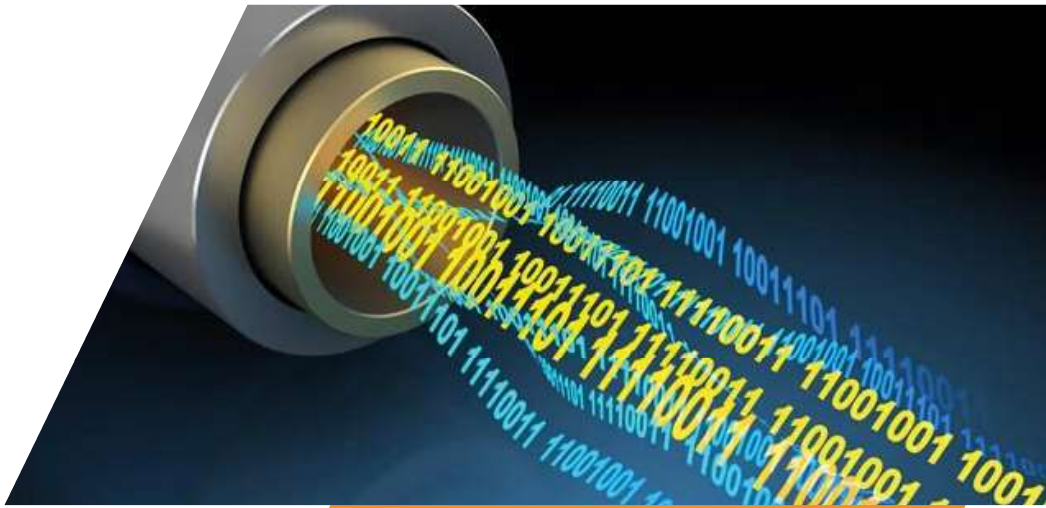
ESTUDIO DEL TRÁFICO DE DATOS EN UNA RED LOCAL ENTRE LOGO V8Y VARIADOR DE FRECUENCIA ABB

STUDY OF DATA TRAFFIC BETWEEN LOGO V8 AND ABB VARIABLE FREQUENCY DRIVE IN A LOCAL NETWORK



ESTUDIO DEL TRÁFICO DE DATOS EN UNA RED LOCAL ENTRE LOGO V8 Y VARIADOR DE FRECUENCIA ABB

STUDY OF DATA TRAFFIC BETWEEN LOGO V8 AND ABB VARIABLE FREQUENCY DRIVE IN A LOCAL NETWORK

Juca Rodríguez Cristian Ronaldo[1]
Lara Márquez Brayan Javier[2]
Tarco Chafla Daniela Alexandra[3]

[1] Escuela Superior Politécnica de Chimborazo, Ecuador, cristian.juca@espoch.edu.ec
[2] Escuela Superior Politécnica de Chimborazo, Ecuador, brayan.lara@espoch.edu.ec
[3] Escuela Superior Politécnica de Chimborazo, Ecuador, daniela.tarco@espoch.edu.ec

RESUMEN

El presente estudio se llevó a cabo en la Facultad de Informática y Electrónica de la ESPOCH, con el objetivo principal de analizar el tráfico generado por una conexión entre un Controlador Lógico Programable (PLC) y un Variador de Frecuencia, que controla la velocidad de un motor trifásico. Para realizar este análisis, se consideró el número de tramas transmitidas por unidad de tiempo, que se identificaron mediante el uso de un software capaz de reconocer los diferentes protocolos de transmisión del modelo TCP/IP. Se determinaron los niveles de seguridad para la transmisión de datos y el acceso a Internet en el monitoreo remoto en tiempo real a partir de los protocolos estudiados.

Palabras clave: Tráfico de red, S7COMM, PLC, Servidor web, Protocolos de red.

ABSTRACT

The present study was carried out at the Faculty of Computer Science and Electronics at ESPOCH, with the main objective of analyzing the traffic generated by a connection between a Programmable Logic Controller (PLC) and a Frequency Inverter, which controls the speed of a three-phase motor. To perform this analysis, the number of frames transmitted per unit of time was considered, which were identified using software capable of recognizing the different transmission protocols of the TCP/IP model. The levels of security for data transmission and access to the Internet were determined in real-time remote monitoring based on the studied protocols.

