https://doi.org/10.17979/spudc.9788497498081.0566

UNA COMPARATIVA DE LA CIBERSEGURIDAD EN SISTEMAS DE CONTROL CRÍTICOS: SMART GRIDS E IACS

Miguel Ángel Iñigo Ulloa
Gestor Proyectos I+D
Virtualware Labs
minigo@virtualwaregroup.com

Isidro Calvo
Departamento de Ingeniería de Sistemas y Automática
EUI de Vitoria-Gasteiz (UPV/EHU), España
isidro.calvo@ehu.eus

Jon Arambarri
Responsible I+D
Virtualware Labs
jarambarri@virtualwaregroup.com

Resumen

Hasta hace unos años, los sistemas de control complejos como los subsistemas del sistema eléctrico o los Sistemas de Control y Automatización Industrial (Industrial Automation and Control Systems, IACS) estaban en gran medida aislados o conectados a través de conexiones restringidas, normalmente con tecnologías propietarias, lo cual facilitaba su seguridad frente a ciberataques. Sin embargo, en los últimos años este panorama ha ido cambiando debido a la generalización de la conectividad, a la adopción de las tecnologías de comunicación modernas (Internet, comunicaciones inalámbricas, etc.), así como al uso de dispositivos electrónicos genéricos.

Por ejemplo, tanto en el ámbito de las Smart Grids como en los IACS se han detectado evidencias significativas de ciberataques que explotan las vulnerabilidades que ofrecen dichos sistemas de control. Esta nueva situación requiere que los nuevos subsistemas de control implanten medidas de ciberseguridad para minimizar las consecuencias de estos potenciales ataques.

Dado que tanto los IACS como las Smart Grids comparten muchas características, en este artículo se realiza una comparativa y se analizan algunas de sus vulnerabilidades más habituales. El artículo pretende servir como punto de partida para adentrarse en el complejo mundo de la ciberseguridad de este tipo de sistemas críticos.

Palabras Clave: Ciberseguridad, Vulnerabilidades, Ciberataques, Smart Grids, IACS

1 INTRODUCCIÓN

La seguridad de la información en las plantas industriales se ha visto claramente comprometida durante los últimos años. Algunos incidentes han adquirido mayor dimensión mediática, como el virus Stuxnet, que tomó el control del sistema de Supervisión, Control y Adquisición de Datos o *Supervisory Control And Data Acquisition* SCADA en una central nuclear en Irán [1]. De hecho, el número de incidentes de ciberseguridad registrados en IACS durante 2012 se ha visto multiplicado por cinco desde el 2010 [2]. Afortunadamente, aunque queda mucho por hacer, poco a poco, la comunidad científica y los comités de normalización internacional se van concienciando acerca de la necesidad de proteger los sistemas críticos de control.

Un buen ejemplo se encuentra en las cada vez más interconectadas redes eléctricas o *Smart Grids*. Éste es un sistema crítico que además ha tenido que soportar un gran aumento de la producción y consumo de energía. En EEUU se estimado que el aumento ha sido entre dos y tres veces desde 1950 hasta 2008 [3]. Y se prevé un aumento medio hasta el 2030 en Europa del 1,4 % anual [4]. Esta situación está obligando a remplazar los antiguos equipos utilizados en las redes eléctricas por nuevos sistemas inteligentes capaces de adaptarse a las nuevas demandas. Las Smart Grids integran los modernos avances de las Tecnologías de la Información y de las Comunicaciones (TICS) mejorando en gran medida la eficiencia, disponibilidad y la fiabilidad, así como la inteligencia de respuesta acorde a la demanda. Sin embargo, la introducción de este tipo de tecnologías también

conlleva la aparición de nuevas amenazas de ciberseguridad, ya que las Smart Grids interconectan millones de dispositivos electrónicos a través de las redes de comunicación a lo largo de las instalaciones hasta el destino final, lo cual tiene un impacto inmediato sobre la fiabilidad de dichas infraestructuras.

Algo similar sucede con los procesos productivos, la inclusión de las TICs y de acceso desde Internet a los IACS ha supuesto un cambio en el paradigma. Estos sistemas han evolucionado de encontrarse completamente aislados a estar interconectados con sistemas IT corporativos a través de Internet. Aunque esto ha traído numerosos beneficios, se ha abierto la puerta a incidentes de ciberseguridad que han obligado a proporcionar soluciones y tomar medidas tanto desde la comunidad científica como desde las propias organizaciones que poseen sistemas críticos (Smart grids o IACS).

