RETOS DE CIBERSEGURIDAD QUE AFRONTA LA TRANSFORMACIÓN DEL SECTOR ELÉCTRICO

AGUSTÍN VALENCIA GIL-ORTEGA

El sector eléctrico está viviendo un momento de gran transformación donde la búsqueda por la integración de fuentes renovables, así como la aparición de la figura de los prosumidores (productores y consumidores) tanto por la faceta de recursos de generación distribuida (DER) como por el impacto del vehículo eléctrico están obligando a acometer una auténtica transformación digital en todos los niveles de la cadena de valor (generación, transporte, distribución y comercialización). Esta transformación lleva asociada la integración con otros sectores como son el de las Telecomunicaciones y los proveedores de servicios digitales así como la proliferación de dispositivos IoT que obligan a pensar en toda un conjunto de riesgos de ciberseguridad para todo el conjunto, desde los operadores críticos a los propios usuarios finales. Por tanto, se tratará de exponer en este artículo el contexto actual, sus amenazas e impactos junto con algunas de las regulaciones más relevantes que están surgiendo.

Siempre que se habla de ciberseguridad en infraestructuras críticas lo que nos viene a la mente es un ataque a una central nuclear y un apagón total. Si bien podríamos pensar que es una cuestión del imaginario colectivo, lo cierto es que se asientan en la base de las preocupaciones de la sociedad.

El temor que despierta la energía nuclear vuelve a cobrar fuerza con la guerra de Ucrania. Por un lado, es una importante fuente de energía ante la posibilidad de escasez de otras como el gas. Por otro lado, entran en juego cuestionamientos, desde un plano puro de análisis de consecuencias, relativos a los escenarios de guerra como el ataque a las centrales de Zaporiyha y otras amenazas que está planteando el conflicto con el uso de nuevas tecnologías y enfoques híbridos, como la combinación de ciberataques y artillería, o el de uso de drones para multitud de propósitos y aplicaciones.

El miedo al apagón total no deja de estar fundado sobre la percepción de la necesidad de la electricidad para todos los planos de la vida, es decir, no se plantea que el sistema eléctrico funcione mal pero sí nos planteamos qué haríamos en caso de ausencia de ésta.

¿Cómo se trasladan esas inquietudes al ámbito de la ciberseguridad? En un primer estadio, nos planteamos un análisis de riesgos, donde valoramos la probabilidad de que un atacante pudiera explotar una o varias vulnerabilidades de los activos del

sistema con los que conseguir un impacto. La probabilidad la relacionaremos con la superficie de ataque, las vulnerabilidades explotables por el atacante y los recursos del mismo. En un segundo estadio, desde el plano defensivo y tomando la definición de niveles de seguridad de la norma ISA/IEC 62443 de ciberseguridad industrial, nos centraremos en los controles que aplicar a los activos en función de la criticidad de estos y de la motivación del atacante.

Como abordamos muchos temas, trataremos de ir lo más ordenadamente posible para evitar confundir al lector. Así pues, hablaremos primero de superficie de ataque y su evolución, para seguir explicando la evolución del sistema eléctrico y su adopción tecnológica.

SUPERFICIE Y VECTORES DE ATAQUE

Desde una óptica tradicional militar, las dimensiones a tratar son Tierra, Mar, Aire y Espacio. En el propio entorno militar, el ciberespacio ya se ha constituido como una nueva dimensión, y el cómo se relaciona este último con los anteriores desde un plano tecnológico, pero también humano, constituye un conjunto nuevo de disciplinas sobre las que formarse, tal y como se muestra en la figura 1.

Hablando del ciberespacio específicamente, lo más fácil es comenzar por un concepto de vectores de ataque por los que conseguir acceso a los sistemas objetivo del ataque:

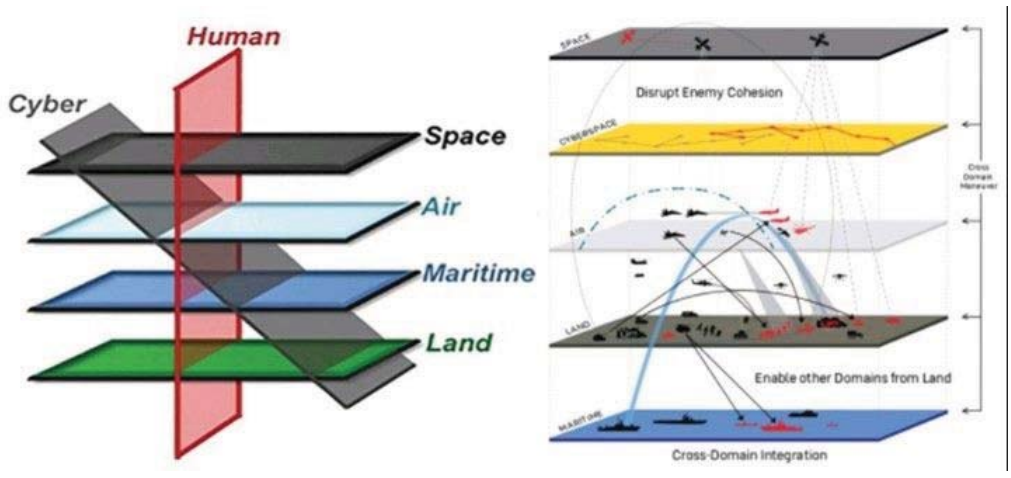
Acceso físico

Los entornos eléctricos siempre han dedicado muchos recursos a proteger el acceso físico a los activos críticos. Sin embargo, pensemos en cuantos nuevos dispositivos se están desplegando que pueden tener acceso a las redes de estas infraestructuras críticas. Aquí debemos prestar especial atención a los puntos de recarga de vehículos eléctricos, pero también centrales de producción fotovoltaica de grandes extensiones, a las que no se puede prohibir el acceso, bien por lo antieconómico,de afrontar tamaña inversión, bien por atravesar caminos y cañadas reales.

Acceso por red, Terceras partes e IoT.

Se trata del gran cambio en el paradigma del riesgo de los operadores eléctricos. Tradicionalmente basados en redes privadas de las que muchas son propietarias, han

FIGURA 1
SUPERFICIES Y VECTORES DE ATAQUE



Fuente: United States Special Operations Command Human Domain Concept, 5 September 2014 y America's Army

visto cómo necesitan conectarse a redes públicas para poder competir en plazos a los requisitos para instalación de nuevas plantas renovables.

Pensemos también en la revolución que potenció la COVID-19 por la que el acceso remoto se multiplicó, permitiendo el acceso para mantenimiento, configuración y puesta en marcha de estos sistemas. Si bien se ganó en eficiencia de recursos evitando desplazamientos, también se multiplicó la superficie de ataque al poder acceder desde redes que no son de las propias infraestructuras, pero a las que éstas les han concedido acceso.

Pensemos también en el crecimiento de dispositivos Smart para entorno doméstico suministrados directamente por las compañías eléctricas en muchos casos con el objetivo de ayudar al consumidor a conocer sus consumos o a planificarlo, tales como termostatos inteligentes, asistentes, etc que, además, se conectan a otras plataformas como Alexa, Amazon Echo, etc. Todos estos dispositivos repiten el error de no considerar la seguridad en el diseño, primando el precio unitario por encima de todo.

