American Journal of Applied Sciences 11 (8): 1398-1404, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.1398.1404 Published Online 11 (8) 2014 (http://www.thescipub.com/ajas.toc)

A REVIEW: INDUSTRIAL CONTROL SYSTEM (ICS) AND THEIR SECUITY ISSUES

[1]Shahzad, A., [1]S. Musa, [1]A. Aborujilah and [2]M. Irfan

[1]Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia
[2]Windfield College, Kuala Lumpur, Malaysia

Received 2014-01-14; Revised 2014-05-13; Accepted 2014-06-24

ABSTRACT

Industrial Control System (ICS) has been designed for critical infrastructure sectors and 90% of these systems are property/owaned and operated by private organizations. Industrial Control System (ICS) were designed to fulfill the basic requirements included system performance and reliability and other basic needs, related with real time transmission, without interlinking with networks (public/private) or/and internet connectivity. In this research, detail review has been conducted which is based on Industrial control system or ICS types and their uses and/or importance within industries or real time industries. The remaining sections highlighted the potential problems or issues which are linked with these systems during communication and detail problem statement has been also conducted and several existing security deployments are reviewed, to find the generic security mechanism that will secure the communication of critical infrastructures.

Keywords: Supervisory Control and Data Acquisition (SCADA) Systems, Security Issues and Solutions

1. INTRODUCTION

1.1. Industrial Control System (ICS)

The term Industrial Control System (ICS) is uses for several types of real time infrastructures (systems) such as Distributed Control Systems (DCS), Supervisory Control And Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLC). The broad term Industrial Control System (ICS) had been used for industries or/and real time infrastructures (Stouffer *et al*., 2006). Industrial Control System (ICS) infrastructures are based on several types of field devices, which are communicating within ICS network for the purposes of message/data and commands delivery and feedback from remote station to master station. The communication between field devices are based on supervisory/automated commands such as an instruction to collect data from sensor connected with remote station, check the alarm status, breakers opening and closing status information and time synchronization, transmitted from control station or master station to field devices using Human Machine Interface (HMI). Industrial Control System (ICS) had been designed for critical infrastructure sectors and 90% of these systems are property/owned and operated by private organizations. Industrial Control System (ICS) has been also operated by Federal agencies usually for the purposes of air traffic system control, nuclear plant operations and controlling and uses within oil industry, gas industry, chemical industry, transportation system and pharmaceutical manufacturing (Stouffer *et al.*, 2006).

1.2. Supervisory Control And Data Acquisition (SCADA) System

Supervisory Control And Data Acquisition (SCADA) system is real time Industrial Control System (ICS), usually uses for monitoring and controlling industrial processes between field devices connected within

Corresponding Author: Shahzad, A., Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia

SCADA network. SCADA systems or fields devices are geographical distributed in different locations and monitor/control by centralized control center using human machine interface and utilized for critical processes sectors included water distribution and treatment plants, power generation stations, water collection and treatment plants, fabrication and refining plants, wind farms stations, telecommunication systems, oil refining station, gas collection and pumping stations, electrical power houses, airports monitoring and controlling systems, ships monitoring and controlling systems, space monitoring and controlling stations and air conditioning and heating ventilation plants/systems. In SCADA system, data/information is collected from devices or actuators/sensors connected within network and this information will proceed to master control center for monitoring and controlling purposes. During SCADA communication, information has been visualized in the form of text or graphical representation, thereby visualization facilitates are located and operator at control center for controlling and monitoring the real time environment usually, automatically or by commands operation. In **Fig. 1**, SCADA system provides communication between the field devices such as Master Terminal Unit (MTU), Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) and entire communication is monitor and operator from center control using various type of communication networks included Public Switched Telephone Network (PSTN), Local Area Network (LAN), Wide Area Network (WAN) and SCADA system has been also deployed wireless technologies such as for communication between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and field devices (Shahzad *et al*., 2014a; Musa and Aborujilah, 2013a). The following detail below depicted the services information usually performed by SCADA system.

