

**LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN
UN MODELO MARKOVIANO**

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

**CARRERA:
INGENIERÍA ELÉCTRICA**

**Trabajo de titulación previo a la obtención del título de
INGENIERO ELÉCTRICO**

**TEMA:
LOCALIZACIÓN DE FALLAS EN MICRONEDES ELÉCTRICAS BASADO EN
UN MODELO MARKOVIANO**

**AUTOR:
JOSÉ LUIS MOREJÓN BASTIDAS**

**DIRECTOR:
LEONY ORTIZ MATOS**

Quito, Julio del 2018

JOSÉ LUIS MOREJÓN BASTIDAS

LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN UN MODELO MARKOVIANO

Universidad Politécnica Salesiana, Quito – Ecuador 2018
Ingeniería Eléctrica

Breve reseña de autores e información de contacto.



José Luis Morejón Bastidas (Y'1991-M11). Realizo sus estudios secundarios en el Colegio Técnico Salesiano San Rafael de la ciudad de Esmeraldas, Bachiller con la especialidad Técnico Industrial, Especialización Instalaciones, Equipos y Maquinas Eléctricas. Egresad de Ingeniería Eléctrica de la Universidad Politécnica Salesiana. Su trabajo se basa Localización de fallas en Micro-redes Eléctricas basado en un modelo Markoviano.

jmorejonb@est.eps.edu.ec

Dirigido por:



Leony Ortiz Matos (Y'1982). Recibió el título de MSc. e Ingeniería en Automática por el Instituto Superior Politécnico Julio Antonio Mella (ISPJAM) de la Universidad de Oriente, Cuba. Actualmente se encuentra estudiando para obtener su título de Doctor en Ingeniería en la Universidad Pontificia Bolivariana-Colombia-Medellín, es miembro del Grupo de Investigación en Redes Eléctricas Inteligentes (GIREI). Forma parte del equipo académico de la carrera de

Ingeniería Eléctrica de Universidad Politécnica Salesiana Quito-Ecuador. Sus principales intereses de investigación Automatización y Control, Control robusto y Control Tolerante a Fallos, Micro-redes Eléctricas Inteligentes híbrida, CA/CC. lortizm@ups.edu.ec

Todos los derechos reservados:

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con la autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos o investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS

©2018 Universidad Politécnica Salesiana
QUITO - ECUADOR

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR/A

Yo, Leony Ortiz Matos declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación ***LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN UN MODELO MARKOVIANO*** realizado por José Luis Morejón Bastidas, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, Julio del 2018



.....

Leony Ortiz Matos

Cédula de identidad: 175423038

CESIÓN DE DERECHOS DE AUTOR

Yo, José Luis Morejón Bastidas, con documento de identificación N°0803478486, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor/es del trabajo de grado/titulación intitulado: “**LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN UN MODELO MARKOVIANO**”, mismo que ha sido desarrollado para optar por el título de: Ingeniero Eléctrico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Firma



.....

Nombre: José Luis Morejón Bastidas

Cédula: 0803478486

Fecha: Quito, Julio del 2018

ÍNDICE GENERAL

Resumen	1
Abstract	1
1.Introducción	2
2.Infraestructura de una Micro-red Inteligente	3
3.Modos de fallas en la Micro-red.	5
3.1.Fallas en líneas y cables	5
3.2.Paneles fotovoltaicos.....	5
3.3.Turbinas eólicas	6
3.4.Fallas en generadores	6
3.5.Fallas en sensores y actuadores.....	7
3.6.Fallas en sistemas de control.....	7
3.7.Fallas por ciberataques.....	8
4.Detección y localización de fallas.....	9
5.Propagación de fallas	11
5.1 Modelos de la propagación de fallas.....	11
5.2.Procesos de Markov	13
6.Formulación del Problema	13
6.1.Propagación de falla en cascada.....	16
6.2.Modelo de Markov	16
6.3.Modelo Propuesto	18
7.Caso de Estudio.....	21
8.Trabajos futuros	22
9.Conclusiones	23
10.Referencias.....	23
10.1.Estado del Arte.....	27
11.Anexos	32

ÍNDICE DE FIGURAS

Figura 1.Evento de falla en cascada típico.....	3
Figura 2: Árbol de dependencias físicas y lógicas de la Micro-red.	4
Figura 3: Árbol de falla de la Micro-red	12
Figura 4. Espectro de impedancia de dos buses cerca de la ubicación de falla simétrica	14
Figura 5.Diagrama de resultado general de los Subsistemas.	19
Figura 6.Diagrama de matriz de transmisión de subsistema Fotovoltaica.....	20
Figura 7.Matriz de calor Fotovoltaica.....	20
Figura 8.Diagrama de matriz de transmisión de subsistema de Turbina Eólica	21
Figura 9.Matriz de calor Turbina Eólica	21
Figura 10.Diagrama de matriz de transmisión de subsistema-Sistema de Control.....	21
Figura 11.Matriz de calor Sistema de Control	21
Figura 12.Caso Benchmark Hachinohe Project del proyecto NIDO en Japón	22
Figura 13.Matriz de Calor.	22
Figura 14.Temática-Indicador de la Matriz del Estado de Arte.....	30
Figura 15.Formulación del Problema-Indicador de la Matriz del Estado del Arte.....	30
Figura 16.Solución-Indicador de la Matriz del Estado de Arte	31

ÍNDICE DE TABLAS

Tabla 1:Variables	14
Tabla 2:Variables del Algoritmo.....	14
Tabla 3.Tasas de falla por componente de la Micro-red.....	16
Tabla 4.Componentes-Modos de Falla-Causas y Efectos.....	32
Tabla 5.Clasificación de Modos de Falla.....	37

LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN UN MODELO MARKOVIANO

Resumen

El presente trabajo analiza el efecto producido por la aparición de un estado o evento de fallo sobre el sistema y su entorno, componente o estructura de control usando un modelo Markoviano, y a partir del resultado de algoritmos de localización de fallas o FDIs para Micro-redes Eléctrica. El método ayudará a comprender la propagación de fallas y su efecto en las Micro-redes, permitiendo además identificar y localizar las fallas importantes a tratar y controlar con técnicas de tolerancia a fallas.

Este método no solo implementa un algoritmo de localización de falla, además logra un esquema para analizar la propagación de las fallas que se presentan en Micro-redes (MG). Para el caso propuesto, la localización de la falla, la detección de los puntos críticos en los que puede ocurrir una falla, así como la determinación de la ruta más probable para la propagación de las mismas, son considerados como un punto clave a resolver.

Es importante considerar que, para que el proceso de Markov obtenga resultados cercanos a la realidad es necesario considerar no solo un modelo que simule el comportamiento dinámico del sistema, también, contar con estudios más profundos que brinden datos estadísticos y probabilísticos de los eventos de fallos, su propagación, y toma de decisiones una vez que estos son localizados.

Palabras Clave: Micro-red (MG) inteligentes, localización de fallas, análisis de propagación, generación distribuida, modelos de Markov.

Abstract

The present paper analyzes the effect produced by the appearance of a state or failure event on the system and its environment, component or control structure from the result of algorithms of fault location or FDIs for Electric Microgrids, using a Markovian model. This method will help to understand the propagation of faults and their effect on the Microgrids, in addition to allowing the identification and location of the important faults and its control with fault tolerance techniques.

This method not only implements a fault location algorithm, it also achieves a scheme to analyze the fault propagation that occur in Microgrids (MG). For this case, fault locations, the detection of critical points in which a failure can occur, as well as the determination of the most probable route for its propagation, are considered the aim to be resolved. The model was created using the Markov process.

It is important to consider that in order for the Markov process to obtain results close to reality, it is necessary to consider not only a model that simulates the dynamic behavior of the system, but also to have more in-depth studies that provide statistical and probabilistic data on failure events, their propagation and decision making once located.

Keywords: Smart Micro-grids, fault locations, propagation analysis, distributed generation, Markov models.

1. Introducción

Las redes eléctricas sufren eventos de falla que provocan pérdidas económicas y que grupos poblacionales se queden sin energía durante tiempos considerables. Los eventos de falla empiezan con una anomalía en la red, lo que puede provocar desperfectos en cascada de los componentes clave de la red, en el caso de MG pueden estar involucradas líneas de distribución, cargas y generadores [1][2]. Por aportes estadísticos se sabe que tales eventos se presentan con cierta regularidad, afectando a millones de personas. Los eventos de falla iniciales pueden ser causados por múltiples razones, incluyendo fenómenos naturales inevitables o fallas humanas, por lo cual se vuelve fundamental el análisis de la propagación de fallas, sabiendo que una red es heterogénea en sus componentes sin importar su tamaño [1].

En este caso, es necesario estudiar a profundidad una característica de cualquier red eléctrica por pequeña (micro-red) o grande (sistemas de potencia) que sea en infraestructura, la interdependencia. Una red es interdependiente porque cuando se presenta cierto evento de falla en una red, las demás partes del sistema también pueden resultar afectadas. También puede referirse a aquellos elementos en los que el comportamiento de un sistema influencia en otros [2].

La interdependencia influye negativamente en la confiabilidad de sistemas críticos, por ejemplo, las redes eléctricas y puede dar lugar a eventos de falla en cascada. Un evento de esta naturaleza puede iniciar como la falla de una de las líneas de distribución, pero puede provocar que líneas y sistemas de generación estén en estado de falla. En este caso es crucial poder hacer un pronóstico de la propagación de fallas

para el diseño y planificación adecuada de nuevos sistemas, habiendo para ello diversos modelos que se han estudiado alrededor del mundo [2].

Las Micro-redes (MG) son un tema de alto interés debido a su potencial para lograr una infraestructura eléctrica confiable. El enfoque de los estudios incluye ser un medio de contingencia durante eventos catastróficos, debido a la habilidad de una MG para ser funcional tanto conectada a la red principal como en forma de isla independiente con sus propias fuentes de energía limpia de generación distribuida (DG) [1].

En una Micro-red inteligente, cada carga y generador deberá poder ser controlado, por tanto, cada actor de la red deberá participar activamente en un ambiente desregulado donde los usuarios finales puedan participar en el comercio de la energía, recibiendo y entregando energía según su necesidad [3].

Esta clase de redes han tenido un gran impacto en las redes eléctricas debido al cambio del sentido de flujo al tipo bidireccional. Se produce un cambio en la coordinación de protecciones eléctricas dependiente de la cantidad de DG instalada. Esto implica impactos significativo a la confiabilidad de los sistemas [3].

Una MG es una red eléctrica de bajo voltaje que está conectada a otras MGs y/o a la red principal por medio de un único punto de conexión [3]. En una MG cada actor puede tomar acciones para el abastecimiento de potencia reactiva, para control de voltaje, control de la frecuencia de la red, así también puede intervenir en la mejora de la calidad de la energía; al mismo tiempo tiene como efecto negativo, aumento de capacidad de corriente de falla [3], [4].

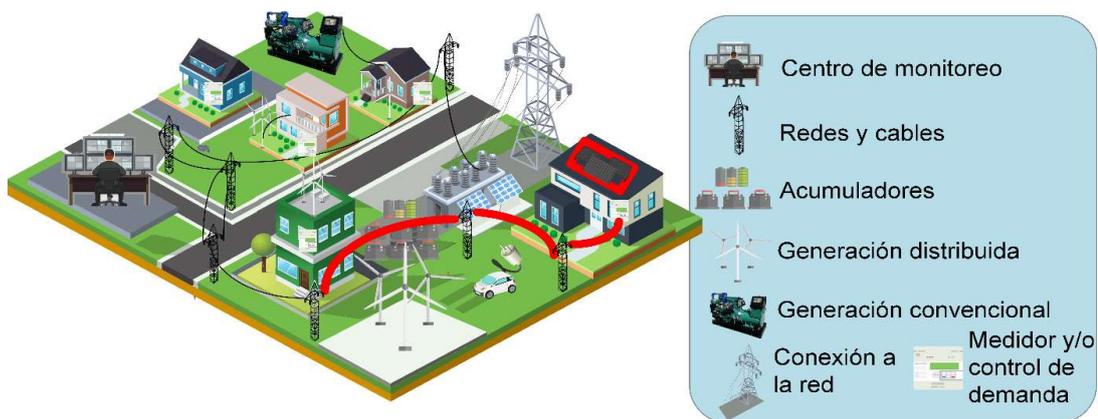


Figura 1.Evento de falla en cascada típico.

Como se puede notar en la figura 1, se muestran los componentes típicos de este sistema, en este caso los componentes señalados en rojo son los que pueden estar en estado de falla o que se vieron afectados por una propagación de falla [1]. Es importante destacar que para cumplir con el funcionamiento de la red inteligente interactúan diversos equipos incluyendo controladores automáticos de generación (AGC) para los sistemas de generación, unidades de medición fasorial (PMU) para las subestaciones y el sistema de transmisión, también son importantes los medidores inteligentes (SM) para sistemas de distribución [1].

En el proyecto se propone un análisis estocástico para la propagación de fallas mediante Markov, evaluar la severidad del efecto final de cada fallo en componentes y estructuras, y la localización de las mismas en Micro-redes. Además, el trabajo permitiría identificar las fallas importantes a tratar con técnicas de tolerancia a fallas.

Además, se propuso obtener mediante la interconexión, la descripción de los efectos de las fallas en los componentes y, el probable efecto final del evento de

fallas para los sistemas de control de la Micro-red eléctrica.

