Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 3, March 2019, pg.181 – 192

EVALUATION OF ETHERNET SERIAL PROTOCOL CONVERTER FOR SCADA SYSTEMS USING RASPBERRY PI

Hamzah Hamed Jasim[1]; Osman Nuri Ucan[2]; Oguz Bayat[3]; Ali Hasan Dakheel[4]
hamzacomputer93@gmail.com, osman.ucan@altinbas.edu.tr

***ABSTRACT:** With recent developments in SCADA systems, Raspberry pi and TCP protocols, there is great potential for the conversion of Ethernet Serial Protocol for SCADA systems using Raspberry Pi. The converter intermediately acts as the SCADA server and communicate with the remote terminal units and buffer all the data locally available, so that, the data requested by the SCADA is delivered immediately. In this approach, the Raspberry Pi acts as an interpreter, where the messages exchanged between the SCADA and the RTU are only converted from one protocol to another. The approach with the highest update rate, from the SCADA's point of view, is going to be selected for the propose method. Raspberry Pi is a small single-board computer that has a variety of interfaces to connect it to the environment it is working it. Ethernet and SPI interfaces present in this device, and has been used to implement different applications using different communication mediums. In this study, the Raspberry Pi is going to be used to implement a protocol converter that allows older SCADA system to communicate with the RTUs, without the installation of expensive hardware and software expansions. Using SCADA systems, unauthorized access to valves and switches could be more tightly controlled while keeping a human in the loop; that is, human supervision and interaction were, and still are, part of SCADA systems. However, technological advances and the maturation of Raspberry Pi has pushed more of the supervisory function onto the computer systems that make up modern SCADA systems.*

***Keywords:** SCADA system, converter, remote terminal, serial protocol, human machine interface*

INTRODUCTION

In this study, a proposed technological advances and the maturation of Raspberry Pi has pushed more of the supervisory function onto the computer systems that make up modern SCADA systems. In the early development of SCADA systems attention was given to physical security, but virtually no attention was given to electronic or Ethernet serial protocol security. The systems were obscure and the skills and technology needed to interact with the systems were simply not readily available; security of this type is often referred to as "security through obscurity". This pattern has continued and today "most dedicated SCADA and PCS applications have not included built-in security" [1]. Unfortunately, open protocols, advanced telecommunication networks, cheap computer electronics, and unlimited access to even the most obscure information through the World Wide Web have made SCADA's

security through obscurity obsolete. The move of SCADA systems to open standards and new technology has allowed SCADA system managers to realize cost savings by using commercial- off-the-shelf (Raspberry Pi) hardware and software. In addition, as computer networks and information systems have become more commonplace throughout the corporate enterprise, managers have seen the economic benefits of having access to Raspberry Pi data and have built network connections into the previously isolated SCADA networks [2]. The connection of porous and less secure corporate networks to once isolated SCADA networks, now using Ethernet-serial protocol systems, has unintentionally exposed SCADA systems to a host of vulnerabilities and threats for which it was ill prepared. SCADA protocols provide no authentication or authorization capabilities. When other networks are connected to the SCADA network, intentionally or unintentionally, a converter who manages to gain access to the Ethernet-serial protocol network can spoof control signals on the SCADA network. Because SCADA protocols do not provide authentication or authorization a SCADA system is unable to distinguish between a real and a spoofed control signal, allowing the converter to control SCADA devices. Remote locations may have a communications network [2], like a LAN, which can be used for local inter-device communication, but this is usually not considered to be part of the SCADA communications network. Communication links take many forms including leased lines, Public Switched Telephone Networks (PSTNs), Internet Protocol (IP) based landlines, radio, microwave and even satellite. SCADA communications security has traditionally referred to error detection and error correction capabilities, and not to features such as authentication and encryption.

The converter and communication protocols developed by different vendors were lean, supporting only the minimal functionality needed to achieve scanning and control of points within a remote device [2]. The transmission medium used to connect RTUs and MTUs lacked a high degree of fidelity, leading to communication security focused exclusively on error detection and error correction codes. In addition, each vendor tended to view their protocols as proprietary, preventing other vendors from developing equipment that could communicate using these protocols. Open standards have removed the limitations that proprietary protocols placed on SCADA systems and therefore make it much easier to use COTS (commercial-off-the-shelf) components to build SCADA systems. One consequence of this move has been the use of WAN protocols like TCP/IP for communication between SCADA components like master stations, RTUs, field communication equipment, and HMIs [5]. A typical generation SCADA architecture [4]. Some advantages of internet based SCADA systems are discussed; the primary advantage cited is lower costs. The eight-bit function code specifies what operation is to be performed by the RTU. The bits following the function code are an addressing scheme that indicates the set point, control point, or data on which the operation is to be carried out. This address has no special meaning to the RTU, and it is up to the MTU and SCADA software to correctly associate an RTU address with the real world value it represents.

