MONITOREO Y CONTROL DE CENTRALES DE GENERACIÓN ELÉCTRICA A TRAVES DE CONTROL CENTRALIZADO

Juan C. Salavarrieta, Consultor en Innovación Tecnológica, **Hermann Fuquen G** Consultor en Innovación Tecnológica (COLINNOVACION)

Resumen — El desarrollo continuo de la tecnología aplicada al sector industrial ha sido fundamental para que los sistemas de monitoreo y control aplicados a procesos de automatización y centralización sean cada vez más eficientes y eficaces mejorando los procesos industriales. Esta tendencia ha sido aplicada con gran éxito en las empresas del sector eléctrico, el cual, en los últimos años ha venido implementando sistemas de monitoreo, supervisión y control y sistemas conexos cada vez más robustos y confiables a unidades de generación energética, al igual que redes de trasmisión y distribución. En este articulo se realiza una breve descripción de los componentes de los sistemas de supervisión y control SCADA, los medios de centralización de los mismos y algunos aspectos básicos de ciberseguridad, así como los ataques y vulnerabilidades más frecuentes presentes en los mismos que se identifican en el estado del arte.

Palabras Clave — SCADA, sistemas de monitoreo y control, ciberseguridad, ataques cibernéticos.

1. INTRODUCCIÓN

A nivel mundial ha crecido el interés por parte de las empresas de servicios públicos en automatizar sus sistemas de producción con el fin de ganar mayores eficiencias que se traduzcan en un servicio confiable y de bajo costo para los usuarios finales (Gray, 2017). Las empresas encargadas de suministrar estos servicios como los generadores de electricidad deben ahondar esfuerzos en hallar eficiencias en su operación que garanticen unos sistemas de control adecuados. Para esto, gran parte de las empresas del sector energético sustentan su operación en sistemas de software tipo SCADA (Supervisory Control And Data Acquisition) los cuales son sistemas de control, supervisión y adquisición de datos que permiten recopilar información de dispositivos de campo lo que permite controlar y monitorear los procesos de manera remota (Boyer, 2009).

Según Hope-Sotherton (2007), garantizar que la integración y homologación de los sistemas SCADA se basen en modelos y metodologías de integración, proporciona ventajas tácticas y estratégicas para las empresas prestadoras de servicios público. Es por esto que la implementación de sistemas de control modernos, permitiría la integración no solo de variables locales sino de procesos corporativos de carácter estratégico, gracias a un mejor manejo y calidad de la información generada (Hope-Sotherton, 2007). En la actualidad, los sistemas de energía basan su operación en los centros de control, los cuales reciben la información de los dispositivos asociados con todo el sistema de generación, operación y dispositivos de medición. Este proceso se hace principalmente a través de un sistema de control de supervisión y adquisición de datos (SCADA) (Tao & Xueyu , 2018).

Sin embargo, el solo hecho de sustentar la operación de unidades independientes en las centrales de generación con sistemas SCADA no es suficiente para las exigencias del mercado actual, puesto que se debe tener en cuenta que la mayoría de las plantas de generación y sistemas de distribución funcionan en red y se debe responder a la demanda agregada de forma conjunta (Garimella, 2018). Por tanto, la centralización y el control integral vienen a ser un factor importante para la operación de las empresas de servicios públicos y sistemas de energía eléctrica.

Para los centros de control en empresas generadoras de energía, la estimación del estado de potencia y funcionamiento del sistema constituye el núcleo de las funciones de monitoreo, análisis y control del sistema en línea. Esta información actúa como un filtro entre las mediciones en bruto recibidas del sistema y las demás mediciones de las funciones de operación que requieren de una toma de datos de mayor confiabilidad necesaria para determinar el estado actual de operación del sistema,

y de manera general, representa un reto en términos de procesamiento de datos, estimación de estado, estimación de errores de parámetros y topología de procesamientos entre otros análisis (ibíd.).

