Classification Errors in Industrial Communication Network (Modbus TCP / IP)

Cristhian Manuel Durán Acevedo, PhD.[1], and Elkin Javier Lizarazo Rivera, Ing.[1]
[1] Universidad de Pamplona, Colombia, cmduran@unipamplona.edu.co, e.lizarazo29@hotmail.com

***Abstract*– This article describes the development of a methodology applied to the classification of errors industrial communication network (Modbus TCP / IP), through a pattern recognition method is described. The tests were conducted with the programming of a PLC TWIDO TWDLCAE40DRF, and was subjected to disturbances or faults generated on the network. Data were acquired and monitored by the ModScan32 tool and were subsequently processed through the Principal Component Analysis (PCA), obtaining a success rate in discriminating 100%. In this study was possible to classify easily and quickly some factors or errors generated in a Modbus communication.**

***Keywords*— Industrial Communication, Modbus TCP / IP, ModScan32, pattern recognition, PCA**

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2015.1.1.250
ISBN: 13 978-0-9822896-8-6
ISSN: 2414-6668

Clasificación de Errores en una Red de Comunicación Industrial (Modbus TCP/IP)

Cristhian Manuel Durán Acevedo, PhD[1], Elkin Javier Lizarazo Rivera, Ingeniero[1]
[1] Universidad de Pamplona, Grupo Multisensoriales, Colombia, cmduran@unipamplona.edu.co, e.lizarazo29@hotmail.com

***Abstract*– En este artículo se describe el desarrollo de una metodología aplicada a la clasificación de errores de una red de comunicación industrial (Modbus TCP/IP), a través de un método de reconocimiento de patrones. Las pruebas se realizaron con la programación de un PLC TWIDO TWDLCAE40DRF, y fue sometido a perturbaciones o fallos generados en la red. Los datos fueron adquiridos y monitoreados por la herramienta ModScan32 y posteriormente fueron procesados a través del Análisis de Componentes Principales (PCA), obteniendo una tasa de acierto en la discriminación de 100%. En este estudio fue posible clasificar de manera fácil y rápida algunos factores o errores generados en una comunicación Modbus.**

***Keywords*-- Comunicación Industrial, Modbus TCP/IP, Modscan32, Reconocimiento de patrones, PCA**

I. INTRODUCCION

Las comunicaciones industriales se pueden definir como un conjunto de reglas que conllevan a realizar un intercambio de información entre diferentes sistemas o procesos, permitiendo a los controladores (es decir, PLC's) intercambiar bits, bytes o paquetes en forma eficiente. Dentro de las diferentes funciones que debe cumplir un protocolo de comunicaciones en una red industrial se pueden mencionar las siguientes: Control de flujo, direccionamiento de datos, detección y solución a los posibles problemas a errores de transmisión [1] y [2].

El análisis del comportamiento de los datos transmitidos a través de una red de comunicaciones industriales es muy necesario, ya que es posible detectar o identificar ciertos fallos que afecten el funcionamiento en la comunicación y el proceso [3]. Actualmente existen métodos para detectar y corregir errores en una trama de datos [4], pero no se evidencian estrategias que puedan detectar el tipo de error en la conexión. En este estudio se utilizó el software ModScan32 [5], el cual permite analizar el comportamiento de una trama de datos cuando un cable de comunicación con conector RJ45 tipo 10BaseT es sometido a diferentes eventos que normalmente provocan errores en la transmisión de los datos. Algunos de estos errores pueden ser generados por desconexión del cable, ruptura interna del cable y corto circuito instantáneo entre los cables de transmisión o recepción. El uso principal del software es escanear la trama de datos que es enviada y recibida entre los diferentes dispositivos conectados a una red Modbus TCP/IP [6] y [7], por lo cual es posible determinar si hay un error en la comunicación, ya que proporciona características específicas en la trama al momento de ocurrir un fallo. Las pruebas fueron realizadas a través de la conexión del PLC TWDLCAE40DRF del fabricante Schneider electric [8], donde el análisis de la trama de datos fue realizado a partir de un PC con el algoritmo de reconocimiento de patrones (Análisis de Componentes Principales (PCA)), con el objetivo de obtener de manera gráfica diferentes comparaciones y aproximaciones de una característica específica del error de comunicación [9] y [10]. Mediante este método fue posible identificar el tipo de evento que genera el error en los datos transmitidos en una red Modbus. A continuación se describen cada una de las etapas desarrolladas para el análisis de los datos obtenidos del autómata y la generación de errores.

