intermediación de enlaces (Edge betweenness)	Redes SF, ER, WS	Tamaño de componentes, grado de disrupción	Ponderada y no ponderada	Ataques múltiples basados en enlaces

Tabla 1 Tabla resumen métodos topológicos

2.2. Nuevas propuestas para evaluar la vulnerabilidad de las redes eléctricas

Una tecnología usada para reducir la vulnerabilidad del sistema son las redes inteligentes que en forma general abarcan las necesidades de mejorar la

accesibilidad a la energía, al implementar tecnologías que respondan a las exigencias de los clientes.[21]

En trabajos como el de Yang et Al.[22]proponen la integración de tecnologías emergentes, como el Internet de las Cosas (IoT) y algoritmos de aprendizaje profundo, en particular las redes de memoria a largo plazo (LSTM), para optimizar la recolección de datos y la predicción de la vida útil de las baterías usadas en las redes de distribución para mejorar su estabilidad y confiabilidad. Además, se propone que la aplicación de la tecnología de evaluación térmica dinámica (DTR) puede mejorar la estimación de la EENS, al permitir un monitoreo en tiempo real y una evaluación más precisa de los componentes vulnerables y los riesgos potenciales de fallos.

2.3. Métodos para evaluar vulnerabilidad en redes eléctricas de distribución

Sí bien existe una considerable cantidad de investigaciones en la evaluación de vulnerabilidad de redes eléctricas, la mayoría de estos estudios se han enfocado principalmente en las redes de transmisión, mientras que los estudios sobre la vulnerabilidad en las redes de distribución son más escasos. A continuación, se presentarán algunos aportes de diferentes investigadores sobre el tema.

En el trabajo de Wen et al. [23] sugieren un enfoque integral para identificar partes vulnerables en redes de distribución, utilizando el método TOPSIS, mejorado con índices de vulnerabilidad basados en la teoría de redes complejas y características eléctricas, como el flujo de potencia y la eficiencia. También implementan índices tanto estructurales como operativos, junto con el Proceso Analítico Jerárquico (AHP) y la ponderación por entropía, para determinar la vulnerabilidad de nodos y líneas.

A través del análisis de la red de prueba IEEE de 24 nodos Shazad [24] propone un marco para evaluar la vulnerabilidad en redes de distribución de sistemas de potencia. En la prueba introduce índices para medir la vulnerabilidad de generadores y se demuestra que su desconexión aumenta el riesgo. El autor hace énfasis en la protección de componentes críticos, como líneas y buses, para mejorar la resiliencia ante eventos de alto impacto y baja probabilidad (HILP), contribuyendo a una mejor planificación y operación de las redes.

ASPECTO	Artículo	
	The concept of vulnerability and resilience in electric power systems[24]	A TOPSIS-Based Vulnerability Assessment Method of Distribution Network Considering Network Topology and Operation Status[23]
Método de Evaluación	Análisis general de vulnerabilidad y resiliencia	Evaluación TOPSIS de vulnerabilidad en la red de distribución

Índices Utilizados	Índices de vulnerabilidad operativa y no operativa	Índices estructurales y de estado (eficiencia de nodos y líneas, etc.)
Modelo de Ataque	Eventos de alto impacto y baja probabilidad (HILP)	Modelos de ataque aleatorio y deliberado
Resultados	Identificación de nodos vulnerables en sistemas de prueba	Identificación de nodos y líneas vulnerables en la red IEEE de 33 nodos
Metodología	Métricas cualitativas y cuantitativas de resiliencia	Método TOPSIS mejorado con el grado de correlación gris

Tabla 2 Comparativa métodos evaluación vulnerabilidad en redes de distribución.

2.4. Métodos para evaluar vulnerabilidad en sistemas de distribución con alta penetración de energías renovables.

En el proceso de transición energética, es fundamental integrar nuevos elementos a las redes de distribución eléctrica, como las fuentes de energía eólica y solar, así como la conexión de vehículos eléctricos. En el artículo de Lu et al. [25] exponen un método para identificar los puntos vulnerables de la red de distribución con generación distribuida y vehículos eléctricos, mediante un enfoque de ponderación subjetiva (relación de orden G1) y objetiva (entropía mejorada), encontrando los puntos críticos como la estabilidad de voltaje y sobrecargas. Los autores además mediante simulaciones con datos reales sugieren la compensación de potencia reactiva y la regulación del voltaje como soluciones a estas problemáticas.

Yang et al. [4] investigan los factores tanto internos como externos que influyen en la vulnerabilidad de las redes de distribución, centrándose en la mayor complejidad e incertidumbre derivadas de la integración de recursos energéticos distribuidos, vehículos eléctricos y su conexión con otras redes. También examinan los métodos de evaluación de vulnerabilidad y destacan indicadores clave, como la energía esperada no suministrada (EENS), la relevancia de los nodos y la duración de las baterías de iones de litio.

En el estudio de la evaluación de nodos vulnerables en la red de distribución bajo la influencia de fuentes de energía renovable, Hu et Al. [26] introducen un método basado en el muestreo de hipercubo latino y matrices booleanas para calcular un índice de vulnerabilidad, considerando la topología de la red, el riesgo de fallas y el impacto del flujo de potencia. Los investigadores validan su modelo en un sistema IEEE de 39 de nodos, demostrando que ciertos nodos críticos son esenciales para la estabilidad de la red, proporcionando una herramienta valiosa para los operadores de red (OR) en el ejercicio de un continuo seguimiento de la complejidad añadida a las redes eléctricas por la integración de recursos de energía renovable.
Uno de los aportes más novedosos es el de Xu et Al. [27] que en su documento usan redes neuronales profundas para analizar y predecir la vulnerabilidad de las

redes de distribución bajo diferentes escenarios operativos. El aporte de esta investigación en un enfoque novedoso para mejorar la resiliencia de las redes de distribución moderna, ayudando a los operadores de red (OR) a anticipar y gestionar las vulnerabilidades que surgen con la transición energética hacia un sistema eléctrico más descentralizado.

En el trabajo de Huang et Al. [28], a través del modelo MDATFA (Evaluación Multidimensional con Asociación Difusa Integrada), que fusiona índices de salud e importancia, se identifican puntos críticos en la red. Se emplean técnicas avanzadas, como la minería de reglas de asociación, para detectar variables poco frecuentes, pero de alto riesgo, y un sistema difuso probabilístico jerárquico para procesar datos continuos, lo que mejora la precisión en la evaluación del estado de las líneas de transmisión. Este enfoque aporta una metodología robusta para gestionar el riesgo y mejorar la planificación operativa de las redes de distribución en entornos complejos y dinámicos.

Dentro de los métodos propuestos en los últimos años, Lin et al. [2] trabajaron en un método integral para evaluar la vulnerabilidad en redes de distribución eléctrica, combinando análisis de la estructura topológica y el estado operativo. Utiliza la teoría de redes complejas para mejorar indicadores como el grado de nodo y la cohesión, y agrega indicadores operativos como la intermediación eléctrica, la inyección de potencia y el desfase de voltaje. Para validar su modelo emplearon una red IEEE de 33 nodos, identificando los nodos más vulnerables

3. Marco Teórico

3.1. Sistemas de transmisión y distribución en Colombia:

El sistema eléctrico en Colombia es crucial para el desarrollo socioeconómico del país, ya que garantiza el suministro de energía a hogares, industrias y comercios. Este sistema se compone de redes de transmisión y distribución, que desempeñan un papel esencial en la entrega eficiente y confiable de la energía generada en las plantas eléctricas hasta los usuarios finales.

La transmisión eléctrica consiste en el transporte de grandes volúmenes de energía desde las plantas generadoras hasta los centros de consumo mediante líneas de alta tensión, que en Colombia oscilan entre 110 y 500 kV.

La red de transmisión del país forma parte del Sistema Interconectado Nacional (SIN), que cubre regiones clave como la Andina, Caribe y Pacífico. Asimismo, se emplean tecnologías avanzadas para asegurar la estabilidad de la red y facilitar la interconexión de múltiples generadores, disminuyendo el riesgo de interrupciones en el servicio.

Por su parte, la distribución de energía es responsable de llevar la electricidad desde las subestaciones de transmisión hasta los consumidores finales. En esta fase, la tensión se ajusta a niveles apropiados para el consumo doméstico, comercial o industrial. El sistema de distribución enfrenta el reto de garantizar la calidad, seguridad y continuidad del servicio, elementos esenciales para asegurar la confiabilidad del sistema eléctrico.

