Journal of Mechanical Science and Engineering 8(1) 13-18, 2021
ISSN 2354-9467

A REVIEW: INDUSTRIAL CONTROL SYSTEM (ICS) AND SYSTEM SECURITY

Herik H A.[1*]

[1]Department of Mechanical Engineering, Faculty of Engineering, Universitas Sriwijaya, South Sumatera, Indonesia

ABSTRACT

Design of Industrial Control Systems (ICS) is used for critical infrastructure sectors. Industrial Control Systems (ICS) aims to meet the basic requirements of performance and system problems and other basic needs, related to the transmission of real-time, without interlink with the network (public/private) or/and internet connectivity. In this research, a detailed study was carried out based on industrial control systems or types of ICS and their use in real-time industries or industries. The next section tug at the potential problems associated with this system during communication and a detailed problem statement was also carried out and several existing security deployments were reviewed, to find the critical infrastructure communication infrastructure.

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

1 INDUSTRIAL CONTROL SYSTEM (ICS)

Industrial Control System (ICS) is used for several types of real-time infrastructure (systems) such as Distributed Control System (DCS), Supervisory Control And Data Acquisition (SCADA), and Programmable Logic Controllers (PLC). The definition of a distributed control system (DCS) is a computerized control system for a process or plant and has multiple control loops, where autonomous controllers are distributed throughout the system, but there is no central operator supervisory control. This differs from systems that use centralized controllers; either a separate controller located in a central control room or within a central computer. The DCS concept can increase reliability and reduce installation costs by localizing its control functions. Furthermore, the term Industrial Control System (ICS) has been used for industry or/and real-time infrastructure [1]. The Industrial Control System (ICS) infrastructure is based on several types of field devices, which communicate in the ICS network to send messages/data and commands and feedback from remote stations to the master station. Communication between field devices is based on surveillance / automatic commands such as instructions for collecting data from sensors connected to remote stations, checking alarm status, breakers. Open and close status information, and time synchronization is sent from the control station or master station to the field equipment using the Human Machine Interface (HMI). Industrial Control Systems (ICS) have been designed for the critical infrastructure sector and 90% of these systems are owned or and operated by private organizations. The Industrial Control System (ICS) has also been operated by Federal agencies usually to control air traffic systems, nuclear plant operations, and control other than that, it also has been used in the oil industry, gas industry, chemical industry, transportation systems, and pharmaceutical manufacturing [1].

2 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

Supervisory Control And Data Acquisition (SCADA) This system is a real-time Industrial Control System (ICS), usually used to monitor and control industrial processes between field devices connected to the SCADA Network. SCADA systems or field devices are geographically distributed in various locations and monitor/control by a centralized control center using a human-machine interface and are used for critical process sectors for example such as processing plants, power stations, monitoring stations, and so on. In this system,

*Corresponding author's email: herikagrisa@gmail.com
https://doi.org/10.36706/jmse.v8i1.51

data/information is collected from networked actuator/sensor devices, and this information will be forwarded to the main control center for monitoring and control purposes. When the information is received, it is then visualized in text or graphical representation, so that the visualization facility is placed, and the operator can monitor it in real-time. In Figure 1, the SCADA system provides communication between field devices such as Master Terminal Units (MTU), Remote Terminal Units (RTUs), and Programmable Logic Controllers (PLCs), and all communications are monitored and operators from the control centre using various types of communication networks including Public Switched Telephone Networks (PSTN), Local Area Networks (LANs), Wide Area Networks (WANs) and SCADA systems have also implemented wireless technology such as for communication between Main Terminal Units (MTU) and Remote Terminal Units (RTU) [2][3]. The following details are described as information on services normally performed by SCADA systems.

SCADA systems provide supervisor control over the field devices and monitor all communications from a central location, usually by software Human Machine Interface (HMI). The SCADA system has used various types of media including radio signals, telephone lines, cable connections, satellites as a centralized controller to control and monitor field devices in the SCADA network such as communication between the Master and microwave media for communication between field devices located at a distance that is placed.

