Vulnerability Assessment of a Large Electrical Grid by New Graph Theory Approach

J. Beyza, J. M. Yusta, G. J. Correa and H. F. Ruiz, *Senior Member, IEEE*

***Abstract*— In previous research a novel methodology to assess structural vulnerability was proposed and applied in IEEE test system and high voltage transmission networks of 94 buses, by using graph theory to investigate various risk scenarios that can trigger cascading failures. In this paper, we ratify the application of this methodology in larger networks by applying a case study on the transmission network 230 and 400 kV of Mexico. The events of cascading failures are simulated through two elimination strategies: by deliberate attacks on critical nodes or by random errors. Iterations are performed by running successive N-1 contingencies on a network that is constantly changing its structure with the elimination of each node. The power flows are not necessary and only the calculation of the graph statistical parameter "geodesic vulnerability" is required. This reduces the computation time and leads to a comparative analysis of structural vulnerability.**

***Keywords*— Vulnerability, power systems, scale-free graphs, complex network, critical infrastructures.**

I. INTRODUCCIÓN

EL FUNCIONAMIENTO de las sociedades modernas depende de sistemas cada vez más complejos e interdependientes, entre otros electricidad, agua, transporte, telecomunicaciones, etc. Estos sistemas esenciales se consideran *infraestructuras críticas* dado que son activos vitales para cada país y la reducción de su operatividad o su destrucción tendría un efecto debilitante sobre la economía y la seguridad ciudadana [1].

Las infraestructuras, en especial los sistemas eléctricos de potencia, pueden estar sujetos a amenazas y riesgos de diferentes tipos, ocasionando que el ataque origine una falla en un componente o activo de la red eléctrica y este, a su vez, cause que la potencia sea redirigida a sus nodos adyacentes, que a su vez pueden verse sobrecargados y redirigir la potencia a sus nodos adyacentes haciendo que también fallen. A este efecto de propagación de las fallas se le denomina *fallas en cascada* [2]. Las amenazas y los peligros pueden ser desastres naturales, condiciones meteorológicas adversas, fallas técnicas, factores humanos, conflictos laborales, ciberataques, terrorismo, actos de guerra, etc. La sensibilidad a tales amenazas y peligros se denomina *vulnerabilidad* [3,4], un concepto que se utiliza para caracterizar la falta de robustez y resiliencia de un sistema. En esta situación, la *robustez* significa que la infraestructura mantendrá su función intacta cuando se expone a las perturbaciones, y la *resiliencia* implica que el sistema puede adaptarse para recuperar una nueva posición estable después de una contingencia [4].

Con el objetivo de evaluar la vulnerabilidad en un sistema de potencia es de suma importancia cuantificar el grado de impacto que pueden ocasionar las fallas en cascada. Entre los criterios más utilizados se encuentran los análisis de contingencias $n-1$ y $n-t$ [4,5]. Por otro lado, algunos autores [6] sugieren asemejar los sistemas de potencia a un grafo de libre escala, lo cual permite tener una representación más cercana del sistema en estudio. En ese sentido, los modelos construidos sobre teoría de grafos proporcionan una nueva visión para pensar en los sistemas eléctricos de potencia como un grafo.

La teoría de grafos o teoría de redes complejas [6,7] facilita el análisis y la visualización de los comportamientos físicos de muchos sistemas. La definición de grafos de libre escala propuesta inicialmente por [6] fue seguida por la aplicación de nuevos conceptos de medidas estadísticas, análisis de vulnerabilidad y estimación de resiliencia, con aplicaciones en sistemas eléctricos de potencia, redes informáticas y otros problemas de ingeniería [7-9]. Por otra parte, en [10] se formuló el problema de fallas en cascada en grafos de libre escala mediante el modelado de una estrategia de eliminación de nodos de una red basada en el *grado nodal* [11].

En [4,12] se justificó que las medidas estadísticas de la teoría de grafos (*clustering*, *grado de conexión*, *distancia geodésica*, *distribución nodal*) son adecuadas para llevar a cabo la evaluación de la vulnerabilidad de un sistema eléctrico de potencia y en particular para el análisis de fallas en cascada. Otros investigadores han utilizado medidas alternativas para modelos de redes complejas, por ejemplo en [13], donde se sugiere el uso de indicadores de *eficiencia geodésica* para analizar fallas en cascada. Otro enfoque para evaluar la resiliencia de la red eléctrica es el formulado en [14] y [15] que proponen medir el *betweenness* entre los nodos del grafo.

J. Beyza, Programa de Graduados e Investigación en Ingeniería Eléctrica, Instituto Tecnológico de Morelia, México, jbbcia4@hotmail.com.

J. M. Yusta, Departamento de Ingeniería Eléctrica, Universidad de Zaragoza, España, jmyusta@unizar.es.

G. J. Correa, Facultad de Ingenierías, Fundación Universitaria Luis Amigó, Medellín, Colombia, gabriel.correahe@amigo.edu.co.

H. F. Ruiz, Programa de Graduados e Investigación en Ingeniería Eléctrica, Instituto Tecnológico de Morelia, México, hfruiz53@yahoo.com.mx.

Entre los modelos de la red eléctrica con grafos merece la pena mencionar algunos estudios llevados a cabo en los países nórdicos [4] [14] [16] y en la red eléctrica europea continental [17], en los que se muestran las ventajas de usar indicadores topológicos (*clustering*, *distancia geodésica*, *eficiencia geodésica*). A su vez, en [18] se estudian las redes eléctricas de Italia, Francia y España con el cálculo de la medida de centralidad de *grado de nodo*, y parámetros estadísticos como *coeficiente de agrupamiento, diámetro de la red y eficiencia*. En [19] se evalúa el funcionamiento de una red mediante el indicador de *eficiencia geodésica* y en [20] se presenta un modelo híbrido entre teoría de grafos y teoría de juegos para definir estrategias de protección.

En [21] y [22] se aplica una novedosa metodología para evaluar la vulnerabilidad estructural de redes eléctricas prescindiendo de la realización de flujos de carga. Sin embargo, los autores aplicaron el método solo a redes de prueba IEEE y redes reales de 94 buses. En nuestro trabajo se pretende ratificar esta técnica de análisis de vulnerabilidad estructural y los nuevos índices de grafos aplicados en una red eléctrica de tamaño considerablemente superior, tomando como caso de estudio la red de transmisión en 230 y 400 kV de México. Se somete la red a simulación de fallas en cascada mediante dos estrategias de eliminación de nodos (errores aleatorios y ataques deliberados) y se determina cómo afecta a la desconexión de la demanda eléctrica de los usuarios considerando tres casos con distintas topologías.

