CEA Comité Español de Automática

XLV JORNADAS AUTOMÁTICA MÁLAGA 2024

UNIVERSIDADE DA CORUÑA

Jornadas de Automática

Demostrador para el análisis de tráfico de red en subestaciones de tracción basadas en IEC 61850.

Baltuille, P.[a], Morán, A.[a], Alonso, S.[a], Prada, M.A.[a], Fuertes, J.J.[a,*], Domínguez, M.[a,*]

[a]*Grupo de Investigación SUPPRESS, Escuela de Ingenierías, Universidad de León, Campus de Vegazana, León, 24007, España*
https://suppress.unileon.es

To cite this article: Baltuille, P., Morán, A., Alonso, S., Prada, M.A., Fuertes, J.J, Domínguez, M.. 2024. Design of a testbed for network traffic analysis in IEC 61850-based traction substations. Jornadas de Automática, 45. https://doi.org/10.17979/ja-cea.2024.45.10920

Resumen

En este artículo se presenta un procedimiento para analizar tráfico de red en subestaciones de tracción ferroviaria basadas en el estándar IEC 61850. Se propone el uso de un conjunto de sondas que detectan los eventos generados por los diferentes dispositivos de la red (relés de protección, unidad de control de subestación, sistema SCADA, etc.), junto con la metodología a seguir para la generación y el análisis de los paquetes de red. Además, se realiza un experimento sobre un armario de control que replica la estructura de automatización de una subestación de tracción. En este sistema se genera tráfico de red de los protocolos IEC 60870-5-104, IEC 61850 GOOSE y MMS a través de la ejecución de una maniobra en condiciones normales. Este tráfico se monitoriza a través de las sondas y se hace un estudio de los eventos mediante la utilización de una herramienta de análisis de paquetes, obteniendo una descripción de los tipos de paquetes detectados durante el periodo de tiempo que dura dicha maniobra.

Palabras clave: Subestaciones eléctricas, Control, Demostrador, Tráfico de red, IEC 61850, MMS, GOOSE

Testbed for network traffic analysis in IEC 61850-based traction substations

Abstract

This paper presents an analysis of the network traffic in modern electrical substations, based on the IEC 61850 standard, which provide energy to the railways. It is proposed to deploy several probes in order to detect the events generated by different Intelligent Electronic Devices (IEDs) in the network, along with a methodology for the generation and analysis of these packets. In addition, an experiment is performed using a cabinet that replicates the automation system of the electrical substation. In this system, IEC 60870-5-104 and IEC 61850 GOOSE and MMS traffic are generated through the execution of an electrical operation under normal conditions. This traffic is monitored through the mentioned probes. A study of the events is performed using a packet analysis tool, resulting in a inspection of the types of packets detected during the period of the operation.

Keywords: traction substations, IEC 61850, network traffic analysis, testbed, modeling and simulation of power systems.

1. Introducción

La digitalización ha supuesto una revolución en la industria, transformando radicalmente los procesos productivos. Este avance tecnológico ha mejorado la automatización de numerosos procesos, lo que ha supuesto una mejora significativa de la eficiencia y una notable reducción de los costes de producción. No obstante, estas mejoras no se han limitado al ámbito puramente industrial, sino también a otras aplicaciones de la automatización, como las infraestructuras críticas. En el ámbito de la distribución de energía, el desarrollo de dispositivos electrónicos inteligentes (*Intelligent Electronic Devices*, IEDs) ha permitido el intercambio estandarizado de datos entre diferentes equipos y la integración de los diversos componentes del sistema eléctrico, garantizando una respuesta rápida

*Autores para correspondencia: jj.fuertes@unileon.es, mdom@unileon.es

ante fallos o interrupciones de suministro (Hunt et al., 2019).

La evolución tecnológica de los últimos años ha provocado también importantes cambios en los protocolos de comunicación industriales. Estos han evolucionado hacia entornos más interoperables y estandarizados, lo cual ha expandido su ámbito de aplicación. Son cada vez más los proyectos que tienen como objetivo la digitalización de los sistemas de gestión y distribución de energía eléctrica que incorporan el estándar IEC 61850. Desde el punto de vista de la investigación y la experimentación, estos ámbitos de aplicación implican el manejo de instalaciones industriales complejas, críticas y que además manejan niveles de tensión y corriente elevados que hacen inviable su utilización a nivel de laboratorio.

Además, estos avances conllevan una exposición a problemas de ciberseguridad y han creado la necesidad de proteger las comunicaciones entre los distintos dispositivos mediante el diseño de estrategias que implementen mecanismos de detección y mitigación de posibles ataques (Mocanu and Thiriet, 2021). Uno de los estándares más destacables en este ámbito de automatización es el IEC 61850, que posee un lenguaje de comunicación estandarizado y elimina diversos costes, como el de migración o integración de equipos (Mackiewicz, 2006).

