RETOS EN MATERIA DE CIBERSEGURIDAD EN SMART GRIDS

Mónica Alonso, Hortensia Amarís, Sergio Pastrana, Jaime Turanzas y Lucía Gálvez, Universidad Carlos III de Madrid
Angel T. Ledo, Centro Universitario de la Guardia Civil

Resumen: En el proceso de digitalización de las redes eléctricas hacia las smart grids, el aumento de comunicación entre los dispositivos que la componen extiende los retos a los que se enfrentan los operadores de las redes eléctricas hasta el campo de la ciberseguridad. En el presente trabajo se muestran los principales retos en materia de ciberseguridad de las smart grids en tres ámbitos: (i) los sistemas de protección de las smart grids, atendiendo al impacto social derivado de la pérdida de una línea y el desabastecimiento de cargas, así como la posibilidad de provocar un colapso de tensión; (ii) los protocolos de comunicación entre dispositivos, dada la necesidad de salvaguardar la confidencialidad, veracidad y disponibilidad de la información intercambiada; y (iii) el marco legal, siendo necesario el desarrollo normativo ligado a las infraestructuras críticas.

Palabras clave: smart grids, ciberseguridad, intelligent electronics devices (IEDs), protocolos de comunicación, infraestructuras críticas.

INTRODUCCIÓN

Es extraña aquella actividad que provea cualquier servicio en la que no esté involucrada la presencia de la energía eléctrica o las tecnologías de la información y la comunicación (TIC). Estos dos sectores se ven claramente interrelacionados en el desarrollo de las Smart grids (figura 1), que suponen la confluencia de estos dos dominios tradicionalmente separados y distintos.

