International Journal of Internet, Broadcasting and Communication Vol.8 No.1 64-68 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.1.64

IJIBC 16-1-8

Sensors Network and Security and Multimedia Enhancement

Seon-mi Woo[1], Malrey Lee[2*]

[1] *JINI Co., Ltd, B-102, Technobill, 109 banryong-road, Deokjin gu, Jeonju, Chon Buk, Korea*
smwoo@chonbuk.ac.kr
[2*]*561-756,Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, Korea*
mrlee@chonbuk.ac.kr

Abstract

These fields are integrated to visualize and finalize the proposed development, in simulation environment. SCADA (supervisory control and data acquisition) systems and distributed control systems (DCSs) are widely deployed in all over the world, which are designed to control the industrial infrastructures, in real ways. To supervise and control the various parts of designed systems; trends to require a deep knowledge to understand the overall functional needs of industries, which could be a big challenge. Industrial field devices (or network sensors) are usually distributed in many locations and are controlled from centralized site (or main control center); the communication provides various signs of security issues. To handle these issues, the research contribution will twofold: a method using cryptography is deployed in critical systems for security purposes and overall transmission is controlled from main controller site. At controller site, multimedia components are employed to control the overall transmission graphically, such as system communication, bytes flows, security embedded parameters and others, by the means of multimedia technology.

Keywords: *Real Time Sensors Network, Industrial Control Systems, Supervisory Control and Data Acquisition, Distributed Control Systems, Cryptography.*

1. INTRODUCTION

Supervisory control and data acquisition (SCADA) systems are type of industrial control systems (ICSs) and have prominent placed in real time industries. SCADA systems are extremely highly distributed and controlling based systems, even dispersed over various remote locations in the world. In SCADA network system, numbers of geographical distributed stations are connected and controlled by designated main controller, the remote stations are may treated as field devices or sensor-devices. Each remote station and its processing is also managed and controlled by designated sub-controller, however, this is depends on requirements and size of

Manuscript Received: Dec. 12, 2015 / Revised: Dec. 30, 2015/ Accepted: Jan. 10, 2016
Corresponding Author: mrlee@chonbuk.ac.kr
Tel: +82-63-270-3993, Fax: +82-63-270-2394
Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University

remote station, meaning that, in case number of field devices are configure to collect real time status (or points) of electric generation and distribution so, there must required a sub-controller to manage and controller the overall network structure of local station. Each sub-controller is remote located and supervised by main controller; this is a form of distributed computing in which applications are distributed in several systems, but supervised from central controller (s) [1], [2].

Typically, SCADA system contains basic five components in its network setup including central controller or master terminal unit (MTU), one or more sub-controllers or remote terminal units (RTUs), communication

media, historian and human machine interface (HMI). Usually, MTU is designated as a main controller and located at main control center, RTUs or/and programmable logical controllers (PLCs) are treated as sub-controllers of SCADA system, which are connected with, and configured to collect information form field devices such as sensors and actuators, SCADA employed various form of communication media such as radio transmission, cable connections, satellite transmission and others, to collected the information from field device and monitor the overall network structure, the real time information is manipulated between MTU and RTUs or/and vice versa and simultaneously stored in historian or in data based (i.e., MySQL) and HMI is a form of graphical user interface that gives the facilities to configure the network setup, monitor the processing and automation, and visualizes the information of points changed and backup record of SCADA system. Nowadays, SCADA systems are connected with several advance networks and by employing of internet technology, the end-users and operators can view the SCADA processes and also may supervisor and control from electronic devices such as laptop, desktop computers, tablets, cellular phones and others[1], [3]. Figure 1visualizes the basic network structure of SCADA system.

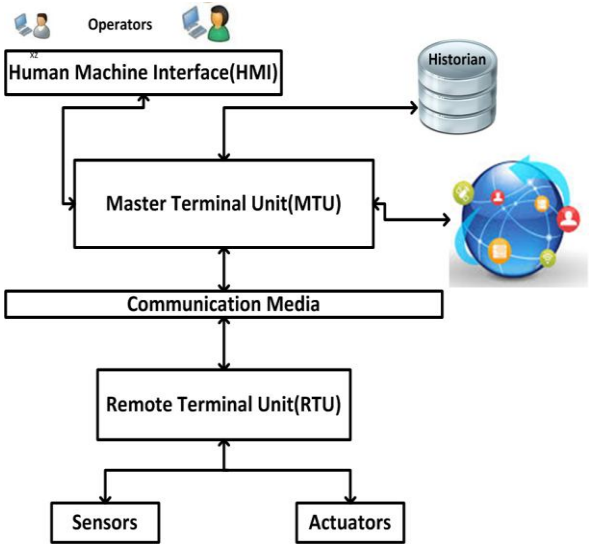

Figure 1. SCADA system

Distributed control system (DCS) is also a part of industrial control system (ICS) and employed to control the industrial productions such as electrical generation and distribution, water and wastewater distribution, oil refineries, and others, which are located in same place. In DCS system, production is carried by various localized controllers (or sub-controllers) and supervisory control loop (or main controller) is used, and placed centrally to carry the overall production that may distribute among various localized controllers. By employing of modularization in DCS, number of tasks is distributed to localize controllers and after processing, they are combined to carry the whole production [1]. As consequence, this is a good approach that distributes the system

load to many sub-controllers and overall production is controlled and monitored via supervisory control loop [1—4]. The basic distributed control system (DCS) is illustrated in figure 2.