Uno de los desafíos más importantes en la transmisión y distribución es mejorar la eficiencia energética, lo que implica reducir las pérdidas de energía mediante la adopción de nuevas tecnologías y optimizar la infraestructura actual. Además, el creciente aumento en la demanda de energía y la incorporación de fuentes renovables presentan nuevos retos técnicos y regulatorios. Las redes deben ser lo suficientemente flexibles para adaptarse a estos cambios y garantizar un suministro de energía seguro y eficiente.[29]

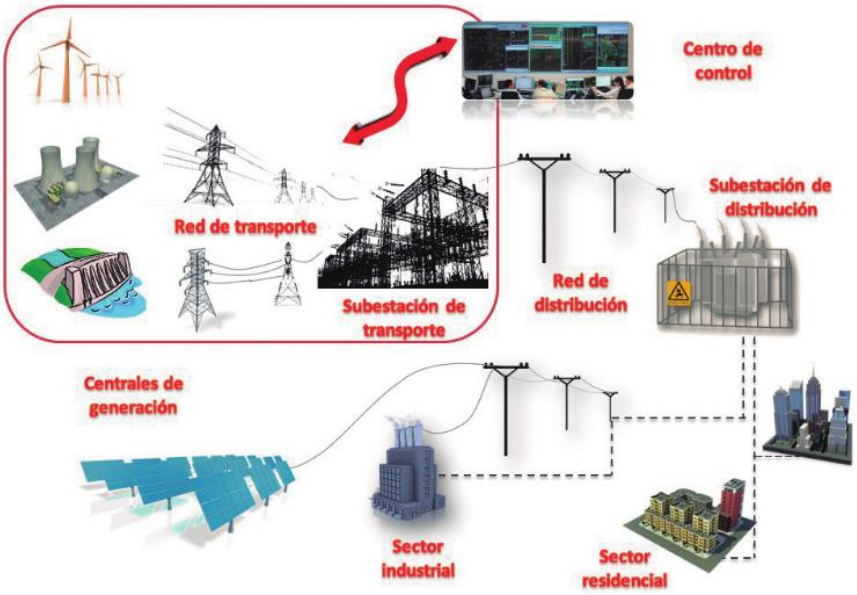

Ilustración 1 Ilustración de un sistema de potencia.[29]

3.2. Definiciones

3.2.1 Definición Vulnerabilidad:

La vulnerabilidad en los sistemas eléctricos se refiere a su incapacidad para resistir eventos disruptivos que comprometan su operación segura y estable. Esto abarca tanto eventos de baja probabilidad, pero alto impacto, como ciberataques, fenómenos naturales extremos (tormentas, huracanes) como fallas técnicas, que pueden causar interrupciones generalizadas y tener consecuencias sociales y económicas significativas.[24][30]

3.2.2 Definición de resiliencia:

La resiliencia es la capacidad de resistir eventos de alto impacto y baja probabilidad, recuperándose rápidamente y mejorando las operaciones y estructuras para mitigar el impacto de eventos similares en el futuro.[30]

3.2.3 Definición de confiabilidad:

La probabilidad de que el funcionamiento de una red eléctrica sea satisfactorio a largo plazo. La probabilidad de que un sistema de energía eléctrica pueda realizar una función requerida en unas condiciones determinadas durante un intervalo de tiempo determinado.[30]

3.2.4 Definición de robustez:

Grado en el que una red es capaz de soportar un evento inesperado sin que se produzca una degradación de su rendimiento. Cuantifica el daño que se produce como consecuencia de esa perturbación inesperada.[30]

3.3. Infraestructuras Críticas:

Las infraestructuras son sistemas a gran escala creados por el hombre que funcionan de forma interdependiente y que suministran bienes o servicios esenciales [31], el concepto de infraestructura crítica incluye todos los activos que son vitales para un país y que su destrucción o degradación tendría un efecto debilitante en las funciones esenciales del gobierno, la seguridad nacional o la economía.[32]

El sistema de energía eléctrica está catalogado como una de las infraestructuras más críticas. La red eléctrica se encuentra en estos momentos experimentando unos cambios significativos como lo son el envejecimiento de la infraestructura y todos los desafíos que implica la transición energética que ayude a disminuir las emisiones de CO2.[14]

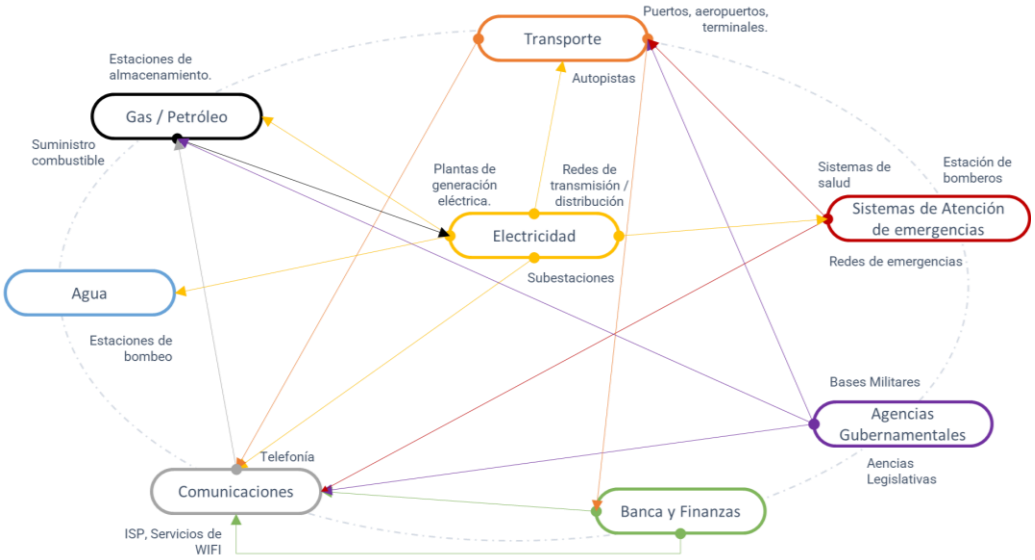

Ilustración 2 Ejemplo de la interdependencia entre el sistema de energía eléctrica y otras infraestructuras críticas.

3.4. Riesgos del sistema eléctrico:

En la Figura x se sugiere una taxonomía que diferencia los fallos aleatorios, los peligros naturales y los ataques intencionados (ataques puntuales y regionales).

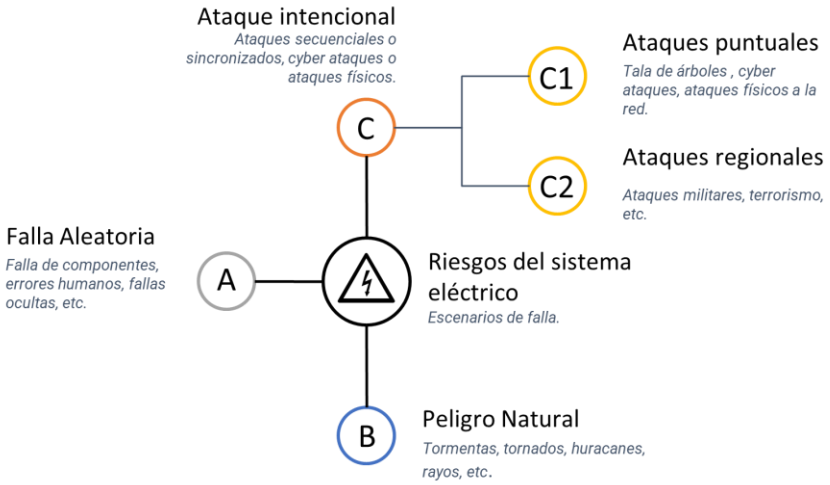

Ilustración 3 Escenarios de fallas en sistemas de potencia.

3.5. Modelos generales utilizados para evaluar el riesgo en las infraestructuras críticas:

Los sistemas eléctricos, como infraestructuras críticas, están expuestos a una variedad de riesgos, incluidas fallas técnicas, desastres naturales y ataques intencionados. Se han desarrollado varios modelos para evaluar el riesgo de estos sistemas y cuantificar sus vulnerabilidades y fallas mediante el uso de conceptos probabilísticos y estadísticos. Los modelos utilizados más comunes se muestran a continuación, junto con las ecuaciones fundamentales correspondientes.

3.5.1 Métodos Topológicos (Análisis de Redes Complejas):

Este enfoque estudia la estructura y dinámica de redes complejas como los sistemas eléctricos. Utiliza métricas como la centralidad (grado, cercanía, intermediación), y puede extenderse para considerar características eléctricas como la impedancia o el flujo de potencia. Las principales centralidades que se aplican son [33]:

- Centralidad de Grado: La centralidad de grado es una métrica sencilla que indica el número de conexiones (aristas) que tiene un nodo en una red, lo que refleja su conectividad directa. En un grafo $G = (V, E)$, donde V es el conjunto de nodos y E es el conjunto de aristas, la centralidad de grado de un nodo v se define como:

$$C_d(v) = \frac{\deg(v)}{n-1}$$

Donde:

- $\deg(v)$ es el grado del nodo v, es decir, el número de aristas que conectan el nodo v con otros nodos.

- n es el número total de nodos en el grafo.
- $n - 1$ es el factor de normalización, que representa el máximo número posible de conexiones que podría tener un nodo.