En adelante este artículo se organiza de la siguiente manera, en la sección 2 se establecen todos los aspectos relacionados a la infraestructura de una Micro-red inteligente. En la sección 3 se describen los modos de falla de los componentes de la Micro-red, inclusive sistemas cibernéticos. En la sección 4 se presentan los modelos empleados para el estudio de la propagación de fallas. La sección 5 se encarga de establecer la formulación del problema en estudio, considerando las fallas en cascada y la modelación por medio de cadenas de Markov. Finalmente se presentan las conclusiones de este artículo en la sección 6. Los anexos muestran otros aportes relevantes a la propagación de fallas en Micro-redes.

2. Infraestructura de una Micro-red Inteligente

Una Micro-red (MG) inteligente posee varios componentes que permiten su funcionamiento autónomo o acoplado a una red eléctrica. Se la puede dividir en elementos de generación de pequeña potencia que pueden ser sistemas fotovoltaicos o turbinas eólicas, así

también generadores térmicos no renovables. Los generadores renovables contarán con sistemas de acoplamiento a

la red por ejemplo inversores trifásicos y reguladores [5]–[9].

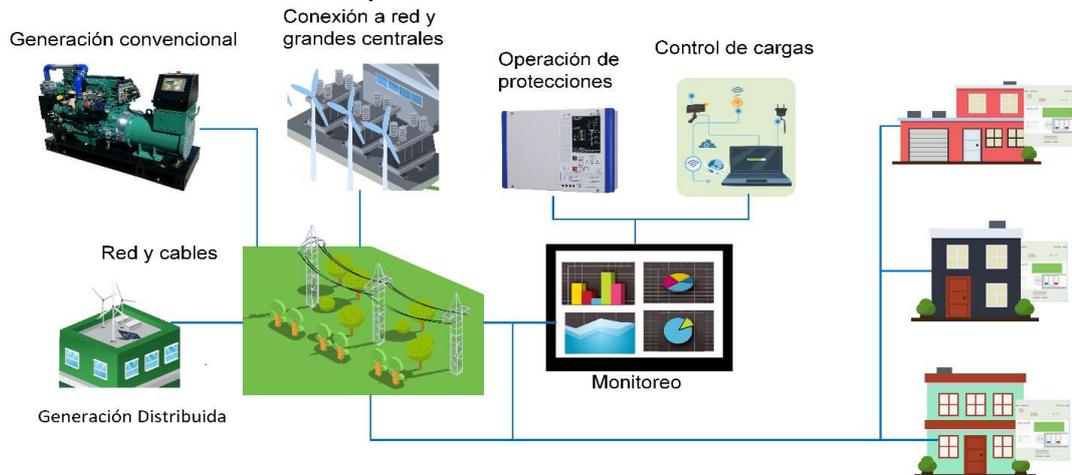


Figura 2: Árbol de dependencias físicas y lógicas de la Micro-red.

Los generadores permitirán alimentar directamente a las cargas normalmente de tipo residencial, y cuya alimentación se podrá controlar. Así mismo es fundamental la existencia de elementos de protección que permitan la circulación de dos sentidos de flujo de la energía eléctrica.

Estas protecciones por su naturaleza se conocen como protección adaptativa [7], [10]. Otro punto a considerar como parte de la infraestructura de la MG son medios de almacenamiento de la energía inmediatos, de tal forma que, en ausencia de generación, la mayor cantidad de cargas puedan continuar siendo alimentadas durante el tiempo en que no es posible contar con los elementos de generación.

Otro punto a considerar como parte de la infraestructura son medios de almacenamiento de la energía inmediatos, de tal forma que, en ausencia de generación, la mayor cantidad de cargas puedan continuar siendo alimentadas. El almacenamiento normalmente es una combinación de

bancos de baterías y supercapacitores [11].

Se debe contar con elementos electrónicos que permitan el acoplamiento a la red eléctrica en un punto de acoplamiento común (PCC) o la desconexión según se requiera. El elemento de acoplamiento es un transformador elevador de tensión con sus respectivas protecciones correctamente dimensionadas [5], [7], [12], [13]

A ello se le debe añadir la necesidad de un sistema complejo de monitoreo y control que permita mantener la estabilidad del sistema y asegurarse que se satisface a la demanda en cada instante de tiempo; por tanto, se deben monitorear todos los elementos de la Micro-red (MG), considerando parámetros adecuados para cada tipo de elemento, incluyendo el nivel de carga de las baterías [7], [14]. La infraestructura de una Micro-red (MG) inteligente con ejemplos de sus componentes se puede observar en la **Figura 2**.

3. Modos de fallas en la Micro-red.

Considerando que una Micro-red (MG) va a funcionar tanto conectada a la red como en modo de isla, los modos de falla existentes son diferentes y deben ser estudiados a profundidad para poder obtener una simulación adecuada de la propagación de falla en los mismos. En este caso los sistemas de microgeneración se conectan hacia la red con sistemas electrónicos de baja potencia, lo que supone que el aporte de tales elementos a la red sea muy bajo y se considere un serio problema [15]. Así mismo los sistemas de almacenamiento son vitales para el funcionamiento en ambos modos antes mencionados. Los sistemas de baterías permiten el cambio de modo de operación de isla a una resincronización a la red y viceversa [16].

En el modo de operación conectado a la red, la corriente de falla tendrá valores elevados que impliquen la activación de fusibles e interruptores, pero esto no ocurrirá en modo aislado, ya que los elementos electrónicos de potencia normalmente tendrán una potencia nominal muy por debajo de la manejada por la red principal [16].

Los modos de falla de una Micro-red según [7] se podrían dividir en función del elemento en el cual ocurre una falla. Es decir, se dividirán en fallas en cables y líneas de transmisión, fallas en sistemas fotovoltaicos y fallas en turbinas eólicas, así como generación convencional.

También pueden ocurrir fallas en elementos de monitoreo. En el anexo 2, se desarrolla además una caracterización y clasificación de las diferentes fallas atendiendo: fallas objetivas, según sus límites, causas fenomenológicas, los

estados de creación u ocurrencia, y persistencia [17]. De cada tipo de elemento serán analizadas las causas de las fallas más comunes y los principales efectos que existirán en la Micro-red (MG) y en los elementos.

3.1. Fallas en líneas y cables

En los sistemas eléctricos de distribución no solo toca analizar las pérdidas asociadas a las líneas de distribución [18]. Estos son los elementos de interconexión entre generadores y cargas y que forman la Micro-red (MG) unificada. Las líneas pueden ser aéreas o soterradas.

Ambos tipos de línea están sujetas a fallas mecánicas y a eventos naturales que pueden provocar fallas como cortocircuitos, sobrecargas, fallas de equipamientos [12][9].

Las causas más comunes de los eventos de falla incluyen descargas atmosféricas, contacto con árboles o animales, fallas humanas y de operación, falta de mantenimiento por nombrar otras [7], [13].

Las fallas más comunes son cortocircuitos línea a tierra, línea-línea, línea-línea a tierra y trifásicos. Todos ellos implican la conexión accidental en un único punto de una o varias líneas, lo que provoca reducciones de la voltaje e incrementos significativos de la corriente circulante. Otro efecto es el disparo de las protecciones de los circuitos, inclusive en puntos lejanos al de ocurrencia de la falla [7], [12], [13].

3.2. Paneles fotovoltaicos

Elementos que debido al efecto fotovoltaico son capaces de generar energía eléctrica debido a la energía solar renovable. Las fallas asociadas a los paneles son de sus celdas, módulos de conversión y de diodos bypass. Las fallas

de celda se originan por degradación de los materiales o falta de mantenimiento y de limpieza. Las celdas pueden generar circuitos abiertos o cortocircuitos, así como puntos calientes debido a la corrosión o un estrés mecánico, así como por efectos naturales [7], [14].

Las fallas de los módulos pueden darse por defectos de fabricación estrés mecánico, quebraduras de cristal, pérdida de resistencia y otros asociados. Los efectos asociados a estas fallas incluyen circuitos abiertos y cortocircuitos. Por otro lado, las fallas de diodos de derivación ocurren por sobrecalentamiento, que origina una pérdida gradual de la potencia de salida de los paneles solares. Las consecuencias mayores son distorsiones de las ondas de corriente y de tensión en todo el circuito de la Micro-red (MG) [7], [14], [19].

3.3. Turbinas eólicas

Son aquellos elementos que aprovechan la energía del viento para generar electricidad. Sus fallas están asociadas a defectos de varias sub elementos, incluyendo la caja de cambios y cojinetes, los sistemas de control eléctricos y electrónicos, del generador eléctrico y fallas de rotores, aspas y elementos hidráulicos. Las fallas más comunes son las de cojinetes y cajas de cambios, se deben a la corrosión y a defectos mecánicos que dan lugar a la pérdida de eficiencia [7], [12], [13].

Las fallas en el generador son causadas por defectos de cojinetes, estator, rotor lo que conlleva la existencia de ondas armónicas destructivas, reducción en la eficiencia, un decremento del torque promedio y excesivas pérdidas calóricas de los devanados. Las fallas de los elementos semiconductores son el origen

de problemas en los elementos electrónicos de control. Estas fallas ocurren debido a circuitos abiertos y a cortocircuitos, así como fallas en circuitos de disparo [7], [12], [13].

Así mismo, la corrosión y estrés mecánico que ocurren debido a causas naturales como congelamiento, descargas atmosféricas y otros. Esto implica que las aspas tengan asperezas y malformaciones, así como cambios de rigidez y reducciones de la eficiencia. Las fallas de los elementos hidráulicos de control se pueden deber a pérdidas de fluido o a contaminación por aire de tubos y cañerías por fugas. Esto implica fallas de piezas mecánicas como aspas y cojinetes. Todos estos problemas originan cambios en formas de onda de corriente y voltaje para toda la MG [7], [12], [13].

3.4. Fallas en generadores

En una Micro-red también existen generadores convencionales que están sujetos a fallar, y normalmente son elementos de respaldo para mantener la operación del sistema y el abastecimiento de la demanda. Este tipo de generador está sujeto a fugas de combustible, fallas en cojinetes y agrietamiento de piezas mecánicas por ejemplo cigüeñales. Normalmente se originan por la corrosión y defectos de fabricación, así como por falta de mantenimiento. El principal efecto de los problemas mencionados es la inhabilidad de rotación de la máquina. Las fugas de combustible llevan a pérdidas de eficiencia de la combustión [5], [7], [22], [23].

Por otro lado, al igual que en los generadores de un sistema eólico, el generador está sujeto a fallas de cojinetes, rotor, estator y devanados; debidas a efectos eléctricos como circuitos abiertos

y cortos, así como efectos mecánicos como pérdida de la excentricidad. Los efectos incluyen sobrecalentamiento, desbalances de voltaje y corriente, cambios de formas de onda de voltaje y corriente y cambios en los flujos circulantes, afectando a la Micro-red(MG) en general [7], [22], [23].

3.5. Fallas en sensores y actuadores

Las Micro-redes (MG) tienen diversos sensores, pero los más importantes son aquellas que se encargan de la medición de voltaje y corriente, debido a que son aquellos que permiten un seguimiento óptimo del equilibrio entre potencia generada y consumida, un desbalance en este sentido puede causar la existencia de importantes señales transientes. Los sensores son transformadores de potencial (PT) y transformadores de corriente (CT). Los errores de esta clase de transformadores normalmente se miden en función de error de magnitud, error de fase y error de armónico. Estos serán los modos de falla de los sensores principales de la red [24].

Existen modos de fallas de sensores y de actuadores que no son posibles de evadir, y que pueden ser originadas por diversos agentes, tanto internos como externos. Tales fallas pueden provocar grandes cambios en la estructura y el rendimiento de toda la red. La propagación de fallas a sistemas de actuación y de sensado complica el panorama ya que se requiere de un sistema robusto que pueda detectar ambos modos de falla, lo que se agrava si el sistema de control está sometido a un ataque externo [25].

Los modos de falla que se pueden presentar en un sensor son:

Salida sesgada: es decir que el sensor muestra una medición que contiene un

cierto nivel de offset, es decir no muestra todo el espectro de medición posible, sin poder alcanzar niveles mínimos de medición, que pueden ser los necesarios para detectar un fallo superior [25].

Salida fija: Aquella en la que el sensor entra en estado en el que únicamente muestra uno o dos estados, también conocido como todo o nada, y se lo considera una falla abrupta [25].

Sensor sin salida: Es aquel estado en que en la salida no existe una señal, puede ocurrir por falta de señal de alimentación al sistema de sensado, ausencia de la señal de entrada e inclusive una falla general del sensor [25].

3.6. Fallas en sistemas de control

Es importante mencionar que los sistemas de control al igual que los sistemas de adquisición de datos también están sujetos a fallas, esto es crítico ya que los lazos de realimentación con el equipo que controla el sistema en falla pueden dar lugar a sistemas sobrecargados, e incluso por encima de sus características nominales, el origen de las fallas puede ser por fallas en las comunicaciones, pérdida de señal, de un canal de comunicación, una mala operación del controlador o una combinación de tales causas.

Esto puede causar que la frecuencia de la Micro-red se desbalancea y no se encuentre dentro de la banda aceptable de operación [26]. Otro sistema que está sujeto a fallas es el que lleva a cabo el control de las máquinas de generación, donde puede ocurrir una apertura o cierre inadecuado de los interruptores de conexión a la Micro-red, las fallas en este caso son las siguientes [27]:

- Cortocircuito de vínculo DC a tierra.
- Cortocircuito de banco de capacitores DC.
- Circuito abierto en interruptor de conexión.
- Cortocircuito en interruptor.
- Cortocircuito bifásico en terminales de conexión de la máquina.
- Cortocircuito de línea a tierra de terminal de conexión de máquina.

