Analysis on Cyber Threats to SCADA systems

Dong-Joo Kang, *Researcher, KERI*, Jong-Joo Lee, *Senior Researcher, KERI,* Seog-Joo Kim, *Principal Researcher, KERI, and* Jong-Hyuk Park, *Professor, Kyungnam University*

***Abstract*—SCADA is the acronym of Supervisory Control and Data Acquisition, which is a communication technology scheme for collecting data from distant facilities and also controlling them on control systems. By SCADA technology it is not necessary to assign operators to remote locations for operating the facilities there. In the beginning SCADA system was locally introduced, and it has been applied to larger and wide-area systems as the information technology evolves. As SCADA system expands to wide area, it has been connected to common communication infrastructure while it was a locally independent control system network initially. Since the Internet came up, all different kinds of communication networks have been being integrated into the Internet for both technological and economic efficiencies. But it also causes the SCADA system to be revealed to the cyber security risks common on the Internet at the same time. Today many major utility services are provided on SCADA networks, so it is very critical to protect the system from those risks. The damage would be very serious if one of the SCADA systems are attacked and thereby stop normal operation, therefore it should be considered to take countermeasures against the threats. Cyber security problem requires multi-directional approach considering many different aspects of vulnerabilities in the system. This paper analyzes the SCADA network vulnerabilities on the aspects of cyber security.**

***Index Terms*—SCADA, wide-area control system, cyber security, vulnerabilities, encryption, security device**

I. Introduction

SCADA technology is widely used for process monitor and control of production, transmission, and distribution in many different fields. 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 widely distributed process, such as an oil or gas field, pipeline system, or hydroelectric generating complex [1]. SCADA systems were originally local to a site to control the control system in that, and used its own network for control communication. However it has extended to wide-area for supervisory control and monitor as the information technology evolves, which requires the interconnection between systems and networks both on economic and technological aspects. With the reasons local networks started to be connected with each other and finally to the Internet for the extension of SCADA systems. Some of SCADA networks like in electric power industry still remain as independent networks disconnected from the Internet for its security reasons. But it is a mega-trend that different networks are integrating into the Internet for the advanced control and automation based on intelligent IT system. There are always good and bad aspects at the same time. The efficiency improvements based on network integration brought the cyber security risks into the control systems of critical infrastructures operated by SCADA system. Compared to IT networks, control systems might be more vulnerable to cyber attacks for its characteristics of the real time operation. Tab. 1 shows the comparison of characteristics between information systems and control systems.

TABLE I
Information system vs. control system

Information System	Control System
Not real-time	Real-time basis
Correctness of Information	Response time is critical
Delay Allowed	Big problems caused by delay
Planned Tasks	Sequential Tasks
Data integrity is important	User's security is important
Task Loss by data corruption	Economic loss or casualties
Restoration by re-booting	Continuous operation required

II. Topologies of SCADA networks

SCADA system is largely composed of three parts which are master terminal units (MTU), remote terminal unit (RTU), and communication links connecting two terminals. A MTU may have at least one RTU or more than one, and communicates with them through several different kinds of communication media. Media or methods for communication could be different depending on the purpose of communication, the size of data, the required speed, etc.

SCADA devices are interconnected by communication links such as optical fiber, radio, telephone line, microwave, satellite, or Ethernet. The IEEE standard C37.1-1994 specifies the communication topologies used in SCADA. They vary from simple a point-to-point to composite architectures with one single master station, multiple sub-master (slave master) stations and multiple RTUs [2]. Fig. 1 shows several patterns of communication link topologies between masters and slaves (RTUs).

The topology of SCADA network depends on the objective and characteristics of the controlled system such as the control

Dong-Joo Kang is with Korea Electro-technology Research Institute, Uiwang-city, Gyeonggi-province, Korea (e-mail: djkang@keri.re.kr).

Jong-Joo Lee is with Korea Electro-technology Research Institute, Uiwang-city, Gyeonggi-province, Korea (e-mail: jongjoo@keri.re.kr).

Seog-Joo Lee is with the Korea Electro-technology Research Institute, Uiwang-city, Gyeonggi-province, Korea (e-mail: sjkim@keri.re.kr).

Jong-Hyuk Park is with the the Department of Computer Science and Engineering, Kyungnam University, Korea (e-mail: hyuks2005@paran.com).

governance, the data type, the required communication speed, etc. The radial structures of ② and ③ in Fig. 1 are mainly used for SCADA systems of utility services especially in electric power industry which is our main concern in this paper.