Dependiendo del propósito o la criticidad de las comunicaciones, se utiliza un protocolo diferente dentro del estándar IEC 61850. De esta forma, el protocolo GOOSE (*Generic Object-Oriented Substation Event*) se utiliza en el envío de órdenes o acciones en el menor tiempo posible, garantizando la comunicación rápida y eficiente entre los dispositivos de protección y control; mientras que los mensajes relacionados con actualizaciones de estados, medidas o eventos que no son críticos son enviados a través del protocolo MMS (*Manufacturing Message Specification*). Por último, los mensajes periódicos correspondientes a los valores analógicos, como corriente y voltaje, digitalizados en tiempo real, se envían mediante el protocolo SV (*Sampled Values*). El estándar asociado IEC 62351 proporciona un marco de protección frente a ataques y amenazas (Hussain et al., 2020). Además, el estándar IEC 60870-5-104 se utiliza para la comunicación remota entre los sistemas de control y el sistema de supervisión.

Existe un creciente interés en capturar el tráfico de red generado por estos protocolos, ya sea para la creación de conjuntos de datos realistas que sirvan como base para el entrenamiento de algoritmos de detección de amenazas, como para el análisis de los propios protocolos desde el punto de vista de la ciberseguridad, observando el comportamiento de ciertos ataques contra la red industrial (Gaspar et al., 2023). En este artículo, se presenta un armario específico que permite la experimentación e investigación en laboratorio, gestionando y manejando las funcionalidades del protocolo IEC 61850 en una subestación de tracción eléctrica como la utilizada en la alimentación de la alta velocidad española. Además, se presenta una metodología para la captura del tráfico de red generado. Esta metodología ha sido evaluada mediante la captura del tráfico generado en el armario de control.

El artículo está organizado de la siguiente manera. En el apartado 2, se hace un análisis del estado del arte actual en relación al diseño de sistemas para analizar tráfico de red del estándar IEC 61850 desde el punto de vista de la ciberseguridad. En el apartado 3, se explica la propuesta realizada, tanto desde el punto de vista del diseño del armario de control como de la arquitectura de sondas para la captura de tráfico en dicho armario. En el apartado 4 se presentan los resultados experimentales. Finalmente, las conclusiones y lineas futuras se describen en el apartado 5.

2. Estado del arte

Las investigaciones previas en este campo se centran en la emulación de subestaciones mediante entornos de experimentación, el estudio de las amenazas y vulnerabilidades y la creación de conjuntos de datos para el entrenamiento de algoritmos que permitan detectar posibles ataques a través del flujo de tráfico que circula a través de la red.

De forma general, existen artículos como (Hussain et al., 2021) que han analizado las vulnerabilidades existentes en las subestaciones, así como el impacto de diferentes ataques sobre las mismas. Otros artículos como (Yildirim Yayilgan et al., 2022) han elaborado metodologías a seguir para la evaluación y la mitigación de los ataques hacia las subestaciones. Además, existen revisiones sistemáticas como (Yang et al., 2019) en las que se investigan los desafíos de la detección de intrusiones en este ámbito.

Respecto a los ataques efectuados contra estas subestaciones, numerosos trabajos investigan el impacto de ciertos tipos de ataques contra distintos entornos que utilizan los protocolos del estándar IEC 61850. El objeto de estudio de estos artículos puede ser más global, como en (Akbarzadeh et al., 2024), (Roomi et al., 2023) o (Hong et al., 2022); o bien centrado en ciertos protocolos del mismo, como GOOSE (Bohara et al., 2020), SV (Hussain et al., 2023) o MMS (Gautam and Ashok, 2020).

Otros trabajos previos han descrito la creación de conjuntos de datos realistas que contienen eventos maliciosos cuya finalidad es comprobar la capacidad de detección de intrusiones en las redes de la subestación (Sarhan et al., 2021) o para entrenar algoritmos de *machine learning* (Chalé and Bastian, 2022). El diseño de algoritmos para la detección y mitigación de ciberataques ha sido destacable debido a la utilidad que éstos presentarían. Sirvan como ejemplo de ello el algoritmo *random forest* de (Quincozes et al., 2022), la red neuronal profunda de (Quincozes et al., 2021) o la estrategia planteada en (Ustun et al., 2021), que han producido buenos resultados.

Por último, algunos trabajos se han centrado en proponer entornos propios sobre los que estudiar el estándar IEC 61850 y su funcionamiento en distintas redes, como (Adepu et al., 2019) o (Chawla et al., 2022). Resulta necesario el desarrollo de entornos ((Yohanandhan et al., 2022)) que emulen de forma realista el comportamiento y las tecnologías utilizadas para la experimentación en ciberseguridad. Estos entornos pueden ser utilizados como objetivos de ataque para estudiar los efectos que causan a los equipos (Hemmati et al., 2022) o para la evaluación de los métodos anteriormente comentados. En los últimos años, se pueden destacar los entornos propuestos por (Soares et al., 2021), (Jorgensen et al., 2022) o (Labonne et al., 2021).

