UNIVERSIDAD DE SANCTI SPÍRITUS
José Martí Pérez
MÁRGENES
Revista multitemática de desarrollo local y sostenibilidad
ISSN: 2664-2190
RNPS: 2460

Fecha de presentación: 22/04/2020 Fecha de aceptación: 29/06/2020 Fecha de publicación: 6/11/2020

¿Cómo citar este artículo?

Yero Gómez, D. E., Vera Montero, R., & Bravo de las Casas, M. (mayo-agosto, 2020). Proceso de implementación del telemando en la subestación eléctrica Sancti Spíritus 1. Revista *Márgenes*, *8*(2), 20-31. Recuperado de http://revistas.uniss.edu.cu/index.php/margenes/issue/view/1123

TÍTULO: METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL TELEMANDO EN LA SUBESTACIÓN ELÉCTRICA SANCTI SPIRITUS 1

TITLE: A METHODOLOGY FOR CONTROL REMOTE IMPLEMENTATION IN THE ELECTRIC SUBSTATION SANCTI SPIRITUS 1

Autores: Ing. Daniel Enrique Yero-Gómez[1], Ing. Roberto Vera-Montero[2], Dra. C. Marta Bravo-de las Casas[3]

[1] Colaborador del Centro de Estudios de Energía y Procesos Industriales (CEEPI) de la Universidad de Sancti Spíritus "José Martí Pérez" (UNISS). Especialista B en Relees, automática y circuitos secundarios. Empresa Eléctrica Provincial de Sancti Spíritus., Cuba. ORCID: http://orcid.og/0000-0003-3000-9340 Correo electrónico: dyero@elecssp.une.cu

[2] Especialista A en Relees, automática y circuitos secundarios. Empresa Eléctrica Provincial de Sancti Spíritus, Cuba. ORCID: http://orcid.og/0000-0002-0495-7251 Correo electrónico: roberto@elecssp.une.cu

[3] Profesora Titular. Universidad "Marta Abreu" de Las Villas (UCLV), Centro de Estudios Electroenergéticos, Facultad de Ingeniería Eléctrica, Santa Clara, Cuba. ORCID: http://orcid.og/0000-0002-8242-0222 Correo electrónico: mbravocasas@gmail.com

RESUMEN

En el presente artículo se propone una metodología para la implementación del telemando en subestaciones eléctricas con el uso del *Modbus*.

Se utiliza el método inductivo-deductivo para establecer las generalidades en cuanto al diseño del telemando de las subestaciones, a partir de las experiencias particulares de los técnicos y especialistas, quienes participarán en la misma. En el desarrollo del artículo se tuvo en cuenta las características del equipamiento disponible en la subestación y las más actuales topologías y tecnologías empleadas en el mundo.

La propuesta, después de analizar y fundamentar teóricamente los riesgos informáticos, presenta una solución factible a este problema para las subestaciones en Cuba.

Palabras clave: riesgos informáticos; subestaciones eléctricas; telemando.

ABSTRACT

An algorithm for remote control implementation in electric substations by using Modbus was proposed in this paper. The inductive-deductive method is used to define the general characteristics of a substation´s remote control design based on the experiences of the technicians and specialists involved in the study. Furthermore, the characteristics of the available equipment in the substation and the cutting-edge technology and topology used in the world were taken under consideration. After analyzing and theoretically expound the computing risks, a feasible solution is proposed to solve this problem in Cuban electric substations.

Keywords: computing risks; electric substations; remote control.

INTRODUCCIÓN

Debido al incremento de la integración de fuentes renovables de energía a la red, se hace necesario contar en Cuba con un sistema eléctrico que, al aprovechar el avance en las tecnologías de las comunicaciones y la información, transforme el sistema eléctrico de potencia tradicional en un sistema complejo y multidimensional: sistema ciber-físico eléctrico de potencia. Todo esto para tener un control en tiempo real, que permita respuestas rápidas en las operaciones del sistema y la asignación eficiente de los recursos energéticos (Vellaithurai, Srivastava, Zonouz, & Berthier**,** 2015).