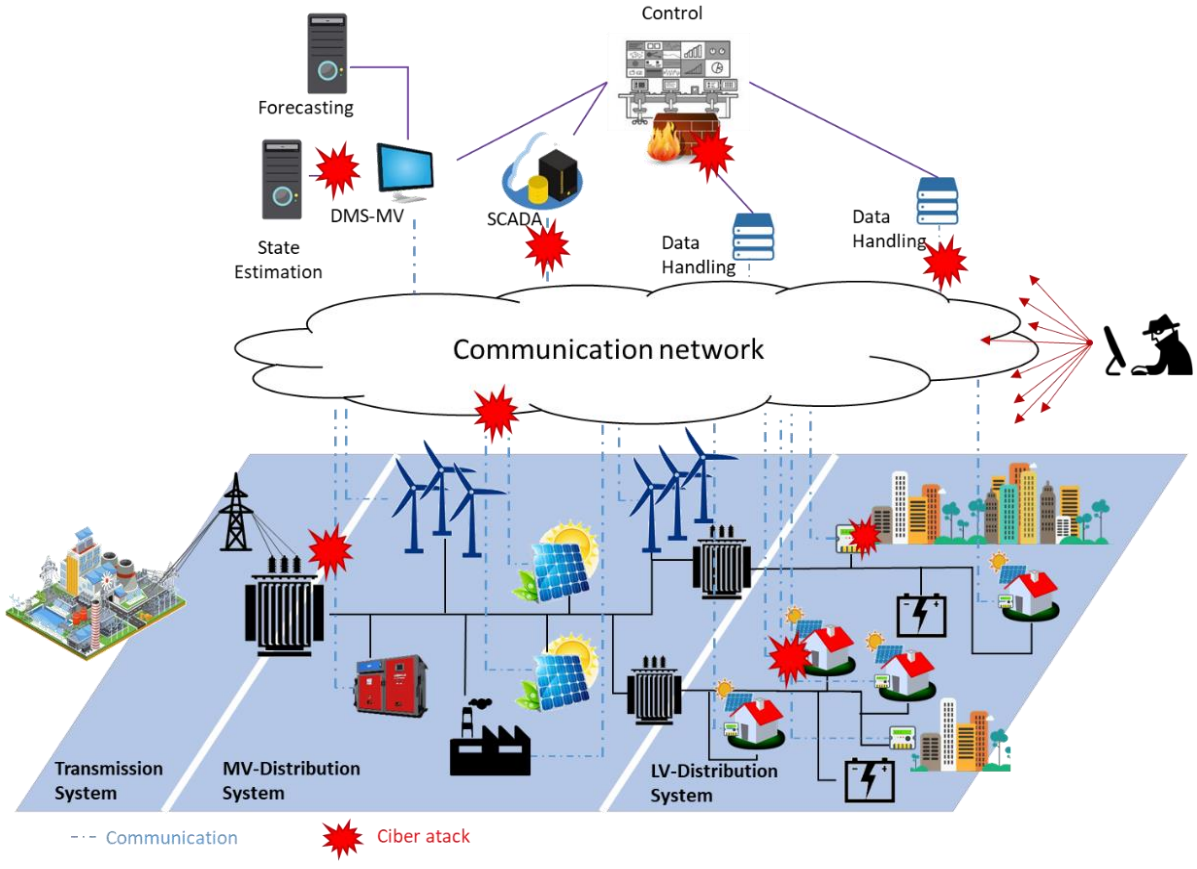

Figura 1. Conexión ciber-física en los sistemas eléctricos

Tanto el sector energético como el de las TIC son de vital importancia, porque la sociedad actual para su sostenimiento, bienestar y desarrollo precisa cubrir una serie de necesidades básicas como la alimentación, la salud, la educación o la justicia junto a otras más elaboradas y evolucionadas. Estas necesidades son cubiertas por unos servicios esenciales, considerados así porque una perturbación grave, el fallo o la caída en su prestación implicará un grave perjuicio a los ciudadanos. Las infraestructuras que dan soporte a estos servicios son amplias y complejas, en muchas ocasiones con dependencias entre sí, y la caída de una puede provocar un gran impacto en otras e incluso una caída en cascada bien en las mismas o en la degradación de los servicios que prestan.

Teniendo en cuenta lo expuesto anteriormente, los Estados tienen la responsabilidad de proteger las infraestructuras que proveen de los servicios esenciales a sus ciudadanos, conocidas como Infraestructuras Críticas (IC).

La integración de la nueva infraestructura cibernética con la infraestructura eléctrica tradicional abre un nuevo abanico de posibilidades, pero a la vez aparecen una serie de problemáticas en materia de seguridad. Los ciberataques en las smart grids tienen consecuencias que abarcan desde grandes pérdidas económicas hasta el propio bienestar social e integridad física de los habitantes de un país. Además, es importante destacar que, en las nuevas redes eléctricas inteligentes, el robo de la información intercambiada entre los diferentes dispositivos puede dar lugar a problemas de seguridad para los clientes, ya que la información substraída está clasificada como sensible. Uno de los ejemplos más representativos de la vulnerabilidad de las redes eléctricas que se ha podido constatar es el ataque cibernético en la red eléctrica ucraniana en 2015 con la pérdida de siete subestaciones de 110 kV y 33 subestaciones de 35 kV, lo que supuso el desabastecimiento de, aproximadamente, 225.000 clientes durante 6 horas (Hong et. al, 2019).

RETOS EN EL ÁMBITO DE LOS SISTEMAS DE PROTECCIÓN DE LAS SMART GRIDS

Como consecuencia de las medidas encaminadas a la descarbonización de los sistemas de potencia y la descentralización de la generación, los sistemas eléctricos de potencia están sufriendo grandes cambios en las últimas décadas. Las nuevas redes eléctricas inteligentes son complejos sistemas ciber-físicos en los que interaccionan los tradicionales sistemas físicos de generación, distribución y transporte de la energía eléctrica, con las Tecnologías de la Información y Comunicación empleadas para la captación de medidas, comunicación y procesado de la información en tiempo real. La incorporación de las TIC permite mejorar el control en tiempo real de las redes eléctricas convencionales, facilita la integración de nuevos elementos como la generación distribuida y los vehículos eléctricos, así como el desarrollo de nuevos métodos de gestión de la demanda, dotando a la red eléctrica de mayor flexibilidad, fiabilidad (reliability) y capacidad de recuperación (grid resilience) ante la aparición de posibles fallos en el sistema. En contrapartida a todas las ventajas que las TIC ofrecen a las redes eléctricas, varios blackouts en redes internacionales demuestran la vulnerabilidad de las nuevas redes eléctricas y la necesidad de analizar el impacto de un ciberataque en la componente física de la red eléctrica.

