J Electr Eng Technol.2015; 10(3): 888-894
http://dx.doi.org/10.5370/JEET.2015.10.3.888

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

# Towards Cyber Security Risks Assessment in Electric Utility SCADA Systems

**Pil Sung Woo*, Balho H. Kim* and Don Hur†**

**Abstract** – This paper presents a unified model based assessment framework to quantify threats and vulnerabilities associated with control systems, especially in the SCADA (Supervisory Control and Data Acquisition) system. In the past, this system was primarily utilized as an isolated facility on a local basis, and then it started to be integrated with wide-area networks as the communication technology would make rapid progress. The introduction of smart grid, which is an innovative application of digital processing and communications to the power grid, might lead to more and more cyber threats originated from IT systems. However, an up-to-date power system often requires the real-time operations, which clearly implies that the cyber security would turn out to be a complicated but also crucial issue for the power system. In short, the purpose of this paper is to streamline a comprehensive approach to prioritizing cyber security risks which are expressed by the combination of threats, vulnerabilities, and values in the SCADA components.

**Keywords**: Asset value, Cyber security, Risk, SCADA (Supervisory Control and Data Acquisition) system, Threat, Vulnerability

## 1. Introduction

According to SANS (SysAdmin, Audit, Networking, and Security) Institute, vulnerabilities would be described as the gateways by which the constantly evolving attacks or threats are manifested [1]. They can best be compared to security holes that would allow unauthorized access. The extent of hazards seems to hinge on how many vulnerabilities are discovered in a system. If a wide range of threats has matured and security weaknesses have not been detected, such offenses are unlikely to have substantial impacts on the asset or facility. That is, flaws in security should be accounted for by the system to evaluate the most serious consequences of actual exposures invoked. Therefore, the vulnerability assessment is fairly linked to a series of activities to find out these weaknesses for preventing the system compromise.

Particularly, in the power system or smart grid consisting of various hierarchies and components, this vulnerability assessment may be more prone to the qualitative property in nature. Nevertheless, the realistic and effective measures would be taken simply by spelling out weaknesses in security and examining them in terms of quantitative aspects. This paper is intended to define criteria on the vulnerability assessment for physically separated individual system components and demonstrate the quantitative scheme as an evaluation tool, thereby providing the framework to help facilitate the consistent decision making of information security professionals.

† Corresponding Author: Department of Electrical Engineering, Kwangwoon University, Seoul, Korea. (dhur@kw.ac.kr)
* School of Electronic and Electrical Engineering, Hongik University, Seoul, Korea. (woopilsung@gmail.com, bhkim@hongik.ac.kr)
Received: October 23, 2014; Accepted: January 26, 2015

## 2. Detailed Formats of Manuscript

The vulnerability assessment is performed in very diverse industrial fields, such as information technology system, energy supply system, water supply system, and transportation system [2]. The interruption cost assessment in the electric power industry may be regarded as one of the examples for the vulnerability assessment inasmuch as both the outage rate and the outage cost are taken into account. In the assessment processes, it is profoundly difficult to exactly articulate and sort out the same vulnerabilities as they are sometimes listed repeatedly by different names, depending on institutions or manufacturers.

A system compromise, a threat, can be realized through the weakness or vulnerability in a system. In this sense, the vulnerability may be recognized as a parameter or a filter to set the relationship between threats and assets. If we define the risk as the financial losses of the damaged system, it is mathematically formulated by (1) when the quantified threats are denoted by $T$, the quantified vulnerabilities by $V$, and assets by $A$. Here the asset can be interpreted as the value or worth of the system under the cyber attack.

$$R = T \times V \times A \tag{1}$$

### 2.1 Analysis of cyber threats in SCADA system

Over the past few decades, vulnerabilities as well as

cyber threats in the conventional information technology system have been steadily manipulated with real-life cases. Among them, some could be tapped into the power system without further modifications while the others might be filtered out or magnified in certain circumstances. For instance, more or less delays in the communication are allowed in the information technology system and otherwise similar phenomenon in the power system would result in a devastating blackout, threatening the control operation itself. First, cyber threats in the existing information technology system need to be investigated and seen whether these are possibly applied to the power system.

The information system and the control system are evidently identified in the light of protocol. Thus the critical attacks tend to be differentiated by the kind of protocol so that they should be tackled based on this hypothesis. The threats may either differ in the physically separated components or be governed by the protocol in use, irrespective of components. The attacks on components are targeted at individual systems whereas those on protocol are directed to the network.