Keywords: *Network traffic, S7COMM, PLC, Web server, Network protocol.*

Recibido: 31/01/2023 Aceptado: 05/04/2023
Received: 31/01/2023 *Accepted: 05/04/2023*

1. INTRODUCCIÓN

El tráfico de datos hace referencia como los paquetes, unidades de datos fundamentales más pequeñas que se transmiten a lo largo de una red. El tráfico consiste en dividir estos paquetes para su transmisión y volver a ensamblarse en el destino. [1]

El estudio del tráfico de red se establece como un método de seguimiento de la actividad de la red para detectar problemas de seguridad y operación.

En la Fig. 1. se muestran los elementos que se involucran en el tráfico de una red, donde la plataforma SOC es el centro de operaciones de seguridad, que monitorea, previene, detecta, investiga y responde a las amenazas cibernéticas. [2]

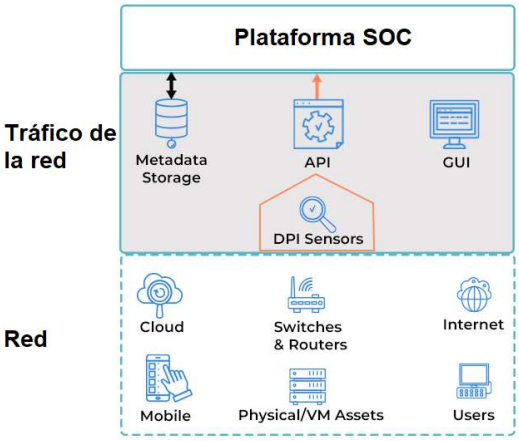


Fig. 1. Descripción general del tráfico en una red

Entre los aspectos más importante por los cuales se debería realizar un análisis de la red son:

Detección automática de anomalías. – Las soluciones de análisis de tráfico de red atribuyen comportamientos a activos específicos proporcionando un amplio contexto para que los equipos de seguridad decidan si una alerta merece una respuesta. [3]

Disponibilidad de red. – El análisis del tráfico de red proporciona información detallada sobre la disponibilidad y el tiempo de actividad de las redes; detectando el tiempo de inactividad causado por interfaces de red defectuosas y falta de disponibilidad de subredes, así como otros obstáculos para la disponibilidad. [3]

Rendimiento de la red. – El rendimiento mejora cuando se realiza un seguimiento en los equipos de TI, al proporcionar una descripción general del uso de recursos, a través de un análisis del tráfico de red. Esto contribuye a identificar las conexiones de red que requieren actualizaciones mediante la localización de aquellas que carecen del ancho de banda necesario para completar una tarea de forma rápida. [3]

Visibilidad robusta. – La creciente adopción de la computación en la nube, e IoT ha evidenciado un crecimiento en los entornos de trabajo remotos, por lo que ha hecho que el mantenimiento de una red sea un proceso complejo. El análisis del tráfico de red genera información que otras fuentes de datos no pueden lograr. [3]

Seguridad mejorada. – En los últimos años han existido numerosos ciberataques, entre los que se destacan: STUXNET [4], SLAMMER [5] y MARIPOSA [6], estos evidencian las vulnerabilidades que presentan los sistemas de control industrial (ICS) frente a amenazas cibernéticas, además de los casos mencionados. Se evidencia que el objetivo de los ciberataques no es elegido al azar, pues las consecuencias pueden llegar a ser desastrosas tanto en lo que respecta al medio ambiente, como a la economía de la empresa y a la salud de las personas.

Por lo expuesto, resulta evidente que el diseño de un sistema de control industrial moderno sea este dedicado para una infraestructura crítica o no, debe contemplar desde su concepción un plan de análisis de tráfico de datos con la finalidad de proteger los activos de la empresa, para garantizar la disponibilidad de sus procesos, la integridad de los datos que se manejan y la confidencialidad de estos.

Las vulnerabilidades en las redes IT, no son la única opción que existe para comprometer una planta industrial, pues un ICS puede ser atacado de manera directa a través de los dispositivos de campo, esto debido a las debilidades de diseño que presentan los equipos de control y monitoreo industrial como se evidencia en [7].