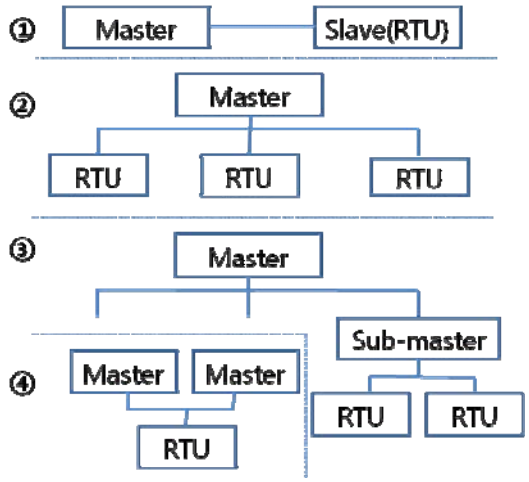

Fig. 1. Communication link topologies in SCADA system

III. Protocols for SCADA Communication

SCADA and other control systems have several standards for their data communication, called protocols. They define physical media, communication procedures, data frame, etc. In order for any entities to communicate, a protocol for that communication has to be established. The SCADA system protocols evolved from propriety hardware and software designed specifically for SCADA systems. The protocols were developed out of necessity to serve the burgeoning market for computer application in real time control situation [3]. Over the past three decades, several hundred of these protocols have been developed for both serial, LAN and WAN based communications in a wide variety of industries including petrochemical, automotive, transportation and electrical generation/distribution. Approximately 10 protocols currently dominate the industrial marketplace and include systems such as MODBUS, DNP3, EtherNET/IP, PROFIBUS and Foundation Fieldbus [4]. Among the above protocols, DNP3 was designed specifically for SCADA, and thereby it has been widely accepted in many industries including the electric power industry.

IV. Potential Threats to SCADA System

IT has been evolving day by day and impacting many other industries. It has improved the productive efficiency in traditional manufacturing sectors and also creating new area of service industries. The application of new technologies to the control systems brought wide-area monitor and control functions to utility services, which has been evolved into SCADA system today. As SCADA systems get larger, they necessarily became connected to other common networks for both economic and technological reasons, which have been finally integrated into the Internet. However this advancement on technology also accompanied new kinds of threats to the industry. The SCADA systems also became revealed to cyber attacks, and thereby the critical infrastructures operated by the SCADA system are also in danger. In this situation it is very important to define and classify the potential risks by the threats for building countermeasures against them.

The most famous threats in this day and age are the threats posed by terroristic groups and hostile nation states. These are organized groups with a clear goal and some level of sophistication. There is also a threat posed by a company's own employees. Company insiders have access to internal controls and data, and either by accident or malicious intent can cause equipment outages. A third category of threat is the threat posed by casual hackers, known as "script kiddies" [5]. When considering the closed characteristics of SCADA system in electric power industry compared to others, 1st and 2nd threats are comparatively probable threats. But the SCADA systems connected to the Internet in the States already have had experiences of being threatened by script kiddies.

A. SCADA system Assets

IT cyber security is concerned with the confidentiality, integrity and availability of information and data assets. Control system and value chain cyber security extend these assets to include equipment and materials that could be manipulated by access to control system and value chain computer system [6]. Therefore the assets to be protected include not only IT based SCADA communication networks but also all physical facilities in the electric power system controlled and operated by the IT infrastructure.

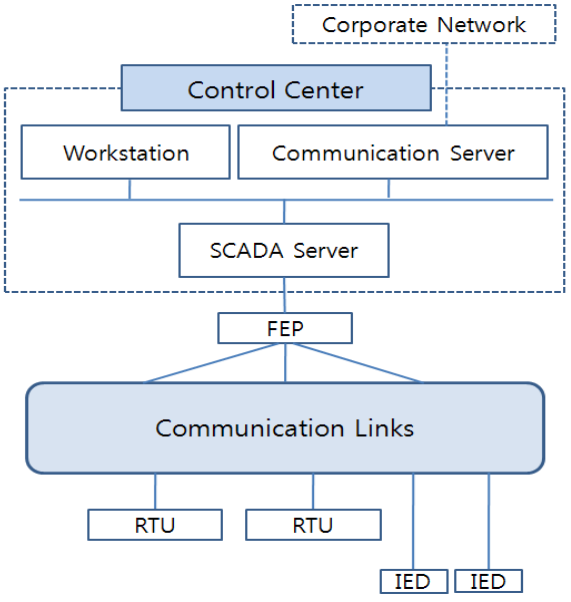

Fig. 2. SCADA system configuration

B. Investigation on Threat Types

"Threat" is commonly, although not consistently, defined as: Threat = Capability + Intent + Opportunity. From the analytic perspective, the definition assumes the existence of a threat "source" – an actor or agent posing the threat. For many reasons, the vulnerability assessment process is developing at a faster pace than the threat assessment process. While vulnerability assessment aids in estimating the capability factor in the threat equation, satisfactory assessment of Intent and Opportunity is more difficult [7]. In spite of the difficulties it is very important and necessary to define and classify the concrete threats and vulnerabilities for building security countermeasures for protecting the SCADA system from them. Therefore it is required to specify the threats at least on the qualitative level before quantitative measurements, which is the main focus of this paper.