Tomemos como referencia informe sobre el "Estado de la Ciberseguridad y Tecnología Operativa 2023", concretamente este punto. La explosión de dispositivos conectados pone de relieve la complejidad de los retos a los que se enfrentan las organizaciones de OT: Casi el 80% de los encuestados afirmaron tener más de 100 dispositivos OT con IP en su entorno OT, lo que pone de manifiesto el importante reto que supone para los equipos de seguridad proteger un panorama de amenazas en constante expansión. Los resultados de la encuesta revelaron que las soluciones de ciberseguridad siguen contribuyendo al éxito de la mayoría (76%) de los profesionales de OT, en particular mejorando la eficiencia (67%) y la flexibilidad (68%). Sin embargo, los datos del informe también desvelan que la proliferación de soluciones hace más difícil incorporar, emplear y aplicar políticas de forma coherente en un entorno de IT/OT cada vez más convergente. Y el problema se agrava con el envejecimiento de los sistemas, ya que la mayoría (74%) de las organizaciones informan de que la edad media de los sistemas ICS de su organización oscila entre 6 y 10 años.

Acceso Inalámbrico

El acceso inalámbrico estaba descrito en todos los marcos teóricos pero es ahora cuando se le empieza a nombrar como un vector de ataque creíble.

Situaciones que lo justifican son el aumento del uso de comunicaciones inalámbricas por su bajada de precio, aumento de soluciones (wifi6, LTE 4G/5G, Nb-IoT) que permiten reducir el coste de comunicaciones cableadas. Pero también por muchas soluciones de movilidad, desde dispositivos inalámbricos para los trabajadores como por vehículos conectados o drones para tareas de mantenimiento.

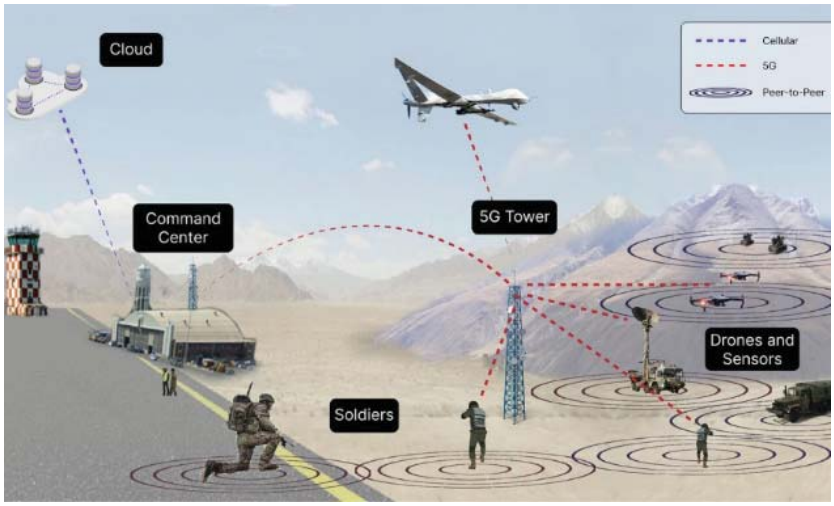
Sin embargo, estos últimos se están viendo especialmente en la guerra de Ucrania como un agente de amenaza a tener en cuenta, especialmente por el gran rango de usos que pueden tener, desde drones armados a drones con conectividad que puedan penetrar en comunicaciones de instalaciones no securizadas donde el alcance de la seguridad se ceñía a la zona de "detrás de la valla", tal y como se muestra en la figura 2.

Acceso por Dispositivos

En línea con lo anterior, el auge de dispositivos que se introducen en estas instalaciones es cada vez mayor, desde sondas para mediciones, a dispositivos de mano para gestión de rondas o mantenimiento a equipos portátiles para configuración de sistemas. Todos ellos son equipos con grandes capacidades de conectividad, almacenamiento o procesamiento y que su diversidad e, incluso obsolescencia, plantea retos de gestión, tanto para su mantenimiento y parcheado como para el control de acceso solamente a las redes permitidas.

No son desdeñables los casos de ciberincidentes por memorias USB u ordenadores portátiles, que siendo vulnerables se conectan a internet, provocando ataques de manera inconsciente al conectarse a la red

FIGURA 2
ACCESOS INALÁMBRICOS



Fuente: Military Embedded Systems

crítica. La ciberinteligencia ya está avisando de que este modelo de ataque se está reactivando, precisamente por persistir en los entornos críticos.

Acceso por Cadena de Suministro y Terceras Partes

En este entorno, nos referimos a cadena de suministro cuando tenemos proveedores que nos proporcionan software o medios de almacenamiento o computación.

Por tanto, el que se puedan comprometer versiones de software en las que los atacantes puedan embeber su malware, o vulnerabilidades Zero-Day en plataformas cloud y que permita a los atacantes moverse entre instancias de las empresas sin ser reconocidos, es algo que dejó de ser ficción. Un caso paradigmático fue el de SolarWinds.

Solarwinds no es, como otras veces ha pasado, el nombre que se le da a un atacante o a un malware, sino el caso de una empresa que fue objeto de este tipo de ataque. Sin querer entrar en demasiado detalle, hablamos de una empresa especialista en desarrollar software para gestión de infraestructura de red de comunicaciones, con un gran foco en el entorno militar y de infraestructuras críticas. Se sabe que una serie de ataques de origen ruso llegaron a penetrar en las instancias de esta empresa en la infraestructura nube Microsoft Azure, llegando al punto de elaborar una nueva versión del software de SolarWinds Orion (pero con el malware ya incluido para permitir abrir conexiones desde los clientes hacia el atacante) y activar la notificación a los usuarios para que la descargaran e instalaran.

Este ataque plantea, además, cuestiones paradójicas. Las infraestructuras críticas manejan siempre la obsolescencia como parte de su entorno, al fin y al cabo son entornos tan grandes y sujetos a necesidades operativas tan exigentes que plantean una gran dificultad en su adecuada actualización. Por tanto, ¿debemos considerar el no fiarnos de las actualizaciones y romper una de esas reglas de oro de "mantener siempre los sistemas actualizados"?

NUEVOS MODELOS EN EL SECTOR ELÉCTRICO

Y partiendo de este contexto, hablamos del impacto que tendría en las nuevas tecnologías que están transformando el entorno eléctrico en orden inverso al tradicional, desde lo más cercano al consumidor a lo más próximo a los operadores del sistema.

Comercialización

IoT Doméstico

La penetración de lo digital en los hogares es innegable, el teléfono móvil como protagonista que ostenta funciones de comunicación, entretenimiento, información... pero también, y aquí está lo principal que nos ocupa, identidad, pagos y control de dispositivos.

Todo el ecosistema de domótica lleva años desarrollándose, pero es cierto que no ha crecido hasta tener un vehículo de conexión sencillo y potente como son los móviles. Y precisamente en aras de esa sencillez, la seguridad ha sido sacrificada en la ecuación. Quien escribe es consciente de la dificultad de encontrar un equilibrio entre seguridad y usabilidad, pero no es menos cierto que aplicaciones de Marketplace como Amazon o de las plataformas bancarias son el mejor referente para poder mantener dicho equilibrio.

