DOI 10.29042/2019-5122-5127

Helix Vol. 9 (4): 5122- 5127

Vulnerability Analysis and Enhancement of Security of Communication Protocol in Industrial Control Systems

*[1]Rajesh L, [2]Penke Satyanarayana

*[1]Research Scholar [2]Professor

[1,2] Department of Electronics & Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A. P, India

Email: locharalarajesh@gmail.com, satece@kluniversity.in

Received: 25th July 2019, Accepted: 10th August 2019, Published: 31st August 2019

Abstract

Industrial Control Systems (ICS) are using for monitoring and controlling process plants like Oil & Gas refineries, Power generation and distribution etc. The data acquisition server in these ICS systems uses communication protocol like MODBUS, DNP to collect the data from PLC (Programmable Logic Controller) or Remote Telemetry Unit (RTU). Currently, infrastructure utilities depend heavily on their ICS systems in real-time. In earlier days these ICS systems were isolated from the external world and used dedicated network. But as technology evolves and time passes, these systems are connected to internet for remote monitoring through web access and data transfer to higher layers like Enterprise Resource Planning **(**ERP). MODBUS is widely used communication protocol for bi-directional data transfer between PLC and SCADA Servers, in industrial control systems and have been using since long time. But there are no security measures in MODBUS protocol. Security of these national critical infrastructures is key important role in safe and secure operations of these plants. The communication protocols are one of critical areas where security vulnerabilities are predominant. In this paper a test bed was set up and various attacks were simulated and analyzed the impact of the various security vulnerabilities/attacks on MODBUS Protocol. We proposed a new method for enhancing the security in MODBUS protocol.

Keywords

SCADA, PLC, MODBUS, Communication Protocol, Industrial Control systems, National Critical Infrastructure

Introduction

The National Critical Infrastructure (NCI) sectors are very crucial for development of any country. They play a vital role in supporting modern society. It can be defined as any functions, systems or facilities whose incapacity or non-functionality cause unbearable impact on national security, governance, economy and social well-being of a nation [1-2]. The safety, protection of NCI for reliable performance and operation is very crucial. Some of the NCI sectors are Nuclear Power Plants, Oil & Gas refineries and pipelines, Power generation and Transportation, Defense and space, Telecommunication systems, Banking & Finance, Transportation, Chemical Plants, Pharmaceuticals and Water supply etc. [3]. Many Industrial Control Systems (ICS) or Process Control Systems (PCS) are using for monitoring and controlling various plants, processes in these critical infrastructures. The protection of these systems from Cyber-attacks is very crucial for the proper safe and secure operation of the plants [4]. These systems are generally spread over miles of distance and programmed control functionality in main central computer. These systems are, now-a-days, connected to corporate networks for interfacing with their enterprise systems such as Energy Management Systems (EMS) or Distribution Management Systems (DMS) etc. [5].

The Industrial Control Systems Cyber Security Emergency Response Team (ICS-CERT), a unit of Department Home Land security of US Government, works to reduce risks in all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors [6]. As per CERT, some incidents where the attacks on these systems have become real like Ukrainian unscheduled power outage in 2015, Stuxnet in 2010 etc. As per ICS-CERT the Cyber-attacks are increasing continuously every year [6].

Recent attacks on Cyber infrastructure shows SCADA/PCS/ICS Systems are become target for attackers and supporting infrastructure mostly used in almost all critical industrial set-ups such as oil & Gas refineries, Power generation etc. The Department of Home Land Security (DHS) of US declared 16 national critical infrastructure sectors where the non-functionality of these sectors very high impact on national economy development, public health and safety [3]. It is required to protect these NCI systems from security vulnerabilities. We can identify number of areas where the security measures have to be considered to be addressed. Communication protocol security is one of the crucial areas where attention is required to protect the systems. We would like to test the effect of various attacks on MODBUS protocol, which is most widely used protocol in ICS systems [7-8]. We set up a test bed in our lab and various attacks were simulated and analyzed the effect of attacks. We also proposed a method to enhance the security

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

in MODBUS protocol.

