ro, los riesgos que conllevan, los requisitos de seguridad, las medidas necesarias para proporcionarlas y los grandes retos que habremos de afrontar. Concluimos que, aunque los esfuerzos necesarios son grandes, los riesgos son en principio manejables y son una llamada a la acción.

Palabras Clave:

Seguridad, tecnologías, información, comunicaciones, amenaza, estrategia, ataques, redes, internet, ciberseguridad, vulnerabilidad, infraestructura crítica, SCADA, Red Inteligente, suministro eléctrico.

Abstract

There are many forces that have led modern societies to embrace a new concept for the production and distribution of electricity in the future: the Smart Grid. They include the scarcity of fossil fuel and the ecological impact of current energy sources. The intelligence of the future grid will depend on the use of technologies of information and communication. Indeed they will be indispensable to meet the challenges of the new energy sources which are intermittent and distributed. The energy supply infrastructures are among the most critical for the modern world, and the reliability of the distribution is the most important requirement to be met. This implies that ensuring the IT security of the smart grid will be of pivotal importance. But this will only be feasible with a demanding and large effort to cope with the security issues, conducted in a determined way by the different sectors of our society, including government authorities and private organizations, research groups and in particular all the different actors that will take part in the new electric grid.

The purpose of this article is to provide an overview of the security landscape of processes related with the management of command and control information and personal data in the context of the Smart Grid. Without entering into technical details that would distract us, we will discuss the purpose and use of smart technologies in the future grid, the risks associated with them, the security requirements that they must meet, and the means to implement them. We conclude that it is crucial to understand and treat the risks, and this endeavour will convey a set of new challenges that our society will have to face.

Keywords

IT security, technology, information, communication, threats, strategy, attacks, grid, Internet, cyber-security, vulnerabilities, critical infrastructures, SCADA, cyber threats, Smart Grid.

La Red Inteligente de distribución

El umbral de la tercera revolución industrial

Ya para el inventor Thomas Edison era evidente que la creación de nuevas tecnologías eléctricas aisladas, como la bombilla eléctrica o los generadores de energía, no es suficiente para lograr un impacto en la sociedad a gran escala. Es necesario también construir un sistema de distribución de energía para poner esos avances al alcance del público en general. Por ende, sus esfuerzos no se limitaban a la creación de equipos eléctricos aislados, sino a la transmisión de energía eléctrica a los hogares privados. En 1882 abrió la primera red de distribución de energía, lo que condujo rápidamente a la utilidad práctica de los avances tecnológicos y a un incremento explosivo en su uso. Sin embargo, él usaba corriente continua (DC), que resultaba útil para transmitir energía solamente en cortas distancias.

Nikola Tesla descubrió que la corriente alterna era capaz de superar las limitaciones de la transmisión de energía y resultaba más adecuada para la transmisión eléctrica sobre distancias largas. En 1895 George Westinghouse usó esta tecnología para conectar un generador en las cataratas del Niágara y transmitir en corriente alterna energía eléctrica a la ciudad de Búfalo, a unos 35 kilómetros, comenzando así lo que Marshall McLuhan denominó Edad de la Electricidad.

Desde entonces, la estructura de la red de distribución ha mantenido la misma arquitectura básica: la generación no tiene que estar cercana al consumo y la electricidad fluye unidireccionalmente y con distribución centralizada desde las plantas generadoras hasta los consumidores finales, ya sean hogares o industria. La fiabilidad del sistema se asegura teniendo un exceso de capacidad (reserva) para responder a la posible demanda en prácticamente cualquier momento. Los sistemas eléctricos fueron diseñados y construidos en tiempos en los que la energía hidráulica y aquella contenida en los combustibles crudos era relativamente abundante y barata y no existía la imponente necesidad de ahorrar energía, o de optimizar, a toda costa, el consumo. La abundancia de energía eléctrica ha sido un factor importantísimo de la industrialización y desarrollo de España, Europa y, por supuesto, del mundo entero.

La sociedad de la información y la tercera revolución industrial se vienen produciendo desde la segunda mitad del siglo pasado, con avances electrónicos y de TIC como el transistor, televisión, computación, robótica, Internet, etc. Pero son varios los autores, como Jeremy Rifkin, que consideran a la Red Inteligente de distribución como la puerta a la tercera revolución industrial, (*The Third Industrial Revolution,* Nueva York, Macmillan, 2011). Los cinco pilares de la tercera revolución industrial, según Rifkin, son:

I. El reemplazo de las fuentes convencionales de energía por energías renovables.
II. La transformación de los edificios y casas en microplantas de energía que pueden acceder a fuentes locales de recursos renovables.
III. La instalación de tecnologías de almacenamiento de la energía, como podrían ser aquellas para la creación, almacenamiento y procesado del hidrógeno. Estas tecnologías se usarán en edificios, casas o ciudades para usar efectivamente la energía intermitente o excedente en momentos de poca demanda.
IV. Usar tecnologías de información y comunicación, y en particular Internet, para crear redes de nodos que, habiendo generado localmente energía, negocian precios y venden sus excedentes a la red local o global.
V. El reemplazo de las flotas existentes de transporte convencional por vehículos eléctricos, que pueden almacenar energía y así comprar en momentos de mayor oferta y vender en momentos de mayor demanda.

El uso de tecnologías de la información y las comunicaciones permitirá descentralizar tanto la producción como el control y la optimización de la generación y distribución de energía eléctrica de una forma sin precedentes y radicalmente diferente a la existente hasta hoy, orientada hacia la generación centralizada de electricidad en grandes centrales eléctricas.

Fuerzas que conducen a la Red Inteligente

Son muchas las razones que obligan actualmente a diseñar de nuevo la arquitectura y el funcionamiento de la red eléctrica y que nos conducen a la Red Inteligente. Las subdividimos en razones de la seguridad de suministro, de protección del medio ambiente, los cambios en el mercado y la necesidad de nuevos mecanismos de optimización de la red.

La seguridad de suministro

Los combustibles fósiles –carbón, petróleo y gas natural– son limitados, y el petróleo está actualmente muy cerca de su clímax de producción. Desde antes de la primera crisis energética en 1973 los precios de los combustibles van aumentando en oleadas y se han presentado varias veces tiempos de gran carencia en el suministro de petróleo, electricidad u otros recursos energéticos. Estas crisis afectan negativamente al resto de la economía, aumentando las probabilidades de una recesión: al crecer los costes de energía suben también los costos de todas las industrias, mientras que el precio de la gasolina lleva al consumidor a una reducción de sus gastos y a una menor confianza en la economía. Los países dependientes del petróleo tienen una gran motivación por ahorrar

energía y buscar e integrar fuentes alternativas. Ninguna de ellas será tan barata como lo ha sido el petróleo, ni tan conveniente o simple de transformar energéticamente, pero serán necesarias para asegurar el suministro energético.

La ecología y la protección del medio ambiente

Muchas razones nos han llevado a tener conciencia de la necesidad de preservar el medio ambiente y nos obligan a buscar energías renovables, de baja emisión y de pocos residuos dañinos. Tres ejemplos son: la creciente contaminación atmosférica, como ha sido observada por ejemplo en los últimos años tan drásticamente en China; el riesgo cada vez más inminente de un cambio climático que podría resultar desastroso para la humanidad, y las dificultades en el dominio de la seguridad de la tecnología nuclear, como lo mostró Fukushima: las grandes dificultades que ha tenido Japón con esta planta nuclear después del tsunami han sido el motivo principal para que el Gobierno alemán decidiera la transición energética (*energiewende*).

El mercado

Uno de los impulsos hacia este cambio en el sistema es la desregulación y liberalización de los mercados, así como la reestructuración de la industria en general y del sector eléctrico en particular. Muchos gobiernos esperan un aumento en la innovación y la competitividad, así como en la reducción de precios y la eficiencia del suministro. Aún hoy en día las redes de energía siguen siendo manejadas en su mayoría por monopolios de generación y transmisión, pero estas estructuras están evolucionando hacia una gran red de muchos productores competitivos de energía y otros participantes en el sistema.

Optimización de las operaciones del sistema de distribución

Por otra parte, la necesidad de recurrir a fuentes alternativas de energía conlleva un costo de inversión y un mayor costo de producción, lo cual incita naturalmente a buscar métodos de usar óptimamente los excedentes de producción. Será imposible mantener reservas tan altas que en cualquier momento cubran la demanda existente: muchas energías alternativas son *intermitentes,* es decir, con una fluctuación de volumen enorme que depende del estado del tiempo (sol y viento), de las mareas, de la cantidad de lluvias, etc. Para resolver este problema será necesario que el usuario final participe activamente en optimizar el uso de energía, allanando las curvas de demanda. Ideal sería que los usuarios tomen menos energía de la red en momentos de baja producción. Esto se logra con mecanismos de *respuesta de la demanda* (DR, por sus siglas en inglés), incen-

tivando al público general a reducir el uso de electricidad en momentos en los que la demanda es alta. También será necesario que los usuarios no solo consuman, sino que también produzcan y almacenen electricidad dentro de la misma red.

Otra consecuencia del uso de fuentes de energía renovable será que las redes eléctricas dejarán de ser unidireccionales. Dependiendo de las condiciones climáticas en las diferentes regiones, la electricidad puede fluir por ejemplo de norte a sur o de sur a norte. Para adaptar la red y lograr que el sistema permanezca estable, es necesario tener una información muy detallada de las características eléctricas en los diferentes puntos así como pronósticos minuciosos de oferta y demanda.

¿Qué es la Red Eléctrica Inteligente (Smart Grid)?

Sucintamente, la función de la Red Inteligente es la de coordinar inteligentemente las acciones de generadores, distribuidores, consumidores y *prosumidores* (que cumplen con los dos papeles, de producir y consumir energía) de una forma eficientemente sostenible, económica y segura, facilitando la integración dinámica de generadores ecológicamente favorables para la conservación del medio ambiente, logrando que el usuario participe activamente en la optimización de las operaciones del sistema y brindándole al consumidor una mayor información y posibilidad de elección. La Red Inteligente usa las tecnologías de la información y las comunicaciones (TIC) tanto en servicios innovadores como en tecnologías inteligentes de monitoreo, control, comunicación y autorregeneración.

Comencemos por decir que la Red Inteligente no es un concepto estático, sino más bien una *visión* con el objetivo de manejar eficientemente los recursos energéticos. Esta propuesta se concretiza en el uso de tecnologías innovadoras, de las cuales muchas están aún en desarrollo, para gestionar eficientemente la generación, distribución, medición, almacenamiento y consumo de la energía eléctrica respondiendo a las necesidades de una creciente demanda de energía y de crear una base sostenible de energía que sea capaz de reducir el impacto climático y ecológico. Para ello, es absolutamente indispensable el uso de TIC, encargadas de tareas vitales a todos los niveles del sistema, desde la adquisición y procesamiento de señales hasta el control técnico del sistema dinámico de flujo de energía eléctrica y la integración de las acciones de todos los actores en un solo sistema coherente.

La Red Inteligente de distribución eléctrica es considerada por muchos autores como el proyecto tecnológico más grande de la humanidad. Un esfuerzo de tal envergadura no podrá llevarse a cabo de un solo golpe. La construcción de la Red Inteligente contará con varias etapas, las inversiones crecerán con el tiempo y los beneficios obtenidos serán visi-

bles paulatinamente. La Red Inteligente no se desarrollará a la misma velocidad en todas partes. Al contrario: poco a poco van apareciendo islas inteligentes de gestión y distribución local, llamadas *microgrids* (microrredes), en universidades, centros industriales o comerciales, etc. Estas redes usan pequeñas fuentes de energía, relativamente baratas y fiables, como lo son microturbinas, paneles fotovoltaicos o pilas de combustible, colocadas en los predios de los clientes. La *microgrid* opera como un módulo controlable, conectado a la red global, con el fin de suministrar potencia eléctrica y energía calorífica localmente, mejorando la fiabilidad, reduciendo el mantenimiento de las tensiones locales, logrando mayor eficiencia al usar el calor residual y disminuyendo las emisiones totales.