3. Propuesta

La propuesta que se presenta en este artículo consiste en un armario de control de un sistema eléctrico bifásico de trac-

ción para el transporte ferroviario, que generará tráfico de red realista basado en la norma IEC 61850. A continuación, se explica la topología del armario, así como la arquitectura de automatización del mismo. Además, se indica cómo se integran sondas con el objetivo de capturar el tráfico que circula a través de la red de la subestación.

3.1. *Armario de control de subestación de tracción*

El armario representa una subestación eléctrica de tracción que dispone de dos líneas eléctricas de alimentación, una principal y otra de respaldo: la línea D y la línea F. Para seleccionar la linea de alimentación, o cambiar de linea en caso de fallo de suministro, se dispone de 5 interruptores (KD, K430, K432, KF y K431). Además, se incorpora una función ATS (*Auto-Transfer Scheme*) que actúa ante un fallo en la alimentación de cualquier línea transfiriendo la carga hacia la otra línea para evitar una pérdida de disponibilidad y que se provoque un fallo en el sistema. En la Figura 1 se muestra un esquema eléctrico de ambas líneas, así como los sistemas de protección y control que manejan los interruptores.

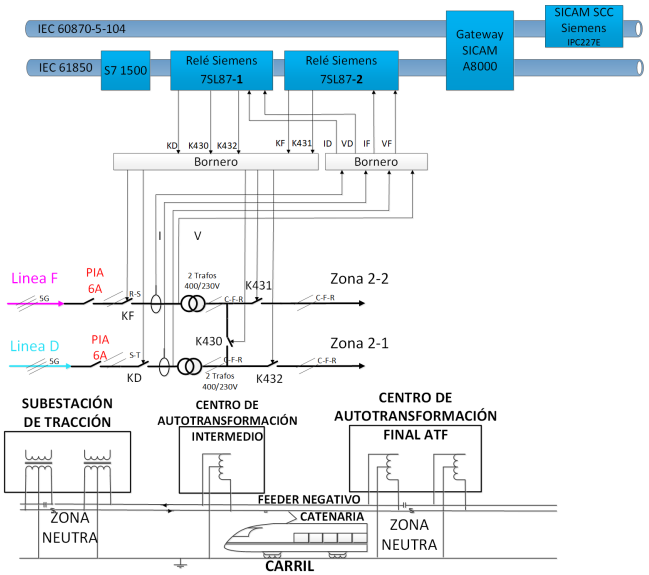

Figura 1: Esquema de líneas del armario de control de la subestación.

El armario está compuesto por una serie de dispositivos especificados en la Figura 2, que se encuentran interconectados en red. La red del armario (ver Figura 3), se divide en dos subredes: la red de supervisión, que se encarga de monitorizar el funcionamiento de la subestación; y la red de control, que se encarga de ejecutar las acciones sobre las líneas D y F. Las comunicaciones de los dispositivos de la red de supervisión siguen el estándar IEC60870-5-104, mientras que las comunicaciones de la red de control utilizan los protocolos del estándar IEC 61850.

A continuación, se enumeran los principales dispositivos que componen el armario, junto con una breve explicación de la función de cada uno de ellos:

- SCADA (*Supervisory Control And Data Acquisition*): El sistema SCADA se encuentra en la red de supervisión y se ejecuta en un computador industrial. Se encarga de la supervisión de la subestación, así como de generar las órdenes dirigidas a los elementos de la red de control.
- *Gateway*: Este dispositivo conecta las redes de control y de supervisión y maneja el intercambio de información entre ambas, realizando conversiones entre protocolos o direccionamientos de datos.
- Controlador de bahía: Es un dispositivo programable de control cuya función consiste en gestionar las maniobras que ejecutan los interruptores.
- Relés de protección: Dos dispositivos que realizan funciones de protección contra sobrecorriente, subtensión y sobretensión sobre las líneas D (relé 1) y F (relé 2). Adicionalmente, el relé encargado de la línea D contiene la función ATS (*Automatic Transfer Scheme*), que garantiza el suministro de corriente eléctrica mediante la línea de respaldo en caso de fallo en la línea principal.