De todas las aplicaciones, destacaremos solamente las que tienen relación con el sistema eléctrico:

Contadores Inteligentes e Infraestructura de Medida Avanzada (AMI)

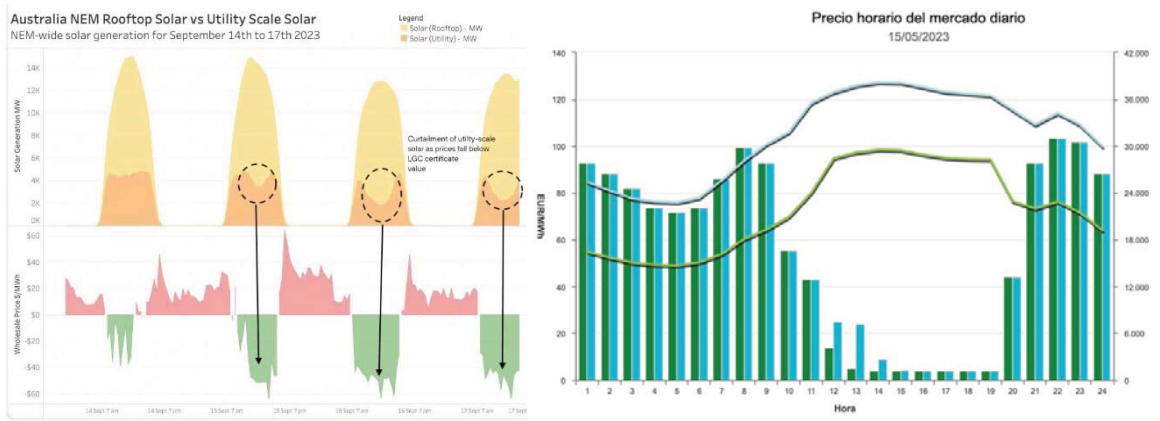
En España, los contadores son todos de este tipo desde 2020. Se encargan de enviar datos a través de las propias redes eléctricas (PLC- Power Line Communications) hasta los centros de transformación que alimentan las distintas zonas. A partir de Centros de transformación la comunicación va hacia subestaciones y centros de control, lo que constituye la AMI, aquí ya con protocolos digitales y enrutables (Prime, DLMS-COSEM). Estos sistemas permiten aplicar perfiles de tarifas según horario, dar información a los propios usuarios para ayudarles a controlar su consumo y también corte y reposición de sistemas sin necesidad de acudir en persona.

Generación fotovoltaica foméstica

La generación fotovoltaica doméstica se ha disparado desde la guerra de Ucrania ante el temor a carestía de energía y ante la subida de los precios de la electricidad. Según Endesa (Julio 2023), el número de instalaciones se ha multiplicado por 26 en los últimos 4 años, contabilizándose más de 200.000 instalaciones domésticas en funcionamiento.

En España ya se ha podido ver este verano cómo la generación solar ha mantenido a cero el precio de la energía durante varias horas y en países como Australia, el impacto de esta fuente de energía está obligando incluso a las empresas eléctricas a reducir la oferta de energía de sus propios parques solares debido al desplome de los precios por exceso de oferta, tal y como se muestra en la figura 3.

FIGURA 3
***CURTAILMENT* ENERGÍA SOLAR Y PRECIO DE LA ENERGÍA**



Fuentes: Fuente ABC News- Gridco y El periódico de la Energía

Estos sistemas se controlan desde el teléfono móvil informando de la producción de las placas a través del inversor que está conectado a la red wifi doméstica. Muchos desconocen que la gestión de los inversores desde el móvil no es directa sino a través de una plataforma en la nube. El fabricante establece conexiones entre el inversor y su entorno en la nube, por un lado y entre su entorno nube y el móvil, por otro.

Cargador de vehículo eléctrico

Se asume que el crecimiento de cargadores domésticos, por ahora, crece en línea con el número de los vehículos eléctricos que se venden. Aquí se indican los números de proyección de ventas a nivel mundial. De ahí que la estimación del mercado de equipos relacionados con el vehículo eléctrico se estima que se multiplicará por más de 5 hasta 2030.

Atendiendo al crecimiento del uso del vehículo eléctrico y al reparto de uso del mismo, la "Global Environment Facility" (GEF) desarrolló una herramienta para medir el uso de la infraestructura de carga de los vehículos eléctricos. Como se puede ver en la figura 4, la mayor parte de la carga de los vehículos se realiza en el domicilio y otra gran parte en el lugar de trabajo. La parte en ruta es prácticamente insignificante por ahora, siendo una de las debilidades del sistema que frenan la adopción de esta tecnología por parte de los consumidores.

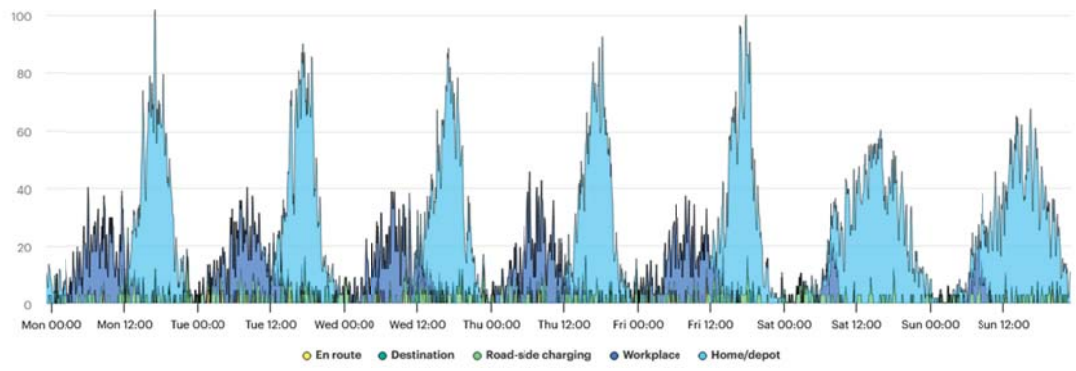
Estos perfiles de demanda plantean varios retos porque no se desea encarecer a los usuarios la factura ampliando el término de potencia necesario si se hacen coincidir los consumos clásicos de calefacción, electrodomésticos e iluminación -que suben por la tarde al retornar al domicilio- junto con el de la carga del vehículo. De esta manera, la programación de la carga del vehículo será casi imperativa y, además, de un modo predictivo tendrá que ir ligada a evitar un consumo excesivo que provoque cortes de suministro.

Por otro lado, el vehículo eléctrico se prevé como una parte de la solución al problema del almacenamiento de energía, partiendo de que los estudios suelen establecer el uso del vehículo al 11% del tiempo total, pudiendo disponerse del otro 89% como medio de almacenamiento e inyección de energía... Sin embargo, estamos hablando de otro cambio de paradigma clásico en el que el usuario permita que haya una gestión externa de sus equipos domésticos.

Vehículo Eléctrico

Derivado de lo anterior, el vehículo eléctrico también es un equipo conectado. Ya no solo hablamos de un consumidor o generador eléctrico sino que toda esa gestión necesita una conexión, tanto con la infraestructura de carga como con la infraestructura del fabricante del vehículo. Y el vehículo, en sí mismo, ya es un ordenador sobre ruedas, como se evidencia en la propuesta

FIGURA 4
DISTRIBUCIÓN DE CARGA DE VEHÍCULOS



Fuente: Global Environment Facility

de valor que hacen fabricantes como Tesla. Por tanto, hablamos de un ecosistema que se hace cada vez más complejo.