3.7. Fallas por ciberataques

La operación normal de una Micro-red (MG) es seriamente amenazada por ciberataques informáticos que afectan la infraestructura de comunicación entre sensores, actuadores y sistemas de monitoreo. La ocurrencia de estos eventos se debe a atacantes que emplean técnicas como negación de servicio (DoS), ataques randómicos y ataques de inyección de datos falsos [28].

Las consecuencias de estos ataques pueden ser similares o peores a fallas en los componentes físicos del sistema, debido a la importancia de un sistema inteligente ciber físico (CPS) en la MG. El riesgo es mayor si el control tiene inteligencia embebida.

En estos sistemas los componentes virtuales y físicos deben trabajar en una estrecha coordinación que provee mejores capacidades y estabilidad al sistema debido a la existencia de comunicaciones de dos vías entre los componentes físicos (sensores y actuadores) y el sistema de control [28].

Una forma de estimar la existencia de falla o ataque consiste en la comparación de los valores medidos y los valores que se estiman y son esperados, si el error es muy grande puede ser una señal de la

existencia de fallas o ataques, sin embargo, si el atacante conoce ciertos parámetros del sistema podría superar este control. Un ataque cibernético se caracteriza por cambios en las magnitudes de corriente, voltaje o de fase, los modos de falla típicos son [28]:

Ataque DoS: Esta es una forma de ataque en la que el atacante hace que uno o varios componentes del sistema de control no sean accesibles. El ataque se puede causar si se bloquean los canales de comunicación, también llenando de paquetes a la red o evitando que los equipos soporten la transferencia de datos. Los ataques se pueden dar en datos de sensado y datos de control.

Ataque randómico: Este ataque normalmente es ejecutado de tal forma que el sistema central no lo pueda identificar, y consiste en la manipulación de las lecturas de los elementos de sensado. Los ataques se pueden presentar en cualquier instante de tiempo t , y pueden ser de larga duración o de una ínfima duración.

Ataque bajo alteraciones de lectura de sensor acotadas (ABSRA): En este caso los datos son manipulados de tal forma que el operador o los encargados de monitoreo de la red crean que existe alguna falla y ejecuten alguna acción para contrarrestar tal malfuncionamiento provocando un fallo aún mayor en la Micro-red (MG). Así mismo puede ocurrir que el atacante lleve al sistema a un estado indeseable mientras envía datos de operación segura al supervisor [29].

Ataque de inyección de datos falsos: En este caso el atacante conoce ciertos parámetros de funcionamiento de la Micro-red (MG) incluyendo la ganancia y otras magnitudes clave, de esta forma puede controlar a un cierto subsistema de

sensores, causando que el sistema no identifique el ataque y llevando a operar el sistema en valores por encima de lo nominal lo que puede causar una propagación de la falla a todo el sistema en conjunto. Un atacante normalmente puede tomar, grabar y manipular de acuerdo a su mejor conveniencia, mediante una observación previa [28], [30], [31].

El autor de [32] establece que un ciberataque muy peligroso es aquel que puede ser infringido al sistema de control de la frecuencia de carga (LFC) de la red inteligente por la naturaleza propia de cambio constante de magnitud de la carga conectada.

En este caso el atacante conoce que un cambio en la carga produce un incremento o decremento de la frecuencia de operación de los elementos de generación. Los cambios en la frecuencia provocan inestabilidad en la red. Un cambio en la frecuencia que esté por debajo o encima de los niveles aceptables provocará que el subsistema de control de los generadores haga cambios en la operación de la máquina motriz para compensar tal cambio, aunque sea provocado por un ciberataque.

Los modos de falla son un ataque con un sesgo positivo o un ataque con un sesgo negativo, que puede ser mayor si se ataca directamente al control automático de generación (AGC) [32]

4. Detección y localización de fallas

El problema de localización de fallas en Micro-redes eléctricas no es un problema sencillo. A lo largo de la historia muchos investigadores realizaron importantes aportes en el área mencionada, la

literatura se concentra en los sistemas de transmisión donde debido a las características de las líneas, la posibilidad de ejecución de mediciones y colocación de nuevo equipamiento, permiten localizar la zona de falla con una alta precisión [33]–[40].

Por otro lado, la localización de fallas en sistemas de distribución de Micro-redes es más compleja debido a las características topológicas del sistema, las características de las cargas, el desbalance del sistema y la carga; también la conexión/desconexión de la GD que provoca un mayor índice de fallas y dificulta considerablemente la localización de eventos anómalos.

$$v(j\omega_{sw}) = V \angle \alpha \quad (1)$$

$$i(j\omega_{sw}) = I \angle \beta \quad (2)$$

La ecuación (1) y (2) es la amplitud y la fase de la forma de onda del voltaje y de la corriente, respectivamente. La frecuencia (f_{sw}) apunta a la frecuencia de conmutación del H-bridge [33].

Otro trabajo interesante en este ámbito se muestra en [38], donde los autores realizan la ubicación de fallas equivalente a la micro-red. El algoritmo se pone a prueba mediante simulaciones y considerando la existencia de diferentes tipos de fallas de derivación en topologías radiales y anilladas. Las simulaciones se ejecutan en dos modos de operación: interconectada a la red principal y aislada.

$$E_{V1} = V_1 + I_{V1} * Z_{V1} \quad (3)$$

La ecuación, V_1 e I_{V1} son el voltaje y la corriente medidos por el valor de PMU1,

Z_{V1} es la impedancia equivalente, E_{V1} es la potencia equivalente[33].

En [39], está propuesto un algoritmo que posibilita la detección de fallas en Micro-redes. El objetivo es distinguir entre los eventos que son perturbaciones y los que no constituyen fallas. Tal distinción se realiza transformando a través de Wavelet y aproximaciones de vector de Park las señales de corriente o tensión trifásicas en componentes dq0, para analizar el comportamiento durante las fallas y reconociendo patrones que se dan al inicio de los eventos de falla.

$$\begin{pmatrix} Va \\ Vb \\ Vc \end{pmatrix} = \begin{pmatrix} v_{ma} \cos(wt) + f_a(t) \\ v_{mb} \cos\left(wt - \frac{2\pi}{3}\right) + f_b(t) \\ v_{mc} \cos\left(wt + \frac{2\pi}{3}\right) + f_c(t) \end{pmatrix} \quad (4)$$

La ecuación (4) donde $f_a(t)$, $f_b(t)$ y $f_c(t)$ representan el transitorio electromagnético en la señal.

En [40] Alwala la idea principal es la utilización de un sistema de agente múltiple (MAS) para la ubicación y aislamiento de fallas. El algoritmo emplea las corrientes de secuencia para determinar el tipo de falla y posteriormente determina la ubicación en función de las corrientes de retorno. Mediante este método los autores se proponen el aislamiento de fallas para una Micro-red inteligente con Generación distribuida ubicadas en varias zonas del caso de estudio que se basa en la red IEEE de 37 barras con modificaciones.

Es importante recalcar trabajos como el de Goudarzi y otros autores, que proponen un enfoque novedoso para localizar fallas basado en transformadas de Wavelet. Este trabajo fue desarrollado para localizar fallas en redes de distribución desequilibradas y gran

tamaño. En el trabajo se propone la utilización de formas de onda transitorias de voltaje en sistemas de distribución. El sistema se pone a prueba en una red de 34 barras desequilibrado y que contiene dos unidades de generación distribuidas [35].

Uno de los grandes problemas de los métodos de falla aplicados a la micro-red es la alta ineficiencia cuando la corriente de falla tiene magnitud ínfima, para hacer frente a tal hecho en [41] se emplea en cada barra en el dominio de la frecuencia, cada carga no lineal se considera una fuente de corriente asociada a la reactancia armónica, detectando según tales autores diversos tipos de fallas puestas a prueba en una red de tipo IEEE con 14 buses con 5 unidades GD.

EL uso de unidades de medición sincrofásorial (PMU) colocados en los puntos extremos de la micro-red es la propuesta de los autores de [42], la medición de tensión y corriente se ejecuta en tales unidades para calcular la impedancia de falla resultante. A través de métodos de decisión distribuida que consideran las variaciones de la impedancia antes y después de las barras del sistema, es posible determinar la ubicación de las fallas y sus orígenes, considerando igualmente importante que una PMU se haya comunicada con otra que se encuentra alejada. En este caso las simulaciones se ejecutaron en Simulink para comprobar la efectividad del algoritmo en una micro-red con 14 barras.

La localización de fallas en micro-redes que operan con corriente continua es abordado por Mohanty y Pradhan [43] usando la técnica de inyección de corriente. En este caso toma especial relevancia el punto de conexión del kit de inyección consistente de capacitancia, inductancia, batería e interruptores; así se

logra inyectar corriente para que circule por el camino que está en falla durante un período corto de tiempo, en este caso las simulaciones se ejecutan variando la distancia y la impedancia de falla.

5. Propagación de fallas

La propagación de fallas ocurre debido a las interdependencias, una característica típica de cualquier sistema eléctrico. La propagación de fallas debe ser predicha, de tal forma de poder anticiparla o de encontrar los puntos críticos que podrían provocar una propagación que implique que la confiabilidad de toda la red esté comprometida.

Para ello es fundamental reseñar los modelos que se emplean para modelar el comportamiento de la propagación de fallas, así también de las técnicas involucradas para el análisis del estado siguiente que tendrá un sistema en el tiempo incluyendo los procesos de Markov y las matrices de transición involucradas.

Para el análisis de las fallas se puede considerar la MG como un árbol en el cual como se muestra en la **Figura 3** existen interdependencias, notando dependencias físicas y lógicas que provocan la propagación de una falla. La red conectada y el sistema de líneas son fundamentales porque permiten la conexión de cargas y generadores entre sí.

La ubicación de fallas es un uso importante entre lo que podemos utilizar para la realización de las Micro-redes (MG). Los datos recopilados de varios componentes, subsistemas y efectos, podrían utilizarse para enfoques inteligentes a la localización de fallas en sistemas de una Micro-red. En lo cual se

podría tener una mayor probabilidad de localización de fallas en Micro-redes (Tabla 4).

Como observamos en la tabla se analiza los enfoques sobre los componentes, modos de fallas causas y efectos que existentes y las tendencias futuras en los métodos de localización de fallas en una Micro-red (MG).

En lo que es la parte del anexo sobre el estudio de las fallas según sus clasificaciones podemos analizar según su objetivo tendremos las fallas maliciosas y fallas no maliciosas (Tabla 4). De igual se tiene según los límites del sistema, como fallas externas y fallas internas. Aparte de estas clasificaciones también se tienen causa fenomenológica en lo cual tenemos fallas naturales, fallas por causas humanas.

5.1 Modelos de la propagación de fallas

En [44] por ejemplo, se considera al evento de falla inicial como un árbol de rutas, tal primer árbol generará que otros sistemas resulten afectados como consecuencia de la propagación de la falla, sabiendo que la cascada puede ser ilimitada, y que en cada instante de tiempo se aumentará la cantidad de dispositivos que estén en estado de falla.

El árbol de una Micro-red, notando que las compuertas OR representan que, si cualquiera de los sistemas falla, el sistema entra en falla, mientras que en una compuerta AND, todos los sistemas deben fallar para que el sistema esté en falla. Para que las cargas estén en estado de falla, se establece que, ningún subsistema de generación y protección esté en funcionamiento.

El árbol de falla que se formará en una Micro-red se puede observar en la **Figura 3**

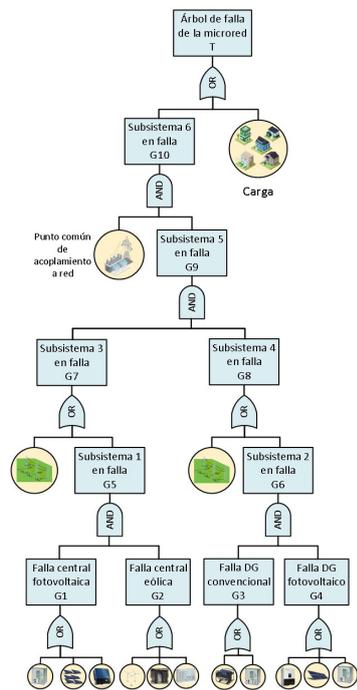


Figura 3: Árbol de falla de la Micro-red

La dispersión de fallas en Micro-redes se puede interpretar grafos no dirigidos, tanto para la red eléctrica como de comunicaciones. Las dependencias son representadas como el conjunto E de aristas que conectan los nodos que son dependientes entre sí, una falla del nodo de una red puede causar que toda o parte de la MG falle. Esta es una característica común a varios modelos, donde la diferencia radica en cómo son asignadas las existencias de interdependencias. Otra diferencia es como cada modelo define las condiciones que debe cumplir cierto nodo o parte del sistema para considerarse que está en estado de operación [1].

En este contexto se puede encontrar al Modelo Uniforme de Buldyrev et al. Este modelo hace varias simplificaciones

incluyendo que se tiene un sistema homogéneo, haciendo uso de la teoría de filtración, ofreciendo una formulación del porcentaje de nodos en falla, en estado estable mientras identifica la influencia de una red con otra. Así mismo determina la cantidad mínima de nodos que deben estar en falla para comprometer al sistema en su totalidad [1] [45].