El presente artículo busca hacer una introducción a la estructura de un sistema SCADA, el cual será aplicado a un centro de control que les permitirá a las empresas del sector eléctrico tener un mayor control de sus activos y de su operación, lo que se traduce en eficiencia tanto de su actividad como en el servicio prestado.

2. SISTEMAS DE CONTROL SCADA

Los sistemas de control SCADA la integran varios componentes los cuales permiten un control integral de complejas operaciones industriales, en el caso de este este artículo, empresas de generación de energía eléctrica. Entre los distintos equipos que componen un sistema como este encontramos los siguientes (Sayed, 2017):

- Hardware de la estación externa: dispositivos remotos de control de subestaciones, monitorean magnitudes como el estado de carga, el transformador de corriente (CT), el transformador de voltaje (VT), las válvulas de combustible e interruptores que pueden controlarse localmente o de manera remota.
- Procesadores de subestaciones locales: recopilan datos de los instrumentos de campo y los equipos de hardware, incluidos los RTU, PLC y dispositivos electrónicos inteligentes (IED), incluyendo relés digitales y medidores digitales. El procesador local es responsable de gran cantidad de entradas / salidas analógicas y digitales de IED y equipos de conmutación.
- Instrumentos digitales: usualmente se instalan en el campo o en una instalación local y detectan condiciones tales como corriente, voltaje, irradiancia, temperatura, presión, velocidad del viento y tasa de flujo.
- Dispositivos de comunicaciones: Pueden ser comunicaciones de corto o largo alcance. Las comunicaciones de corto alcance se instalan entre RTUs (Unidad Terminal Remota, por sus siglas en inglés) locales, instrumentos y equipos operativos.

- Computadoras / servidores host: computadoras host, tales como servidores para equipos de cómputo destinados a adquisición de datos, estaciones de trabajo de ingeniería / operación, se consideran el punto central de monitoreo y control, estarán en la sala de control o en la estación principal. La estación de trabajo operativa (central) es donde un ingeniero u operador puede supervisar el proceso, así como recibir alarmas del sistema, revisar los datos y ejercer el control remoto.

La Figura 1 muestra una arquitectura básica de lo que podría integrar a un sistema de control por monitoreo de SCADA de una empresa de generación eléctrica donde se cuenta con estaciones de control que pueden reportar de forma remota e inalámbrica variables como corriente, voltaje, sensores de presión, estado de bombas, válvulas, las cuales se conectan a través de un router a una red SCADA general que junto a un equipo de servidores reciben y procesan la información, reportando a los computadores de ingeniería y a las estaciones de trabajo de los operadores de manera centralizada (Sayed, 2017).

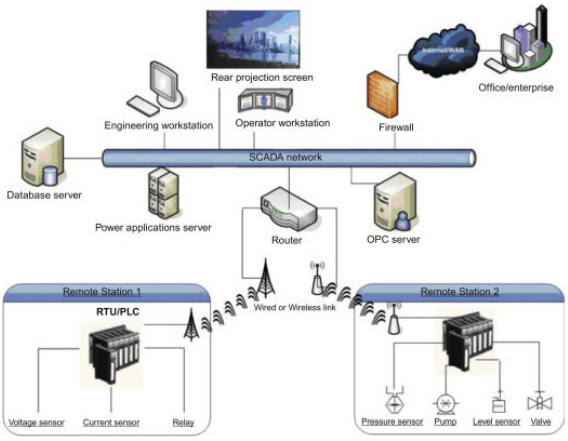

Figura 1. Diagrama de arquitetura de sistema SCADA. Fuente: Fuente: (Sayed, 2017)