El artículo está organizado de la siguiente manera: la Sección II introduce la metodología de estudio, así como el concepto de grafos de libre escala y su equivalente en los sistemas eléctricos de potencia. La Sección III describe los casos de estudio analizados y muestra los resultados de la simulación de los modelos propuestos de análisis de fallas en cascada. Finalmente, en la Sección IV se resumen las conclusiones finales del artículo.

II. METODOLOGÍA DE ESTUDIO PARA EL ANÁLISIS DE FALLAS EN CASCADA EN SISTEMAS ELÉCTRICOS DE POTENCIA

La gran aplicación en los últimos años de la teoría de grafos, también conocida como teoría de redes complejas [7], es debido a que permite fácilmente la representación abstracta de un sistema como un grafo con medidas estadísticas, así como la evaluación de los efectos de cada topología en su robustez ante diferentes tipos de ataques y fallas.

Matemáticamente una red compleja es representada como un grafo $G(V,E)$ que consiste en un conjunto de V nodos o vértices, representando los componentes de la red, y un conjunto E de líneas o enlaces representando la interacción o relación entre los nodos o componentes [23]. Los enlaces corresponden a un conjunto de pares de la forma (i,j) tal que $i,j \in E$.

Los estudios sobre la desintegración de redes de libre escala mostrados en [8] demostraron el desempeño que tiene la red compleja ante eventos de eliminación de nodos, ya sea mediante errores aleatorios o ataques deliberados. El análisis de estas contingencias que conducen a fallas en cascada en redes libres de escala precisa el uso de parámetros estadísticos de grafos que permitan medir la funcionalidad de la red.

A. Vulnerabilidad Geodésica

En [21] se demuestra que el índice de *vulnerabilidad geodésica* tiene relación directa con el índice de desconexión de cargas *PLS.* Este índice estadístico de grafos permite medir de una manera adecuada la funcionalidad de un grafo frente a contingencias, dado que permite normalizar la eficiencia geodésica y hacer un balance en el proceso de evolución de la eliminación de nodos en una red eléctrica respecto del caso base previa a la aparición de contingencias. Se calcula mediante la aplicación de la ecuación 1.

$$\bar{v} = 1 - \frac{\Sigma_{i \neq j}\left(\frac{1}{d_{ij}^{LC}}\right)}{\Sigma_{i \neq j}\left(\frac{1}{d_{ij}^{BC}}\right)} \tag{1}$$

Donde:

d_{ij}^{LC}= Distancia geodésica entre los pares de nodos del grafo de libre escala, después de cada iteración de eliminación de un nodo.

d_{ij}^{BC}= Distancia geodésica entre los pares de nodos del grafo de libre escala, para el caso base.

La distancia geodésica describe la menor distancia directa entre dos nodos, mediante el conteo del número mínimo de nodos que deben recorrerse para unirlos [14].

El índice de vulnerabilidad geodésica $\bar{v}$ varía entre cero y uno, cuanto mayor sea este índice mayor será el impacto en la interrupción del suministro eléctrico.

B. Impacto en la conectividad de la red

El *impacto en la conectividad de la red* es el número de nodos que permanecen conectados al grafo de libre escala después de cada proceso de remoción. Se evalúa mediante la aplicación de la ecuación 2.

$$S = 1 - \frac{N^{LC}}{N} \tag{2}$$

Donde:

N^{LC} = Número de nodos que permanecen conectados en el grafo de libre escala después de una interrupción de nodo.

N = Número total de nodos en el caso base.

El índice de impacto en la conectividad de la red S varía entre cero y uno, entre más grande sea este índice mayor será el número de nodos aislados en la red eléctrica.

C. Procedimiento para evaluar la vulnerabilidad estructural en redes eléctricas

Partiendo de un sistema que opera en condiciones estables (caso base) se desarrolla un modelo dinámico de fallas en cascada. Se realiza mediante iteraciones sucesivas en las que se van eliminando nodos del grafo, lo que implica el cálculo

de contingencias $n-1$ de una red eléctrica que cambia constantemente su topología después de cada eliminación de un nodo. Cada remoción de nodo está asociada con una nueva contingencia y, por tanto, con una iteración en el proceso de desintegración de la red. La eliminación de un nodo implica también la eliminación de todos los enlaces del grafo conectados a él. El análisis de vulnerabilidad se realiza mediante el cálculo del índice de vulnerabilidad geodésica en función de la cantidad de nodos que quedan aislados ($f = S$), lo que permite obtener el impacto ocasionado sobre la red eléctrica por su desintegración ante distintos tipos de eventos [3]. Este impacto se relaciona con la cantidad de carga desconectada de la red [21].

La Fig. 1 muestra el algoritmo propuesto implementado en el software de Matlab® para evaluar la vulnerabilidad estructural a través de la evolución de los índices de vulnerabilidad geodésica $\bar{v}$ de la ecuación 1 y la fracción de nodos eliminados f de la ecuación 2. Obsérvese que para la implementación del algoritmo de la Fig. 1 no se requiere incluir todos los parámetros eléctricos de la red bajo análisis. Por lo tanto, la metodología propuesta implica una ventaja, ya que la mayoría de la información relativa a la topología de la red es pública, mientras que el acceso a los datos eléctricos es muy limitado. Las distancias geodésicas se calculan mediante el algoritmo de Bellman-Ford de trayectorias más cortas [26].

