



RESILIENCIA Y VULNERABILIDAD DE SISTEMAS ELÉCTRICOS

Luis Alfonso Cárdenas Durán, Luis Alejandro Arias Barragán

**Fundación Universidad Autónoma de Colombia
Bogotá, Colombia**

Resumen

El presente artículo aborda la temática referente a la resiliencia y vulnerabilidad de los sistemas eléctricos ante eventos disruptivos tales como ataques cibernéticos o daños severos en la infraestructura por fenómenos naturales como sismos, vendavales e inundaciones entre otros. Los sistemas eléctricos son extremadamente necesarios para suplir las necesidades de la población en general, ya sea a nivel doméstico, industrial, comercial, de salud y seguridad; pero estos sistemas están propensos a sufrir algún tipo de vulnerabilidad, la cual puede ser a causa tanto de la naturaleza (clima, fauna y flora), como del ser humano (vandalismo y accidentes) y aspectos técnicos (fallas de equipos e interrupciones no-planificadas). Además de esto, también los bajos niveles de redundancia en la infraestructura generan afectación a un sistema eléctrico, aumentando así su nivel de vulnerabilidad, teniendo esto grandes consecuencias ya sean de índole técnico, social y político. La vulnerabilidad en las redes genera pérdidas millonarias en los diferentes países, traducidas en daños a equipos industriales, de networking y electrodomésticos.

Debido a la vulnerabilidad que existe en la red eléctrica, en todo su conjunto, se deben tomar medidas para que los fallos en sistemas eléctricos no sean tan severos, y que en caso de que llegase a suceder, se tengan opciones para mitigar, corregir y reparar rápida y eficientemente cuando estos se presenten. La resiliencia no se refiere exactamente a que la red nunca falle, sino a que una vez suceda, esta esté en la capacidad de mantener el servicio lo mejor posible y a la mayor cantidad de usuarios. La red deberá estar en capacidad de retornar a la normalidad lo más pronto posible y con la menor pérdida económica. En el sector eléctrico, la resiliencia se puede definir como la capacidad de un sistema de energía de tolerar perturbaciones, continuando con el suministro de energía a los consumidores.

Una alternativa para hacer un sistema resiliente es optar por incluir generación de energías renovables como apoyo a la red, convirtiendo al consumidor también en productor (prosumidor), de hecho, esta opción permitiría que un conjunto de prosumidores intercambie energía entre ellos y la red.

La propuesta que se muestra en el presente artículo implementa Plantas Virtuales de Potencia que se encargan de agrupar las fuentes de generación distribuida, elementos de almacenamiento y la gestión de las cargas de la red a través de elementos de control.

Palabras clave: resiliencia y vulnerabilidad; microrredes de energía; plantas virtuales de potencia

Abstract

The present article exposes the subject of Resilience and vulnerability of electrical systems to disruptive events such as cyber-attacks or severe damage to infrastructure due to natural phenomena such as earthquakes, windstorms, and floods, among others. Electrical systems are vital to meet the needs of the population in general, whether domestic, industrial, commercial, health or safety; but these systems are always willing to suffer some kind of vulnerabilities that can be caused by nature (climate, fauna and flora), human beings (vandalism and accidents) or technical aspects (equipment failures and unscheduled interruptions), in addition, the low levels of redundancy in infrastructure generate affectation to an electrical system, in consequence increasing its level of vulnerability, producing great consequences either of a technical, social or political nature. Vulnerability in these grids generate millions of losses in different countries, also translated to what is related damage to industrial, networking equipment and household appliances.

Due to the vulnerability that is present in the power grid, as a whole, procedures must be taken so that failures in electrical systems are not so brutal, and in case it could happen, there would be ways to mitigate, correct and repair quickly and efficiently when they occur. Resilience does not mean exactly to the grid never failing, but once it does, it will be able to keep up the service as best as possible to the greatest number of users. The grid must be able to revert to normality as soon as possible with the smallest economic loss. In the electricity sector, resilience can be well-defined as the ability of an energy system to endure disturbances, by continuing with the supply of energy to consumers.

an alternative to make a system resilient is by choosing renewable energies as support to the commercial grid, aiming the consumer as a producer (prosumer), in fact, this would allow a set of prosumers exchange energy between them and the grid.

The proposal presented in this article implements Virtual Power Plants; responsible for grouping distributed generation sources, storage elements and management of network loads through control elements.

Keywords: resilience and vulnerability; energy microgrids; virtual power plants



1. Introducción

El presente trabajo aborda la temática acerca del comportamiento de las redes eléctricas ante fluctuaciones o eventos disruptivos que amenacen el normal funcionamiento de las mismas; se indicará la importancia de tener en cuenta diferentes eventos que hacen vulnerables el sistema eléctrico, así como aquellos que amenacen la resiliencia del mismo.