- Centralidad de Eigenvector: Mide la influencia de un nodo, no solo por sus conexiones directas, sino también por la importancia de los nodos conectados.
  El modelo matemático para la centralidad de eigenvector se expresa como el siguiente sistema de ecuaciones:

$$C_e(v_i) = \frac{1}{\lambda} \sum_{j \in V} A_{ij} C_e(v_j)$$

  Donde:
  - $C_e(v_i)$ es la centralidad de eigenvector del nodo v_i.
  - λ es el mayor eigenvalor asociado a la matriz de adyacencia A del grafo.
  - A_{ij} es el valor de la matriz de adyacencia que indica si existe una conexión entre los nodos i y j (generalmente, 1 si están conectados, 0 si no lo están).
  - La suma se realiza sobre todos los nodos *i* conectados a *j.*

- Centralidad de Cercanía: Mide la distancia promedio de un nodo a todos los demás, lo que refleja cuán cerca está el nodo del "centro" de la red. El modelo matemático de la centralidad de cercanía para un nodo v es:

$$C_c(v) = \frac{n - 1}{\sum_{u \in V} d(v, u)}$$

  Donde:
  - $C_c(v)$ es la centralidad de cercanía del nodo v.
  - n es el número total de nodos en la red.
  - $d(v, u)$ es la distancia más corta entre el nodo v y el nodo u, que generalmente se mide en número de enlaces o aristas.
  - La suma se realiza sobre todos los nodos $u \in V$, excepto v.

- Centralidad de Intermediación (o centralidad de betweenness): Mide cuántas veces un nodo o una línea actúa como un puente en los caminos más cortos entre otros nodos. El modelo matemático para la centralidad de intermediación de un nodo v es:

$$C_b(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

Donde:

- $C_b(v)$ es la centralidad de intermediación del nodo v.
- σ_{st} es el número total de caminos más cortos entre el nodo *s* y el nodo *t*.
- $\sigma_{st}(v)$ es el número de esos caminos más cortos que pasan por el nodo v.
- La suma se realiza sobre todos los pares de nodos *s* y *t* diferentes v (es decir, ***s*≠ *v*≠ *t***).

Estas medidas se han adaptado para redes eléctricas incluyendo características eléctricas como la impedancia de las líneas y el flujo de potencia, lo que proporciona un análisis más preciso de la vulnerabilidad estructural y funcional de la red eléctrica.

3.5.2 Métodos Basados en Flujos:

Los Métodos Basados en Flujos para evaluar la vulnerabilidad de sistemas eléctricos se dividen en enfoques deterministas y probabilísticos, y se usan para analizar y optimizar la capacidad máxima de flujo en redes ponderadas, como las eléctricas.

- **Método determinista:** El método determinista basado en el teorema del flujo máximo determina la máxima cantidad de flujo que un sistema de potencia puede manejar, teniendo en cuenta las restricciones de capacidad y el diseño de la red eléctrica. Aspectos como la capacidad de las líneas, los niveles de voltaje y la generación de los generadores afectan los flujos de potencia, aunque pequeñas perturbaciones pueden causar cambios significativos en el sistema [22]. El modelo se describe a través de los siguientes elementos y ecuaciones:

  1. **Representación de la red:**
     El sistema de potencia se modela como un grafo dirigido $G(V, E)$, donde V es el conjunto de buses y E es el conjunto de líneas de transmisión. Cada $e \in E$ tiene una capacidad $c(e)$, que representa la máxima potencia que puede transmitir.
  2. **Función objetivo:**
     El objetivo es maximizar el flujo $\boldsymbol{f}$ desde el nodo fuente $\boldsymbol{s}$ hasta el nodo sumidero $\boldsymbol{t}$, sujeto a la conservación de flujo y las restricciones de capacidad

$$\textbf{Maximizar} \sum_{(s,v)\in E} \boldsymbol{f(s,v)}$$

     El flujo $\boldsymbol{f(s,v)}$ debe respetar la restricción de capacidad $\boldsymbol{f(s,v)} \leq \boldsymbol{c(s,v)}$ para todas las líneas $\boldsymbol{(s,v)} \in \boldsymbol{E}$.

3. **Conservación de flujo:**
   En cada bus $\boldsymbol{v} \in \boldsymbol{V} \setminus \{\boldsymbol{s}, \boldsymbol{t}\}$, el flujo total que entra en el bus debe ser igual al flujo total que sale:

$$\sum_{(u,v)\in E} f(u,v) = \sum_{(v,w)\in E} f(v,w)$$

4. **Ecuaciones de flujo de potencia:**
   Los balances de potencia activa y reactiva en cada bus se rigen por las ecuaciones de flujo de potencia, especialmente en los buses de carga:

$$P_i = V_i \sum_{j=1}^{N} V_j\left(G_{ij}\cos\left(\theta_i - \theta_j\right) + B_{ij}\sin\left(\theta_i - \theta_j\right)\right)$$

$$Q_i = V_i \sum_{j=1}^{N} V_j\left(G_{ij}\sin\left(\theta_i - \theta_j\right) - B_{ij}\cos\left(\theta_i - \theta_j\right)\right)$$

   Donde P_i y Q_i son las potencias activas y reactiva en el i, Vi y Vj son las magnitudes de los voltajes, $\theta i \; y \; \theta j$ son los ángulos de voltaje, y G_{ij} y B_{ij} son la conductancia y susceptancia de la línea entre los buses i y j.

5. **Restricciones de capacidad:**
   El flujo de potencia en cada línea no debe exceder su capacidad:

$$|f(u,v)| \leq c(u,v) \quad \text{para todas } (u,v) \in E$$

   Este modelo es una simplificación del teorema del flujo máximo aplicado a los sistemas de potencia y se resuelve típicamente utilizando técnicas de optimización como la programación lineal o métodos iterativos [34].

- **Método probabilístico:** Existen diversos algoritmos analíticos de flujo de carga probabilístico, como la aproximación lineal, el método de estimación puntual, combinaciones de cumulantes y expansiones de Gram–Charlier, la estimación estadística de mínimos cuadrados y la transformación de Nataf, además del muestreo hipercubo latino. Estos algoritmos linealizan las ecuaciones de flujo de potencia en corriente alterna (AC), pero emplean una función de densidad probabilística en lugar de asumir valores fijos en las entradas[31].

3.5.3 Métodos Lógicos (Teoría de Juegos y Métodos Jerárquicos):

- **Teoría de juegos:** Von Neumann creó la teoría de juegos para estudiar el comportamiento estratégico. En tiempos recientes, esta teoría se ha aplicado en el estudio de la seguridad de infraestructuras, como las redes eléctricas, los sistemas de transporte y las cadenas de suministro. Se emplea para modelar ataques deliberados y amenazas inteligentes, representando la interacción entre los operadores de infraestructuras y los atacantes[31].
- **Métodos jerárquicos:** El análisis de vulnerabilidad utiliza métodos jerárquicos, como representaciones gráficas, agrupamientos y jerarquías lógicas, los cuales facilitan un análisis cualitativo y cuantitativo de infraestructuras críticas.[31]

3.5.4 Métodos Funcionales (Modelado Basado en Agentes): el modelado basado en agentes (ABM) como una técnica válida para estudiar sistemas de energía caracterizados por interacciones entre sus componentes puede modelar el comportamiento de "agentes" individuales (como operadores o componentes de la red) para evaluar cómo sus decisiones o fallos afectan al sistema completo[35].

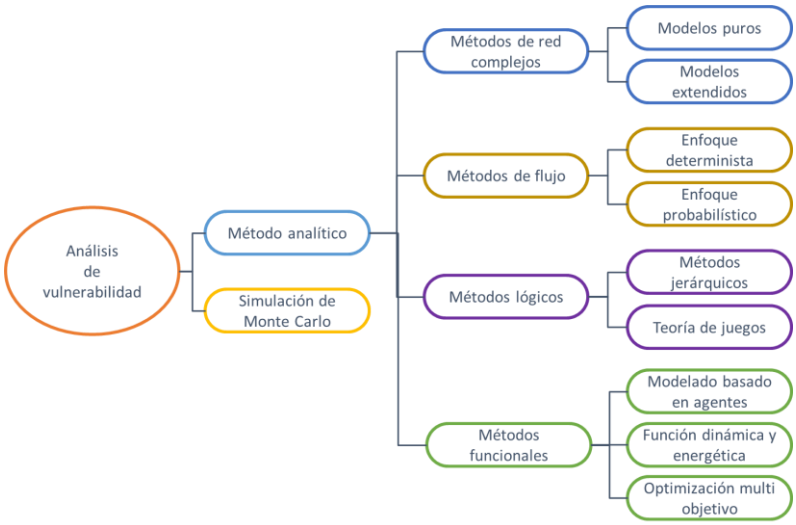

Ilustración 4 Diferentes métodos para el análisis de vulnerabilidad

3.6. Modelos para analizar redes eléctricas.

3.6.1 Redes “Small-World”” (Mundo Pequeño):
La mayoría de los nodos de una red "Small-World" están interconectados de tal manera que la distancia promedio entre ellos es pequeña, pero aun así tienen un alto coeficiente de agrupamiento. Estas redes combinan una gran conectividad local con la capacidad de conectar nodos lejanos, lo que hace que la propagación de información o flujos en la red sea más eficiente.