En la mayoría de los casos, un sistema SCADA monitoreará y hará pequeños cambios en su funcionamiento para hacer más eficiente su comportamiento y rendimiento. Los sistemas SCADA se consideran sistemas de control de circuito cerrado y funcionan con poca interacción humana (Ibid). Una de las ventajas clave de los sistemas SCADA es su capacidad para supervisar todo un sistema o conjunto de ellos, en tiempo real. Esta operación se hace mediante la adquisición de datos, incluida la lectura del medidor y la verificación de los estados de los sensores, que se comunican a intervalos regulares de tiempo reducido. Un sistema SCADA como sistema de automatización industrial adquiere datos de instrumentos y sensores ubicados en sitios remotos y transmite datos a una unidad central de control maestro para fines de control o monitoreo (Boyer, 2009). Los datos recopilados de los sensores e instrumentos por lo general están ubicados en una o más computadoras anfitrionas SCADA en el centro de control. Sobre la base de los datos recibidos de las subestaciones remotas, los comandos de supervisión automatizados o dirigidos por el operador se pueden enviar a los dispositivos de control

de subestaciones remotos, generalmente llamados dispositivos externos o de campo (Sayed, 2017).

Los dispositivos remotos de control y comunicación se utilizan para ofrecer una solución óptima para cada operación con estructuras de control y funcionamiento flexibles y avanzadas. Esto se puede hacer mediante el uso de controladores PLC, dispositivos de adquisición de datos RTU y enlaces de comunicación avanzados junto con software y hardware SCADA en plantas y estaciones generadoras de energía. La estructura de SCADA en la industria de generación de energía, supervisa varias tareas de operación, incluidas las funciones de protección, el control y el monitoreo de los procedimientos de mantenimiento programados y no programados. Las funciones de control del sistema SCADA en la generación de energía incluyen (Sayed, 2017):

- Monitoreo continuo de la velocidad y frecuencia.
- Observación del estado dinámico de CB, interruptores y relés de protección.
- Planificación de operaciones de generación.
- Control de potencias activas y reactivas.
- Protección contra viento / vapor / turbina de gas
- Monitoreo del sistema de combustible y servicios auxiliares de la estación.
- Programación de carga basada en voltaje y frecuencia
- Procesamiento de datos históricos para parámetros relacionados con la generación.
- Observación de estaciones meteorológicas en caso de plantas eólicas y solares.

3. SALAS DE CONTROL CENTRALIZADAS:

Una sala de control que use un sistema SCADA, teniendo en cuenta las características particulares de cada industria, contará con varios equipos de cómputo que permiten una visualización amplia de los procesos que supervisa. También puede contar con sistemas de visualización tipo Video-wall u otras tecnologías similares para una visualización amplia entre todos los miembros del equipo de visualización de control. (Mehta, 2015).

La implementación de un sistema de control y monitoreo central permite que varios grupos operativos resuelvan problemas diferentes de manera simultánea (y proporcionen redundancia de equipos) inclusive si la problemática proviene de diferentes fuentes. Dado que la gran mayoría de los sistemas SCADA están construidos con cierto nivel de redundancia, el sistema ofrece la seguridad de que el equipo de respaldo funcione de manera adecuada, e incluso con un medio para iniciar manualmente una transferencia operativa al equipo de respaldo.

La Figura 2 muestra una posible distribución de equipos, sistemas de visualización (pantallas) y equipos en una sala de control.

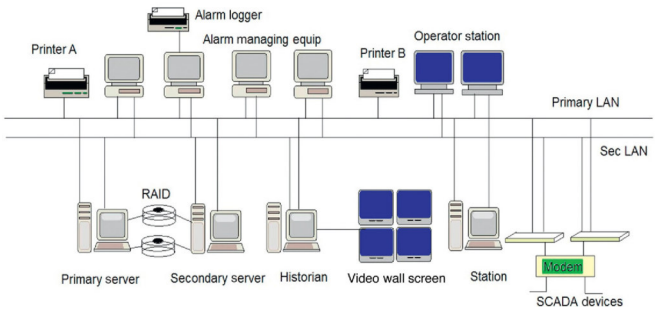

Figura 2. Distribución de equipos en una sala de control con sistema SCADA.
Fuente: (Mehta, 2015)

La utilidad de los sistemas SCADA centralizados son variados. Estos van desde los beneficios de la administración y configuración de la seguridad centralizada, hasta la estandarización operativa y la toma de decisiones a gran escala (Hudson, 2016). Es de gran importancia la gestión de alarmas y señalización de eventos, por lo que la creación de una arquitectura centralizada permite que las alarmas en los subsistemas se gestionen, desde una perspectiva de empresa de servicios públicos, en lo que respecta a la priorización, la asignación de responsabilidades, la coherencia y el análisis de datos. Los estándares clave de la industria proporcionan una dirección importante en el establecimiento de una política de alarmas y eventos de manera estandarizada los cuales pueden aplicarse a nivel de toda la red (Gray, 2017).