Hay que tener en cuenta que la ciberseguridad en las Smart Grids y en los IACS no puede abordarse de la misma forma que en los sistemas de redes corporativas, principalmente debido a que son sistemas que tienen diferentes requisitos de funcionamiento (p.e. requisitos de tiempo real y de rendimiento). Además, ciertas medidas de seguridad como son las actualizaciones de software requieren paradas y/o reinicios del sistema, algo inviable en sistemas de control industrial.

En los siguientes apartados vamos a analizar las peculiaridades de las Smart Grids e IACS, identificar sus principales vulnerabilidades en cuanto a ataques cibernéticos y realizar una comparativa entre ambos dominios con la intención de buscar paralelismos y diferencias. El artículo acabará con unas conclusiones finales

2 SMART GRIDS

2.1 DEFINICIÓN

Existen diferentes definiciones para precisar que es una Smart Grid. Según el Grupo de Reguladores Europeos de la Electricidad y el Gas (ERGEG) y la Plataforma Europea de Tecnologia o *European Technology Platform* [5], una Smart Grid es "una red eléctrica que se pueden integrar de forma inteligente las acciones de todos los usuarios conectados a ella (generadores, consumidores y aquellos que hacen ambas cosas) con el fin de suministrar eficientemente, de forma sostenible, económica y segura el suministro de electricidad" [6]. Las Smart Grids integran junto a la red eléctrica redes de comunicaciones de datos que recogen y analizan en tiempo real los datos capturados acerca de la transmisión de energía, distribución y consumo [7]. Sobre la base de estos datos se proporciona información predictiva y recomendaciones a los servicios públicos, sus proveedores y sus clientes sobre la mejor manera de manejar la energía. De acuerdo con el modelo propuesto por el National Institute of Standards and Technology (NIST) las Smart Grids constan de siete dominios lógicos: generación, transmisión, distribución, atención al cliente, Mercados, Proveedor de Servicio y Operaciones [8] (Ver Figura 1).

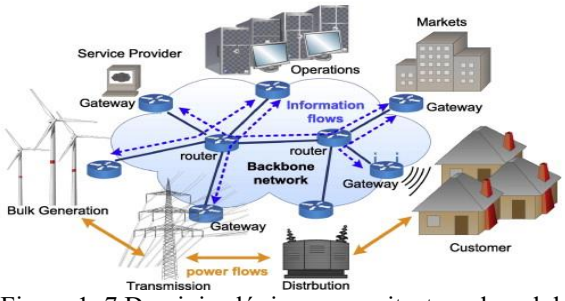

Figura 1: 7 Dominios lógicos y arquitectura de red de una Smart Grid. [5]

Los componentes principales de un sistema Smart Grid están muy jerarquizados y comprenden diferentes subsistemas hardware y software [9]: Sistemas de gestión de energía o *Energy Management Systems* (EMS), SCADAs a diferentes niveles, incluyendo a las subestaciones, *Remote Terminal Units* (RTUs), *Programmable Logic Controllers* (PLCs), Timers, *Human Machine Interaction* (HMI), diferentes dispositivos de comunicaciones como routers, switchs o hubs, servidores de logs, dispositvos inteligentes como *Intelligent electronic devices* (IEDs) y/o *Advanced Metering infraestructure* (AMIs).

2.2 CARACTERISTICAS

El incremento de las Smart Grids se justifica por razones de eficiencia energética (para poder acometer las necesidades de energía de la sociedad para los años venideros), y se visualiza en el aumento de proyectos de I+D [10] y publicaciones científicas [11] que se están desarrollando en los últimos años. Las características principales se van a describir a continuación. Una primera y aconsejable comparación respecto a sistemas de redes eléctricas tradicionales se puede ver en [12]. Uno de los motores clave está resultando la implantación de los contadores inteligentes (AMIs) que están proporcionando un impulso significativo al tratarse de millones de nuevos dispositivos conectados [5], [13]. Los AMIs son fundamentales dentro de las Smart Grids puesto que se usan para conectar el domicilio del cliente con la central de servicios y el mercado de la electricidad [5]. De igual forma, IEDs más sofisticados permiten capturar información de campo más precisa y actuar sobre los dispositivos de control y protección de los centros de control [14]. Ambos tipos de dispositivos

se distribuyen en nuevas y más complejas topologías utilizando diferentes tipos de redes de comunicación.