The SCADA (Supervisory Control and Data Acquisition) system may be usually classified into global and local systems. Also, these systems may be grouped into the TCP/IP protocol region and the serial (DNP and Modbus) protocol region. As illustrated by Fig. 1, this system is composed of server, communication infrastructure in an intermediate stage, and terminal digital devices. In the general network, the upper part is implemented with the TCP / IP protocol and the lower part is equipped with the serial communication network. Under the basic structure of the SCADA system, security threats of the already established information technology system are briefly summarized in Table 1 [3]. Moreover, they are divided by three categories, which would be reliant on the location of damages incurred by external attacks. The threats of the information technology system would still affect the upper TCP / IP based network whilst errors by inherent vulnerabilities of the serial protocol can occur at the lower network.

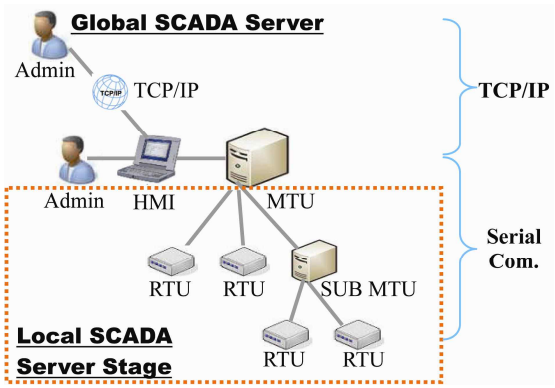


**Fig. 1.** Basic structure of the SCADA system

**Table 1.** System components and cyber threats

| Cyber Threats \ Components | | SCADA Server | Com. Infra | | RTU & Device |
|---|---|---|---|---|---|
| | | | TCP/IP | Serial | |
| Confidentiality | Eavesdropping | $V_{0101}$ | $V_{0102}$ | $V_{0103}$ | $V_{0104}$ |
| | Traffic Analysis | $V_{0201}$ | $V_{0202}$ | $V_{0203}$ | $V_{0204}$ |
| | EM/RF Interception | $V_{0301}$ | $V_{0302}$ | $V_{0303}$ | $V_{0304}$ |
| | Indiscretions by Personnel | $V_{0401}$ | $V_{0402}$ | $V_{0403}$ | $V_{0404}$ |
| | Media Scavenging | $V_{0501}$ | $V_{0502}$ | $V_{0503}$ | $V_{0504}$ |
| In + Con | Trojan Horse | $V_{0601}$ | $V_{0602}$ | $V_{0603}$ | $V_{0604}$ |
| | Trapdoor (Backdoor) | $V_{0701}$ | $V_{0702}$ | $V_{0703}$ | $V_{0704}$ |
| | Service Spoofing | $V_{0801}$ | $V_{0802}$ | $V_{0803}$ | $V_{0804}$ |
| Integrity | Masquerade | $V_{0901}$ | $V_{0902}$ | $V_{0903}$ | $V_{0904}$ |
| | Bypassing Controls | $V_{1001}$ | $V_{1002}$ | $V_{1003}$ | $V_{1004}$ |
| | Authorization Violations | $V_{1101}$ | $V_{1102}$ | $V_{1103}$ | $V_{1104}$ |
| | Physical Intrusion | $V_{1201}$ | $V_{1202}$ | $V_{1203}$ | $V_{1204}$ |
| | Replay | $V_{1301}$ | $V_{1302}$ | $V_{1303}$ | $V_{1304}$ |
| | Theft & Illegitimate Use | $V_{1401}$ | $V_{1402}$ | $V_{1403}$ | $V_{1404}$ |
| Availability | Denial of Service | $V_{1501}$ | $V_{1502}$ | $V_{1503}$ | $V_{1504}$ |

## 2.2 Analysis of vulnerabilities in SCADA system

The cyber threats in Table 1 will have considerable effects on the risks of the overall SCADA system due to vulnerabilities. The grayed cells in Table 1 indicate the vulnerabilities involved in de facto risks. Besides, these vulnerabilities are given by the statistical probabilities or estimates. As there are no possibilities to be harmed in the remaining uncolored cells, the corresponding vulnerabilities are numerically reduced to zero. The vulnerability may be interpreted by the probability when the threats work on a specific portion of assets. Ultimately, it ranges between 0 and 1.

## 2.3 Analysis of assets in SCADA system

It is pretty difficult to evaluate the value of the asset. The asset in the information technology system refers to not only the tangible hardware asset including the network equipment but the intangible asset, for example, software and knowledge information [4]. Once the information asset becomes part of the system, its value does not merely mean a purchase price of the facility or the depreciated economic value.