En el campo de la operación de las Smart grids, el National Electric Sector Cybersecurity Organization Resource establece los principales escenarios de fallo en función de 6 niveles funcionales a los que pueda ser dirigido el ciberataque: (i) la infraestructura de medida, (ii) los recursos energéticos distribuidos, (iii) los sistemas de monitorización, protección y control, (iv) el transporte eléctrico, (v) la gestión de la demanda (vi) y finalmente los sistema encargados de la gestión de las redes eléctricas de distribución (NIST, 2015).

Dentro del campo de la protección de las smart grids, los modernos relés digitales (IEDs) se han convertido en uno de los principales objetivos de los ciberataques, a través de la manipulación de datos produciendo lecturas falsas de las tensiones y corrientes en el sistema enviadas a los IEDs así como el retraso temporal en el envío de mensajes a los dispositivos de protección y apertura de las líneas (Liu et. Al, 2017). Las consecuencias de un ciberataque en un IED encargado de la protección de una red eléctrica pueden ser muy amplias: desde la desconexión de una línea y desabastecimiento de cargas, como consecuencia de la orden de apertura de un interruptor, hasta la pérdida en cascada de numerosas líneas que deriven en un colapso de tensión (Hong et. al, 2019), (Liu et. Al, 2017). Por lo tanto, todas las estrategias que permitan mejorar la robustez de los IEDs ante ciberataques es un aspecto de relevancia en el campo de las smart grids.

Ante esta nueva realidad de las smart grids, varios comités técnicos internacionales han creado grupos de trabajo, como el comité B5 de CIGRE o el IEEE PES Power System Relaying Committee Working Group C1 (Ward et. al, 2007), para analizar las vulnerabilidades que pueden aparecer en los modernos relés de protección (IEDs) al incrementar las comunicaciones por medio de las TIC. La norma IEC 61850 emplea mensajes GOOSE o valores reales (sample values,

SV) para la comunicación entre dispositivos, sin embargo, dichos mensajes no incluyen medidas de seguridad frente a ciberataques, por lo que la información contenida en dichos paquetes de comunicación es susceptible de ser suplantada, modificada o reproducida.

Las técnicas principales empleadas en las smart grids ante ciberataques se centran en el desarrollo de software antivirus y mejora del firewall, o bien en el desarrollo de sistemas de detección de intrusión. Recientemente, se están empezando a desarrollar nuevos algoritmos de detección de ataques en las protecciones IEDs empleando técnicas basadas en machine learning y deep learning (Xin et. al, 2018).

El objetivo principal de un sistema de detección de intrusión o ciberataque es determinar si la aparición de un evento en la red (por ejemplo, lectura de una medida "errónea" o una orden "falsa" de apertura de línea) es veraz o es un ataque a la smart grid. A lo largo de la literatura se pueden encontrar diferentes metodologías para la detección de anomalías en smart grids, desde algoritmos metaheurísticos, hasta modernos desarrollos basados deep o machine learning, así como el empleo de teoría de juegos.

Una vez que se ha producido un ciberataque es necesario realizar acciones encaminadas a la mitigación del impacto del mismo en la operación de la smart grid. Algunas de las técnicas empleadas en la mitigación de ciberataques se han centrado en esquemas basados en el control Volt/Var, reconfiguración de la red eléctrica, o métodos basados en criterios económicos para minimizar el número de cargas desabastecidas como consecuencia de un ciberataque.

RETOS EN EL ÁMBITO DE LAS COMUNICACIONES

Las medidas de ciberseguridad aplicadas a los protocolos de comunicación existentes deben adecuarse a las particularidades de las comunicaciones entre los distintos dispositivos de una smart grid, como son los relés, lectores inteligentes o puntos de carga. Estas medidas deben abarcar mecanismos de prevención, detección y recuperación (Li et. Al, 2011).

En cuanto a las medidas de prevención, es necesario proteger la información intercambiada entre los distintos dispositivos de la smart grid antes de que esta salga a la red. Por un lado, se debe garantizar la confidencialidad de los datos, de forma que un atacante no pueda acceder a datos para los cuales no ha sido autorizado. En este sentido, es necesario cifrar las comunicaciones mediante algoritmos de cifrado ligero, ya que en muchos casos el cifrado se realizará en dispositivos embebidos donde el consumo de batería y recursos debe ser optimizado. Adicionalmente, se debe procurar a las comunicaciones de mecanismos de verificación de la integridad de los datos intercambiados. De esta manera, un atacante no podrá alterar ni generar datos que puedan influir en el desarrollo normal de la red. Para ello, es necesario implementar códigos de autenticación de mensajes (MAC) que permitan a un receptor verificar la integridad de los datos recibidos, a la vez que se autentica al emisor del mismo. Igualmente, los algoritmos existentes como HMAC (Hash over MAC) deben ser revisitados y analizados para su uso con los protocolos de comunicación de las smart grids. Finalmente, los datos deben tener una disponibilidad inmediata, previniendo ataques de denegación de servicio que influyan en la operatividad de la red eléctrica. La protección frente a estos ataques conllevará medidas como un control de acceso a la red de usuarios y dispositivos, mediante el uso de cortafuegos (firewall) y segmentación de redes.