II. CONFIGURACIÓN DE LA COMUNICACIÓN

Incialmente se realizó una programación del autómata TWDLCAE40DRF a través del software TwidoSuite v2.30, en el cual se implementó una aplicación teniendo en cuenta la descripción tanto de las entradas (%I0.X) como de las salidas físicas (%Q0.X). Como variable principal de comunicación se definió el registro interno (%MX) para que poder ser analizado por el software ModScan32. La configuración de la comunicación del autómata puede ser realizada por medio de los puertos seriales y Ethernet, donde es posible acoplarlo a una computadora mediante una sencilla conexión. Este proceso es muy importante porque permite enlazar al PLC con una computadora, a través del analizador de tramas. La Fig.1 ilustra la interfaz del software ModScan32.

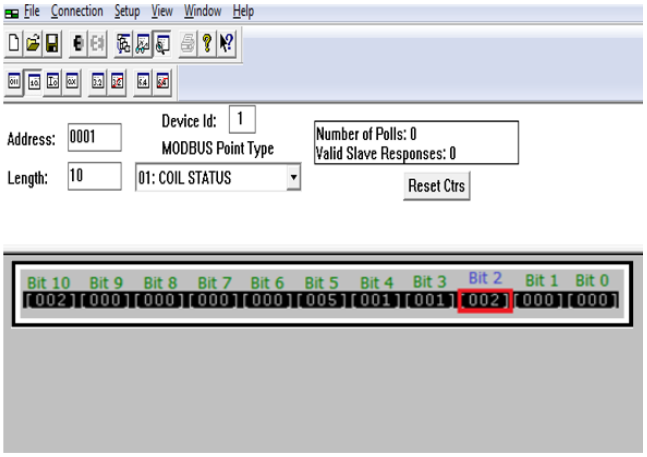

Fig.1. Interfaz de ModScan32

La función "Lenght" permite introducir un determinado valor (ejemplo, 10), el cual refleja la longitud de los datos que se generan en la trama. Este valor varía de uno en uno, según

la longitud del dato que se esté utilizando. Por ejemplo, si seleccionamos una longitud de 8, en el Byte 2 de la trama se verá reflejado el número 1, pero si por el contrario ingresamos un valor mayor a 8 y menor de 16, en el byte 2 se verá reflejado el número 2.

La opción "Address" (Dirección 0001), indica la conexión a un solo PLC y ese es el valor de la dirección del dispositivo. La función Device ID está relacionada con el número de esclavos conectados a la red, ya que solo se tiene un esclavo con valor 1 y está en el byte 4 de la trama. Para el monitoreo continuo de las entradas, bobinas y registros, es necesario seleccionar una de las opciones que ofrece la opción MODBUS Point Type.

Este estudio está encaminado al análisis de las tramas generadas en la comunicación maestro-esclavo, por lo cual cada una de las opciones permite visualizar una trama de datos, por ejemplo en el caso de seleccionar la opción 1 (COIL STATES), permite analizar los estados de las bobinas.

Hay parámetros importantes como Scan Rate, el cual fue configurado a un tiempo de 1 segundo, evitando que las secuencias en las tramas generen errores. Esto podría suceder en cualquier sistema sí la velocidad con que es muestreada una señal afecta directamente la adquisición y cantidad de datos.

A. Enlace del Autómata

Para el enlace con el autómata se realizó la comunicación vía Ethernet mediante el protocolo Modbus TCP Server. Esta opción permite realizar una comunicación con otro dispositivo mediante el protocolo Ethernet.

Inicialmente se ingresa la dirección IP del PLC y se selecciona el puerto de comunicación 502, el cual se usa como un puente de comunicación entre el PLC y la computadora. En este punto el software ModScan32 inicia la recolección de tramas en configuración de la red local.

Para crear una trama de datos en forma dinámica se realizó un programa a través de la aplicación TwidoSuite v2.30, donde debe ser sido transferido al PLC y permanecer en ejecución.

B. Generación de campo magnético

Para las pruebas de errores con campo magnético se utilizó un sistema generador de cambios magnéticos focalizados, el cual genera hasta un máximo de 1000 Gauss de intensidad de campo magnético (ver Fig.2) [11].

La prueba consistía en focalizar un campo magnético directo sobre un cable de comunicaciones en forma de solenoide, esto con el fin de generar algunos cambios de voltaje o corriente sobre el mismo.

Por otro lado se realizaron pruebas mediante la aplicación de diferentes bobinas conectadas a corriente alterna (AC). Estas pruebas se hicieron con el cable de datos en forma de solenoide y de manera rectilínea.