Control centers such as master terminal stations are used Terminal Units (MTU) and Remote Terminal Units (RTUs). Remote Terminal Units (RTUs) are used to collect information from sensors/actuators, which are connected to the physical environment, and transmit that information to a control center or Master Terminal Unit (MTU) for monitoring purposes. The network topology is used as a static means in the SCADA system and the network nodes are known in advance, for communication between the Main Terminal Unit (MTU) and the Remote Terminal Unit (RTU).

3 DISTRIBUTED CONTROL SYSTEM (DCS)

Distributed Control System (DCS) is another part of the Industrial Control System (ICS) and is used to control and monitor industrial production includes processing sectors such as water distribution and treatment plants, power plants, system boilers, wastewater collection and treatment plants, fabrication and refining plants, wind power stations, oil refining stations, gas collection and pumping stations, electric powerhouses, and factories. / air ventilation and heating systems. Distributed Control System (DCS) usually used looper control station also contains control loops and intermediate control for task distribution purposes, to manage processes/tasks, which are distributed locally between controllers in the DCS network. Distributed Control System (DCS) collects all the information from these local controllers and then produces the entire production or processing execution result. The DCS application is distributed among multiple controllers (or computers) to minimize the load on each controller or/and the main controller (or main server). The basic implementation of Distributed Control Systems (DCS) is comparatively the same as SCADA systems but in the production phase, applications or tasks are distributed among several localized ones.

The controller in such a way that each controller has assigned the function of the supervisory supervisor. The supervisory supervisor or master controller initializes the request and sends it to the field device. When responding, localized controllers produce results according to supervisory control requests and collect data/information from field devices then send responses back to the main server or superintendent supervisor [1].

4 PROGRAMMABLE LOGIC CONTROLLER (PLC)

Supervisory Control And Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), both have used Programmable Logic Controllers (PLC), to control the overall network architecture. PLC is mostly used for data/information collected from the physical environment and after collection, processes the information back to the master station based on the request of the master station. Remote Terminal Units (RTUs) in a SCADA system are used as PLCs to collect data/information from sensors/actuators and send them back to the master station for control and monitoring purposes. On the other hand, field controllers or local controllers perform the function or use as

Programmable Logic Controllers (PLCs) in Distributed Control Systems (DCS). Local controllers collect data/information from field devices and send responses back to the master controller or supervising supervisor. Typically, all types of Programmable Logic Controllers (PLCs) have their memory or storage area storing information related to the instruction being executed or upon request of the master controller/master station or implementation of functions such as input/output control functions, session management, arithmetic, and logical functions. , alarm control function, and data/information processing [3].

5 BACKGROUND PROBLEMS: SCADA SYSTEM

The SCADA system has been spread geographically in various locations in the world using Wide Area Network (WAN) technology. The SCADA system can be connected to several remote terminal devices or PLCs through several types of networks such as LAN / WAN, protocols, and transmission media such as cable / wireless. Major improvements in SCADA, connectivity with multiple sophisticated networks, and use of advanced Infrastructure make SCADA communications more desirable to end-users as they can control thousands of stations or terminal fields remotely. However, the high interconnection of open standard networks, protocols, and the use of open IT infrastructure in the SCADA system, makes the SCADA platform more vulnerable to various types of threats and attacks [2][1]. More details on the vulnerabilities and threats to SCADA are described below.

The Supervisory Control And Data Acquisition (SCADA) system is designed to meet basic requirements such as system performance and reliability and other basic needs associated with real-time industrial infrastructure SCADA system operation, without interlinking with networks such as public/private and internet connectivity.

Traditionally, SCADA systems were linked by proprietary hardware/software and protocols. With the revolution in advanced I.T infrastructure, SCADA systems are also moving/changing from traditional networks to advanced networks or open standard network protocols, rather than proprietary such as LAN / WAN through internet connectivity significantly improving system performance, reliability, and scalability [2][4].