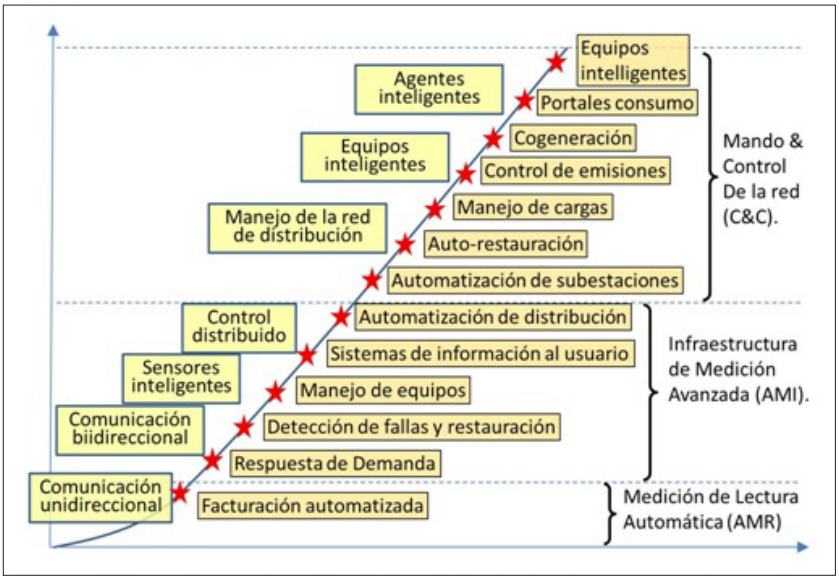

Figura 1 Etapas de construcción de la red. Tanto las inversiones en tecnología e infraestructura (rectángulos a la izquierda) como las características del sistema y los beneficios obtenidos como retorno de la inversión (rectángulos de la derecha) van produciéndose con el tiempo (eje horizontal). Algunos de estos conceptos los discutiremos en la Sección EL PAPEL DE LAS TIC EN LA RED INTELIGENTE. Las características de la Red Inteligente

La Figura 1 muestra las tres fases principales de la implementación de la red: la introducción de medidas automáticas de medición, la infraestructura de medición avanzada y los mecanismos de mando y control de la infraestructura, incluyendo la provisión de las herramientas para los mercados electrónicos de energía. La figura muestra también que el retorno de la inversión se logrará en los diferentes pasos, según el arquitecto principal de la primera *microgrid* en Canadá, el profesor H. Farhangi[1].

[1] FARHANGI, Hassan. "The path of Smart Grid". *Power & Energy Journal.* IEEE enero de 2010, vol. 8, n.º 1.

La Red Inteligente abarcará toda la cadena del negocio de la energía eléctrica; va a integrar a otros actores en áreas vecinas, como lo son el gas y el agua, y además cruzará las fronteras geográficas y políticas, ya que en muchos casos será necesario complementar los servicios de generación y de almacenamiento de los diferentes países. Así como en el sur de Europa es más fácil generar energía solar, en los países escandinavos es más fácil almacenar la energía en embalses hidroeléctricos. Aún más: la Red Inteligente entrará a formar parte de una red más global, con funciones que van más allá del suministro de energía, incluyendo la supervisión del transporte, la distribución de bienes, el bienestar de los habitantes, el servicio médico, la calidad del agua y mucho más. Ya son un buen número los proyectos que están construyendo estas redes inteligentes, en particular en el contexto de las ciudades inteligentes (*smart cities*).

El sistema actual de suministro eléctrico

Arquitectura y características del sistema actual

El sistema de suministro eléctrico comprende el conjunto de recursos útiles para la generación, transporte y distribución de la energía eléctrica. La Figura 2 presenta muy esquemáticamente el sistema de distribución eléctrico actual. La red actual es unidireccional y está dividida en varias partes que operan con cierta relativa independencia las unas de las otras, controladas por equipos SCADA que comparten alguna información de una forma muy limitada. Todas estas características de la red cambiarán en la red futura.

Este sistema está dotado de un sistema de supervisión que actúa en tiempo real, compuesto de mecanismos de control, seguridad y protección cuyo fin primordial es mantener la calidad del servicio, balanceando la generación con la demanda de los usuarios y compensando las posibles incidencias y fallas que se presenten. No es fácil mantener el balance porque la electricidad fluye casi a la velocidad de la luz y no es fácil almacenarla de una forma ni rentable ni inmediata; por lo tanto, tiene que ser producida en el momento en que se usa. El flujo de electricidad no se deja manejar como el de los líquidos, abriendo o cerrando válvulas, ni se deja dirigir como las conexiones telefónicas: la energía eléctrica se mueve libremente por todos los caminos abiertos, dividiéndose de acuerdo con las reglas físicas de la impedancia.

Por otra parte, la red está equipada con un sistema de administración y gestión empresarial compuesto de mecanismos para pronosticar recursos, planificar la producción y gestionar el comercio, incluyendo tanto las subastas de energía como la facturación y remuneración a los distintos agentes del mercado. Estos dos, el sistema de supervisión y control y el

de administración y gestión empresarial, son distribuidos y dependen en gran parte de tecnologías de la información y las comunicaciones.

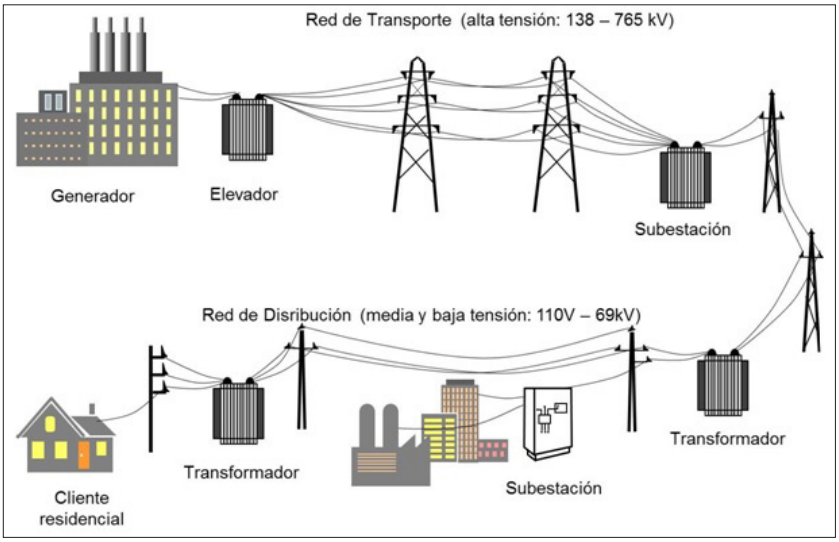

Figura 2. El sistema de distribución eléctrico actual (esquema simplificado).

Con frecuencia, diferentes partes del sistema están operadas y gestionadas por compañías distintas. Por lo tanto, el sistema de control es de carácter distribuido y jerárquico: los equipos controladores en las centrales de generación, la red de transporte, las subestaciones, la red de reparto y las redes de distribución están supervisadas y controladas por equipos autónomos pero que se comunican entre sí para lograr un equilibrio global.

Las subestaciones o los transformadores tienen con frecuencia unidades terminales remotas, más conocidas como RTU (por la sigla en inglés), dispositivos dotados con microprocesadores que obtienen las señales de los procesos con equipos sensores integrados o por medio, por ejemplo, de unidades de medición de fase. Las RTU envían la información agregada a un sitio remoto donde se encuentran equipos SCADA que procesan la información de un gran número de señales de diferentes lugares, con precisión de milisegundos. Los sistemas SCADA, acrónimo en inglés de "supervisión, control y adquisición de datos", permiten monitorear, controlar y supervisar procesos de distribución eléctrica a distancia controlando el proceso automáticamente. Además, estos equipos, estando conectados con salas de control, permiten la visualización del estado de la red y la entrada de comandos de control, retroalimentando en tiempo real los dispositivos de campo.

Anunciando ya la Red Inteligente, las líneas de transmisión y distribución están siendo dotadas de dispositivos inteligentes que controlan localmente sensores y actuadores. Un ejemplo nos lo dan los relés de medición y de protección, capaces de calcular las condiciones operativas de los circuitos y, por ende, de detectar y localizar los fallos y, dependiendo de su inteligencia y de las condiciones, incluso de diagnosticar el tipo de fallo y de accionar interruptores inteligentes cuando se detectan problemas. Estos interruptores son necesarios para aislar equipos y redes, para así protegerlos y minimizar el número de usuarios afectados al producirse apagones.

Podemos concluir que las TIC ya son, hoy en día, absolutamente esenciales para mantener la estabilidad del sistema de suministro eléctrico.

Los sistemas de administración y gestión empresarial relacionados con la industria eléctrica dependen también enormemente de las TIC. Pero para nuestros propósitos estos sistemas son algo menos interesantes por dos razones: primero, son, en comparación, menos críticos, ya que la estabilidad de la red no depende tanto de ellos y porque son más fáciles de mantener redundantes; segundo, son similares a los que convencionalmente se usan en el mundo comercial diversificado, donde los problemas de ciberseguridad han sido bien estudiados.

Fiabilidad

Una infraestructura crítica es aquella que al fallar, causa graves problemas de suministro a la sociedad. Más precisamente, la Ley 8/2011, *por la que se establecen medidas para la protección de las infraestructuras críticas,* la define de la siguiente forma: un servicio es llamado *esencial* si es necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento del Estado y la Administración Pública; un conjunto de redes, instalaciones, sistemas y equipos físicos y de TIC sobre los que descansa el funcionamiento de un servicio esencial se llama *infraestructura crítica* si su funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

La fiabilidad es la primordial exigencia de la sociedad moderna para cualquiera de las tecnologías usadas en las infraestructuras críticas.

Con frecuencia se considera la infraestructura del sector de energía eléctrica, tanto de generación como de transmisión eléctricas, como la más crítica de las infraestructuras: cuando esta deja de funcionar se paralizan todas las otras (los transportes, incluyendo la distribución de bienes de uso común; el servicio de salud en hospitales y clínicas; las redes de comunicación públicas; etc.). Por ejemplo, los daños en el sistema eléctrico

de Auckland, Nueva Zelanda, en 1996 obligaron a 60.000 de los 74.000 empleados en las áreas afectadas a trabajar desde su casa o desde oficinas alternas, mientras que la gran mayoría de los residentes de los 6.000 apartamentos afectados se vieron forzados a mudarse mientras se buscaba una solución al problema.

La fiabilidad del sistema eléctrico puede definirse en términos de la capacidad del sistema de entregar la potencia eléctrica a los consumidores de una forma aceptada y en las cantidades establecidas y deseadas.

La Corporación de Fiabilidad Eléctrica de América del Norte (por sus siglas en inglés: NERC) divide la fiabilidad en dos categorías: adecuación o (con)fiabilidad estática, y seguridad o (con)fiabilidad dinámica.

Adecuación significa que los recursos necesarios están presentes y accesibles para generar, operar, transmitir y suministrar electricidad de la forma proyectada y de acuerdo con los requisitos de calidad de onda esperados de una forma continua –en todo momento–, incluyendo los casos de una demanda muy alta, durante reparaciones rutinarias o cuando haya fallas, contingencias o problemas previsibles, como las debidas a tormentas eléctricas fuertes en la región. Entre esos recursos podemos contar los programas de respuesta de demanda, que, como ya veremos, reducen los picos de demanda energética.

La *seguridad*, por otra parte, es la capacidad del sistema de soportar perturbaciones imprevistas, como cortocircuitos o pérdida de elementos debida a causas naturales así como a ataques intencionales y no intencionales, tanto físicos o cibernéticos, de consumidores no maliciosos, trabajadores internos, competidores, terroristas o enemigos. En particular, la seguridad implica que el sistema como tal resultará intacto después de salidas u otras fallas ocurridas en los equipos. Seguridad incluye la capacidad de recuperarse de los problemas cuando se presenten fallas de la forma más rápida posible, restaurando la prestación del servicio y el desempeño de los elementos.