RELATED WORK

The research efforts converting the Ethernet serial protocol have been in rush since the great intervene by the SACAD system in this particular domain. The developed and implemented functionalities for Industrial Shields PLCs in this work are highly demanded in industrial automation, supervision and control systems. Finally, the work developed should serve as a proof of concept and reference showing that developing a SCADA system using low-cost alternative hardware, based on open-source, is nowadays a feasible alternative to traditional and closed-standard automation solutions and conversion of Ethernet serial protocol conversion using SCADA systems and raspberry pi. The results and conclusions of the study will serve to provide some ready-to-use solutions to Industrial Shields customers and thus, upgrade the value-for-money of the products. The ultimate application of this study is to provide a prototype of a SCADA system based on Industrial Shields PLCs [6]. The SCADA systems of this era reflect this paradigm. They were special purpose

standalone systems that were not intended to be connected to other systems and tended to be very hierarchical and centralized in nature. A standard first generation SCADA architecture. The master station in these SCADA systems was typically a single mainframe computer [6]. A second redundant master station was usually present and shared the communications bus with the active master station. In the event of a system failure the second system could take over. Following are the main points that this study will cover. Implementation of Modbus RTU protocol over master and slave mode for conversion of Ethernet serial protocol. Development of a Human Machine Interface (HMI) for supervision and control purposes. Implementation of TCP protocol over Ethernet and Local Area Network (LAN) for interaction between the control unit and the HMI. Practical integration of sensors, data acquisition equipment and actuators with a raspberry pi. The SCADA system prototype is focused on a real - case project, which is a better for conversion of Ethernet serial protocol where an upgrading of the current supervisory and control system is wanted.

METHODOLOGY

In this section, we describe the preprocessing steps we used in our conversion of Ethernet serial protocol for SCADA system using the functional raspberry pi, as well as approaches to address the problem. Some of the preprocessing steps follow the tutorial provided on the competition website and use some of the provided code. These indicate the operation to be carried out (read or write), the point type (analog input, analog output, digital input, digital output), and the point index (beginning at index 0) respectively. These fields are sufficient for the middleware layer to translate the request into an appropriate protocol. Upon receipt of a request the Ethernet-serial Security Middleware first consults the protocol access control policy to determine whether the operation is allowed or not by calling the check access function, based on the algorithm.

These processes perform operation on the data for smarter decisions [7]. These System of communication problems to solve the mitigate down-time. Simple Supervisory control and data acquisition structure instigates through program logical controller/remotes terminals units (RTUs). PLC and remotes terminals units are microcomputers which talk through array of the gadget including HMI, machines of the factory, Sensor and more give up gadgets, course of records to the ones of the object the computer systems with help of Supervisory control and data acquisition software [6-7]. Deregulation in the power industry has created vulnerabilities for electric power generation, transmission, and distribution Raspberry pi. As a result of deregulation, data exchanges between single vertically integrated organizations have been replaced by many horizontal relationships among independent entities. Some of the vulnerabilities that result from deregulation are described. The complex interaction among entities not only increases the network connectivity of raspberry pi but can require multiple master and multiple remote architectures with many different entities needed varying degrees of access. SCADA systems have different performance requirements than do traditional IT systems [8]. Though not all SCADA systems and process control systems have hard real time requirements, it is important that the SCADA system (in this case the RTU) have reasonably short response times. Since different systems have different requirements, there is no established targeted response time. Each layer includes some form of examination, detection, and prevention. According to this model, the storage are segmented and compartmentalized based on functional groups and access control plans. Access control matrices are developed that provide a detailed security policy, which is then implemented using security products for examination, detection, prevention, and encryption at the various layers.

This paper describes the development and testing of a prototype hardened RTU for the conversion of Ethernet serial protocol for SCADA systems. The prototype implements the developed RTU role based access control model as a middleware layer available to other RTU processes, and uses a reduced Ethernet-serial protocol kernel [9]. A security enhanced DNP protocol similar to that described by Patel was included to provide SCADA access to the prototype [9]. RTUs and other industrial controllers

usually have less available memory and processing power than traditional computing systems and have different performance requirements as well. The prototype was developed on actual RTU hardware from six-net and evaluated in a test bed environment including actual SCADA hardware. Both performance analysis and security testing were conducted in the prototype evaluation.