With its advanced interconnectivity, the SCADA platform is vulnerable to multiple types of communications and cyber-attacks and threads. Several solutions were developed to secure SCADA communications but most are based on physical security and limited communication security using secure socket layer or SSL / internet protocol or IP security. But this solution also has several limitations when it comes to implementing SCADA communications because it relies on cryptographic algorithms. So, the current research proposes a solution that has been developed successfully in the SCADA system and successfully secures SCADA communication between the Main Terminal Unit (MTU) and the Remote Terminal Unit (RTU) or/and the Remote Terminal Unit (RTU) and the master Terminal Unit (MTU).

SCADA systems have several characteristics, risks, and priorities that are quite different from internet-based systems such as factors, risks, and priorities and have different communication specifications such as network and protocol requirements. There are several considerations to be taken when traditional SCADA infrastructure is replaced with current communication infrastructure using open standard protocols and networks such as performance, session/time management, expected / unexpected outcome management, risk and disaster management, infrastructure problems, processes, communication response management, operations management, resource groups, and management, protocol, and media management and field device replacement, device live sessions, permissions to access and organizational support.

Several threads interfere with or intercept SCADA communications such as internal/outside communications attackers, attackers or bot networks, attackers using spam, attackers using phishing, attackers using spyware, and attackers using malware.

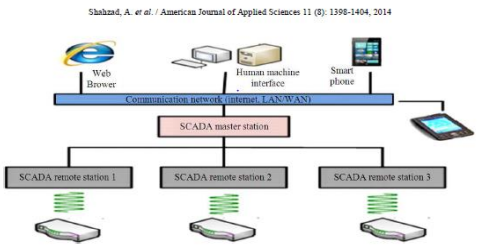

Figure 1 SCADA Communication System

Vulnerabilities such as non-conforming or network installation and configuration,

communication architecture, password policies, system authentication and authorization, absence of intrusion detection and prevention systems, non-existent software/hardware firewalls, and cryptographic protection are usually located within the SCADA system, which makes communication less secure. After doing a detailed analysis, that is what has been done based on these SCADA communication security issues as threads, vulnerable platforms, and non-compliant security policies and solutions analysis in SCADA communications. Security solutions have been successfully developed in the SCADA system and have succeeded in securing SCADA communications and providing research direction to address security issues that warm SCADA communications [3].

6 PROBLEM STATEMENTS: SCADA SYSTEM

The problem statement has been made from a detailed study, based on existing SCADA security issues such as threads/attacks and vulnerabilities. Several security issues and challenges have occurred in terms of existing SCADA implementations. According to the review analysis, there is no proper solution that communicates and solves SCADA to fully secure the security issues associated with them such as eavesdropping, data modification, data playback, key distribution, and other generic attacks [5][6].

According to the review, all existing solutions (generic safety solutions) are already based on the cryptographic method such as encryption, digital signature, and hashing algorithms for secure data or message communications between SCADA nodes [7].

SCADA communications have been vulnerable to several types of cyberattacks; rapidly increasing the connectivity of SCADA systems with IP-based or open standard protocols. Based on SCADA security, cryptographic solutions such as Symmetric and Asymmetrical have been used to achieve security service objectives such as data confidentiality, data authentication, data integrity, and non-denial functions, and long-term secure SCADA communications. SCADA systems are vulnerable to cyber-attacks. Several solutions exist to overcome the security associated with SCADA communications with limitations.

Four main components have been highlighted for SCADA security issues such as authenticity, availability, integrity, confidentiality. The SCADA system has reduced risk, gained control, and provided secure communication over attacks/threads using cryptographic solutions or modules [8]. Asymmetric and symmetric solutions are implemented in multiple networks and successfully achieve service security including authentication, integrity, non-repudiation, and confidentiality as the main part of SCADA security protection.