Las comunicaciones en este tipo de sistemas tienen unos requisitos diferentes a las que encontramos en comunicaciones de entornos ofimáticos. En Smart Grids no es prioritario proporcionar servicios de alto rendimiento si no asegurar ciertos parámetros de calidad de servicio (QoS) como garantizar la entrega de los mensajes de manera fiable, segura y en tiempo real. La latencia en este caso es más importante que el rendimiento, lo que conduce al diseño de protocolos de comunicación que se adecúen a estos requisitos. A modo de ejemplo, si en aplicaciones genéricas de Internet retardos de 100 a 150 ms pueden ser aceptables [5], en algunas aplicaciones de Smart Grids como por ejemplo las aplicaciones de control de subestaciones el retardo máximo aceptable es de 3ms [15]. Además, en redes de energía al contrario de lo que pasa en el tráfico de Internet la mayoría del flujo de tráfico es periódico con muestreo y monitorización constante de los datos de las subestaciones y de los AMIs

Con respecto al modelo de comunicación, Internet funciona de acuerdo al modelo extremo a extremo de manera que soporta comunicación de igual a igual entre nodos. En redes tradicionales de electricidad la comunicación es normalmente unidireccional, un dispositivo produce información y otro la recoge. Por el contrario, en las Smart Grids se usa un modelo bidireccional, que normalmente involucra a centros de control y dispositivos. Aunque en Smart Grids también se pueden soportan modelos extremo a extremo normalmente se restringen por motivos de seguridad.

Los protocolos de comunicación utilizados en Smart Grids tratan de dar respuesta a estas necesidades. Algunos están estandarizados por diferentes organismos internacionales: DNP3, IEC 61850, IEC 60834, otros se utilizan en otros entornos industriales como ModBus o ProfiBus y también se usan protocolos y tecnologías de ámbito más general como redes de telefonía móvil (GPRS, GSM, etc.), RF Mesh, WiFi (802.11), WiMAX, ZigBee, etc [14]. A nivel de protocolos de comunicación se utilizan los protocolos más comunes de la pila TCP/IP como IP, TCP, UDP, ssh, https, FTP, etc. [16].

2.3 CIBERSEGURIDAD Y VULNERABILIDADES EN SMART GRIDS

Varios acontecimientos relevantes han sacado a la luz algunas vulnerabilidades de los sistemas de energía desde el año 2003. Por ejemplo, una central nuclear se colapsó debido a una infección del gusano Slammer en la red del sistema de control. El virus saltó el firewall y obligó al sistema de monitorización de seguridad física a estar deshabilitado durante 5 horas [1]. En un estudio realizado sobre 291 compañías del sector energético en USA el 76% de ellas sufrió uno o más incidentes de seguridad en 2010 [17]. Estos ciberataques obligaron a analizar y desarrollar soluciones para intentar evitarlos.

Como conclusión de los ataques previos se puede concluir que los objetivos de ciberseguridad para las Smart Grids según [8] son:

- *Disponibilidad*: garantizar el acceso oportuno y de confianza para garantizar el servicio de energía.
- *Integridad*: garantizar que la información no es modificada o destruida asegurando el no-repudio y su autenticidad para tomar la decisión correcta.
- *Confidencialidad*: preservar el acceso a la información únicamente a las personas y dispositivos pertinentes para proteger los datos personales y la propiedad de la información.

Antes de describir las vulnerabilidades más relevantes es importante conocer cuáles son los casos de uso en los que se debe poner mayor interés dentro de las Smart Grids, teniendo en cuenta que se encuentran diferentes tipos de sistemas implicados (SCADAs, IEDs, AMIs y subsistemas de control energía). Se han tenido en cuenta fundamentalmente los siguientes dos casos, acerca de los que se puede ampliar información en [8] y [5]. También se puede encontrar otros casos de uso interesantes en dichos trabajos.

- Operación y transmisión de la información en el que los requisitos de tiempo real son críticos.
- AMIs y las redes denominadas *home-area* en las que existe comunicación entre el cliente y los proveedores de suministro del servicio de energía.

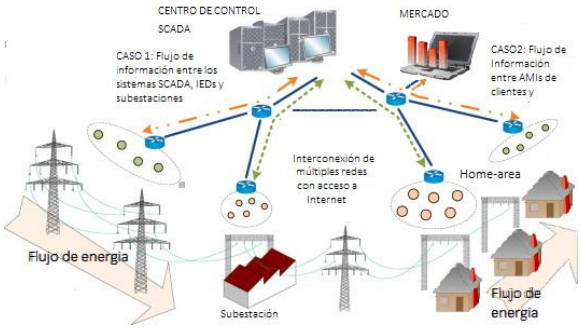

Figura 2: Casos de uso y flujo de información de una Smart Grid (Adaptado de [5]).

Las vulnerabilidades en relación a la ciberseguridad se originan en diversas causas. Conviene considerar que tradicionalmente los sistemas de red eléctrica se encontraban físicamente aislados de los sistemas de red corporativos proporcionando una seguridad

directa teniendo en cuenta únicamente decisiones de seguridad física y la propia del programa de control.