Aerotermia y termostatos inteligentes

La aerotermia se presume como uno de los grandes cambios en los hogares en los próximos años. Bombas de calor que, por su propia tecnología, podrían llegar a reducir el consumo energético en más de un 40% en los hogares, tanto para frío como para calor. Estos equipos ya incluyen en su mayoría termostatos inteligentes que permiten un control y programación, tanto local como desde el móvil. Estas soluciones facilitan la reducción de consumo cuando no se está en casa, pre-calentar (o enfriar) antes de llegar o cambiar el perfil diferenciando el día de la noche. De nuevo, las comunicaciones no son necesariamente directas entre el móvil y el termostato, sino mediante una plataforma del fabricante ubicada en la nube. Como se ve en el siguiente gráfico, la estimación de crecimiento en Europa hasta 2030 es que se multiplique por 5 la cantidad de unidades vendidas.

Redes de Carga de Vehículos eléctricos

Como ya se comentó analizando los cargadores domésticos, los principales frenos para la adopción del vehículo eléctrico es la menor autonomía y la necesidad de reforzar la red de recarga pública. Esta recarga pública plantea muchísimos retos, tanto tecnológicos como de planificación, interoperabilidad y de ciberseguridad:

- **Retos Tecnológicos**. Partimos de que la tecnología y requerimientos van cambiando en este tiempo. Los primeros cargadores eran de potencia similar a la doméstica, sin embargo, se ha pasado de cargadores lentos (3,6kW) a semirrápidos (Entre 22kW y 50kW) rápidos (Entre 50kW y 250kW) y ultrarrápidos (>250kW). Estos equipos comunican el entorno del vehículo conectado con el de la red eléctrica desde la comercializadora -agente del sector eléctrico no mencionado hasta ahora-, que requiere también de la coordinación con la red de distribución. Además, en muchos casos los fabricantes de los puntos de recarga precisan conexión, en algunos casos para mantenimiento y atención a averías, si bien algunos fabricantes ofrecen un servicio de pago por uso, ubicándose entre la empresa eléctrica y el usuario.
- **Retos de Planificación**. A nivel de planificación, porque requiere coordinar áreas de despliegue de puntos de recarga con capacidades de la red, tal como se hace con la generación renovable y se prevé que se multiplique por 10 la cantidad de puntos de recarga a desplegar hasta 2030, llegando a 240.000 según AEDIVE. Esto puede significar un valor alrededor de los 24GW adicionales a gestionar por las redes de distribución.
- **Retos de Interoperabilidad**. La carga se va a hacer desde redes de distintas comercializadoras, necesitando interconectar sistemas de información y pagos, lo que involucra la infraestructura de los propios puntos de recarga, los vehículos y los dispositivos móviles de los usuarios, así como fuentes de control de identidad compartidas.
- **Retos de Ciberseguridad.** Centrándonos en el ámbito de la ciberseguridad, los retos más destacados serían los siguientes:
  - Consideración de los puntos de recarga para la aplicabilidad del Cyber Resilience Act (CRA) en cuanto a garantías de soporte por un mínimo de 5 años y requisitos de ciberseguridad desde el diseño e integrados en el ciclo de vida del producto.
  - Consideración de los puntos de recarga según la nueva ley de seguridad de maquinaria, que obliga a establecer almacenamientos de logs así como controles respecto al acceso remoto y de control de modificaciones de configuración, especialmente todas las relacionadas con la seguridad física (safety). No olvidemos que un control

inadecuado de la carga rápida o de la comunicación con el vehículo podría comprometer la seguridad de las baterías, teniéndose conocimiento de incendios de algunos vehículos.

– Securización de las comunicaciones hacia la nube M2M (Machine to Machine). Principalmente se están usando protocolos como MQTT, OCPP o OpenADR, estos ya incluyen capacidades de cifrado que no se están desplegando suficientemente en muchos casos. Además, se deben aplicar capacidades ZTNA (Zero Trust Network Access) que permitan bloquear comunicaciones si se detectan intrusiones en los canales de comunicación.

– Se deberán plantear esquemas de segmentación interna y externa de los entornos nube para asegurar tanto la integridad como la privacidad de los datos, especialmente considerando el gran número de actores que forman parte de estos procesos.

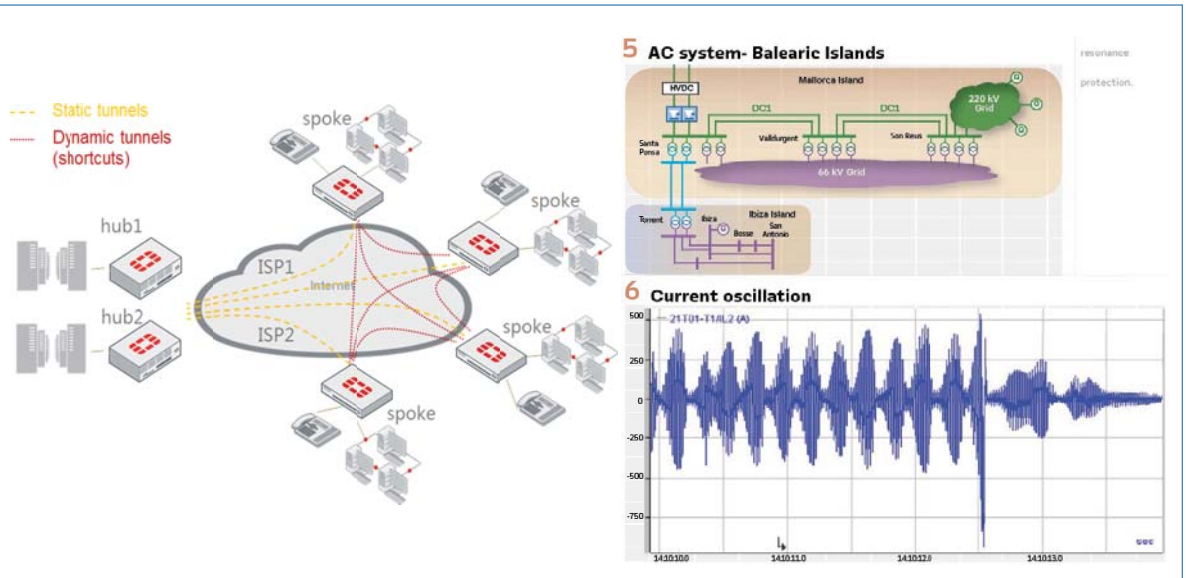
– Se recomienda desarrollos de seguridad de accesos para aplicaciones hacia la nube como el empleo de tecnologías SASE (Secure Access Service Edge) de un único proveedor que permitan simplificar varios de los requisitos identificados.

Redes de Distribución

Las redes de distribución siempre han tenido como objetivo llevar la energía desde la gran infraestructura de generación y transporte de energía hacia el nivel de los consumidores y ciudadanos. Este modelo, clásicamente unidireccional se ve alterado por los factores indicados anteriormente. Además, debido a la naturaleza no industrial de la generación doméstica, se pueden producir interrupciones en múltiples puntos que van a requerir tanto de una adecuada gestión de los flujos de energía, como de la gestión de las faltas y de la calidad del suministro.