Entre los eventos que hacen vulnerables los sistemas eléctricos sobresalen principalmente los del tipo APBI (alta probabilidad bajo impacto), en los cuales se tienen en cuenta las fallas propias de los equipos y dispositivos necesarios tanto para la generación o conversión de energía; estas fallas pueden estar asociadas al tiempo de uso, así como relacionados a problemas por envejecimiento, exposición al agua, polvo, etc.; además de este, también están los conocidos como BPAI (baja probabilidad alto impacto), los cuales están directamente asociados a las afectaciones de tipo climático, ya sean relacionados al clima o posiblemente a algún tipo de desastre natural; es por ello que se busca desde diferentes frentes tratar de volver esas redes más resilientes ante los diversos escenarios que se puedan presentar, tratando en lo posible generar la menor afectación posible a los consumidores de esa energía.

Como propuesta de solución se plantea la utilización de plantas virtuales de potencia que se encargaran de la gestión de las fuentes de generación distribuida (GD), los sistemas de almacenamiento energético y los controladores de las cargas de los usuarios.

El presente artículo se encuentra estructurado de la siguiente manera: Inicialmente, una breve introducción sobre la temática de las redes ante eventos disruptivos; en la sección 2 se abordan los conceptos de vulnerabilidad y resiliencia; en la sección 3 se muestra la estrategia propuesta para mejorar la vulnerabilidad y resiliencia en sistemas eléctricos; en la sección 3 los resultados y en la sección 4 las conclusiones.

2. Vulnerabilidad y resiliencia

Los sistemas eléctricos de potencia, principalmente se componen por líneas de transmisión, las cuales se encuentran expuestas a todo tipo de condiciones, haciéndose demasiado vulnerables y por ello pueden presentar alguna falla o disturbio en su funcionamiento; además de las líneas de transmisión, también se pueden presentar fallas tanto en las subestaciones de potencia como en las centrales eléctricas, y dichas fallas o disturbios se presentan por diferentes fuentes, las cuales se atribuyen principalmente a aquellas ocasionadas por factores externos como el clima, el medio ambiente e inclusive las provocadas por el vandalismo.

Según Hernández en su investigación enfocada a la vulnerabilidad en subestaciones de Cundinamarca (Colombia) determinó que estas presentan cierto grado de amenaza, y a las cuales calificó con valores que están entre media-baja y media-alta; esto para eventos relacionados a derrames potenciales de aceite, explosiones, incendios, atentados, robos y tormentas eléctricas (Hernández Romero, 2005). Y es que es tan importante tener al día en mantenimiento y monitoreado el sistema eléctrico nacional, ya que, de no hacerse, esto podría causar una falla de



gran importancia en el suministro de energía, es por ello que para el caso Venezuela y según lo reporto Díaz, a causa de la falta de mantenimiento en las redes tanto del estado Aragua como en otros estados del país, los cortes de electricidad son cada vez más constantes y frecuentes, tanto así que ocurren varias veces en un día, esto debido a la falta de mantenimiento de las termoeléctricas y de las subestaciones (Díaz, 2019).

En el trabajo de Cortés y Melo, para el análisis de la vulnerabilidad de sistemas de potencia, proponen una metodología de optimización binivel entera-mixta, y para ello se deben tener en cuenta las variables del entorno geográfico con sus respectivos grados de incertidumbre, y así los operadores de sistemas de potencia determinarían que elementos del sistema tienen mayor grado de vulnerabilidad y de acuerdo a esto se podrán tomar medidas con el fin de proteger los componentes críticos para la operación del sistema (Cortés & Melo Rodríguez, 2016). Para monitorear las redes eléctricas, es necesario tener un sistema de seguridad robusto, esto para tratar de disminuir al máximo los riesgos cibernéticos, y es que según Gálvez, la seguridad a nivel informático es muy importante, ya que con ella se trata de conseguir que las instalaciones eléctricas sean más fiables, y con ello se busca reducir el tiempo de inactividad en el caso de que se presente algún tipo de falla (Gálvez Fernández, 2019).

Tal y como lo indican otros autores, por ejemplo, en el caso de las redes inteligentes, las cuales basan dicho monitoreo en un sistema de comunicaciones sobre IP, y haciendo referencia en el trabajo de Ángeles, García y Velasco, con este tipo de comunicación se aumenta la vulnerabilidad de la red, debido a los riesgos cibernéticos, y es por ello que cualquier falla en la red eléctrica sin importar que sea intencional o no, puede llegar a ser muy devastador, ya que cualquier persona que incluso tenga pocos conocimientos de ingeniería inversa, estaría en capacidad de dejar sin alimentación a uno o varios usuarios que se encuentren conectados a una Red inteligente (Ángeles Camacho et al., 2013).