Por un lado, a pesar de que los protocolos de comunicaciones típicamente utilizados en el ámbito eléctrico como ModBus, ProfiBus, ICCP, DNP normalmente no incluían funcionalidades de ciberseguridad, se trataba de protocolos propietarios o escasamente conocidos fuera de los ámbitos industriales, con lo que se trabajaba bajo el concepto de *Seguridad por obscuridad*. No obstante, estos protocolos han sido diseñados sin tener en cuenta la seguridad y presentan vulnerabilidades. P.e. el protocolo DNP3, que es uno de los más utilizados en este ámbito en EEUU, es posible explotarlo mediante ingeniera inversa para realizar un ataque *Man in The Middle* (MitM) [16]. En este tipo de ataques un intruso es capaz de leer y escribir mensajes comunicados entre dos partes sin que ninguna de las partes de sea consciente de ello. Existen en la literatura algunos trabajos dedicados a la detección y análisis de este tipo de ataques [18, 19, 20].

Por otro lado, a medida que se han empezado a utilizar protocolos más cercanos a los sistemas corporativos basados en TCP/IP como HTTP o FTP, con lo que el concepto de Seguridad por obscuridad desaparece totalmente, ya que es posible utilizar gateways desde donde atacar los sistemas. Además, a pesar de que los protocolos TCP/IP ofrecen grandes ventajas: (1) interoperabilidad entre una amplia gama de componentes de las Smart Grids; (2) flexibilidad ante la evolución de la red; (3) fiabilidad en caso de enrutamiento dinámico; y (4) asequibilidad para ser utilizados por la industria; sin embargo, tienen un amplio abanico de vulnerabilidades bien conocidas. Por ejemplo, los atacantes han aprendido a enmascarar el origen de un paquete que salta de router en router haciendo difícil su rastreo. Un resumen exhaustivo de los posibles ciberataques, impactos adversos y a qué objetivos de seguridad aplica lo vemos en la Tabla 1 de [9]. Se tiene en cuenta para su confección el tipo de comunicación, la topología, el protocolo utilizado y los parámetros de calidad del servicio o *Quality of Service* (QoS).

Si el diseño y dimensionamiento del sistema es inadecuado pueden realizarse ataques de denegación de servicio o *Denial of Service* (DoS) [9]. En este caso, se saturará el maestro SCADA o RTU con mensajes de protocolo válidos reduciendo o colapsando sus recursos (memoria, CPU, ancho de banda) y por tanto afectando al rendimiento del sistema, dando lugar a retrasos o inhibiciones de los servicios. Como consecuencia del ataque se producirá un mal funcionamiento de los dispositivos electrónicos y los operadores del centro de control pueden tomar decisiones erróneas. Este tipo de ataque se puede dirigir a cualquier capa de la pila de TCP/IP (i.e. capa física, capa *Media Access Control* (MAC), capa de red, transporte y de aplicación) [5]. El efecto de este ataque puede producir desde la pérdida de las comunicaciones con el dispositivo hasta inhibir o alterar servicios específicos dentro del propio dispositivo (como almacenamiento o procesamiento de E/S). Aunque los ataques DoS en sistemas corporativos no tienen consecuencias negativas significativas, un DoS bien planeado en un sistema crítico puede desconectar un sistema y provocar un apagado lo que resulta inadmisible en una Smart Grid. La configuración adecuada de la arquitectura de red es importante en Smart Grids ya que no sólo hay que tener en cuenta la ciberseguridad para los servidores o centros de control principales, sino que es importante tener en cuenta los *Energy Management System* (EMS) y SCADAs además de todos los dispositivos que se ejecutan en los nodos como los PLCs, RTUs, IEDs o AMIs

Si tenemos en cuenta los dispositivos de campo utilizados por los sistemas de distribución y transmisión de energía como los RTUs e IEDs, estos disponen de un panel HMI para que los ingenieros puedan realizar su configuración y mantenimiento. En muchos casos estas operaciones se realizan mediante acceso remoto basado en IP. Este acceso remoto puede introducir vulnerabilidades que involucran la generación de datos erróneos con la consiguiente mala interpretación, errónea actuación en las operaciones de control y/o suspensión del servicio. Para hacer las cosas aún más complicadas, muchos de estos RTUs son sistemas obsoletos heredados, basados en tecnologías propietarias, que cuentan con 20 o 30 años de antigüedad, que además están diseñados para realizar tareas de control pero que carecen de potencia de cálculo y memoria para realizar funciones de seguridad [9].