Test Set Up

In our test set up, three computer systems were connected in a network using a network LAN Switch. One of the computers was configured as Data Acquisition Server (DAQ), another computer system as Man/Human Machine Interface (MMI or HMI) and a 3rd system was configured as Web server. One of the two LAN ports of the Web server is connected to the internet. Another port was connected to above LAN network. The LAN Switch was used for network connectivity. Vijeo Citect SCADA software package was loaded with MODBUS protocol in DAQ Server. SCADA GUI software was loaded in HMI Client system. We developed a MODBUS Master simulator and slave simulator using visual studio. The slave simulator can be configured to accept the connection from Master (Client), registers starting address, number of registers and other parameters. The master simulator can be configured with IP address, TCP port number, starting and number of registers of data to be polled and response time out parameters. In place of PLC, as shown in figure, we used soft PLC with MODBUS Salve simulator. Tag database was created in DAQ Server. GUI Mimics (screens) for displaying the data from PLC were created in HMI Client system using picture editor tool. Fig. 1 depicts set up using for testing. MODBUS simulator was installed in web server which was used for creating the simulation of attacks. It will be used for interfacing PLC and sending the commands to PLC. It was observed that RED dotted lines indicate normal actual data transfer between the DAQ Server and PLC. The bi-directional data transfer between MODBUS Simulator, running in Web Server, which was configured as Master and PLC was shown in GREEN dotted lines.

An application was developed in the SCADA system to study or visualize the effect of attacks. The application is developed using picture drawing tools in a SCADA package. The mimic of the application is as shown in Fig. 2. In this application, two tanks are available to transfer the fluid, say Petrol, from tank 101 A to tank 101 B. The fluid will transfer by pressurizing the pipeline using a Pump MP 101, which is connected between the tanks. There are two values connected with the pump i.e. inlet valve 101 and outlet valve 102. The Pump will be started whenever inlet and outlet valves are already opened. The tank levels, pump trip set point are analog values which will be monitored by the DAQ server. The pump will be automatically tripped whenever tank 101-B level reaches the set point tank level, set by the operator. The interlock logic was programmed in PLC. The tank levels and set point were configured as trend tags, so that operator or user can visualize the graphical form of the parameters.

Now, various attack scenarios were simulated, tested and studied the impact. The various vulnerabilities like Man-in-the-middle attack like False response injection, False command response, Packet sniffer, sending wrong requests continuously to make the PLC busy and sending commands to PLC to destroy the field or plants were simulated using the developed application and understood the impact on MODBUS protocol.

Testing

The above said MODBUS simulator was loaded in the web server to simulate attack environment. The simulator can be configured as Master or Slave. If the communication between the devices is through serial, then the entities are called Master and Slave, if it is through Ethernet then they will have called as Server and Client. The simulator was configured as Client (MODBUS Master). The PLC IP address was configured as a slave IP address in the simulator. If an attacker knows PLC IP address, he/she can do anything to the PLC or plant system. Even the attacker can run any tool like network analyzer to know the IP address of the PLC. As we do not know the MODBUS addresses of a slave in PLC, for trial and error purpose all data types i.e. coils, status, Input Registers, Output Registers were assigned as starting address 1, the number of registers as 10. Then it was connected to PLC. MODBUS simulator is successfully connected to the PLC because there was no authentication or checking of IP address at MODBUS slave in the PLC.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