La NERC ha desarrollado un método y varios estándares para asegurar la fidelidad del suministro eléctrico basado en varios principios fundamentales, de los cuales el más importante es, como ya se ha dicho, balancear continuamente la demanda y la oferta y mantener el sistema estable, pese a contingencias o fallos que se presenten. La demanda es hasta cierto punto predecible, como también lo son las desviaciones estadísticas a esperar, y las curvas de demanda son analizadas y actualizadas permanentemente.

El peligro de un desequilibrio entre oferta y demanda radica sobre todo en que la frecuencia de la corriente alterna (50 o 60 Hz normalmente) puede ser afectada sustancialmente, subiendo si la demanda es menor o bajando si la demanda es mayor. Variaciones pequeñas en la frecuencia

no son problemáticas, pero si sube demasiado, la velocidad a la que giran los generadores empieza a fluctuar, causando vibraciones que los pueden dañar. Las bajas frecuencias se manejan automáticamente mediante cortes sistemáticos de energía en pueblos o en barrios, cada uno a su vez, para evitar una caída total. Por otra parte, un desequilibrio también puede ser el efecto de contingencias inesperadas, como cuando se aíslan partes de la red, causando a su vez un efecto cascada.

El otro peligro en un desequilibrio es la pérdida o subida de voltaje, que puede dañar motores o provocar inestabilidades en la red, o puede exceder los límites de capacidad de los aislantes y causar descargas disruptivas y arcos eléctricos muy peligrosos que ocurren cuando ráfagas de electricidad saltan de un conductor eléctrico a otro. Los problemas de inestabilidad pueden aparecer en cuestión de fracciones de segundo. En Norteamérica, en agosto del 2003, una parte del sistema de interconexión oriental se desestabilizó, creando un apagón muy fuerte en un área muy grande. Mantener la fiabilidad de la red eléctrica es un proceso continuo y complejo que requiere operadores muy hábiles y altamente capacitados, de equipos inteligentes especializados y de una planificación, diseño y desarrollo supremamente cuidadosos.

Es interesante entender cómo, aun siendo tantos los peligros y posibles problemas que pueden presentarse en el suministro de energía, el sistema es relativamente tan estable. Las razones son: primero, hay un sistema estandarizado y riguroso para mantener y verificar planes de operación, incluyendo evaluaciones sistemáticas a largo plazo, análisis de contingencias y planes bastante detallados tanto a corto, mediano y largo plazo; segundo, el sistema siempre está preparado para todas las posibles contingencias simples (donde falla tan solo un equipo), aun en el peor de los casos; tercero, el sistema está preparado para dar respuestas rápidas aun si hay fallas múltiples, y, por último, el sistema cuenta con capacidades extras para todas sus funciones, como por ejemplo equipos redundantes, pero también reservas en las capacidades de producción y transmisión.

Lo que debemos asegurar es que estos procesos de seguridad y fiabilidad se apliquen también en la Red Inteligente, adaptándolos a las necesidades de la ciberseguridad y las amenazas a las tecnologías de la información y las comunicaciones que la red de distribución del futuro va a requerir.

Requisitos de seguridad de las TIC en el suministro eléctrico

La seguridad en TIC es un concepto muy amplio que cubre diferentes propiedades con muchos matices, una gran cantidad de mecanismos técnicos que pueden ser implementados en *hardware* o en *software* y una serie

de procesos que deben ser seguidos durante todo el ciclo del sistema, desde la definición de requisitos hasta el uso del sistema y su actualización o corrección. Wikipedia restringe el concepto de seguridad de las TIC (http://es.wikipedia.org/wiki/Seguridad_informática) de una forma que, para nosotros, resulta totalmente insuficiente:

> *La seguridad informática comprende (…) todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.*

Si bien es cierto que, en general, la *confidencialidad* es uno de los aspectos más importantes de la seguridad informática, hay otras tres propiedades que para la red de distribución inteligente son aún más importantes: *integridad, disponibilidad y privacidad* (esta última se refiere a la protección de información personal de un individuo o un grupo de ellos). La privacidad está muy cercana a la confidencialidad, y a veces se les ve como sinónimos, pero para nuestros propósitos es conveniente considerarlas por separado. En este contexto, se llama "información personal" o "dato personal" (*Personally Identifiable Information* o PII es el término predominante en los Estados Unidos) a cualquier información relacionada con una persona natural que puede usarse, conjuntamente con otras fuentes de información, para identificar, contactar o localizar a esta persona en concreto, directa o indirectamente.

En lo que concierne a las redes de distribución, la propiedad de seguridad más vital es, indudablemente, la *integridad*. En su sentido común, este concepto está relacionado con completitud (la condición de no carecer de ninguna de sus partes) y la coherencia o la condición de ser intachable. El sentido técnico de la palabra en el contexto de las TIC, aunque siendo bastante preciso, abarca muchos aspectos diferentes. En una Red Inteligente, una gran cantidad de datos son generados por sensores o por la introducción de datos por medio de usuarios o por las interfaces con otros sistemas. Estos datos pueden ser modificados, y en algún momento serán leídos con el propósito de procesarlos, agregarlos, filtrarlos o analizarlos. Las reglas que determinan quién puede crear o modificar datos y bajo qué condiciones son las reglas de *integridad*. Las reglas que definen quién puede leer los datos, son las reglas de *confidencialidad*. Las reglas que rigen el uso de los datos personales, los propósitos válidos para su uso, los terceros a quienes pueden ser distribuidos, etc. son las reglas de *privacidad*. La *disponibilidad*, en su aspecto de seguridad de las TIC, es la resistencia del sistema a los así llamados ataques de denegación de servicio, que serán discutidos más abajo.

Las cuatro exigencias de seguridad –integridad, privacidad, confidencialidad y disponibilidad– son requisitos de alto nivel y son independientes de los dispositivos a disposición y de la tecnología con que van a ser im-

plementados. Para garantizar estos requisitos, es necesario reducirlos sistemáticamente a unos más específicos y concretos, que luego es necesario implementar. Ejemplos de tales requisitos concretos son: sistemas de alarma, detección de intrusos o de ataques, mecanismos para resistir intrusos o ataques y de recuperación si es necesario, métodos de identificación, autenticación, autorización y control de acceso, así como protocolos para proteger la comunicación, distribución de claves criptográficas y sistemas para calcular la fiabilidad de los elementos en el sistema.

Este artículo no intentará discutir cómo o con que tecnologías se pueden garantizar estos requisitos.

Integridad

Para que la red funcione correctamente es necesario que los datos procesados por el sistema estén completos y que correspondan a lo esperado, es decir, que sean coherentes con los valores de los sensores, con los parámetros que entran los administradores, con los usuarios y con los datos que provienen de otros sistemas, como el pronóstico del tiempo, de las horas de sol, de la intensidad de los vientos o del caudal de las aguas.

Esta propiedad, precisamente, es la integridad del sistema. Para que se cumpla, es necesario que los datos no puedan ser modificados sin autorización al transitar en los canales de comunicación o cuando están en un banco de datos o en otra memoria, temporal o permanente. Estos aspectos de integridad pueden ser implementados con métodos criptográficos, como son las firmas digitales. Las dos dificultades en este contexto residen en la necesidad de usar tales mecanismos en procesadores de poca capacidad computacional (como son los sensores) y en la necesidad de distribuir las claves necesarias y protegerlas contra atacantes. Otro aspecto de integridad es que los datos sean solamente generados por las entidades autorizadas. Para esto son necesarios adicionalmente los métodos de control de acceso, que, por lo menos en teoría, se comprenden bien y no presentan mayores dificultades, excepto por la gran cantidad de elementos que actúan en el sistema. El siguiente aspecto de integridad es el más difícil de asegurar: que al crear, modificar o comunicar los datos los procesos correctos hayan sido usados en las secuencias correctas y en el contexto correcto. De nada sirve asegurarse de que tan solo un administrador muy fiable sea capaz de cambiar la configuración del sistema si el programa que usa para hacerlo es malicioso y actúa de una forma no esperada.

Privacidad

La protección de la privacidad significa, antes que nada, respetar los límites establecidos por la ley para la recogida y utilización de los datos personales. El texto de referencia en este respecto en el marco europeo

es la Directiva Europea 95/46/CE, que define las pautas principales y los principios de orientación para la protección de los datos. Los estados miembros han implementado esta directiva, creando legislaciones nacionales que prevén recursos judiciales para los casos en los que los derechos de privacidad no sean respetados, así como organismos nacionales independientes encargados de la supervisión de la protección de los mencionados datos. En España, esta entidad de control encargada de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal es la Agencia Española de Protección de Datos (AEPD), creada ya hace más de veinte años. Las directivas y las legislaciones se aplican no solo a los datos tratados por medios automatizados de las TIC, sino también a aquellos manejados en ficheros tradicionales en papel.

La privacidad de un trozo de información dado, en un momento dado, puede tener distinta importancia dependiendo de la situación concreta, de las costumbres y de la cultura de los individuos en cuestión y de la sociedad en que viven. Esto es particularmente válido para aquella información que delata las costumbres, actividades, convicciones, estado familiar, etc. de un individuo. Para una persona en un cierto contexto social, no es problema revelar que es musulmán o que su familia cuenta con seis hijos, pero para otra persona en otro contexto, esta información puede ser muy delicada.

Esto es pertinente con la Red Inteligente por dos razones: primero, el interesado mismo tiene el derecho a oponerse a cierto tratamiento de sus datos, a la forma de su uso o al nivel de detalle que contengan, y segundo, los datos personales procesados en la Red Inteligente pueden dar información sobre asuntos realmente personales de los individuos. Ya hoy en día, con la aparición de contadores inteligentes, hay bastantes dudas respecto a la privacidad de la información personal de los consumidores. Datos sobre el consumo eléctrico en una familia, si son muy minuciosos y tomados a una alta frecuencia, pueden ofrecer muchos detalles sobre la vida de la familia: en qué momento se encendió y se apagó el televisor o el horno, la lavadora, etc. Se puede saber si la familia no está en casa o si tiene invitados, si la ducha fue tomada deprisa, si hubo desayuno, etcétera. Los datos del coche eléctrico pueden presentar evidencia sobre los sitios que ha visitado el usuario, y tal vez podrían ser un indicio de las actividades relacionadas. Si los usuarios acceden al sistema remotamente, tal vez los datos podrían indicar si están de vacaciones y dónde.

Muy sucintamente, los principios básicos de privacidad son los siguientes: los datos deben ser correctos y actualizados; los datos deben ser recogidos y procesados con fines determinados, explícitos y legítimos, y solo ser usados para tales fines; el interesado debe conocer esos fines y la forma de tratamiento de los datos y haber dado su consentimiento de uso; el interesado tiene derecho de acceso a sus datos; ciertas categorías o tipos de datos (aquellos que puedan revelar algo sobre el origen racial

o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, el estado de salud, la orientación o actividad sexualidad o la situación personal o familiar) no pueden ser recogidos o requieren de permisos y provisiones especiales; las autoridades competentes han de recibir información sobre la transmisión ilícita, alteración, difusión o acceso no autorizados de los datos personales, y, por último, los datos deben ser tratados en un sistema seguro que ofrezca confidencialidad.

En esta lista se ve claramente la diferencia entre confidencialidad y privacidad: la privacidad presupone la confidencialidad, pero la primera abarca mucho más.

Confidencialidad

En términos generales, la confidencialidad es la propiedad de que los datos almacenados en sistemas de información o transmitidos por redes de comunicación no queden al alcance de personas que no cuenten con la debida autorización de leer los datos. En el caso de la red de suministro, hay bastante cantidad de datos que deben ser protegidos en este sentido. Por ejemplo, detalles sobre la arquitectura física de la red son importantes de asegurar porque en manos de terroristas facilitan un ataque físico. Similarmente, los datos sobre planes en caso de contingencia, reservas en la producción o transmisión, pronósticos de consumo, datos económicos del sistema, etc. deben también ser protegidos. En cuanto a los datos personales de los usuarios, de su consumo y sus cuentas tienen un valor particularmente importante por motivos de privacidad, como hemos discutido arriba.