Por último, dentro de las Smart Grids es necesario evitar vulnerabilidades de autenticación e identificación de los usuarios en todos (millones) los dispositivos electrónicos (AMIs, IEDs). Se debe forzar a que cada dispositivo disponga de un identificativo y que únicamente los usuarios que tengan los permisos adecuados puedan hacer las operaciones permitidas previniendo así accesos no autorizados. A su vez, dicha información para cada uno de los nodos debe tener una función de cifrado de los datos para asegurar su integridad, así como estar debidamente auditada para una posterior consulta.

3 IACS

3.1 CARACTERISTICAS

Los sistemas de control y automatización industrial o *Industrial Automation and Control Systems* (IACS) abarcan varios tipos de sistemas de control entre los

que se incluyen los sistemas SCADA, los sistemas de control distribuidos o *Distributed Control System* (DCS) así como PLCs y subestaciones de control compuestas por RTUs.

La introducción de nuevas tecnologías y diferentes tipos de sistemas de comunicación en el entorno industrial ha logrado avances significativos en el ámbito del control y la automatización. Por un lado, se han mejorado significativamente las posibilidades de los sistemas SCADA que monitorizan en tiempo real muchas de las infraestructuras críticas en sistemas de energía, transporte, agua, procesos químicos, de gas y de petróleo [21]. Por otro, se han ampliado las opciones de conectividad a un gran número de dispositivos industriales, especialmente con la adopción de los protocolos TCP/IP y estándares como OPC, u OPC-UA para este tipo de sistemas.

Estas nuevas configuraciones han cambiado la forma de proceder de los sistemas y redes industriales. Tradicionalmente, los IACS se encontraban aislados del mundo exterior e Internet de forma que la información que se transmitía desde estas redes a la red de la oficina era mínima [22].

Anteriormente, al verse aislada por completo de los sistemas corporativos y sin acceso a Internet la adopción de hardware y software propietario era suficiente para garantizar un alto nivel de seguridad de los datos. En estos momentos las redes de IACS están amenazadas de manera similar a los sistemas corporativos y es necesario dividir las redes en zonas seguras como se muestra en la figura 1.

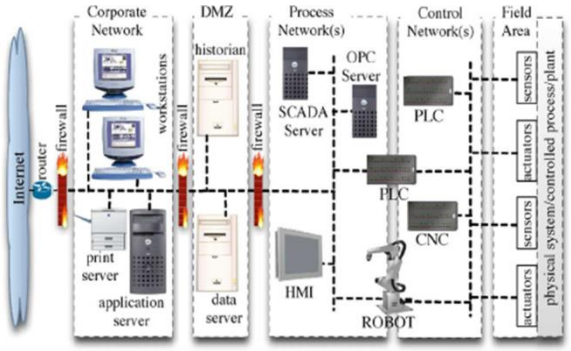

Figura 3: Conexiones típicas de IACS a las redes corporativas e Internet [23]

Los protocolos de comunicación más utilizados en IACS, como Modbus, DNP3, ProfiBus, DeviceNet, HSE [24], están muy jerarquizados de acuerdo a la pirámide de automatización. A grandes rasgos, estos protocolos se pueden clasificar en la siguiente jerarquía:

- *Nivel de campo*, distribuyendo los datos desde sensores y actuadores hasta controladores y dispositivos de campo.
- *Nivel de control*, distribuyendo la información desde dispositivos de campo hacia controladores y también desde los propios controladores
- *Nivel de planta*, conectando segmentos de redes a nivel de supervisión, seguimiento y sistemas corporativos

Las arquitecturas de redes utilizadas en los sistemas industriales tienen más niveles de profundidad que las redes ofimáticas. En estos niveles, fundamentalmente en los niveles inferiores, se usan multitud de protocolos y/o medios físicos que aun siendo similares o incluso idénticos a los utilizados en las redes ofimáticas, requieren pasarelas para facilitar la comunicación con las capas superiores. Además, es frecuente que se utilicen protocolos propietarios o basados en estándares de uso industrial, lo cual limita su conocimiento a un público restringido.

Por último, como pasa en las Smart Grids, la mayoría de los protocolos industriales tienen que satisfacer una serie de requisitos específicos como cumplir con los requisitos de tiempo real, ofrecer latencias bajas y valores de jitter constante y bajo [19].

3.1 VULNERABILIDADES DE LOS IACS

Según un informe generado para sistemas de control industrial por el ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*), el número de incidentes registrados en 2012 se ha multiplicado por cinco desde el 2010 [25]. Uno de los casos más sonados es el gusano *Stuxnet* descubierto en 2010, que operó durante tres años sin ser detectado [26].

En muchos casos dichos ciberataques aprovechan las vulnerabilidades que ofrecen los IACS y que se pueden clasificar en los siguientes tipos según [27] y [28]:

- Políticas y procedimientos
- Plataforma
- Red.