Este proceso de gestión de las alarmas es importante ya que los sistemas SCADA manejan grandes volúmenes de datos que cambian constantemente (2,000–70,000 etiquetas, dependiendo de la aplicación), lo que hace inviable, y lleva demasiado tiempo, que un operador humano recorra constantemente todos los datos en busca de problemas. Es por eso, que cobra gran importancia que el sistema SCADA proporcione al menos validez básica y comprobación de alarma sobre todos los datos, así como detectar alarmas y condiciones anormales, y llamar la atención de los operadores, como función primordial de los sistemas SCADA. La configuración para poner en servicio un sistema SCADA implica definir los umbrales de alarma que se utilizarán para cada punto. Algunos sistemas permiten un conjunto predetermina-

do de límites de alarma, y la mayoría también tiene comprobaciones integradas para entradas no válidas (Mehta, 2015).

A continuación, se introducirá el tema de ciberseguridad aplicada a sistemas de información, debido a que cobra gran importancia en la actualidad gracias a la interconexión diaria en la que se procesan datos y se manejan funciones críticas de operación mediante redes de comunicación como los sistemas SCADA.

4. Ciberseguridad en Sistemas de Control SCADA

Las amenazas a la seguridad de sistemas informáticos pueden llevar a comprometer los activos de las empresas afectando los sistemas de información y producción que controlan, más aún en sistemas industriales, que cuentan con procesos basados en el Internet de las cosas (alta interconexión de dispositivos por Internet). Por tanto, se hace critico establecer políticas de ciberseguridad que eviten intromisiones en los sistemas SCADA (Falco, 2018).

Sistemas informáticos inseguros pueden provocar interrupciones con efectos nefastos para la integridad de los equipos, también se puede producir una divulgación de información confidencial y fraudes tanto para la empresa como para sus usuarios. Las amenazas cibernéticas son el resultado de la explotación de las vulnerabilidades del sistema cibernético por parte de usuarios con acceso no autorizado más aun en sistemas SCADA con alta conectividad a Internet. Deben ser identificada la amenaza cibernética potencial para los sistemas de control de supervisión y adquisición de datos (SCADA), que puede impactar desde el sistema informático hasta los aspectos del sistema de potencia eléctrica, para enfrentar estos ataques (Ericsson, 2007), y crear el respectivo plan de mitigación del riesgo. Los riesgos de seguridad han aumentado, ya que anteriormente los sistemas SCADA estaban aislados de otros sistemas. por el contrario, los sistemas modernos, son cada vez más complejos y con atributos digitales, también están conectados a redes externas vulnerables como el Internet. Por lo tanto, un pirata informático puede acceder e interferir en sistemas de control críticos si no se toman las precauciones de seguridad adecuadas. El campo de la seguridad cibernética en relación con SCADA e ICS (sistemas de control industrial) es complejo, y las consecuencias de ignorar las amenazas o implementar controles inadecuados pueden tener consecuencias significativas. Por tanto, es de vital importancia entender los orígenes y los puntos críticos de ciberataques para sistemas SCADA (Irmak, 2018).

Los ataques al software de los sistemas SCADA tienen diferentes orígenes, de manera genérica se pueden clasificar las vulnerabilidades de la siguiente manera:

4.1 Diseño del código fuente y su implementación

Se hace necesaria una codificación segura para minimizar las vulnerabilidades en las aplicaciones y servicios que ofrece el sistema SCADA. Las vulnerabilidades en el software pueden explotarse con fines maliciosos, lo que hace necesario que los administradores del sistema eviten realizar cambios luego de la configuración inicial (Ibid).