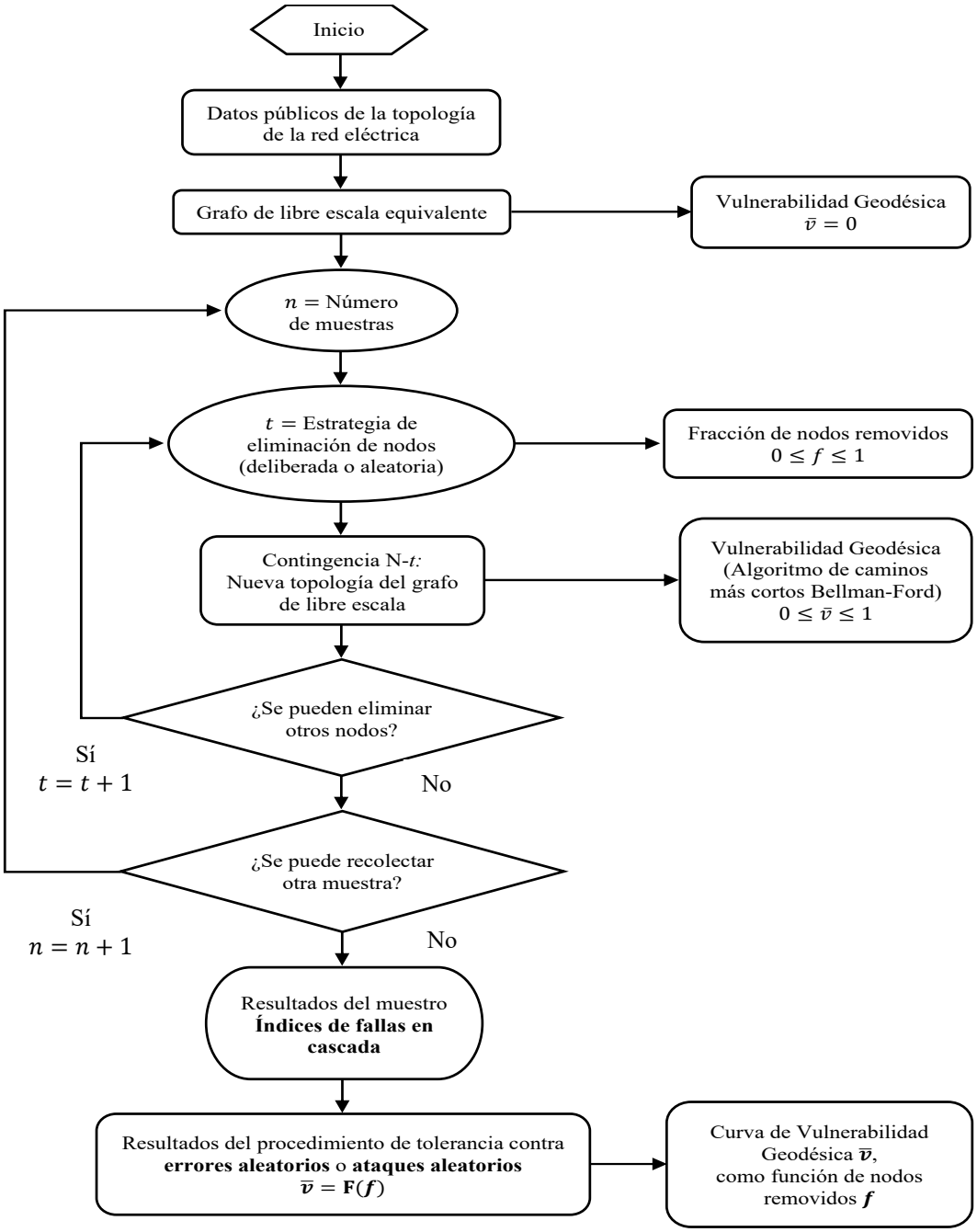


Figura 1. Diagrama de flujo para calcular la vulnerabilidad estructural en redes de alta tensión.

La simulación de las fallas en cascada se realiza mediante dos estrategias distintas de eliminación de nodos:

- Ataques deliberados: se eliminan sucesivamente los nodos más fuertemente conectados en orden descendente de grado nodal.
- Errores aleatorios: se eliminan nodos al azar. De acuerdo al teorema del límite central, es necesario repetir más de 30 veces cada experimento para obtener una muestra estadística idónea [24].

Por último, una característica del algoritmo desarrollado permite la identificación de los nodos que están aislados. Cada paso de iteración tiene en cuenta la existencia de estos nodos para el correcto cálculo del impacto sobre la conectividad de la red por el índice S de la ecuación 2 representado como la fracción de nodos eliminados f. El código fuente de Matlab® completa su ejecución hasta que no sea posible eliminar más nodos del grafo.

D. Ejemplo de ilustración

Con el fin de ilustrar la aplicación del algoritmo de la Fig. 1 en el cálculo de la vulnerabilidad estructural mediante teoría de grafos en redes eléctricas, el primer paso consiste en representar al sistema de potencia como un grafo de libre escala.

La Fig. 2 muestra la representación topológica propuesta de una red simple de cinco nodos, en comparación con la representación tradicional que solo considera nodos y enlaces [21,22,27]. La red resultante está compuesta por 18 nodos y 20 enlaces.

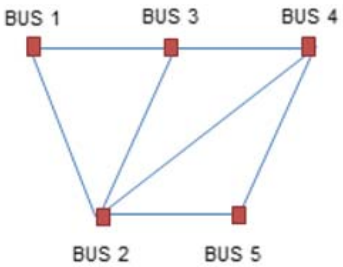
Considérese ahora a modo de ilustración la estrategia de eliminación de nodos mediante ataques deliberados (aquellos llevados a cabo por personas mal intencionadas, actos de vandalismo, ciberataques, etc.,), para este caso solo se necesita una muestra. En la Tabla I se observa el grado nodal, es decir el número de enlaces (k) que son incidentes a cada uno de los nodos de la red de libre escala del modelo propuesto de la Fig. 2.

TABLA I
GRADO NODAL DEL MODELO PROPUESTO (RED DE CINCO NODOS)

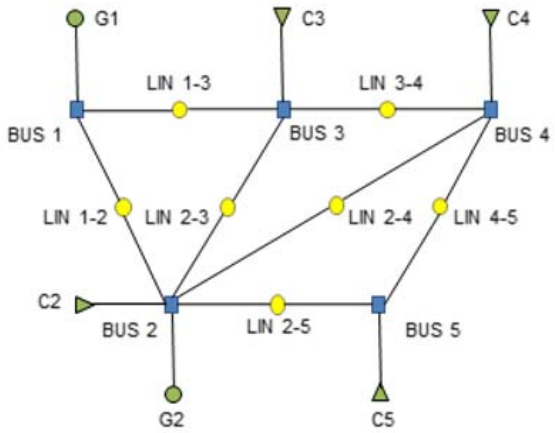
Nombre	Nodos	Grado nodal (k)
BUS 1	1 (slack)	3
BUS 2	2	6
BUS 3	3	4
BUS 4	4	
BUS 5	5	3
LIN 1-2	6	2
LIN 1-3	7	
LIN 2-3	8	
LIN 2-4	9	
LIN 3-4	10	
LIN 4-5	11	
LIN 2-5	12	
G1	13	1
C2	14	
G2	15	
C3	16	
C4	17	
C5	18	

A continuación, en cada paso de iteración (t) se elimina un nodo fuertemente conectado en orden descendente de grado nodal, comenzando por aquel que tenga el mayor número de enlaces incidentes, y además se calculan paralelamente los índices de vulnerabilidad estructural representados mediante las ecuaciones 1 y 2. Obsérvese que dichos cálculos corresponden únicamente al conjunto que contenga al nodo slack, e ignorando todos aquellos sub-grafos y nodos aislados que se formen durante el proceso iterativo.