Disponibilidad

La disponibilidad es la propiedad de que los sistemas se encuentren a disposición de los usuarios o quienes tienen que acceder a ellos en los momentos en los que lo necesiten. En este sentido general, es prácticamente lo mismo que la fiabilidad del sistema. Pero hay un sentido particular de la palabra relacionado con los requisitos de seguridad de las tecnologías de la información y las comunicaciones. Se trata de que tales sistemas deben ser inmunes o altamente robustos a los así llamados ataques de denegación de servicio: una forma típica de ataque que se da por saturación del servicio o de las redes de comunicación, bloqueando el servicio con un enorme número de solicitudes o sobrecargando la red con mensajes artificiales que dificultan o impiden el acceso legítimo. Hay otras formas más sofisticadas de poner en riesgo la disponibilidad del sistema, atentando contra su integridad; por ejemplo, cambiando las credenciales que usa. Hay una gama amplia de mecanismos que se pueden implementar en la infraestructura de TIC: el uso de sistemas con re-

dundancia, arreglos de discos, equipos en alta disponibilidad, servidores espejo, virtualización, replicación de datos, redes de almacenamiento, enlaces redundantes, etc. La solución adecuada depende de los servicios o datos que se necesita proteger y del nivel de servicio que es necesario proporcionar.

Problemas de ciberseguridad en el sistema actual de suministro eléctrico

Cómo funcionan los ataques

No queremos aquí discutir en profundidad los ataques que han sido descubiertos al sistema de distribución eléctrico. Más allá de los ataques casuales, nos han de preocupar los que son llamados una *amenaza avanzada permanente* (en inglés: APT, *advanced persistent threat*), que son formas avanzadas de ganar inteligencia clandestinamente, de una forma continua y persistente sobre una compañía, un sector, una infraestructura crítica o un grupo particular de individuos.

Es necesario entender cuáles son los peligros en líneas generales, cómo funcionan los ataques avanzados y qué es necesario hacer para mitigar los riesgos correspondientes, sin entrar a discutir las técnicas usadas. En términos muy generales, un ataque avanzado se logra de la siguiente manera:

Primero, se recoge información relevante para el ataque inicial. Los atacantes buscan información en Internet y en otros medios accesibles al público para saber qué empleados de las diferentes compañías eléctricas o las empresas relacionadas pueden ser atacados. Para completar la información se usan métodos de la así llamada *ingeniería social*, por ejemplo, pidiendo datos por teléfono haciéndose pasar por una persona autorizada a tener la información. Ya teniendo una lista de primeras víctimas, de sus cargos, entorno de trabajo, nombres de colegas, etc., se les envía mensajes electrónicos fraudulentos que fingen venir de un jefe, de un compañero de trabajo, de un centro que organiza conferencias de interés profesional, de compañías que proporcionan sistemas de protección, etc.

Este tipo de *mail* fraudulento se usa para obtener más información o para robar las credenciales de la víctima y poder entrar en servidores donde la víctima tiene acceso. En ciertas ocasiones, es posible usar estos correos fraudulentos para inyectar código malicioso al sistema de la víctima. Este método de usar mensajes maliciosos construidos para ciertas personas en particular y ya dirigidos a un objetivo preestablecido se llama *spear-phishing*, y es combinado con el de robar credenciales, contraseñas o claves secretas para lograr una suplantación de identidad. Una vez dentro de la organización, se buscan nuevas contraseñas, programas

vulnerables, servicios de comunicación o de administración de los que se pueda abusar y se inyectan códigos maliciosos dentro de programas ya existentes y conocidos, tratando de esconder su verdadero carácter e intenciones. Este *malware* usualmente tiene capacidades de contactar a un servidor malicioso que lo controla o lo guía y abre un canal para que el atacante "entre" al sistema comprometido. Esto se conoce como una *puerta trasera*.

Con frecuencia, se inyectan otros troyanos en archivos más importantes para el sistema operativo del ordenador, hasta lograr la persistencia del ataque. De esta forma, aunque se reinicie el ordenador, el troyano, habiendo infectado archivos del sistema, sigue presente. Este puede ahora espiar las actividades de los administradores y hasta leer lo que escriben en el teclado (esto se conoce como *keyloggers*) o enviar señales a otros ordenadores, buscar claves criptográficas, etc. Mientras espera el momento adecuado para el ataque final, tal vez coordinándose con otros programas maliciosos a través del servidor malicioso, puede seguir coleccionando información sobre los sistemas de defensa física o cibernética, la estructura del sistema SCADA y los programadores lógicos, documentos relevantes, nombres de personas o direcciones de email, valores de parámetros, etc. En ciertos casos, el *malware* puede quedarse inactivo durante semanas o meses antes de empezar el ataque interno para el cual fue diseñado.

Stuxnet

Stuxnet es el nombre de un código malicioso (troyano o *malware*) descubierto en julio de 2010 por una anomalía funcional que atrajo la atención de operadores. Hay indicios recientes de que versiones preliminares (versión 0.5) aparecieron ya en el año 2005. Es el primer código malicioso descubierto que reprograma sistemas de control y supervisión de procesos SCADA, así como los controladores lógicos programables (PLC) conectados a los mismos. El análisis del *malware* duró muchos meses, porque usa diferentes tipos de cifrado y ofuscación muy avanzados. El *software* puede espiar, afectar, y dañar las infraestructuras críticas controladas sin que el personal administrativo sea capaz de reconocer los daños a tiempo.

Stuxnet es un *software* de una complejidad nunca vista antes, que con seguridad necesitó un equipo de programadores expertos muy completo, con conocimientos muy detallados acerca de distintas técnicas de programación, de los equipos a los cuales los ataques están dirigidos y de los procesos industriales que se quieren manipular. La dimensión de ese esfuerzo indica que fue muy costoso de programar y que probablemente su construcción contó con el apoyo de una organización grande o de un organismo estatal de algún país. Stuxnet emplea cuatro vulnerabilidades

en el sistema operativo de Windows de Microsoft, hasta ese momento desconocidas, para penetrar al sistema SCADA de Siemens. Adicionalmente, Stuxnet puede generar firmas digitales con dos certificados auténticos robados de autoridades de certificación.

Son muchas las indicaciones de que Stuxnet fue diseñado explícitamente para retrasar la puesta en marcha de la planta nuclear de Bushehr en Irán. Por ejemplo, la mayoría de los ordenadores contaminados por Stuxnet se encuentran en ese país.

Como muchos de los equipos de control industrial no son accesibles desde Internet, Stuxnet tiene la facultad de infectar mediante memorias de USB. Además, es capaz de usar otros medios de comunicación y tiene la capacidad de actualizarse cuando sea necesario.

Hasta marzo de 2011, se habían notificado un total de 24 clientes de Siemens en el sector industrial, a nivel mundial, que se habían visto infectados con el troyano. El código malicioso se pudo eliminar en todos los casos. Siemens ha puesto a disposición del público en Internet (http://support.automation.siemens.com) programas para detectar la presencia de Stuxnet, así como una lista de pasos y herramientas para eliminar el troyano.

Nuevos parientes de Stuxnet: Flame, Duqu, Gauss y Madi

Flame, también llamado Flamer o sKyWIper, es un *malware* modular descubierto en 2012 de alta complejidad y un tamaño muy sustancial. Las organizaciones que lo han estudiado, el laboratorio de criptografía de la Universidad de Budapest y la compañía Kaspersky coinciden en que es una de las piezas de *malware* más complejas que han encontrado y que es muy difícil de entender en su totalidad. Esto es debido a los varios mecanismos de ofuscación que usa, contando con tres métodos de compresión, varios formatos propios de archivos y, por lo menos, cinco mecanismos de cifrado. También usa métodos especiales para inyectar el código en las víctimas.

Flame tiene una funcionalidad muy avanzada para robar información, almacenarla y comunicarla, además de mecanismos avanzados para propagarse de un ordenador a otro. Es capaz de interceptar prácticamente todas la interfaces del ordenador, incluyendo el USB, el teclado, la cámara, el Bluetooth, el micrófono, la pantalla y las conexiones a la red. Por lo tanto, puede grabar audio y las conversaciones de Skype, capturar las imágenes de la pantalla o las pulsaciones de teclado, etc. Estos datos, junto con los documentos almacenados, son enviados a uno de los varios servidores maliciosos dispersos alrededor del mundo; entonces, el programa espera a recibir nuevas instrucciones de esos servidores y puede bajar módulos adicionales que extienden su funcionalidad.

El programa se ha usado para llevar a cabo ataques de ciberespionaje en países de Oriente Medio y ha infectado unas 1.000 máquinas. En junio del 2012, la firma Kaspersky publicó indicios que revelan que los autores de Stuxnet y Flame están conectados y cooperaron por lo menos en la primera etapa de desarrollo. Un ejemplo de la colaboración entre los dos grupos de atacantes es el código del mecanismo de infección del USB, que es idéntico en Flame y Stuxnet.

Duqu es una variante de Stuxnet, aparecida a finales del año 2011, que contiene una variedad de herramientas de *software* que ofrecen diferentes tipos de servicios a los atacantes, como el robo de información sensible, incluyendo certificados criptográficos y claves privadas con las cuales es posible firmar *software* maligno y hacerlo pasar por actualizaciones autorizadas del *software* del sistema bajo ataque. Además, tiene controladores de *kernel* (o núcleo) y herramientas para inyectar código en programas existentes y puede leer las pulsaciones del teclado. Duqu busca información que podría ser útil para atacar sistemas de control industrial como SCADA, aunque parece que allí su propósito no es directamente destruir sino espiar; pero es posible que la información extraída se use luego para crear ataques muy especializados. En ordenadores personales sí se ha observado que Duqu destruye información almacenada en los discos.

Duqu está siendo aún analizado por los expertos de seguridad, que aún no han podido descifrar todo el código y entender cómo funciona exactamente el troyano y, en particular, cómo se distribuye y se multiplica. Parece que el código se elimina a sí mismo después de aproximadamente un mes, lo que hace su identificación más difícil.

Duqu ha sido encontrado en un número limitado de compañías, incluyendo aquellas dedicadas a la construcción de sistemas de control industrial, como SCADA. La información extraída puede tal vez ser usada como base para diseñar y perpetrar nuevos ataques como el Stuxnet.

Gauss, descubierto a finales del año 2012, es capaz de espiar transacciones bancarias, robar información de acceso a redes sociales o correo electrónico y atacar infraestructuras críticas. Gauss es un complejo conjunto de herramientas de espionaje cibernético altamente modular y aparentemente relacionado con Flame. Contiene un código binario cifrado que aún no se comprende y que se activa en determinadas configuraciones del sistema. Gauss parece haber sido usado para robar información de autenticación a personas en el Oriente Medio, en particular en el Líbano.

Las compañías Kaspersky y Seculert estudiaron el troyano Madi e identificaron más de 800 víctimas en varios países, incluyendo personas relacionadas con los proyectos de infraestructuras críticas en Irán e Israel, instituciones financieras israelíes y estudiantes de ingeniería del Orien-

te Medio, pero también grupos de reflexión, agencias gubernamentales, algunas de ellas en el sector eléctrico, y consulados extranjeros en los Estados Unidos. Los atacantes usan métodos de ingeniería social para localizar personas y equipos específicos, en los cuales, ya una vez comprometidos, Madi es capaz de buscar y robar la información almacenada en archivos, de leer correos electrónicos y mensajes instantáneos e inclusive de registrar las pulsaciones de las teclas, leyendo lo que el usuario está escribiendo en su teclado, por ejemplo claves y contraseñas. Toda esta información la envía a un servidor espía. También es capaz de actualizarse a nuevas versiones.