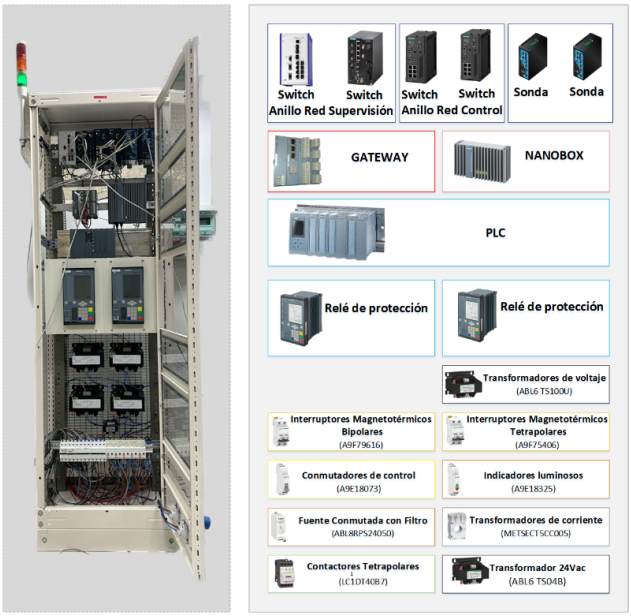

Figura 2: Estructura del armario de control de la subestación.

En cuanto al sistema de comunicaciones hay que destacar los *switches* situados en ambas redes y que se pueden observar en la Figura 3. En cada red hay dos switches que se encuentran interconectados entre sí formando un anillo redundante, de forma que no se interrumpa la comunicación entre dispositivos en caso de un fallo de red. Dentro de la red de supervisión se ha implementado una estación de ingeniería que se encuentra en una máquina virtual. Este equipo permite centralizar todos los programas necesarios utilizados para la configuración de los diferentes dispositivos de la red. Además, en el armario se encuentran dos sondas utilizadas para el análisis de los eventos y la información de la red, cuya funcionalidad se explica en el apartado siguiente.

3.2. *Arquitectura de sondas*

Con el objetivo de analizar las comunicaciones y los eventos de la red de forma detallada, se han implementado dos sondas en la red del armario. Cada una de las sondas contiene un conjunto de reglas de detección y filtrado orientadas a los

protocolos que resultan de interés en cada red. La ubicación de ambas sondas en la red se puede observar en la Figura 3, junto con el flujo del tráfico de red representado a través de las líneas discontinuas.

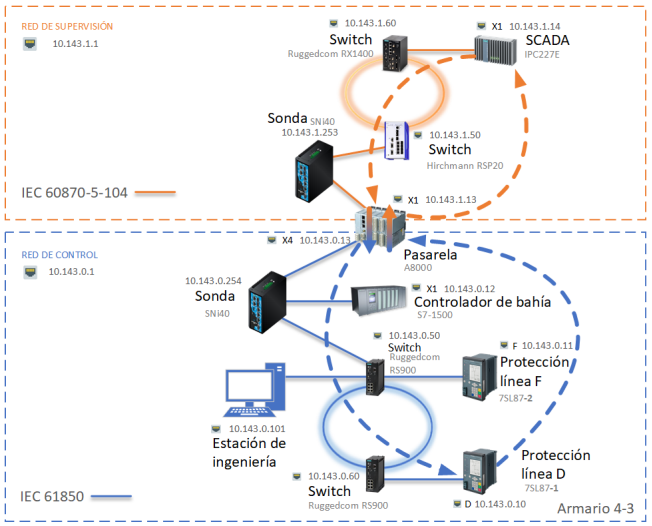

Figura 3: Topología de las redes que forman el sistema.

La primera sonda se ha conectado entre la pasarela y un *switch* del anillo redundante de la red de supervisión. Esta ubicación permite monitorizar el tráfico entrante a la red de supervisión basado en el estándar IEC60870-5-104 y los eventos intercambiados por el SCADA, incluso en el caso de que el número de dispositivos aumente.

La segunda sonda se ha establecido entre la pasarela, el controlador de bahía y un *switch* del anillo redundante de la red de control, cuyo objetivo es la detección del tráfico basado en el estándar IEC 61850. De esta forma se puede detectar el tráfico del protocolo MMS que circula entre la pasarela y el resto de dispositivos y el tráfico GOOSE procedente de los relés.

3.3. Metodología propuesta para el análisis de tráfico de red

La metodología a seguir para la monitorización y el análisis del tráfico de red generado tiene tres fases. En primer lugar, se define la operativa para generar tráfico de red (por ejemplo, se realiza una maniobra de cierres/aperturas de los interruptores desde el SCADA). Esta acción desencadena una secuencia de eventos que genera tráfico IEC 60870-5-104 y MMS en la red de supervisión y MMS, GOOSE o SV en la red de control.

En segundo lugar se procede a la detección/captura del tráfico mediante las sondas que se han definido. Para ello, se utiliza la interfaz web proporcionada por las sondas para visualizar los paquetes, junto con el protocolo utilizado, el origen y el destino del paquete o la hora en la que se ha detectado el mismo. Los paquetes detectados por las sondas se pueden descargar a través de la interfaz para su posterior análisis.