En la Fig. 3 se ilustra el proceso de desintegración de la red de cinco nodos. Nótese que cuando se elimina inicialmente el Bus 2 $(t = 1)$ la red se divide en ocho grupos independientes, de ellos siete nodos sin enlaces. A continuación se procede a remover, del grupo que contiene en su conjunto al nodo slack, el siguiente nodo (Bus 3) en la línea de ataque de grado nodal $(t = 2)$. Es importante resaltar que, de los grupos anteriores, tan solo uno de ellos contiene al nodo slack. Debido a eso, se



REPRESENTACIÓN TOPOLÓGICA TRADICIONAL DE UN SISTEMA DE POTENCIA



MODELO PROPUESTO DE EL SISTEMA DE POTENCIA COMO UNA RED DE LIBRE ESCALA

Figura 2. Representación propuesta de una red eléctrica como un grafo de libre escala (red de cinco nodos).

debe tener presente que en la siguiente iteración (t) el nodo a eliminar se encuentre dentro de este mismo conjunto como se evidencia en $t = 3$. El proceso iterativo finaliza una vez que no haya más nodos que eliminar o bien el nodo slack se encuentre aislado $(t = 4)$.

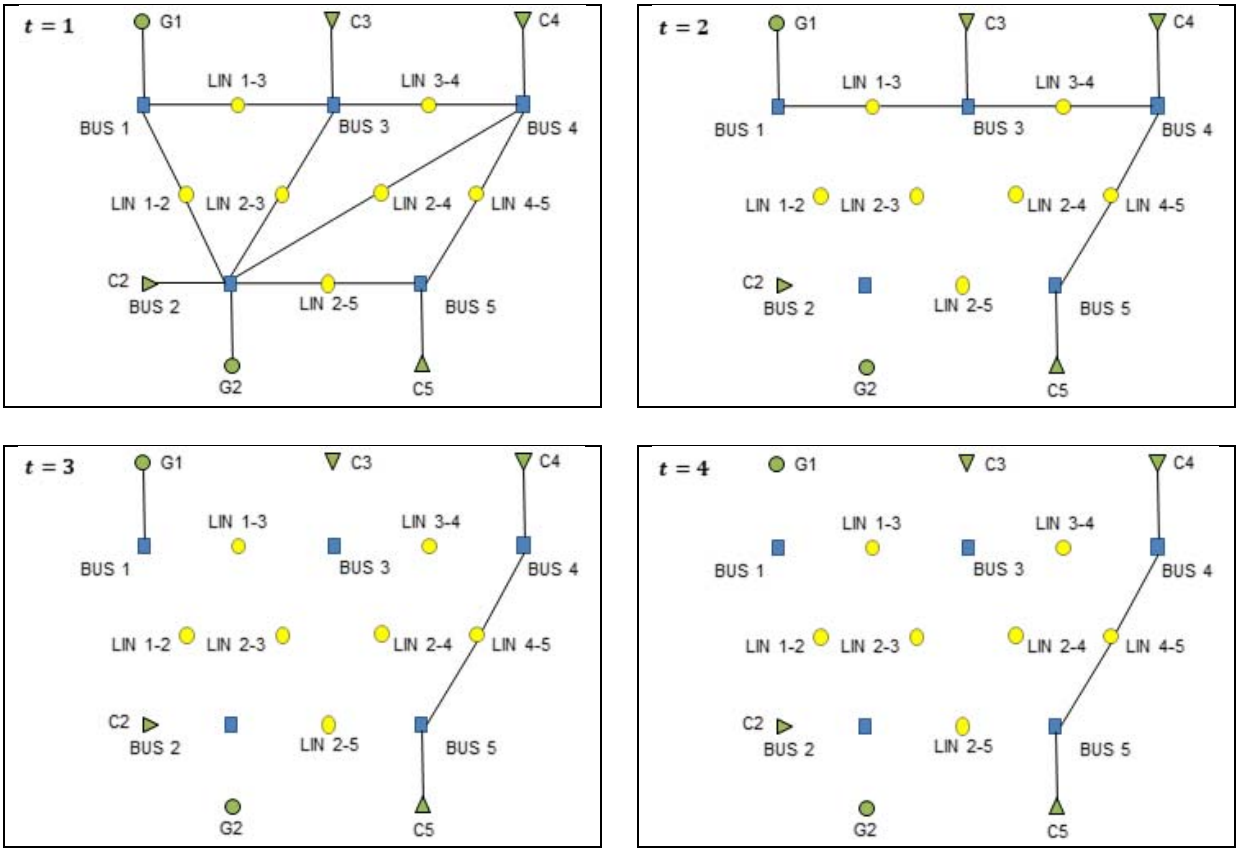


Figura 3. Proceso de desintegración de la red de cinco nodos mediante el algoritmo propuesto.

En la Tabla II se muestran los parámetros de vulnerabilidad estructural calculados según las ecuaciones 1 y 2 en cada paso de iteración (t) del proceso de desintegración de la red de la Fig. 3. La curva de vulnerabilidad geodésica de la Fig. 4 se construye con base en los resultados obtenidos en la eliminación de los nodos de la red mostrados en la Tabla II.

TABLA II
ÍNDICES DE VULNERABILIDAD ESTRUCTURAL PARA LA RED DE CINCO NODOS

Iteración (t)	Nodos en el grafo	f (%)	$\overline{v}$
1 (caso base)	18	0	0
2	11	38.88	0.6370
3	2	88.88	0.9847
4	1	94.44	1.0

En la Fig. 4 se puede observar que la eliminación de un $f \approx$39% de los nodos tiene un impacto muy alto sobre el sistema. Esto ilustra que todos aquellos ataques dirigidos contra los nodos con un grado de conectividad muy alto representarán una caída de funcionamiento de la mayor parte de la red eléctrica. Adicionalmente, cuando se pierde más del 88% de los nodos se obtiene una pérdida casi total del sistema de potencia.

Como se evidencia en este ejemplo, la metodología propuesta es muy útil para evaluar la vulnerabilidad estructural en redes de transmisión sin necesidad de recurrir a la aplicación de parámetros eléctricos, ya que tan solo basta conocer la topología de la infraestructura que se analiza y además el tiempo computacional requerido es muy pequeño. Adicionalmente, la estrategia de eliminación de nodos de manera aleatoria sigue la misma metodología de estudio que el caso de ejemplo, con la consideración que es necesario repetir más de 30 veces cada experimento para obtener una muestra estadística idónea [24].

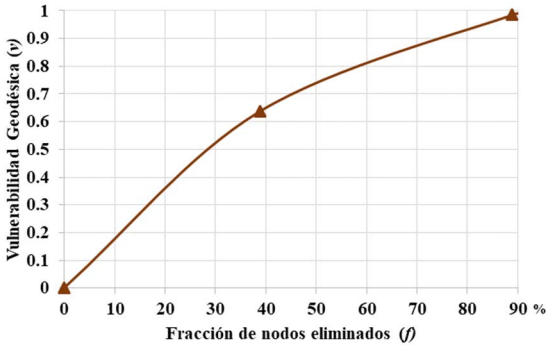


Figura 4. Curva de vulnerabilidad geodésica de la red de cinco nodos del ejemplo de ilustración.