Los sistemas ciber-físicos actuales, comparados con los relativamente robustos sistemas eléctricos de potencia antiguos, tienen más vulnerabilidades a la seguridad que deben ser estudiados. Lo anterior se refiere a los ataques cibernéticos a la operación y control de los sistemas eléctricos de potencia que, pueden tener un serio impacto dentro del sistema, por la afectación a la seguridad, la producción industrial y el servicio a la población (Sun, Hahn, & Liu, 2018).

Con el desarrollo de la Revolución Energética en Cuba se ha realizado un proceso inversionista que incluye un paso de modernización de subestaciones, la mayoría con una tecnología de más

de veinte años de explotación. El primer paso en la implementación del telemando en Sancti Spíritus es la construcción de la subestación Cabaiguán 110/33 kV, hoy un ejemplo de los beneficios en cuanto operatividad y eficacia para el manejo de la red. Todo realizado con la utilización de la tecnología aportada por fabricante chino *NRTechnology.*

En el presente artículo, después de analizar los distintos elementos que componen estos sistemas y sus riesgos, se plantea una solución eficaz de implementación del telemando en las subestaciones, para su aplicación en la red eléctrica de Cuba.

MATERIALES Y MÉTODOS

Método de trabajo

En el desarrollo de la metodología que se propone para la implementación del telemando, los autores establecieron un ordenamiento. Esta estructura mostrada en la Figura 1, facilita y es consistente para la realización de trabajos similares de este perfil.

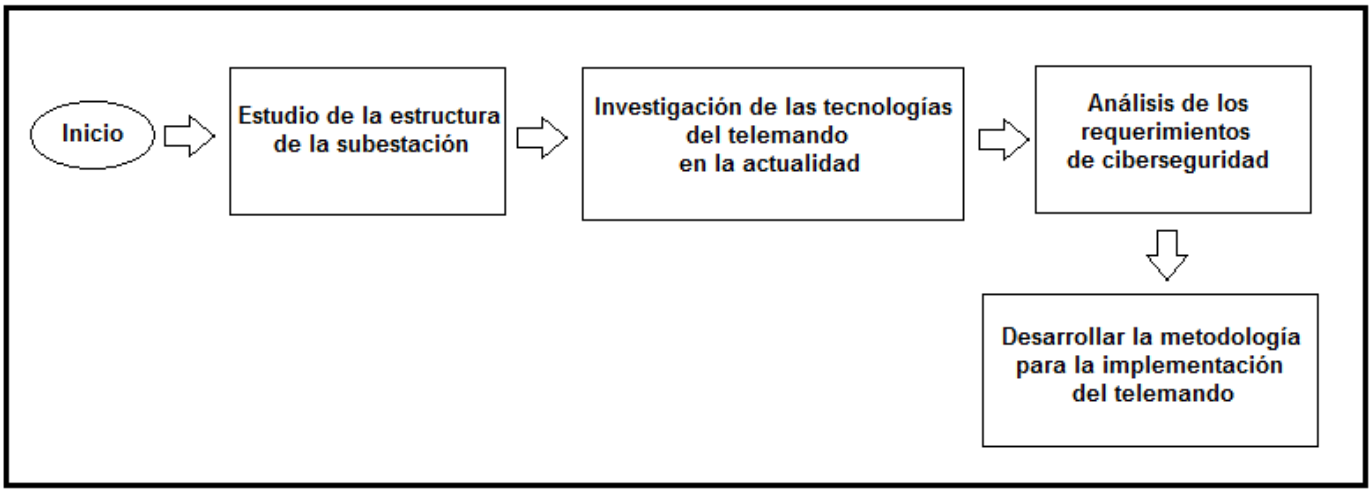

Figura 1. Pasos para la elaboración de la metodología
Fuente: Elaboración propia

Elementos de la subestación

A partir de un estudio del diseño físico de la subestación Sancti Spíritus 1, se define la existencia de una configuración de barra única. Este proceso se realiza con el objetivo de precisar los requerimientos técnicos y prácticos necesarios en la implementación del Telemando.

