SCADA 네트워크 보안 이슈

김학만, 강동주
한국전기연구원

Security Issues in SCADA Network

Hak-Man Kim, Dong-Joo Kang
KERI

Abstract - SCADA (Supervisory Control and Data Acquisition) system has been used for remote measurement and control on the critical infrastructures as well as modern industrial facilities. As cyber attacks increase on communication networks, SCADA network has been also exposed to cyber security problems. Especially, SCADA systems of energy industry such as electric power, gas and oil are vulnerable to targeted cyber attack and terrorism. Recently, many research efforts to solve the problems have made progress on SCADA network security. In this paper, we introduce recent security issue of SCADA network and propose the application of encryption method to Korea SCADA network.

1. Introduction

SCADA (Supervisory Control and Data Acquisition) system is a system operation with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment [1]. Recently Intelligent Electronic Device (IED) which is control unit having communication function with master station is replacing the role of RTU.

SCADA system has been used for remote measurement and control on the critical infrastructures such as electric power, gas and oil as well as modern industrial facilities such as chemical factories, manufacturing facilities. SCADA network has been exposed to cyber security problems with IT advancement and network growth. Especially, SCADA systems of energy industry such as electric power, gas and oil are vulnerable to targeted cyber attack and terrorism. Recently, research efforts to solve the problems have been progressed throughout the world.

we introduce recent security issue of SCADA network and propose the application of encryption method to Korea SCADA network.

2. SCADA System Security

SCADA systems have been used for remote measurement and control for many industrial applications. A SCADA system allows an operator to make set-point changes on distant process controllers, to open or close valves or switches, to monitor alarms, and to gather measurement information from a location central to a widely distributed process, such as groups of small hydroelectric generating stations, oil or gas production facilities, pipelines for gas, oil, chemicals and water, electrical power systems and so on [1].

2.1 System Configuration

A general SCADA system is composed of human operat ors, Man Machine Interfaces (MMI), Master Terminal Units (MTU), communication means and Intelligent Electronic De vices (IED) or remote terminal units (RTU). The IED is a type of control element, which includes sensors, relays, and control blocks / terminals with communication functions. Co mmunication methods between the MTU and IED or RTU include radio, leased line, landline, microwave, etc. Figure 1 shows the general configuration of a SCADA network in electrical power systems.

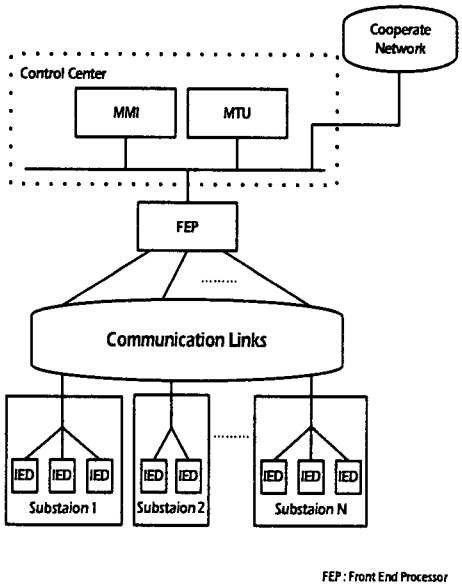

Fig. 1. SCADA system configuration

2.2 SCADA Network in Korea Power System

Fig. 2 shows configuration and communication protocols and of SCADA in Korea power system. Central SCADA communicates with RCC SCADA using TCP/IP protocol. TCP/IP protocol is also used in the communication between RCC SCADA and SCC SCADA. EMS (Energy Management System) uses ICCP to communicate with RCC SCADA. ICCP is the acronym of Inter-Control Center Communication Protocol which is one of the global standard communication protocols for wide area communication between centers of the electric power transmission network such as power plants and network

control centers and substations[2]. ICCP is useful for the communication between control centers which transmit and receive a large scale of data periodically like real time measurement and control data.