III. CASOS DE ESTUDIO

La Fig. 5 representa la red troncal del Sistema Eléctrico Mexicano de 230 y 400 kV formada por 406 nodos. Sin embargo, frente a la representación tradicional de los sistemas de potencia como grafo de libre escala donde comúnmente los nodos del grafo representan los buses del sistema y los enlaces las líneas de transmisión [6], se propone un grafo de la red eléctrica de México compuesto por 1,620 nodos, donde éstos representan no solo los buses sino también las líneas eléctricas, transformadores, cargas, generadores, etc. De esta manera, siguiendo el modelo de representación propuesto en la Fig. 2, se consideran como nodos del grafo todos los activos del sistema de transmisión y no solamente los buses, lo cual eleva el grado de complejidad del problema, pero ofrece la posibilidad de un análisis de vulnerabilidad del sistema mucho más completo y detallado.

La vulnerabilidad estructural del sistema eléctrico de México se evaluará por un lado de acuerdo a la topología actual de la red de transmisión, y por otro lado de acuerdo a las nuevas topologías de la red que resultarían de la aplicación de los planes de expansión previstos [25]. Por lo tanto, se consideran tres casos de estudio:

- Caso 1: Evaluación de la vulnerabilidad estructural sobre el estado actual de la red (caso base), sin considerar los sistemas aislados de la península de Baja California. Se aplicará el procedimiento de la Sección II, apartado C al grafo de 1,620 nodos propuesto en la parte introductoria de esta Sección III.

- Caso 2: Evaluación de la vulnerabilidad estructural sobre una topología de la red mejorada de acuerdo al plan de expansión [25]. Se considera solamente la construcción de nuevas líneas de transmisión, sin interconectar los sistemas aislados de la península de Baja California, lo cual corresponde a un grafo de 1,773 nodos.

- Caso 3: Evaluación de la vulnerabilidad estructural según los planes de interconexión de los sistemas aislados de la península de Baja California [25]. La metodología se aplica aquí al grafo resultante de añadir las dos líneas de interconexión planificadas al grafo del caso 1, sumando el nuevo grafo un total de 1,765 nodos.

A. Distribución de Grado Nodal y Parámetros Estadísticos en el grafo de libre escala

La distribución de grado nodal permite estandarizar las redes complejas, donde varios nodos con gran número de conexiones se convierten en puntos clave en la red. En la Fig. 6 se observa la distribución de grado nodal del grafo de libre escala del Sistema Eléctrico Mexicano en 230 y 400 kV. También se incluye la representación de la distribución de grado nodal para las topologías de los casos 2 y 3, de acuerdo con el plan indicativo de expansión de la red [25].

La distribución de grado nodal $P(k)$ presentada en la Fig. 6 indica la probabilidad de que un nodo elegido al azar en el análisis tenga exactamente k conexiones [6]. En el caso 1 la probabilidad de que un nodo del grafo tenga un grado de conexión k=1 es $P(k)$=0.009, lo que significa que el 9% de los nodos de la red tienen solo una conexión con otros nodos de la red. El valor k=1 se refiere a los nodos en el grafo que quedan en antena, situación que corresponde normalmente a centrales de generación o centros de carga. Sin embargo, un 36% de nodos tienen un grado de conexión k=2 y un 10% de nodos de la red tienen un grado k=3.

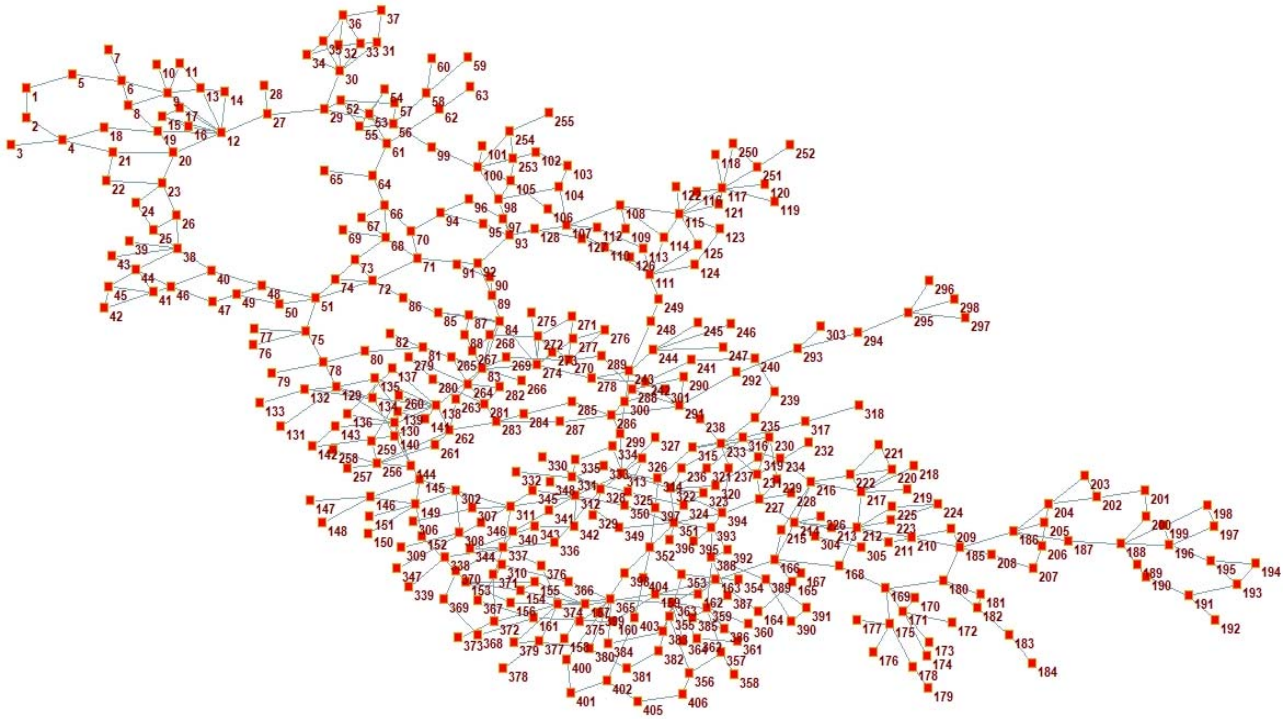


Figura 5. Representación esquemática del Sistema Eléctrico Mexicano de 230 y 400 kV.