En tercer lugar, se estudia el tráfico detectado anteriormente mediante una herramienta de análisis de paquetes de red. Esta herramienta permite visualizar de forma completa la estructura y el contenido de los paquetes, así como la operación que realizan o los valores a actualizar de los dispositivos.

4. Resultados experimentales

El experimento realizado consiste en la generación de tráfico IEC 61850 mediante la acción de cierre del interruptor KD. Con esta acción el suministro de energía se realizaría desde la linea D. De esta forma, se generan eventos que circulan a través de ambas redes mediante los protocolos IEC 60870-5-104, GOOSE y MMS.

Para realizar la maniobra anterior se ha accionado el interruptor KD desde el SCADA ubicado en la red de supervisión. La captura de una de las pantallas de dicho SCADA se puede observar en la Figura 4.

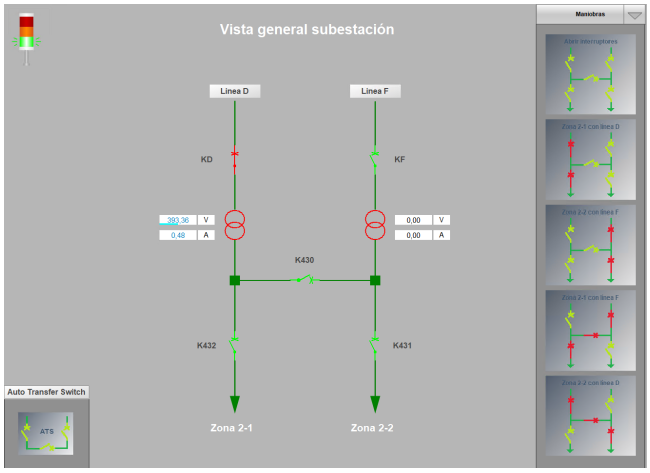

Figura 4: Interfaz del SCADA al accionar el interruptor KD.

Una vez ejecutada la acción en el SCADA, éste envía una orden mediante el protocolo IEC 60870-5-104 a la pasarela cuyo destino es la red de control para cerrar el interruptor KD. Al recibir el paquete anterior, la pasarela envía un paquete confirmando la recepción de la orden al SCADA.

En la red de supervisión y a través del protocolo MMS, se envía la orden del SCADA desde la pasarela al relé 1 indicando la selección del interruptor KD para su posterior cierre (*Select Before Operate*). Una vez recibido el paquete, el relé 1 reserva el interruptor KD para su cierre y responde con otro paquete indicando que la acción anterior se ha realizado con éxito (*Success*).

09:06:54 AM	IEC61850-MMS : service type denied (5)	Controlador_S7-1500	Pasarela_SICAM-A8000
09:06:54 AM	IEC61850 : forbidden service type (Operate)	Controlador_S7-1500	Pasarela_SICAM-A8000
09:06:54 AM	IEC61850 : forbidden service type (SetDataValues)	Controlador_S7-1500	Pasarela_SICAM-A8000
09:06:54 AM	IEC61850-MMS : service type denied (5)	Controlador_S7-1500	Pasarela_SICAM-A8000
09:06:54 AM	IEC61850 : forbidden service type (Report)	Pasarela_SICAM-A8000	Rele_7SL87-2
09:06:54 AM	IEC61850 : forbidden service type (CommandTerminatio...	Pasarela_SICAM-A8000	Rele_7SL87-1
09:06:54 AM	IEC61850 : forbidden service type (Operate)	Pasarela_SICAM-A8000	Rele_7SL87-1
09:06:52 AM	IEC61850 : forbidden service type (Report)	Pasarela_SICAM-A8000	Rele_7SL87-1
09:06:52 AM	IEC61850-MMS : service type denied (5)	Pasarela_SICAM-A8000	Rele_7SL87-1
09:06:52 AM	IEC61850 : forbidden service type (SetDataValues)	Pasarela_SICAM-A8000	Rele_7SL87-1
09:06:52 AM	IEC61850-MMS : service type denied (5)	Pasarela_SICAM-A8000	Rele_7SL87-1

Figura 5: Extracto de los paquetes detectados por la sonda.

A continuación, se envía otro paquete desde la pasarela que indica la operación de cierre del interruptor KD (*Operate*) al relé 1. Este relé ejecuta la acción y envía otro paquete indicando que se ha realizado la acción (*Success*).

Por último, el Controlador de Bahía envía un paquete a la pasarela en el que indica la escritura de una de sus varia-

bles. Una vez escrita la variable, la pasarela responde con un paquete que indica la realización de la operación con éxito.

Respecto al tráfico mediante el protocolo GOOSE, se han detectado paquetes enviados desde ambos relés de protección con destino a todos los dispositivos (*broadcast*). Este tipo de tráfico se envía de forma continua a través de la red para indicar que los relés se encuentran activos.