Debido al carácter altamente distribuido de las smart grids, las medidas de detección deben incluir tanto información proporcionada por los distintos sensores locales, como por ejemplo IDS de dispositivos, con información global, tales como trazas de netflow para evaluar la congestión de la red en un momento determinado (Cokic et. Al, 2019). Toda esta información debe ser correlada, analizada y procesada en un sistema central como un SIEM (Security Information and Event Management) (Leszczyna et. al, 2015). Centralizar la información tiene dos aplicaciones importantes. Por un lado, permite proporcionar información en tiempo real sobre el estado global de la red (Alcaraz & Lopez, 2014). Por otro, el gran volumen de datos recolectados permitirá enriquecer la detección de ciberataques, tanto a nivel local (es decir, enfocados a los dispositivos) como a nivel global (es decir, enfocados a la red y las comunicaciones) basados en Machine Learning.

RETOS EN EL ÁMBITO NORMATIVO

Tras los atentados del 11-S y el 11-M en Nueva York y en Madrid respectivamente, la mayoría de los estados, pero fundamentalmente en occidente, los Estados Unidos y la Unión Europea, reconocieron la importancia de mantener la prestación de los servicios esenciales y las IC que los prestan.

Las peculiares características de las conductas antisociales y antijurídicas que podrían constituir los ciberdelitos, así como características como la transnacionalidad, la ubicuidad, el relativo anonimato del atacante, la diversidad de objetivos geográficamente dispersos, la superficie de ataque sobre los sistemas víctimas, entre otros, condicionan en gran medida la investigación, persecución, enjuiciamiento y radicación de los ciberdelitos, que atentan contra las infraestructuras en las que se apoya el desarrollo tecnológico de las Smart grid. Iniciativas como el Convenio sobre Ciberdelincuencia de Budapest o el estudio académico, encargado por la OTAN, sobre el Derecho Internacional de aplicación para las operaciones en materia cibernética, conocido como el Manual de Tallín 2.0, muestran el camino y la complejidad de la normalización en materia de ciberseguridad.

Los primeros pasos en el ámbito legal de la protección de las infraestructuras críticas comienzan como respuesta a la solicitud del Consejo Europeo en relación a la elaboración de una estrategia global para mejorar la protección de dichas infraestructuras, que se materializó en la Comunicación COM/2004/0698. Dos años más tarde, en 2006, se presenta el Programa Europeo para las IC (sus siglas en inglés EPCIP), en él se establece un marco de acción encaminado a la protección de las IC de todos los sectores económicos relevantes en el ámbito de los estados miembros de la UE. La COM/2004/0698 derivará en la ley europea por excelencia en el ámbito de la protección de IC, la Directiva Europea 2008/114/CE de 8 de diciembre, que debía entrar en vigor en los estados miembros e incorporarse en su ordenamiento jurídico antes del 12 de marzo de 2011. En España, se realiza la transposición de esta Directiva mediante la Ley de Protección de Infraestructuras Críticas, Ley 8/2011, de 28 de abril, (conocida como LPIC) y desarrollada por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras críticas (conocido como RDPIC).

Desde el punto de vista de la ciberseguridad, la verdadera innovación normativa surgió con la promulgación de la Directiva, 1148/2016/UE, de 6 de julio de 2016, conocida como la Directiva NIS que señala la necesidad de la designación de autoridades competentes, la creación de grupos de trabajo encargados de reportar los ciberincidentes, así como la adopción de estrategias de ciberseguridad nacional en todos los países miembros, junto con la obligatoriedad de notificar los ciberincidentes a las autoridades competentes en cada país. Además, en esta directiva los operadores de las redes eléctricas son considerados como “operadores de servicios esenciales” y tienen obligación de entregar informes correspondientes a los cibertaques que hayan sufrido en sus sistemas. La directiva 1148/2016/UE se encuentra traspuesta al ordenamiento jurídico español a través del Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información. Los sistemas de información y la información gestionada y mantenida por estos en relación a las Infraestructuras Críticas gozan de una especial protección en el artículo 264.bis del código penal español.