SCADA system provides supervisor control over the field devices and monitors the entire communication from center location, usually by Human Machine Interface (HMI) software. SCADA system has been used various types of media included radio signals, telephone line, cable connection, satellite and micro waves media for communication between field devices located at distance placed.

Control center such as master terminal station is uses as centralized controller to control and monitor the field devices in SCADA network such as communication between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs).

Remote Terminal Units (RTUs) are use to collect information/data from sensors/actuators, that are connected with physical environment and transmits the information to control center or Master Terminal Unit (MTU) for monitoring purposes. Network topology is deployed as static manners in SCADA system and networks nodes are know in advance, for communication between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs).

1.3. Distributed Control System (DCS)

Distributed Control System (DCS) is another part of Industrial Control System (ICS) and uses to control and monitor industrial production included processing sectors such as water distribution and treatment plants, power generation stations, wastewater collection and treatment plants, fabrication and refining plants, wind farms stations, oil refining station, gas collection and pumping stations, electrical power houses and air conditioning and heating ventilation plants/systems.

Distributed Control System (DCS) is usually used control loopor upervisory station also contain control loops and intermediate control for the purpose of tasks distributio, to manage the processes/tasks, that are distributed locally between the controllers within DCS network. Distributed Control System (DCS) gather all information from these localized controllers and then produce whole production or processing execution results. DCS applications are distributed among several controllers (or computers) to minimizes the load on each controller or/and on main controller (or main server). Basic implementation of Distributed Control System (DCS) is comparatively same as SCADA system but in production phase, application or tasks are distributed among several localized controllers such that each controller has assigned function from supervisory controller. Supervisory controller or master controller initial the request and send to field devices. On response, localized controllers generate the results according to supervisory control request and collect data/information from field devices then send response back to main server or supervisory controller (Stouffer *et al*., 2006).

1.4. Programmable Logic Controllers (PLC)

Supervisory Control And Data Acquisition (SCADA) system and Distributed Control Systems (DCS), both of them have been using Programmable Logic Controllers

(PLC), for controlling overall network architecture. PLCs are mostly uses for data/information collection from physical environment and upon collection, process the information back to master station based on master station request. Remote Terminal Units (RTUs) within SCADA system are used as PLCs to collect data/information from sensors/actuators and transmit back to master station for the purposes of controlling and monitoring. At other side, field controllers or local controllers perform functions or uses as Programmable Logic Controllers (PLCs) within Distributed Control System (DCS). Local controllers are collect data/information from field devices and send response back to master controller or supervisory controller. Usually, all types of Programmable Logic Controllers (PLCs) have their own memory or storage area for storing information related with instructions being execute or basis on master controller/master station request or functions implementation such as input/output controlling functions, session management, arithmetic and logical functions, alarm controlling function and processing of data/information, (Shahzad *et al*., 2013; 2014b).

1.5. Background Problems: SCADA System

SCADA systems have been geographical distributed across different locations over the world using Wide Area Network (WAN) technology. SCADA systems have been connected with numbers of remote terminal devices or PLCs through several types of networks such as LAN/WAN, protocols and transmission media such as wire/wireless. The great enhancement within SCADA, connectivity with several advance networks and used of advance I.T infrastructures, brought SCADA communication more demandable for end users. SCADA uses centralized station with advance I.T infrastructure, therefore able to control thousand of remote terminal stations or field devices at the same time without limitation of networks and protocols or open standards. At the other side, large interconnectivity of open standards networks, protocols and uses of open I.T infrastructure within SCADA system, made SCADA platform more vulnerable from several types of threads and attacks (Stouffer *et al*., 2006; Musa and Aborujilah, 2013b). More detail related with SCADA vulnerabilities and threats are depicted below.