The additional outcomes arising from the damage must be reflected given that this damage may be provoked by the violation of the security at the information asset. More important, nonetheless, is the above issue in the SCADA system as the information asset is closely related to the neighboring information asset and the power system. The value of the asset in the power system, namely $A$ in (1), would consequently converge to the expected outage cost when the corresponding information technology facility was attacked. The attacks against the individual RTUs would aggravate the reliability of the corresponding region

and possibly influence the nation unless we take immediate actions on these disturbances.

### 2.4 Formulation of computing risks in SCADA system

We will replace (1) with the following equation on the basis of 15 threats described in the previous subsection. In the element $T_{ij}$, the row $i$ ($i$ = 01, 02, 03, 04) represents the components in the SCADA system, i.e., SCADA server, TCP/IP network, serial network, RTUs and device while the column $j$ ($j$ = 01, 02,…, 15) designates the type of external threats in Table 1. In (2), the element $V_{ji}$ stands for the vulnerability of the component $i$ against the attack $j$. Plus, $R_n$ is the risk in monetary value when the cyber threats have penetrated into the asset $n$.

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} \sum_{j=01}^{15} T_{01j}V_{j01} & 0 & 0 & 0 \\ 0 & \sum_{j=01}^{15} T_{02j}V_{j02} & 0 & 0 \\ 0 & 0 & \sum_{j=01}^{15} T_{03j}V_{j03} & 0 \\ 0 & 0 & 0 & \sum_{j=01}^{15} T_{04j}V_{j04} \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \tag{2}$$

$$A_n = \sum_{k=1}^{K} \left( LV_n^k + OC_n^k \right) \tag{3}$$

In (3), the value ($A_n$) that the n-th facility as the information asset in the SCADA system is expected to have would comprise the lost value ($LV_n$) of the information asset and the outage cost ($OC_n$) owing to the removal of this asset. Here the superscript $k$ was adopted to assume that the n-th facility would be made up of several subcomponents.

## 3. Estimation of Numerical Data

The significant concepts in security, threats and vulnerabilities, are thought to be quantitative. Hence it is indeed vital in the establishment of the assessment model to map these properties onto their quantitative values. As Burris pointed out, the reason why it was somewhat troublesome to model the occurrences of security accidents quantitatively was largely because of the fact that sudden happenings might not necessarily be mitigated by defense robustness. To put it in a nutshell, the accidents may not take place in a loose defense system and at the same time, they may come about in a very tight security system. Eventually, a stroke of luck plays the leading role in security problems [5]. In this context, this section has to be preceded prior to calculating the risks algebraically by ranking the relative extent of damage with respect to 15 cyber threats and 4 components of the SCADA system in 3 buses as well as the potential vulnerabilities.

### 3.1 Quantification of cyber threats

M. Negrete-Pincetic et al. carried out their research on the quantification of the effects of attacks on the power grid, where the difficulty and the impact of four kinds of cyber threats were compared. These are Denial of Service, Replay, Man-in-the-middle, Reprogramming RTUs. Now that the difficulty is directly proportional to the efforts exerted, the chosen threats would be placed in the difficulty ascending order: Denial of Service, Replay, Man-in-the-middle, Reprogramming RTUs [6]. Recent years have witnessed many vigorously attempts to quantify these cyber threats. Unfortunately, numerous studies were based solely on the previous experiences and/or the difficulty, entailing a lot of comparison by the subjective weights or scores. As noted by [7], the attacks from an availability perspective are remarkably easier than those from a confidentiality standpoint. This is mostly because there is no need for internal information or authentication processes in the former. On the contrary, the threats from an integrity viewpoint are by far the toughest. If the relative degree of damage in a control system is considered, the types of threats will be arranged in the severity ascending sequence: confidentiality, mixture of confidentiality and integrity, integrity, and availability.

The numerical values regarding the threats will be imposed by ranking them with regard to two axes.

The weights of 0, 1, 2, 3, and 4 are assigned to the components in the SCADA system along with the horizontal axis, allowing for the potential scale of damage. On one hand, the server is afforded by the highest weight of 4, which it is largely attributable to the server's immense damage caused by the grave threats. The RTUs, on the other hand, are eligible for the relatively low weight of 1 since they are located at the end of the network and their damages may be slight. Supposing that threats may not be concerned with the components in the SCADA system, the zero point will be granted to the corresponding cell in Table 2. This notion was, in part, aided by the methodology that could determine appropriate values through the interactive comparison between objects when there exist no accurate quantified values to be applied in the analytic hierarchy process [8].