Con el análisis del sistema automatizado se concluye que este es descentralizado, según la definición aportada por Bamber et al., 2011. El siguiente paso en la implementación del telemando es la definición de los equipos que componen el sistema:

Dispositivos electrónicos inteligentes (IEDs por sus siglas en inglés). Introducen una función específica o varias de ellas, en un circuito o barra de conexión en la subestación. Ejemplos: microprocesador base de un relee de protección o de un instrumento de medición, etc. (Hawk & Kaushiva, 2014; Wei & Wang, 2016).

Módulo o controlador de bahía. Dispositivo que contiene, en la mayoría de las ocasiones, todo el software requerido para el control y manejo remoto de una bahía en la subestación (alimentador de un circuito, línea de trasmisión, etc.).

Interfaz hombre-máquina (HMI por sus siglas en inglés). Principal usuario final de la interfaz de comunicación, generalmente es una PC (computadora) de escritorio, usada de forma común, pero pueden encontrarse computadoras especializadas en aplicaciones específicas.

Bus de comunicaciones, enlaces de varios dispositivos. En una nueva subestación, todos los elementos del sistema automatizado usan el mismo bus o varios buses, para obtener una adecuada relación costo-efectividad.

Enlace al sistema Supervisor de Control y Adquisición de Datos (SCADA por sus siglas en inglés)**.** Este puede ser provisto por una unidad dedicada a este fin, puede ser un HMI o de un IEDs con un esquema de sincronización en tiempo real, y un sistema de comunicaciones que permita un monitoreo remoto de todas las funciones y parámetros de la subestación, siendo este un punto crítico de los ciberataques dentro del sistema (Wang, Hui, & Yiu, 2015; Yan, Tang, Zhu, He, & Sun, 2015; Yu & Chin, 2015).

Una vez puntualizados los elementos presentes se procede a seleccionar la topología de implementación para el sistema de comunicaciones, que son definidas por Bamber et al**.,** 2011. En este proyecto se selecciona la Unidad Terminal Remota (RTU por sus siglas en inglés) básica debido a su rentabilidad económica y disponibilidad de equipos. Esto se aprecia en la Figura 2.

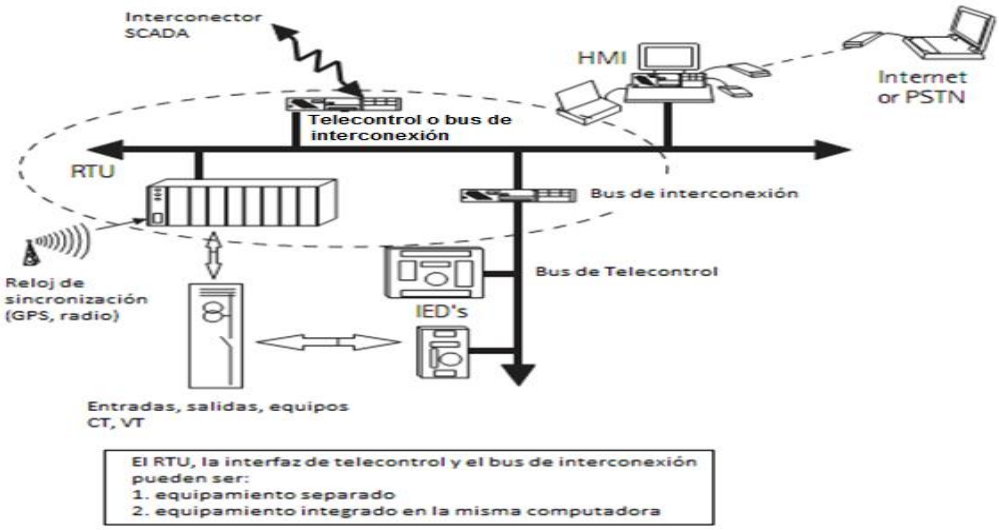

Figura 2. RTU- topología básica

Fuente: Adaptado de (Bamber et al. 2011)

Tecnologías de las comunicaciones

El modelo de transferencia de datos emplea un sistema abierto de interconexión (OSI por sus siglas en inglés) descrito por Aguilar, 2014. De los estándares de conexión física más comunes en las subestaciones eléctricas son el RS-232, el RS-485 y el *Ethernet*, en este proyecto se emplean los dos últimos. El primero de ellos en la conexión entre los dispositivos con el *ION7350* y el segundo para la conexión de este con el despacho provincial de carga, esto se logra apoyados en la información que aportan Rush et. al., 2016.