Propiedades matemáticas:

- **Longitud de camino promedio baja:** La distancia media entre dos nodos cualesquiera es pequeña en comparación con la cantidad total de nodos.
- **Alto coeficiente de agrupamiento:** Los vecinos de un nodo tienen una alta probabilidad de estar conectados entre sí.
- **Modelo de Watts-Strogatz:** Es el modelo matemático más común para generar redes de tipo small-world. Este modelo reconfigura una red regular introduciendo aleatoriedad para crear una estructura que tenga características de mundo pequeño.

En el contexto de redes eléctricas, las propiedades de las redes "small-world" permiten que los sistemas sean más robustos frente a fallos aleatorios debido a que existen múltiples rutas de acceso entre nodos. No obstante, fallos en nodos o enlaces importantes podrían generar un impacto desmedido, en particular en aquellos nodos que funcionan como puentes esenciales dentro de la red [36].

3.6.2 Redes “Scale-Free”” (Libres de Escala):

Las redes “Scale – Free” se caracterizan por tener una distribución de grados que sigue una ley de potencia, lo que quiere decir que el número de conexiones por nodo varía significativamente. Estas son redes resistentes frente a fallos aleatorios, pero altamente vulnerables a ataques estratégicos. [36]

Propiedades matemáticas:

- **Distribución de grados:** En las redes "scale-free", la distribución de grados sigue una ley de potencia $P(k) \sim k^{-\gamma}$, donde k es el número de conexiones de un nodo y γ es un parámetro positivo.[37]
- **Robustez y vulnerabilidad:** Las redes "libres de escala" son resistentes a fallos aleatorios, ya que la mayoría de los nodos cuenta con pocas conexiones, por lo que eliminar nodos de manera aleatoria tiene un impacto mínimo. No obstante, estas redes son susceptibles a ataques dirigidos a los nodos más conectados, ya que su eliminación puede provocar la fragmentación de la red.[38]

4. Diseño Metodológico

4.1. Fases y Metodología

4.1.1 Tipo de investigación y enfoque

El trabajo es una revisión del estado del arte, con enfoque en vigilancia tecnológica y prospectiva. Este tipo de investigación se centrará en analizar y evaluar las publicaciones científicas y tendencias actuales en el campo de la medición de la vulnerabilidad de las redes eléctricas de distribución con integración de generación distribuida. La prospectiva permitirá proyectar cómo los métodos y modelos actuales podrían evolucionar para enfrentar los retos de futuros escenarios con alta penetración de energías renovables.

4.1.2 Fases del desarrollo y actividades

El trabajo se desarrolló entre el 3 de septiembre y el 20 de septiembre, estructurado en las siguientes fases:

Fase 1: Revisión del Estado del Arte (3 de septiembre - 8 de septiembre)

Actividades:

1. Búsqueda y recolección de información en bases de datos académicas (IEEE, Scopus, ScienceDirect) sobre modelos y métodos que evalúan la vulnerabilidad de las redes eléctricas de distribución con integración de generación distribuida.
2. Uso de herramientas como research rabbit y elicit para encontrar trabajos similares a los artículos encontrados en las bases de datos científicas.
3. Identificación de métodos que aborden el tema de la medición o evaluación de la vulnerabilidad de las redes eléctricas de distribución destacando aquellos con escenarios de alta penetración de fuentes renovables.
4. Lectura crítica y análisis comparativo de los métodos existentes, con énfasis en la identificación de sus objetivos, suposiciones y enfoques.

Entregables:

- Lista de artículos científicos.

Relación con los objetivos:

- Se da cumplimiento al **objetivo específico 1**: revisar la bibliografía de los métodos de evaluación de vulnerabilidad.

Fase 2: Categorizar los Métodos (9 de septiembre - 12 de septiembre)
Actividades:

1. Clasificación de los métodos encontrados en función de sus características: enfoques probabilísticos, determinísticos, basados en simulación, etc.
2. Categorizar los métodos: métodos usados para evaluar vulnerabilidad, métodos para evaluar vulnerabilidad en redes de distribución y para evaluar vulnerabilidad en redes de distribución con integración de generación distribuida.

Entregables:

.

- Cuadro categorización.

Fase 3: Simulación de un Método Seleccionado (13 de septiembre - 18 de septiembre)
Actividades:

1. Selección de un método adecuado para la simulación, basado en la revisión y categorización realizada en las fases anteriores.
2. Preparación del entorno de simulación utilizando software especializado (ej. MATLAB, pandapower) para evaluar la vulnerabilidad de una red de distribución bajo escenarios de alta penetración de generación distribuida.
3. Ejecución de la simulación y análisis de los resultados obtenidos.

Entregables:

- Simulación ejecutada de un método específico.

Relación con los objetivos:

- Se da cumplimiento al **objetivo específico 3**: simular un método existente para evaluar la vulnerabilidad de una red de distribución con integración de generación distribuida.

Fase 4: Conclusiones y Recomendaciones Prospectivas (19 de septiembre - 20 de septiembre)
Actividades:

1. Integración de los hallazgos de la revisión del estado del arte, categorización y simulación en un documento final.
2. Elaboración de conclusiones sobre los métodos más adecuados para evaluar la vulnerabilidad de las redes con alta penetración de generación distribuida.
3. Identificación de tendencias futuras y recomendaciones para el desarrollo de nuevos métodos o mejoras en los existentes.

Entregables:

- Documento final del trabajo de grado.
- Recomendaciones sobre posibles líneas de investigación futuras.

Relación con los objetivos:

- Se concluye el trabajo dando cumplimiento al **objetivo general** y presentando una propuesta prospectiva para el futuro de la evaluación de la

vulnerabilidad en redes eléctricas con integración de fuentes de generación distribuida.

4.2. Cronograma

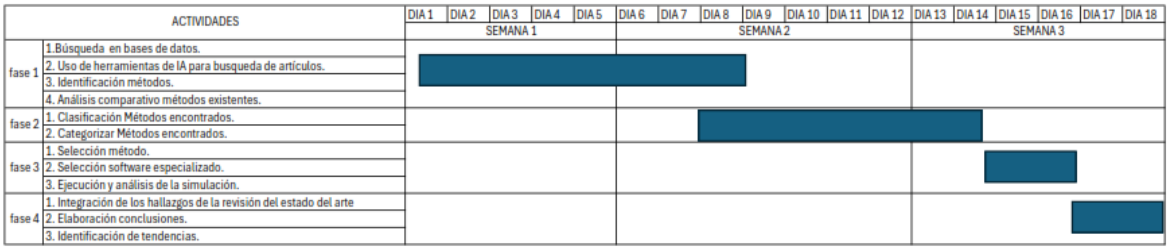

Ilustración 5 Cronograma de Actividades

5. Resultados y Discusión

En la primera fase del proyecto se realizan unas actividades que tenían como objetivo seleccionar las referencias bibliográficas que tuviesen información sobre métodos para evaluar y/o medir la vulnerabilidad obteniendo como resultado los siguientes artículos.

Title	Source	Year
A Comprehensive Assessment Method of Distribution Network Vulnerability Considering Topological Structure and Operation Status	Proceedings - 2023 8th Asia Conference on Power and Electrical Engineering, ACPEE 2023	2023
Review on vulnerability analysis of power distribution network	Elsevier Ltd.	2023
A TOPSIS-Based Vulnerability Assessment Method of Distribution Network Considering Network Topology and Operation Status	IEEE Access	2023
The concept of vulnerability and resilience in electric power systems	Australian Journal of Electrical and Electronics Engineering	2021
Vulnerability Assessment and Governance of Distribution Network Considering New Energy Integration	Proceedings of 2024 IEEE 13th Data Driven Control and Learning Systems Conference, DDCLS 2024	2024
Identification of critical nodes in power system under the influence of new energy sources	Proceedings - 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2021	2021
Deep Learning-Based Vulnerability Assessment of Distribution Grids Containing Distributed Power Sources and Electric Vehicles	Institute of Electrical and Electronics Engineers (IEEE)	2024
An integrated risk assessment model for the multi-perspective vulnerability of distribution networks under multi-source heterogeneous data distributions	International Journal of Electrical Power and Energy Systems	2023

Tabla 3 Lista artículos sobre evaluación de vulnerabilidad en redes de distribución con integración de generación distribuida.