Una alternativa para detectar este tipo de malware es también el análisis de tráfico de red, mediante este se consigue monitorear la disponibilidad y la actividad de la red para identificar anomalías, incluidos problemas operativos y de seguridad. Recopilando registros históricos en tiempo real de lo que sucede en su red, a través de la detección y uso de protocolos mejorando la visibilidad interna y eliminando los puntos ciegos

2. METODOLOGÍA Y MATERIALES

El presente trabajo inició con una revisión bibliográfica que permitió identificar trabajos previos realizados, tomando como referencia la investigación de la Universidad de Chile [8] la cual propone un análisis de datos de redes para seguridad mediante la ejecución de simulaciones de tráfico web en diferentes condiciones para capturar el comportamiento a nivel de la capa de Internet.

La metodología de investigación utilizada fue la inductiva, estableciendo premisas singulares de cada caso estudiado a través de la observación de las gráficas resultantes del tráfico de datos para posteriormente establecer una conclusión general.

Para la situación de estudio propuesta, se requiere una selección adecuada de componentes, ya que no todos los PLC tienen las características necesarias para conectarse a la red y algunos modelos necesitan módulos adicionales para su conexión.

Los parámetros técnicos y selección de componentes se desglosarán a continuación; considerando los equipos existentes en el laboratorio de Industria 4.0 de la Facultad de Informática y Electrónica.

- ☐ Especificaciones del PLC
- ☐ Especificaciones del Motor
- ☐ Detalles del Variador de Frecuencia
- ☐ Descripción del Editor Web
- ☐ Parámetros técnicos
- ☐ Implementación

Especificaciones del PLC

SIEMENS LOGO 8.3. – Tiene la capacidad de conectarse y permitir almacenamiento permanente en la nube alcanzando el procesamiento de grandes volúmenes de datos. Adicional, se puede crear dashboard usando la herramienta LOGO Web. [9]

La encriptación de seguridad se realiza mediante *Transport Layer Security,* al tener la comunicación con la nube integrada también se puede utilizar como gateway para Modbus TCP/IP. [9]

Especificaciones del Motor

Se trabajó con un motor trifásico jaula de ardilla cerrado de hierro fundido de tipo M2QA. El modelo al cual se tuvo acceso fue 90S4A, con potencia de 1kW e IP55 - IC 411, con aislamiento clase F / ΔT B y voltaje de 220-230 YY y 440-460 Y. [10]

Detalles del Variador de Frecuencia

De los modelos existentes: ABB ACS 350 y Lenze 152X2, se seleccionó el primero debido a sus características.

El ACS 350, puede trabajar en rangos de voltaje de 200 - 240 V y 380 - 480 V. Soporta los buses de campo: DeviceNet, PROFIBUS DP, CANopen, Modbus RTU y Ethernet. [11]

Descripciones del Editor Web

Existen varios editores web para diseñar *dashboard*, sin embargo en este trabajo se considerarán dos: Logo Web Server, Node-Red.

Logo Web Server. – software que permite web sities personalizados, que se utilizan para controlar y monitorear tareas automatizadas en LOGO. A través de los componentes se puede integrar valores digitales y analógicos [12].

Node-Red. – Herramienta de programación para conectar dispositivos de hardware, API y servicios en línea. Con este los dispositivos pueden actuar como dispositivos *edge* o *pre-edge* similares a los dispositivos actuadores o sensores en una red IoT [13].

MODELO TCP/IP

Su diseño se basa en protocolos estándar; este modelo ayuda a determinar cómo se deben conectar los dispositivos finales a Internet y cómo transmitir datos entre ellos. Creando redes virtuales cuando varias redes informáticas están conectadas entre sí [14]. El modelo contiene cuatro capas:

1. Capa de enlace

Encargado de la transmisión entre dos dispositivos en la misma red.

2. Capa de Red

Brinda la movilidad de los paquetes de origen a destino, para facilitar la interconexión. Realiza cuatro procesos básicos: [15]

- ☐ Direccionamiento de dispositivos finales
- ☐ Enrutamiento
- ☐ Encapsulación
- ☐ Des-encapsulación

3. Capa de transporte

La capa de transporte proporciona comunicación lógica entre los procesos de aplicación que se ejecutan en diferentes *hosts* dentro de una arquitectura en capas de protocolos y otros componentes de red; se encapsula en TCP o UDP. [14]

4. Capa de aplicación

Permite el acceso a los recursos de la red.