Del conjunto de protocolos de comunicación serie que se emplean en el telemando de subestaciones IEC 61850 *Ethernet* (Bamber et al., 2011), IEC 60870-5-103 (Rush et. al., 2016), DNP3 (Pánuco, 2017), (González, 2017), *Profibus* (CarrionGordillo, 2018), y el Modbus, este trabajo emplea la última alternativa en su versión: *Modbus*TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet) para comunicarse con el despacho. Esto se logra a partir de la información que se brinda por Buendía**,** 2008 y Rush, et. al., 2016. *Modbus*TCP/IPencapsula una trama *Modbus*RTU estándar en un segmento TCP. Este proporciona un servicio orientado de conexión fiable, lo que significa que toda consulta del maestro espera una respuesta del *esclavo*. El encapsulado se muestra en la Figura 3.

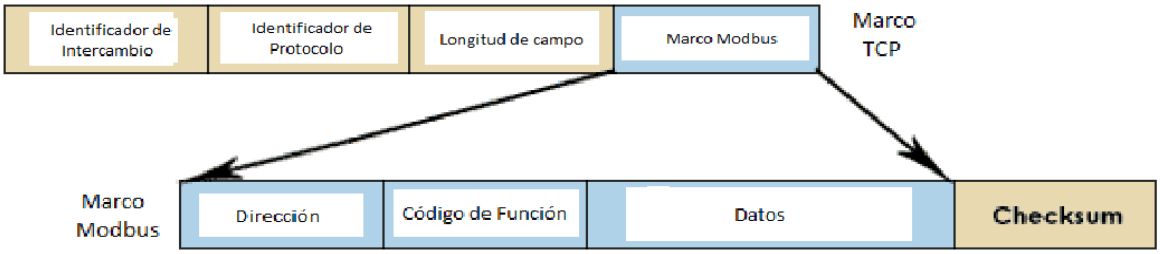

Figura 3. Encapsulamiento de *Modbus* RTU en segmento TCP.

Fuente: Adaptado de Buendía (2008)

Esta técnica de consulta/respuesta encaja perfectamente con la naturaleza *Maestro/Esclavo* de *Modbus*, añadido a la ventaja del determinismo que las redes Ethernet conmutadas ofrecen a los usuarios para su aplicación en el telemando de subestaciones.

Ciberseguridad

Con el incremento de la utilización de protocolos abiertos de comunicación en lainterconexión de las subestaciones, aumentan de forma significativa los riesgos a los que estas se exponen. Algunos delos factores a considerar en la ciberseguridad se muestran en la Tabla 1.

Tabla 1. Factores en el contexto de la ciberseguridad

FACTORES	UTILIDAD
Confidencialidad	Prevenir el acceso no autorizado a la información.
Integridad	Prevenir la modificación no autorizada de la información, como inyección datos falsos.
Disponibilidad/ Autenticación	Prevenir la denegación del servicio, y asegurar la autorización al acceso a la información
No rechazo	Prevenir la denegación de una acción que teniendo lugar.
Rastreo/ Detección	Monitorear y registrar las actividades para detectar intrusiones y analizar los eventos.

Fuente: Elaboración propia

En el marco de la ciberseguridad es necesario eliminar los errores no intencionados (desastres naturales, errores humanos) o intencionados (llamados ciberataques, entre los que se destacan la inyección de datos falsos que pueden provocar el colapso de un sistema estable. Variantes y sus consecuencias se abordan de forma detallada por Hawk & Kaushiva, 2014; Beck, Vu, Huang, &

Xiang, 2015; Liang, Sankar & Kosut, 2016 y Liu & Li, 2016. En la actualidad los controles de seguridad son implementados dentro de las capas de transporte y aplicación, aunque esta última es más común debido a las flexibilidades de implementación que brinda.