3.1.1 VULNERABILIDADES DE POLÍTICAS Y PROCEDIMIENTOS

Las vulnerabilidades relacionadas con las políticas y procedimientos para los sistemas de control industrial están relacionadas con:

- Pobre o inadecuada política de seguridad para los IACS sin procedimientos específicos documentados
- Inexistente definición formal de un programa de sensibilización y formación sobre seguridad en los IACS; arquitectura y diseño de seguridad inadecuada

- Directrices de seguridad a implementar en los IACS deficientes o inadecuadas
- Pocas o inexistentes auditorias para los IACS
- Carencia de un plan específico ante desastres
- Brecha relacionada con la gestión del cambio de configuración en IACS específicos.

3.1.2 VULNERABILIDADES DE PLATAFORMA

En cuanto a las vulnerabilidades de plataforma se deben a la propia plataforma del hardware que la compone, del software y de la protección contra software malicioso o malware. Las más destacadas están relacionadas con:

- Desactualización de equipos y su software, en muchos casos con más de 15 años de vida [22]
- Configuraciones por defecto y/o nulas y/o carencia de copias de seguridad de las configuraciones críticas
- Pérdida de configuraciones por entornos no adecuados y/o saltos de voltaje o pérdida de energía
- Accesos remotos mal configurados o inadecuados
- Contraseñas mal definidas o nulas
- Inadecuados controles de autenticación a equipos y software
- Software mal diseñado ante vulnerabilidades de desbordamiento de buffer [29] o de DoS [30]
- Medidas y/o software inadecuadas o inexistentes sobre el software malicioso
- Uso de servicios innecesarios en funcionamiento.

3.1.3 APLICACIÓN Y CONFIGURACIÓN DE FIREWALLS

Por último, las vulnerabilidades de red pueden ser de la configuración de la red, del hardware, del perímetro, de la monitorización y autenticación de las comunicaciones y de las conexiones inalámbricas. Todas ellas están relacionadas con:

- Arquitectura de red inadecuada con medidas de seguridad inexistentes o inadecuadas
- Control y configuración del flujo de datos inadecuado
- Configuraciones no almacenadas y/o sin copias de seguridad
- Contraseñas no cifradas y/o con valores por defecto y/o sin cambios en mucho tiempo
- Puertos físicos no asegurados
- Replicaciones inexistentes en redes críticas
- Perímetro de seguridad inexistente
- Cortafuegos inexistentes o mal configurados,
- Configuraciones de control de la red para redes no destinadas a sistemas de control industrial,
- Monitorización inexistente
- Uso de protocolos estándar como telnet o FTP con comunicaciones no cifradas
- Autenticación de los protocolos inexistente en cualquier nivel
- Comprobaciones de integridad inexistentes
- Autenticación entre el cliente inalámbrico y el punto de acceso inadecuada
- Protección de los datos en las conexiones inalámbricas inadecuada.

Las vulnerabilidades más comunes que presentan los protocolos de comunicación, tanto cableados como para comunicaciones inalámbricas son:

- Falta de autenticación de los mensajes
- Falta de cifrado de los mensajes
- Ataques MitM
- Ataques de DoS
- Desbordamiento de búfer o *Buffer*

Un búfer es una memoria continua asignada donde se almacenan los datos de proceso. Un desbordamiento de búfer se produce cuando los datos escritos en un búfer debido a la insuficiencia de espacio corrompen los valores de direcciones adyacentes al búfer asignado. Esto permite al sobrescribir los datos que controlan la ruta lógica de programación para secuestrar el programa y ejecutar en su lugar un software malicioso.

4 COMPARATIVA DE CIBERSEGURIDAD SMART GRIDS E IACS

Existen diversas similitudes entre las Smart Grids y los IACS que les hacen compartir vulnerabilidades ante ciberataques. En ambos casos se trata de sistemas críticos, muy complejos y jerarquizados en los que las comunicaciones adoptan un papel preponderante. Ambos dominios comparten la introducción de las últimas tecnologías de las comunicaciones bajo diversas denominaciones: Industry 4.0, Industrial IoT (IIoT), Smart Grids, etc. Ambos dominios comparten unas arquitecturas muy jerarquizadas basadas en sistemas, dispositivos y protocolos específicos. La pérdida y/o modificación y usurpación de información, produce perdidas económicas, inutilización o funcionamiento erróneo de dispositivos ya sean de control, maquinaría especifica del sector, etc.

Ambos utilizan sistemas similares como SCADAs, RTUs, PLCs y protocolos estandarizados como ModBus, Profibus, DNP3 etc. que deben integrarse cada vez más con los protocolos de la pila TCP/IP por razones de integración, lo cual está abriendo la puerta a nuevas amenazas. Además, en ambos dominios hay un interés creciente en utilizar tecnologías

inalámbricas (IEEE802.11, Zigbee, etc.) que todavía son más susceptibles desde el punto de vista de ciberseguridad.