PROTOCOLOS ESTUDIADOS

TCP.- Esta orientado a la conexión para los servicios que utilizan reconocimientos y respuestas para establecer una conexión virtual entre las estaciones de envío y recepción. Este protocolo usa *acknowledgments* los cuales se emplean para garantizar que se mantenga la conexión. [15]

HTTP.- Empleado para transferencia de hipertexto es un protocolo de aplicación para sistemas de información hipermedia distribuidos y colaborativos que permite a los usuarios comunicar datos en la World Wide Web, brindando a los usuarios una forma de interactuar con recursos web. [16]

ARP.- Usado en la resolución de direcciones, el cual es importante a nivel de la capa de red, ayuda a encontrar la dirección MAC dada la dirección IP del sistema [17].

De manera que, la dirección IP del PLC (32 bits) es convertida en una dirección MAC (48 bits) para poder monitorear el estado de los sensores y actuadores a través del IDE, es decir, determina la dirección de hardware de un dispositivo a partir de una dirección IP.

S7COMM.- Se basa en el modelo TCP/IP, usando el servicio de transporte ISO orientado a bloques. Está envuelto en los protocolos TPKT e ISO-COTP, lo que permite que la unidad de datos de protocolo (PDU) se transmita a través de TCP. [18]

Se orienta a funciones/comandos, hecho que implica que una transmisión consiste en una solicitud S7 y una respuesta adecuada. El número de transmisiones en paralelo y la longitud máxima de una PDU se negocian durante el establecimiento de la conexión.

IMPLEMENTACIÓN

La implementación del sistema se ha realizado siguiendo los siguientes pasos:

- **Selección de los componentes adecuados:** Se han seleccionado los componentes necesarios para la implementación del sistema, teniendo en cuenta las especificaciones técnicas y los requisitos del proyecto.
- **Conexión de los componentes:** Los componentes se han conectado de acuerdo a los diagramas de conexión previamente diseñados.
- **Programación del PLC:** Se ha programado el PLC utilizando el software LOGO Soft Comfort. Se han definido las entradas y salidas, se ha creado el programa de control y se han establecido las comunicaciones con los demás dispositivos.
- **Configuración del variador de frecuencia:** Se ha configurado el variador de frecuencia utilizando el software de programación proporcionado por el fabricante. Se han establecido los parámetros necesarios para el correcto funcionamiento del motor.
- **Diseño de dashboard:** Se han diseñado los dashboard utilizando las herramientas Logo Web Server y Node-Red. Se han creado visualizaciones en tiempo real de los datos obtenidos del sistema.
- **Pruebas del sistema:** Se han llevado a cabo pruebas del sistema para comprobar su correcto funcionamiento. Se han realizado pruebas de conexión, pruebas de comunicación y pruebas de control del motor.

ARQUITECTURA

En la Fig. 2 se observa el escenario sobre el cual se va a desarrollar el estudio de tráfico. Allí se puede notar que en el funcionamiento del sistema intervienen dos agentes principales:

El ICS con sus dispositivos de campo y red de comunicaciones, el centro de control y monitoreo remoto SOC con sus dispositivos y personal de ingeniería.

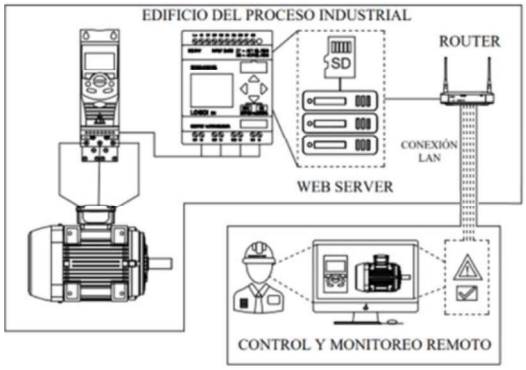


Fig. 2. Propuesta de Arquitectura del estudio

Funcionamiento

El ICS está conformado por un motor trifásico, un variador de frecuencia y un PLC conectado mediante un cable Ethernet a un router.