A continuación, en la figura 5, se expone someramente un caso reciente, realizado en Baleares, mediante el cual se mostraba la mejora del suministro en cuanto a reducción de armónicos gracias a la interconexión de distintos ramales mediante equipos de análisis de red y una estándar denominada SD-WAN (Software Defined-Wide Area Network) que permite aplicar

FIGURA 5
REDES DE DISTRIBUCIÓN Y APLICACIÓN DE SD-WAN



Fuentes: Fortinet // Enhanced Grid Reliability & Resilience – Wide-Area PAC (WAPAC) case studies

FIGURA 6
CIBERSEGURIDAD DE SUBESTACIONES

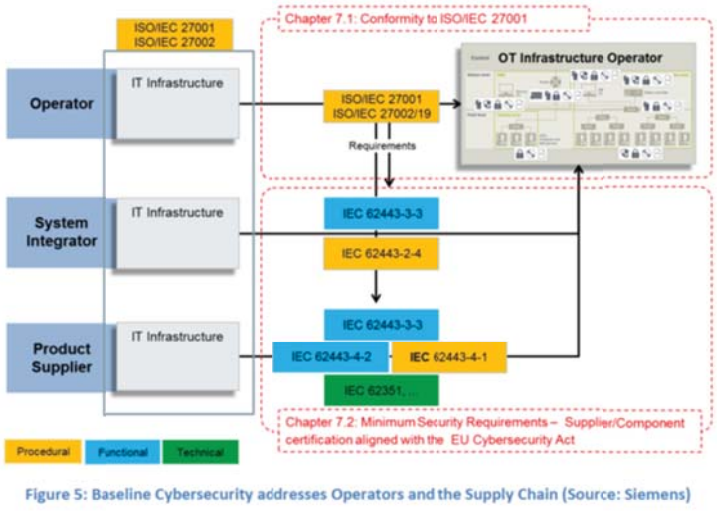


Figure 5: Baseline Cybersecurity addresses Operators and the Supply Chain (Source: Siemens)

Fuente: Smart Grid Task Force Experts Group 2 Final Report 2019

flexibilidad a la hora de establecer enlaces y vías alternativas en caso de fallo junto con un nivel suficiente de cifrado las comunicaciones.

Esta respuesta rápida requiere de digitalización de las subestaciones. El estándar que marca este nuevo tipo de subestaciones es la IEC 61850 y la securización se hace a dos niveles con dos estándares distintos: por un lado, arquitectura, zonas, niveles y capas de seguridad (ISA/IEC 62443), y por otro, Seguridad de Comunicaciones, Aplicaciones y Protocolos específicos (IEC 62351), tal y como se muestra en la figura 6.

La evolución de la digitalización de subestaciones y la adición de sus capas de seguridad es muy dispar, tanto en España (con alrededor de 5000 subestaciones en funcionamiento) como en el resto del mundo. Muchas de ellas cuentan con una protección perimetral (firewall) y en algunas se están desplegando soluciones de monitorización OT. Parte de esta disparidad se debe a la naturaleza de estos activos, puesto que hay zonas sin líneas redundantes que permitan grandes mejoras por tiempo prolongado fuera de servicio y también se aduce lentitud administrativa al ser un negocio regulado, lo que también necesita de una priorización o reconocimiento estatal para que se dediquen más recursos a este tipo de mejoras.

Generación renovable

Las plantas tradicionales (térmicas, hidráulicas. Nucleares) se basaban en una contratación a un tecnólogo principal (Siemens, ABB, General Electric...) y a una empresa de ingeniería como integrador principal. Toda la instalación y pruebas se realizaba con medios y personal in situ y se hacía una serie de pruebas durante la fase de puesta en marcha para asegurar que se cumplían los criterios de acoplamiento a red, tanto de la empresa eléctrica que la opera como de del Operador del Sistema de Transporte (TSO con sus siglas en inglés, en España es REE).

En la generación eólica, parte del ecosistema permanece, habiendo algunos actores nuevos entre los tecnólogos pero produciéndose dos grandes cambios. Toda la operación es en remoto y las plantas tienen una conexión permanente con la infraestructura del tecnólogo para labores de seguimiento, evaluación de rendimientos, indicadores contractuales, atención a eventos etc. Esta conexión se hacía tradicionalmente por satélite y fue algo muy comentado cuando, al inicio de la guerra de Ucrania,

el ciberataque de Rusia a los Satélites VSat provocó la parada de una buena parte de la infraestructura eólica alemana, más de 11GW, que perdieron esta comunicación.

El crecimiento sostenido de la energía eólica en el mix energético español (y mundial) ha hecho evolucionar la tecnología eólica de manera significativa. Los primeros modelos tenían como único objetivo la optimización del aprovechamiento eólico, tanto en potencia eléctrica como en rendimiento aerodinámico. Sin embargo, las últimas evoluciones son a nivel de control y protección, desde sistemas que permitan responder rápidamente a las necesidades del despacho (a subir y, especialmente a bajar) hasta sistemas de detección de aves que hagan parar las unidades ante su paso. Todos estos sistemas no pertenecen necesariamente al tecnólogo principal, requieren accesos remotos y se debe asegurar que se ha realizado un correcto análisis de riesgos conforme al impacto que estos tienen respecto a la continuidad del proceso.

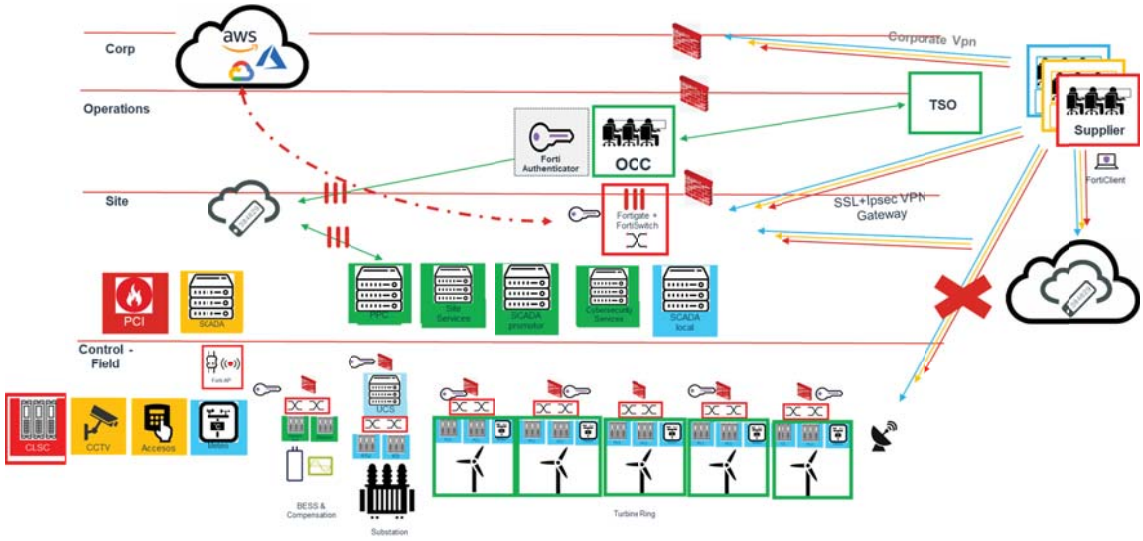
Además, ahora se empieza a hablar de plantas híbridas, donde se incluyen baterías de gran almacenamiento, que se denominan, como conjunto, BESS (Bulk Energy Storage Systems). Una evolución que tiene todo el sentido para acoplar generación y demanda pero que requiere una gestión local a nivel de emplazamiento para decidir cuándo se evacúa o cuándo se almacena energía o qué porcentaje de cada.