Por otro lado, está el modelo conocido como Small Clusters, más avanzado y reciente, toma en cuenta los roles de la red eléctrica y de comunicaciones, los modelos de interdependencias son más complejos, así también los esquemas de propagación. Introduce nodos de control de la funcionalidad de la red de potencia y nodos de relé que proveen la infraestructura de comunicaciones. Se dan nuevas interdependencias entre las dos clases de nodos, por ejemplo, un nodo de relé depende de un nodo de control para tener energía. Las interdependencias son direccionales y asimétricas.

Una limitación es que aún considera que los nodos de red eléctrica no pueden producir, transmitir o consumir energía. Tampoco puede determinar que no se puede consumir energía si no hay un nodo de generación conectado [1], [45]. Finalmente, los autores de [1] proponen un esquema que pretende emular la heterogeneidad de la red (nodos de generación, transmisión y distribución) y distingue entre las interdependencias físicas y lógicas. Las dependencias físicas ocurren entre elementos de red de potencia y entre elementos de red de comunicaciones para poder funcionar, las lógicas son aquellas necesarias para el control de los nodos, de esta forma la propagación de falla es más compleja y tiene un análisis más profundo, pero a la vez más realista de lo que puede ocurrir

en una red eléctrica durante un evento de falla.

5.2. Procesos de Markov

Un proceso de Markov podría ser propuesto para el análisis de la propagación de las fallas, ya que permitiría predecir el comportamiento de las diferentes interdependencias de un sistema, formando parejas de elementos críticos, teniendo esta aproximación como objetivo final determinar la susceptibilidad a un evento de falla en cascada de tal interdependencia y la caracterización de los efectos de dependencia mutua en la confiabilidad del sistema [46], [32], [6].

Para que el proceso de Markov pueda obtener resultados cercanos a la realidad, se considera que la red puede estar operando en estados randómicos o en diversos ambientes[46], esto es que el sistema puede estar operando con baja, media o alta carga; notando que cuando está con mayor carga es cuando es más susceptible de que ocurra un evento de falla.

Típicamente un proceso markoviano considera el estado anterior de una red o varias como ya se ha indicado antes en un tiempo t , para obtener el estado o en este caso la propagación de la falla en un tiempo $t+1$. Se debe conocer que un evento de cascada se dará cuando uno o más elementos son afectados por un evento, lo que da lugar a que más elementos resulten afectados o a que la totalidad del sistema entre en estado de falla [46].

El modelo de Markov por medio de las matrices de transición, será de gran utilidad para el estudio de la propagación de fallas en una Micro-red ya que es

capaz de indicar cual parte de esta clase de red tiene una mayor probabilidad en generar esta clase de eventos debido a que soportará una mayor presión, dadas ciertas condiciones iniciales de trabajo del sistema y otros que se consideren necesarios. Otro objetivo de este análisis es determinar el camino más crítico y probable de evolución o propagación de las fallas en la red de baja voltaje, considerando todos sus componentes previamente mencionados [6] [46].

6. Formulación del Problema

Una de las técnicas para la localización de fallas en MGs es asumiendo que la frecuencia natural del sistema es igual a frecuencia de resonancia amortiguada de la corriente detectada por los sensores de corriente (TCs), donde se evidencia un error significativo en la localización de la falla. El método propone descubrir una falla en Micro-redes (MG) obtener la distancia de falla mediante el cálculo de armónicos e impedancia así se tendría los cálculos para el dominio de la frecuencia en el cual este método proporciona el uso del cálculo en la línea para la detección de fallas se aplica un equipo de monitoreo mediante una red y de control remoto de supervisión se usa para cálculos y comandos [41].

$$V \frac{h^*}{m} = Z \frac{h^*}{busmk} * i \frac{h}{k} \quad (5)$$

Donde:

$Z \frac{h^*}{busmk}$ es el elemento asociado a la fila m y la columna k de la matriz de

$Z \frac{h^*}{bus}$.

$Z \frac{h^*}{bus}$ la matriz de impedancia de la red.

$V \frac{h^*}{m}$ Tensión de la matriz.

i inductancia para unidad de longitud.
 h es orden armónico.
 k es la impedancia armónica.

Tabla 1: Variables

Nomenclatura	Variables
T	Tiempo
$i_p(t)$	kit de Corriente inyectada
D	didtancia para localización de la falla.
S_{pf}	Conmutador
S_p	Conmutador
α	atenuación
ω_d	frecuencia de amortiguación

PSEUDOCÓDIGO

Paso 1 **Entrada:** $i_p(t)$; t ;
Paso 2 **Salidas:** d
Paso 3 **Inicializar:** $S_{pf} \rightarrow \{1\}$; $S_p \rightarrow \{0\}$;
 $t = 0$;
Paso 4 **Leer** $i_p(t)$;
Paso 5 **Si** $i_p''(t) < 0$;
 Haga $i_p(j, t) \leftarrow \{i_p'(t) = 0\}$;
 Fin Si
Paso 6 **Haga** $i_{p_1} = i_p(1,1)$; $i_{p_2} = i_p(2,1)$;
 $t_1 = i_p(1,2)$; $t_2 = i_p(2,2)$;
 $\alpha_1 = \frac{\ln i_{p-1} - \ln i_{p-2}}{t_1 - t_2}$;
 $\alpha = \frac{\sum_{i=1}^n \alpha_i}{n}$;
Paso 7 **Si** α es despreciable;
 Haga $S_{pf} \rightarrow \{2\}$;
 $\omega_d = \mathcal{F}\{i_p(t)\}$;
 $d = \frac{1-L_p(w_d^2 + \alpha^2)C_p}{L_u(w_d^2 + \alpha^2)C_p}$;
 Sino $\omega_d = \mathcal{F}\{i_p(t)\}$;
 $d = \frac{1-L_p(w_d^2 + \alpha^2)C_p}{L_u(w_d^2 + \alpha^2)C_p}$;
 Fin Si
Paso 5: **Retorna:** d ;

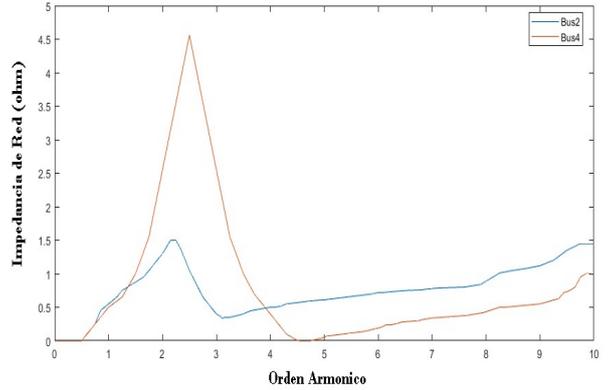


Figura 4. Espectro de impedancia de dos buses cerca de la ubicación de falla simétrica

En la **Figura 4** se puede apreciar mediante la localización de falla el corte de los buses 2 y 4 al final de la línea, se observa la localización de la falla en dos picos de 4,5 del bus 4 y 1,5 del bus 2, siendo el pico más bajo el más cercano a la falla siendo está permanente, con la aplicación de este método se detecta que la falla se encuentra más cerca al bus 2, por lo que este método ayuda a la detección de fallas permanentes, transitorias, alimentadores de conmutación y energización [41].

En la siguiente tabla se presentan las representaciones de las variables que se emplearán en los algoritmos planteados para la resolución del problema planteado.

Tabla 2: Variables del Algoritmo

Nombre	INTERPRETACIÓN
N	Cantidad de tipos de componentes de la Micro-red
B	Conjunto de los tipos de componentes de la Micro-red
J	Tipo de componente j-ésimo específico
M	Número de componentes de tipo j-ésimo en estado de falla

r_j	Cantidad de componentes idénticos por tipo j
T	Instante de tiempo de análisis
$Z_0(t)$	Ambiente de análisis del sistema randómico
E	Conjunto de ambientes
ν_e	Probabilidad de entrar en ambiente e
$\delta_{e,e'}$	Probabilidad de cambio de ambiente e a e'
$\lambda_{j,e}$	Tasa de falla de componente j -ésimo en ambiente e -ésimo
$\mu_{j,e}$	Tasa de reparación de componente j -ésimo en ambiente e -ésimo
B	Cantidad de componentes simultáneos que están en falla
τ_j	Conjunto de componentes ordenado que fallarán instantáneamente si el tipo de componente j -ésimo falla
$\phi_{j,k}$	Probabilidad de que el componente k -ésimo falle simultáneamente si j ha fallado
$Z(t)$	Matriz de Markov de tiempo continuo en el espacio de estado
S	Espacio de estado del sistema
$T(V, E, r)$	Árbol de representación de la propagación de fallas
V	Número de nodos o componentes en falla
E	Número de interdependencias de componentes en falla
R	Origen del árbol de falla T

Se establece un modelo Markoviano que represente a la Micro-red y sus componentes, así como las interdependencias, donde se forma el conjunto $\beta = \{1, 2, \dots, N\}$ que representa a los tipos de componentes de la red, tanto físicos como cibernéticos. Así mismo, existe un número de componentes, incluyendo aquellos redundantes r_j , siendo j un tipo de componente específico

y que pertenece a β . Se asume que todos los componentes j -ésimos son idénticos.

La Micro-red puede estar trabajando en diversos ambientes, es decir con diversos niveles de cargas, así mismo puede tener diversas tasas de reparación y de falla, todo ello forma parte de las condiciones iniciales del sistema. Es bastante típico que las tasas de falla se incrementen si el sistema está sometido a una carga elevada [44].

Es posible modelar al sistema en un instante t con un ambiente dado, pero que puede cambiar randómicamente, con una variable $Z_0(t)$ que representa el ambiente, existiendo una cantidad de ambientes $\mathcal{E} = \{1, 2, \dots, M\}$.

En este caso, si el sistema ha entrado en el ambiente $e \in \mathcal{E}$ se mantendrá en este ambiente durante un tiempo probabilístico con una tasa $\nu_e > 0$ y que se moverá a $e' \in \mathcal{E}$ con una probabilidad $\delta_{e,e'}$, se asume que $\delta_{e,e} = 0$ es decir un sistema no puede quedarse en el mismo ambiente, además la matriz de transición de ambiente es irreducible y considera todos los cambios posibles [44].

Luego se considera que cada tipo de componente j existe una tasa constante de falla $\lambda_{j,e} > 0$. La distribución exponencial será la usada para determinar los tiempos de vida útil de los componentes de la Micro-red, existiendo siempre componentes que son más susceptibles de entrar en estado de falla.

Así mismo existirá una tasa de reparación $\mu_{j,e} > 0$, existiendo un cierto número de componentes que están en falla, por lo

cual la tasa de reparación se divide $\mu_{j,e} / b$ [44].

6.1. Propagación de falla en cascada

Para llevar a cabo el modelamiento de los eventos en cascada, cada tipo de componente j , $\tau_j \subseteq \beta$ hay un conjunto de componentes que fallarán instantáneamente si el componente j falla, siendo el orden de los componentes de τ , el orden en el que ocurre las fallas de componentes, aspecto a considerar para determinar la probabilidad de un evento en cascada.

Si un componente tipo j ha fallado cada de elemento $k \in \tau_j$ fallará con $\phi_{j,k}$ como la probabilidad de que un componente de tipo j cause que un elemento tipo k falle simultáneamente y $1 - \phi_{j,k}$ de que no ocurra la falla [44].

Tabla 3. Tasas de falla por componente de la Micro-red

Componente	Tasa de falla (fallas/hora e-6)
Lineas aéreas [48]	1.0616
Postes [48]	0.0959
Transformadores [48]	0.2283
Panel Solar PV [49]	4.5662
Generador Diesel [49]	11.4155
Celda Combustible [49]	14.2694
Inversor DC/AC [49]	14.2694
Punto de conexión común a la red [49]	2.3831
Carga [49]	2.3831

Se determina el árbol de falla, cuya ruta es directamente dependiente del primer componente que entró en falla como un

sistema probabilístico. Los nodos del árbol son los que fallan instantáneamente y se asume que existe un orden en que fallan.

Las tasas de falla que se van a emplear para este trabajo se proponen en la tabla 1, considerando la respectiva referencia de la cual fue tomado el dato.

6.2. Modelo de Markov

Para que el proceso de Markov obtenga resultados que sean cercanos a la realidad, y teniendo en cuenta que no se puede tener valores reales debido a que Markov necesita de datos estadísticos, y estos datos estadísticos son monitoreados por varios años y este tipo de Micro-redes se encuentran todavía en estudio y análisis.

Por lo tanto, es necesario considerar un modelo que simule el comportamiento de la propagación de fallas, considerando las condiciones específicas que supone la existencia de una Micro-red.

Para este análisis de las fallas es necesario que el sistema se puede considera las respectivas interdependencias, notando como se ha indicado antes que hay dependencias físicas y lógicas que pueden provocar la propagación de una falla, se nota que la red y el sistema de líneas son primordiales ya que permiten la conexión de cargas, generadores y otros que forman parte de la Micro-red (MG).

Todas las matrices se utiliza valores aproximados y coherentes en donde podría ver una falla, Markov es un programa en el cual nos ayudara analizar donde hay una falla posible en una MG; las matrices son construidas a partir de las condiciones específicas planteadas.

Las matrices de transición, nos ayudan a conocer como un subsistema se va comportar frente a una falla y esto es de gran utilidad para el estudio de la propagación de fallas y como se comportaría una MG, ya que es capaz de indicar cual parte de esta clase de red tiene una mayor probabilidad de generar esta clase de eventos.