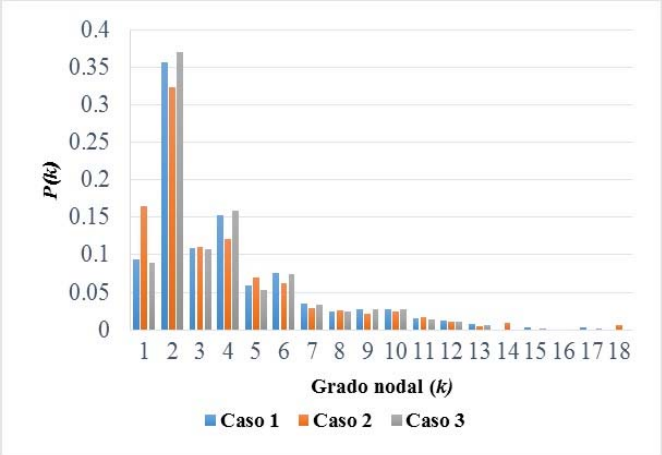


Figura 6. Distribución de grado nodal en los casos de estudio.

El valor k=2 corresponde típicamente a la representación en el grafo de aquellos nodos que corresponden a las líneas de transmisión [22]. Analizando la Red Mexicana para k=2, se observa una disminución de $P(k)$ en el caso 2 respecto al caso 1, lo cual es coherente ya que la expansión de la red en el caso 2 se realiza añadiendo algunas nuevas líneas eléctricas en nodos existentes, lo que disminuye la proporción de nodos en el grafo de tipo k=2 y aumenta en otros nodos, sobre todo de tipo k >14.

Comparando el caso 3 con el caso 1 se observa que tienen un comportamiento similar en $P(k)$. El enlace de la península de Baja California al sistema nacional de transmisión en el caso 3 provoca solo un ligero aumento en los nodos de tipo k=2 y k=4. Por otro lado, la distribución de grado nodal $P(k)$ en el caso 3 disminuye respecto al caso 2 para k=3, pero aumenta para k=4 lo que significa que las nuevas líneas y subestaciones se conectan preferentemente en nodos con alto grado de conectividad.

Desde el punto de vista del grafo, existe una pequeña cantidad de nodos que por su elevado número de conexiones son fundamentales y su ausencia podría acelerar una falla en cascada del resto de la red.

Para facilitar la comprensión del enunciado anterior, en la Fig. 7 se representa la subestación número 83, con los respectivos valores del grado nodal en los elementos que lo conforman. Con propósitos de ilustración el índice k indica el número de enlaces totales (líneas de transmisión en el sistema de potencia) que son adyacentes entre el nodo en cuestión y cada uno de los nodos de destino.

Como se evidencia en la Fig. 7, el nodo 83 tiene un grado nodal total de k=17, por lo cual debe considerarse como un nodo crítico en el análisis de vulnerabilidad del sistema. Adicionalmente, se deben definir estrategias de protección para este tipo de nodos que por su gran conectividad son blancos fáciles de ataques, o bien su pérdida podría repercutir en la operación de la red eléctrica.

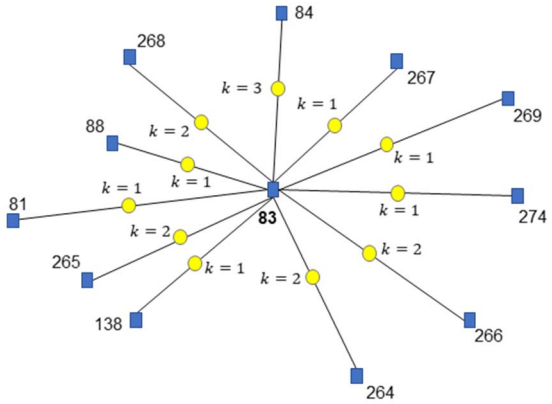


Figura 7. Valores de grado nodal en cada uno de los enlaces de la subestación número 83 de la Red Mexicana.

B. Vulnerabilidad ante errores aleatorios

Los errores aleatorios son aquellos que están relacionados con escenarios de riesgos de naturaleza aleatoria, como fenómenos naturales, fallos humanos involuntarios o fallos técnicos en equipos y hardware de la red [3].

Los resultados de las curvas de la Fig. 8 corresponden a cada uno de los casos de estudio descritos al comienzo de la Sección III, obtenidos como el promedio de los cálculos realizados mediante contingencias $n-1$ en la desintegración aleatoria completa de la red en 35 experimentos independientes [24].

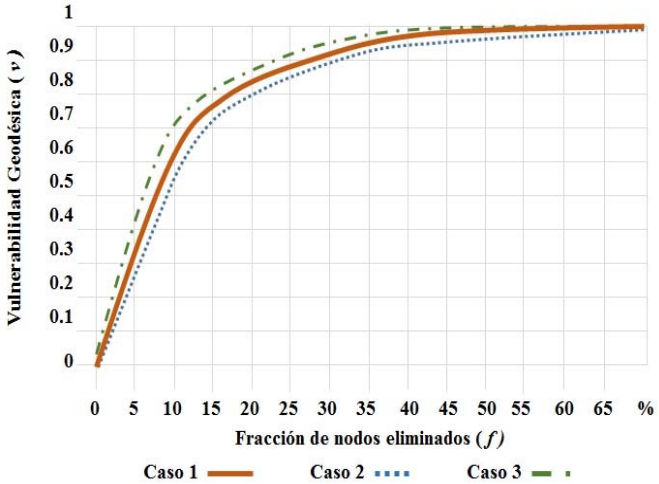


Figura 8. Curva de Vulnerabilidad Geodésica ante errores aleatorios.

Si se comparan en la Fig. 8 las curvas del caso 1 (caso base del sistema) con el caso 2 (adición de nuevas líneas), se observa que en el caso 2 se obtiene una ligera mejora en los resultados correspondientes a la vulnerabilidad geodésica para una misma fracción de nodos eliminados. Por otro lado, al comparar gráficamente las curvas de la Fig. 8 para el caso 1 y el caso 3, se evidencia que la curva del caso 3 está siempre por encima de la curva del caso 1, lo que corresponde a un empeoramiento de la robustez del sistema al añadir la interconexión de la península de Baja California.

En la Tabla III se muestran algunos resultados correspondientes a la eliminación de una determinada cantidad de nodos en la red (*f*) y su impacto sobre la desconexión de cargas del sistema mediante el índice de vulnerabilidad geodésica ($\bar{v}$).

TABLA III
IMPACTO EN LA DESCONEXIÓN DE CARGA ELÉCTRICA DE LOS USUARIOS ANTE ERRORES ALEATORIOS (VULNERABILIDAD GEODÉSICA ($\bar{v}$) vs FRACCIÓN DE NODOS ELIMINADOS (*f*))

	f=5%	*f*=10%	*f*=20%	*f*=30%
$\bar{v}_{caso1}$	0.287	0.557	0.828	0.904
$\bar{v}_{caso2}$	0.286	0.545	0.807	0.903
$\bar{v}_{caso3}$	0.353	0.578	0.893	0.907

Como se observa en la Tabla III, los valores del índice de vulnerabilidad geodésica obtenidos en el caso 2 para fracciones de nodos eliminados f=10% y f=20% resultan ligeramente inferiores a los obtenidos en el caso 1, lo que indica que el aumento de mallado de la red mejora la robustez del sistema ante errores aleatorios.