Several approaches are highlighted, such as TLS wrapping, the use of digital certificates, and the use of challenge response with a pre-shared secret. The DNP3 protocol is extended to include the necessary authentication objects so that RTUs or MTUs can use the proposed protocol to verify sender authenticity and detect modifications to messages. A threat analysis and formal proof techniques support security claims about the communication protocol. The focus of the protocol is on integrity of message and sender authenticity and is not concerned with confidentiality.

The security enhancements were applied to the DNP3 protocol. A more detailed description of the DNP3 protocol is described in appendix B, and Patel's enhancements are fully explained in [9]. This section provides a brief description of the modifications related to the prototype implementation [11]. The scheme as described by Patel is based on a single key and lacks the notion of a user. For the hardened RTU prototype implementation the scheme was extended to include the notion of a user. This was done by adding a user field to challenge-response messages, identifying the user providing the response. Moreover, there are some features that are not expressed in a numerical manner, such as the IP addresses of the IP's associated country. In these cases, these features are mapped to numerical values, which can be reversed to text.

$$yi = \frac{yi - min(x)}{max(x) - min(x)}, yi \in [0,1]$$

There is also a summation for all the times that a conversion flag is sent which this mathematical function states [12], and in the end of the processing, this value is divided by the total number of packets for that key, resulting in the feature Conversion-Rate, and the same applies to Non-Conversion-Rate, where the total number of times the Internet Control Message Protocol (ICMP) protocol is used is divided by the total number of packets.

Like in many kind of conversion techniques, for a novice user is most often a human being, but the notion of user can be extended to other entities like devices, networks or autonomous agents. Roles attempt to approximate different job functions within the organizational construct in which the system is participating. A permission is the right to carry out an operation on one or more objects. An operation is some type of function to be carried out by the system for a user. Objects are entities that contain or receive information; their exact type depends on the system. A device using Modbus/TCP typically lacks packet filtering capabilities and therefore will carry out any legitimate command that reaches it [13-14]. A common network security solution would be to filter the Modbus/TCP port as it passes through a firewall or router, enforcing an access control policy for device connection. However, this only allows access control at a source level, while some organizations' security policy may dictate that some hosts have read access to data, while other hosts have both read and write access to the device. Botnets are used to carryout coordinated conversions, send spam, or carryout phishing schemes. Botnets make use of automated conversion software [15]. Botnets present two threat vectors, one they can be used to carry-out a conversion on SCADA systems, or two, SCADA systems may become part of a botnet and have their resources depleted by the botnet activities. Seek to acquire trade secrets, or inside knowledge that can give one organization advantage over another. SCADA systems in manufacturing industries will have knowledge of trade secrets, or just private status data. Corruption of a competitor's SCADA system at the appropriate time could have financial benefits for the competitor. Terrorist seek to destroy or incapacitate critical infrastructure in order to damage public moral [14]. Ethernet serial protocol-

conversions on SCADA systems are one way to achieve this and may be possible from a point of relative obscurity. Ethernet serial protocol-conversions on SCADA systems may also be used to leverage a physical conversion given by in (Figure: 1) down below:

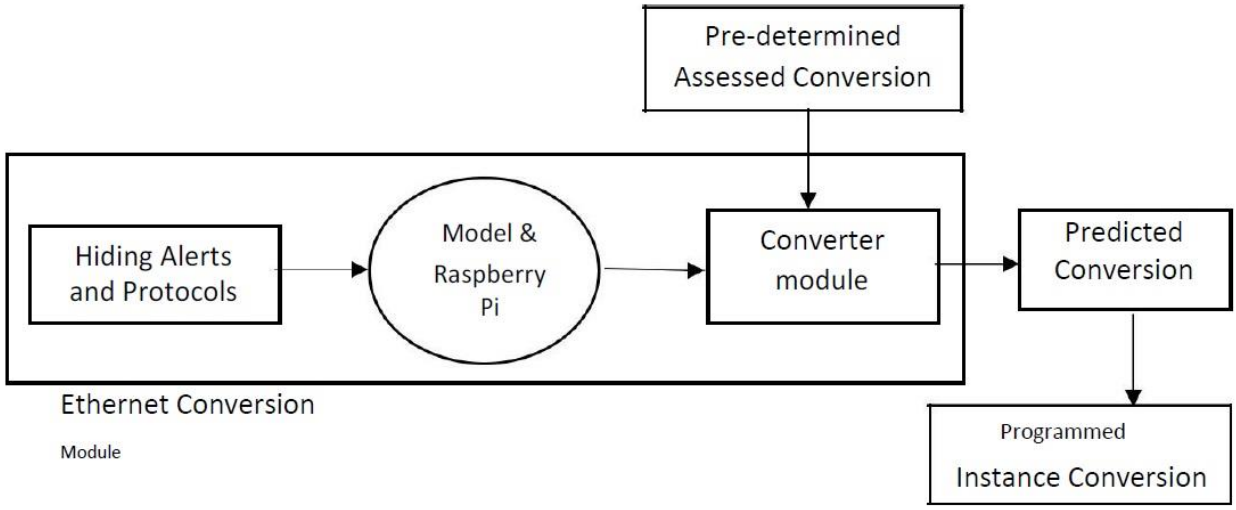

Figure 1: *Describes the overall process of converting the Ethernet serial Protocol through pre-determined assessed conversion for predicting the programmed conversion using raspberry pi and models.*

Hiding alerts of a malicious physical conversion [17]. A converter is a program that can replicate itself and pass on malicious code to other non-malicious programs. Converter can corrupt files and disrupt or interfere with the normal operation of a computer system. Worms are automated programs that propagate themselves though networks by exploiting a common vulnerably. Worms can exhaust network and computer resources, as well as harm files on the victims. Disgruntled insiders have been main source of computer crime since they have knowledge of and access to internal systems. Insiders include employees, business partners and vendors. Insiders may not necessarily be malicious, but accidental mistakes can have the same consequences as malicious conversions.

In the previous approach, we followed a simple heuristic to remove the converted protocol but most SCADA systems are privately owned and operated, and operators are driven by economic forces. For these reasons the economic advantages offered by open standards and open architectures has strongly motivate the adoption and integration in SCADA. In addition to assumption the SCADA networks were isolated, was a widely held belief that it was difficult to acquire information about SCADA system. Open standards and open application layer interfaces that make use of available commodity software, such as a web interface. These additional application layer interfaces in to device introduce additional vulnerabilities and conversion vectors into SCADA systems [18]. This lack of computing resources along with performance constraints can make it difficult or impossible to apply standard security technologies. One of the real challenges presented by fiber optic network is the relatively long life of SCADA components compared to their IT counter parts. The policy they develop is broken down into eight main categories at level one, ranging from data security and personnel security to network security and physical access and converted by given converter in (Figure 2) which provides the internal view of converter architecture.

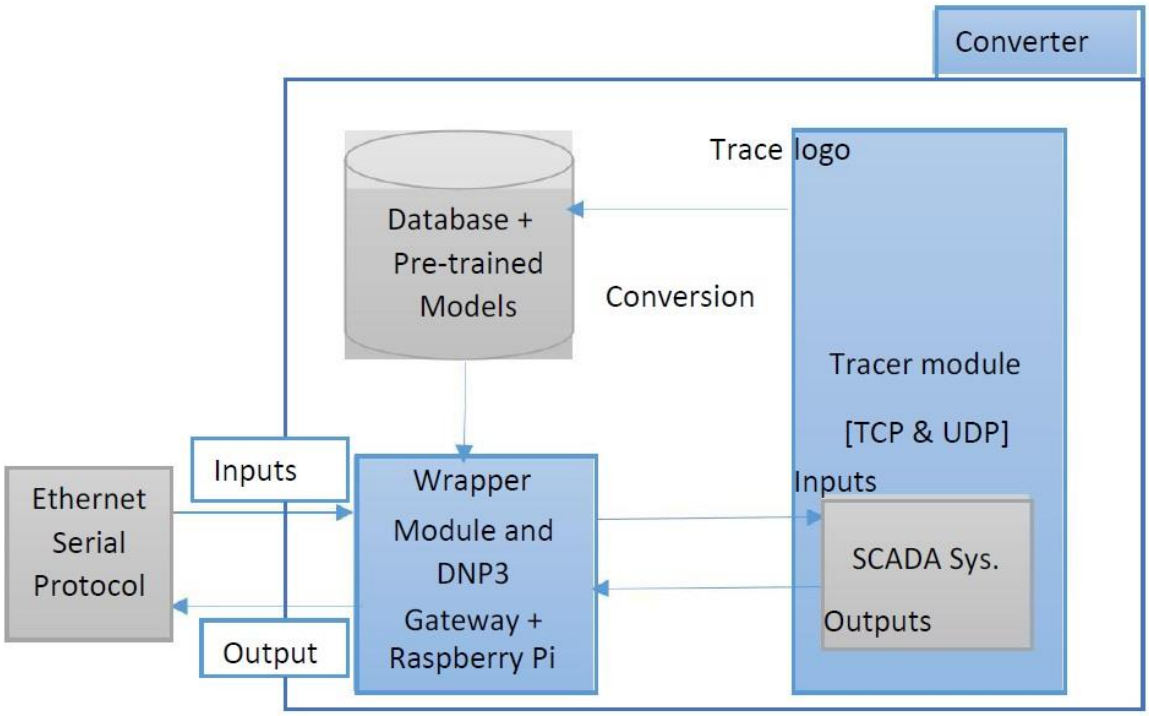

Figure 2: *Ethernet assessments and secure communication system development and implementation for the converter using the tracer module for both TCP/UDP conversion in wrapper module with DNP3 gateway communication for the conversion of Ethernet Serial Protocol.*