Supervisory Control And Data Acquisition (SCADA) systems were designed to fulfill the basic requirements such as system performance and reliability and other basic needs related with SCADA system operations of real time industrial infrastructure, without interlinking with networks such as public/private and internet connectivity. Traditionally, SCADA systems were connected with proprietary hardware/software and protocols. With the revolution of advance I.T infrastructure, SCADA systems are also move/change from traditional network to advance networks or open standards network protocols, rather than proprietary such as LAN/WAN through internet connectivity significantly increase the performance, reliability and scalability of system (Musa and Aborujilah, 2013a; Raghini *et al*., 2013). With advance interconnectivity, SCADA platform has been vulnerable from several kinds of communication and cyber attacks and threads.

Several solutions were developed to secure SCADA communication, but mostly were based on physical security and limited-communication security using secure socket layer or SSL/internet protocol or IP security. But these solutions have also number of limitations, while deploying within SCADA communication because these solutions have been depending on cryptography algorithms. So, current research proposes the solution that has been developed successfully within SCADA system and successfully secure the SCADA communication between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU).

Traditionally, SCADA systems have several characteristics, risks and priorities that are quite different from internet based communication systems such as characteristics, risks and priorities and have different specifications for communication such as network and protocol requirements. There are few considerations that must be taking placed, when traditional SCADA infrastructure is replaced with current communication infrastructure by using of open standards protocols and networks such as performance such as session/time management, availability such as expected/unexpected results management, management of risk and disaster, infrastructure security issues, processes consequences, communication response management, operation management, Resource availability and management, protocols and media management and replacement of field devices, devices life session, permission to access and organization support.

There are numbers of threads that disturb or intercept the SCADA communication such as communication attackers inside/outside organization, attacker or bot-network, attacker using spam, attacker using phishing, attacker using spyware and attacker using malware.

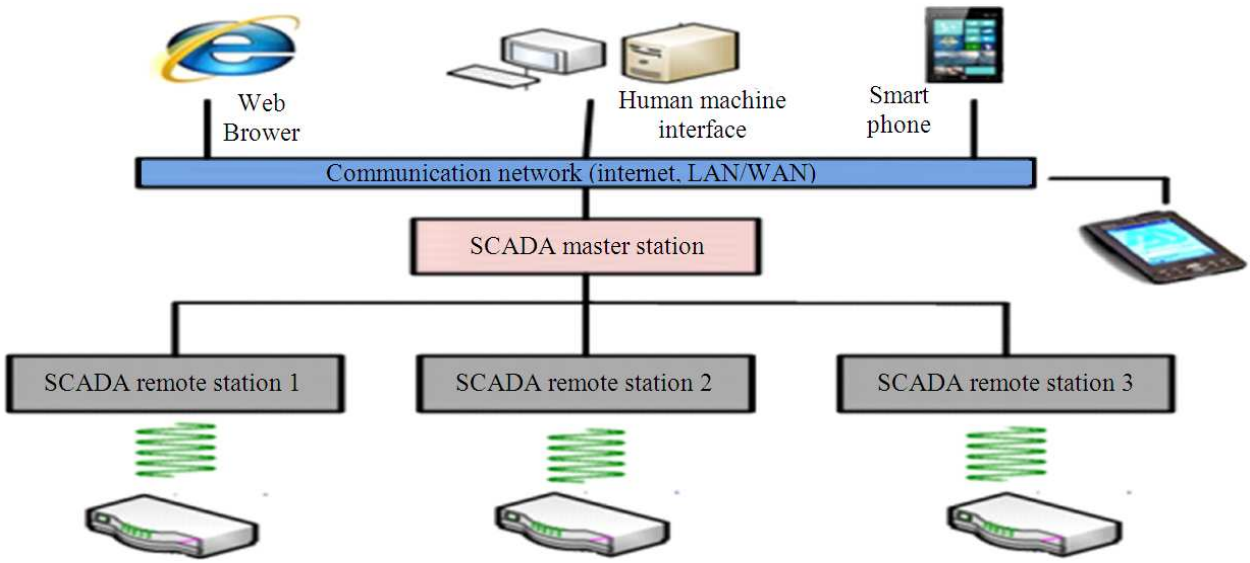

Fig. 1. SCADA system communication

The vulnerabilities such as installation and configuration of networks or inappropriate, communication architecture, password policy, system authentication and authorization, nonexistence of intrusion detection and prevention system, nonexistence software/hardware firewall and cryptography protection are usually located within SCADA system, that make communication more unsecure.