Sin embargo, al comparar en la Tabla III los resultados de vulnerabilidad geodésica del caso 1 con los del caso 3, se deduce un empeoramiento en la robustez de la red. Esto se explica debido a que la interconexión de los sistemas aislados de la península de Baja California se realiza únicamente mediante dos enlaces añadidos a un mismo nodo de alta conectividad. La pérdida de este nodo crítico ocasiona que los dos sistemas de Baja California queden aislados del resto del sistema interconectado del país, contribuyendo a una mayor pérdida de carga en el sistema eléctrico en su conjunto.

Las conclusiones obtenidas son similares a las extraídas en otros estudios realizados en redes de transmisión mucho más pequeñas [16] [22], lo que permite validar la metodología en redes de tamaño superior.

C. Vulnerabilidad ante ataques deliberados

Considerando los ataques deliberados como aquellos perpetrados por personas malintencionadas, actos de terrorismo, ciberataques, actos de vandalismo, etc., la construcción de la curva de vulnerabilidad geodésica se realiza a partir de los resultados obtenidos en la eliminación de los nodos de la red de acuerdo a su grado nodal en orden descendente, comenzando por el que esté más conectado.

En la Fig. 9 se puede observar que la eliminación de un pequeño número de nodos tiene un impacto muy alto sobre el sistema, mucho mayor que para la misma fracción de nodos de la Fig. 8. Esto significa que un ataque dirigido contra nodos o subestaciones con alto grado de conectividad representa una caída de funcionamiento de la mayor parte de la red eléctrica y, en consecuencia, se genera rápidamente un *"blackout"* con graves consecuencias.

Al comparar el caso 1 (correspondiente al caso base) y el caso 2 (adición de nuevas líneas) las curvas de vulnerabilidad son muy similares, apenas se aprecia una leve mejora de robustez. Por otro lado, la comparación de las curvas resultantes del caso 1 y del caso 3 (adición de la península de Baja California al caso 1) evidencia que la red expandida es claramente más vulnerable frente a los ataques deliberados.

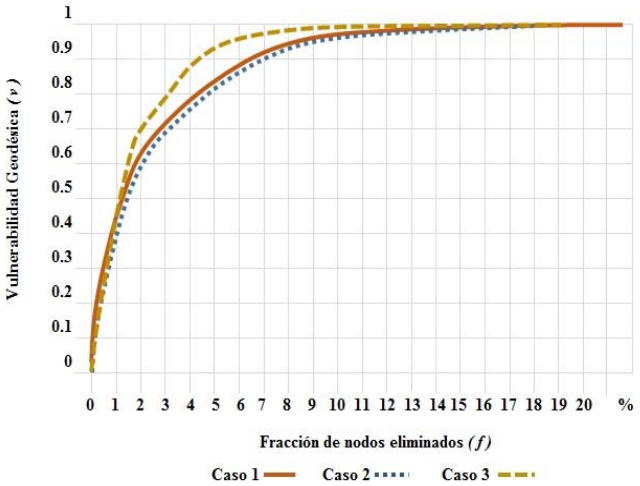


Figura 9. Curva de Vulnerabilidad Geodésica ante ataques deliberados.

En la Tabla IV se muestran algunos datos de las consecuencias asociadas a la eliminación de una fracción de nodos con alto grado de conectividad, y su impacto sobre la desconexión de cargas del sistema (vulnerabilidad $\bar{v}$).

TABLA IV
IMPACTO EN LA DESCONEXIÓN DE CARGA ELÉCTRICA DE LOS USUARIOS ANTE ATAQUES DELIBERADOS (VULNERABILIDAD GEODÉSICA ($\bar{v}$) vs FRACCIÓN DE NODOS ELIMINADOS (*f*))

	f=0.5%	*f*=1%	*f*=2%	*f*=5%	*f*=10%
$\bar{v}_{caso1}$	0.182	0.438	0.639	0.836	0.953
$\bar{v}_{caso2}$	0.182	0.428	0.626	0.834	0.952
$\bar{v}_{caso3}$	0.189	0.447	0.656	0.929	0.985

Si se comparan los casos 1 y 2 apenas se observan mejoras en la tolerancia contra ataques deliberados, salvo en f=1% y f=2% donde el índice de vulnerabilidad en el caso 2 es ligeramente mejor que en el caso 1, lo que indica que la estrategia de mejorar el mallado de la red no es tan efectiva para el caso de los ataques deliberados.

Por otro lado, de los valores de la Tabla IV se observa que el caso 3 es más vulnerable a los ataques deliberados que el caso 1. Esto se explica porque al extender el sistema incorporando la península de Baja California se construye una red menos compacta y la eliminación de los nodos de mayor conectividad tiene como efecto el aumento dramático de la distancia geodésica entre los nodos de la red que quedan conectados. Esta observación deducida de los resultados de las simulaciones realizadas es coherente con la topología de la red del caso 3, que interconecta la península de Baja California con el resto del sistema nacional mediante dos enlaces a la subestación del bus 41 de la red de transmisión, por lo cual la pérdida de este nodo aumenta la vulnerabilidad del sistema al implicar el aislamiento de toda la península.

Los resultados del análisis comparativo de vulnerabilidad ante ataques deliberados realizado sobre la red de transmisión de México son muy similares a los obtenidos en estudios anteriores sobre redes más pequeñas [16] [22].

IV. CONCLUSIÓN

La aplicación de la teoría de redes complejas en los sistemas eléctricos de potencia ha demostrado su utilidad para evaluar la vulnerabilidad estructural de la red de transmisión sin la necesidad de aplicar parámetros eléctricos. Los resultados obtenidos en este trabajo, aplicando por primera vez esta metodología a redes de gran tamaño, apoyan la conclusión de investigaciones anteriores de que el uso de la teoría de grafos, utilizando los índices adecuados, puede ser apropiado para el análisis comparativo de topologías de red ante distintos tipos de contingencias. Gracias a esa metodología se obtiene una visión conceptual de todos los activos de una red eléctrica y una implementación computacional más rápida, ya que solo es necesario conocer la distribución topológica de la infraestructura.

REFERENCIAS

[1] US Department of Homeland Security, «Homeland Security,» September 22, 2015. [Online]. Available: https://www.dhs.gov/homeland-security-presidential-directive-7. [Access: January 13, 2018].

[2] Paul Hines and Seth Blumsack, «A Centrality Measure for Electrical Networks," Proceedings of the 41st Hawaii International Conference on System Science,» *Proceedings of the 41st Hawaii International Conference on System Sciences,* pp. 1-8, 2008.