Ejemplos de las vulnerabilidades más frecuentes a las que están sometidas las redes de telemando para las subestaciones se destaca por Bamber et al**., (**2011); Langer, Skopik, Smith, & Kammerstetter (2016) y Wei & Wang (2016).

RESULTADOS Y DISCUSIÓN

En las condiciones económicas actuales de Cuba, este trabajo desarrolla la metodología para la implementación de telemando con un el aprovechamiento máximo de los recursos instalados en la subestación Sancti Spíritus 1. El algoritmo empleado se muestra en la Figura 4.

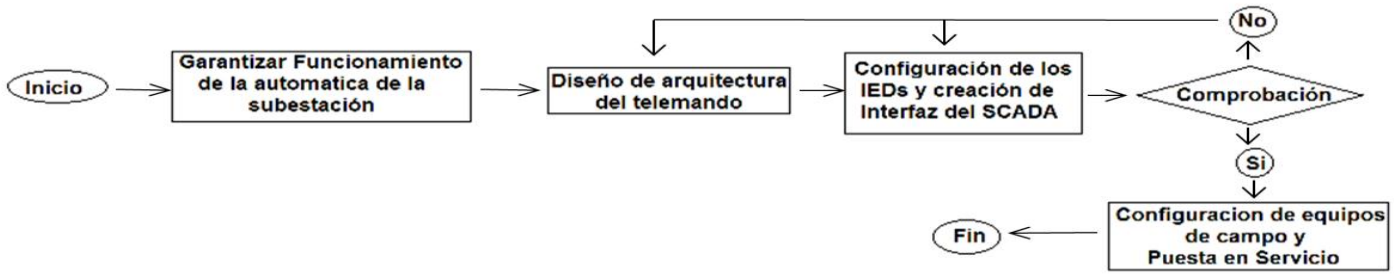

Figura 4. Algoritmo para la implementación del telemando.

Fuente: Elaboración propia

El primer paso previo a la aplicación de esta investigación, es garantizar que la automática de la subestación que incluye alcambia *taps* del transformador y mecanismos de apertura-cierre de los interruptores funcionen de forma correcta. Un detalle para tener en cuenta es que el control de encendido de la ventilación y el cambia *taps* del transformador de la subestación Sancti Spíritus 1, se realiza a través de un Controlador Lógico Programable (PLC por sus siglas en inglés)que trabaja de forma independiente y autónoma al conjunto de la subestación, lo que implica que no sea necesario tenerlo en cuenta dentro del diseño de esta propuesta.

A continuación, se define el diseño dela arquitectura del sistema propuesto para la implementación del telemando. El sistema seleccionado se muestra en la Figura 5, definido como una conexión en estrella simple (Bamber et al., 2011).