La parte principal del modelo planteado es que por medio de este análisis se podría determinar el camino más crítico y probable y cómo evoluciona o propaga falla en la Micro-red eléctrica

En este caso se determina que el modelo de cadena de Markov de tiempo continuo (CTMC) por siglas en inglés que puede representar lo que ocurre en una Micro-red, tiene el espacio de estado (1) [44].

$$S = \{(x_0, x_1, x_2, \dots, x_M) : x_0 \in \varepsilon, 0 \leq x_j \leq r_j\} \quad (6)$$

Para todo j que pertenece a β

Para el espacio de estado (1), X_0 es el ambiente, y hay componentes fallados X_j para cada $j \in \beta$. El tamaño del espacio de estado es (2) [44].

$$|S| = L \prod_{j=1}^M (r_j + 1)^\infty \quad (7)$$

El espacio de estado crece linealmente en función del número de ambientes que tenga el modelo, así como del número de tipos de componentes.

Calculo de la probabilidad de la secuencia parcial.

$B(t)$ es la que se puede observar de la secuencia parcial al encontrarse en un instante de tiempo para un estado determinado.

$$B(t) = \sum_{m=1}^N \frac{[Y(m)=z]}{\# \text{eventos}} \quad (8)$$

Se plantea de forma que la ecuación:

$$Z(t) = (Z_0(t), Z_1(t), \dots, Z_M(t)), \quad \text{siendo}$$

$Z_0(t)$ es el ambiente inicial del tiempo t y $Z_j(t), j=1, 2, \dots, M$ es el número de componentes en falla del tipo j . Resulta que $Z(t) = (Z(t) : t \geq 0)$ es un proceso estocástico que sigue la evolución del sistema en el tiempo y por los supuestos dados, Z es la CTMC en el espacio de estado S .

En este caso $Q = (Q(x, y) : x, y \in S)$ denotando $|S| \times |S|$ -dimensional como el generador de matriz infinitesimal de la cadena CTMC Z . $Q(x, y)$ es la tasa de probabilidad total de paso de estado de x hacia y [44].

Si los estados $(X_0, X_1, X_2, \dots, X_M)$ y $(Y_0, Y_1, Y_2, \dots, Y_M)$ pertenecen a S , es bastante claro que solo ciertos pares (x, y) representan a transiciones validas de la CTMC Z . Las transiciones permitidas son dependientes de los elementos j y de que aquellos susceptibles de fallar k como se ha indicado previamente, dependiendo también de las probabilidades de la existencia de un efecto en cascada, así mismo de las tasas de falla y de reparación. Aquellas transiciones que no son posibles se representan como $Q(x, y) = 0$ y $Q(x, x) = -\sum_{y \neq x} Q(x, y)$ [44].

Entendido lo ya indicado, para analizar la propagación de una falla se considera la apreciar cuales son los puntos en donde tienen una mayor probabilidad de que se produzca una falla; y mientras mayor sea la probabilidad el color se oscurece más por lo que en aquellos estados donde tienen una mayor probabilidad su tonalidad de color tiende a color rojo oscuro.

Basándonos en metodologías para la escritura de algoritmos [50], a continuación, se presenta el al algoritmo propuesto.

Con base en las reglas mencionadas anteriormente para el modelado de Markov, se desarrolla una estrategia, como se muestra en la Figura 4, una estrategia de tolerancia a fallas mencionada.

Considerando:

1. Configure la distribución de $Q =$ conjunto de Estados $Q = [q_1, q_2, q_3, \dots, q_n]$.
2. Determine la inicialización característica, $P_i =$ Probabilidades iniciadas $P_i = [p_{i1}, p_{i2}, p_{i3}, \dots, p_{in}]$.
3. Construya la matriz de transición, Modelo. $A =$ matriz de transición $A = [a_{ij}]$;
4. Determine el modelo de proceso de emisión Modelo. $T =$ matriz de emisión $A = [T_{ij}]$;
5. Estado: $Y(i) =$ max probabilidad acumulativa de Estados.
 $\sum_{i=1}^{\# \text{eventos}} P_i(i)$.
6. Secuencia: $K(i) =$ max probabilidad acumulativa de datos inicial.
 $\sum_{i=1}^{\# \text{eventos}} Q(i)$.
7. $Z =$ la más alta probabilidad que se obtiene a lo largo del algoritmo en un instante tiempo.
8. $Z = \max (Y(t))$;

9. $B(t)$ es la que se puede observar de la secuencia parcial al encontrarse en un instante de tiempo para un estado determinado.

10.

$$B(t) = \sum_{m=1}^N \frac{[Y(m)=z]}{\# \text{eventos}} \quad (9)$$

SEUDOCODIGO

Paso 1: **Entrada** ($P_i, Q, \text{Modelo. } A, \text{ Modelo}$)

Entrada: $Q = (q_1, q_2, q_3 \dots q_n)$;

Entrada: $P_i = (p_{i1}, p_{i2}, p_{i3} \dots p_{in})$;

Paso 2: **Salida:** ($Z, B(t)$)

Paso 3: **Inicialización:** $\text{Modelo. } A(a_{ij}),$

$\text{Modelo. } T(T_{ij}),$

$\text{Modelo. } P_i(p_{in})$

Paso 4: $Y(i) = \text{máx. } (\sum_{i=1}^{\# \text{eventos}} P_i(i))$

leer F_i

switch k {case 1, case 2, case 3, case 4, case 5, case 6, case 7, case 8, case 9, case 10};

Paso 5: $K(i) = \text{máx. } (\sum_{i=1}^{\# \text{eventos}} Q(i))$

Paso 6: $Z(i) = \text{máx. } (Y(i))$;

Paso 7: $B(t) = \sum_{m=1}^N \frac{[Y(m)=z]}{\# \text{eventos}}$

Paso 8: **Repetir** Paso 1 al Paso 7 para subsistemas

Paso 9: **Repetir** Paso 1 al Paso 7 para Sistema

6.3. Modelo Propuesto

Los cambios que suponen como voltaje, corriente y frecuencia por la existencia de una Micro-red (MG), ha implicado que se realice un análisis del comportamiento del sistema y de sus componentes como son por ejemplo Generación convencional, microturbinas, generación renovable, almacenamiento de energía, bancos de baterías, interfaz basado en electrónica de potencia, inversores y conexiones a la red.

Para que sea un Recurso Energético Primario debe ser modificado incluyendo la localización de la propagación de fallas y que por medio de Markov podríamos tener una probabilidad donde sería el fallo en la Micro-red, para los elementos físicos y los de comunicaciones, ambos fundamentales para un funcionamiento óptimo del sistema.

Para el planteamiento metodológico se basó en intentar localizar o realizar un análisis de las fallas por medio de las tasas de probabilidades descritas en el anexo (Tabla 4. Componentes-Modos de Falla-Causas y Efectos).

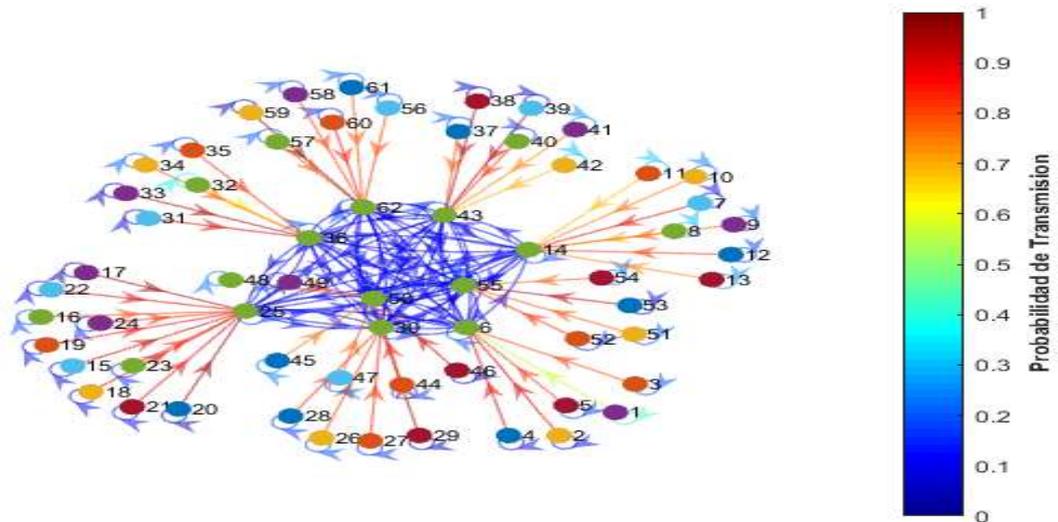


Figura 5. Diagrama de resultado general de los Subsistemas.

Ya que por medio de los métodos markovianos se realiza un análisis de la Micro-red con la finalidad de tener una mayor facilidad en lo que se refiere a la ubicación de la misma falla y conocer principalmente el funcionamiento de cada uno de los subsistemas que integran el sistema o el caso de estudio propuesto.

Por lo tanto, de lo planteado anteriormente se propone realizar un análisis partiendo de cada uno de los subsistemas, es decir que se determinaría la probabilidad de falla de cada subsistema y cuando ya se haya obtenido esta probabilidad para cada uno de los 9 subsistemas se realiza un análisis general del sistema completo

para determinar la probabilidad del sistema en general.

La **Figura 5** representa el modelo de la matriz de transición, la representación gráfica de la matriz con cada uno de los estados que van a representar el sistema de generación y transmisión de la red eléctrica; y cuáles son las probabilidades de fallo del sistema; también se puede apreciar cuales son los estados vulnerables de fallos y como se puede trasladar una falla a otros sistemas; la representación gráfica de la matriz de transición nos ayuda a realizar una estimación que la probabilidad de falla de todo el sistema en general.

En la **Figura 6** se presenta la conexión de los subcomponentes hacia el

subsistema fotovoltaica en el cual podemos tener modos de fallas o efectos que incluyen circuitos abiertos, cortocircuitos, puntos abiertos y celdas en circuito abierto y se tiene las fallas de derivación que ocurren debido a sobrecalentamiento de tales elementos semiconductores. Cada uno de los subcomponentes van a representar una posible falla que se puede ocurrir en el sistema en general; mientras que el subsistema va a reflejar la falla en el sistema interconectado que se ilustrara más adelante. En el caso de la matriz de calor obtenido por el diagrama de la matriz fotovoltaica se logra apreciar las fallas o punto donde tiene la probabilidad que exista una falla en la Micro-red en la parte de eventos tendremos desde el punto 0 a 0,9 de la probabilidad de transmisión tendremos un espacio de 7,5 a 8,5 de eventos donde es reflejada la falla.

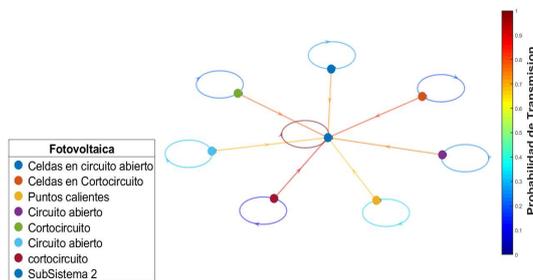


Figura 6. Diagrama de matriz de transmisión de subsistema Fotovoltaica

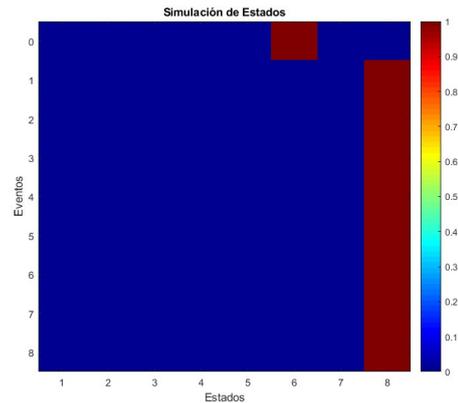


Figura 7. Matriz de calor Fotovoltaica

En este diagrama podremos observar elementos de transmisión de energía del viento para generar electricidad. Sus fallas están asociadas de varios subcomponentes como son, la caja de cambios, cojinetes, pérdida de fluidos, cortocircuito en los sistemas de control eléctricos y electrónicos, del generador. eléctrico y fallas de rotores, aspas y elementos hidráulicos. Las fallas más comunes son las de cojinetes y cajas de cambios, pero aquí podremos observar donde podría localizarse la falla en un subsistema de transmisión. De la misma manera que la **Figura 5** la gráfica va a representar como se puede generar una falla y como esta falla va afectar al sistema interconectado entre cada una de los estados o microgeneración que se encuentra asociada o enlazada entre sí para transmitir la energía La parte de la matriz de calor podemos apreciar la falla y sin importar el evento o el fenómeno tendremos la probabilidad en ese punto.

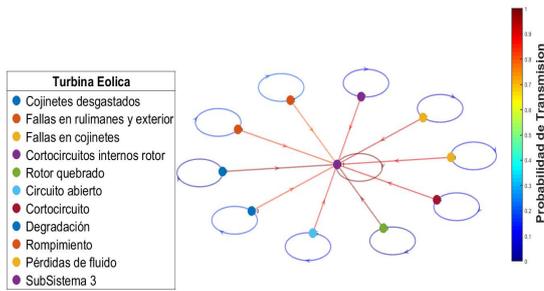


Figura 8.Diagrama de matriz de transmisión de subsistema de Turbina Eólica

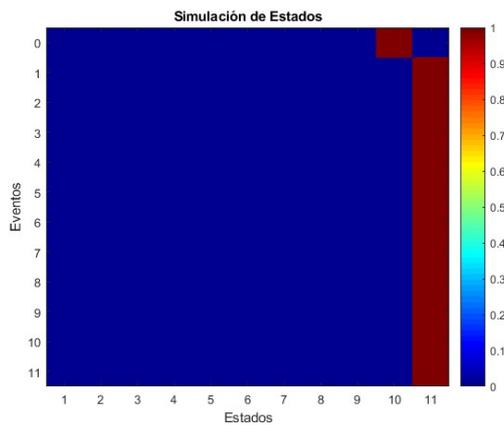


Figura 9.Matriz de calor Turbina Eólica

En este diagrama de transmisión del sistema de Control se lleva a cabo el control de las máquinas de generación, donde se puede verificar tipos de subcomponentes que puede ocurrir en una apertura o cierre inadecuado de los interruptores de conexión a la Micro-red (MG).