Las plantas solares son quizás el mejor ejemplo de cómo se está transformando el sector. Ya no hay un tecnólogo principal sino que hay varios componentes principales. Cada uno de estos componentes puede requerir accesos para configuración o mantenimiento remoto y la infraestructura de acceso de los tecnólogos es, en muchos casos, a través de infraestructura en la nube.

Siendo proyectos con gran presión por los plazos y muchos construyéndose para después venderse, la ciberseguridad no ha sido un pilar principal hasta que los ataques se han incrementado en los últimos dos años. Aun así, dada su especial arquitectura, la segmentación interna, la microsegmentación, controles de acceso basados en la filosofía "zero trust" deben ser algo a incorporar urgentemente por lo que aporta ya esta tecnología al mix energético, tal y como se muestra, muy esquemáticamente, en la figura 7.

Por lo tanto, si bien la gestión y despacho de las unidades de generación que hacen las empresas eléctricas no ha cambiado en cuanto a arquitectura y tecnologías, es cierto

FIGURA 7
CIBERSEGURIDAD ENTORNO RENOVABLE



Fuente: elaboración propia

que el panorama de ciberseguridad ha evolucionado enormemente por cuanto lo que antes era únicamente una red privada entre el despacho de generación y las plantas, ahora dispone de múltiples conexiones desde las plantas que podrían suponer intrusiones al sistema. Si no cambia el paradigma de arquitectura de conexiones se multiplicará la superficie de ataque proporcionalmente a la inversión en energías renovables.

Esto nos lleva a considerar especialmente el riesgo de terceras partes y de cadena de suministro porque, como comentábamos antes, hablamos de comunicaciones hacia la nube y de comunicaciones entre nubes. Se requiere tener una segmentación interna en planta que permita que un malware no dañe toda la infraestructura y, de la misma manera, controlar qué instancias en la nube deben estar expuestas a cuales, lo que implica tanto arquitectura como monitorización en la nube. Permítanme una mención obligada a las soluciones de acceso remoto seguro, así como a los pilares de la filosofía "Zero Trust" que se deben implantar en este entorno tales como el control estricto de las identidades que acceden, a los múltiples factores de autentificación, al chequeo continuo de los dispositivos que se conectan y a la comprobación de la postura de seguridad de dichos dispositivos.

Estos pilares a menudo se ofrecen como tecnologías de nicho y es necesario abordarlas de manera integral considerando los flujos de los procesos que se necesita asegurar. Además, se debe considerar también que la arquitectura de las conexiones está cambiando. Si bien las conexiones en el entorno eléctrico utilizan mayoritariamente un estándar denominado MPLS, las necesidades de desplegar conexiones seguras en más puntos y más rápido está llevando a tener que conectarse a infraestructura de fibra óptica de terceros, utilizando la mencionada tecnología SD-WAN.

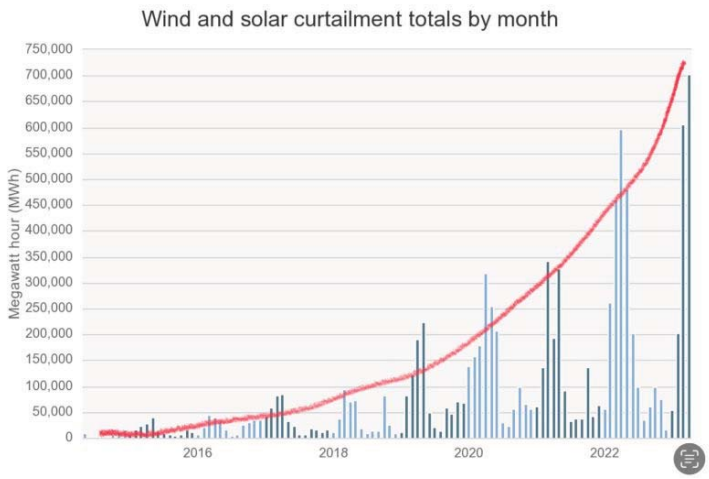
Redes de Transporte

Las redes de transporte también se enfrentan a este cambio global. Antiguamente se trataba de redes propias aisladas que, poco a poco, se han ido interconectando. Mayores interconexiones ayudarán a cubrir mejor las oscilaciones de la generación renovable pero también requieren de mayor intercambio de datos para su correcto control. Además, al estar las infraestructuras críticas en el objetivo de los ciberatacantes, se ha puesto de manifiesto la necesidad de establecer unos mecanismos de requisitos de seguridad mínimos para conectar a la red así como de monitorización y detección para reporte de actividad maliciosa a los operadores del sistema.

A nivel normativo, la referencia es el "Network Code on cybersecurity", sobre el que se está trabajando en varias líneas: definir un marco de gobernanza común; definir guías de gestión de crisis, de seguridad de la cadena de suministro; definir un conjunto de controles mínimos de ciberseguridad; y definir un conjunto de controles avanzados de ciberseguridad para entidades de impacto crítico, entre los que se debe resaltar las protecciones contra amenazas desde otro país y la integración en un sistema específico de amenaza temprana. Esto último puede complementarse o solaparse con las normativas NIS2 o CER (Critical Entities Resilience) e iniciativas derivadas como la Red Europea de Enlace para Ciber Crisis (EU-CyCLONe).

Además, las redes de transporte también se ven tensionadas por el auge de la generación renovable, concentrada en una parte del día y, a la vez distante de los focos de consumo. En España ha habido polémicas en redes sociales en estos últimos años por un fenómeno denominado "curtailment" o en castellano, deslastre de la generación; mediante el cual, habiendo capacidad de producir energía renovable, ésta se tenía que desaprovechar por no haber capacidad para gestionarla. Es decir, aunque a nivel país podría haber demanda para esa energía producida, hay limitaciones a nivel local que implican tener embudos que no permitan evacuar la energía dentro de los parámetros de seguridad eléctrica establecidos. REE prevé que en 2026 la red eléctrica tendrá que soportar un curtailment de un 5,5% respecto al potencial total. A continuación, en la figura 8. se muestra la evolución de este problema en el estado de California:

FIGURA 8
DESLASTRE EÓLICOS Y SOLARES



Fuente: California Public Utilities Commission

No es una problemática sencilla de atajar puesto que instalar nuevas subestaciones requiere conocer mejor la evolución de la demanda y de la generación. De hecho, las empresas distribuidoras tienen la obligación de listar sus nodos y capacidades -tanto ocupada como la admitida y no resuelta- (RD 1183/2020) para la determinación de la capacidad de acceso de generación a las redes de distribución.

Además de este tipo de evaluaciones, otra aproximación se basa en tener mejor información de los flujos de energía en las subestaciones de distribución con los que poder hacer una estimación más precisa que permita reducir los curtailment, tanto por tiempo como por unidades a deslastrar. Esta cuestión, que parece sencilla, sin embargo también significa un cambio de paradigma tradicional, donde cada operador tenía su propia red unida con sus nodos sin ningún impacto de otros actores y ahora necesita de modos seguros para extraer la información de esas otras redes. Se sabe que es una cuestión conocida y que se lleva tiempo debatiendo cómo debería ser la aproximación, que satisfaga a ambas partes (TSO y DSOs) a nivel técnico, de riesgos y que, obviamente, requerirá también negociar desembolsos.