Y aunque hasta el momento se ha tocado el tema tanto de vulnerabilidad en los componentes de la red, como de la parte de comunicación y seguridad, hay un componente que es muy susceptible a los cambios climáticos, y es el relacionado a la generación de energía por medio de recursos hídricos, y es por esto que Esquivel, Grunwaldt, Paredes y Flores, en su Monografía que publicaron ante el BID, agregan que para el caso de Centroamérica, por su ubicación geográfica, se hace extremadamente vulnerable en cuanto a la generación de energía hidroeléctrica debido a que esa región se ve afectada por cambios climáticos, sequías y huracanes; además esa vulnerabilidad que afecta los sistemas eléctricos de Centroamérica, se puede medir evaluando la sustentabilidad teniendo en cuenta diferentes dimensiones (económicas, sociales, ambientales, políticas) incorporando en ellas los efectos del cambio climático determinando, al menos cualitativamente, sus efectos (Esquivel et al., 2016).

Varios autores recalcan la importancia de la automatización en los sistemas eléctricos, es el caso de Inampúes quien a su vez destaca el hecho de que un sistema eléctrico tiene cierto grado de resiliencia cuando se anticipa a un peligro, y es por eso que toma importancia el hecho de que un sistema eléctrico puede ser robusto y frágil a la vez, pues aunque se pueden rediseñar para que absorban mejor las perturbaciones y estén en capacidad de funcionar en una gran variedad de condiciones, también es cierto que pueden ser demasiado frágiles ante amenazas no previstas e



inesperadas (Inampués Borda, 2014). Este tema también fue abordado por Rojas, quien en su tesis con la cual recomienda sobre cómo mejorar la resiliencia en la red eléctrica de Santo Domingo, indica la importancia de realizar procesos de automatización, para lo cual se requiere realizar una inversión para lograr una renovación en la infraestructura existente, además resalta que al conocer a fondo el comportamiento de la red eléctrica, se tendría una operación más eficiente de la misma (Rojas Selmo, 2014).

Es por esto que impulsar el uso e implementación de energías renovables, es tan importante como el poder integrarla a una microrred, y tal como lo indican Molina, Paredes y Serrano en su investigación, ellos exaltan la importancia de los ESS (energy storage systems) o sistemas de almacenamiento de energía para servir de respaldo a los sistemas de (GD) y microrredes, ya que estos dispositivos de almacenamiento garantizan una alta potencia y densidad de energía, con mucha eficiencia en la conversión y respuesta tanto dinámica como estática en términos de potencia y tensión; desde luego siendo apoyados por sistemas electrónicos de conversión y regulación de esta energía, con ello garantizando que puedan aportar esta energía de manera muy rápida y eficiente pudiendo mejorar así las condiciones de seguridad, confiabilidad, resiliencia y calidad de energía en las microrredes (Molina et al., 2019).

Dentro de algunas propuestas revisadas se ha planteado la utilización de redes redundantes en anillo, la utilización de microrredes, la implementación de sistemas SCADA para monitoreo en tiempo real entre otras (Sagintayev & Collins, 2017) (Battistelli & Conejo, 2014) (Sridhar et al., 2012). Para la presente propuesta investigativa se ha planteado hacer uso de una planta virtual de potencia VPP (Yu et al., 2015) (Wojaszczyk, 2012) (Asmus, 2010) para realizar el monitoreo y gestión de diferentes fuentes de generación distribuida GD, y con ello aprovechar esas energías renovables que además de ser amigables con el medio ambiente, se pueden generar prácticamente en cualquier lugar y desde el mismo momento en que se instala su correspondiente infraestructura.

3. Algoritmo de gestión para la estrategia propuesta y secuencia de operación

En la figura 1 se puede observar el diagrama de flujo de la estrategia propuesta haciendo uso de la planta virtual de potencia VPP. Inicialmente en la VPP a través de su sistema de adquisición captura diferentes datos tales como condiciones climatológicas, estado de la red eléctrica, estado y ubicación de elementos de gestión distribuida (GD), sistemas de almacenamiento energético y usuarios con cargas gestionables o controlables.

Una vez se tienen estos datos, se verifica la cantidad de energía que se tiene disponible en los diferentes puntos de GD, de sistemas de almacenamiento y el potencial ahorro a partir de la desconexión total o parcial de las cargas gestionables de algunos usuarios de la red.