Otros ataques a centros SCADA y a la Red Inteligente

El *Wall Street Journal,* en su edición del 8 de abril de 2009, informó de que la red eléctrica estadounidense fue penetrada por espías extranjeros que colocaron troyanos capaces de perturbar el sistema, según oficiales de seguridad que no brindaron detalles. El mismo año, la actualización de un *software* presente en un ordenador de una planta nuclear en Georgia (USA) hizo que inesperadamente el sistema de control y supervisión SCADA iniciara una parada de emergencia de la planta. Es incluso posible que ataques a Internet en general, o a ciertos tipos de sistemas no directamente asociados con los sistemas de suministro de energía, afecten los centros SCADA del sector. Esto sucedió tanto en 2004 con el gusano SQL Slammer como con el virus Conflicker en 2009.

Es difícil saber cuántos ataques realmente existen contra los servidores SCADA, sobre todo aquellos que están dirigidos a un sistema en particular y de carácter avanzado. Es más fácil calcular con qué frecuencia se producen los intentos de ataque a servidores SCADA indiscriminados. La compañía TrendMicro reportó en el 2013 en una investigación que a pocas horas de activar un sistema SCADA poco bien defendido con el único propósito de observar ciberataques, estos se manifiestan de forma continua. La estadística final cuenta con 28 días seguidos de ataques, con un total de 39 ataques procedentes de 14 países diferentes. En la conferencia de Black Hat de 2013, se demostró que es posible tomar el control sobre unidades de control PLC para encender y apagar equipos en un sistema simulado.

Aurora, Night Dragon y Shady Rat son los nombres de otros ataques relacionados con sistemas de control de infraestructuras críticas.

Sin embargo, es importante mencionar que, aunque los controladores SCADA y los ordenadores asociados tienen vulnerabilidades fáciles de encontrar si se tiene acceso directo a los equipos, explotar estas vulnerabilidades a distancia y cruzando las medidas de protección normalmente existente es bastante más difícil. En muchos casos, el monitoreo continuo de estos sistemas impide que un atacante consiga información por medio

de ensayo y error. De todas formas, un código malicioso como Stuxnet prueba que las medidas actuales son insuficientes si un atacante es muy sofisticado.

En la Red Inteligente la así llamada *superficie de ataque* va creciendo: tanto la cantidad de conexiones a Internet como el número de vulnerabilidades en los sistemas conectados va en aumento. En el Reino Unido existen hoy 53 millones de contadores inteligentes y en España, hasta el año 2018 aproximadamente, 28 millones de consumidores de energía recibirán un contador inteligente.

Muchas veces, los dispositivos de los usuarios utilizados para la medición inteligente están conectados mediante redes inalámbricas entre sí o con el proveedor de energía. Las redes inalámbricas son con frecuencia fáciles de acceder para un atacante, quien podría interceptar, capturar, grabar, repetir y manipular la información en las dos direcciones, modificando tanto los mensajes de facturación y consumo enviados al proveedor como los comandos, los pronósticos y precios de oferta en el mercado de energía. En ciertos dispositivos inteligentes, ha sido posible extraer los secretos de la memoria, permitiendo manipular la comunicación con todos los contadores del mismo proveedor que usan estos mismos secretos predeterminados de fábrica. El atacante podría desconectar remotamente hogares, oficinas y edificios a gran escala por conexión alámbrica e inalámbrica (GSM). La seguridad actual de los contadores inteligentes y de los otros equipos para los usuarios y consumidores deja mucho que desear, la protección de dichos dispositivos no cuenta con medidas fuertes de seguridad preventiva y no existe un sistema para responder a eventualidades en caso de ataques.

Otros ataques a la infraestructura del entorno de las TIC

Hay también formas más indirectas pero no menos eficaces de atacar las infraestructuras de suministro energético. Si se pueden infectar las infraestructuras de las cuales depende la producción de sistemas o la comunicación global o las fuentes de confianza en Internet, se consigue también abrir las puertas a ataques muy serios al suministro energético.

Un escenario sería infectar a un fabricante de equipos, corrompiendo sus sistemas de producción e introduciendo troyanos en las máquinas que se usan para diseñar, desarrollar o equipar los equipos usados en los sistemas de seguridad o de control de infraestructuras críticas. Si un atacante logra entrar allí, los parches de *software*, los archivos y los compiladores del productor serían el mecanismo perfecto para desmantelar cualquier instalación. En los años ochenta del siglo xx un artículo ya clásico de la ACM (Association for Computing Machinery) escrito por Ken Thomson, ganador del renombrado premio Turing, demostró cómo es posible modificar maliciosamente un compilador fundamental de una forma que los

sistemas de autenticación y autorización del sistema operativo quedan completamente abiertos al atacante.

Un segundo escenario está dado por ataques a las fuentes de confianza (anclajes de confianza, en inglés: *trust anchors*) de Internet. Si es posible atacar a los que distribuyen las claves y contraseñas (los certificados y los equipos usados para identificar, autenticar o autorizar equipos o personas), es entonces fácil entrar a cualquier parte que dependa de los servicios de seguridad correspondientes. Un ejemplo de estos ataques fue el perpetrado a la compañía RSA en el año 2011, que comenzó con *mails* a empleados de relativamente bajo perfil con un archivo malicioso de Excel. Al final, el ataque tuvo éxito en extraer información relacionada con los productos de autenticación de dos factores SecurID de los servidores de la compañía. Estos ataques parecen estar conectados con por lo menos 64 infiltraciones que han invadido unas 100 víctimas identificadas que permanecieron sigilosas durante muchos meses, robando información secreta que puede ser probablemente usada para ataques a infraestructuras críticas.

Estos ataques son masivos, pero no imposibles de contrarrestar. Un ejemplo ha sido la reacción de Lockheed Martin en esta emergencia. El equipo de seguridad de esta compañía ha invertido una buena cantidad de tiempo estableciendo una metodología para reconocer los ataques, monitorear sus actividades y prevenir el robo de información importante.

Un año más tarde, un equipo de expertos en criptografía encontró otro ataque al SecurID de RSA gracias a ciertas fallas criptográficas sutiles, logrando comprometer dispositivos criptográficos existentes que incluían tarjetas inteligentes y la credencial de identificación emitida por Estonia. Similarmente, se han encontrado fallas en un número grande de tarjetas inteligentes de diferentes compañías.

Otros ataques a proveedores de credenciales y autoridades certificadoras, como los casos de Comodo y Diginotar, han tenido gran despliegue en los medios. Además, hay un tercer tipo de escenario, que es atacar las redes de comunicación (como el sistema GSM) o de los pilares de Internet, como las tablas de ruta, los servidores de nombre de dominio, etc.

El papel de las TIC en la Red Inteligente

Las características de la Red Inteligente

Regresando a la Figura 1 allí encontramos muchas de las características de la red:

I. Facturación automatizada con una red unidireccional. Este sistema ofrece una facturación relativamente detallada por franjas horarias, permitiendo a los consumidores observar y entender sus patrones

de consumo y elegir las horas más favorables del mismo. Este es un mecanismo rudimentario de respuesta de demanda que, como veremos en un momento, procura dar un mejor uso de la capacidad en red, motivando a los consumidores finales a bajar su demanda de energía en respuesta a las diferencias de precios de las diferentes franjas de horas. Para ofrecer la información relevante al usuario son necesarios mecanismos de almacenamiento y procesamiento de la información en los predios del consumidor o, en su defecto, canales de comunicación que permitan pasar los datos de consumo en la granularidad deseada al servidor.

II. Respuesta de demanda con una red bidireccional. Una operación fiable del sistema electrónico necesita un balance adecuado entre oferta y demanda en tiempo real. "Respuesta de demanda" se puede definir como el conjunto de acciones y medidas cuyo fin es influir sobre los hábitos de consumo de la electricidad por parte de los usuarios finales. Más concretamente, subiendo los precios de energía en las horas que normalmente hay más demanda, o inclusive modificándolos en tiempo real, dependiendo de la oferta y la demanda, se podrá influenciar el momento en el cual un usuario bien informado o dotado de equipos inteligentes consume energía, ayudando a balancear el sistema. La respuesta de demanda ayudará con seguridad a ahorrar energía en su totalidad, pero su importancia radica en "mover" la demanda de ciertos momentos a otros menos críticos, allanando así la diferencia entre las curvas de reservas disponibles y de consumo demandado. Usualmente se espera que el usuario reduzca su consumo cuando los precios son elevados, apagando luces o equipos que no tienen que estar funcionando o trasladando algunas de sus operaciones de horas de alta demanda a horas de baja demanda, por ejemplo, usando la lavadora en otros horarios. En el futuro, además, los consumidores podrán optar por generar su propia energía o comprar para almacenarla, por ejemplo, en vehículos eléctricos para más tarde usarla o venderla suministrándola a la red local o global. En todo caso, es necesario proveer al consumidor con interfaces a sistemas de información y comunicación para notificarlo en tiempo real acerca de los precios actuales y pronosticados, los montos de consumo, etc. Sin embargo, no será posible obligar al consumidor a estar presente en cada decisión de consumo de energía. El usuario ha de fijar reglas (llamadas también sus "preferencias" o "políticas") que habrán de determinar las acciones de un sistema inteligente de toma de decisiones. Este autómata actúa sin intervención humana, controlando los equipos o electrodomésticos inteligentes de acuerdo a las preferencias del usuario. Las medidas de la respuesta de demanda no se limitan a la gestión de la cantidad y el momento del consumo, sino que incluyen también, por ejemplo, subvencio-

nes para la reintegración de energía localmente generada en los hogares y otras medidas. Los mecanismos requieren la recogida continua de datos, así como el procesamiento y la comunicación de grandes cantidades de información, tanto la relacionada con el consumo por los diferentes equipos en los hogares como de los precios previstos y otros.

III. Detección de fallas y restauración de equipos usando sensores inteligentes. Hoy, la red de distribución, en la medida en que está más cerca de los consumidores, es muchas veces "ciega": los operadores y las compañías de energía tienen muy poca información sobre el estado de la red, y en muchos casos no saben de la existencia de problemas de suministro hasta que un cliente llama a quejarse por falta de servicio. Usando el sistema de infraestructura de medición avanzada (por sus siglas en inglés: AMI), las compañías de distribución sabrán rápidamente de cualquier falla en el sistema. Adicionalmente, la red estará equipada de un mayor número de dispositivos electrónicos inteligentes que son capaces de detectar y resolver problemas localmente y de comunicarse con las unidades de supervisión y control más altas en la jerarquía.
IV. Sistemas de información al usuario y portales para consumidores. El usuario podrá supervisar y administrar sus aparatos eléctricos tanto localmente, desde su hogar, como a larga distancia. Esto presupone la disposición de información detallada sobra el estado y las actividades de los electrodomésticos. Además, se requiere un sistema para que el usuario pueda definir las políticas (reglas) que representan sus necesidades o preferencias, y según las cuales se enciende o apaga el servicio de un aparato o se cambian sus parámetros. La clave será el desarrollo de sistemas de información intuitivos para el usuario que, para ser ampliamente aceptados, deben cumplir con requisitos de seguridad y de protección de información personal.
V. Automatización de distribución. La infraestructura del futuro será capaz de identificar e integrar dinámicamente nuevas fuentes de energía independientemente de la forma de generación o de la localización en la red. En casos de sobrecarga será posible recargar reservas asegurando que la red mantenga el suministro eficiente y confiable.
VI. Autorrestauración. La autorrestauración (*self-healing*) es un tema de investigación considerado por muchos como una de las ramas críticas para la realización de la Red Inteligente. El concepto es realmente un eufemismo bajo el cual se agrupan las técnicas que intentan proporcionar a la red la capacidad autónoma de detectar, analizar y aislar fallas y de encontrar medidas compensatorias para recuperar inmediatamente el servicio. Su implementación implicaría aumentar el mantenimiento de la estabilidad y la fiabilidad del sistema, aun si sube el número de componentes que fallen.