[3] Gerd Kjølle, Ruth Helene Kyte, Matz Tapper and Kenneth Hänninen, «Major storms-main causes, consequences and crisis management,» *22nd International Conference on Electricity Distribution*, Stockholm, June 10-13, 2013.

[4] Åke J. Hölmgren, «Using Graph Models to Analyze the Vulnerability of Electric Power Networks,» *Risk Analysis,* vol. 26, nº 4, pp. 955-969, 2006.

[5] A. Gómez-Expósito, Análisis y operación de sistemas de energía eléctrica, Madrid: McGraw-Hill. (ISBN: 9788448135928), 2002.

[6] A. Barabási and R. Albert, «Emergence of Scaling in Random Networks,» *Science,* vol. 286, nº 5439, pp. 509-512, 1999.

[7] M. E. J. Newman, «The Structure and Function of Complex Networks,» *Society for Industrial and Applied Mathematics,* vol. 45, nº 2, pp. 167-256, 2003.

[8] R. Albert and AL. Barabási, «Statistical mechanics of complex networks,» *Review of Modern Physics,* vol. 74, pp. 47-97, 2002.

[9] AT. Murray, TC. Matisziw and TH. Grubesic, «Critical network infrastructure analysis: interdiction and system flow,» *Journal of Geographical Systems,* vol. 9, nº 2, pp. 103-117, 2007.

[10] AE. Motter and YC. Lai, «Cascade-based attacks on complex networks,» *Phys Rev E Stat Nonlin Soft Matter Phys,* vol. 66, pp. 1-4, 2002.

[11] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, «Error and attack tolerance of complex networks,» *Phys A: Stat Mech and its Appl,* vol. 340, pp. 388-394, 2004.

[12] Åke J. Hölmgren, «A Framework for Vulnerability Assesment of Electric Power Systems,» in *Advances in Spatial Science,* Springer, Berlin, Heidelberg, ADVSPATIAL, 2007, ch. 3, pp. 31-55.

[13] G. Chen, ZY. Dong, DJ. Hill and GH. Zhang, «An improved model for structural vulnerability analysis of power networks,» *Phys A: Stat Mech and its Appl,* vol. 388, nº 19, pp. 4259-4266, 2009.

[14] J. Johansson, «Risk and Vulnerability Analysis of Interdependent Technical Infrastructures,» PhD. Dissertation, Department of Measurement Technology and Industrial Electrical Engineering, Lund University, Sweden, 2010.

[15] K. Wang, BH. Zhang, Z. Zhang, XG. Yin and B. Wang, «An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load,» *Phys A: Stat Mech and its Appl,* vol. 390, pp. 4692-4701, 2011.

[16] E. Jenelius, «Graph Models of Infrastructures and the Robustness of Power Grids,» M.S. thesis, Center for Safety Research, Royal Institute of Technology, Stockholm, 2004.

[17] RV. Solé, M. Casals, B. Murtra and S. Valverde , «Robustness of the European Power Grids under intentional attack,» *Physical Review E,* pp. 1-7, 2008.

[18] V. Rosato, S. Bologna and F. Tiriticco, «Topological properties of high-voltage electrical transmission networks,» *Electric Power Systems Research,* vol. 77, pp. 99-105, 2007.

[19] G. Chen, ZY. Dong, DJ. Hill, GH. Zhang and KQ. Hua, «Attack structural vulnerability of power grids: A hybrid approach based on complex networks,» *Phys A: Stat Mech and its Appl,* vol. 389, nº 3, pp. 595-603, 2010.

[20] Åke J. Hölmgren, E. Jenelius and J. Westin, «Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks,» *IEEE Transactions on Power Systems,* vol. 22, nº 1, pp. 76-84, 2007.

[21] GJ. Correa and JM. Yusta, «Grid vulnerability analysis based on scale-free graphs versus power flow models,» *Electric Power Systems Research,* vol. 101, pp. 71-79, 2013.

[22] GJ. Correa and JM. Yusta, «Structural vulnerability in transmission systems: Cases of Colombia and Spain,» *Energy Conversion and Management,* vol. 77, pp. 408-418, 2014.

[23] J. Reichardt, *Structure in complex network*, Springer-Verlag Berlin Heidelberg, 2009.

[24] Minitab Inc, «Soporte de Minitab 17,» Minitab Inc, 2016. [Online]. Available: http://support.minitab.com/es-mx/minitab/17/topic-library/basic-statistics-and-graphs/introductory-concepts/basic-concepts/central-limit-theorem/. [Access: January 13, 2018].

[25] SENER, «Programa de Desarrollo del Sistema Eléctrico Nacional 2016 - 2030. PRODESEN,» Secretaría de Energía, México, 2016.

[26] JL. Gross, J. Yellen. *Handbook of graph theory.* New Tork, USA, CRC Press, 2004.

[27] Stagg and El-Abiad, «Load Flow Studies,» in *Computer Methods in Power Systems Analysis,* USA, McGraw Hill, 1968, pp. 270-276.

Jesus Beyza received his Bachelor's degree of electromechanical engineering from the Instituto Tecnologico de la Costa Grande, Mexico in 2014, and the MSc. in electrical engineering from the Instituto Tecnologico de Morelia, Mexico in 2017. In 2014, he received the National Award of ANFEI (National Association of Schools of Engineering). He is currently pursuing a PhD. in electrical engineering. His areas of interest are vulnerability of critical infrastructure, operation and control of power systems.

Jose M. Yusta received his Bachelor's degree of industrial engineering in 1994 and Ph.D. degree in electrical engineering in 2000 from the Universidad de Zaragoza, Spain. He is currently professor of Department of electrical engineering at Universidad de Zaragoza. From 2004 to 2007 he was vice-dean of Faculty of Engineering from Universidad de Zaragoza. His areas of interest are electricity markets and vulnerability analysis of critical infrastructure.

Gabriel J. Correa-Henao received his Bachelor's degree of electrical engineering and the MSc. in system engineering from the Universidad Nacional de Colombia in 2001 and 2004, respectively and Ph.D. degree in electrical engineering from the Universidad de Zaragoza, Spain in 2012. He is currently a lecturer and researcher at Faculty of Engineering in Universidad Luis Amigó, in Medellin, Colombia, with interests on distributed generation and power system security.

Hector Francisco Ruiz (M'78, SM'06) received his Bachelor's degree of electrical engineering from the Instituto Tecnologico de Morelia, Mexico in 1976, the MSc. in electrical engineering from the Instituto Tecnologico y de Estudios Superiores de Monterrey (ITESM) in 1977 and Ph.D. degree in electrical engineering from the University of Manchester, UK in 1992. He was founder of the "Graduate Program and Research in Electrical Engineering" from the Instituto Tecnologico de Morelia, Mexico, where he is currently professor. His areas of interest are power and distribution systems.