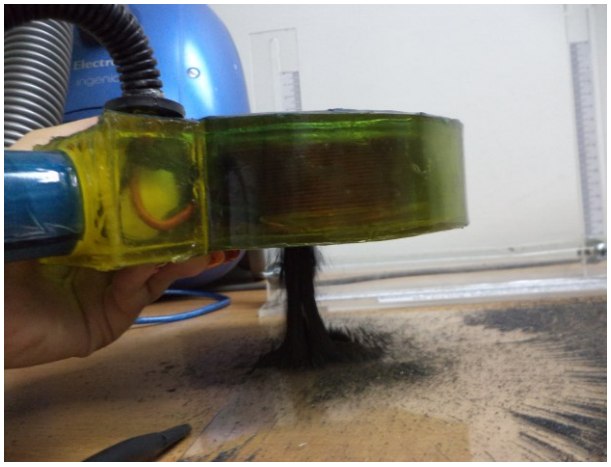

Fig.2. Generación de campos magnéticos focalizados

C. Desconexión del cable-conector (RJ45)

Tal y como se muestra en la Fig.3 en la siguiente prueba se obtuvo otro factor de error mediante la desconexión del cable RJ45 desde la configuración maestro-esclavo. Para este caso el resultado fue desplegado en la trama de datos, dando como resultado un error similar al anterior.

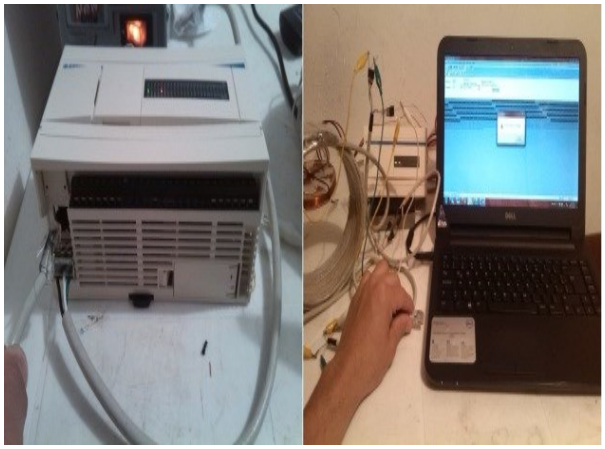

Fig. 3. Desconexión del cable en la terminal de la computadora y el PLC.

D. Corto circuito instantáneo en la línea de transmisión

Para este caso se acondiciona el cable con conector RJ45, con el fin de simular una situación que realice un corto circuito entre las líneas de transmisión de datos. Este evento se asume de forma instantánea, donde el corto no se mantiene, sino que las líneas de transmisión se cruzan entre sí y se sueltan inmediatamente (ver Fig.4).

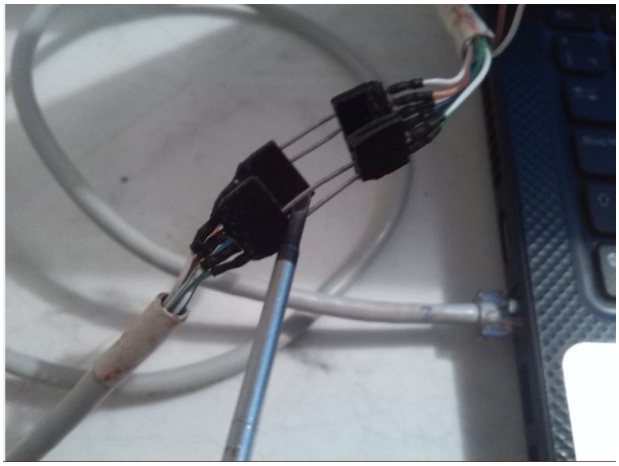

Figura 4. Prueba de corto circuito generado

D. Pruebas de ruptura en la línea de transmisión

En la Fig.5 se muestra el otro caso donde se realiza en forma manual y repentina una desconexión directa en uno de los cables, esto con el objetivo de determinar el efecto que causaría en la trama de datos. En total 4 líneas (2 para transmisión y 2 para recepción) fueron sometidas a la ruptura del cable.