Open standards have removed the limitations that proprietary protocols placed on SCADA systems and therefore make it much easier to use Ethernet-serial protocols to build SCADA systems [46]. A secure protocol that addresses message integrity and sender authentication is presented by Patel. Several approaches are highlighted, such as TLS wrapping, the use of digital certificates, and the use of challenge response with a pre-shared secret. The DNP3 protocol is extended to include the necessary authentication objects so that RTUs or MTUs can use the proposed protocol to verify sender authenticity and detect modifications to messages. A threat analysis and formal proof techniques support security claims about the communication protocol [20]. The focus of the protocol is on integrity of message and sender authenticity and is not concerned with confidentiality.

The approach, we tried is similar to the pre-determined approaches with a machine learning, except that the conversion method to reduce non-conversion rate of serial protocol and target of these principles is to ensure that due diligence has been followed in securing an organizations control systems. Cost is based on three features: committed information rates, access circuit and port speed. This vulnerable device has the highest vulnerability level. Additional research is needed in determining the initial assignment of vulnerability levels.

IMPLEMENTATION

The SCADA architecture is generally broken down into a master station or MTU used by human operators to monitor and control remote terminal units, or RTUs. A communications network provides communication channels between MTUs and RTUs. Security hardening techniques are needed for the various components as well as for the SCADA system as a whole. RTUs interact with physical devices like valves and switches. A primary SCADA security objective is to prevent unauthorized or improper operation of valves, switches, or other physical devices, since these devices could have economic consequences for a SCADA operator as well as potentially disrupting normal operation of U.S. critical infrastructures [18]. The fact that RTUs can, and often are, physically remote makes securing them that much more important. This dissertation describes research and development of a security hardened RTU. While protecting and securing existing systems is important, the aim of this dissertation is to explore the development of next generation RTUs. As existing RTUs are replaced in existing SCADA deployments and as new SCADA systems are deployed, it is important that these RTUs be security hardened against Ethernet serial protocol based conversions. This dissertation presents an RTU role based access control model for hardening RTUs. The model is developed to prevent unauthorized alteration of analog and digital 10 points. In addition, a middleware layer deployment architecture is advocated to allow fine grained and homogenous application of an RTU access control policy. Operating system support for a middleware layer deployment is a critical factor in the assurance of the security hardened RTU. Two approaches for reduced kernel RTUs are presented. A reduced commercial-off-the-shelf kernel is one approach, and is used in the development of a prototype for testing using raspberry pi.

Data Unit	**Layer**	**Protocols**	**Address**
Message	Application	FTP, DHCP, TFTP, DNS, SMTP, HTTP	Application(i.e. email address)
Segment	Transport	TCP,UDP	Port (Port number)
Datagram	Network	IP,ICMP,IGMP,ARP	Logical(IP)
Frame	Data	Ethernet, Wireless	Physical or link (MAC)
Bits	Physical	Ethernet, Wireless	Conversion

Table 1: *TCP/IP protocol suite summary chart for conversion of Ethernet through different layers of Network.*

Supervisory control and data acquisition (SCADA) and some protocols are built in the current version of CORE emulator. SCADA specific communication protocols are not included in CORE emulator and TCP/IP protocols suite used in (Table: 1) for the conversion of Ethernet serial protocol through different layer. A mechanism to integrate Modbus in CORE emulator. They integrated Modbus as service in the emulator. Since in SCADA system there might be large number of RTUs or PLCs with different functionalities it is not feasible to include all such component as service in CORE emulator. In our proposed approach, we developed a python script for each of the components of the SCADA system based on their functionalities. In such scenarios the normal operation of the SCADA system will be disrupted. The bandwidth consumed on the link between the RTU and MTU for converting the Ethernet serial during execution. The experiment was made for 120 s. In this period on the converter machine we made ESPC three times on the RTU. The first conversion was attempted between 20 to 30 s and the second and the third were from 55 to 65 and 90 to 100s respectively. In those periods the conversion easily consumed the bandwidth of the link between the RTU and MTU [12-14]. We demonstrated how conversion could disrupt the normal operation of SCADA systems. With the