Las revisiones de software y los estudios de ingeniería inversa muestran que el software SCADA no siempre representa una estructura segura. Para evaluar la vulnerabilidad de los sistemas de control de distribución de energía, incluidas las redes SCADA, el Departamento de Energía de EE. UU ha desarrollado el programa Nacional SCADA Test Bed (NSTB – 2011). Se ha identificado que las vulnerabilidades del software SCADA observadas en las evaluaciones NSTB son el resultado de software inseguro y pruebas insuficientes. Las tres vulnerabilidades más importantes observadas fueron: Validación de entrada, autenticación y control de acceso. También se entendió que la ejecución remota de código causa funciones peligrosas en la mayoría de las vulnerabilidades (Irmak, 2018). El anterior escenario muestra que es necesario una evaluación constante de los códigos de programación y estar en constante actualización.

4.2 Desbordamiento de búfer

El desbordamiento de búfer es la vulnerabilidad de validación de entrada más común en los sistemas SCADA. Esta ocurre cuando el software escribe más datos en la memoria que el espacio asignado. La aparición de esos datos "extra" sobrescriben la memoria contigua y hacen que el programa no se ejecute con normalidad. Algunos códigos de explotación utilizan el desbordamiento de búfer para crear una sesión interactiva y enviar scripts maliciosos con los privilegios del programa explotado. El desbordamiento de búfer se logra abortando y cambiando los valores de entrada durante la transferencia de datos en las aplicaciones de tráfico de red. Como resultado, las implementaciones de protocolo de red donde los valores de entrada no están validados son vulnerables este tipo de ataques (Irmak, 2018).

4.3 Inyección al SQL (lenguaje de consulta estructurada)

La filtración incorrecta o insuficiente de la entrada de usuario que no garantiza la integridad de los caracteres especiales utilizados en el comando de consulta SQL, puede afectar a la base de datos SCADA, lo que da como resultado la inyección de SQL. Las consultas SQL también se pueden usar para verificaciones de seguridad como la autenticación, y los atacantes pueden modificar la lógica de estas consultas superando la integridad del sistema. Las vulnerabilidades de inyección de SQL generalmente se encuentran en las aplicaciones de cliente (típicamente Web) y explotan la base de datos al enrutar los comandos SQL a la base de datos. Incluso si todas las demás conexiones al firewall están bloqueadas, un ataque exitoso le permite al atacante controlar el servidor SQL a través de una red segura.

4.4 Secuencias de comandos entre sitios (XSS)

El motivo principal de la vulnerabilidad XSS (secuencia de comandos en sitios cruzados) se origina en la validación de entrada, al igual que con la inyección SQL. Sin embargo, en los ataques XSS, la aplicación web envía un código malicioso al usuario. Su peligro es alto porque le permite al atacante colocar código en la página web creada con la aplicación web vulnerable. El código de ataque se ejecuta en el lado del usuario con la autorización del servidor web haciéndolo muy difícil de identificar por parte del usuario (Irmak, 2018).

4.5 Administración de parches (actualizaciones)

La administración de parches efectiva es crucial para los sistemas operativos, servicios, usuarios y software de terceros. Los fabricantes de SCADA pueden mitigar las vulnerabilidades mediante la aplicación de parches en sus productos. La identificación rápida y el parcheo de vulnerabilidades pueden minimizar el riesgo de aparición de vulnerabilidades. A su vez, los fabricantes de sistemas SCADA pueden probar sus parches en productos de terceros antes de usarlos en el producto base. Los parches del sistema operativo se emiten para cerrar las vulnerabilidades de seguridad que permiten a un atacante ejecutar código en el sistema operativo.