El PLC, tiene la función de controlador del proceso y a la vez de servidor web, este último, será creado a través de Logo Soft Comfort y el *dashboard* para control y monitoreo en Logo Web Editor, podrá ser accedido desde el SOC para controlar el encendido del motor, su sentido de giro y establecer tres velocidades constantes distintas mediante una red WI/FI local.

Diagrama de Conexión Eléctricas

En la Fig. 3 se muestra la bornera de conexión del variador de frecuencia hacia la red de alimentación la cual debe ser una fuente de voltaje trifásica de 220-230V AC.

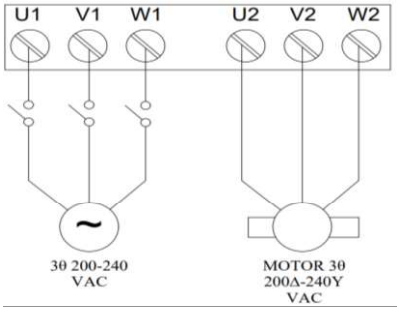


Fig. 3. Conexiones entre el convertidor de frecuencia, la fuente de alimentación y el motor eléctrico

Adicional se muestra, la conexión entre el variador y el motor. En ambos circuitos de potencia el calibre de cable a utilizar será AWG 14 y se incluye un interruptor termomagnético de 15A para desconectar la alimentación del variador, la conexión al motor no necesita de protecciones extra pues el variador se encarga de proteger los conductores contra sobre corrientes.

La Fig. 4 presenta el esquema de conexiones entre las salidas del PLC y las entradas/salidas digitales del variador.

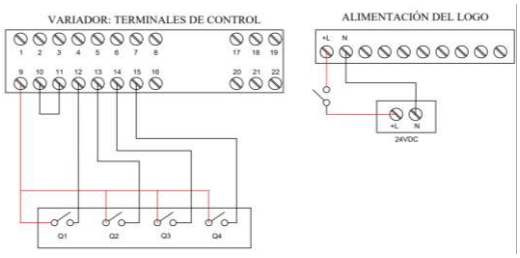


Fig. 4. Conexiones entre las salidas del Logo y las entradas del variador de frecuencia y alimentación del Logo

Estas conexiones están basadas en lo establecido por el fabricante del variador cuando se pretende usar el macro de aplicación en el estándar ABB. El calibre del conductor a utilizar tanto para las conexiones de control, como la alimentación del PLC es AWG 16, además se incluye un interruptor termomagnético de 2A entre el PLC y la fuente de alimentación, la misma que debe ser de 24V DC y debe suministrar 4A.

Tabla 1. Detalle de los tronillos de la bornera de control del variador de frecuencia

1: SCR	**9: +24V- max 200mA**
2: EA1	10: GND
3: GND	11: DCOM
4: +10V	12: ED1
5 EA2	13: ED2
6: GND	14: ED3
7: SA	15: ED4
8: GND	16: ED5

3. RESULTADOS

El control del motor y el variador con el PLC LOGO se puede llevar a cabo de varias maneras, de las cuales, para el estudio de este trabajo se basó en el control a través de Node-Red, Logo Web Server y un monitoreo desde el IDE de programación de LOGO.

El objetivo de la misma es identificar los protocolos que presentan en cada proceso de adquisición y la vulnerabilidad que se puede presentar debido a la encapsulación de los paquetes, como también el tipo de control que se puede llevar a cabo a través de los mismos.

En el proceso de comunicación de los casos expuestos se genera un tráfico de

datos por protocolo, mismos que son identificados a través del software WireShark.

Se exponen en la Tabla *2* los protocolos en estudiados.

Tabla 2. Protocolos de comunicación generados.

1er Caso	2do Caso	3er Caso
TCP	TCP	TCP
ARP	S7COMM	HTTP

1er Caso: Monitoreo a través del ide de LOGO
2do Caso: Monitoreo a través de Node-Red
3er Caso: Monitoreo a través de Logo Web Server

1er Caso:

Cuando no existe una conexión a la red, la información se lleva a cabo a través de TCP y ARP. A través del IDE de programación se puede realizar un monitoreo de los sensores y actuadores que se están ejecutando en el proceso, la utilización de esta herramienta de visualización genera un tráfico para la obtención de estos valores. En la Fig. 5 y Fig. 6 se puede observar el flujo de datos que conducen los protocolos TCP y ARP. Dichos datos comunican el estado de las variables usadas: indicadores y actuadores que están ejecutándose en el momento.