SSL / TLS and IP based security solutions have been implemented in several traditional network applications or/and network or SCADA communication protocols. SSL / TLS and IP based solutions have several communication and security issues, including running the Transport Control Protocol (TCP), based on cryptographic algorithms for security purposes and limited security mechanisms for non-repudiation functions and other advanced security features that are not available [9][10].

SCADA security issues such as the absence of proper authentication mechanisms for SCADA systems in terms of design and processing or operation of using proprietary or vendor protocols with open standard protocols (TCP / IP), belief in the concept of physical security, and degraded performance over the internet with multiple vulnerabilities. From this security issue; Cryptographic solutions such as asymmetric using the ECC algorithm and symmetrical using the AES algorithm have been implemented in end-to-end SCADA communications and achieve security services such as data confidentiality, data authentication, data integrity, and non-rejection functions. As "Schweitzer Engineering Laboratories, Inc." suggested that cryptographic solutions are the best approach to solve SCADA security problems during communication [11].

Based on the vulnerability of SCADA; homeland security (department) has been used as a cryptographic mechanism (solution) to secure critical infrastructure “Nation” from cyber-attacks / threads. In conclusion, cryptographic solutions are the best approach to secure or protect SCADA communications over the internet and successfully reduce risks [3] [12]. Advanced Encryption Standard (AES) 256, HMAC, and MD5 as part of the cryptographic solution have been implemented, to protect SCADA communications, while intrusion (anomaly) is detected by Intelligent Electronic Device (IED) as part of the substation controller [13][14] The

"American National Security Service" has suffered from potential attacks and hackers which are a serious problem for the critical infrastructure sector. Thus, it requires a solution that significantly secures critical infrastructure communications, when connected to an open standard network or protocol [15]. SCADA system vendors and developers only focus on functional parts of SCADA systems such as scalability, reliability, performance, and access control without security considerations. There is no general solution that meets the security requirements of a SCADA system. All functional performance of SCADA depends on security issues, if the SCADA system is completely secure then the overall system performance will be achieved [16].

SCADA system implementations using control protocols such as Distributed Network Protocol (DNP3), Fieldbus, Modbus, and other IP-based protocols are dangerous and essential for SCADA communication between field devices. This protocol has been designed without any security concerns which fully or partly protects against cyber-attacks and threads. Some firewalls are used between SCADA systems and corporate networks or the internet but cannot fully integrate with SCADA networks, such as in the case of SCADA protocols such as DNP3 or Modbus development and configuration. Thus, less information security and protocol configuration unconsciousness, which rapidly increases more vulnerabilities for the SCADA platform and causes major security issues for critical infrastructure [17][2].

DNP3 is the most important protocol used in SCADA systems. DNP3 uses almost all over the world; about 70% in America in electricity and water utilities and the remaining 30% in other parts of the world such as Europe, Asia, and Australia (TD, 2011). Secure DNP3 protocol or security implementation in DNP3 protocol, significantly increase the security of SCADA systems and reduce the potential for attacks and vulnerabilities in communications.

7 CONCLUSIONS

Detailed literature has been reviewed which is based on the deployment of Industrial Control Systems (ICS), its main architecture, and its importance in the industry. Security issues have been highlighted that warm-up communications and existing security mechanisms are also reviewed which are useful for protecting communications from attacks and making Industrial Control Systems (ICS) platforms that are secure from vulnerabilities. In future work, a strong cryptography-based security solution will be implemented to protect the Industrial Control System (ICS), when connecting with multiple open networks.

REFERENCES

[1] I. Silva, L. A. Guedes, P. Portugal, and F. Vasques, "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," *Sensors*, vol. 12, no. 1, pp. 806–838, 2012, doi: 10.3390/s120100806.

[2] S. Musa, Aa. Shahzad, and A. Aborujilah, "Secure Security Model Implementation for Security Services and Related Attacks Base on End-to-End, Application Layer and Data Link Layer Security," *Proc. 7th Int. Conf. Ubiquitous Inf. Manag. Commun. ICUIMC 2013*, 2013, doi: 10.1145/2448556.2448588.