Tanto la **Figura 4**, la **Figura 6** y la **Figura 8** podemos visualizar los siguientes parámetros, la probabilidad de transición, esta probabilidad va a representar el estado más probable de fallo de acuerdo a la matriz de transición; mientras más se acerque a 1 el estado de transición mayor probabilidad de fallo; esto podemos apreciar en cada uno de las gráficas ilustradas. En cambio, para las figuras 7, 9,11 la matriz de calor también refleja

los Estados en el que podemos tener la probabilidad de falla del evento y también podemos observar cómo se desencadena la falla desde el estado hacia el subsistema.

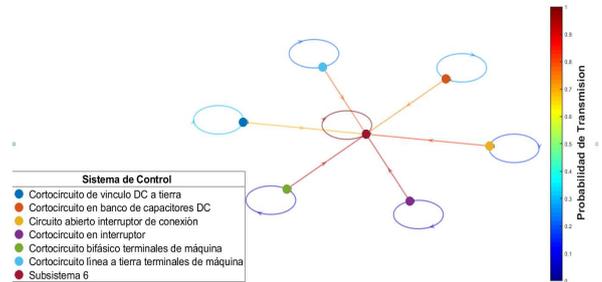


Figura 10.Diagrama de matriz de transmisión de subsistema-Sistema de Control

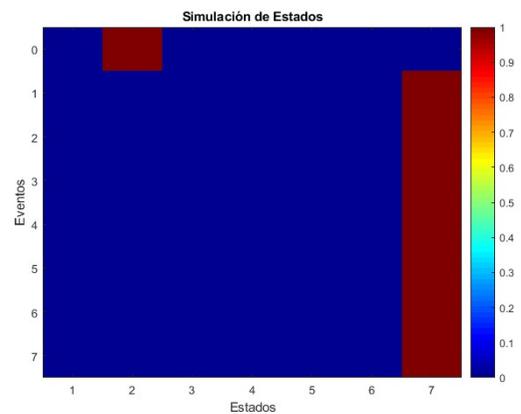


Figura 11.Matriz de calor Sistema de Control

7. Caso de Estudio

En esta parte tendremos las simulaciones usando datos del sistema para pruebas de localización en fallas en una Micro-red (MG) eléctrica.

Para este caso de estudio la detección de los puntos más críticos en los que puede ocurrir una falla, así como la determinación de la ruta más probable (primero guiándome en una posible falla en la parte de subcomponentes para poder llegar a la falla o una probabilidad que pueda verse en un subsistema).

El caso de estudio se plantea de la siguiente manera; dos centrales una eólica, cuatro solares, dos generaciones distribuidas y un generador Diesel entonces de cada central están los componentes, por ejemplo, la solar está con protección, inversor, paneles y transformador, que consumen la energía (Figura 12). El sistema de control utilizado para equilibrar la oferta y la demanda y así se tendría un buen funcionamiento para lo que es problema del desequilibrio de potencia. [38].

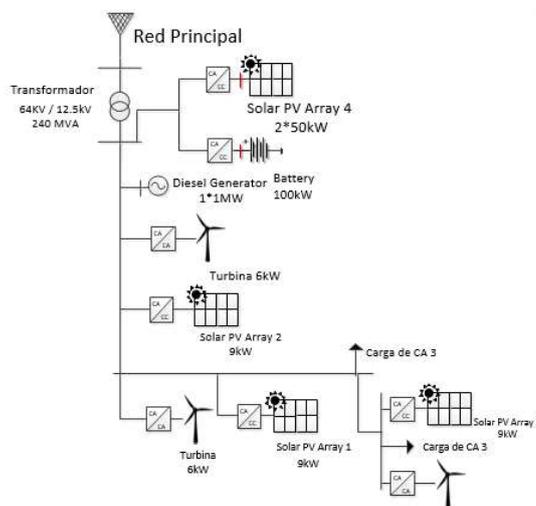


Figura 12. Caso Benchmark Hachinohe Project del proyecto NIDO en Japón

En la Figura 13 se representa como se puede producir una falla en el sistema de transición realizado; se aprecia cuáles son los puntos en donde tienen una mayor probabilidad de que se produzca una falla; y mientras mayor sea la probabilidad el color se oscurece más, por lo que en aquellos estados donde tienen una mayor probabilidad su tonalidad de color tiende a color rojo oscuro, siendo estos los puntos más vulnerables a generar un evento de falla en cascada.

Tales puntos de mapa de calor en mención deben tomar especial

relevancia durante la planificación o modificación de la estructura de la Micro-red (MG) y en trabajos futuros serán motivo de análisis de estrategias para la reducción de riesgos de existencias en eventos de fallas.

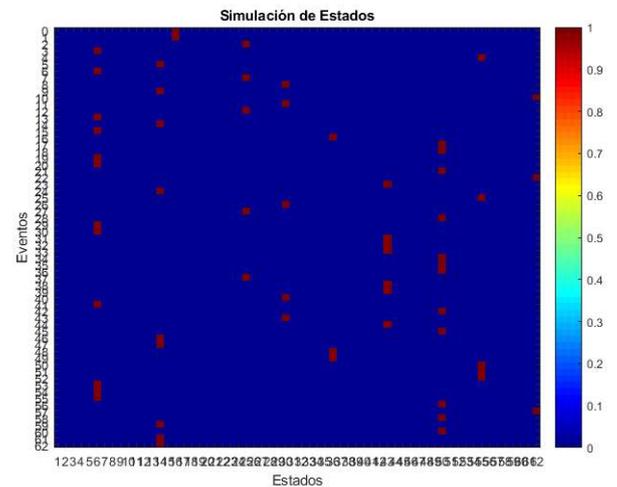


Figura 13. Matriz de Calor.

8. Trabajos futuros

Par trabajos futuros se podría determinar las ubicaciones más probables para que exista una localización de falla, para el diagnóstico de fallas en el cual se emplean valores probables que consisten principalmente en el análisis de elementos como el mapa de calor de los puntos de existencia de falla, alimentando al método propuesto con las tasas de falla probabilísticas de los componentes en estudio en función de sus modos de falla para la detección de algún error interno y evitar que hallan averías en el sistema

El algoritmo establecido posibilita determinar el estado más probable en el que se van a encontrar componentes y subsistemas en una Micro-red en un tiempo inicial, pudiendo establecerse

los lugares más vulnerables a fallos de la MG y como trabajos futuros se tiene una estrategia para reducir la cantidad de fallos o la probabilidad de propagación de la falla al resto del sistema, para ello es determinante simular otras condiciones típicas de las micro-redes y que previamente se describieron

9. Conclusiones

En el presente trabajo se ha mostrado que las matrices de transición tienen una facilidad en Markov en el cual pueden ser consideradas como un método efectivo para la localización y propagación del estado de falla en el que se encuentre en los componentes de una MG.

Debido a la complejidad de una MG, para tener una correcta aproximación a la ocurrencia de la propagación de una falla, su sugiere tomar como estrategia dividir la MG en subsistemas, permitiendo determinar la probabilidad de falla de cada subsistema y entender la dependencia entre sí que involucra la existencia de fallas en cascada según los efectos y el origen de la falla.

La matriz de transición es un método de tabla en cual se basa en experiencias previas obtenidos a los resultados cercanos a la realidad, siendo clave considerar la deficiencia o carencia de datos históricos probabilísticos del comportamiento de los sistemas en las Micro-redes que son la base de los resultados del estudio realizado.

Es primordial que en experiencias futuras se ponga a prueba al algoritmo, posibilitando un análisis más cercano a la realidad de la propagación de fallas en los cuales se producen debido a la existencia de flujo bidireccional y el aumento de la capacidad de corriente de falla.

En la parte de la investigación se logró la detección de puntos probables de una falla en un sistema de Micro-red.

10. Referencias

- [1] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "Towards a realistic model for failure propagation in interdependent networks," *2016 Int. Conf. Comput. Netw. Commun. ICNC 2016*, 2016.
- [2] M. Rahnamay-Naeini and M. M. Hayat, "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1997–2006, 2016.
- [3] P. Arbolea *et al.*, "Efficient energy management in smart micro-grids: ZERO grid impact buildings," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 1055–1063, 2015.
- [4] M. Falvo, L. Martirano, D. Sbordone, I. Bertini, B. Di Pietra, and F. Vellucci, "A flexible customer power device for energy management in a real smart micro-grid," in *IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society*, 2013, pp. 7586–7591.
- [5] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, 2012.
- [6] D. Carrión and L. Ortiz, "Generación distribuida a partir de bicicletas estáticas y sistemas híbridos," *Ingenius*, vol. 10, pp. 44–48, 2013.
- [7] J. Hare, X. Shi, S. Gupta, and A. Bazzi, "A review of faults and fault diagnosis in micro-grids electrical energy infrastructure," *2014 IEEE*

- Energy Convers. Congr. Expo. ECCE 2014*, no. August 2003, pp. 3325–3332, 2014.
- [8] D. Arias Cazco, R. A. Robayo Vasco, and L. Ortiz Matos, “Novel inteligente Step Voltaje Regulator (SVR) for residential electrical connections,” *IEEE Lat. Am. Trans.*, vol. 14, no. 4, pp. 1656–1661, 2016.
- [9] F. M. Armas Chamorro and L. Ortiz Matos, “Modelización con Petri Net de una aplicación automática de diagnóstico y restauración de avería en sistema de distribución,” Universidad Politécnica Salesiana, 2015.
- [10] R. H. Lasseter, “MicroGrids,” *2002 IEEE Power Eng. Soc. Winter Meet. Conf. Proc. (Cat. No.02CH37309)*, vol. 1, pp. 305–308, 2002.
- [11] D. E. Olivares *et al.*, “Trends in microgrid control,” *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, 2014.
- [12] J. G. B. Sánchez and L. O. Matos, “Estrategia de tolerancia a fallas por condiciones ambientales para IEDS en subestaciones de distribución,” Universidad Politécnica Salesiana, 2016.
- [13] M. Kezunovic, “Smart Fault Location for Smart Grids,” *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 11–22, 2011.
- [14] E. M. Gui, M. Diesendorf, and I. MacGill, “Distributed energy infrastructure paradigm: Community microgrids in a new institutional economics context,” *Renew. Sustain. Energy Rev.*, vol. 72, no. October, pp. 1355–1365, 2017.
- [15] G. K. Chinchuña Toledo and L. Ortiz Matos, “Mejoramiento de la fiabilidad en microredes mediante el control robusto de voltaje usando técnicas pasivas de tolerancia a fallos,” Universidad Politécnica Salesiana, 2018.
- [16] N. Jayawarna, C. Jones, N. Jenkins, and M. Barnes, “Operating MicroGrid Energy Storage Control during Network Faults,” 2007.
- [17] L. O. Matos, J. Wilson, and G. Sanchez, “Reconfiguration Strategy for Fault Tolerance of Power Distribution Systems Using Petri Net,” 2016.
- [18] A. Aguila, D. Carrión, and L. Ortiz, “Analysis of power losses in the asymmetric construction of electric distribution systems,” *IEE Lat. Am. Trans.*, vol. 13, no. 7, pp. 2190–2194, 2015.
- [19] P. Manganiello, M. Balato, and M. Vitelli, “A Survey on Mismatching and Aging of PV Modules: The Closed Loop,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7276–7286, 2015.
- [20] H. Arabian-Hoseynabadi, H. Oraee, and P. J. Tavner, “Failure Modes and Effects Analysis (FMEA) for wind turbines,” *Int. J. Electr. Power Energy Syst.*, vol. 32, no. 7, pp. 817–824, 2010.
- [21] Z. Hameed, Y. S. Hong, Y. M. Cho, S. H. Ahn, and C. K. Song, “Condition monitoring and fault detection of wind turbines and related algorithms: A review,” *Renew. Sustain. Energy Rev.*, vol. 13, no. 1, pp. 1–39, 2009.
- [22] I. A. Craighead and T. G. F. Gray, “Investigation of diesel generator shaft and bearing failures,” *Proc. Inst. Mech. Eng. Part K J. Multi-body Dyn.*, vol. 218, no. 3, pp. 153–158, 2004.
- [23] F. J. Espadafor, J. B. Villanueva, and M. T. Garc??a, “Analysis of a diesel generator crankshaft failure,”