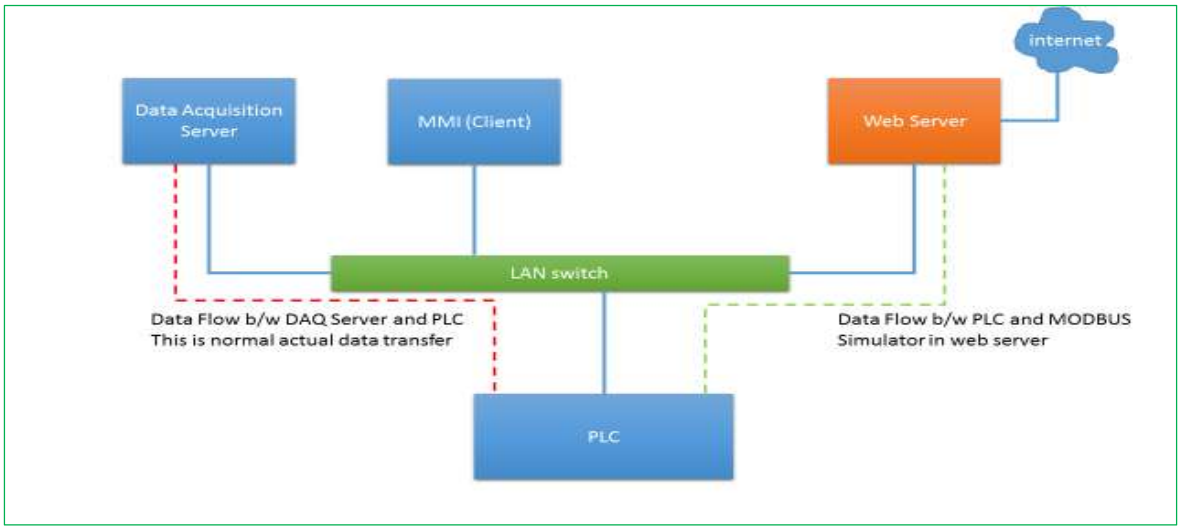

Figure 1: Test Set up Modules

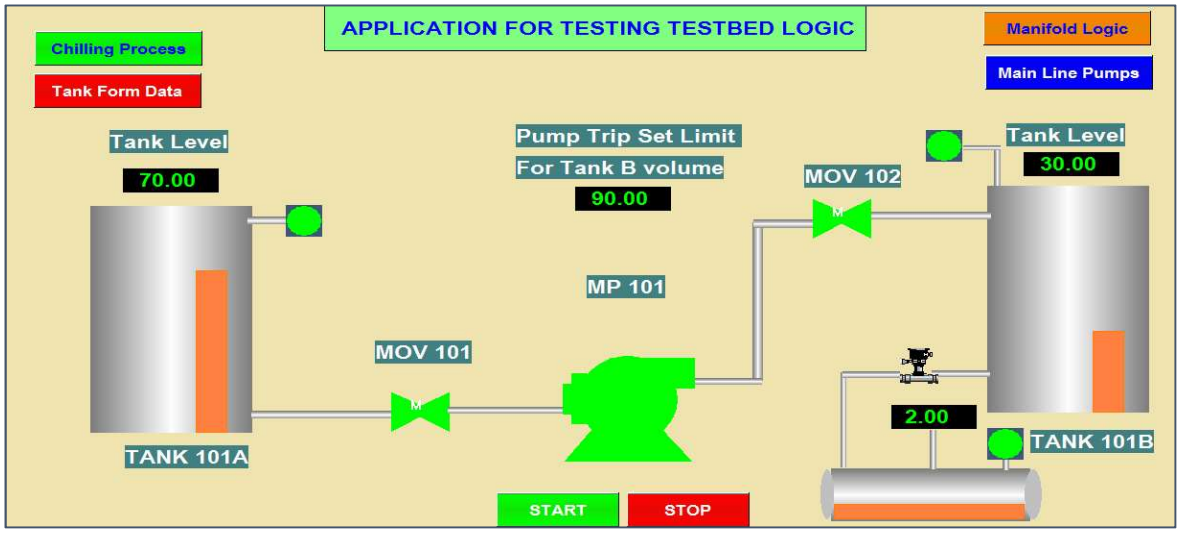

Figure 2: Typical Application MIMIC on SCADA System for Testing

The simulator successfully connected the PLC and received the response from PLC for the transmitted request. As the response is received without any security blocking the attacker could analyze the values. These are measured instrument values from the field. The attacker can read any value from the field because MODBUS slave at PLC responds to the request from the server with all field values. It shows that there is no confidentiality in the MODBUS protocol.

We sent control commands to coils on/off and set values to holding registers also. As there is no authentication feature in MODBUS slave at PLC, it accepted these commands and we got a successful response from PLC. This indicates PLC MODBUS do not have any mechanism to verify whether the commands were from the intended server or not. If the field is available, the attacker can do anything by sending control commands like Emergency Shutdown (ESD), pump trip etc. which will affect adversely the field or factory or process. For example, if it is a pipeline application, the pipeline may burst if the pump is started without opening outlet value. In the developed SCADA application, the set value of the pump trip set point was sent to PLC and the effect on the pump is depicted in Fig. 3. The set point was set at 50 instead of 80. The pump was tripped whenever the tank level 101B crosses 50. Again the pump trip was set as 105. The maximum storage capacity of tank 101 is 100. The pump was still running, not closed even though the tank 101 was empty. This will affect the pump and the pump may not work.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