[3] A. Shahzad, S. Musa, M. Irfan, and A. Aborujilah, "Industrial Control Systems (ICSs) Vulnerabilities Analysis and SCADA Security Enhancement Using Testbed Encryption," *Proc. 8th Int. Conf. Ubiquitous Inf. Manag. Commun. ICUIMC 2014*, 2014, doi: 10.1145/2557977.2558061.

[4] M. Raghini, N. Uma Maheswari, and R. Venkatesh, "Overview on Key Distribution Primitives in Wireless Sensor Network," *J. Comput. Sci.*, vol. 9, no. 5, pp. 543–550, 2013, doi: 10.3844/jcssp.2013.543.550.

[5] K. M. Anandkumar and C. Jayakumar, "Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks," *J. Comput. Sci.*, vol. 8, no. 10, pp. 1691–1699, 2012, doi: 10.3844/jcssp.2012.1691.1699.

[6] S. P. Manikandan and R. Manimegalai, "Survey on Mobile Ad Hoc Network Attacks and Mitigation Using Routing Protocols," *Am. J. Appl. Sci.*, vol. 9, no. 11, pp. 1796–1801, 2012, doi: 10.3844/ajassp.2012.1796.1801.

[7] W. S. Bhaya and S. A. AlAsady, "Prevention of Spoofing Attacks in the Infrastructure Wireless Networks," *J. Comput. Sci.*, vol. 8, no. 10, pp. 1769–1779, 2012, doi: 10.3844/jcssp.2012.1769.1779.

[8] S. Aris, A. Messai, M. Benslama, M. Nadjim,

and M. M-Elharti, “Integration of Quantum Cryptography through Satellite Networks Transmission,” *Am. J. Appl. Sci.*, vol. 8, no. 1, pp. 71–76, 2011, doi: 10.3844/ajassp.2011.71.76.

[9] G. D. Bhatt and J. H. Graham, “ACM-提高SCADA网络安全性.pdf,” pp. 7–10.

[10] B. Preneel, “Cryptographic Hash Functions: An Overview,” *Proc. 6th Int. Comput. Secur. Virus Conf. (ICSVC 1993)*, no. Icsvc 1993, p. 19, 1993.

[11] A. Risley, J. Roberts, and P. LaDow, “Electronic Security of Real-Time Protection and SCADA Communications,” *5th Annu. West. Power Deliv. Autom. Conf.*, 2003.

[12] A. M. Babu and K. J. Singh, “Performance Evaluation of Chaotic Encryption Technique,” *Am. J. Appl. Sci.*, vol. 10, no. 1, pp. 35–41, 2013, doi: 10.3844/ajassp.2013.35.41.

[13] Q. Zhang, H. Lu, N. Kawazoe, and G. Chen, “Pore Size Effect of Collagen Scaffolds on Cartilage Regeneration,” *Acta Biomater.*, vol. 10, no. 5, pp. 2005–2013, 2014, doi: 10.1016/j.actbio.2013.12.042.

[14] N. M. G. AL-Saidi, M. R. M. Said, and A. M. Ahmed, “Efficiency Analysis for Public Key Systems Based on Fractal Functions,” *J. Comput. Sci.*, vol. 7, no. 4, pp. 526–532, 2011, doi: 10.3844/jcssp.2011.526.532.

[15] J. Pollet, “Developing a Solid SCADA Security Strategy,” pp. 148–156, 2003, doi: 10.1109/sficon.2002.1159826.

[16] S. Rautmare, “SCADA System Security,” *India Conf.*, pp. 1–4, 2011.

[17] N. Cai, J. Wang, and X. Yu, “SCADA System Security: Complexity, History and New Developments,” *IEEE Int. Conf. Ind. Informatics*, pp. 569–574, 2008, doi: 10.1109/INDIN.2008.4618165.