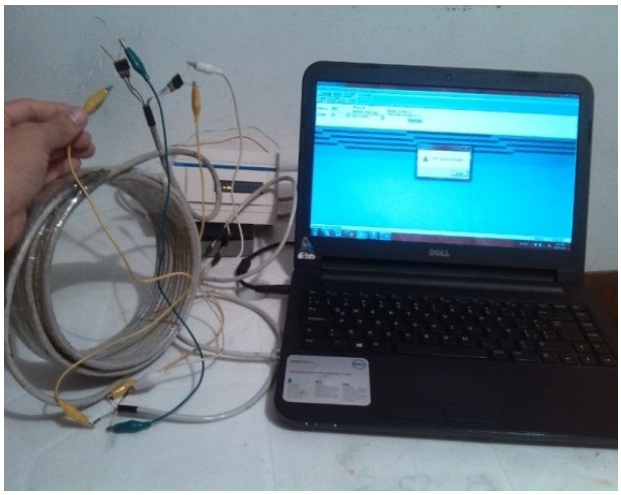

Fig.5. Simulación de una ruptura interna en la línea de transmisión.

E. Discriminación de errores mediante PCA (Análisis de Componentes Principales)

Con el objetivo de observar gráficamente la discriminación de los errores generados en una red Modbus a partir de las diferentes pruebas descritas previamente, en este estudio se aplicó un método de reconocimiento de patrones a la base de datos (tramas) obtenida. Para tal fin se aplicó PCA, el cual es un método no supervisado donde permite proyectar en un plano bidimensional un conjunto de datos con diferentes categorías (clusters), partiendo de la máxima variación de los mismos. Por lo tanto fue posible determinar cuál fue la causa del error en los datos transmitidos en la red Modbus.

F. Adquisición de datos

A través de una tabla con los datos obtenidos, se obtuvo una cantidad de conteos y secciones específicas de cada trama. Esto permitió crear una base de datos para analizar el comportamiento de la trama, la cual fue necesaria para obtener un modelo de la PCA. Se realizaron diferentes medidas por conteo (6 muestras), las cuales se obtuvieron resultados satisfactorios y se evidenció una mejor correlación de todos datos por cada uno de los errores.

III. ANÁLISIS DE RESULTADOS

En cada una de las pruebas realizadas se obtuvo una diferencia marcada en cada una de las tramas adquiridas, ya que los datos obtenidos a partir los errores pudieron ser analizados de forma individual para su posterior identificación o clasificación.

1) Efecto del Campo magnético

A través del sistema de generación de cambios magnéticos focalizados no se pudo obtener resultados satisfactorios debido a que el campo magnético aplicado no afectó la comunicación. Aunque la variación de voltaje fue notoria en el cable, esta prueba demostró la robustez en la comunicación vía Ethernet.

2) Desconexión del cable

Cuando ha ocurrido una desconexión eléctrica del cable de comunicación, en la trama se obtiene un nuevo byte, por lo que con este detalle se evidencia que hay un error en la comunicación y su característica principal es la cantidad de veces que aparece en las tramas próximas a la desconexión. Este número de veces equivalen a las preguntas hechas por el maestro al esclavo.

3) Ruptura del cable

Para cada una de las pruebas experimentales en base a simulación de una ruptura en el cable de transmisión, se tuvo en cuenta la ruptura de cada una de las 4 líneas del cable de datos que refleja la comunicación Ethernet, dando como resultado una secuencia de trama característica y específica para la transmisión y para la recepción de los datos.

En el momento de la trasmisión el maestro (PC) se queda preguntando 9 veces al esclavo (PLC) a partir del momento de la ruptura del cable, se logró evidenciar que el cable de transmisión compartía una misma característica en la trama cuando eran desconectados.

4) Clasificación de los eventos (errores)

Para la discriminación de las muestras fue necesario realizar seis combinaciones distintas para lograr que todos y

cada uno de los cables interactuaran de forma individual con los otros. Este proceso permitió evidenciar que cuando se realiza un corto circuito de forma instantánea entre las líneas de transmisión o entre las líneas de recepción del cable de datos, la conexión vía Ethernet se interrumpe inmediatamente dejando un rastro en la trama el cual puede ser usado para generar la base de datos. A través de la herramienta PCAGUI del software Matlab, se realizó la discriminación de cada uno de los errores generados de manera experimental (ver figura 6). En la Fig.6 se ilustra una buena clasificación de los cuatro eventos, permitiendo identificar los tipos de errores en la comunicación. Un 100 % en la varianza capturada y discriminación fue obtenido con los dos primeros PCs.