La seguridad de las TIC en la Red Inteligente del futuro

Una tendencia global para los sistemas de información y comunicación en las infraestructuras críticas, y muy en particular para aquellos pertinentes al sistema de suministro eléctrico, es que se están abriendo, conectándose al mundo exterior y a la Internet global.

Hace una década o dos el modelo general era –y en muchos casos sigue siendo– el de los castillos o fortalezas medievales: con fosos profundos, muros altos, puertas seguras vigiladas permanentemente por guardias y pasajes secretos que solo conocen un pequeño grupo de personas muy selecto y confiable. Concretamente, en este modelo los sistemas de supervisión y control en los sistemas de suministro eléctrico están prácticamente aislados de sistemas externos y tienen centros de control donde solo pueden entrar personas de absoluta confianza y donde cada comunicación con el exterior es vigilada con gran escrutinio. Pero es de notar que es imposible que estos sistemas realmente estén aislados del todo, porque es necesario actualizar programas o introducir nuevos ordenadores, conectar bancos de datos externos o coordinar la producción o la distribución de energía con otros centros de control. La seguridad depende de la llamada protección del perímetro. Dentro del sistema interno del centro de control no es vital que los ordenadores no tengan vulnerabilidades, lo importante es que nadie no autorizado pueda acceder a ellos.

Este modelo se está desvaneciendo paulatinamente y con la Red Inteligente el modelo habrá cambiado sustancialmente. Ya no serán solo las compañías de energía las interesadas en proteger su propia información, sino que el público general también es dueño de información sensible, no solo de sus datos de consumo, sino también de sus políticas de consumo de energía, de sus comandos a los equipos en su residencia privada, etc. Y habrá aún múltiples actores involucrados que provean y lean información de todo tipo y confíen en su integridad, confidencialidad y disponibilidad.

El modelo de las fortalezas medievales se ha convertido en el de un grupo de residentes en un edificio de apartamentos de una ciudad moderna. Pronto –con la Red Inteligente– este modelo se mutará en aquel de un piso compartido: los diferentes participantes tienen ciertos intereses comunes de seguridad y otros diferentes y se ven obligados a lograr acuerdos que determinen de qué forma qué objetos de valor van a ser protegidos. En el caso de la Red Inteligente de distribución, los diferentes participantes tienen un claro interés común: la integridad del sistema global. Además, cada uno requiere que su propia información personal o comercial sea protegida. Si bien los diferentes requisitos de los participantes no son contradictorios entre sí, en todo caso compiten con la eficiencia del sistema y son costosos de instalar y supervisar. Aún más: para que un servidor ofrezca un servicio a un participante, con frecuencia requiere de información personal del mismo y cuanto mejor, más precisa y más

abundante sea esa información, mejor es el servicio que puede ofrecer. Existe pues, además de la tensión entre seguridad, de un lado, y eficiencia y costo, del otro, también una tensión entre privacidad y funcionalidad.

Así como las personas que comparten un piso tienen que ponerse de acuerdo sobre ciertas reglas básicas, qué objetos quedan bajo llave y a quién se puede dejar entrar, en la futura red eléctrica será necesario negociar las reglas de seguridad que el sistema tiene que imponer. Debido al gran número de participantes y a la dinámica del sistema, esto nos lleva a la necesidad de que cada parte escriba sus *políticas* de seguridad o privacidad en un lenguaje que pueda ser procesado automáticamente. Así, un sistema inteligente puede analizar las preferencias de los participantes y encontrar compromisos adecuados.

Es importante recordar que es imposible construir un sistema complejo, basado en tecnologías de información, que sea perfectamente seguro. Lo que necesitamos es que sea suficientemente confiable, que tengamos evidencia creíble de que va a cumplir una serie de requisitos. La seguridad no es un tema estático. Si hoy encontramos métodos para protegernos de ataques como el de Stuxnet o de otro en particular usando programas que verifican ciertas condiciones en la memoria o en los programas ejecutables, es posible pensar que las futuras versiones del troyano ataquen primero nuestros sistemas de defensas, los programas de detección y monitoreo para luego atacar al sistema de interés. En tal caso, será igualmente posible construir defensas para ese ataque y así sucesivamente.

Los riesgos de seguridad que las organizaciones confrontan se van resolviendo pero igualmente van apareciendo nuevos, con frecuencia más complejos, por lo que la seguridad requiere de procesos continuos de aseguración, monitoreo, escrutinio, verificación, y mucho más. Particularmente en un sistema abierto, como lo será la Red Inteligente, es necesario involucrar a todos los participantes, incluyendo al público general, en los procesos de seguridad. Para protegerse contra los intrusos y ladrones no es suficiente cerrar debidamente todas las puertas con todo tipo de candados, ya que tampoco se puede dejar ninguna ventana abierta. Y así como un ladrón que entra por una ventana del baño puede pasar a la sala o a las alcobas, un intruso cibernético puede entrar por un ordenador, buscar allí claves o contraseñas, y pasar a otro más importante y luego a otro tal vez vital.

Medidas de seguridad en la Red Inteligente

La seguridad de un sistema de procesamiento de la información se implementa con un conjunto de medidas *preventivas* que intentan resguardar y proteger tanto la información misma como los procesos de tratamiento de la información, así como de medidas *reactivas* que ayudan a

recuperar el estado correcto en caso de un evento crítico. Es importante contar con que, por mucha prevención que tomemos, es imposible evitar del todo los defectos o fallas de seguridad, es decir, las vulnerabilidades. Si un atacante encuentra formas de acceder a ellas, los ataques van a ser inevitables y es necesario tomar medidas para hacer manejables los riesgos.

El ciclo de seguridad se puede separar en cuatro tareas: primero, facilitar el proceso de seguridad, que implica definir una estrategia de seguridad, políticas y reglas, roles y responsabilidades, procesos, educación y entrenamiento; segundo, construir sistemas seguros, usar tecnología de protección adecuada, definir una arquitectura de seguridad, implementar y configurar con codificación segura y buenas prácticas; tercero, evaluar tanto los procesos de seguridad como la seguridad misma de los sistemas y, en particular, la presencia de vulnerabilidades y fallos, usando por ejemplo pruebas de penetración (*pen-tests*); y cuarto, responder, detectando y analizando incidentes de seguridad y reaccionando rápidamente para establecer el funcionamiento normal y minimizar el impacto de los incidentes.

Facilitar los procesos de seguridad

La primera tarea, la de facilitar los procesos de seguridad, le corresponde a los órganos y las funciones de gobernanza empresarial (o corporativa). Dentro de cada compañía que participe en el suministro eléctrico debe existir una unidad que cuente con el compromiso de la dirección de la empresa y su soporte financiero. Esta unidad, y en particular su jefe, un ejecutivo de alto nivel, el director de seguridad de la información (en inglés, CISO, *chief information security officer*), es responsable de:

I. Definir roles y responsabilidades de control. Es necesario definir quién es responsable de la información y de los procesos relevantes en la compañía.
II. Definir las políticas internas. Las políticas delinean el comportamiento de todos los actores que tienen acceso directo o indirecto al sistema y, en particular, a los procesos o datos críticos. Los responsables de la ejecución y gestión deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.
III. Proveer planes y recursos de acción factibles y probados. Las políticas y los procesos de seguridad definidos deben cristalizarse en planes concretos donde participen los administradores, propietarios del sistema y el personal de seguridad en la organización, sobre todo el equipo de respuesta de emergencia. Los recursos físicos y económicos, así como los equipos de expertos y los servicios de respaldo, deben ser adecuadamente confirmados por los análisis de riesgos, y una vez justificados, deben ser proporcionados.

IV. Establecer un proceso continuo de análisis y de gestión de riesgos. Además de establecer el proceso, la gobernanza de seguridad debe también decidir cuál es el tratamiento adecuado de los riesgos. Para determinar los riesgos es necesario estudiar en detalle las dependencias del sistema, las consecuencias que los ataques puedan tener sobre los procesos físicos y la integridad de los elementos, funciones y servicios del sistema, así como los flujos de información; es decir, cómo la información relevante es identificada, capturada o medida, procesada e intercambiada y determinar cuáles son los procesos, herramientas, sistemas y datos que hay que proteger. Además, es necesario determinar modelos realistas de atacante, su motivación, capacidades, los pasos que pueden tratar de seguir, sus metas y el esfuerzo que están dispuestos a invertir. Una vez los riesgos están identificados y evaluados, es necesario decidir cuál es la reacción adecuada (p. ej., evitar, mitigar o aceptar el riesgo). En términos muy generales, los riesgos se pueden evitar (cuando la organización elimina la posibilidad de exposición al riesgo, evitando la razón que lo origina), mitigar (las consecuencias de los riesgos pueden ser mitigados hasta un cierto nivel por medidas de seguridad), se pueden transferir (por ejemplo, se transfieren los costos resultantes de un riesgo aceptado a compañías aseguradoras) o se responde a ellos (en caso de un incidente, el riesgo resultante puede ser mínimo si la repuesta al incidente es adecuada). La decisión debe caracterizarse por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las pérdidas involucradas.

V. Determinar los métodos para evaluar la efectividad de los controles y del monitoreo. Es necesario saber cómo de adecuados son los controles de seguridad existentes y las herramientas, y los procesos de detección de intrusos, de vulnerabilidades y de incidentes. Recordemos que hemos visto *malware* que pasa varios años sin detectarse.

VI. Garantizar el informe de cada paso en cada proceso global de seguridad. Para poder aprender de los eventos de seguridad, sean hallazgos de violaciones de políticas o presencia de vulnerabilidades o de incidentes, es necesario protocolar en detalle no solo la situación correspondiente, sino también los análisis que se lograron durante y después del suceso, las medidas que se tomaron, etc. También regularmente, sin motivos particulares, es necesario describir los procesos usados y los resultados obtenidos.

VII. Identificar continuamente oportunidades para la mejora de seguridad. Los informes regulares, la discusión a través de grupos de seguridad como el Foro de Equipos de Respuesta ante Emergencias Informáticas (FIRST) debe ser escrudiñada en la búsqueda de mejoras en la seguridad o la evaluación.

VIII. Definir una estrategia legal revisada y aprobada. Incidentes de seguridad pueden tener variadas consecuencias, incluso penales en mu-

chas ocasiones. La planificación de seguridad debe ser desarrollada con miembros del equipo de asesoría jurídica. La asesoría jurídica ha de tener el conocimiento sobre las consecuencias legales de una violación, el valor y los peligros de información personal de un cliente y procedimientos médicos o financieros. Las regulaciones locales, de estado o federales dictará, al menos en parte, la metodología para llevar a cabo el análisis post mórtem.

Construir sistemas seguros

Las organizaciones deben adoptar un conjunto integral de controles de seguridad para proteger su información y sistemas de información. El propósito de la arquitectura de seguridad es una visión holística de los requisitos de seguridad del sistema, de los mecanismos que los aseguran y de cómo se integran en la arquitectura global.

Evaluar la seguridad y los procesos

Para entender la eficacia de los métodos de evaluación, es conveniente usar con cierta regularidad pruebas profundas y extensas en laboratorios controlados para sistemas de gran importancia, pruebas de intrusión (*test* de penetración, en inglés *penetration test*) y pruebas de caja blanca tanto automáticas como revisiones sistemáticas del código fuente; es decir, usar los así llamados *honeypots* (tarros de miel), *software* o *hardware* minuciosamente monitoreados cuya intención es atraer a atacantes simulando ser sistemas productivos y comparar los riesgos calculados con los incidentes reales observados. Es importante compararlos con los métodos de evaluación externos, contratar expertos de seguridad externos para asistir al equipo local y participar en laboratorios colaborativos de estudio de vulnerabilidades.