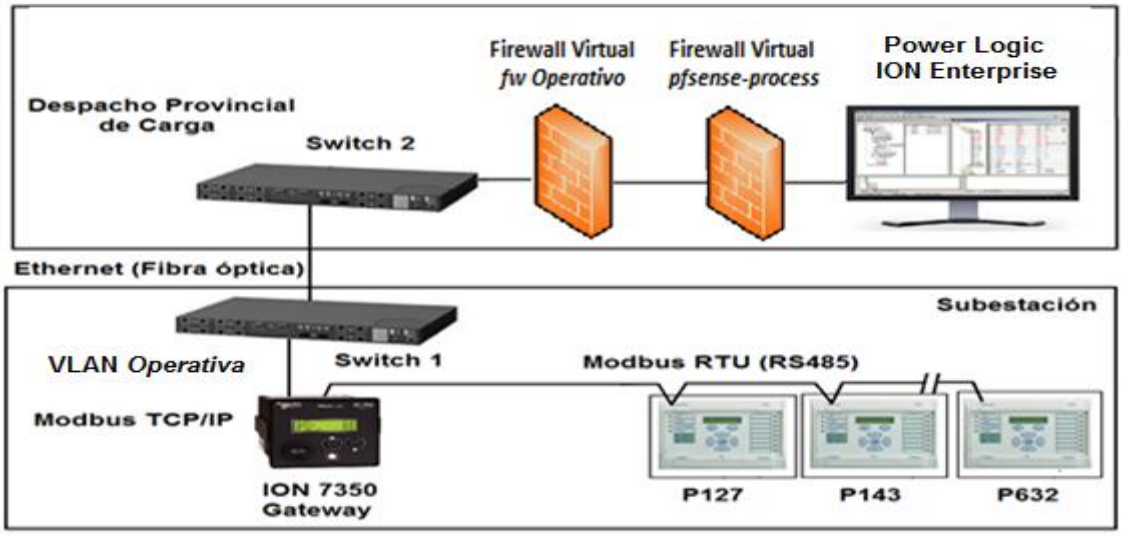

Figura 5. Arquitectura para la implementación del telemando

Fuente: Elaboración propia

Una vez precisados estos aspectos se propone la tecnología a utilizar. En este artículo se emplea el protocolo serie *Modbus* RTU sobre una conexión RS-485entre cada uno de los IEDsque tiene al ION 7350 como *Gateway* (convertidor de protocolo), para luego unirse con un protocolo *Modbus* TCP/IP a una red *Ethernet*sobre la fibra óptica que hoy es la red de comunicación existente entre en el despacho provincial de carga y la subestación Sancti Spíritus 1. El software empleado para el *SCADA* del telemando es el *PowerLogicION Enterprise*, Figura 6, cuya licencia está disponible en Cuba.

Figura 6. Portada del software *PowerLogicION Enterprise*

Dentro del *ManagementConsole* del *PowerLogicION Enterprise*, se realiza el proceso de configuración de los IED, en este caso los P127, P143 y el P632, todos bajo el protocolo *Modbus* con la información disponible en (Rush, et. al. 2016).La ventana de configuración de los IED aparece en la Figura 7.