Se puede apreciar que un 50% de los artículos fueron publicados en 2023 y un 25% en 2024, eso quiere decir que un 75% de los artículos que fueron encontrados con información sobre medición de la vulnerabilidad en redes de distribución con integración de generación distribuida han sido publicados en los últimos años.

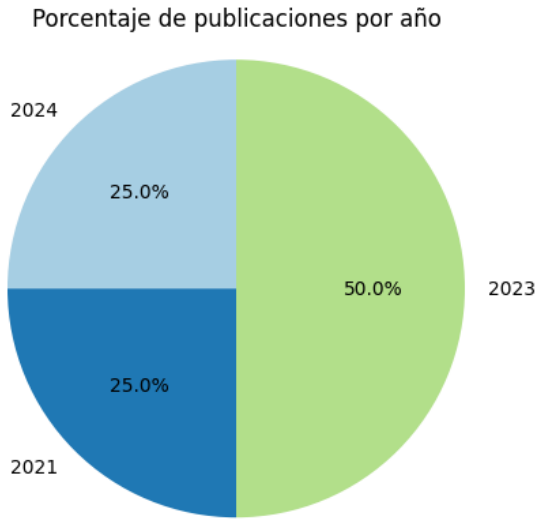

Ilustración 6 Porcentaje de publicaciones por año de la muestra seleccionada sobre métodos para evaluar la vulnerabilidad en redes de distribución con integración de fuentes renovables.

Para la fase 2 se realizó una clasificación de la información en una tabla donde se categoriza los diferentes métodos utilizados para la evaluación de vulnerabilidad en redes de distribución que incluyen generación distribuida o nuevas fuentes de energía.

Método de Evaluación de Vulnerabilidad	**Descripción**	**Generación Distribuida/Nuevas Fuentes de Energía Integradas**	**Artículo**	**Referencia**	**Año de Publicación**
TOPSIS (Technique for Order Preference by Similarity to Ideal Solution)	- Método de decisión multiatributo que clasifica nodos vulnerables basándose en la distancia de las soluciones ideales positivas y negativas. - Evalúa tanto la estructura como el estado de operación de la red.	Evaluado con la integración de fuentes de energía renovable, como la solar y la eólica, para identificar los nodos vulnerables en redes de distribución activas.	A Comprehensive Assessment Method of Distribution Network Vulnerability Considering Topological Structure and Operation Status	[2]	2023
Análisis Jerárquico (AHP) combinado con Método de Entropía	- Método para ponderar indicadores subjetivos (AHP) y objetivos (entropía). - Combina múltiples indicadores para clasificar nodos y líneas vulnerables en redes de distribución.	Considera el impacto de la generación distribuida (DG) y vehículos eléctricos (EV) para evaluar la vulnerabilidad de las redes de distribución activas con nuevas energías.	Vulnerability Assessment and Governance of Distribution Network Considering New Energy Integration	[25]	2024
Método basado en Redes Complejas	- Evalúa la vulnerabilidad de la red a través de la teoría de redes complejas. - Se centra en la estructura topológica, analizando la cohesión de la red y el grado de los	Se aplica en redes con alta penetración de fuentes de energía renovable, evaluando cómo la estructura de la red se ve afectada por la volatilidad de estas nuevas fuentes.	A Comprehensive Assessment Method of Distribution Network Vulnerability Considering Topological Structure and Operation Status	[2]	2023

	nodos para identificar los más vulnerables.				
Método de Muestreo Hiperlátice y Ordenación de Matriz Booleana	- Utiliza el muestreo hiperlátice para calcular probabilidades de falla de nodos en la red y un sistema de ordenación con matrices booleanas para identificar los nodos vulnerables. - Evalúa la influencia de nuevas energías en la red.	Diseñado específicamente para redes con integración de fuentes de energía renovables (eólica, solar) y generación distribuida. Se enfoca en la identificación de nodos críticos.	Identification of Critical Nodes in Power System under the Influence of New Energy Sources	[26]	2021
Aprendizaje Profundo (Deep Learning)	- Método basado en inteligencia artificial que utiliza aprendizaje profundo para predecir vulnerabilidades en redes con integración de nuevas energías. - Evalúa la vulnerabilidad en tiempo real considerando la dinámica del sistema.	Integra fuentes de energía distribuidas y vehículos eléctricos (EV), permitiendo la evaluación dinámica de vulnerabilidad y mejorando la precisión en redes con energías renovables.	Deep Learning-Based Vulnerability Assessment of Distribution Grids Containing Distributed Power Sources and Electric Vehicles	[27]	2021
Modelo de Evaluación de Riesgo Multiperspectiva	- Integra múltiples fuentes de datos heterogéneas para evaluar la vulnerabilidad de las redes de distribución. - Evalúa la vulnerabilidad de las redes a través de perspectivas múltiples, considerando tanto factores internos como externos.	El modelo incluye la integración de generación distribuida (DG) y nuevas energías, considerando las fluctuaciones y la intermitencia de estas fuentes para predecir puntos vulnerables.	An Integrated Risk Assessment Model for the Multi-Perspective Vulnerability of Distribution Networks	[28]	2021
Método basado en el Entropía Mejorada y Ponderación Objetiva	- Utiliza el método de entropía mejorada para asignar pesos a indicadores de vulnerabilidad de la red. - Se basa en el análisis del impacto de la nueva energía y su influencia en la estabilidad de la red.	Se enfoca en la evaluación de redes con alta penetración de generación distribuida (solar y eólica) y su impacto en la estabilidad y calidad del suministro eléctrico.	Vulnerability Assessment and Governance of Distribution Network Considering New Energy Integration	[25]	2024

Tabla 4 Categorización métodos evaluación de vulnerabilidad en redes de distribución con integración de generación distribuida.

En la fase 3 se decidió optar por simular el método de relación de orden G1 que clasifica dentro de la categoría de “Análisis Jerárquico (AHP) combinado con el método de Entropía”, ya que este método se enfoca en la asignación de pesos a los indicadores para evaluar la vulnerabilidad de la red. La relación de orden G1 es un método subjetivo, similar al AHP, y puede ser complementado con métodos objetivos, como el de entropía, para una evaluación más completa.

En el artículo de Lu et al. [25] se menciona el método de relación de orden G1 como parte del enfoque para asignar pesos a los indicadores de vulnerabilidad.

Para poder simular un escenario de una red de distribución con integración de energías renovables se opta por el software **pandapower** el cual es una herramienta de código abierto en Python para el modelado, análisis y optimización de sistemas de energía eléctrica equilibrados. Ofrece funcionalidades como flujo de potencia, flujo de potencia óptimo, estimación de estados y cálculos de cortocircuito según IEC 60909. Se basa en la biblioteca **pandas** para una manipulación eficiente de datos y permite modelar elementos eléctricos como líneas y transformadores. Su facilidad de uso, flexibilidad y automatización hacen que sea ideal para estudios científicos, aplicaciones educativas y análisis de redes de distribución simétricas.[39]

Pandapower tiene varias redes de prueba y dentro de esas se encuentra la red de distribución de media tensión basada en un modelo CIGRÉ (Consortium of International Large Power Grid Experts), esta red de prueba contiene 8 generadores fotovoltaicos y una turbina de viento.

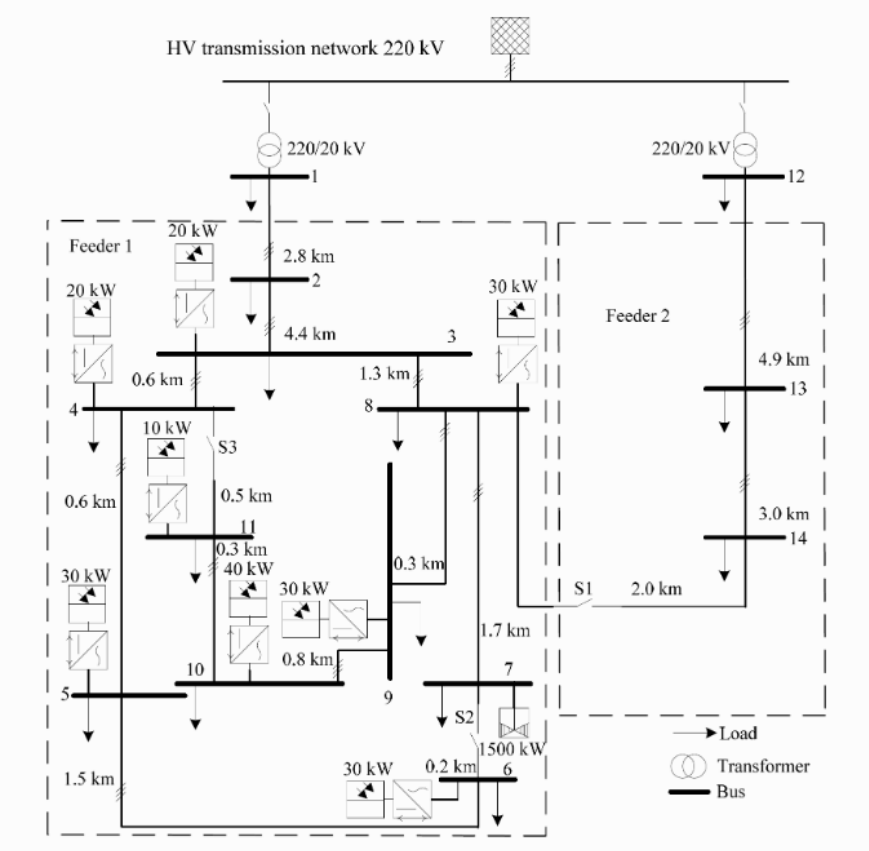

Ilustración 7 CIGRE Networks - Medium voltage distribution network with PV and Wind DER

Pasos a seguir para simular la red en pandapower:

1. Cargar la red:

```
net = pn.create_cigre_network_mv(with_der="pv_wind")
```

2. Realizar un análisis de flujo de potencia:

```
pp.runpp(net)
```

3. Obtener resultados de flujo de carga:
   Voltajes en cada nodo:

```
voltages = net.res_bus['vm_pu']
```

   Esto recupera los valores de voltaje (en pu, por unidad) en los nodos (barras) de la red.