Responder

La imposibilidad de evitar del todo los defectos o fallas de seguridad hace esencial la creación de un equipo de respuesta a emergencias de computación, así como la formulación de un plan de respuestas a incidentes. Esto no solo minimizará los efectos de una intrusión o ataque, sino también la publicidad negativa. Un plan de respuesta a incidentes tiene que contar con el apoyo y participación de toda la organización y debe ser ensayado con frecuencia. El plan de respuesta tiene que reconocer incidentes de seguridad, es decir, aquellos estados inesperados o indeseables respecto a los objetivos de protección del sistema, pero su fin primordial es la detención del incidente, la restauración inmediata del estado esperado y de los recursos afectados y la limitación de daños para toda la organización. Dado que en caso de un incidente existe muy poco espacio para errores, las acciones de emergencias tienen que proceder de forma decisiva y rápida. Un elemento

importante es el análisis forense que facilita el reconocimiento del proceso de ataque o intrusión y de las vulnerabilidades, fallas o descuidos que condujeron al incidente. De paso, este análisis va aumentando la experiencia del equipo de seguridad y su capacidad de responder a condiciones adversas de una manera rápida, formal y oportuna a base de la experiencia adquirida. Por último, es necesario dar instrucciones apropiadas para el tratamiento de las causas e informar sobre el incidente a través de los canales apropiados.

Retos

Son muchos los retos relacionados con la protección de las redes futuras de energía, y muchos los pasos a tomar por las diferentes partes involucradas o interesadas: los fabricantes o vendedores de equipos, los operadores de infraestructuras de producción y distribución de energía, las compañías que prestan servicios de información u otros servicios auxiliares o complementarios, los vendedores de sistemas de seguridad, los investigadores en seguridad, las organizaciones de estandarización, las organizaciones del Estado, etc.

Dividimos los retos en siete grupos diferentes: los aspectos técnicos de operación y de la infraestructura; los aspectos operativos de la infraestructura y procesos relacionados; la educación, difusión y sensibilización; el intercambio de información; la creación de estándares, guías y regulación; la investigación y desarrollo de nuevas soluciones, y la protección de la privacidad de datos personales.

Aspectos técnicos de operación y de la infraestructura

Los fabricantes de equipos y los operadores deben colaborar para hallar y definir soluciones técnicas para la prevención de incidentes. Esto debe resultar en una colección de mecanismos de seguridad que han de implementarse e integrarse durante la producción de los equipos, y en mecanismos adicionales y configuración de parámetros, claves, etc. durante el despliegue de los sistemas.

I. Definición de una arquitectura de seguridad. Los operadores, junto con los vendedores de servicios y equipos de seguridad, deberán analizar en detalle todos los riesgos y diseñar en consecuencia una "arquitectura de seguridad" adecuada para los sistemas de operación.
II. La implementación de programas de seguridad para sistemas industriales de control abiertos a las redes de Internet puede ser muy costosa. Muchos operadores hacen uso de controles que compensan la falta de mecanismos de control intrínsecos para evitar la inversión de grandes sumas de dinero en la renovación de equipos y dispositivos antiguos y en sistemas operativos y *software* general. Para facilitar este camino, dos requisitos son: por una parte, crear versiones

de productos con funcionalidad limitada y que brinden pocas opciones pero suficientes para algunos sistemas SCADA específicos; por otra, definir una arquitectura de defensa profunda, es decir, la inclusión de múltiples capas de protección y mecanismos de seguridad solapantes, los cuales actúan como varias barreras contra atacantes. Este enfoque constituye un buen camino para proteger sistemas industriales de control.

III. Un aspecto fundamental de la arquitectura de seguridad es dado por los mecanismos de protección del acceso remoto de los sistemas. El acceso remoto para el control de sistemas por parte de los vendedores o personal de gestión para labores de mantenimiento expone algunos aspectos de la arquitectura a manipulación externa.
IV. Programación segura. Los fabricantes de *hardware* y *software* de sistemas industriales de control deben aplicar las metodologías y reglas adecuadas de programación segura durante el ciclo de desarrollo del sistema.
V. Análisis de los requisitos de seguridad durante todo el ciclo de vida de los sistemas. Los requisitos de seguridad deben ser incluidos desde el principio en la especificación y análisis del sistema. En otras palabras, la seguridad debe acompañar el desarrollo del sistema y no convertirse en una serie de mecanismos adicionales para compensar las deficiencias de seguridad encontradas por falta de previsión.
VI. Consideración de vida útil del sistema. El *software* y *hardware* para oficinas tiene una vida útil de tres a cinco años. En sistemas industriales de control, los cuales son diseñados para un propósito muy específico, la vida útil puede durar mucho más. Por esta razón, es difícil asegurar los componentes de los sistemas industriales de control continuamente a lo largo de toda su vida útil contra nuevas amenazas de seguridad, y es necesario tener planes detallados para poder modificar los sistemas en producción.

Aspectos operativos de la infraestructura y procesos relacionados

Aquí incluimos las actividades de los operadores del sistema, incluyendo la provisión de seguridad física, la gobernanza de la seguridad (en particular: definición y aplicación de roles y responsabilidades), la gestión de crisis y la gestión de riesgos, pero la educación y la sensibilización de los empleados y usuarios la consideramos separada porque es una actividad que no incumbe tan solo a los operadores, sino a todos los actores del sistema.

I. Establecimiento de programas integrales de seguridad. Los operadores de redes de transmisión y distribución tienen que establecer programas integrales de seguridad que incluyan todos los procesos y equipos, tanto de escritorio como de computación comercial y de control de los sistemas industriales. Muchas organizaciones tienen programas detallados de ciberseguridad para sus sistemas de computa-

ción comercial, pero las prácticas para la gestión de seguridad no están adaptadas adecuadamente para los sistemas de control industriales.

II. Endurecimiento (*hardening*). Durante la instalación de equipos, es necesario eliminar los módulos y servicios innecesarios y seleccionar la configuración más segura de parámetros y las versiones de SW más apropiadas. Esto es fundamental para reducir la superficie de ataques y, por tanto, los riesgos.

III. Gestión controlada de cambios. A medida que aparecen informes de incidentes, internos o externos, vulnerabilidades descubiertas o parches de SW, es necesario revisar a configuración del sistema, los parámetros de sistemas SCADA y de controladores lógicos programables (PLC), las versiones de *firmware,* propiedades, ficheros o cualquier otro programa o aplicación. Una gestión adecuada es particularmente importante con el fin de evitar interrupciones o problemas serios en sistemas de control industriales.

Educación, difusión y sensibilización

En la labor de educación y sensibilización han de participar todos los actores a todos los niveles, incluyendo las altas esferas de las compañías involucradas.

I. Campañas de educación, sensibilización y concienciación. Es imperativo crear una cultura consciente de los temas pertinentes a la seguridad, logrando sobre todo un cierto nivel de profundización de los conocimientos necesarios, sobre todo sobre los riesgos y los procedimientos reconocidos que fomentan la seguridad, así como de las prácticas que la ponen en peligro. Con este fin, es necesario definir e implementar programas de educación del personal de sistemas industriales de control y campañas de sensibilización y concienciación de usuarios finales y de los proveedores de servicios.
   Como hemos visto, muchos ataques se pueden evitar si el personal y otros actores del sistema actúan imponiendo reglas de conducta no siempre evidentes. Por ejemplo, el *spear-phishing* intenta engañar a la víctima con una información (un *link* a una página web o un anexo en un mensaje electrónico) aparentemente interesante. No solo la empresa tiene que tener políticas sobre las reacciones en tales casos, sino que el empleado tiene que conocer tales reglas y entender su valor en la protección del sistema.

Intercambio de información

No es fácil para los operadores de infraestructuras críticas cooperar en la detección de ataques y compartir la información sobre incidentes. La Comunidad Europea está buscando formas de incentivar esta colaboración, estudiando la posibilidad de crear bancos de pruebas y de un Equipo de Res-

puesta ante Emergencias Informáticas, sistemas de control industrial (ICS CERT, por sus siglas en inglés) de coordinación, superando la diversidad de capacidades de que disponen los diferentes países y organizaciones de la Comunidad, así como problemas legales, estratégicos e intereses privados.

I. Creación de grupos de evaluación. Los incidentes en sistemas industriales de control deben servir como base de evaluaciones actualizadas del riesgo y de las posibles medidas correctivas y reasignación de recursos. Tanto los fabricantes como los operadores deben abordar el reto de crear comités de análisis que se reúnan regularmente para discutir los incidentes de seguridad y reevaluar los riesgos. En estos equipos no debe faltar, además del personal experto en seguridad y los ingenieros de procedimiento, personas en puestos de dirección medios, y se debe contar con el respaldo incondicional de los mandos altos.
II. Intercambio de información. Todos los días se descubren nuevas vulnerabilidades en el *software* de los sistemas industriales de control. Los operadores deben estar preparados para enfrentarse a nuevos problemas. Al mismo tiempo, fabricantes de sistemas industriales de control deben ofrecer respuestas rápidas y efectivas a la necesidad de crear y distribuir parches de corrección e informes de vulnerabilidad. La industria y la investigación académica o independiente deben cooperar, permitiendo que los fabricantes corrijan sus sistemas antes de hacer pública la información.

Estándares, guías y regulación

I. Incentivos, reglas, legislación y regulación. La Comunidad Europea está estudiando formas de obligar o, por lo menos, motivar a los operadores a ajustarse a procesos definidos de inspección de sistemas industriales de control y análisis de riesgo. La regulación en Norteamérica está dirigida por las organizaciones FERC y NERC.
II. Guías auxiliares. Adicionalmente a las reglas anteriores, es necesario definir guías auxiliares, las cuales incluyen un conjunto de controles de seguridad y de buenas prácticas, alternativas compensatorias y procesos suplementarios. Ejemplos de los temas incluidos en estas guías pueden ser: gestión de cuentas, separación de funciones, el principio del mínimo privilegio, control de sesiones concurrentes, acceso remoto, control de cambios de configuración, pruebas y planes de contingencia, instrumentos de mantenimiento, mantenimiento remoto, protección contra códigos maliciosos, métodos de pruebas, etc.
III. Estandarización. Es necesario definir y estandarizar soluciones ágiles y elegantes para los propósitos específicos de la Red Inteligente y analizar si es necesario definir un conjunto de protocolos básicos de comunicación segura, adoptando un sistema criptográfico adecuado para los requisitos, pero permitiendo la introducción de algoritmos nuevos cuando se requieran.

IV. Certificación. Los tres puntos anteriores pueden –y en muchos casos deben– estar acompañados de procesos de certificación, obligatoria u opcional, que verifican la conformidad con las guías correspondientes.

Investigación y desarrollo de nuevas soluciones

Los investigadores en seguridad deben desarrollar nuevas técnicas y soluciones para los sistemas de control y supervisión y los otros elementos de la Red Inteligente. Esto ha de incluir nuevos métodos forenses, técnicas automáticas, no intrusivas y en tiempo real de monitoreo que aprovechen el tipo singular de sistemas usados. También será conveniente definir protocolos de comunicación y criptográficos, así como controles compensatorios adaptados a las necesidades de la distribución futura de energía, tanto para los equipos grandes pero específicos como para los dispositivos con pocos recursos de computación, almacenamiento o batería.

Protección de la privacidad de datos personales

Ya en el mundo de hoy, en los sistemas médicos o comerciales se ha demostrado que asegurar la privacidad de los usuarios es una dificultad inmensa. Un reto particularmente relevante en la Red Inteligente será el tener que administrar una cantidad enorme de elementos sin precedentes y, al mismo tiempo, que asegurar el anonimato y privacidad de muchos de ellos.

Conclusiones

La Red Inteligente de suministro eléctrico será una realidad; son muchas las presiones en la sociedad moderna que nos obligan a seguir este desarrollo tecnológico, que ha sido descrito como el más grande esfuerzo de ingeniería de la humanidad. El uso de tecnologías de la información y las comunicaciones (TIC) es imprescindible, pero conllevará nuevos riesgos de seguridad. Es prácticamente imposible calcular la probabilidad real de que suceda un ataque serio, hoy o en el futuro, al sistema de suministro eléctrico en un país desarrollado, o saber cuáles son los equipos o funciones que serían el blanco de los ataques. Lo más importante no es intentar la construcción de sistemas absolutamente seguros, lo cual sería un ideal inalcanzable y una empresa fútil, sino más bien tener un concepto holístico de seguridad que determine qué procesos seguir para prevenir o dificultar los ataques, qué herramientas usar para reconocerlos rápidamente y qué acciones tomar para responder y recuperar el funcionamiento normal en el menor tiempo posible y antes de que causen estragos. Los retos de seguridad son grandes pero no imposibles de gestionar. Son una llamada a la acción coordinada y determinada de nuestra sociedad.