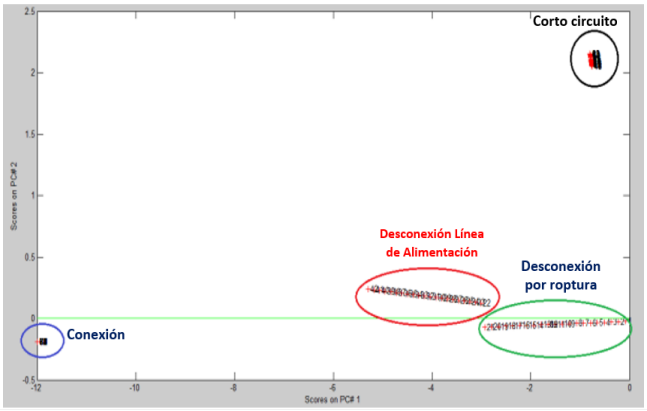

Fig. 6. Discriminación de errores en la comunicación Modbus TCP/IP a través de la herramienta PCA de Matlab 2010.

Con el desarrollo de este proyecto se aporta una herramienta que permite al operador de un proceso industrial, responder con mayor eficacia ante un posible fallo en la comunicación, detectándolos y analizándolos a través de la clasificación de errores, y así ejecutar procedimientos preventivos y/o correctivos que permitan al sistema trabajar en forma continua estableciendo parámetros se seguridad y eficiencia en la producción. Permitiendo una reducción de costos y tiempo de respuesta ante un fallo en comunicación.

IV. CONCLUSIONES

Durante este estudio fue de gran utilidad el software ModScan32, el cual es un analizador de tramas Modbus, generadas por la conexión de un PLC TWDLCAE40DRF (Esclavo) al ordenador (maestro).

Así mismo no se encontraron registros que permitan analizar cada uno de los segmentos que conforman la trama Ethernet a través de la conexión entre el Autómata y la computadora.

Las distintas pruebas llevadas a cabo confirmaron el efecto que se produce en la comunicación debido a los errores producidos en el sistema en general. Mediante el algoritmo PCA fue posible discriminar en forma gráfica los tipos de errores, los cuales fueron comparados individualmente partiendo de una conexión normal. Los errores generados por campos magnéticos no afectaron la comunicación, por lo que podemos decir que fueron corregidos automáticamente por los códigos de redundancia cíclica que maneja el protocolo Ethernet.

La trama Ethernet generada por el software evidencia un error en la comunicación, pero hasta el momento no se puede hacer uso de esta evidencia ya que sucede de formar esporádica y no hace que la comunicación se pierda de forma total, por lo que impide extraer sus datos de la interfaz de software ModScan32.

AGRADECIMIENTOS

The Research Group appreciate the financial support obtained for the project about the 50 years of the Pamplona University (Colombia).

REFERENCES

1] E. Knapp and J. Thomas, Chapter 6, *Industrial Network Protocols Industrial*, Network Security (Second Edition), 2015, pp. 121-169.
2] S. Radek and S. Karel, "The Common Industrial Protocol in Machine Safety", *Procedia Engineering*, vol. 100, 2015, pp. 773-781.
3] P. Santos, F.Villa, A. Reñones, A. Bustillo and J. Maudes, "An SVM-Based Solution for Fault Detection in Wind Turbines", *Sensors 2015*, 15(3), pp. 5627-5648.
4] J. Park, S. Mackay, E. Wright, "Industrial protocols", *Practical Data Communications for Instrumentation and Control*, 2003, pp. 205-238.
5] L. Hui, Z. Hao, P. Daogang, "Design and Application of Communication Gateway of EPA and MODBUS on Electric Power System", *Energy Procedia*, vol. 17, Part A, 2012, pp. 286-292.
6] Q. Liu, Y. Li, "Modbus/TCP based Network Control System for Water Process in the Firepower Plant", *Intelligent Control and Automation*, 2006. WCICA 2006, the Sixth World Congress on, vol. 1, 2006, pp. 432 – 435.
7] N. Goldenberg, A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems", *International Journal of Critical Infrastructure Protection*, vol. 6, Issue 2, June 2013, pp. 63-75.
8] Schneider Electric Colombia S.A, TWDLCAE40DRF compact PLC base Twido, http://www.schneider-electric.com/products/, consulta: 10 de marzo de 2015.
9] L. Bergh, S. Acosta, "On-Line Fault Detection on a Pilot Flotation Column Using Linear PCA Models", *Computer Aided Chemical Engineering*, vol. 27, 2009, pp. 1437-1442.
10] P. Ralston, G. DePuy, J. Graham, "Graphical enhancement to support PCA-based process monitoring and fault diagnosis", *ISA Transactions*, vol. 43, Issue 4, October 2004, Pages 639-653.
11] A. Jaimes, L. Mendoza, "Desarrollo de un sistema generador de campos magnéticos focalizados, *Tesis de maestría en Controles Industriales*, Universidad de Pamplona, 2014, pp. 2014; 1-123.