The impact matrix in (4), **I**, was created by normalizing the related weights with respect to the horizontal axis in Table 2. This normalization signifies the impacts of a specific threat on the components in the SCADA system when the occurrence probability of this event is assumed to be one.

In a similar fashion, we can prioritize the predefined 15 threats along the longitudinal axis by taking advantage of their severity. As outlined by Table 1, these are classified by confidentiality, mixture of confidentiality and integrity,

**Table 2.** Effects of each threat on components in the SCADA system (on the basis of row)

| Threats | Server | $L_1^{TCP}$ | $L_2^{TCP}$ | $L_3^{TCP}$ | $L_1^{Serial}$ | $L_2^{Serial}$ | $L_3^{Serial}$ | $RTU_1$ | $RTU_2$ | $RTU_3$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Eavesdropping | 4 | 3 | 3 | 3 | 2 | 2 | 2 | 1 | 1 | 1 |
| Traffic Analysis | 0 | 2 | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 0 |
| EM/RF Interception | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Indiscretions by Personnel | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Media Scavenging | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Trojan Horse | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Trapdoor (Backdoor) | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Service Spoofing | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Masquerade | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Bypassing Controls | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Authorization Violations | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Physical Intrusion | 4 | 3 | 3 | 3 | 2 | 2 | 2 | 1 | 1 | 1 |
| Replay | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Theft & Illegitimate Use | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Denial of Service | 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 3.** Severity of threats in a particular component of the SCADA system (on the basis of column)

| Threats | Server | $L_1^{TCP}$ | $L_2^{TCP}$ | $L_3^{TCP}$ | $L_1^{Serial}$ | $L_2^{Serial}$ | $L_3^{Serial}$ | $RTU_1$ | $RTU_2$ | $RTU_3$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Eavesdropping | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Traffic Analysis | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| EM/RF Interception | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Indiscretions by Personnel | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Media Scavenging | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Trojan Horse | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| Trapdoor (Backdoor) | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| Service Spoofing | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| Masquerade | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 3 | 3 |
| Bypassing Controls | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 3 | 3 |
| Authorization Violations | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 3 | 3 |
| Physical Intrusion | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 3 | 3 |
| Replay | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 3 | 3 |
| Theft & Illegitimate Use | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 3 | 3 |
| Denial of Service | 4 | 3 | 3 | 3 | 0 | 0 | 0 | 0 | 0 | 0 |

$$\mathbf{I} = [i_{ij}] = \begin{bmatrix} 0.18 & 0.14 & 0.14 & 0.14 & 0.09 & 0.09 & 0.09 & 0.05 & 0.05 & 0.05 \\ 0 & 0.22 & 0.22 & 0.22 & 0.11 & 0.11 & 0.11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.18 & 0.14 & 0.14 & 0.14 & 0.09 & 0.09 & 0.09 & 0.05 & 0.05 & 0.05 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0.4 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \mathbf{S} = [s_{ij}] = \begin{bmatrix} 0.04 & 0.13 & 0.13 & 0.13 & 0.2 & 0.2 & 0.2 & 0.04 & 0.04 & 0.04 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.04 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.12 & 0.12 & 0.12 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.12 & 0.12 & 0.12 \\ 0.12 & 0.25 & 0.25 & 0.25 & 0.4 & 0.4 & 0.4 & 0.12 & 0.12 & 0.12 \\ 0.12 & 0.25 & 0.25 & 0.25 & 0.4 & 0.4 & 0.4 & 0.12 & 0.12 & 0.12 \\ 0.12 & 0 & 0 & 0 & 0 & 0 & 0 & 0.12 & 0.12 & 0.12 \\ 0.12 & 0 & 0 & 0 & 0 & 0 & 0 & 0.12 & 0.12 & 0.12 \\ 0.16 & 0.38 & 0.38 & 0.38 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4)$$

integrity, and availability. Table 3 was proposed by the fundamental postulate that the importance or the severity of threats in the control system would be enumerated in the ascending order: confidentiality, mixture of confidentiality and integrity, integrity, and availability. By normalizing the severity with respect to the vertical axis in Table 3, we can obtain the severity matrix in (4), **S**. This normalization represents the severity of any threats against a specific component in the SCADA system when the extent of damages resulting from all attacks is assumed to be one.

With both matrices, **I** and **S**, the matrix of threats, **T**, is finally derived by (5), which is called array multiplication.