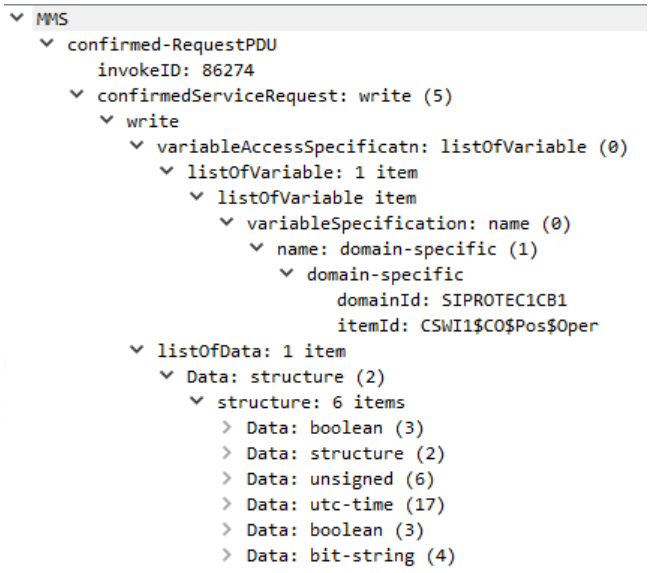

Figura 6: Ejemplo del contenido de un paquete MMS *Operate*.

El tráfico de red se ha capturado mediante las sondas incorporadas en el demostrador y se ha analizado utilizando la herramienta *Wireshark*. En la Figura 5 se muestra un extracto de los eventos capturados por la sonda de la red de supervisión que se corresponden con tráfico IEC 61850. A modo de ejemplo, se explica a continuación el contenido de dos paquetes representativos de los protocolos MMS y GOOSE.

Analizando la estructura del paquete MMS que se muestra en la Figura 6, se puede observar que se está solicitando una operación de escritura sobre la variable *CSWI1COPos$Oper* dentro del dominio *SIPROTEC1CB1* para escribir el conjunto de valores que se especifica en la estructura de datos. Entre estos valores se encuentran datos de tipo booleano, cadenas de bits que contienen la operación o variables de tiempo en formato UTC (*Universal Coordinate Time*).

Respecto a los paquetes GOOSE analizados por la herramienta, se puede observar la estructura de un paquete de la red en la muestra de la Figura 7. Los valores de la estructura indican que se trata de un paquete enviado mediante *broadcast* cuyo origen es el relé 1. El paquete que se muestra como ejemplo contiene información sobre el estado del conjunto de interruptores, la cual se envían como cadenas de bits.

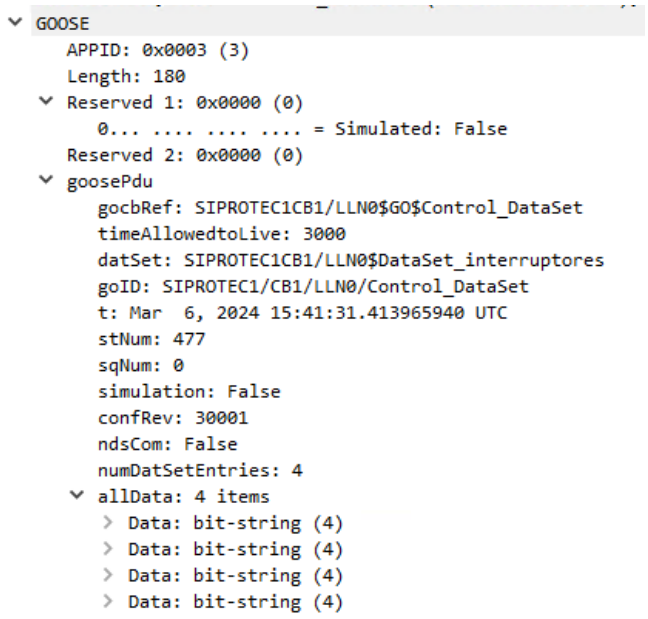

Figura 7: Ejemplo del contenido de un paquete GOOSE.

Para finalizar el experimento, se ha monitorizado el tráfico entrante en la pasarela a través de la sonda ubicada en la red de supervisión durante un rango de tiempo de 8 segundos. Esta captura de tráfico se ha realizado durante la ejecución la maniobra descrita anteriormente con objeto de analizar el número de paquetes intercambiados. Tal y como se puede observar en la Tabla 1, el número de paquetes más detectado corresponde con operaciones de lectura y actualización de valores de los protocolos MMS y GOOSE. Estos paquetes forman parte del tráfico cíclico existente en la red. Se pueden destacar los paquetes resaltados *Op* (*Operate*) y *SBOw* (*SelectBeforeOperate*), los cuales contienen las órdenes de ejecución de la maniobra.

Tabla 1: Número de paquetes intercambiados en la red de supervisión.