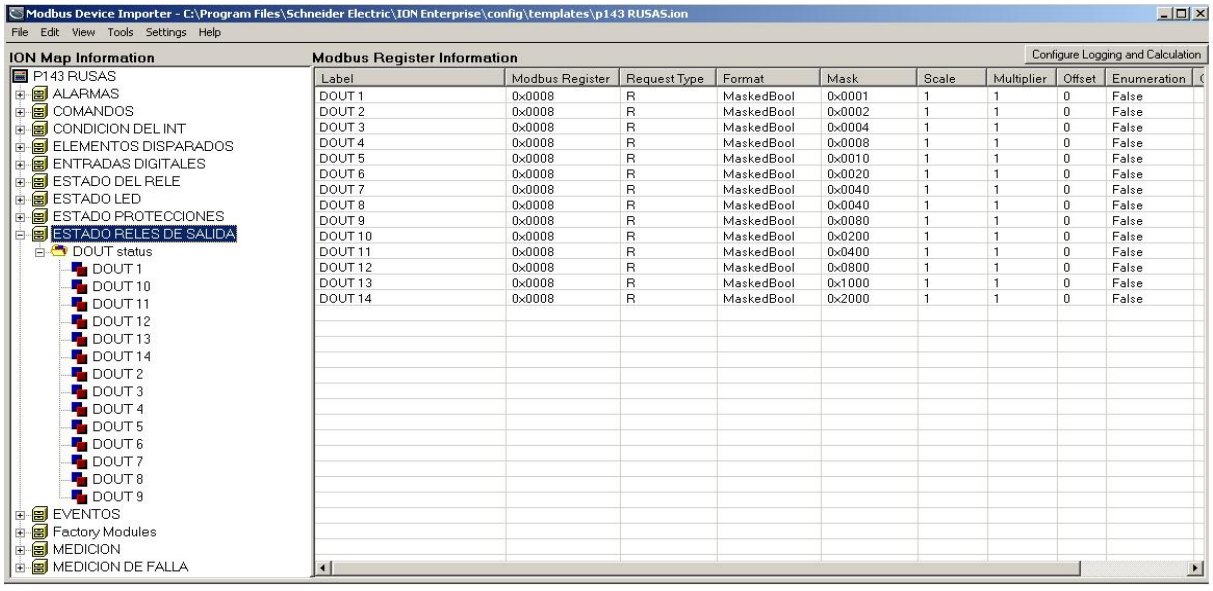

Figura 7. Ventana de configuración del P143 en *PowerLogicION Enterprise*.

Fuente: Elaboración propia

Luego se crea la interfaz para el manejo por parte del usuario dentro de la pestaña Vista del*PowerLogicION Enterprise*. Una vez terminado este proceso se procede a la creación del servidor de sistema, un punto importante a destacar es la definición de los niveles de acceso para cada usuario, mediante el uso de claves con diferentes privilegios. Todo lo cual contribuye a garantizar la ciberseguridad requerida, a través un adecuado manejo de los datos durante la operación del sistema.

Una vez terminado el proceso de configuración de los equipos, el servidor y el diseño del *SCADA*, se realiza la comprobación la ejecución de los comandos y las lecturas de las mediciones con el uso de la maleta de calibración *PONOVO* de fabricación China, con el propósito de detectar y eliminar posibles errores humanos en el proceso de configuración. Esta acción es realizada por el departamento de protecciones de la provincia Sancti Spíritus.Se comprueba solo hasta el relé, quedando para la prueba de campo la comprobación total del esquema.

Durante la puesta en servicio en la subestación del telemando diseñado, se necesita la configuración del ION 7350, donde se define la dirección IP, velocidad de trasmisión de datos y la paridad, entre otros parámetros del equipo obligatorios para que el ION 7350 funcione como Gateway en la conversión del *Modbus* RTU al *Modbus* TCP/IP. Otro paso que debe cumplirse es pasar a los relésP127, P143 y el P632 al modo de operación: opto-remoto-normal (que ejecute los comandos que provengan de entradas binarias, llaves y a través del relé)con el objetivo de que estos respondan a los comandos desde el servidor creado.

Para enfrentar los desafíos de la ciberseguridad citados por Liu & Li, 2017 y después de analizar para la investigación algunos sistemas de defensa, se propone un esquema que utiliza los datos extraídos por el *SCADA* de tele medición de la subestación, hoy en servicio y los datos del sistema propuesto para la implementación de un algoritmo simple de comparación de los datos obtenidos.

El procedimiento desarrollado se basa en la obtención de la potencia que circula y que es medida por cada relé, para luego aplicar una ecuación similar a la ley de Kirchhoff de las corrientes Ecuación (1).

$$\sum \vec{P}_{entrada} = \sum (\vec{P}_{salida1} + \vec{P}_{salida\ 2} + \ldots + \vec{P}_{salida\ n}) \quad (1)$$

Una vez obtenido este valor se procede a comparar su resultado, con el de un esquema similar que es logrado con los datos del sistema de tele medida. Esta propuesta se justifica gracias a la configuración de barra única del sistema en la subestación representada en la Figura 1.

A la vez se debe garantizar la protección de los instrumentos de medición, ubicados dentro de la subestación con el personal de seguridad y los operadores de subestaciones. De esta forma se promueven las buenas prácticas detalladas en el acápite llamado Ciberseguridad. Mientras tanto los programas *fw* Operativo y *pfsence-process* son los encargados de brindar la necesaria protección *firewall* (corta fuegos) dentro del sistema, para este caso estos son *firewall*s virtuales.