Massoud Amin in EPRI defined three different kinds of threats related to power systems as follows [8]:

- *Attacks upon the power system*. In this case, the electricity infrastructure itself is the primary target-with outages rippling into the customer base. The point of attack could be a single component – a critical substation or transmission tower. Or there could be a simultaneous, multipronged attack intended to bring down an entire regional grid. Similarly the attack could target electricity markets, highly vulnerable because of their transitional status.
- *Attacks by the power system*. Here, the ultimate target is the population, using parts of the electricity infrastructure as a weapon. Terrorists could use power plant cooling towers, for example, to disperse chemical or biological agents.
- *Attacks through the power system*. The target is the civil infrastructure in this case. Utility networks include multiple conduits for attack, including lines, pipes, underground cables, tunnels, and sewers. For example terrorists could couple an electromagnetic pulse through the grid to damage computer or telecommunications infrastructure.

Among three categories 1st one is related to cyber security while the 2nd and 3rd ones are more close to the area of physical security. Cyber security problems on SCADA networks are introduced from the information networks as the networks are integrated with each other. But some of problems are caused by human physical access with the application of general cyber attack method on IT networks to SCADA or control system networks. This could be understood as cyber attack based on physical access. If the SCADA network is disconnected from other networks or the Internet, the physical access is prerequisite to attack the system, one example of which is tapping the line on communication links between a SCADA server and RTUs in Fig.2. The physical access to a point of SCADA network might not be that difficult because the network is a huge system whose facilities are dispersed over a wide range of area.

Many threats in communication networks are also applied to SCADA systems since they are connected to each other directly or indirectly. It is strongly believe that many SCADA systems are exclusive to other networks, but it has been proved many times that they are indirectly connected to the Internet through the facilities for on-line maintenance. Threats to SCADA systems are classified into many kinds according to [9] as shown in Table 2.

TABLE II
Common RT Computer System Threats

1.Authorization Violation	9.Information leakage	17.Sabotage	25.Traffic Analysis
2.Bombs (Logic or Time)	10.Intercept/ Alter	18.Scavenging	26.Trap Door/ Back Door
3.Browsing	11.Interference Database Query Analysis	19.Spying	27.Trojan Horse
4.Bypassing Controls	12.Masquerade	20.Service Spoofing	28.Tunneling
5.Data Modifications	13.Physical Intrusion	21.Sniffers	29.Unauthorized Access Violations of Permission
6.Denial of Service	14.Replay	22.Substitution	30.Unauthorized Access Piggybacking
7.Eavesdropping	15.Repudiation	23.Terrorism	31.Virus
8.Illegitimate Use	16.Resource Exhaustion	24.Theft	32.Worm

The treats elaborated in table 2 could be mapped into Fig.2 as shown in Fig.3. There might be other types of attacks and vulnerabilities, and combinations of them different from the concept proposed in Fig.3, which is going to be dealt with in future studies.