Protocolo	Operación	Contador
IEC 61850 MMS	Respuesta	130
IEC 61850 MMS	Lectura	126
IEC 61850 GOOSE	Lectura	38
IEC 61850 MMS	**Escritura (Op)**	3
IEC 61850 MMS	**Escritura (SBOw)**	1

5. Conclusiones

En el presente artículo se ha analizado el tráfico generado por los dispositivos de un sistema de automatización para subestaciones eléctricas de tracción basado en los protocolos definidos en el estándar IEC 61850. Este análisis ha sido posible gracias a la implementación de dos sondas que detectan y monitorizan los eventos generados por los dispositivos. Para la generación de eventos de utilidad, se ha ejecutado una maniobra eléctrica básica consistente en el cierre de un interruptor.

La ejecución de la maniobra anterior ha permitido detectar tráfico en la red mediante los protocolos GOOSE y MMS, los cuales se han analizado de forma completa a través de la herramienta *Wireshark*. Mediante este análisis se ha podido

estudiar el contenido y la estructura de cada uno de los paquetes, así como los dispositivos que se encuentran implicados y las acciones ejecutadas sobre los mismos. Además, se ha averiguado la cronología de los eventos que circulan por la red.

Este trabajo abre nuevas líneas de investigación, como la implementación de algoritmos de detección de anomalías y extracción de características sobre este entorno de automatización. Del mismo modo, se puede completar el sistema existente mediante la inserción de nuevos dispositivos con el objetivo de alcanzar un sistema de pruebas lo más realista posible. Además, el trabajo puede ser utilizado como base para la creación de conjuntos de datos de ciberseguridad o para el análisis del impacto de posibles ciberataques sobre la red. Otra línea de trabajo consistiría en la generación de tráfico de red de otros protocolos del estándar IEC 61850 (como SV o PTP).

Agradecimientos

Este trabajo ha sido realizado dentro del Proyecto Estratégico del Instituto Nacional de Ciberseguridad, S.A. (INCIBE) " Investigación en Ciberseguridad Industrial en los Sistemas de Automatización y Control de las Subestaciones de Tracción", perteneciente a la convocatoria de Proyectos Estratégicos INCIBE (2020-2023).

Referencias

Adepu, S., Kandasamy, N. K., Mathur, A., 01 2019. Epic: An electric power testbed for research and training in cyber physical systems security. In: 17th International Workshop, IWDW 2018, Jeju Island, Korea, October 22-24, 2018, Proceedings. pp. 37–52.
DOI: 10.1007/978-3-030-12786-2_3

Akbarzadeh, A., Erdődi, L., Houmb, S., Soltvedt, T., 05 2024. Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation. International Journal of Information Security, 1–20.
DOI: 10.1007/s10207-024-00856-6

Bohara, A., Ros-Giralt, J., Elbez, G., Valdes, A., Nahrstedt, K., Sanders, W. H., 2020. Ed4gap: Efficient detection for GOOSE-based poisoning attacks on IEC 61850 substations. In: 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). pp. 1–7.
DOI: 10.1109/SmartGridComm47815.2020.9303015

Chalé, M., Bastian, N. D., 2022. Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems. Expert Systems with Applications 207, 117936.
DOI: 10.1016/j.eswa.2022.117936

Chawla, A., Aftab, M. A., Hussain, S. S., Panigrahi, B., Ustun, T. S., 2022. Cyber–physical testbed for wide area measurement system employing IEC 61850 and IEEE C37.118 based communication. Energy Reports 8, 570–578, 2022 The 4th International Conference on Clean Energy and Electrical Systems.
DOI: 10.1016/j.egyr.2022.05.207

Gaspar, J., Cruz, T., Lam, C.-T., Simões, P., 2023. Smart substation communications and cybersecurity: A comprehensive survey. IEEE Communications Surveys & Tutorials 25 (4), 2456–2493.
DOI: 10.1109/COMST.2023.3305468

Gautam, A., Ashok, S., 01 2020. Problem Diagnostic Method for IEC61850 MMS Communication Network. pp. 41–54.
DOI: 10.1007/978-981-32-9346-5_4

Hemmati, M., Palahalli, H., Gajani, G., Gruosso, G., 01 2022. Impact and vulnerability analysis of IEC61850 in smartgrids using multiple HIL real-time testbeds. IEEE Access PP, 1–1.
DOI: 10.1109/ACCESS.2022.3209698

Hong, J., Song, T.-J., Lee, H., Zaboli, A., 2022. Automated cybersecurity tester for IEC61850-based digital substations. Energies 15.
DOI: 10.3390/en15217833

Hunt, R., Flynn, B., Smith, T., 2019. The substation of the future: Moving toward a digital solution. IEEE Power and Energy Magazine 17 (4), 47–55.
DOI: 10.1109/MPE.2019.2908122