4.6 Otros aspectos necesarios

Es importante identificar medios y sistemas de detección de intrusos para la infraestructura industrial más crítica (Irmak, 2018). Se han propuesto sistemas de protección en la investigación de Yun et al., (2018) en los cuales se aplican metodologías de proximidad y cercanía para que sistemas informáticos aprendieran de los patrones de actividad causados por las actividades normales de los usuarios, con el fin de detectar anomalías. Se utiliza sistemas de Machine Learning para identificar anomalías y crear alertas, anticipando situaciones de riesgo. Su comportamiento se basa en el aprendizaje del comportamiento normal en el intercambio de información entre dos sistemas PLC basados en los paquetes de datos transmitidos y recibidos en un intervalo de tiempo, cuando se detectan intercambios fuera de los patrones, se reportan a un sistema superior que supervisa toda la operación y genera la alarma y protección necesaria para que no se vea afectado el sistema. (Yun, 2018)

6. 5. Conclusiones

En la actualidad las empresas de servicios públicos y en el caso de este artículo, aquellas asociadas con el sector eléctrico, han ahondado esfuerzos en construir sistemas de control y monitoreo centralizado, los cuales cuentan con una serie de funciones de operación del sistema y de equilibrio entre la oferta y la demanda que respalda el suministro estable de energía y de la operación en conjunto. A su vez cuentan con varias funciones de operación aplicadas al análisis del sistema y funciones de monitoreo de seguridad de voltaje que proporcionan información adecuada en tiempo real beneficiando tanto a la empresa como a los usuarios (Ericsson, 2007).

Al centralizar las configuraciones de hardware y empaquetar las funciones del software en sistemas SCADA, se agregan funcionalidades propias para la operación de cada unidad de generación, lo que permite la construcción de sistemas altamente flexibles logrando una mayor eficiencia en el funcionamiento del sistema de energía y una respuesta más rápida a las fallas desde una sala central de operación.

La evolución de estos sistemas implica tener esquemas de seguridad más eficientes para evitar ciberataques o violaciones a los sistemas encargados de la operación. En un futuro cercano se espera el uso de Machine Learning para detectar patrones de operación basados en información histórica, estos sistemas de aprendizaje permitirán generar mapas entre características de comportamientos y clases, los cuales ayudarán a robustecer los sistemas de seguridad y de operación de las empresas de energía eléctrica (Kalech, 2019)

BIBLIOGRAFÍA

Boyer, A. (2009). SCADA Supervisory Control and Data Acquisition. *International Society of Automation*.

Ericsson, G. (2007). Toward a framework for managing information security for an electric power utility.

IEEE Trans. Power del, 1461-1469.

Falco, G. C. (2018). IIOT cybersecurity risk modeling for scada systems. *IEEE Internet of Things Journal, 5*(6), 4486-4495.

Garimella, P. (2018). IT-OT Integration Challenges in Utilities. *IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, (págs. 199-204).

Gray, A. P. (2017). A Standardised Modular Approach for Site SCADA Applications within a Water Utility. *IEEE Access, 5*, 17177-17187.

Hope-Sotherton, J. (2007). *Eskom Integrates Area SCADA Systems.* Obtenido de Transmission & Distribution World: https://www.xtensible.net/wpcontent/uploads/Eskom-Integrates-Area-SCADA-Systems.pdf

Hudson, A. (2016). Alarm Management and Reliable Architecture Needed for Utility-wide SCADA Systems. *2016 ISA WWAC Symposium*, (págs. 1-9). Orlando.

Irmak, E. E. (2018). An overview of cyber-attack vectors on SCADA systems. *International Symposium on Digital Forensic and Security (ISDFS) IEEE*, (págs. 1-9).

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, 225-238.

Mehta, B. R. (2015). *SCADA systems Industrial Process Automation Systems.* Chapter 7: pp. 237-300.

Sayed, K. G. (2017). SCADA and smart energy grid control automation. *Smart Energy Grid Engineering*, 484-514.

Tao , J., & Xueyu , S. (Diciembre de 2018). A Mixed WLS Power System State Estimation Method Integrating a Wide-Area Measurement System and SCADA Technology. *Energies*, 1-22.

Yun, J. H. (2018). Statistical Similarity of Critical Infrastructure Network Traffic Based on Nearest Neighbor Distances. *International Symposium on Research in Attacks, Intrusions, and Defenses.*