After conducting the detail analysis, that has been based on SCADA communication security issues such as threads, vulnerable platforms and nonappropriates security policies and solutions analysis within SCADA communication. The security solution has been developed successfully within SCADA system and successfully secures the SCADA communication and gives research directions to overcome the security issues that are warming SCADA communication (Musa and Aborujilah, 2013a).

1.6. Problem Statements: SCADA System

The problem statement has been conducted from detail study, based on existing SCADA security issues such as threads/attacks and vulnerabilities. More detail related with SCADA systems and protocols security issues and challenges are depicted below.

Several security issues and challenges have been reviewed from existing SCADA implementations. According to the review analysis, there are no proper solutions that SCADA communication and overcome completely secure the the security issues related with them such as eavesdropping, data modification, data replay, key distribution and other generic attacks (Anandkumar and Jayakumar, 2012; Manikandan and Manimegalai, 2012).

Based on review, all existing solutions (generic security solutions) have been based on cryptography techniques such as encryption, digital signature and hashing algorithms, for the purpose of secure data/message communication between SCADA nodes (Hong and Lee, 2008; Bhaya and AlAsady, 2012).

SCADA communication has been vulnerable from several types of cyber attacks; by rapidly increasing SCADA system connectivity with IP based protocols or open standard protocols. Based on SCADA security, cryptography solutions such as Symmetric and Asymmetric have been deployed to achieve the security services goals such as data confidentiality, data authentication, data integrity and non-repudiation function and secure SCADA communication long run (Drahansky and Balitanas, 2011; Majdalawieh *et al*., 2006).

SCADA systems are vulnerable from cyber attacks. Several existing solutions address the security related with SCADA communication with limitations. Four main components have been highlighted for SCADA security issues such as authenticity, availability, integrity, confidentiality. SCADA system has been reduced the risks, gain control and provides secure communication over attacks/threads using cryptography solution or module (AGA, 2003; Aris *et al*., 2011). Asymmetric and symmetric solutions are deployed within several

networks and successfully achieved the security services included authentication, integrity, non repudiation and confidentiality as main part of SCADA security protection.

SSL/TLS and IP based security solutions have been implemented within several traditional networks applications or/and SCADA communication network or protocols. SSL/TLS and IP based solutions have number of issues related with their communication and security, included running on Transport Control Protocol (TCP), base on cryptography algorithms for security purposes and security mechanism is limited for non repudiation function and other unavailable advance security features (Patel and Graham, 2009; Preneel, 1993).

SCADA security issues such as no proper authentication mechanism for SCADA system in the term of designed and processing or operation, uses of proprietary or vendors protocol with open standards Protocols (TCP/IP), trust on physical security concepts and performance decreases over internet with several vulnerabilities. From these security issues; cryptography solution such as asymmetric using ECC algorithm and symmetric using AES algorithm has been deployed within SCADA communication end-to-end and achieved security services such as data confidentiality, data authentication, data integrity and non-repudiation function. As "Schweitzer Engineering Laboratories, Inc" suggested that cryptography solutions is best approaches to overcome the SCADA security issues during communication (Risley and Ladow, 2003).

Based on SCADA vulnerabilities; homeland security (department) has been used cryptography mechanism (solution) to secure "Nation"s critical infrastructure" from cyber attacks/threads. As conclusion, cryptography solutions are the best approaches to secure or protect SCADA communication over internet and successfully decrease the risks (Shahzad *et al*., 2014a; Asenjo, 2005; Babu and Singh, 2013). Advance Encryption Standard (AES) 256, HMAC and MD5 as part of cryptography solutions have been deployed, to protect SCADA communication, while intrusions (anomaly) are detected by Intelligent Electronic Device (IED) as part of substation controller (Musa and Aborujilah, 2013a; Hong, 2010; AL-Saidi *et al*., 2011).