current version of the SCADA systems, we have already collected network and control data for SCADA security research and development [19]. The collected dataset will be freely available for security researchers in a near future. From results, we can conclude that the developed test-bed can be effectively used for Ethernet serial protocol security assessment and vulnerability investigation on SCADA systems, which can be easily extended to various critical infrastructure sectors. More importantly, different from previously developed ESCP, the proposed SCADA ESCP is user friendly and easily reconfigurable for different types of conversions. In addition to this, in this ESCP multiple conversions can be simultaneously initiated from different places in the ESCP. This feature of the ESCP helps security researches to investigate the effect of simultaneous conversions on SCADA Systems.

The conversion can be used for security assessment and vulnerability investigation on SCADA systems. With our client, one can also generate benchmark dataset to develop and evaluate conversion and protection technologies for SCADA systems. With the current version of the ESCP, we have already collected network and control data for SCADA security research and development. Though the ESCP is primarily developed for SCADA security research, it can also be used for educational purpose. Occasionally intrude on correspondence between two sequential gadgets associated with the ESPC. Under typical conditions, there is a bidirectional correspondence between gadgets on the 3 ESPC sequential ports. On the off chance that the ESPC recognizes a Transmission Control Protocol attachment ask for, it supersedes the sequential to-sequential interchanges. While the Transmission Control Protocol attachment is built up, any information from the other sequential gadget is disposed of. Two standard of Serial Master – User Datagram Protocol communicate and Remote Terminal units address based steering for conversion of Ethernet serial protocol in SCADA systems.

In User datagram protocol, sequential message is communicated to a rundown of User Datagram Protocol slaves. The User Datagram Protocol communicate mode is convention free. This mode can be utilized for ESPC Serial Master Mode Configured for User Datagram Protocol Broadcast. The distribution of system functionality across multiple machines increased the overall processing capability of the system, but LAN technology was only capable of handling relatively short distances, typically hundreds of feet, this meant that the systems still had to be housed within a single room. Off-the-shelf LAN protocols were available, but some vendors still choose to use propriety protocols [19]. Communication links with RTUs were largely unchanged relative to first generation systems, and in general vendors maintained control over what hardware, software, and devices were available for a specific SCADA system.

RESULTS

The results obtained at each intermediate step of the converting procedure is indicated. It can be seen that after certain no. of conversion iterations summarizes important design and process principles for securing control systems [20]. The goal of following these principles is to ensure that due diligence has been followed in securing an organizations control systems. Cost is based on three features: committed information rates, access circuit and port speed. This vulnerable device has the highest vulnerability level. Additional research is needed in determining the initial assignment of vulnerability levels. SCADA installations were characterized by closed systems and proprietary protocol standards. Most SCADA systems are privately owned and operated, and operators are driven by economic forces. For these reasons the economic advantages offered by open standards and open architectures has strongly motivate the adoption and integration in SCADA. In addition to assumption the SCADA networks were isolated, was a widely held belief that it was difficult to acquire information about SCADA system. Open standards and open application layer interfaces that make use of available commodity software, such as a web interface. These additional application layer interfaces in to device introduce additional vulnerabilities and conversion vectors into SCADA systems.

Converted Ethernet Serial Protocol (Ethernet).
Converted Ethernet Serial Protocol: 10993452383473434624
MAC1: 0d: a7: a0: 00: 08: 00
MAC2: 45:00:00:3c:b5:4a
Ether-Type: 0
Version: 3
IHL: 8
TOS: 6
TOTAL LENGTH: 22301
IDENTIFICATION: 44249
FLAGS: 00
FRAGMENT OFFSET: 7652
TTL: 172
PROTOCOL: 16
CHECKSUM: 65414
IP SOURCE: 0.80.198.148
IP DESTINATION: 136.3.144.16
Conversion of User Datagram Protocol for Ethernet Protocol
Source Port of UDP for Ethernet Serial Protocol: 44381
Destination Port of UDP for Ethernet Serial Protocol: 57474
Length: 40978
Checksum: 42408
5.2 Version: 4 (ESPC)
Version 4 (ESPC) conversion results for the Ethernet serial protocol typed with SCADA system using raspberry pi and packages available.
ETHERNET
MAC1: 98:90:96:b2:6c:1b
MAC2: 00: 27: 0d: a7: a0: 00
Ether-Type: 2048
5.2.2 IP
Version: 4
IHL: 5
TOS: 0
TOTAL LENGTH: 60
IDENTIFICATION: 46410
FLAGS: 00
FRAGMENT OFFSET: 0
TTL: 56
PROTOCOL: TCP
CHECKSUM: 22301
IP SOURCE: 172.217.29.228
IP DESTINATION: 172.16.255.134
Evaluation of Ethernet Protocol
Source Port of Ethernet Serial Protocol: 80
Destination Port of Ethernet Serial Protocol: 50836
Sequence Number: 2281934864
Acknowledgement Number: 2908610690
Header Length: 10
Reserved: 0
Bits: 010010

Window Size: 42408
Checksum: 23727
Urgent Pointer: 0.