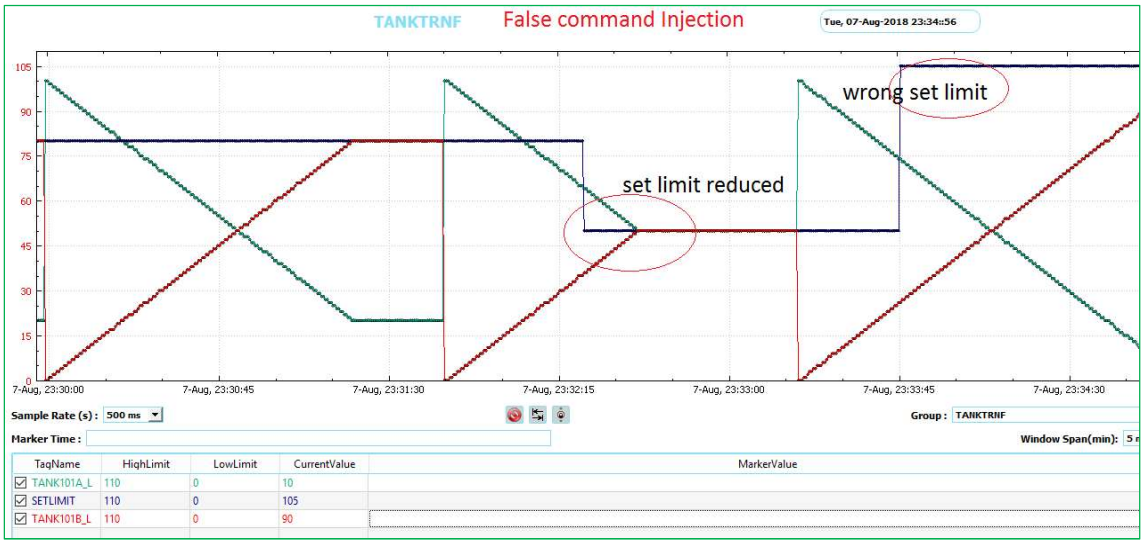

Figure 3: Effect of Sending a False Set Value for Pump Trip.

We also connected a laptop in the network and configured IP address of Laptop as PLC address. The MODBUS slave (server) simulator was running in the laptop. The request from actual DAQ server received in Laptop also. The simulator in laptop responded and a response sent to DAQ server which is not the intended or actual response. This is a false response injection in the network. As there is no security measurement at MODBUS Master at DAQ Server to differentiate between false responses and actually intended response. An attacker can run MODBUS Slave in a system which can be connected in the same network and can send unwanted or garbage values to DAQ Server. If these values are configured in interlocks at the SCADA level, adverse action will be driven by the SCADA system. For example, if Inlet Pressure of a pipeline station is more than some predefined value the Main Pump should stop to reduce the pressure to avoid the pipeline burst. If the MODBUS address of the holding register which is used for the Inlet Pressure value from the simulator is some garbage value like 1000 then immediately the SCADA sends the Pump Trip Signal. In our experiment, we wrote a script in DAQ Server to send Pump Trip command when Inlet or Outlet pressure crosses some predefined limit i.e Inlet Pressure more than 80 kg/ cm2 or Outlet Pressure less than 50kg/ cm2. Then we set some values in holding registers of the simulator in Laptop and DAQ Server received the wrong values and sent a trip signal to the field. Fig. 4 depicts the effect of false data injection in the MODBUS frame. The values of tank levels were disturbed with some junk values and the same was displayed in the trend display as shown in the figure.

Discussion and Enhancing Security in MODBUS

From the above analysis we concluded that MODBUS protocol is vulnerable to various security attacks. It is required to implement security enhancement methods to remedy the problem of MODBUS security. Some scholars already proposed or stated methods to address the issue i.e security of MODBUS. Fovino I.N. et al [9] incorporated cryptography methods in MODBUS protocol but the method suffers from delays which effects the real time performance. This method will not work when an attacker seizes the control of the devices. Aamir Shahzad [10,12,16] proposed cryptographic solution in different scenarios but the methods do not simulate in real time and also the method modified the MODBUS frame structure which is not suitable for 3rd party open protocol defined devices. Hayes [11] proposed a new method using hash-based streaming control protocol STCP with the security of the scheme is based on pre-shared key, if the pre-shared key is cracked, the security will be destroyed. Graham et al. [13] explained list of attacks on industrial control systems but they not provided any valid method. Morris et al. [14] proposed fifty rules to detect MODBUS attacks but no practical analysis was mentioned by authors. Luo, Xuan et al. [15] proposed a method with time delay and modifying the Modbus frame structure which is not possible for interoperability of systems. Rajesh.L et al [17] explained existing methods to provide the security of MODBUS protocol.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