The "American National Security Agency" has been suffering from potential attacks and hackers that are serious problems for critical infrastructure sectors. So, need a solution that significantly secures the critical infrastructure communication, while connected with open standard networks or protocols (Pollet, 2002).

SCADA system vendors and developers have been only focusing on functional parts of SCADA system such scalability, reliability, performance and access control without security consideration in mind. There is no generic solution available that fulfill the requirements of SCADA system security. All SCADA functional performances are depending on security issues, if SCADA system is fully secure then whole system performances would absolutely achieve (Rautmare, 2011).

SCADA system implementations using control protocols such Distributed Network Protocol (DNP3), fieldbus, modbus and other IP based protocols are harmful and critical for SCADA communication between field devices. These protocols have been designed without any security concerned that fully or partially provides protection against cyber attacks and threads. Several firewalls have been used between SCADA system and corporate networks or internet but unable to fully integrate with SCADA networks, such as in term of SCADA protocols such as DNP3 or Modbus development and configuration. So, lack of security information and protocols configuration unawareness, rapidly increasing more vulnerabilities for SCADA platform and causing major security issues for critical infrastructures (Cai *et al*., 2008; Shahzad *et al*., 2013).

DNP3 is most important protocol uses within SCADA system. DNP3 is uses almost all over the world; approximately 70% in America within electric and water utilities and remaining 30% in other parts of the world such as Europe, Asia and Australia (TD, 2011). Securing DNP3 protocol or security deployment within DNP3 protocol, significantly enhance the security of SCADA system and reduce the potential attacks and vulnerabilities within communication.

2. CONCLUSION

The detail literature has been reviewed which is based on Industrial Control System (ICS) deployment, their main architecture and the importance within industries. The security issues have been highlighted that are warming the communication and the existing security mechanisms are also reviewed that are useful to protect the communication from attacks and make Industrial Control System (ICS) platform secure against vulnerabilities. In future work, the

cryptography based strong security solution will implement to protect the Industrial Control System (ICS), while connecting with several open networks.

3. ACKNOWLEDGMENT

I would like to thank to my parents and my friend, M. Irfan boosted me morally and provided me great information resources.

4. REFERENCES

AGA, 2003. Cryptographic protection of SCADA communications. American Gas Association's.

AL-Saidi, N.M.G., M.R.M. Said and A.M. Ahmed, 2011. Efficiency analysis for public key systems based on fractal functions. J. Comput. Sci., 7: 526-532. DOI: 10.3844/jcssp.2011.526.532

Anandkumar, K.M. and C. Jayakumar, 2012. Pro-active prevention of clone node attacks in wireless sensor networks. J. Comput. Sci., 8: 1691-1699. DOI: 10.3844/jcssp.2012.1691.1699

Aris, S., A. Messai, M. Benslama, M. Nadjim and M.M-Elharti, 2011. Integration of quantum cryptography through satellite networks transmission. Am. J. Applied Sci., 8: 71-76. DOI: 10.3844/ajassp.2011.71.76

Asenjo, 2005. A retrofit security solution for SCADA communications and maintenance port access Authentication. Encryption Key Manage.

Babu, A.M. and K.J. Singh, 2013. Performance evaluation of chaotic encryption technique. Am. J. Applied Sci., 10: 35-41. DOI: 10.3844/ajassp.2013.35.41

Bhaya, W.S. and S.A. AlAsady, 2012. Prevention of spoofing attacks in the infrastructure wireless networks. J. Comput. Sci., 8: 1769-1779. DOI: 10.3844/jcssp.2012.1769.1779

Cai, N., J. Wang and X. Yu, 2008. SCADA system security: Complexity history new develop. Proceedings of the 6th IEEE International Conference on Industrial Informatics, Jul. 13-16, IEEE Xplore Press, Daejeon, pp: 569-574. DOI: 10.1109/INDIN.2008.4618165

Drahansky and M. Balitanas, 2011. Cipher for internet-based supervisory control and data acquisition architecture. J. Security Eng., 6: 337-348.