The conversion was done by tracer module after getting an input from the wrapper module which ultimately passed that output result to the remote terminal unit address based routing utilizes a Remote Terminal Units deliver query to course to an internet protocol gadget. In the model underneath, door A courses the standard utilizing the query format. Ethernet Serial Protocol Converter Configured for remote terminal units Address Standard Based Routing. In User datagram protocol, sequential message is communicated to a rundown of User Datagram Protocol slaves. The User Datagram Protocol communicate mode is convention free. This mode can be utilized for ESPC Serial Master Mode Configured for User Datagram Protocol Broadcast for the conversion of Ethernet Serial Protocol for SCADA system.

DISCUSSION

In this paper, we describe the methods, implementation steps, and results of our project on the developed solution for the reference conversion implies an upgrading of the management and maintenance system [20], which in turn derives to savings of resources and time, and thus diminishes the effect on the environment. For instance, avoiding regular personnel check-ups to the network as a consequence of remote availability of information of the system status through the developed SCADA system. On a different note, another environmental advantage in this work ensues from using conversion for Ethernet serial protocol in open-source [21]. The flexibility and adaptability that these devices offer result, in many cases, in a reduction of reinvestment in new equipment as a consequence of close-standard incompatibilities or outdated versions between existing installations when carrying out extensions of it or retrofitting tasks.

The development of this work is of particular interest to conversion of Ethernet serial protocol in a firm and, more generally, to the industrial and automation sector [21]. This new technologies will broaden the range of solutions for automation systems and boost the interaction capabilities between devices and systems of different nature or firms. The present project is encased within that framework and it will provide an example on how a SCADA system can be developed based on open technology, integrating devices from different firms, which communicate with each other via different open protocols. The election of Modbus RTU and TCP-IP protocols as part of the development of this project lies on the reasons. Modbus RTU, and Modbus more generally, area widely extended protocols in the industry nowadays. Therefore, it is a feature demanded in the automation sector. TCP-IP is the standard protocol of the Internet and, for all the exposed reasons in this section, the devices supporting it bear a greater potential.

CONCLUSION

We have presented a work for the conversion of Ethernet serial protocol for SCADA system using the raspberry Pi, the ultimate goal of the study was to develop and implement conversion of Ethernet serial protocol and communication protocols with SCADA systems using Raspberry Pi. It can be assert that this objective has been wholly fulfilled. It has been shown how to establish a TCP-IP communication between client and a server and define the functions and structures for exchanging data. Furthermore, Modbus RTU protocol over serial bus has been adapted and implemented to a conversion of Ethernet serial protocol in order to interface with a data acquisition device from another firm. These two developed protocols are widely extended in the industry nowadays, and TCP-IP has still a vast potential of expansion, as the standard protocol for Internet. The integration of these two communications with Industrial Shields products has already had a positive effects for customers, which have been implementing it from

the beginning see Raspberry Pi. Real case examples. Moreover, the integration of this communication protocols has boost interest on the devices. Another of the goals of this work was to develop a SCADA system integrating conversion of Ethernet serial protocol along with other systems. This point has been achieved indeed, as a SCADA system itself has been developed and tested. The communications between the Raspberry Pi and the interactive HMI comprising the required variables and parameters to meet the specifications set has been shown to work. Moreover, this has already been a topic of interest among potential customers. Several of them contact us in about communication between converter for Ethernet serial protocol and other part of it, part of the work developed in this study serves as response, example and model for their applications. Developments of this study are useful realizations. Finally, taking into the fact that conversion of Ethernet serial protocol are based on open-source, it can be concluded as well that this study serves as a proof of concept of a SCADA system developed with alternative open hardware and software solutions to traditional existing closed systems.

REFERENCES

[1]. Marcuse, J, Menz, B., Payne, J.R., Servers in SCADA applications, Industry Applications, IEEE Transactions on, Volume: 33, Issue: 5, Sept.-Oct. 1997 Pages: 1295 – 1299.

[2]. Luque, J., Gomez, I., The role of medium access control protocols in SCADA systems, Power Delivery, IEEE Transactions on , Volume: 11 , Issue: 3 , July 1996 Pages:1195 – 1200.