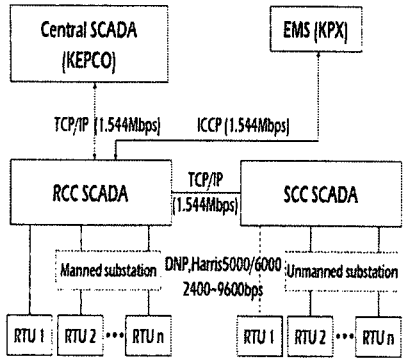

Fig. 2. Communication protocols of Korea SCADA

It is possible for different systems provided by various vendors to communicate each other and to be integrated into one entire system. RCC and SCC communicate with RTU or IED using DNP or Harris protocol. DNP is also telecommunication standard with ICCP, which defines communication between master stations, RTUs and other IEDs.

Currently the SCADA system of Korea network only use its private network not connected to Internet for the communication, and has not considered any measure for the security. We just focus on the cyber security of the private network of Korea in this paper, although it is expected to be integrated into other networks or Internet sooner or later.

2.3 SCADA System Vulnerability

The use of IT within SCADA systems of critical infrastructures such as electric power, gas and oil transportation systems has made them exposed to cyber security problems and the have been targeted by cyber attacks and terrorism. According to [3] and [4], cyber risk of SCADA systems has been increased by the following:

The adoption of standardized technologies with known vulnerabilities, such as the use of common operating systems, like Microsoft Windows and UNIX, in SCADA and control system platforms

The connectivity of SCADA systems to other networks by demand from corporate users for operational data on a near-real-time basis, etc.

Insecure remote connections

The widespread availability of technical information about SCADA system

The increased use of TCP/IP communication

The general attack types of SCADA systems are the following [5]:

Denial of service attacks by delaying or blocking the flow of information through control networks

Unauthorized changes made to programmed instructions in IEDs at remote sites, resulting in damage to equipment, premature shutdown of processes, or even disabling control equipment

False information sent to control system operators to disguise unauthorized changes or to initiate inappropriate actions by system operators

Modification of the control system software, producing unpredictable results

Interference with the operation of safety systems

2.4 Challenges for SCADA Security Enhancement

There is firewall that is a basic function for security in Korea SCADA Network. Firewalls are depend on Protocol types. The firewalls in Korea SCADA Network were not designed to DNP or Harris protocols. So, there are risks in Korea SCADA Network.

There are many types of Security tools such as followings;

Access control

Firewalls and intrusion detection systems

Crytography and key management

OS security, etc.

Among the upper tools, crytogrphy and key management is the most common and powerful approach to securing the system. So, we suggest crytography application to Korea SCADA network ahead of upper other tools.

3. Conclusions

Cyber security problems of SCADA network of power systems are very important against cyber attack and terrorism. Recently, researching efforts to resolve the problem are accelerating and bringing the improvement.

There is firewall that is a basic function for security in Korea SCADA Network. Firewalls are depend on Protocol types. The firewalls in Korea SCADA Network were not designed to DNP or Harris protocols. So, there are risks in Korea SCADA Network. So, we suggest crytography application for enhancing Korea SCADA network security.

We are going to do more studies on mathematical formulation for security function or economic investments.

Reference

[1] Stuart A. Boyer, "SCADA: Supervisory Control and Data Acquisition", 2nd Edition, Instrument Society of America, 1999.

[2] Dacfey Dzung, Mario Crevatin, "Security for Industrial Communication Systems", Proceedings of the IEEE, 2005

[3] Thomas Kropp, "System Threats and Vulnerabilities - An EMS and SCADA Security System Overview", IEEE Power and Energy Magazine, March, pp.46-50, 2006.

[4] GAO-04-628T, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. Testimony before the Subcommittee on Technology Information Policy", Intergovernmental Relations and the Census, House Committee on Government Reform, March, 2004.

[5] Yongge Wang and Bei-Tseng Chu: sSCADA, " Securing SCADA Infrastructure Communications", August, 2004.

[6] William Stallings, "Cryptography and Network Security - Principles and Practices", Pearson International Edition, 2006.

[7] Ronald L. Krutz, "Securing SCADA Systems", Wiley Publishing Inc., Indiana, 2006.