Las señales de curtailment son señales de protección y que se deben considerar como críticas, puesto que una penetración en la red y abuso de estas comunicaciones podría conllevar alteraciones significativas en el parque de generación y, en cascada, en toda la red.

Mercado: *Virtual Power Plant*

Desde la Dimensión de cómo se comercializa la energía en el Pool, estos modelos están introduciendo cambios, siendo el concepto de Virtual Power plant el más innovador.

Dado el crecimiento esperado de equipos que pueden tener tanto impacto en el ecosistema eléctrico, las empresas eléctricas están planteando distintas aproximaciones. Por ejemplo, aplicaciones con las que situarse en un punto medio de las infraestructuras descritas para poder tomar los datos y controlar, o habilitar conexiones con las infraestructuras nube de los fabricantes mediante API.

¿Qué se busca conseguir? Por un lado, enriquecer la información de consumo detallando el impacto de uno de los mayores contribuidores domésticos como es la calefacción. Por otro lado, y previo consentimiento del usuario, tener acceso al control

del termostato para poder variar su ajuste y, por tanto, su consumo. Si bien es incipiente en España, es algo muy desarrollado en Estados Unidos. De esta manera, una gran masa de equipos gestionados remotamente puede suponer un control de una parte significativa del consumo de modo que, en ciertas situaciones, el ajuste entre oferta y demanda no se consiga aumentando la generación de energía sino reduciéndola en parte o, lo que es lo mismo, ofreciendo al operador del sistema una cantidad de energía negativa a producir. Y a este concepto se le denomina "Virtual Power Plant".

La Virtual Power plant podría manejar el ajuste de los termostatos digitales pero también otros dispositivos como calentadores de agua, cargadores de coche o reguladores de paneles fotovoltaicos, tal y como se muestra en la figura 9.

A nivel de ciberseguridad este modelo plantea varios retos. El primero, relativo a las conexiones a la nube para datos críticos de usuarios así como el control de los dispositivos en los hogares. La seguridad de las APIs es una cuestión fundamental y una de las mayores razones de las brechas de seguridad de los entornos en nube está siendo la deficiente seguridad de las APIs. Recordemos que el mundo de la nube puede permitir comunicar muchas APIs dentro de una misma comunicación y, por tanto, ya no es válido analizar el flujo de comunicaciones sino inspeccionar la correcta definición de la infraestructura API.

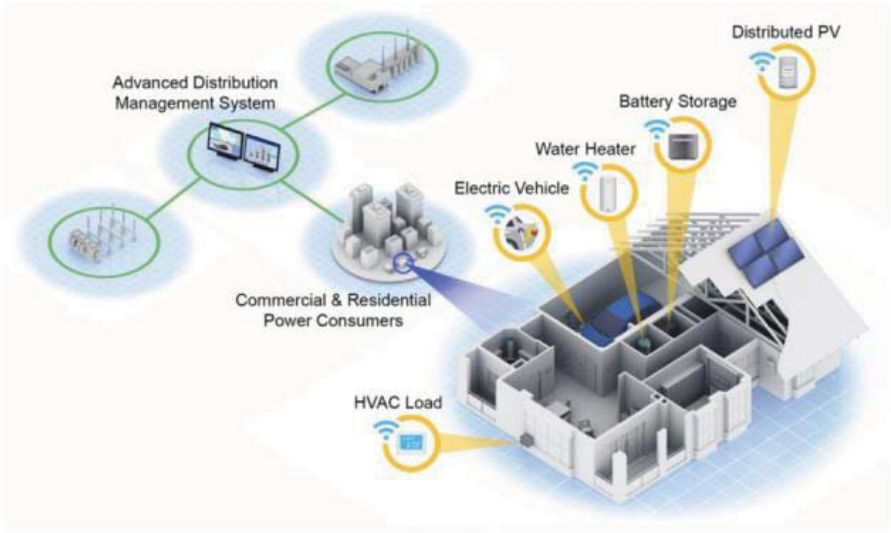
Un segundo reto es de infraestructura. Los despachos de generación son entornos críticos, con varias capas de seguridad entre ellos y los entornos corporativos de sus empresas así con conexiones dedicadas con el operador del mercado eléctrico (OMIE). La incorporación de la Virtual Power Plant supone agrupar la información de millones de dispositivos en un entorno nube sobre el que aplicar algoritmos y después conectarlos a la infraestructura crítica. Además, esta conexión es bidireccional, en función de la energía "casada", se deberá mandar de vuelta una consigna a la infraestructura en nube para que esta reparta la energía mediante la modificación del ajuste de los dispositivos.

SITUACIÓN ACTUAL Y PERSPECTIVAS FUTURAS

Obsolescencia

La obsolescencia es una cuestión siempre presente al hablar de ciberseguridad. Los

FIGURA 9
VIRTUAL POWER PLANT



Fuente: NREL

ciclos de vida de los equipos informáticos y del software (3-5 años) dista mucho de los ciclos de vida operativos planteados para los activos del sector eléctrico (10-25-50 años).Aquí es necesario abordar el problema desde dos perspectivas.

La primera es afrontando la magnitud del problema desde la óptica de la gestión del inventario y de la criticidad de las vulnerabilidades. El entorno eléctrico cuenta con millones de dispositivos, y precisamente los niveles descritos anteriormente tienen que ayudar a pensar que cada nivel aporta unas capas de seguridad y, por tanto, no sería práctico ni económico pedir a cada uno de los dispositivos contar con todos los controles.Por un lado es necesario conocer las vulnerabilidades de los equipos, identificar su vector de ataque y la criticidad de la vulnerabilidad en cuanto al proceso del que forman parte. Este enfoque debe ayudar a priorizar qué parchear y también a cuantificar el riesgo de no hacerlo, sabedores de que acometer un ciclo de parcheo de equipos inaccesibles que se cuentan por millones, puede llevar más de un año.Por otro lado tener un inventario correcto y determinar las conexiones entre activos y otros sistemas es crítico, y más donde el escenario lleva a un incremento de dichas conexiones.

La segunda perspectiva es el del enfoque de las medidas mitigadoras. El uso de herramientas que tienen en cuenta el legacy (obsolescencia) desde su diseño permiten aportar una seguridad continuada aunque el equipo tenga un sistema operativo antiguo. Este tipo de herramientas protegen la red y los endpoints, de modo que se acomete el denominado “parcheo virtual”, mediante el cual la vulnerabilidad detectada -explotada por un agente de amenaza pero generalmente no usada en el proceso- se puede cubrir a nivel de comunicación de red o no permitiendo la ejecución del proceso vulnerable en el equipo.

Evolución Futura

El sistema eléctrico se ha constituido en la base sobre la que se edifica la digitalización de toda la sociedad. La transformación del sector está obedeciendo en buena parte a una búsqueda de fuentes renovables, tanto desde la parte de la generación como del consumo, el rol del consumidor en el centro de ambas, y la adaptación de las ventajas de tecnologías de comunicación y computación ubicuas plantean también nuevas oportunidades y retos.

Este tipo de modernizaciones permite también la gestión descentralizada de la generación distribuida, modelo que tiene muchas ventajas ya expuestas pero que obliga a los agentes implicados a inversiones para aprovechar capacidades en el Edge, de abrir conexiones entre agentes y mediante entornos nube, restructurar equipos y procedimientos muy asentados para atender a las nuevas necesidades y, además, hacerlo involucrando a todos los agentes desde el principio.