[3]. Luque, J., Gomez, I., Escudero, J.I., Determining the channel capacity in SCADA systems using polling protocols, Power Systems, IEEE Transactions on , Volume: 11, Issue: 2 , May 1996 Pages:917 – 922.

[4]. Sciacca, S.C., Block, W.R., Advanced SCADA concepts, Computer Applications in Power, IEEE Volume: 8, Issue: 1, Jan. 1995 Pages: 23 – 28.

[5]. Dagle, J.E., Widergren, S.E., Johnson, J.M., Enhancing the security of supervisory control and data acquisition (SCADA) systems: the lifeblood of modern energy infrastructures, Power Engineering Society Winter Meeting, 2002. IEEE, Volume: 1, 27- 31 Jan. 2002 Pages: 635 vol.1.

[6]. Qian Wang, Qingquan Qian, Design and analysis of communication network for distributed SCADA system, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2062 - 2065 vol.3.

[7]. Wu Sitao, Qian Qingquan, Using device driver software in SCADA systems, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2046 - 2049 vol.3.

[8]. Chen Qizhi, Qian Qinquan, The research of UNIX platform for SCADA, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 2041 - 2045 vol.3.

[9]. Ebata, Y., Hayashi, H., Hasegawa, Y., Komatsu, S., Suzuki, K., Development of the Intranet-based SCADA (supervisory control and data acquisition system) for power system, Power Engineering Society Winter Meeting, 2000. IEEE, Volume: 3, 23-27 Jan. 2000 Pages: 1656 - 1661 vol.3.

[10]. Chen Qizhi, Optimization of a SCADA system based on client/server mode, Power System Technology, 1998. Proceedings. POWERCON '98. 1998 International Conference on, Volume: 2, 18-21 Aug. 1998 Pages: 1237 - 1240 vol.2.

[11]. Medida, S., Sreekumar, N., Prasad, K.V., SCADA-EMS on the Internet, Energy Management and Power Delivery, 1998. Proceedings of EMPD '98. 1998 International Conference on, Volume: 2, 3-5 March 1998 Pages: 656 - 660 vol.2.

[12]. Zecevic, G., Web based interface to SCADA system, Power System Technology, 1998. Proceedings. POWERCON '98. 1998 International Conference on, Volume: 2, 18-21 Aug. 1998 Pages: 1218 - 1221 vol.2.

[13]. Marcuse, J., Menz, B., Payne, J., Servers in SCADA applications, Industry Applications Conference, 1995. Thirtieth IAS Annual Meeting, IAS '95, Conference Record of the 1995 IEEE, Volume: 3, 8-12 Oct. 1995 Pages: 2124 - 2129 vol.3.

[14]. Bruce, A.G., Lee, R., A framework for the specification of SCADA data links, Power Industry Computer Application Conference, 1993. Conference Proceedings, 4-7 May 1993 Pages: 117 – 121.

[15]. McDonald, J.D., Developing and defining basic SCADA system concepts, Rural Electric Power Conference, 1993. Papers Presented at the 37th Annual Conference, 25-27 April 1993 Pages: B3/1 - B3/5.

[16]. Quartey, B., Shaw, D., Waked, P., An application of PLC's as an RTU in SCADA systems, Petroleum and Chemical Industry Conference, 1992, Record of Conference Papers., Industry

Applications Society 39th Annual , 28-30 Sept. 1992 Pages:271 – 274.

[17]. Hoge, D.J., Jensen, J.R., A comparison of protocol conversion methods for the retrofit of SCADA systems, Petroleum and Chemical Industry Conference, 1988, Record of Conference Papers., Industrial Applications Society 35th Annual , 12-14 Sept. 1988 Pages:245 – 248.

[18]. IEEE recommended practice for master/remote supervisory control and data acquisition (SCADA) communications, IEEE Std. 999-1992, 12 Feb. 1993.

[19]. Blackman, J.M., Hissey, T.W., Impact of local and wide area networks on SCADA and SCADA/EMS systems, Advanced SCADA and Energy Management Systems, IEE Colloquium on , 6 Dec 1990 Pages:8/1 – 815.

[20]. Kwok-Hong Mak, Holland, B.L., Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking, Power Engineering Journal, Volume: 16, Issue: 6, Dec. 2002 Pages: 305 – 311.

[21]. Su, C.-L., Lu, C.-N., Lin, M.-C., Migration path study of a distribution SCADA system, Generation, Transmission and Distribution, IEE Proceedings- , Volume: 146 , Issue: 3, May 1999 Pages:313 - 317