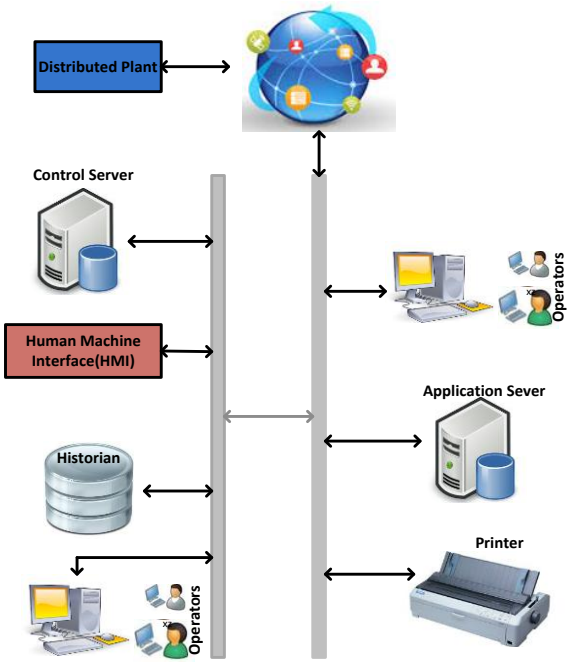

Figure 2. Distributed control system

In table 1, the potential attacks and vulnerabilities are accounted that have been usually resided in industrial control system (ICS) [1—8].

Table 1. Security Attacks and Vulnerabilities

Attacks	Vulnerabilities[1]
Integrity Attacks, Authentication Attacks, confidentiality Attacks, Non-Repudiation Attacks, Unauthorized Access Control, Bot-network operators, Criminal groups, Phishers, Spammers , Spyware/malware, etc.	Inadequate security policy , No formal ICS security Inadequate security architecture, Lack of security administrative, no security audits, Lack of configuration, No proper OS and application security, Lack of adequate password policy Inadequate access controls applied, Inadequate testing of security changes, Insecure remote access on ICS components, Use of insecure industry-wide ICS protocols, Incidents are not detected, Malware protection software not installed, Weak network security architecture, Poorly configured security equipment, Passwords are not encrypted in transit, Inadequate access controls applied, No security perimeter defined, Inadequate firewall and router logs, No security monitoring on the ICS network, Lack of integrity checking for communications, Authentication of users, Inadequate authentication between clients and access points, Inadequate data protection between clients and access points and others.

2. SECURITY DIRECTIONS

As consequence, number of vulnerabilities and security issues are accounted in transmission of industrial control system (ICS). At other side, security mechanisms are also used to defense or protect the communication

of ICS. Two generic solutions are identified for ICS that would be significant during security selection and design.

I. The end-to-end cryptography mechanisms and other commercial security software's are mean full, in case general industrial control system (ICS) security issues are considered.

II. ICS uses proprietary protocols that will further interact with non-proprietary protocols for internet message delivery. Therefore, the best solution is to employs security mechanism (or cryptography mechanism) as a part of proprietary protocols rather than depending on end-to-end mechanisms and commercial security software's.

3. CONCLUSION AND FUTURE WORK

This research will be employed the multimedia technology to visualize the industrial control system (ICS) communication in graphical senses, which made easy for system controllers or/and end-users to view and control; the bytes are flowed with implementation of security and also visualized to better understand able for end-user purposes. The attacks influence is usually high in critical systems due to their operations or/and connection orientation, over physical link. In proposed study, security via cryptography will be implemented and accounted as a part of critical systems, which protects the ICS transmission over physical channel against attacks. For assessment and validation purposes, the mathematical flows would be generated for each operation during whole payload design and security deployment in ICS.

ACKNOWLDEGEMENT

This work (Grants No: 1401001175) was supported by Business for Academic-industrial Cooperative establishments funded Korea Small and Medium Business Administration in 2015.

REFERENCES

[1] Stouffer, J. Falco, K.Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security," Recommendations of the National Institute of Standards and Technology, 2006

[2] H.Chae, Shahzad. A, M.Irfan, H.Lee, M.Lee, "Industrial Control Systems Vulnerabilities and Security

[3] Issues and Future Enhancements," Advanced Science and Technology Letters Vol.95 (CIA 2015), pp.144-148, http://dx.doi.org/10.14257/astl.2015.95.27

[4] S. Musa, A. Shahzad, A.Aborujilah, "Secure security model implementation for security services and related attacks base on end- To-end, application layer and data link layer security," Proceeding ICUIMC '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, doi: 10.1145/2448556.2448588

[5] Aamir Shahzad, Kalum Priyanath Udagepola, Young-keun Lee, Soojin Park, and Malrey Lee, "The Sensors Connectivity within SCADA Automation Environment and New Trends for Security Development during Multicasting Routing Transmission," International Journal of Distributed Sensor Networks, Article ID 738687..

[6] Sugwon Hong; Myongho Lee, "Challenges and Direction toward Secure Communication in the SCADA System," Communication Networks and Services Research Conference (CNSR), 2010 doi: 10.1109/CNSR.2010.52

[7] A. Shahzad, S. Musa, M. Irfan, "N-Secure Cryptography Solution for SCADA Security Enhancement," Trends in Applied Sciences Research, 2014, 9: 381-395 doi:10.3923/tasr.2014.381.395

[8] HyungJun Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2012, Article ID 268478, pp.10

[9] 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