En caso de que se presente alguna contingencia que requiera energía eléctrica y la planta virtual de potencia tenga información de excedente de energía por parte de algún GD, esta identificará las cargas críticas de la red que deben ser inicialmente abastecidas tales como hospitales, albergues para población vulnerable, centros de operación y logística ante un desastre. Posterior



a esta identificación la VPP coordinará la entrega de esta energía de forma óptima implementando algoritmos de despacho, buscando suplir hasta donde sea posible la contingencia presentada.

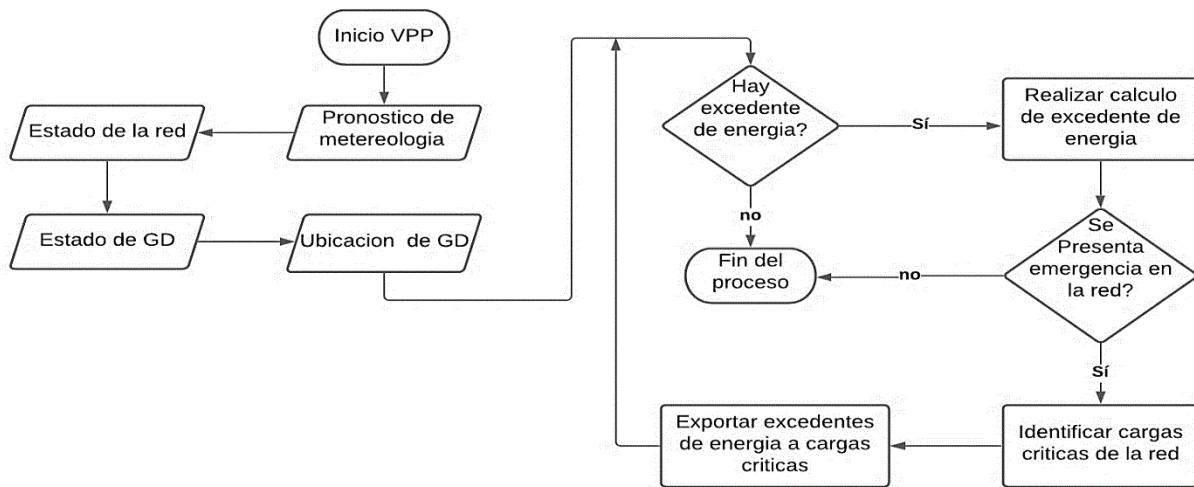


Figura 1. Algoritmo de gestión para la estrategia propuesta

La idea principal de la propuesta investigativa es poder trabajar de manera coordinada con entidades estatales como el Ministerio de minas y energía y con la Unidad Nacional para la gestión de Riesgo de Desastres(Bonanno & Capizzi, 2014).

4. Red eléctrica de pruebas

Como escenario de prueba, se tomó una red IEEE-34 en la que se encuentran los edificios a los que se van a gestionar el consumo energético y sus fuentes de autogeneración (Figura 2).

La tabla 1 muestra las características de la red probada y los niveles de potencia de las cargas.

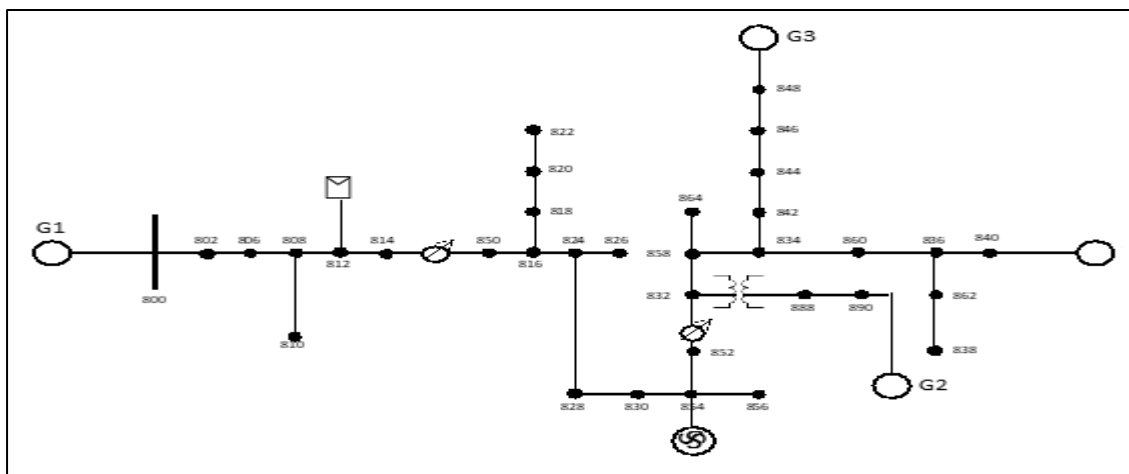


Figura 2. Red IEEE-34 utilizada como escenario de prueba.