   Cargabilidad de las líneas:

```
line_loading = net.res_line['loading_percent']
```

   Obtiene el porcentaje de carga de cada línea, que indica cuánta capacidad de la línea está siendo utilizada.

   Cargabilidad de los transformadores:

```
trafo_loading = net.res_trafo['loading_percent']
```

   Similar al caso de las líneas, esto obtiene la carga de cada transformador en la red.

4. **Definición de pesos relativos**:

```
r_volt = 2
r_trafo = 1.5
r_line = 1.2
r_phase = 1
```

   Aquí se asignan pesos relativos a diferentes indicadores que se usarán para el cálculo del índice de vulnerabilidad, dándole mayor o menor importancia a cada factor.

5. **Asignar pesos iniciales:**

```
weights = {}
weights['phase_unbalance'] = 1
weights['line_loading'] = weights['phase_unbalance'] * r_line
weights['trafo_loading'] = weights['line_loading'] * r_trafo
weights['voltage_stability'] = weights['trafo_loading'] * r_volt
```

Esto asigna pesos iniciales a los indicadores de la red basados en los factores de importancia relativa definidos previamente.

6. **Normalización de los pesos:**

```
total_weight = sum(weights.values())
for key in weights:
    weights[key] /= total_weight
```

Aquí se normalizan los pesos para que la suma total sea igual a 1, lo que garantiza que cada indicador tenga una contribución proporcional en el cálculo final.

7. **Normalización de las variables:** Para calcular los índices de vulnerabilidad, se normalizan las variables:

Voltaje:

```
voltages_normalized = (voltages - voltage_min) / (voltage_max - voltage_min)
```

Cargabilidad de líneas:

line_loading_normalized = (line_loading - line_loading_min) / (line_loading_max - line_loading_min)

Cargabilidad de transformadores:

trafo_loading_normalized = (trafo_loading - trafo_loading_min) / (trafo_loading_max - trafo_loading_min)

8. **Cálculo del índice de vulnerabilidad:**

Para los nodos:

```
for bus in net.bus.index:
    voltage_stability = voltages_normalized[bus]
    index = weights['voltage_stability'] * voltage_stability
    vulnerability_index[bus] = index
```

Se calcula un índice de vulnerabilidad para cada nodo basado en la estabilidad de voltaje y el peso asociado a este indicador.

Para las líneas:

```
for line in net.line.index:
    line_loading_norm = line_loading_normalized[line]
    index = weights['line_loading'] * line_loading_norm
    if line in vulnerability_index:
        vulnerability_index[line] += index
    else:
        vulnerability_index[line] = index
```

Similar a los nodos, se calcula el índice de vulnerabilidad para las líneas basándose en su cargabilidad.

Para los transformadores:

```
for trafo in net.trafo.index:
    trafo_loading_norm = trafo_loading_normalized[trafo]
    index = weights['trafo_loading'] * trafo_loading_norm
    if trafo in vulnerability_index:
        vulnerability_index[trafo] += index
    else:
        vulnerability_index[trafo] = index
```

9. **Mostrar el índice de vulnerabilidad**: Finalmente, se imprimen los índices de vulnerabilidad calculados para cada elemento (nodos, líneas y transformadores):

```
print(vulnerability_index)
```

Este análisis entrega un diccionario en Python que contiene los nodos y su índice de vulnerabilidad, mostrando que aquellos elementos con un índice más alto son más vulnerables a sobrecargas o inestabilidades de voltaje, lo que puede ser relevante para estudios de confiabilidad o planificación de expansión de la red.

Resultados simulación:

Nodo	Índice
0	0,87
1	0,42
2	0,27
3	0,10
4	0,05
5	0,09
6	0,08
7	0,08
8	0,03
9	0,06
10	0,03
11	0,02
12	0,30
13	0,28
14	0,26

Tabla 5 Tabla resultados simulación.

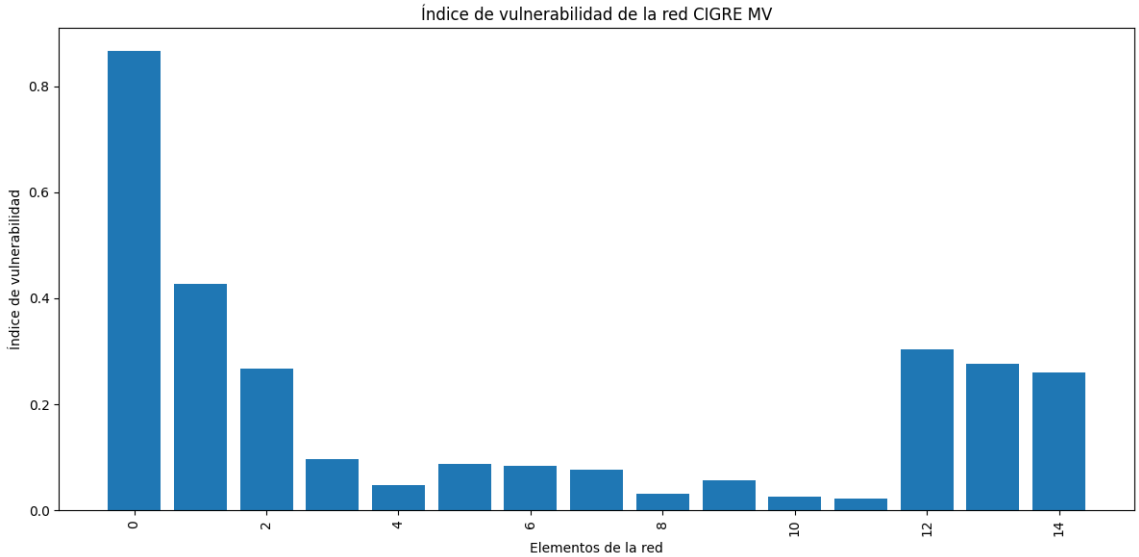

Ilustración 8 Gráfica de barras con el índice de vulnerabilidad de los nodos de la red CIGRE MV

Como se puede apreciar en los resultados de la simulación los puntos más vulnerables en la red son el nodo 0, nodo 1 y nodo 12. Por lo cual estos deberían ser priorizados en intervenciones preventivas en la red para mitigar riesgos.

6. Conclusiones y Trabajos futuros

La revisión del estado del arte mostró que existe una variedad de métodos para evaluar la vulnerabilidad en redes eléctricas, desde enfoques basados en la teoría de redes complejas hasta métodos deterministas y probabilísticos. Sin embargo, los estudios sobre redes de distribución con alta penetración de generación distribuida son limitados en comparación con los enfoques aplicados a redes de transmisión. Este trabajo contribuye a cerrar esa brecha, destacando la importancia de métodos como el TOPSIS y las redes complejas, los cuales permiten una evaluación más precisa de la vulnerabilidad estructural y operativa.

La clasificación de los métodos existentes según su enfoque probabilístico, determinista o basado en simulación permitió identificar ventajas y limitaciones de cada uno en escenarios con alta penetración de generación distribuida. El análisis mostró que los métodos que combinan análisis topológico con indicadores operativos, como el flujo de potencia, son más robustos para evaluar redes de distribución en comparación con enfoques puramente estructurales. Este trabajo aporta claridad al estado del arte al proponer una categorización clara que facilita la selección del método adecuado dependiendo de las características de la red.

La simulación del método de relación de orden G1, en combinación con la ponderación objetiva de entropía, mostró que ciertos nodos y líneas de la red presentan mayor vulnerabilidad debido a inestabilidades de voltaje y sobrecargas. Esta evaluación confirma la utilidad del enfoque G1 en la identificación de puntos críticos en redes con alta penetración de energías renovables. El aporte metodológico de este estudio radica en la adaptación y validación de este enfoque en redes de distribución modernas.