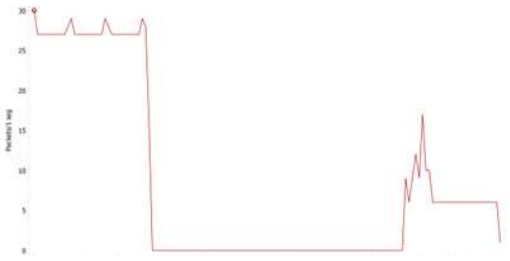


Fig. 5. Tramas generadas por el protocolo TCP (1er caso)

Fig. 6. Tramas generadas por el protocolo ARP (1er caso)

En este caso se presenta el tráfico que genera el protocolo TCP (Fig. 5) y el generado por ARP (Fig. 6) van cambiando según las solicitudes realizadas por el controlador y la recepción desde el entorno de programación de LOGO. Este tráfico es la cantidad de tramas que son enviadas como entrada y salida, tomadas en una instancia de tiempo en la cual el motor fue variando su velocidad a través del variador ABB implementado. El tráfico generado por ARP se debe a la codificación realizada para obtener la dirección MAC del PLC una vez entablada la comunicación con el direccionamiento IP.

2do Caso:

Para la ejecución de la plataforma Node-Red se requiere del puerto 102 de comunicación, a través del cual se lleva a cabo el intercambio de todo el tráfico generado de la red, es decir, será el medio por el cual se controla el PLC. A partir del análisis de este puerto se puede hallar la Fig. 7.

Analizando la gráfica se puede ver que al cabo de 7 segundos que se establece la comunicación, una cantidad de tramas fueron llevadas por este puerto, mismas que contienen información de monitoreo y control de las variables utilizadas, tanto en la interfaz de control como en LOGO.

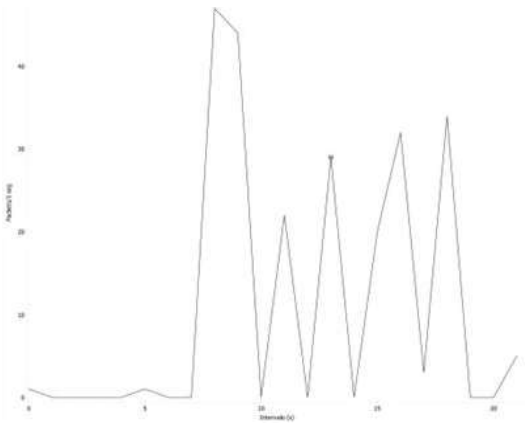


Fig. 7.Flujo de datos que atraviesa el puerto 102.

Para la transmisión de datos entre Node-Red y el PLC, se utiliza un protocolo denominado S7COMM. Este tráfico se puede observar en la Fig. 8.

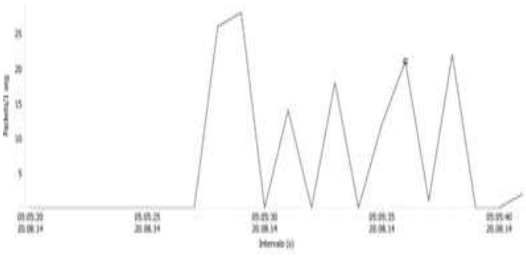


Fig. 8.Tramas generadas por unidad de tiempo por el protocolo S7COMM.

La Fig. 8 muestra cómo los datos son adquiridos, la unidad de los paquetes enviados se mantiene en 0, ya que no existe un intercambio de datos si no se realiza una petición directa desde la plataforma remota y el PLC emita una respuesta. La lectura de la variables establecidas desde los sensores y los actuadores a ser controlados desde la interfaz inician la comunicación, además, se observa que a 6 segundos de haber iniciado el proceso, la transmisión se ha iniciado

3er Caso

Para el control y monitoreo a través del servidor web de logo, se presentan los protocolos TCP y HTTP, los cuales se muestran en la Fig. 9 y Fig. 10, respectivamente.