Tabla 1. Parámetros de potencia para las cargas de la red IEEE-34 utilizadas,
Fuente: elaboración propia. Nota: En color gris se indican las cargas que poseen sistema de gestión.

Nodo de usuario	Potencia		Nodo de usuario	Power	
	Activa (kW)	Reactiva (kVAr)		Activa (kW)	Activa (kW)
816	5	2,5	824	24,5	12
842	5	2,5	806	27,5	14,5
864	5	2,5	802	27,5	14,5
856	5	2,5	846	34	17
854	5	2,5	840	47	31
828	5,5	2,5	830	48,5	21,5
832	7,5	3,5	836	61	31,5
810	8	4	822	67,5	35
808	8	4	848	71,5	53,5
862	14	7	820	84,5	43,5
838	14	7	834	89	45
818	17	8,5	860	174	106
826	20	10	844	432	329
858	24,5	12,5	890	450	225

5. Resultados

Se han realizado simulaciones mediante el software DigSilent, usando como prototipo un sistema de 34 nodos IEEE, en el cual se incluyó generación de energía mediante el uso de paneles fotovoltaicos, así como sistemas eólicos. Al simularse una falla en una línea de transmisión, se evidencia como satisfactoriamente estos sistemas pueden suplir energía a las cargas que se encuentran dentro de esas barras; para este caso en particular, se garantiza un nivel de energía estable en la barra 23, en la cual se encuentra la carga correspondiente al hospital El Tintal. En la figura 3 se observa el diagrama de red en el momento previo a la ocurrencia de una falla.

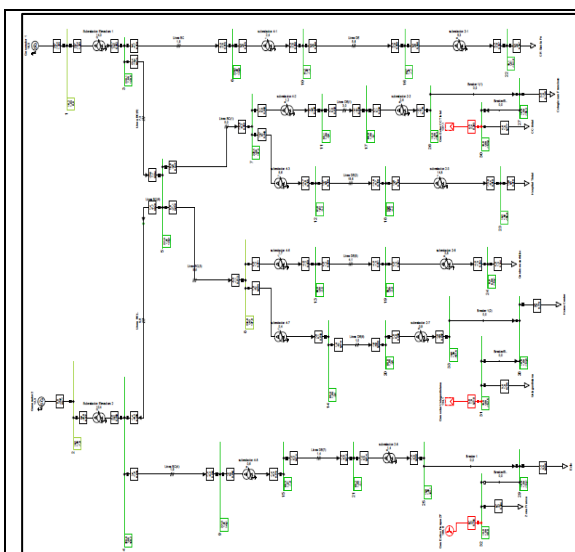


Figura 3. Red IEEE-34 antes de una falla

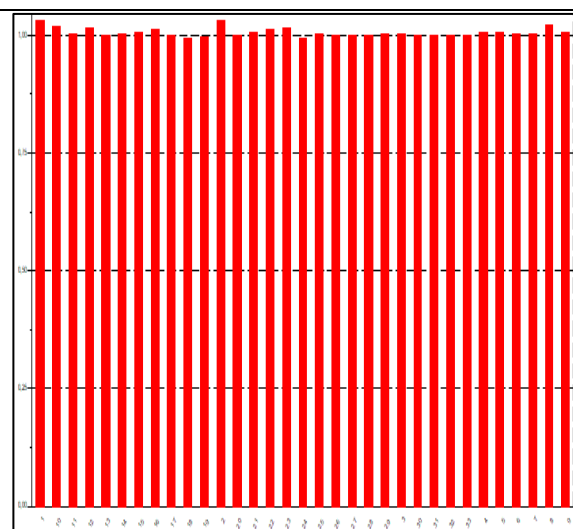


Figura 4. Magnitud de voltaje de las barras en p.u. antes de una falla

En la figura 4 se muestra que los perfiles de tensión en los diferentes barrajes de la red se mantienen dentro de límites óptimos del valor de tensión en p.u. (por unidad). Los niveles se encuentran en valor de 1.0 y ligeramente superior lo que muestra que la red se encuentra estable en cuanto al perfil de tensión se refiere(Orduña et al., 2012)(Rojas Cubides et al., 2014). Posteriormente, se procedió a simular una falla en un sector de la red de prueba (figura 5) y se analiza como el perfil de tensión de muchas barras se distorsiona incrementándose en aquellos puntos diferentes al sector de la falla (figura 6), lo cual puede acarrear inconvenientes de desbalance en cuanto al flujo de potencia se refiere(Kanwar et al., 2015)(Vaschetti et al., 2012).