CONCLUSIONES

En la propuesta, teniendo en cuenta las especificidades del equipamiento que se encuentra instalado en la subestación Sancti Spiritus 1, se diseña la metodología para la implementación de un sistema de telemando en subestaciones eléctricas. El trabajo profundiza en los requerimientos y las características de los protocolos de comunicación que se emplean en la actualidad, en especial en el MODBUS y sus variantes. Aporta una solución efectiva a los desafíos de la ciberseguridad en estos sistemas. Su implementación de estos sistemas, con la aplicación de esta metodología, en el escenario actual de la integración de fuentes renovables de energía intermitentes, puede, contribuye a aumentar la eficiencia con la que se manejan los recursos energéticos y la estabilidad del servicio.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, E. J. V. (2014). *Análisis de los protocolos de comunicación para automatización de centrales eléctricas Licenciatura en Ingeniería eléctrica y electrónica*. UNAM, Ciudad de México. México.

Bamber, M. et al. (2011). *Network protection and automation guide*. Stafford UK.

Beck, J., Vu, Q. H., Huang, J. K., & Xiang, Y. (2015). A secure could computing based framework for big data information managament of smart grid. *IEEE transactions on could computing*, 233-244.

Buendía, M. J. (2008). Protocolo Modbus. Universidad Politécnica de Cartagena, Colombia.

Carrion Gordillo, K. F. (2018). *Diseño de un Prototipo de Red LAN IEC 485 para su Implementación como Medio Diagnóstico del Control de una Subestación Eléctrica* (Tesis de maestría. Pontificia Universidad Católica del Ecuador, Quito. Ecuador.

González Morales, O**.** (2017). National Instruments. Recuperado de http://www.ni.com/white-paper/52134/es/

Hawk, C., & Kaushiva, A. (2014). Cybersecurity and the Smarter Grid.*Electric Journal*. doi: http://dx.doi.org/10.1016/j.tej.2014.08.008

Liang, J., Sankar, L. & Kosut, O. (2016).Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Trans Power Syst*, 3864-3872.

Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: assessing cybersecurity risks for an evolving smart grid. *Computers & Security*. doi: http://dx.doi.org/doi:10.1016/j.cose.2016.07.008

Liu, X. & Li, Z. (2016). Making trassmitission line outage via false data attack. IEEE Trans Inf Forensics, 1592-1602.

Liu, X. & Li, Z. (2017). False data attack models, impact analyses and defense strategies in the electricity grid. The Electricty Journal, 2-8. doi: http://dx.doi.org/10.1016/j.tej.2017.04.001

Pánuco, C. A. (2017). *Norma IEC 61850 Siemens*. Paperpresented at the Curso UNE_SIEMENS 4to Encuentro. La Habana. Cuba.

Rush, P. et. al. (2016). *MiCOM P14X, P141, P142, P143, P144 & P145*. *Feeder management Relay*. Francia: Schneider Electric.

Sun, C. C., Hahn, A., & Liu, C. C**.** (2018). Cyber security of a power grid: State of the art. Int J *Electr Power Energy Syst*, *99*(3), 45–56.

Vellaithurai, C., Srivastava A., Zonouz S., & Berthier, R. (2015). Cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Trans Smart Grid*, 6, 566–75.doi: https://doi.org/10.1109/TSG.2016.2561266.1–1

Wang, J., Hui, L. C., &Yiu, S. *(2015). Data framing attacks against no linear state estimation in smart grid*. Global Communications Conference Workshop (GLOBECOM), IEEE,http://dx.doi.org/10.1016/Glocomw.2015.7414067

Wei, M., & Wang, W. (2016). Data-centric threats and their impacts to real-time communications in smart grid. *Computer Networks*, 174-187. doi: http://dx.doi.org/10.1016/j.comnet.2016.05.003

Yan, J., Tang, Y., Zhu, Y., He, H., & Sun, Y. (2015).*Smart grid vulnerability under cascade-based sequencial line-switching attacks*. IEEE Global Communications Conference (GLOBECOM), IEEE, 1-7. Recuperado de http://www.ieeexplore.ieee.org

Yu, Z. H., & Chin, W. L. (2015). Blind false data injection attack using pcaapproximation method in smart grid. *Smart Grid, IEEE Transactions*, 1219-1226. doi: http://dx.doi.org/10.1009/TSG.2015.2382714