Las principales vulnerabilidades encontradas en ambos tipos de sistemas son similares, algunas originadas por el envío de información de manera no cifrada. Entre los ataques más frecuentes en ambos casos se pueden citar los siguientes: DoS, MitM, desbordamiento de buffer. Estos ataques se producen en gran parte porque estos sistemas todavía no están preparados para este tipo de amenazas ya que normalmente los ingenieros normalmente se preocupan fundamentalmente del rendimiento y la productividad en tiempo real.

Las vulnerabilidades anteriores se unen a las vulnerabilidades de plataforma donde encontramos que los dispositivos y software utilizados en muchos casos tienen tiempos de vida muy largos llegando frecuentemente a los 20 años sin ninguna actualización de seguridad (ya que frecuentemente predomina el principio: *"Si funciona no lo toques"*) produciéndose vulnerabilidades de 0-day [31], lo que implica que quedan obsoletos con las consecuencias que conlleva.

Ambos dominios requieren la partición de la red con zonas seguras con protecciones de tipo Firewall y control de accesos para dificultar accesos no autorizados y limitar los daños en caso de que se produzcan ataques por malware, ataques DoS, MitM etc. A día de hoy es posible usar accesos remotos desde cualquier ubicación con acceso a Internet a plantas con sistemas de control que pueden ser realizados sin ningún tipo de cifrado, a servicios con puertos abiertos facilitando la labor de los ciberataques.

Con respecto a la integridad y confidencialidad de la información, tanto en los entornos IACS como en las Smart Grids se trata de un requisito indispensable. Por tanto, es de obligado complimiento el aseguramiento de la autenticación de los múltiples dispositivos principalmente AMIs, IEDs y usuarios, así como una protección completa para garantizar la integridad de los datos que son enviados. Tanto en este apartado como en el diseño de red y cifrado de la información existen investigaciones que ayudan a solucionar dichas casuísticas como podemos ver de manera exhaustiva en [5].

Por último, en ambos casos los sistemas pueden ofertar servicios críticos, por lo que los ataques DoS, que en sistemas ofimáticos pueden no resultar tan críticos, en este tipo de sistema son inaceptables. Se trata de una amenaza de primer orden.

5 CONCLUSIONES

Aunque está empezando a haber mayor concienciación con respecto a la ciberseguridad en los sistemas de control, todavía es posible encontrar muchos IACS amenazados por ataques cibernéticos debido a la nula o pobres medidas de seguridad implementadas. Se puede concluir que en muchos casos estos sistemas se han conectado a Internet sin considerar los efectos que puede producir su exposición.

La problemática es similar en las Smart Grids puesto que se comparten sistemas SCADA, RTUs, PLCs, protocolos propietarios y su acercamiento e integración con las TIC y a sistemas corporativos. De hecho, existen investigaciones y soluciones para su uso con los millones de dispositivos electrónicos avanzados como los IEDs y AMIs que están conectados a los nodos de estas redes. A pesar de dichas investigaciones y soluciones es necesario la continuidad de las mismas para proveer de soluciones que se adapten de manera más fiable y eficaz tanto en las Smart Grids ya implementadas como en las futuras.

En este artículo se han analizado algunas de las vulnerabilidades más frecuentes tanto en los IACS como en las Smart Grids. Muchas de estas vulnerabilidades se deben a la carencia de medidas de autenticación y de control, falta de cifrado en las comunicaciones lo cual posibilita diferentes tipos de ataques como ataques Man in The Middle, Denial of Service y desbordamiento de Buffer que pueden producir que los sistemas de control dejen de funcionar total o parcialmente. No obstante los autores han constatado que en la actualidad el dominio de las Smart Grids está más concienciado que el de los IACS.

Por último, cabe señalar que a pesar de que es imposible conseguir un sistema totalmente seguro ante ciberataques es fundamental realizar análisis de riesgos adecuados para implementar medidas de defensa en profundidad tanto a nivel de red y de plataforma acordes con la naturaleza de los sistemas que se desean proteger.

Referencias

[1] Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. Renewable and Sustainable Energy Reviews, 54, 1552-1562

[2] Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., and Jones, K. (2013). Towards Real-Time Assessment of Industrial Control Systems (ICSs): A Framework for Future Research. In Proceedings of the 1st International

Symposium on ICS & SCADA Cyber Security Research 2013, (BCS), pp. 106–109.