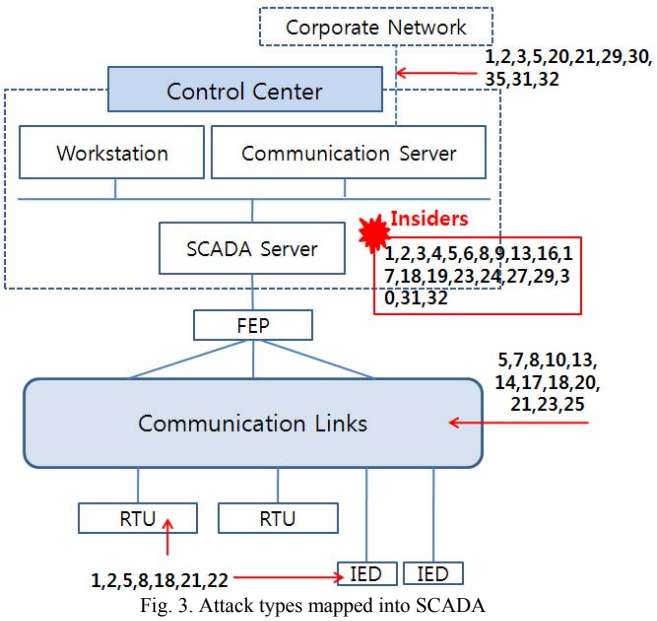

Fig. 3. Attack types mapped into SCADA

It has been not that long since the cyber security issues on SCADA system came on. Some people even believe that SCADA system is not involved in cyber security problem because it is a isolated system disconnected from the Internet. In fact many SCADA systems are still operated as a private network while others are already connected to or have used the Internet as their main communication link. However, even an isolated SCADA network might have also indirect routes to the net by SCADA facilities on the SCADA network because many facility vendors keep maintenance activities on their products by monitoring them based on the internet connection. So various vulnerability points should be investigated and analyzed to specify possible attack routes or scenarios to the SCADA system.

V. Conclusion

SCADA system is a kind of new variable having started to be connected into the internet according to the network integration. It is strongly related to our daily life, therefore the normal operation of the system is very critical and that is the reason why the system should be strongly secured. The recent movie "Diehard4.0" also dealt with the cyber security issues on SCADA systems and its impacts when it fails by hostile hackers' attack. However the study is still in the beginning stage although people started to pay attention to the issue. There are several reasons for the slow progress on the study. One of the representative one is the lack of recognition on cyber security of SCADA system. As stated above even the managers and workers on that field think the system is isolated and thereby it is safe while the reality is different. However the risk is real and many hacking incidents already happened on SCADA network. Therefore it is very critical to build the countermeasures against potential threats. The priority is to analyze and define the vulnerability points of the system and possible attack types based on the results. This paper is a try to specify the threats to SCADA system based on general cyber threats on communication networks.

VI. References

[1] Stuart A. Boyer, "SCADA-Supervisory Control and Data Acquisition, 2-nd Edition" *Instrument Society of America7*, 1999.

[2] Edward Chikuni, Maxwell Dondo, Investigating the Security of Electrical Power Systems SCADA, *AFRICON 2007*, pp. 1-7, 26-28 September, 2007

[3] Ronald L. Krutz, *Securing SCADA Systems*, Wiley Publishing, Inc., 2006

[4] Eric J. Byres, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", *International Infrastructure Survivability Workshop (IISW 2004)*, 2004

[5] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development", *Power Symposium, 2006. NAPS 2006. 38th North American*, pp.483-488, Sep. 2006

[6] Paul Baybutt, "Comprehensive Cyber Security Vulnerability Analysis for Manufacturing Plants", *Hydrocarbon Engineering*, vol. 10, No.1, pp. 12-18, Jan. 2005

[7] Peter D. Gasper, Cyber Threat to Critical Infrastructure – 2010-2015, *Information & Cyberspace Symposium*, Sep.2008

[8] Amin Massoud, "Security Challenges for the Electricity Infrastructure", *Special Issue of the IEEE Computer Magazine on Security and Privacy*, April 2002: 8-10

VII. Biographies

Dong-Joo Kang was born in Busan in Korea, on September 9, 1975. He graduated from Hong-ik University for his bachelor's and master's degrees on electrical engineering. He has been working for KERI (Korea Electro-technology Research Institute) since 2001. His research interests are on electric power system operation, electricity markets, optimization, operation research, SCADA, cyber security, etc.

Jong-joo Lee was born in Seoul in Korea, on November 27, 1975. Received his B.S degree from the University of Suwon, Korea, in 1999. He received an M.S. degree from Sungkyunkwan University, Korea, in 2002. From 2002 to 2004 he was a senior researcher at SATURN Information & Communication Co., Ltd, Korea, and from 2004 to 2007 he was a senior researcher at Sungkyunkwan Univ, Regional Innovation Center. He received an Ph.D. degree from Sungkyunkwan University, Korea, in 2008. He has been working for KERI (Korea Electro-technology Research Institute) since 2008. His research interests are on protective digital relay, digital signal processing, embedded system, SCADA, cyber security, etc.

Seog-Joo Kim received PhD degree in electrical and electronic engineering from Yonsei University. Since 1987, he has been working for KERI, and is currently with smart grid center. His research interests include the design and implementation of highly reliable embedded controllers and communication networks, power system control and cyber security for power systems.

Jong-Hyuk Park received his Ph.D. degree in Graduate School of Information Security from Korea University, Korea. Before August, 2007, he had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. He is now a professor at the Department of Computer Science and Engineering, Kyungnam University, Kore a. His research interests include Digital Forensics, Security, Ubiquitous and Pervasive Computing, Context Awareness, Multimedia Service, etc. He is a member of the IEEE, IEEE Computer Society, IEEE Communications Society, KICS, KIISC, KMMS, KDFS and KIIT.