Luego, se evaluó un escenario con la solución propuesta de implementación de una VPP que a través de su sistema de gestión ha coordinado la inclusión de recursos energéticos distribuidos (DER)(Lloret-Gallego et al., 2017)(Battistelli & Conejo, 2014)(A. Rahman et al., 2015) la conexión de las fuentes de GD en la zona afectada, la activación de sistemas de almacenamiento energético tales como acumuladores y baterías y la disminución de consumo de usuarios dentro de la zona de falla mediante el control de cargas gestionables. Con estas acciones se logra abastecer energéticamente las cargas críticas de la zona por un espacio de tiempo determinado en función a las capacidades de los DER y la rapidez en la respuesta que tengan las entidades estatales ante la contingencia.

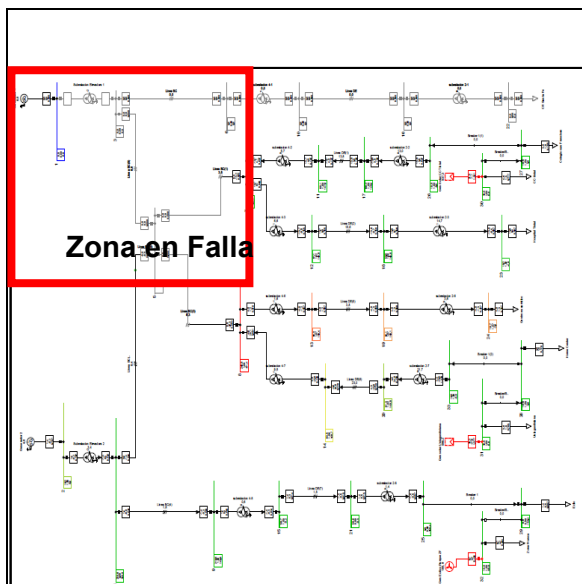


Figura 5. Red IEEE-34 con indicación de una afectada

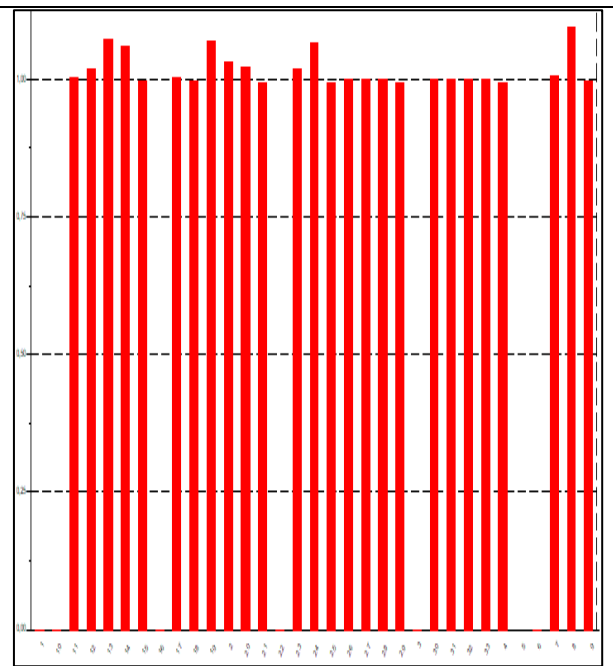


Figura 6. Magnitud de voltaje de las barras fuera de la zona de avería en p.u., después de una falla

En las figuras 7 se observa la red de prueba con la zona de falla gestionada por medio de la VPP. Como se evidencia la influencia de la gestión de la VPP no solo se limita a la activación de fuentes de GD en la zona de falla, sino que también permite que se controlen cargas que estén por fuera de la zona de falla físicamente, lo cual permite entre otros acopar mejor los flujos de potencia en los demás elementos de la red y estabilizar el perfil de tensión en los puntos de la red por fuera de la zona de avería. En la figura 8 se muestra como el perfil de tensión en los barrajes toman ahora



valores más estables en cuanto a incrementos de p.u se refiere. Hay que tener en cuenta que aún se presenta la falla tanto en la subestación elevadora 1 y en la barra número 5.

7. Conclusiones

Ante situaciones de avería o falla en la red se puede aprovechar la inclusión de DER gestionados mediante VPP en procura de incrementar la resiliencia de la red.

La mejora de los perfiles de tensión a partir de la utilización de VPP permite pensar que esta solución puede usarse no solo en regímenes de falla, sino también en situaciones que requieran regulación durante la operación normal de la red.

La mayor ventaja de la VPP radica en la posibilidad que tiene de agrupar los DER que poseen los usuarios con lo cual se garantiza la sostenibilidad en las soluciones gracias a la intervención de los usuarios de la red aportando sus recursos en el momento de respuesta ante la contingencia de la red para abastecer las cargas críticas.