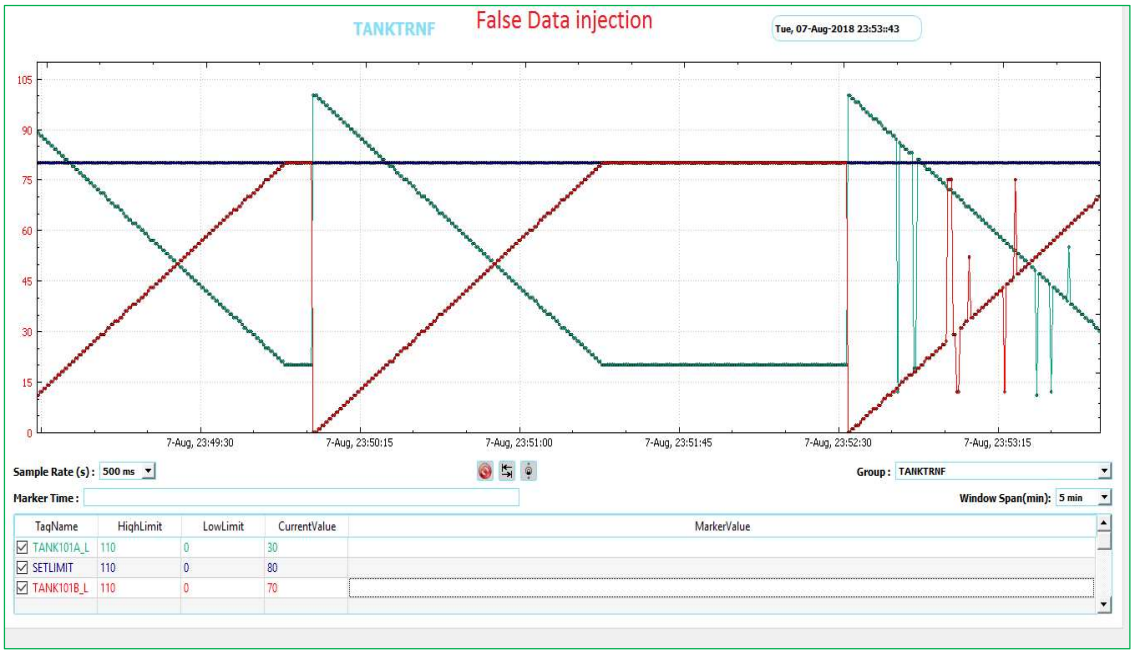

Figure 4: False Data Injection in MODBUS Data

From the above methods it was understood that these methods were not suitable to all types of PLC, SCADA systems which are available in market. Some methods provide additional overheads which may affect performance of the real time system. Some methods are changing MODBUS protocol itself which will become customization of the open protocol. There is no interoperability in these solutions. We are proposing a method – instead of sending and receiving plain MODBUS frames between PLC and SCADA, we want to transfer the data through gateway modules where the frames will be converting to modified formats which are not known to outsiders. Gateways receive the plain MODBUS Tx/Rx and converts the frames to cipher frames. The gateways also convert the encrypted messages to plain text/actual messages. We would like to design, develop the gateways with required encryption methods like AES, RSA, HASH algorithms to provide the security in MODBUS data transfer. The request frame from DAQ Server will be received at PLC and it will be verified for communication errors. If any communication errors are detected then the frame will be discarded, otherwise, it will be accepted for further processing. The same philosophy will be followed at DAQ Server for response frame from PLC/Controller through gateways. This solution provides the interoperability and can be used for existing and as well as new systems. Fig 5 shows the block diagram of the connectivity of gateways in the network.