A la vista de los resultados negativos de la evaluación de las directivas dictadas en el ámbito de la protección de las IC, en 2019 la UE publicó una serie de recomendaciones para los estados miembros (European Commission, 2019), entre las que se encuentran el desarrollo de planes para analizar los riesgos de las IC en materia de ciberseguridad, y los principales retos a los que se enfrentan las smart grids en este campo: los requerimientos en materia de actuación en tiempo real en las redes smart grids, los efectos en cascada derivados de un ciber ataque, la combinación de las tecnologías convencionales y emergentes para mejorar la actuación de las smart grids ante un ciber ataque, y finalmente la identificación de las acciones principales para implementar las medidas de preparación necesarias para adecuar el funcionamiento del sistema eléctrico a esta nueva realidad.

Los futuros retos normativos se encuentran focalizados en el desarrollo de códigos de red en el ámbito de la ciberseguridad, como se establece en el COM/2019/943. A este respecto, el grupo de trabajo sobre Smart Grids de la UE recomienda: realizar una gestión de riesgos transfronteriza y entre organizaciones; establecer un sistema de alertas tempranas en el ámbito de la ciberseguridad y requisitos mínimos de seguridad para los diferentes componentes de las IC, así como para los operadores de sistemas energéticos; desarrollar un marco europeo de madurez de la ciberseguridad energética y de gestión de riesgos de la cadena de suministro.

CONCLUSIONES

En el proceso de digitalización de las redes eléctricas hacia las smart grids, el aumento de comunicación entre los dispositivos que la componen extiende los retos a los que se enfrentan los operadores de las redes eléctricas hasta el campo de la ciberseguridad. En este artículo se presentan los principales retos a los que se enfrentan las smart grids en materia de ciberseguridad en tres ámbitos: (i) en la operación de los sistemas de protección, encaminados a desarrollar algoritmos de detección de inyección de datos falsos (corrientes de cortocirucito) y modificación de las

consignas de operación de los IEDs que puedan dar lugar a un fallo en cascada del sistema; (ii) en los protocolos de comunicación para el envío de información entre dispositivos, que deben ser actualizados para incorporar mecanismos de protección, autentificación y disponibilidad de la información intercambiada; y, para finalizar, (iii) en aspectos legales relacionados con el desarrollo de un marco normativo de protección del sector eléctrico como infraestructuras crítica frente a ciberincidentes.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por la Fundación Iberdrola España, dentro del programa de becas de apoyo a la investigación 2020.

REFERENCIAS

- Alcaraz, C., & Lopez, J., 2014. WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids. Future Generation Computer Systems, 30, 146-154.
- Cokic, Mita, and Ivan Seskar, 2019. "Software defined network management for dynamic smart GRID traffic." Future Generation Computer Systems 96: 270-282.
- European Commission, 2019. 1240 Commission Recommendation on cybersecurity in the energy sector. Brussels, 3.4.2019 SWD (2019).
- J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko and A. Martin, 2019. "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4332-4341, July 2019.
- Li, Husheng, Lifeng Lai, and Weiyi Zhang, 2011. "Communication requirement for reliable and secure state estimation and control in smart grid." IEEE Transactions on Smart Grid 2, no. 3 (2011): 476-486.
- Leszczyna, Rafał, and Michał R. Wróbel, 2015. "Evaluation of open source SIEM for situation awareness platform in the smart grid environment." In 2015 IEEE World Conference on Factory Communication Systems (WFCS), pp. 1-4. IEEE, 2015.
- NIST, 2015. Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability.
- S. Ward et al., 2007. "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee," IEEE Power Engineering Society General Meeting, Tampa, FL, 2007, pp. 1-8.
- X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao and Z. Li, 2017. "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," IEEE Transactions on Smart Grid, vol. 8, no. 2, pp. 572-580, March 2017.
- Y. Xin et al., 2018. "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, pp. 35365-35381, 2018.