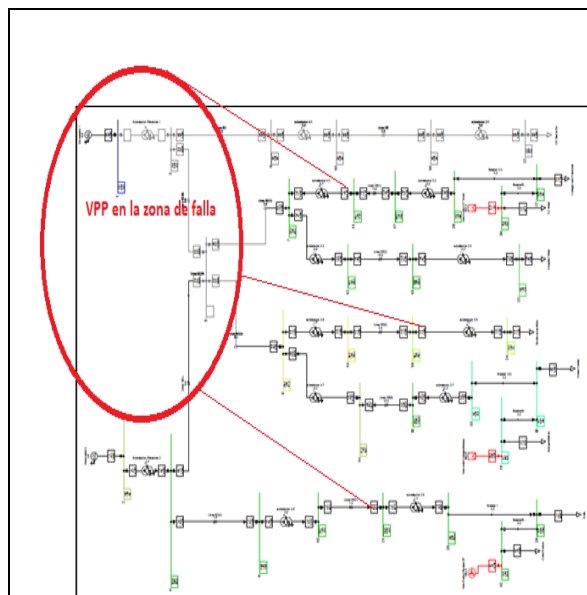


Figura 7. Red de prueba IEEE-34 nodos indicando la gestión de la zona de falla apoyada en una VPP

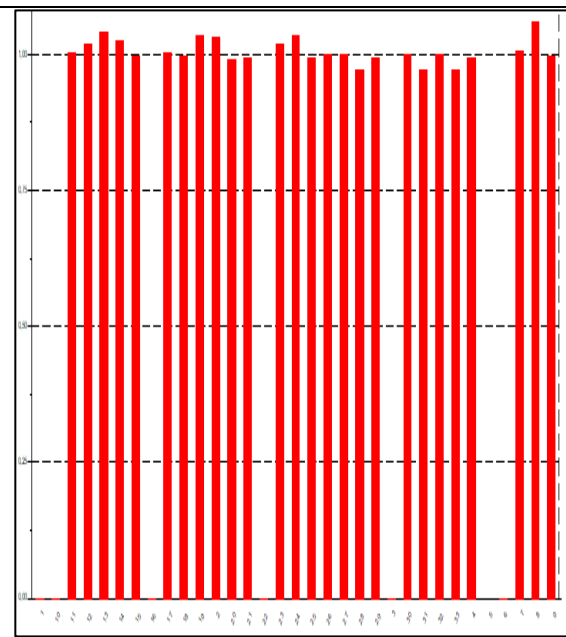


Figura 8. Magnitud de voltaje de las barras en p.u. utilizando la gestión de cargas mediante la VPP

8. Referencias

- A. Rahman, H., Majid, M. S., Rezaee Jordehi, a., Chin Kim, G., Hassan, M. Y., & O. Fadhl, S. (2015). Operation and control strategies of integrated distributed energy resources: A review. *Renewable and Sustainable Energy Reviews*, 51, 1412–1420. <https://doi.org/10.1016/j.rser.2015.07.055>
- Angeles Camacho, C., Garcia Martinez, M., & Velasco Ramirez, E. (2013). Redes de transmisión