[3] G. Lu, D. De, W.-Z. Song, SmartGridLab: A laboratory-based smart grid testbed, in: Proc. of IEEE Conference on Smart Grid Communications, 2010

[4]. Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., & Covrig, C. F. (2016). A survey on the critical issues in smart grid technologies. Renewable and Sustainable Energy Reviews, 54, 396-405.

[5] Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5), 1344-1371.

[6] ETP SmartGrids. The SmartGrids European technology platform. Online. URL ⟨ http://www.smartgrids.eu/ETPSmartGrids

[7] Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. P. (2012). A survey of communication/networking in Smart Grids. *Future Generation Computer Systems*, *28*(2), 391-404

[8] Locke, G., & Gallagher, P. D. (2010). NIST framework and roadmap for smart grid interoperability standards, release 1.0. *National Institute of Standards and Technology*, *33*.

[9] Wei, Dong, et al. "An integrated security system of protecting smart grid against cyber attacks." *Innovative Smart Grid Technologies (ISGT), 2010*. IEEE, 2010.

[10] Colak, I., Fulli, G., Sagiroglu, S., Yesilbudak, M., & Covrig, C. F. (2015). Smart grid projects in Europe: Current status, maturity and future scenarios.*Applied Energy*, *152*, 58-70.

[11] Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews*, *59*, 710-725

[12] Yu, Y., Yang, J., & Chen, B. (2012). The smart grids in China—a review.*Energies*, *5*(5), 1321-1338.

[13] Pearson, I. L. (2011). Smart grid cyber security for Europe. Energy Policy, 39(9), 5211-5218.

[14] Wang, W., Xu, Y., & Khanna, M. (2011). A survey on the communication architectures in smart grid. Computer Networks, 55(15), 3604-3629.

[15] Laverty, D. M., Morrow, D. J., Best, R., & Crossley, P. A. (2010, July). Telecommunications for smart grid: Backhaul solutions for the distribution network. In Power and Energy Society General Meeting, 2010 IEEE (pp. 1-6). IEEE.

[16] Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K. (2010, January). An integrated security system of protecting smart grid against cyber attacks. In*Innovative Smart Grid Technologies (ISGT), 2010* (pp. 1-7). IEEE.

[17] Ponemon Institute (2011) "State of IT Security. Study of Utilities & Energy Companies".

[18] Asokan, N., Niemi, V.,Nyberg, K. (2003) "Man-in-the-Middle in Tunnelled Authentication Protocols", Security Protocols Workshop, volume 3364 of LNCS, pages 28-41. Springer.

[19] Kügler, D., (2003) ""Man in the Middle" Attacks on Bluetooth", Financial Cryptography, volume 2742 of LNCS, pages 149-161. Springer

[20] Meyer U., Wetzel, S. (2004) "A man-in-the-middle attack on UMTS", Proc. 3rd ACM Workshop on Wireless Security (WiSe), pp. 90-97

[21] Jain, M., Jain, A., Srinivas, M., (2008) "A web based expert system shell for fault diagnosis and control of power system equipment", Proceedings of International Conference on Condition Monitoring and Diagnosis (CMD-08), 2008, pp. 1310–1313

.

[22] Fischer, K., Gesner, J., (2012) "Security Architecture Elements for IoT enabled Automation Networks", 17th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA).

[23] Cheminod, Manuel, Luca Durante, and Adriano Valenzano. "Review of security issues in industrial networks." Industrial Informatics, IEEE Transactions on 9.1 (2013): 277-293.

[24] Knapp, E.D., and Langill, J.T. (2015a). Chapter 6 - Industrial Network Protocols. In Industrial Network Security (Second Edition), E.D.K.T. Langill, ed. (Boston: Syngress), pp. 121–169.

[25] ICS-CERT (2012) "ICS-CERT Monitor Newsletters", October–December 2012. https://ics-cert.us-cert.gov/monitors.

[26] McDonald, G., Murchu, L.O., Doherty, S., Chien, E., (2013) “Stuxnet 0.5: The Missing Link”, Symantec, Mountain View, California

[27] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82

[28] Eric D. Knapp and Joel Thomas Langill, Chapter 8 - Risk and Vulnerability Assessments, In Industrial Network Security (Second Edition), edited by Eric D. KnappJoel Thomas Langill, Syngress, Boston, 2015, Pages 209-260

[29] Feifei, L., (2012) “The principle and prevention of windows buffer overflow”, 7th Intl. Conf. Computer Science & Education (ICCSE).

[30] Liu, W., (2009) “Research on DoS attack and detection programming”, 3rd IEEE Intl. Symp. Intelligent Information Technology Application (IITA), pp. 207-210.

[31] FireEye (2013). LESS THAN ZERO: A Survey of Zero-day Attacks in 2013 and What They Say About the Traditional Security Model.