Hong and S.J. Lee, 2008. Challenges and perspectives in security measures for the SCADA system. Proceedings of the 5th International Conference, Myongji-Tsinghua University Joint Seminar, (IC' 08).

Hong, S., 2010. Experiments for embedded protection device for secure SCADA communication. Proceedings of the Power Energy Engineering Conference, Mar. 28-31, IEEE Xplore Press, Chengdu, pp: 1-4. DOI: 10.1109/APPEEC.2010.5448606

Majdalawieh, F., P. Presicce and D. Wijesekera, 2006. DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework. In: Advances in Computer Information and Systems Sciences and Engineering, Khaled E., T. Sobh, A. Mahmood, M. Iskander and M. Karim (Eds.)., Springer, Netherlands, ISBN-10: 978-1-4020-5260-6, pp: 227-234.

Manikandan, S.P. and R. Manimegalai, 2012. Survey on mobile ad hoc network attacks and mitigation using routing protocols. Am. J. Applied Sci., 9: 1796-1801. DOI: 10.3844/ajassp.2012.1796.1801

Musa, S. and A. Aborujilah, 2013a. Simulation base implementation for placement of security services in real time environment. Proceedings of the 7th International Conference on Ubiquitous Information, (CUI '13), ACM, New York, USA. DOI: 10.1145/2448556.2448587

Musa, S. and A. Aborujilah, 2013b. Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, (MC'13), ACM, New York, USA. DOI: 10.1145/2448556.2448588

Patel, G. and J.H. Graham, 2009. Improving the cyber security of SCADA communication networks. Commun. ACM., 52: 139-142. DOI: 10.1145/1538788.1538820

Pollet, J., 2002. Developing a solid SCADA security strategy. Proceedings of the 2nd IEEE Sensors Conference for Industry, Nov. 19-21, IEEE Xplore Press, pp: 148-156. DOI: 10.1109/SFICON.2002.1159826

Preneel, B., 1993. Cryptographic hash functions: An overview. Proceedings of the 6th International Computer Security and Virus Conference, (VC' 93), pp: 1-22.

Raghini, M., N.U. Maheswari and R. Venkatesh, 2013. Overview on key distribution primitives in wireless sensor network. J. Comput. Sci., 9: 543-550. DOI: 10.3844/jcssp.2013.543.550

Rautmare, S., 2011. SCADA system security: Challenges and recommendations. Proceedings of the 1st IEEE India Conference, Dec. 16-18, IEEE Xplore Press, Hyderabad, pp: 1-4. DOI: 10.1109/INDCON.2011.6139567

Risley, J. and P. Ladow, 2003. Electronic security of real-time protection and scada communications. Schweitzer Engineering Laboratories Inc.

Shahzad, A.A., S. Musa, A. Aborujilah and M. Irfan, 2014a. Industrial Control Systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, Jan. 09-11, ACM, New York. DOI: 10.1145/2557977.2558061

Shahzad, A., A. Aborujilah and M. Irfan, 2014b. A new cloud based supervisory control and data acquisition implementation to enhance the level of security using testbed. J. Comput. Sci., 10: 652-659. DOI: 10.3844/jcssp.2014.652.659

Shahzad, S., S. Musa, A. Aborujilah, M.N. Ismail and M. Irfan, 2013. Conceptual model of real time infrastructure within cloud computing environment. Int. J. Comput. Netw., 5: 18-24.

Stouffer, K., J. Falco, K. Scarfone, K. Stouffer and J. Falco, 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security. Pennsylvania State University.

TD, 2011. Increases in substation automation, integration program spending reported by North American Utilities. Transmission and Distribution.