- inteligente. Beneficios y riesgos. *Ingeniería Investigación y Tecnología*, 16(1).
- Asmus, P. (2010). Microgrids, Virtual Power Plants and Our Distributed Energy Future. *The Electricity Journal*, 23(10), 72–82. <https://doi.org/10.1016/j.tej.2010.11.001>
 - Battistelli, C., & Conejo, a. J. (2014). Optimal management of the automatic generation control service in smart user grids including electric vehicles and distributed resources. *Electric Power Systems Research*, 111, 22–31. <https://doi.org/10.1016/j.eprsr.2014.01.008>
 - Bonanno, F., & Capizzi, G. (2014). A novel cloud-distributed toolbox for optimal energy dispatch management from renewables in IGSs by using WRNN predictors and GPU parallel solutions. 1077–1084.
 - Cortés, C. A., & Melo Rodríguez, J. A. (2016). Análisis de vulnerabilidad de sistemas de potencia incluyendo incertidumbre en las variables con lógica difusa tipo 2. *Tectura*, 20(49). <https://doi.org/10.14483/udistrital.jour.tecnura.2016.3.a07>
 - Diaz, G. (2019, November). Vulnerabilidad del sistema eléctrico amenaza con otro apagón nacional. *Cronica Uno*.
 - Esquivel, M., Grunwaldt, A., Paredes, J. R., & Rodriguez Flores, E. (2016). VULNERABILIDAD AL CAMBIO CLIMÁTICO DE LOS SISTEMAS DE PRODUCCIÓN HIDROELÉCTRICA EN CENTROAMÉRICA Y SUS OPCIONES DE ADAPTACIÓN. *BID*.
 - Gálvez Fernández, L. (2019). *Ciberseguridad en las redes eléctricas*. Universidad carlos III de Madrid.
 - Hernández Romero, L. V. (2005). *EVALUACIÓN DEL RIESGO TECNOLÓGICO EN LAS SUBESTACIONES MT/MT DEL ÁREA DE DISTRIBUCIÓN CUNDINAMARCA DE CODENSA S.A. Y FORMULACIÓN DEL PLAN DE EMERGENCIAS PARA UNA SUBESTACIÓN PILOTO*. Universidad de La Salle.
 - Inampué Borda, J. C. (2014). *Integración de los Sistemas de Alerta de Tormentas Eléctricas en Redes Inteligentes*. Universidad Nacional de Colombia.
 - Kanwar, N., Gupta, N., Niazi, K. R., & Swarnkar, A. (2015). Simultaneous allocation of distributed resources using improved teaching learning based optimization. *Energy Conversion and Management*, 103, 387–400. <https://doi.org/http://dx.doi.org/10.1016/j.enconman.2015.06.057>
 - Lloret-Gallego, P., Aragüés-Peñalba, M., Van Schepdael, L., Bullich-Massagué, E., Olivella-Rosell, P., & Sumper, A. (2017). Methodology for the evaluation of resilience of ICT systems for smart distribution grids. *Energies*, 10(9), 1–16. <https://doi.org/10.3390/en10091287>
 - Molina, M. G., Paredes, L. A., & Serrano, B. R. (2019). Nuevo Paradigma de los Sistemas Eléctricos: Generación Distribuida y Microrredes Eléctricas. Un Vínculo de Accesibilidad a la Electricidad en América Latina y el Caribe. *EnerLAC*, 2(2), 110.
 - Orduña, I. F., Aponte, G., & Echeverry, D. F. (2012). Compensación paralelo de reactivos durante la prueba de aptitud al cortocircuito en transformadores de distribución. *Informacion Tecnologica*, 23(5), 47–56. <https://doi.org/10.4067/S0718-07642012000500006>
 - Rojas Cubides, H. E., Rivas Trujillo, E., & Jaramillo Matta, A. A. (2014). Aspectos técnicos y normativos para el monitoreo y medición de armónicos. *Ingeniería*, 19(2), 6–11. <https://doi.org/10.14483/udistrital.jour.reving.2014.2.a07>
 - Rojas Selmo, F. Y. (2014). *Mejora de la Resiliencia en la Red Eléctrica de Santo Domingo, República Dominicana*. Universitat Politècnica de Catalunya.
 - Sagintayev, Z., & Collins, N. (2017). Power to the People: Disaster Resilience support with advance energy storage systems. *Materials Today: Proceedings*, 4(3), 4555–4560. <https://doi.org/10.1016/j.matpr.2017.04.029>
 - Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber attack-resilient control for smart grid. 2012 *IEEE PES Innovative Smart Grid Technologies, ISGT 2012*, 1–3. <https://doi.org/10.1109/ISGT.2012.6175567>



- Vaschetti, J. C., Magnago, F., & Sauchelli, V. H. (2012). Control automático de voltaje en sistemas eléctricos de potencia basado en sistemas expertos. *Informacion Tecnologica*, 23(5), 69–84. <https://doi.org/10.4067/S0718-07642012000500008>
- Wojszczyk, B. (2012). Deployment of advanced Smart Grid solutions - Global examples & lessons learned. *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 1. <https://doi.org/10.1109/ISGT.2012.6175544>
- Yu, J., Jiao, Y., Wang, X., Cao, J., & Fei, S. (2015). Bi-level optimal dispatch in the Virtual Power Plant considering uncertain agents number. *Neurocomputing*, 167, 551–557. <https://doi.org/10.1016/j.neucom.2015.04.035>

Sobre los Autores

- **Luis Alfonso Cárdenas Durán.** Estudiante de último semestre de ingeniería electrónica de la Universidad Autónoma de Colombia. lcardenas.duran@fuac.edu.co.
- **Luis Alejandro Arias Barragán.** Ingeniero Electromecánico. Master of Science en Ingeniería Eléctrica, Magíster en Ciencias de la Información y Las Telecomunicaciones. Doctor en Ingeniería. Docente investigador del programa de Ingeniería Electromecánica de la Universidad Autónoma de Colombia. Correo: larias.barragan@fuac.edu.co lincarias@yahoo.com

Los puntos de vista expresados en este artículo no reflejan necesariamente la opinión de la Asociación Colombiana de Facultades de Ingeniería.

Copyright © 2021 Asociación Colombiana de Facultades de Ingeniería (ACOFI)