Futuras investigaciones pueden explorar cómo tecnologías emergentes, como el Internet de las Cosas (IoT) y la inteligencia artificial (IA), podrían mejorar los métodos de evaluación de vulnerabilidad, especialmente en la predicción de fallos y en la gestión en tiempo real de redes de distribución.

Se recomienda la simulación de redes de mayor complejidad que incluyan no solo generación distribuida, sino también la presencia de vehículos eléctricos y sistemas de almacenamiento de energía. Esto permitiría evaluar el impacto de la carga fluctuante y la variabilidad en la generación sobre la estabilidad y vulnerabilidad de la red.

Investigaciones futuras podrían centrarse en desarrollar estrategias de optimización que permitan reforzar la resiliencia de redes de distribución ante eventos como desastres naturales o ataques cibernéticos. La combinación de simulaciones de vulnerabilidad con herramientas de toma de decisiones optimizadas será clave para la robustez de futuras redes eléctricas.

Sería relevante desarrollar métricas adicionales que combinen tanto indicadores técnicos como económicos para evaluar no solo la vulnerabilidad, sino también el costo de reforzar puntos críticos en la red, especialmente en redes con alta penetración de renovables.

En el marco de la transición energética que Colombia está experimentando, es fundamental desarrollar una estrategia integral para la protección y optimización de las redes de distribución eléctrica. La creciente penetración de energías renovables, como la solar y eólica, plantea nuevos desafíos para garantizar la estabilidad y resiliencia del sistema eléctrico. A estos desafíos se suman problemas de orden público, como actos vandálicos y sabotajes, que pueden vulnerar las infraestructuras críticas, y afectaciones socioeconómicas que aumentan las pérdidas no técnicas (robo de energía y conexiones ilegales).

Es urgente que las empresas de distribución de energía eléctrica, en colaboración con el gobierno, implementen tecnologías de vigilancia y monitoreo en tiempo real para detectar y mitigar ataques a las redes, así como desarrollar planes de contingencia ante eventos deliberados que afecten la red eléctrica. El uso de drones y sensores inteligentes integrados en una infraestructura IoT podría ayudar a identificar vulnerabilidades antes de que escalen en grandes interrupciones.

Se deben implementar sistemas avanzados de medición y control basados en tecnologías de inteligencia artificial y big data, para identificar rápidamente patrones de uso anómalos y reducir las pérdidas no técnicas. Programas sociales y educativos que promuevan la legalización de las conexiones eléctricas en comunidades vulnerables también son esenciales para abordar las causas socioeconómicas de estas pérdidas.

Dada la susceptibilidad de la red a fenómenos de orden público y naturales, es clave mejorar la robustez del sistema a través de la diversificación del suministro energético, mediante la integración de generación distribuida (GD) y almacenamiento de energía. Estas medidas permitirían reducir la dependencia de infraestructuras centralizadas, facilitando una respuesta más rápida y eficaz ante incidentes.

El desarrollo de proyectos piloto que combinen energías renovables con sistemas de almacenamiento, en áreas donde las pérdidas no técnicas y los problemas de orden público son más evidentes, ofrecería un laboratorio real para explorar nuevas soluciones. Además, estos esfuerzos ayudarían a preparar mejor las redes para futuras ampliaciones y optimizaciones tecnológicas.

Estas sugerencias pueden contribuir a avanzar en el campo de la evaluación de vulnerabilidad y optimización de las redes eléctricas de distribución, ayudando a los operadores a prepararse mejor para los desafíos que se presentan con la transición energética.

7. Anexos

A. Código fuente en Python usando pandapower:

```
import pandapower as pp
import pandapower.networks as pn
import pandapower.plotting as plot

net = pn.create_cigre_network_mv(with_der="pv_wind")

# Ejecutar el análisis de flujo de carga
pp.runpp(net)

# Obtener el voltaje en cada nodo
voltages = net.res_bus['vm_pu']

# Obtener la carga de las líneas
line_loading = net.res_line['loading_percent']

# Obtener la carga de los transformadores
trafo_loading = net.res_trafo['loading_percent']

# Definir la importancia relativa (r) entre los indicadores
r_volt = 2
r_trafo = 1.5
r_line = 1.2
r_phase = 1

# Asignar los pesos iniciales
weights = {}
weights['phase_unbalance'] = 1
weights['line_loading'] = weights['phase_unbalance'] * r_line
weights['trafo_loading'] = weights['line_loading'] * r_trafo
weights['voltage_stability'] = weights['trafo_loading'] * r_volt

# Normalizar los pesos
total_weight = sum(weights.values())
for key in weights:
    weights[key] /= total_weight

# Calcular el índice de vulnerabilidad para cada elemento
vulnerability_index = {}

# Normalización para voltaje
voltage_max = max(voltages)
voltage_min = min(voltages)
```

```
voltages_normalized = (voltages - voltage_min) / (voltage_max - voltage_min)

# Normalización para carga de líneas
line_loading_max = max(line_loading)
line_loading_min = min(line_loading)
line_loading_normalized = (line_loading - line_loading_min) / (line_loading_max - line_loading_min)

# Normalización para carga de transformadores
trafo_loading_max = max(trafo_loading)
trafo_loading_min = min(trafo_loading)
trafo_loading_normalized = (trafo_loading - trafo_loading_min) / (trafo_loading_max - trafo_loading_min)

# Vulnerabilidad de nodos
for bus in net.bus.index:
    voltage_stability = voltages_normalized[bus]
    index = weights['voltage_stability'] * voltage_stability
    vulnerability_index[bus] = index

# Vulnerabilidad de líneas
for line in net.line.index:
    line_loading_norm = line_loading_normalized[line]
    index = weights['line_loading'] * line_loading_norm
    if line in vulnerability_index:
        vulnerability_index[line] += index
    else:
        vulnerability_index[line] = index

# Vulnerabilidad de transformadores
for trafo in net.trafo.index:
    trafo_loading_norm = trafo_loading_normalized[trafo]
    index = weights['trafo_loading'] * trafo_loading_norm
    if trafo in vulnerability_index:
        vulnerability_index[trafo] += index
    else:
        vulnerability_index[trafo] = index

# Mostrar el índice de vulnerabilidad
print(vulnerability_index)
```

B. Presupuesto

Se indican los roles de los participantes en el proyecto y los valores de las licencias a usar en el desarrollo del proyecto.

Título Profesional	Nombre	Rol en el Proyecto
Ingeniero Electrónico Magíster Teleinformática Doctor en Ingeniería Sísmica y Dinámica Estructural	Jaime Vitola Oyaga	Director del Proyecto
Ingeniero Electrónico Magister en ingeniería eléctrica Doctor en ingeniería eléctrica	Billy Vladimir Toro Tovar	Codirector del proyecto
Ingeniero Electrónico Magíster en Ingeniería Electrónica y de Computadores	Alexander Cortés Llanos	Asesor Externo
Ingeniero Electrónico	Randy José Agustín Montenegro Socha	Investigación

Tabla 6 Personas que intervienen en el proyecto y su rol

LICENCIA	VALOR
Pandapower	Gratuita

Tabla 7 Valor licencia

8. Referencias Bibliográficas

[1] J. A. Melo Rodriguez and C. A. Cortés Guerrero, “Análisis de vulnerabilidad de sistemas de potencia incluyendo incertidumbre en las variables con lógica difusa tipo 2,” *Revista Tecnura*, vol. 20, no. 49, p. 100, Sep. 2016, doi: 10.14483/udistrital.jour.tecnura.2016.3.a07.

[2] S. Lin and J. Wen, “A Comprehensive Assessment Method of Distribution Network Vulnerability Considering Topological Structure and Operation Status,” in *Proceedings - 2023 8th Asia Conference on Power and Electrical Engineering, ACPEE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 2168–2173. doi: 10.1109/ACPEE56931.2023.10135904.

[3] M. Wang, X. Sheng, Q. Wang, C. Xu, D. Pan, and H. Gao, “Vulnerability Assessment Method of Distribution Network Nodes Based on Jaya-AHP-EWM-MARCOS,” in *Proceedings - 2023 Power Electronics and Power System Conference, PEPSC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 421–430. doi: 10.1109/PEPSC58749.2023.10395374.

[4] L. Yang and J. Teh, “Review on vulnerability analysis of power distribution network,” Nov. 01, 2023, *Elsevier Ltd*. doi: 10.1016/j.epsr.2023.109741.

[5] H. Sabouhi, A. Doroudi, M. Fotuhi-Firuzabad, and M. Bashiri, “A novel matrix based systematic approach for vulnerability assessment,” *COMPEL - The International Journal for Computation and Mathematics in Electrical and Electronic Engineering*, vol. 40, no. 1, pp. 1–17, Feb. 2021, doi: 10.1108/COMPEL-01-2020-0031.