- Eng. Fail. Anal.*, vol. 16, no. 7, pp. 2333–2341, 2009.
- [24] S. Gholami, S. Saha, and M. Aldeen, “Sensor fault tolerant control of microgrid,” in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016, pp. 1–5.
- [25] L. Wang, M. Cai, H. Zhang, and F. Alsaadi, “Active Fault-tolerant Control for Wind Turbine with Simultaneous Actuator and Sensor Faults.”
- [26] M. Aldeen and R. Sharma, “Robust Detection of Faults in Frequency Control Loops,” *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 413–422, Feb. 2007.
- [27] R. L. De Araujo Ribeiro, C. B. Jacobina, E. R. C. Da Silva, and A. M. N. Lima, “Fault detection of open-switch damage in voltage-fed PWM motor drive systems,” *IEEE Trans. Power Electron.*, vol. 18, no. 2, pp. 587–593, 2003.
- [28] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter,” vol. 5870, no. c, 2014.
- [29] R. Su, “A Cyber Attack Model with Bounded Sensor Reading Alterations,” pp. 3200–3205, 2017.
- [30] M. M. Rana, L. Li, and S. W. Su, “Cyber attack protection and control in microgrids using channel code and semidefinite programming,” *IEEE Power Energy Soc. Gen. Meet.*, vol. 2016–Novem, pp. 16–20, 2016.
- [31] M. M. Rana, L. Li, and S. W. Su, “Cyber attack protection and control of microgrids,” *IEEE/CAA J. Autom. Sin.*, pp. 1–8, 2017.
- [32] B. Dutta and M. Hassan, “Impact of Cyber-Attack on Isolated Power System,” pp. 8–11, 2016.
- [33] R. Kheirollahi and A. P. Fault, “Developing a New Fault Location Topology for DC Microgrid Systems,” no. Pedstc, pp. 16–18, 2016.
- [34] M. Majidi, L. S. Member, M. S. Fadali, and S. Member, “A Novel Method for Single and Simultaneous Fault Location in Distribution Networks,” vol. 30, no. 6, pp. 3368–3376, 2015.
- [35] M. Goudarzi, B. Vahidi, R. A. Naghizadeh, and S. H. Hosseinian, “Electrical Power and Energy Systems Improved fault location algorithm for radial distribution systems with discrete and continuous wavelet analysis,” *Int. J. Electr. Power Energy Syst.*, vol. 67, pp. 423–430, 2015.
- [36] “No Title.”
- [37] S. A. Hosseini, H. A. Abyaneh, S. H. H. Sadeghi, F. Razavi, and M. Karami, “MICROGRIDS , USING HARMONIC IMPEDANCE,” vol. 39, pp. 167–182, 2015.
- [38] T. Gush *et al.*, “Fault detection and location in a microgrid using mathematical morphology and recursive least square methods,” *Int. J. Electr. Power Energy Syst.*, vol. 102, no. April, pp. 324–331, 2018.
- [39] R. Escudero, J. Noel, J. Elizondo, and J. Kirtley, “Microgrid fault detection based on wavelet transformation and Park ’ s vector approach &,” *Electr. Power Syst. Res.*, vol. 152, pp. 401–410, 2017.
- [40] S. Alwala, A. Feliachi, and M. A. Choudhry, “Multi Agent System based fault location and isolation in a smart microgrid system,” *Innov. Smart Grid Technol. (ISGT), 2012 IEEE PES*, pp. 1–4, 2012.

- [41] S. A. Hosseini, H. A. Abyaneh, S. H. H. Sadeghi, F. Razavi, and M. Karami, "Presenting a new method for identifying fault location in microgrids, using harmonic impedance," *Iran. J. Sci. Technol. Trans. Electr. Eng. Shiraz*, vol. 39, no. E2, pp. 167–182, 2015.
- [42] P. Liu, Y. Wu, Y. Su, and B. Duan, "Fault detection and location of microgrid based on distributed decision," *IECON 2017 - 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, pp. 5054–5059, 2017.
- [43] A. K. Pradhan and R. Mohanty, "Cable fault location in a DC microgrid using current injection technique," in *2016 National Power Systems Conference (NPSC)*, 2016, pp. 1–6.
- [44] S. M. Iyer, M. K. Nakayama, and A. V. Gerbessiotis, "A Markovian Dependability Model with Cascading Failures," vol. 58, no. 9, pp. 1238–1249, 2009.
- [45] X. Shi and A. M. Bazzi, "Fault tree reliability analysis of a micro-grid using Monte Carlo simulations," in *2015 IEEE Power and Energy Conference at Illinois (PECI)*, 2015, pp. 1–5.
- [46] Z. Wang, A. Scaglione, and R. J. Thomas, "A Markov-transition model for cascading failures in power grids," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 2115–2124, 2011.
- [47] I. N. Con *et al.*, "ESCUELA DE ELÉCTRICA Tesis Previa A La Obtención Del Título De DIRECTOR ;," 2013.
- [48] F. Roos and S. Lindah, "Distribution system component failure rates and repair times—an overview," *Nord. Distrib. Asset Manag. Conf.*, pp. 1–6, 2004.
- [49] X. Shi, S. Member, and A. M. Bazzi, "Reliability Modeling and Analysis of a Micro-grid with Significant Clean Energy Penetration," pp. 202–207, 2015.
- [50] L. Ortiz Matos, A. Aguila Tellez, R. C. Hincapié Reyes, and J. . González Sanchez, "Multi-Criteria Optimization of the Deployment of a Grid for Rural Electrification Based on a Heuristic Method," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 73, no. 1, p. 012020, 2017.

10.1. Estado del Arte

LOCALIZACIÓN DE FALLAS EN MICROREDES ELÉCTRICAS BASADO EN UN MODELO MARKOVIANO

ITEM	DATOS			TEMÁTICA				FORMULACIÓN DEL PROBLEMA				RESTRICCIONES DEL PROBLEMA		PROPUESTAS PARA RESOLVER EL PROBLEMA			SOLUCIÓN PROPUESTA															
	AÑO	TÍTULO DEL ARTÍCULO	REFERENCIA	CITAS	MICRORED	METODO ESTOCÁSTICO	META DATA	DIAGNÓSTICO DE EVENTOS (fallos)	DETECCIÓN	SUPERVISIÓN Y CONTROL	Markov	Detección de fallos	MINIMIZACIÓN DE COSTOS	LOCALIZACIÓN DE FALLAS	MODELO DE MARKOV	PROPAGACIÓN DE FALLA EN CAS CADA	COSTO	OPTIMIZACIÓN	CONDICIÓN DE CAPACIDAD	CONDICIONES DE DETECCIÓN	ALGORITMOS, Cadenas de Markov	MODELACIONES	MODELACION CON MARKOV	SEGURIDAD	SCHEDULING	CAPACIDAD	COBERTURA	ESCALABILIDAD	DELAY - LATENCY	COSTOS	MULTICAST	ENRUTAMIENTO
1	2007	Robust Detection of Faults in Frequency Control Loops	\cite{Aldeen2007}	32	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
2	2017	Assessment of the Impact of Microgrid Control Strategies in the Power Distribution Reliability Indices	\cite{Araujo2017}	6	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
3	2005	Markov Chain Algorithms: A Template for Building Future Robust Low Power Systems	\cite{Deka2005}	3	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
4	2016	Impact of Cyber-Attack on Isolated Power System	\cite{Dutta2016}	0	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
5	2013	Fault Tolerance for Distributed Real Time Dynamically Reconfigurable Systems from Modeling to Implementation	\cite{Gabsi2013}	4	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
6	2016	Sensor Fault Tolerant Control of Microgrid Sasan	\cite{Gholami2016}	2	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
7	2009	A Markovian Dependability Model with Cascading Failures	\cite{Iyer2009}	46	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

8	2007	Operating MicroGrid Energy Storage Control during Network Faults	\cite{Jagawarna2007}	62	*	*																*			*	
9	2014	Modeling and control of microgrid: An overview	\cite{Mahmoud2014}	95		*	*						*	*		*			*							
10	2014	Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter	\cite{Manandhar2014}	86	*		*	*	*	*	*					*	*					*		*		
11	2016	Reconfiguration Strategy for Fault Tolerance of Power Distribution Systems Using Petri Net	\cite{Matos2016}	2		*	*	*	*	*	*	*	*	*	*	*	*								*	
12	2016	A Fault-Tolerant Control Paradigm for Microgrid-Connected Wind Energy Systems	\cite{Morshed2016}	12	*	*		*	*	*	*	*	*	*	*	*						*				
13	2003	Fault Detection of Open-Switch Damage in Voltage-Fed PWM Motor Drive Systems	\cite{Motor2003}	438			*			*												*		*	*	
14	2010	Control Tolerante a Fallos (Parte I): Fundamentos y Diagnóstico de Fallos	\cite{Ocampo-martinez2010}	33	*		*	*	*	*					*	*										
15	2017	Active Fault-Tolerant Control for a Quadrotor with Sensor Faults	\cite{Qin2017}	1	*	*	*	*	*	*	*	*	*	*	*	*						*		*		
16	2016	Cyber Attack Protection and Control in Microgrids Using Channel Code and Semidefinite Programming	\cite{Rana2016}	1	*		*		*	*	*	*	*	*	*											
17		Cyber Attack Protection and Control of Microgrids	\cite{Rana}	0	*	*				*		*		*		*		*	*	*						
18	2015	Reliability Modeling and Analysis of a Micro-grid with Significant Clean Energy Penetration	\cite{Shi2015}	2	*		*					*			*							*		*		
19	2012	Microgrids Availability Evaluation using a Markov Chain Energy Storage Model: a Comparison Study in System Architectures	\cite{Song2012}	17	*		*	*	*	*	*	*	*	*	*	*	*					*				
20	2017	A Cyber Attack Model with Bounded Sensor Reading Alterations	\cite{Su2017}	0	*	*	*	*	*	*	*	*	*	*	*	*	*					*		*	*	*
21		Active Fault-tolerant Control for Wind Turbine with Simultaneous Actuator and Sensor Faults	\cite{Wang}	1	*	*	*	*	*	*	*	*	*	*	*	*									*	