Bibliografía

AKYILDIZ, I. F; WEILIAN, Su; SANKARASUBRAMANIAM, Y. & CAYIRCI, E. "A survey on sensor networks". *IEEE Communications Magazine*, n.º 40, 8 de agosto de 2002, pp. 102-114.

ANAGNOSTAKIS, K. G.; SIDIROGLOU, S.; AKRITIDIS, P.; XINIDIS, K.; MARKATOS, E. & KEROMYTIS, A. D. "Detecting targeted attacks using shadow honeypots", 9. *Proceedings of the 14th Conference on USENIX Security Symposium*, volumen 14, 2005.

ANDERSON, Ross. "Why information security is hard: An economic perspective". *Computer Security Applications Conference*, Anual, 0, 358. Los Alamitos, CA, EE. UU.: IEEE Computer Society, 2001.

ANDERSON, Ross & FULORIA, Shailendra. "Who controls the off switch?". *International Conference on Smart Grid Communications.* IEEE, octubre de 2010.

ANDERSON, Ross & KUHN, Markus. "Low cost attacks on tamper resistant devices". *Security Protocols*, 1361/1998. 1998, pp. 125-136. http://dx.doi.org/10.1007/BFb0028165.

ANDERSON, Ross J. *Security engineering: A guide to building dependable distributed systems*. Second, Wiley Publishing, 2008.

http://www.cl.cam.ac.uk/~rja14/book.html.

AYCOCK, J. "A design for an anti-spear-phishing system". *7th Virus Bulletin International Conference.* 2007.

BARNES, Ken & JOHNSON, Briam. *Introduction to SCADA protection and vulnerabilities.* INEEL/EXT-04-01710. Idaho National Engineering and Environmental Laboratory, marzo de 2004.

http://www.inl.gov/technicalpublications/Documents/3310860.pdf.

BISHOP, Matt. *Computer security: Art and science*. Addison-Wesley, 2003.

CARL, Glenn; KESIDIS, George; BROOKS, Richard R. & RAI, Suresh. "Denial-of-service attack detection techniques". *IEEE Internet Computing,* 10, 1, pp. 82-89. Los Alamitos, CA, EE. UU.: IEEE Computer Society, 2006.

COHEN, F. "The smarter grid". *Proceedings of IEEE Symposium on Security and Privacy,* n.º 8, 2010, pp. 60-63.

COHEN, Fred. "Simulating cyber attacks, defences, and consequences". *Computers & Security.* 1999, 18, 6, pp. 479-518. http://www.sciencedirect.com/science/article/pii/S0167404899801151.

Consejo Europeo. Directiva 2008/114/CE del Consejo, *sobre identificación y designación de las infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección,*

http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_es.htm.

CREESE, Sadie; GOLDSMITH, Michael H. & ADETOYE, Adedayo O. "A logical high-level framework for critical infrastructure resilience and risk assessment". *The 3rd International Workshop on Cyberspace Safety and Security* (CSS 2011), por aparecer. Milán, Italia: septiembre de 2011.

ENISA. *CERT cooperation and its further facilitation by relevant stakeholders.* Deliverable WP2006/5.1(CERT-D3).

http://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport.

ENISA. ENISA *Smart Grid security recommendations.* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport.

ERICSSON, G. N. "Cyber-security and power system communication 2014: Essential parts of a Smart Grid infrastructure". *Transactions on power delivery.* 25, 3, pp.1501-1507. IEEE, 2010.

IGURE, Vinay M.; LAUGHTER, Sean A. & WILLIAMS, Ronald D. "Security issues in SCADA networks". *Computers & Security*, n.º 25, 2006, pp.498-506.

TØNDEL, Inger Anne, JAATUN, Martin Gilje y LINE, Maria Bartnes. "Security threats in demo Steinkjer". *Report from the Telenor-SINTEF collaboration project on Smart Grids.* http://www.demosteinkjer.no/attachment.ap?id=2.

KALOGRIDIS, G.; EFTHYMIOU, C.; DENIC, S. Z.; LEWIS, T. A. & CEPEDA, R. "Privacy for smart meters: Towards undetectable appliance load signatures", pp.232-237. *First IEEE International Conference on Smart Grid Communications.* SmartGridComm, 2010.

KHURANA, H.; HADLEY, M.; LU, Ning & FRINCKE, D. A. "Smart Grid security issues". *Security Privacy.* IEEE, 2010, 8, 1, pp.81-85.

KOEPSELL, Stefan; WENDOLSKY, Rolf & FEDERRATH, Hannes. *Revocable anonymity, emerging trends in information and communication security*. 2006, pp. 206-220. http://dx.doi.org/10.1007/11766155_15.

LIU, Yao; NING, Peng & REITER, Michael K. *False data injection attacks against state estimation in electric power grids.* 2009.

LU, Zhuo; LU, Xiang; WANG, Wenye & WANG, C. "Review and evaluation of security threats on the communication networks in the smart grid". *Military Communications Conference-MILCOM 2010.* 2010, pp. 1830-1835.

MCDANIEL, P. & MCLAUGHLIN, S. "Security and privacy challenges in the Smart Grid". *Security Privacy,* 7, 3, pp. 75-77. IEEE, 2009.

MCGRAW, Gary. "Software security". *Security and Privacy,* 2, 2, pp. 80-83. IEEE, 2004.

METKE, A. R. & EKL, R. L. "Security technology for Smart Grid networks". *Transactions on Smart Grid,* 1, 1, pp. 99-107. IEEE, 2010.

Microsoft. *Spear phishing: Highly targeted phishing scams,* http://www.microsoft.com/protect/yourself/phishing/spear.mspx.

MINGHAN, Zou & YUN, Miao. "Summary of Smart Grid technology and research on Smart Grid security mechanism". *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM).* 1 de abril de 2011.

Ministerio de Defensa. *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia,* n.º 149. http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029.

Ministerio del Interior. Ley 8/2011, de 28 de abril, *por la que se establecen medidas para la protección de las infraestructuras críticas.* http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-7630.

Ministerio del Interior. Real Decreto 704/2011, *por el que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas.* http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849.

MO, Yilin; KIM, T. H.-H.; BRANCIK, K.; DICKINSON, D.; LEE, Heejo; PERRIG, A. & SINOPOLI, B. "Cyber-physical security of a Smart Grid infrastructure". *Proceedings of the IEEE*. 2012, 100, 1, pp. 195-209.

NERC. *CIP-009-4: Cyber-security: Recovery plans for critical cyber assets.* North American Electric Reliability Corporation (NERC).

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

OGWU, Francis Joseph; TALIB, Mohammad; ADEROUNMU, Ganiyu & ADETOYE, Adedayo. "A framework for quality of service in mobile ad hoc networks". *Int. Arab J. Inf. Technol.* 2007, 4, 1, pp. 33-40.

PAAR, Christof & WEIMERSKIRCH, André. Embedded security in a pervasive world., *Information security technical report.* 2007, n.º 12, pp. 155-161.

PALMER, Graham. "De-perimeterisation: Benefits and limitations". *Information security technical report.* 2005, 10, 4, pp. 189-203.

http://www.sciencedirect.com/science/article/B6VJC-4HN-F68X-3/2/65c03ea72fa1ff3c61a53447fc8dd9ca.

RIFKIN, Jeremy. *The Third Industrial Revolution: How lateral power is transforming energy, the economy, and the world,* p. 304. 2013.

MACMILLAN, Palgrave. *Symantec, Stuxnet dossier.*

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

SYMANTEC. *W32. Stuxnet variants.*

.http://www.symantec.com/connect/blogs/w32stuxnet-variants.

WACK, John; TRACY, Miles & SOUPPAYA, Murugiah. *Guideline on network security testing {NIST}. Special publication,* 800, 42, octubre de 2003. http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

WANG, Wenye & LU, Zhuo. "Survey cyber security in the Smart Grid: Survey and challenges". *Comput. Netw.,* 57, 5, pp. 1344-1371. Nueva York, NY, EE. UU.: Elsevier North-Holland, Inc., abril de 2013. http://dx.doi.org/10.1016/j.comnet.2012.12.017.

WANG, Yong; RUAN, Da; GU, Dawu; GAO, J.; Liu, DAMING; Xu, JIANPING; Chen, FANG; Dai, FEI & YANG, Jinshi. "Analysis of Smart Grid security standards". *International Conference on Computer Science and Automation Engineering (CSAE),* 4, pp. 697-701. IEEE, 2011.

YANG, Y.; LITTLER, T.; SEZER, S.; MCLAUGHLIN, K. & WANG, H. F. "Impact of cyber-security issues on Smart Grid". *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe).* IEEE, 1 de julio de 2011.

Capítulo cuarto

Impacto geopolítico del desarrollo de los hidrocarburos no convencionales

Mariano Marzo

Resumen

Los recursos no convencionales de petróleo y gas son abundantes y su producción resulta económicamente viable. Además, la distribución geográfica de estos recursos diversifica las fuentes de suministro tradicionales, muy concentradas en Oriente Medio y Rusia. El estancamiento e inminente caída de la producción de crudo convencional hará que en el futuro los petróleos no convencionales ganen protagonismo. Durante la próxima década, el aumento de su extracción, particularmente en los Estados Unidos y Canadá, ayudará a debilitar temporalmente la hegemonía de la OPEP que, sin embargo, recobrará el control del mercado a mediados de la década de los veinte. Por su parte, la producción de gas no convencional se extenderá en el futuro desde Norteamérica a otras partes del mundo, consolidando a largo plazo su aportación al suministro global de gas. El cambio en la geografía de la demanda, cuyo centro se desplaza hacia Asia, junto a los cambios que la producción de hidrocarburos no convencionales introduce en el actual balance entre países exportadores e importadores, comportará una reorganización del flujo comercial del petróleo y del gas natural con implicaciones sobre la seguridad de las rutas de suministro global. Estados Unidos, que gracias a los no convencionales logra la autosuficiencia en el caso del gas natural y un bajo grado de dependencia de las importaciones de crudo, es el gran beneficiario a medio plazo de la revolución de los no convencionales. La Unión Europea,

por el contrario, verá incrementar su dependencia de las importaciones de petróleo y gas.

Palabras clave

Hidrocarburos no convencionales, OPEP, autosuficiencia energética, dependencia energética.

Abstract

Non-conventional oil and gas resources are abundant and their production is economically viable. In addition, the geographical distribution of these resources helps to diversify the traditional sources of supply currently highly concentrated in the Middle East and Russia. Stagnation and imminent fall in production of crude oil will make non-conventional oil to gain prominence in the future. Over the next decade, its increasing extraction, particularly in the United States and Canada, will help to temporarily weaken the hegemony of the OPEC which nevertheless will regain control of the market shortly after the mid-1920s. Meanwhile, the production of unconventional gas will extend in the future from North America to other parts of the world, consolidating its contribution to the global supply of gas on a long-term basis. The change in the geography of demand, whose centre is moving towards Asia, along with the changes introduced by the non-conventional hydrocarbons production in the current balance between exporting and importing countries, will incur a reorganization of the trade flows of oil and natural gas, with implications upon the security of the global supply routes. The United States, which thanks to non-conventional, achieves the auto-sufficiency in the case of natural gas as well as a low degree of dependence on crude oil imports, is the big beneficiary in the medium term of the so-called non-conventional revolution. The European Union, by contrast, will see an increase on its imports and external dependence.

Keywords

Non-conventional hydrocarbons, OPEC, Energy self-sufficiency, energy dependence.