En la Fig. 9 se observa la cantidad de tramas que se envían por unidad de tiempo, las cuales llevan la mayor cantidad de información y estado de las variables para su monitoreo, razón por la cual existe una elevada cantidad de información, expresadas con picos elevados, así también, existen otros que tardan en descender a cero, ya que se requiere que el enlace permanezca establecido.

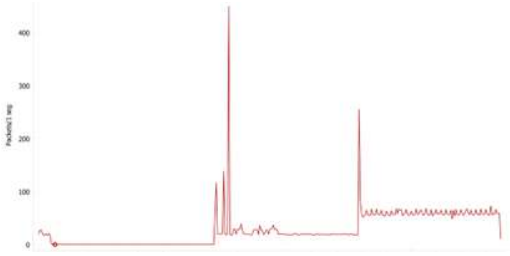


Fig. 9. Tramas generadas por el protocolo TCP (3er caso)

Mientras que en la Fig. 10 está presente únicamente el tráfico de salida a la red generado, el cual permite que los valores estudiados puedan ser llevados al servidor de logo, estos valores permiten que el intercambio de información permanezca en un constante estado de recepción y emisión.

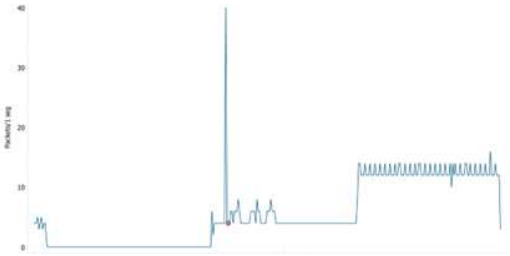


Fig. 10. Tramas generadas por el protocolo HTTP (3er caso)

Cabe mencionar que además de los protocolos mencionados, en el 3er caso existe el protocolo UDP, el cual permite que la salida a la red sea mediante un servidor DNS.

4. DISCUSIÓN

Establecer una conexión entre un servidor (Node-Red, Logo Web Server) o un entorno de programación (LOGO ide) crea un flujo de datos que transporta la información necesaria para resolver problemas, verificar el estado de los sensores como variables o ejecutar los actuadores correctos. . El protocolo TCP, como se puede observar en el apartado de salida de los tres casos estudiados, está presente en todos ellos e incluye algunas modificaciones. Además, incluye protocolos propios para cada plataforma, como S7COMM, que se incluye para atravesar el puerto 102 sobre TCP. En cualquier caso, existen similitudes en el número de tramas enviadas por un protocolo similar debido al tipo de datos que transmiten, aunque representen una diferente a la otra y cumplan una función diferente.

El protocolo ARP se encarga de encontrar la dirección IP y así obtener la dirección MAC del dispositivo, lo que permite la conexión entre el controlador y el entorno de monitoreo. Mientras que S7COMM es un tráfico diseñado para establecer un vínculo entre LOGO y la plataforma Node-Red, lo que permite la comunicación y el posterior intercambio de datos. Este protocolo es propiedad de Siemens y se utiliza para los controladores Siemens S7, que también se pueden utilizar en algunos PLC LOGO.

Muestra el protocolo HTTP que se produce cuando el PLC se conecta al propio servidor de LOGO, que se encarga de cifrar los datos enviados. El cifrado de datos mediante el protocolo de cifrado y consulta se realiza para proteger la integridad de los datos y aumentar la seguridad.

5. CONCLUSIÓN

La comunicación de un controlador lógico programable o PLC hacia un entorno de control y/o monitoreo, genera un tráfico que puede ser vulnerado según el tipo de proceso en el cual se vea involucrado; sin considerar el tamaño de este, se presentará una variación de protocolos según el requerimiento o solicitud realizada. A través de un estudio del tráfico se puede verificar hacía que tipo de ataques puede estar expuesto.

Según la plataforma de red local que se pueda implementar en este tipo procesos, el cifrado de datos e integridad de estos va a cambiar de acuerdo con la necesidad, a través de un estudio de tráfico generado, elegir un método de monitoreo remoto puede ser más preciso y eficaz si de salvaguardar la información se trata, llevando a cabo la no vulneración de estos.