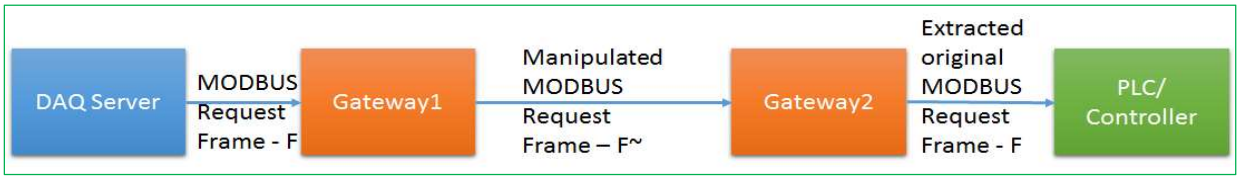

Figure 5: MODBUS Request Frame Data Flow from DAQ Server to PLC/Controller.

Conclusion

MODBUS is an industry standard communication protocol which is widely used in industrial control systems. An ICS system is using in national critical infrastructure for monitoring and controlling the field operations and automation to achieve high productivity. MODBUS protocol was developed without considering security features, which can be easily accessed by attackers. In this project, a test bed was set up and various attack scenarios were simulated to understand the possible attacks in the MODBUS protocol. A new method was proposed with gateways to manipulate the MODBUS frame formats which can be easily integrated with all types of SCADA and PLCs from various vendors. It provides interoperability with available products in the market. In future the proposed method will be implemented and tested.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

References

1. Presidential Decision Directive on Critical Infrastructure Protection, United States, 22 May 1998, available at http://www.fas.org/irp/offdocs/pdd/ pdd-63.htm
2. Ministry of Law and Justice, GoI, "The Information Technology (Amendment) Act, 2008", 05 February 2009, pp. 13–14, available at http:// www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/ it_amendment_act2008.pdf
3. https://www.dhs.gov/critical-infrastructure-sectors
4. A. A. Cardenas, S. Amin, and S. Sastry. Research ´ challenges for the security of control systems. In Proceedings of 3rd USENIX workshop on Hot Topics in Security (HotSec), San Jose, CA, USA, July 2008.
5. Simon Duque Antón, Daniel Fraunholz, Christoph Lipps, Frederic Pohl, Marc Zimmermann, Hans D. Schotten, "Two decades of SCADA exploitation: A brief history", Application Information and Network Security (AINS) 2017 IEEE Conference on, pp. 98-104, 2017.
6. https://ics-cert.us-cert.gov/
7. MODBUS Messaging On Tcp/Ip Implementation Guide V1.0b, Modbus Organization, Oct 24, 2006
8. MODBUS Appl Protocol Specification V1.1 b3, Modbus Organization, April 26, 2012
9. Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A. (2009). Design and Implementation of a Secure Modbus Protocol. IFIP Advances in Information and Communication Technology Critical Infrastructure Protection III, 83-96. doi:10.1007/978-3-642-04798-5_6
10. A. Shahzad, S. Musa, M. Irfan, and S. Asadullah, 2014. Key Encryption Method for SCADA Security Enhancement. Journal of Applied Sciences, 14: 2498-2506.
11. G. Hayes and K. El-Khatib, "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol," 2013 Third International Conference on Communications and Information Technology (ICCIT), Beirut, 2013, pp. 179-184. doi: 10.1109/ICCITechnology.2013.6579545
12. A. Shahzad, S. Musa, and M. Irfan, 2014. Security Solution for SCADA Protocols Communication during Multicasting and Polling Scenario. Trends in Applied Sciences Research, 9: 396-405.
13. J. Graham, J. Hieb, and J. Naber, "Improving cybersecurity for Industrial Control Systems," 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE), Santa Clara, CA, 2016, pp. 618-623. doi: 10.1109/ISIE.2016.7744960
14. Morris, T. H., Jones, B. A., Vaughn, R. B., & Dandass, Y. S. (2013). Deterministic Intrusion Detection Rules for MODBUS Protocols. 2013 46th Hawaii International Conference on System Sciences. doi:10.1109/hicss.2013.174
15. Luo, Xuan & Li, Yongzhong. (2019). Security Enhancement Mechanism of Modbus TCP Protocol. DEStech Transactions on Computer Science and Engineering. 10.12783/dtcse/iciti2018/29146.
16. Shahzad, A.; Lee, M.; Lee, Y.-K.; Kim, S.; Xiong, N.; Choi, J.-Y.; Cho, Y. Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information. *Symmetry* 2015, *7*, 1176-1210.
17. Rajesh, L & Satyanarayana, P. (2017). Communication protocol security in industrial control systems to protect national critical infrastructure. Journal of Advanced Research in Dynamical and Control Systems. 9. 290-304.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495