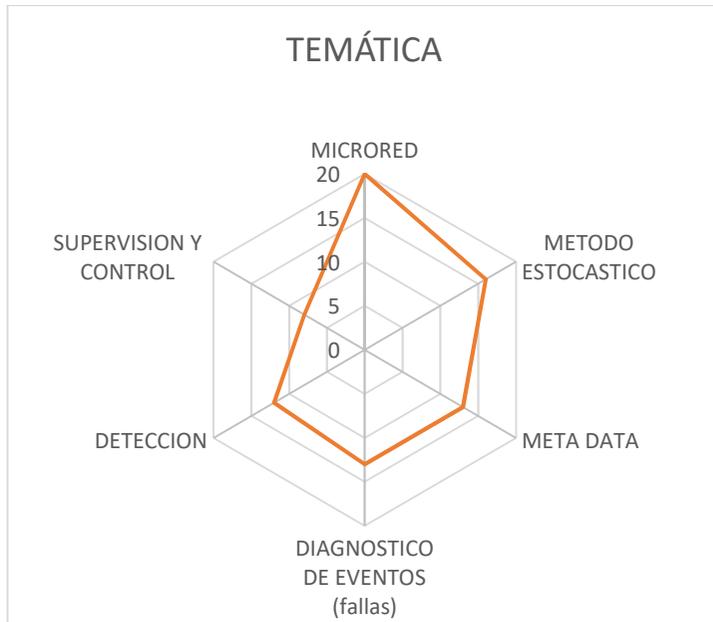


Figura 14. Temática-Indicador de la Matriz del Estado de Arte

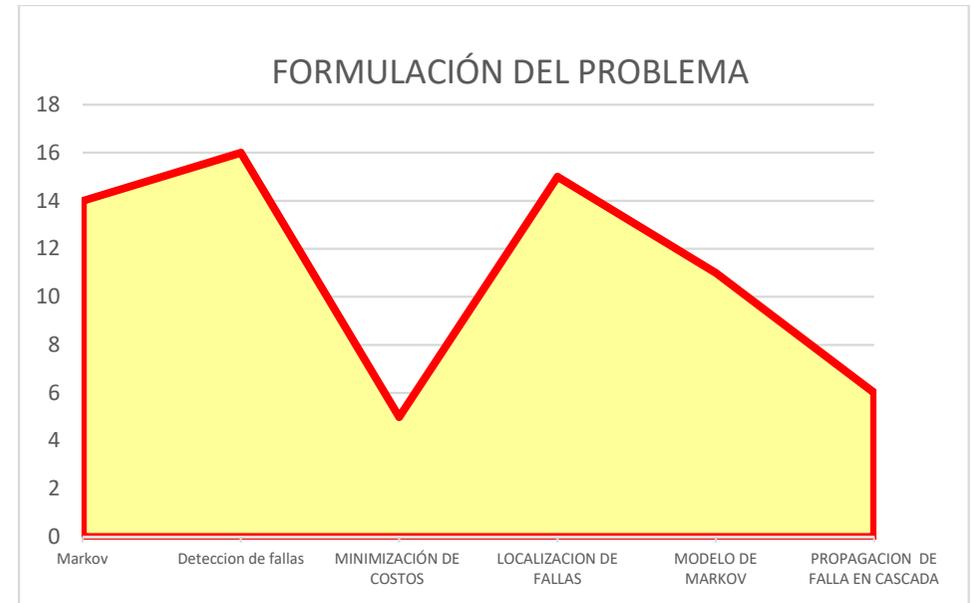


Figura 15. Formulación del Problema-Indicador de la Matriz del Estado del Arte

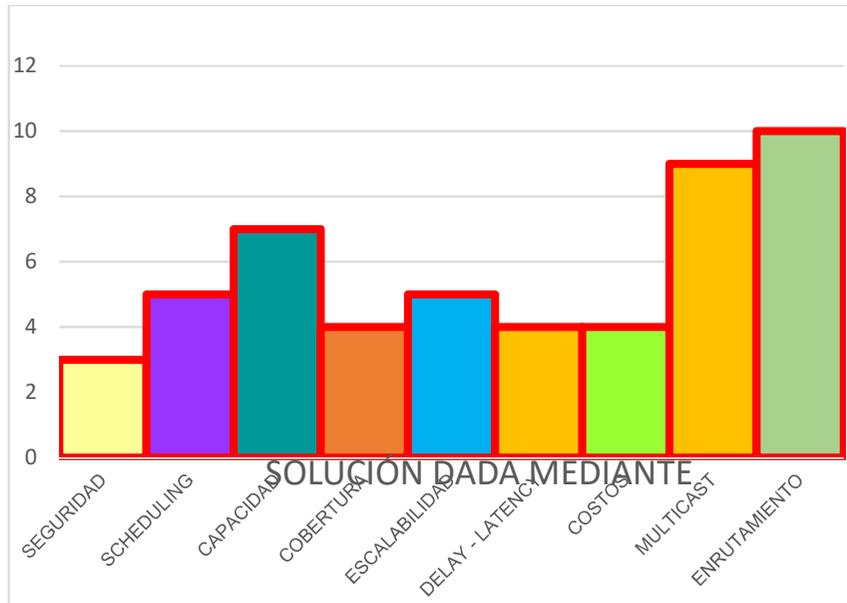


Figura 16. Solución-Indicador de la Matriz del Estado de Arte

11. Anexos

Tabla 4. Componentes-Modos de Falla-Causas y Efectos

Componente	Subcomponente	Modo de falla	Causa	Efecto	Probabilidad O tasa de fallos / horas Dato / variable
Cables y líneas de distribución		Cortocircuito línea a tierra	Contactos físicos con animales, árboles, personas entre fases o fase	Reducciones de la voltaje	1.0616 e-6
		Cortocircuito línea a línea		Incrementos significativos de corriente circulante	
		Cortocircuito línea línea a tierra			
		Cortocircuito trifásico			
		Sobrecargas	Fallas humanas, de operación, falta de mantenimiento	Disparo de protecciones	
		Falla en aisladores		Pérdida de flujo circulante	
Paneles fotovoltaicos	Celdas	Celdas en circuito abierto	Degradación de materiales	Reducción de potencia de salida	4.5662e-6
		Celdas en Cortocircuito	Falta de mantenimiento y limpieza	Cambios en formas de onda de corriente y voltaje	
		Puntos calientes	Corrosión y estrés mecánico	Mal funcionamiento del sistema	
	Módulos	Circuito abierto	Defectos de fabricación	La radiación y la temperatura	
		Cortocircuito	Estrés mecánico Quebradura de cristal Pérdida de resistencia		
	Diodos By-pass	Circuito abierto y cortocircuito	Sobrecalentamiento		

Turbina eólica	Caja de cambios y cojinetes	Cojinetes desgastados	Corrosión y estrés mecánico	Cambios y desbalances en formas de onda de corriente y voltaje	5.7077e-6
		Fallas en rulimanes y exterior	Defectos mecánicos	Reducción en eficiencia	
	Generador	Fallas en cojinetes	Defectos en cojinetes, estator y rotor	Ondas armónicas destruktivas	
		Cortocircuitos internos rotor	Pérdida de aislamiento	Decremento torque promedio	
		Rotor quebrado	Sobrecalentamiento Corrosión, contaminación y estrés mecánico		
	elementos electrónicos de control	Circuito abierto	Fallas en elementos semiconductores		
		Cortocircuito	Sobrevoltaje de componentes Fallas en circuitos de disparo		
	Aspas	Degradación	Corrosión y estrés mecánico	Cambios de rigidez	
		Rompimiento	Congelamiento y descargas atmosféricas	Reducción de eficiencia	
	Fallas en elementos hidráulicos	Pérdidas de fluido	Corrosión y desgaste Defectos mecánicos		

Microgeneradores y generación convencional	Máquina motriz	Fugas de combustible	Corrosión	Inhabilidad de rotación de la máquina	14.2694e-6
		Agrietamiento de piezas mecánicas	Defectos de fabricación	Pérdidas de eficiencia en la combustión	
	Estator y rotor	Cortocircuito	Falta de mantenimiento		
		Circuito abierto	Fricción incrementada	Pérdida de excentricidad	
			Sobrecalentamiento	Desbalances de voltaje y corriente	
	Cigüeñal		Fatiga mecánica		
			Corrosión y estrés mecánico	Cambios en flujos circulantes	
Sensores y actuadores	Sensores de voltaje y corriente		Defectos en semiconductores	Fallas en el sistema de control	0.50577e-6
		Salida sesgada			
		Salida fija	Ruido electromagnético	Disparo de protecciones	
		Sensor sin salida	Ausencia de señal de entrada	Estados todo o nada	
			Falla general del sensor	Cambios de estructura	
		Desconexión y fallas en cables	Pérdida de rendimiento		
	Actuadores	Falsa operación	Ruido electromagnético	Pérdida de rendimiento	
			Fallas de sensores	Cambios en potencia y desbalances	
		Operación tardía			
			Corrosión y estrés mecánico		

Sistemas de control	Controlador ("Controlador PLC")	Cortocircuito de vínculo DC a tierra	Fallas en elementos semiconductores	Desbalance de frecuencia	1.2557e-6
		Cortocircuito en capacitores DC	Defectos de fabricación	Desbalance de potencia	
		Circuito abierto interruptor de conexión	Fallas en comunicaciones	Microrred sobrecargada	
		Cortocircuito en interruptor	Fallas en cableado		
		Cortocircuito bifásico terminales de máquina	Pérdida de canal de comunicación		
		Cortocircuito línea a tierra terminales de máquina	Apertura/cierre inadecuado interruptores de operación		
	Sistema inteligente ciber físico	Negación de servicio o Denial of Service (DoS)	Conocimiento de parámetros de funcionamiento	Desbalance de frecuencia	
		Perdidas de realimentación i/o errores en el sensado	Ataques randomicos maliciosos(DoS)	Desbalance de potencia	
		Ataque bajo alteraciones de lectura de sensor acotadas (ABSRA)	Falta de detección de ataque	Microrred sobrecargada	
		Ataque de inyección de datos falsos	Toma, grabación y manipulación de datos	Desconexión de todo el sistema	
		Ataque con un sesgo positivo	Falta de control de ataques	Operación insegura de supervisor	
		Ataque con un sesgo negativo		Inestabilidad de la red	
Celda de combustible	Membrana, catalizador y capas de difusión de gas	Degradación mecánica	Perforaciones, quiebres, agujeros	Reducción de eficiencia	14.2694e-6
		Degradación térmica	Ciclo de humidificación	Pérdida de potencia de salida	
		Degradación química	Inundación/sequedad	Cambios en formas de onda de corriente y voltaje	
	Plato bipolar	Pérdida de conductividad	Corrosión		
	Paquete sellador	Falla mecánica			
	Motor de compresor	Degradación	Fricción incrementada		

Convertidores DC/DC DC/AC	IGBT y dispositivos de switching	Cortocircuito	Falla de circuito de disparo	Desbalances de voltaje y corriente	14.2694e-6
		Circuito abierto	Diferencias de coeficientes térmicos de expansión y estrés térmico	Reducción de potencia de salida	
		Falla de encapsulado		Microred sobrecargada	
		Falla circuitos electrónicos	Fatiga de soldas y elementos electrónicos		
			Pérdidas pulsatorias		
			Variación de la velocidad		
		Falla de no disparo monopolar	Degradación de materiales y elementos mecánicos	Incendios y daños de elementos principales	2.5114e-6
Breakers		Falla de no disparo bipolar y tripolar	Sobrecalentamiento		
		Falla de disparo erróneo	Errores de cableado	Sobrecalentamiento barras	
		Circuito abierto	Cambios súbitos de magnitudes eléctricas	Riesgo de electrocución	
		Ruptura de dieléctrico		Arcos en cámaras	
		Bloqueo de disparo			

Tabla 5.Clasificación de Modos de Falla

Según el Objetivo	Fallas Maliciosas	Ciberataques de negación de servicio (DoS)
		Ciberataques de tipo Randomico
		Ciberataques bajo alteraciones de lectura de sensor acotadas (ABSRA).
		Ciberataques de inyección de datos falsos
		Ciberataques con sesgo positivo o negativo
	Fallas No Maliciosas	Cortocircuitos
		Sobrecargas
		Corrosión y degradación mecánica
		Puntos calientes
		Circuitos abiertos
		Pérdidas de fluido
		Degradación térmica
		Degradación química
		Pérdida de conductividad
		Agrietamiento de piezas mecánicas
		Salidas sesgadas de sensores y actuadores.
		Sensor y actuador sin salida
		Falsa operación de actuadores
		Cortocircuitos en capacitores
		Cortocircuitos en vinculo DC
		Cortocircuitos en máquinas y terminales
		Fallas de encapsulado
		Fallas de circuitos electrónicos
		Fallas de disparo erróneo de protecciones
Fallas de no disparo de protecciones		
Ruptura de dieléctrico		

Según los Límites del Sistema	Fallas Internas	Falsa operación de actuadores por fallas en cableado
		Celdas y otros elementos en cortocircuito
		Celdas y otros elementos en circuito abierto
		Puntos calientes
		Fallas en cojinetes, rulimanes, cigüeñales, estatores, rotores y demás elementos mecánicos
		Pérdidas de fluidos y fugas de combustible en celdas de combustible
		Cortocircuitos en máquinas y terminales
		Fallas de encapsulado
		Fallas de circuitos electrónicos
		Fallas de disparo erróneo de protecciones
		Degradación térmica
		Degradación química.
		Pérdida de conductividad
	Fallas Externas	Cortocircuitos originados por causas medioambientales (animales, árboles, tormentas eléctricas).
		Fallas por defectos de fabricación
		Ciberataques de negación de servicio (DoS)
		Ciberataques de tipo randómico.
		Ciberataques bajo alteraciones de lectura de sensor acotadas (ABSRA)
		Ciberataques de inyección de datos falsos
		Ciberataques con sesgo positivo o negativo
Rompimiento de elementos mecánicos por descargas atmosféricas y/o congelamiento.		
Salidas fijas de sensores por ruido electromagnético		

Causa fenomenológica	Fallas naturales	Cortocircuitos originados por causas medioambientales (animales, árboles, tormentas eléctricas)
		Rompimiento de elementos mecánicos por descargas atmosféricas y/o congelamiento
		Degradación térmica
		Degradación química
		Corrosión mecánica por condiciones atmosféricas y ambientales
		Agrietamiento de piezas mecánicas por contaminación.
		Pérdidas de fluidos y fugas de combustible en celdas de combustible por contaminación y corrosión
	Fallas por causas humanas	Fallas en interruptores por mala operación
		Celdas en cortocircuito y circuito abierto por falta de mantenimiento
		Cortocircuitos por mala operación
		Fallas de disparos erróneos de protecciones por mala calibración o programación
		Fallas de disparos erróneos de protecciones por cableado y conexiones erróneas
		Ciberataques de negación de servicio (DoS)
		Ciberataques de tipo randómico
		Ciberataques bajo alteraciones de lectura de sensor acotadas (ABSRA)
		Ciberataques de inyección de datos falsos
		Ciberataques con sesgo positivo o negativo

Fase de creación u ocurrencia	Fallas conceptuales	Fallas de disparos erróneos de protecciones por mala calibración o programación
		Fallas de circuitos electrónicos
		Fallas de disparo erróneo de protecciones
		Falsa operación de actuadores por fallas en cableado
		Fallas por defectos de fabricación
	Fallas operacionales	Celdas y otros elementos en cortocircuito
		Celdas y otros elementos en circuito abierto
		Ciberataques de negación de servicio (DoS)
		Ciberataques de tipo randómico
		Ciberataques bajo alteraciones de lectura de sensor acotadas (ABSRA)
		Ciberataques de inyección de datos falsos
		Ciberataques con sesgo positivo o negativo
		Cortocircuitos por mala operación
		Sobrecargas
		Corrosión y degradación mecánica
		Puntos calientes
		Fallas en cojinetes, rulimanes, cigüeñales, estatores, rotores y demás elementos mecánicos
		Pérdidas de fluidos y fugas de combustible en celdas de combustible
		Degradación térmica
		Degradación química
Cortocircuito de vinculo DC a tierra		

Persistencia	Fallas permanentes	Celdas y otros elementos en cortocircuito
		Celdas y otros elementos en circuito abierto
		Corrosión y degradación mecánica
		Puntos calientes
		Fallas en cojinetes, rulimanes, cigüeñales, estatores, rotores y demás elementos mecánicos
		Pérdidas de fluidos y fugas de combustible en celdas de combustible
		Degradación térmica
		Degradación química
		Fallas de encapsulado
		Fallas de circuitos electrónicos
		Pérdida de conductividad
		Agrietamiento de piezas mecánicas
		Salidas sesgadas de sensores y actuadores
		Fallas de disparo erróneo de protecciones
		Fallas Temporales
	Sobrecargas	
	Ciberataques de negación de servicio (DoS)	
	Ciberataques de tipo randómico	
	Ciberataques bajo alteraciones de lectura de sensor acotadas (ABSRA)	
	Ciberataques de inyección de datos falsos	
	Ciberataques con sesgo positivo o negativo	
	Cortocircuitos en máquinas y terminales	
	Cortocircuitos originados por causas medioambientales (animales, árboles, tormentas eléctricas)	
Falsa operación de actuadores		
Operación tardía de actuadores		