Si bien existen protocolos que fueron generados y estudiados en este trabajo, también se presentaron otros que por su contribución menor pero no menos importante dentro de un entorno de comunicación típico, no fueron abordados debido a la cantidad de tramas que estos transportan, mismos que no causaron una variación significativa en la obtención de históricos en cada caso.

El protocolo UDP genera un tráfico que se utiliza para comunicar de manera rápida un servidor con un dispositivo o acceso remoto, este protocolo es capaz de enviar información con un intervalo de tiempo corto pero vulnerando la información debido a que no posee un cifrado de datos confiable. Este protocolo está incluido dentro del tráfico generado TCP y HTTP, los cuales de manera colectiva presentan un rendimiento mayor a nivel de seguridad.

Una conexión de red local usando un entorno de visualización como el ide de programación, si bien es útil, no puede ser utilizado para un monitoreo, debido a su complejo entendimiento y conocimiento previo de manejo, mientras que una plataforma como Node-Red, presenta varias ventajas sobre los demás, presenta un entorno visual agradable y de fácil manipulación; su vulnerabilidad y uso de herramientas propias de la plataforma como lo es su protocolo S7COMM, si bien es compatible con LOGO, no es recomendable al no ser un protocolo predispuesto para este tipo de PLC, mientras que la implementación de su propio servidor web, permite tener una mejor experiencia con respecto a la manipulación de variables y monitoreo de estados.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] Deke Guo, Data Center Networking: Network Topologies and Traffic Management in Large-Scale Data Centers, Springer Nature, 2022.

[2] Check Point Software Technologies, «SOC (Security Operation Center),» Check Point Software, 2018. [En línea].

[3] H. Ashtari, «Network Traffic Analysis,» Spiceworks, 2022. [En línea]. Available: https://www.spiceworks.com/tech/networking/articles/network-traffic-analysis/.

[4] R. McMILLAN, «Stuxnet worm hit industrial systems,» Siemens, 2010. [En línea]. Available: https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html. [Último acceso: 31 Octubre 2022].

[5] V. P. S. S. C. S. S. S. y. N. W. D. Moore, «Inside the slammer worm,» *IEEE Secur Priv,* vol. I, nº 4, pp. 33-39, 2003.

[6] A. B. V. H. B. y. M. D. P. Sinha, «Insights from the analysis of the Mariposa botnet,» *5th International Conference on Risks and Security of Internet and Systems,* nº 4, 2010.

[7] G. Tzokatziou, L. A. Maglaras y H. Janicke, «Using Human Interface Devices to exploit SCADA systems,» *Insecure,* 2015.

[8] J. Chávez Barbaste, «Análisis y modelos de datos de redes para seguridad informática,» *Universidad de Chile - Facultad de Ciencias Físicas y Matemáticas,* 2016.

[9] Siemens, «SIMATIC LOGO! Manual,» 2013.

[10] ABB LV Motors, «Motores Eléctricos Trifásicos - 50 y 60 Hz,» 2008.

[11] ABB, «Convertidores de frecuencia ABB para maquinaria general ACS350, 0,37 a 22 kW / 0,5 a 30 CV,» 2009.

[12] SIEMENS, «SIEMENS. LOGO! Software,» 2002. [En línea]. Available: https://new.siemens.com/global/en/products/automation/systems/industri. [Último acceso: 15 12 2022].

[13] OpenJS Foundation., «Node-RED:Low-code programming for eventdriven applications.,» 2022. [En línea]. Available: https://nodered.org/. [Último acceso: 19 12 2022].

[14] L. Williams, «Modelo TCP/IP: ¿Qué son las capas y el protocolo? Pila TCP/IP,» 3 Diciembre 2022. [En línea]. Available: https://www.guru99.com/tcp-ip-model.html. [Último acceso: 26 Diciembre 2022].

[15] J. F. Kurose y K. W. Ross, «La capa de red: el plano de datos,» de *Redes de computadoras, Un enfoque descendente*, Madrid, Pearson, 2017, pp. 253-299.

[16] Noite.pl, HTTP Protocol: Network Basic. AL0-034, NOITE S.C..

[17] B. Hartpence, Packet Guide to Core Network Protocols, "O'Reilly Media, Inc., 2011.

[18] Siemens, «S7 Communication,» 2019.