[6] C. Fant *et al.*, “Climate change impacts and costs to U.S. electricity transmission and distribution infrastructure,” *Energy*, vol. 195, Mar. 2020, doi: 10.1016/j.energy.2020.116899.

[7] A. Abedi, L. Gaudard, and F. Romerio, “Review of major approaches to analyze vulnerability in power system,” Mar. 01, 2019, *Elsevier Ltd*. doi: 10.1016/j.ress.2018.11.019.

[8] L. Alfonso Cárdenas Durán and L. Alejandro Arias Barragán, “RESILIENCIA Y VULNERABILIDAD DE SISTEMAS ELÉCTRICOS,” *Encuentro Internacional de Educación en Ingeniería ACOFI*, Sep. 2021.

[9] J. Beyza and J. M. Yusta, “The effects of the high penetration of renewable energies on the reliability and vulnerability of interconnected electric power systems,” *Reliab Eng Syst Saf*, vol. 215, Nov. 2021, doi: 10.1016/j.ress.2021.107881.

[10] O. S. Omogoye, K. A. Folly, and K. O. Awodele, “Review of Proactive Operational Measures for the Distribution Power System Resilience Enhancement against Hurricane Events.,” in *2021 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa, SAUPEC/RobMech/PRASA 2021*, Institute of Electrical and Electronics

Engineers Inc., Jan. 2021. doi: 10.1109/SAUPEC/RobMech/PRASA52254.2021.9377252.

[11] Y. Y. Haimes, “On the definition of vulnerabilities in measuring risks to infrastructures,” Apr. 2006. doi: 10.1111/j.1539-6924.2006.00755.x.

[12] X. Wei, S. Gao, T. Huang, T. Wang, and T. Zang, “Electrical Network Operational Vulnerability Evaluation Based on Small-World and Scale-Free Properties,” *IEEE Access*, vol. 7, pp. 181072–181082, 2019, doi: 10.1109/ACCESS.2019.2906286.

[13] T. Fu, D. Wang, X. Fan, and Q. Huang, “Component Importance and Interdependence Analysis for Transmission, Distribution and Communication Systems,” *CSEE Journal of Power and Energy Systems*, vol. 8, no. 2, pp. 488–498, Mar. 2022, doi: 10.17775/CSEEJPES.2020.05520.

[14] M. Saleh, Y. Esa, and A. Mohamed, “Applications of complex network analysis in electric power systems,” *Energies (Basel)*, vol. 11, no. 6, Jun. 2018, doi: 10.3390/en11061381.

[15] A. A. Tahirovic, D. Angeli, and G. Strbac, “A Complex Network Approach to Power System Vulnerability Analysis based on Rebalance Based Flow Centrality,” in *IEEE Power and Energy Society General Meeting*, IEEE Computer Society, 2021. doi: 10.1109/PESGM46819.2021.9638145.

[16] X. Wu, S. Li, A. Li, B. Zhou, Z. Tian, and D. Zhao, “Structural vulnerability of complex networks under multiple edge-based attacks,” in *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 405–409. doi: 10.1109/DSC.2018.00065.

[17] 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, Sep. 2023, doi: 10.1016/j.physa.2023.129072.

[18] V. Tamhane and G. Ambika, “Structure and stability of the Indian power transmission network,” *Journal of Physics: Complexity*, vol. 4, no. 2, Jun. 2023, doi: 10.1088/2632-072X/acd611.

[19] Z. Wan, X. Liu, Y. Zhang, Y. Wang, and Y. Zeng, “Research on vulnerability assessment method of electric power network based on graph neural,” in *2023 IEEE 4th China International Youth Conference on Electrical Engineering, CIYCEE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/CIYCEE59789.2023.10401565.

[20] X. Wei, S. Gao, T. Huang, T. Wang, and T. Zang, “Electrical Network Operational Vulnerability Evaluation Based on Small-World and Scale-Free Properties,” *IEEE Access*, vol. 7, pp. 181072–181082, 2019, doi: 10.1109/ACCESS.2019.2906286.

[21] L. Paredes, B. Serrano, and M. Molina, “NUEVO PARADIGMA DE LOS SISTEMAS ELÉCTRICOS: GENERACIÓN DISTRIBUIDA Y MICRORREDES ELÉCTRICAS. UN VÍNCULO DE ACCESIBILIDAD A LA ELECTRICIDAD EN AMÉRICA Y EL CARIBE.,” *ENERLAC*, pp. 4–26, 2020. [Online]. Available: www.olade.org

[22] L. Yang and J. Teh, “Review on vulnerability analysis of power distribution network,” Nov. 01, 2023, *Elsevier Ltd*. doi: 10.1016/j.epsr.2023.109741.

[23] J. Wen, S. Lin, X. Qu, and Q. Xiao, “A TOPSIS-Based Vulnerability Assessment Method of Distribution Network Considering Network Topology and Operation Status,” *IEEE Access*, vol. 11, pp. 94358–94370, 2023, doi: 10.1109/ACCESS.2023.3309188.

[24] U. Shahzad, “The concept of vulnerability and resilience in electric power systems,” *Australian Journal of Electrical and Electronics Engineering*, vol. 18, no. 3, pp. 138–145, 2021, doi: 10.1080/1448837X.2021.1943861.

[25] Y. Lu, L. Shuo, Y. Luo, P. Yang, and Y. Chen, “Vulnerability Assessment and Governance of Distribution Network Considering New Energy Integration,” in *Proceedings of 2024 IEEE 13th Data Driven Control and Learning Systems Conference, DDCLS 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1615–1620. doi: 10.1109/DDCLS61622.2024.10606611.

[26] L. Hu, X. Li, and L. Zhai, “Identification of critical nodes in power system under the influence of new energy sources,” in *Proceedings - 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 294–297. doi: 10.1109/AEMCSE51986.2021.00069.

[27] W. Xu, Y. Guo, and Y. Chen, “Deep Learning-Based Vulnerability Assessment of Distribution Grids Containing Distributed Power Sources and Electric Vehicles,” Institute of Electrical and Electronics Engineers (IEEE), Jul. 2024, pp. 1041–1046. doi: 10.1109/ccdc62350.2024.10587758.

[28] J. Huang, C. Chen, C. Sun, Y. Cao, and Y. An, “An integrated risk assessment model for the multi-perspective vulnerability of distribution networks under multi-source heterogeneous data distributions,” *International Journal of Electrical Power and Energy Systems*, vol. 153, Nov. 2023, doi: 10.1016/j.ijepes.2023.109397.

[29] D. S. García Miranda and W. A. Riaño Maldonado, *Transmisión y distribución de energía eléctrica (Tomo I)*, vol. Primera Edición. Editorial Universidad Distrital Francisco José de Caldas, 2019.

[30] R. Rocchetta, “Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics,” *Renewable and Sustainable Energy Reviews*, vol. 159, May 2022, doi: 10.1016/j.rser.2022.112185.

[31] A. Abedi, L. Gaudard, and F. Romerio, “Review of major approaches to analyze vulnerability in power system,” Mar. 01, 2019, *Elsevier Ltd*. doi: 10.1016/j.ress.2018.11.019.

[32] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, “Methodologies and applications for critical infrastructure protection: State-of-the-art,” *Energy Policy*, vol. 39, no. 10, pp. 6100–6119, Oct. 2011, doi: 10.1016/j.enpol.2011.07.010.

[33] Z. Wang, A. Scaglione, and R. J. Thomas, “Electrical Centrality Measures for Electric Power Grid Vulnerability Analysis,” in *49th IEEE Conference on Decision and Control (CDC) DOI: 10.1109/CDC.2010.5717341.*, IEEE, 2010, pp. 5792–5797.

[34] Mohamed E. El-Hawary, *Electrical Power Systems Design and Analysis*. IEEE Press, 1995.

[35] A. Fichera, A. Pluchino, and R. Volpe, “A multi-layer agent-based model for the analysis of energy distribution networks in urban areas,” *Physica A: Statistical Mechanics and its Applications*, vol. 508, pp. 710–725, Oct. 2018, doi: 10.1016/j.physa.2018.05.124.

[36] R. Espejo, S. Lumbreras, and A. Ramos, “Analysis of transmission-power-grid topology and scalability, the European case study,” *Physica A: Statistical Mechanics and its Applications*, vol. 509, pp. 383–395, Nov. 2018, doi: 10.1016/j.physa.2018.06.019.

[37] A.-L. Barabási and R. Albert, “Emergence of Scaling in Random Networks Downloaded from,” 1995. [Online]. Available: www.sciencemag.orghttp://science.sciencemag.org/

[38] A. R., J. H., and B. A.-L., “Error and attack tolerance of complex networks,” *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[39] L. Thurner *et al.*, “pandapower - an Open Source Python Tool for Convenient Modeling, Analysis and Optimization of Electric Power Systems,” Sep. 2017, doi: 10.1109/TPWRS.2018.2829021.