CONCLUSIONES

El sistema eléctrico está cambiando sustancialmente tanto desde la oferta como desde la demanda de energía. Existen grandes áreas que se están transformando y creciendo enormemente como son el vehículo eléctrico y conectado o los hogares inteligentes y prosumidores (productores y consumidores) gracias a la conjunción de paneles fotovoltaicos, baterías, aerotermia o termostatos inteligentes, tal y como se muestra en la figura 10.

Dichas áreas traen riesgos de para los IoT y plataformas en Nube de suplantación de identidades, fraude o malware masivo que pueden afectar al sistema eléctrico de modos que no se habían planteado hasta ahora y requieren un enfoque específico. El auge de energías renovables y el reto de la descarbonización ya está obligando a modificar pautas del sistema eléctrico y, además, las energías renovables tienen una exposición mucho mayor a los vectores de ataque identificados que los sectores tradicionales.

Todas estas vías implican una exposición a la nube y una gran población de dispositivos IoT vulnerables sobre los que se deben establecer mecanismos de protección y de actualización que no recaigan en la responsabilidad del usuario. Esto implica considerar el riesgo a nivel de ecosistema y no dejarlo a

FIGURA 10
REAJUSTE DE OFERTA Y DEMANDA

Fuente: elaboración propia

nivel de dispositivo que, hasta ahora, ha llevado a no valorar medidas de protección en equipos IoT o IIoT, así como considerar que haya organismos que asuman las tareas de protección y parcheo de los dispositivos, involucrando a fabricantes y a operadores. Especial mención merecen los puntos de recarga de vehículo eléctrico, accesibles desde la calle por cualquiera, en los que se deben plantear cuestiones de protección, no ya solo a nivel de punto de recarga, sino de control de comunicaciones, acceso por red, accesos desde nube de terceras partes etc, y todo involucrando una red que se estima que puede llegar a suponer un consumo de más de 20GW. Se debe requerir más madurez a la aplicación de protocolos actuales para IoT y Nube (MQTT principalmente), de modo que los desarrollos permitan separar el envío de información de las operaciones de control y configuración así como de la adecuada notificación a los operadores críticos de cuándo los sistemas están siendo controlados o configurados por terceros.

Las redes de distribución también requieren una atención especial. Tal como se ha explicado anteriormente, se convierten en la gran correa de transmisión que habilita los múltiples flujos de energía y en varias direcciones, sin embargo, el 40% del parque eléctrico europeo tiene más de 40 años de antigüedad. Y esto solo será posible con más fortalecimiento de dicha red pero también con la digitalización de las subestaciones que permitan una gestión y optimización local de estos flujos.

Desde un plano tecnológico, tanto para conseguir eficiencias como seguridad, se propone avanzar en redes seguras definidas por software (Secure SD-WAN) que permitan la flexibilidad adecuada para estas redes que se estás redefiniendo así como una consolidación de arquitecturas seguras en la nube para los distintos planos de compartición de datos para asegurar la interoperabilidad. Además, se debe analizar la correcta aplicación de la filosofía de confianza cero (Zero Trust), desde la parte de dispositivos y comunicaciones M2M (Machine to Machine) como para la adecuada gestión de usuarios, tanto externos como propios pero con mayor movilidad; y todo dentro de las especificidades que conlleva el sistema eléctrico, tanto por obsolescencia como requerimientos de tiempo real o consecuencias en cascada. Y que estas pueden venir tanto de ataques como de inconsistencias ante transitorios, y que los transitorios serán cada vez más habituales, tanto a nivel de generación (curtailments) como a nivel de distribución (coincidencia de prosumers).

En definitiva, más tecnología para dar cobertura a las necesidades crecientes del sistema eléctrico, que abarca a más esferas de la vida, y la necesidad de un enfoque de ciberseguridad en todas esas esferas que permita crecer en resiliencia de todo el ecosistema.

REFERENCIAS

ABC News- Gridcog: Rooftop solar 'cannibalising' power prices as Australian generators pay to stay online https://www.abc.net.au/news/2023-09-23/rooftop-solar-cannibalising-australian-power-market/102889710

ACER: Network Code on sector-specific rules for cybersecurity aspects of crossborder electricity flows (NCCS) 2022

AEDIVE: Anuario de la Movilidad Eléctrica 2022-2023

America's Army: Ready Now, Investing in the future. Multidomain Operations 2019. https://www.army.mil/e2/downloads/rv7/about/usarmy_fy19_21_accomplishments_and_investment_plan.pdf

California ISO. Managing Oversupply. http://www.caiso.com/informed/Pages/ManagingOversupply.aspx

EMBER: Global Electricity Review 2023. https://ember-climate.org/insights/research/global-electricity-review-2023/

EPRI: A Guidebook to Centralized, Distributed, and Decentralized Intelligence, December 2017

EPRI: FEDERATED ARCHITECTURE FOR DISTRIBUTED ENERGY RESOURCES INTEGRATION, December 2020

Fortinet - State of Operational Technology and Cybersecurity Report, 2023. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Global Environment Facility. Military Embedded Systems – IoT, AI, and the future battlefield 2023 https://militaryembedded.com/ai/deep-learning/iot-ai-and-the-future-battlefield

Rooftop solar 'cannibalising' power prices as Australian generators pay to stay online. https://www.abc.net.au/news/2023-09-23/rooftop-solar-cannibalising-australian-power-market/102889710

El periódico de la Energía. https://elperiodicodelaenergia.com/la-curva-de-pato-ya-esta-aqui-la-solar-provoca-esta-temida-figura-en-el-pool-los-fines-de-semana/

NREL Distribution Grid Management in the Presence of Distributed Energy Resources https://www.nrel.gov/docs/fy23osti/84827.pdf

PACWorld: Enhanced Grid Reliability & Resilience – Wide-Area PAC (WAPAC) case studies. https://www.pacw.org/enhanced-grid-reliability-resilience-wide-area-pac-wapac-case-studies

PV-Magazine.com https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/

Siemens: Secure Substation Security Manual, 2021. https://cache.industry.siemens.com/dl/files/171/109759171/att_1090365/v1/securesubstation-securitymanualeng.pdf

Smart Grid Task Force Experts Group 2 Final Report 2019. https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

United States Special Operations Command Human Domain Concept, 5 September 2014.

SOBRE EL AUTOR

Agustín Valencia Gil-Ortega es Ingeniero Industrial por el ICAI, con 20 años de experiencia en el mundo de la energía con visión global de procesos, tecnología, riesgos, evolución regulatoria. Con formación adicional en distintas disciplinas como Director de Seguridad (UDIMA), Gestión de Mantenimiento (US), Tecnología Nuclear BWR (Tecnatom), Master Seguridad Informática (UPC-VIU) o CISM (ISACA). Actualmente como responsable de Desarrollo de Negocio de Ciberseguridad OT para Fortinet apoyando los proyectos de transformación digital segura en entornos como energía, agua, fabricación, sanidad, logística o movilidad, desde ICS/OT a XIoT y Cloud. Presidente del WG de Ciberseguridad en la ISA (International Society of Automation) Spain Chapter, miembro del "Cyber Resilience in electricity" WG por el World Economic Forum y miembro del grupo de expertos del Centro de Ciberseguridad Industrial (CCI). Profesor Asociado en la Universidad Pontificia Comillas-ICAI para los Masters de Ciberseguridad, Industria Conectada y Transformación Digital de la Industria.