Hussain, S., Hernandez Fernandez, J., Al-Ali, A. K., Shikfa, A., 2021. Vulnerabilities and countermeasures in electrical substations. International Journal of Critical Infrastructure Protection 33, 100406.
DOI: 10.1016/j.ijcip.2020.100406

Hussain, S., Ustun, T. S., Kalam, A., 09 2020. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Transactions on Industrial Informatics 16, 5643–5654.
DOI: 10.1109/TII.2019.2956734

Hussain, S. M. S., Aftab, M. A., Farooq, S. M., Ali, I., Ustun, T. S., Konstantinou, C., 2023. An effective security scheme for attacks on sample value messages in IEC 61850 automated substations. IEEE Open Access Journal of Power and Energy 10, 304–315.
DOI: 10.1109/OAJPE.2023.3255790

Jorgensen, P.-A., Waltoft-Olsen, A., Houmb, S. H., Toppe, A. L., Soltvedt, T. G., Muggerud, H. K., 2022. Building a hardware-in-the-loop (hil) digital energy station infrastructure for cyber operation resiliency testing. In: 2022 IEEE/ACM 3rd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS). pp. 9–16.
DOI: 10.1145/3524489.3527299

Labonne, A., Caire, R., Braconnier, T., Guise, L., Jardim, M., Hadjsaid, N., 2021. Teaching digital control of substation and iec 61850 with a test bench validation. IEEE Transactions on Power Systems 36 (2), 1175–1182.
DOI: 10.1109/TPWRS.2020.3010446

Mackiewicz, R., 2006. Overview of IEC 61850 and benefits. In: 2006 IEEE PES Power Systems Conference and Exposition. pp. 623–630.
DOI: 10.1109/PSCE.2006.296392

Mocanu, S., Thiriet, J.-M., 04 2021. Real-time performance and security of iec 61850 process bus communications. Journal of Cyber Security and Mobility.
DOI: 10.13052/jcsm2245-1439.1021

Quincozes, S. E., Albuquerque, C., Passos, D., Mossé, D., 2021. A survey on intrusion detection and prevention systems in digital substations. Computer Networks 184, 107679.
DOI: 10.1016/j.comnet.2020.107679

Quincozes, V. E., Quincozes, S. E., Albuquerque, C., Passos, D., Mossé, D., 2022. Feature extraction for intrusion detection in IEC-61850 communication networks. In: 2022 6th Cyber Security in Networking Conference (CSNet). pp. 1–7.
DOI: 10.1109/CSNet56116.2022.9955599

Roomi, M. M., Hussain, S. M. S., Mashima, D., Chang, E.-C., Ustun, T. S., 2023. Analysis of false data injection attacks against automated control for parallel generators in iec 61850-based smart grid systems. IEEE Systems Journal 17 (3), 4603–4614.
DOI: 10.1109/JSYST.2023.3236951

Sarhan, M., Layeghy, S., Portmann, M., Nov. 2021. Towards a standard feature set for network intrusion detection system datasets. Mobile Networks and Applications 27 (1), 357–370.
DOI: 10.1007/s11036-021-01843-0

Soares, A. A. Z., Soares, L. F., Mattos, D. P., Pinheiro, P. H. B. S., Quincozes, S. E., Ferreira, V. C., Apostolo, G. H., Carrara, G. R., Moraes, I. M., Albuquerque, C., Lopes, Y., Fernandes, N. C., Muchaluat-Saade, D. C., 2021. Enabling emulation and evaluation of IEC 61850 networks with titan. IEEE Access 9, 49788–49805.
DOI: 10.1109/ACCESS.2021.3068366

Ustun, T. S., Hussain, S. M. S., Ulutas, A., Onen, A., Roomi, M. M., Mashima, D., 2021. Machine learning-based intrusion detection for achieving cybersecurity in smart grids using IEC 61850 GOOSE messages. Symmetry 13 (5).
DOI: 10.3390/sym13050826

Yang, Y., Xu, H., Mclaughlin, K., Sezer, S., Jiang, H., Huang, W., 01 2019. Cybersecurity Testing Technology in Smart Substations. pp. 223–254.
DOI: 10.1016/B978-0-12-815158-7.00007-X

Yildirim Yayilgan, S., Holik, F., Abomhara, M., Abraham, D., Gebremedhin, A., 2022. An approach for analyzing cyber security threats and attacks: A case study of digital substations in norway. Electronics 11 (23).
DOI: 10.3390/electronics11234006

Yohanandhan, R. V., Elavarasan, R. M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., Zhao, J., Terzija, V., 2022. A specialized review on outlook of future cyber-physical power system (CPPS) testbeds for securing electric power grid. International Journal of Electrical Power & Energy Systems 136, 107720.
DOI: https://doi.org/10.1016/j.ijepes.2021.107720