**Table 4.** Quantified results of cyber threats

| Threats | Server | $L_1^{TCP}$ | $L_2^{TCP}$ | $L_3^{TCP}$ | $L_1^{Serial}$ | $L_2^{Serial}$ | $L_3^{Serial}$ | $RTU_1$ | $RTU_2$ | $RTU_3$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Eavesdropping | 0.0072 | 0.0182 | 0.0182 | 0.0182 | 0.0180 | 0.0180 | 0.0180 | 0.0020 | 0.0020 | 0.0020 |
| Traffic Analysis | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| EM/RF Interception | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0132 | 0.0132 | 0.0132 |
| Indiscretions by Personnel | 0.0400 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Media Scavenging | 0.0400 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Trojan Horse | 0.0320 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0160 | 0.0160 | 0.0160 |
| Trapdoor (Backdoor) | 0.0320 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0160 | 0.0160 | 0.0160 |
| Service Spoofing | 0.0320 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0160 | 0.0160 | 0.0160 |
| Masquerade | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0396 | 0.0396 | 0.0396 |
| Bypassing Controls | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0396 | 0.0396 | 0.0396 |
| Authorization Violations | 0.0480 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0240 | 0.0240 | 0.0240 |
| Physical Intrusion | 0.0216 | 0.0350 | 0.0350 | 0.0350 | 0.0360 | 0.0360 | 0.0360 | 0.0060 | 0.0060 | 0.0060 |
| Replay | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0396 | 0.0396 | 0.0396 |
| Theft & Illegitimate Use | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0396 | 0.0396 | 0.0396 |
| Denial of Service | 0.0640 | 0.0760 | 0.0760 | 0.0760 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 0.3168 | 0.1292 | 0.1292 | 0.1292 | 0.054 | 0.054 | 0.054 | 0.2516 | 0.2516 | 0.2516 |

**Table 5.** Quantified results of vulnerabilities

| Components in SCADA | Server | $L_1^{TCP}$ | $L_2^{TCP}$ | $L_3^{TCP}$ | $L_1^{Serial}$ | $L_2^{Serial}$ | $L_3^{Serial}$ | $RTU_1$ | $RTU_2$ | $RTU_3$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Vulnerability Weight | 1 | 2 | 2 | 2 | 3 | 3 | 3 | 4 | 4 | 4 |
| Normalized Weight | 0.0357 | 0.0714 | 0.0714 | 0.0714 | 0.1071 | 0.1071 | 0.1071 | 0.1429 | 0.1429 | 0.1429 |
| Vulnerability Index multiplied by 0.5 | 0.0179 | 0.0357 | 0.0357 | 0.0357 | 0.0536 | 0.0536 | 0.0536 | 0.0714 | 0.0714 | 0.0714 |

This is found by multiplying the corresponding entries in each matrix, as shown in Table 4.

$$\mathbf{T} = \lfloor t_{ij} \rfloor = \lfloor i_{ij} \times s_{ij} \rfloor \tag{5}$$

When a specified threat is assumed to break out once, Table 4 exhibits the level of the threat that would be faced by the components in the SCADA system.

### 3.2 Quantification of Vulnerability

Typically, the threat is an exogenous variable and the vulnerability is an endogenous variable as the latter may rise or fall in accordance with the investment in security.

Three assumptions were envisaged on the ground that the vulnerability could not be unconditionally known. First, in the absence of the archived historical data, the probability of 0.5 may be presumed for simplicity.

In other words, we can look upon it as the matter of whether the threat may break into the asset through the vulnerability. Second, the components in the SCADA system have different security robustness so that they are entitled to their prioritized vulnerabilities, as conducted in the quantification of threats. The server has the lowest vulnerability weight of 1 and the RTUs have the highest index of 4 while TCP/IP and serial networks have 2 and 3, respectively. This is because the server must meet the most thorough security standard and the security of components at the end of the network is rather weak. These vulnerability weights are normalized with respect to the total weights summed over the components in the SCADA system. And then the probability of 0.5 is applied to the normalized vulnerability indices.

In Table 5, the vulnerability indices were finalized. Third, each component in the SCADA system has the same vulnerability index with regard to the type of cyber threats.

## 4. Numerical Results

The viability of the proposed assessment paradigm will be ensured with the 3-bus system, as portrayed in Fig. 2. Each generating unit is connected with Bus 1 and Bus 2, respectively. Commercial load is attached to Bus 1, industrial load to Bus 2, and residential load to Bus 3. Likewise, Bus 1, Bus 2, and Bus 3 in each region are linked to $RTU_1$, $RTU_2$, and $RTU_3$ in the SCADA system. The communication lines joining the SCADA server to $RTU_1$, $RTU_2$, and $RTU_3$ are dubbed $L_1$, $L_2$, $L_3$ as well. Each communication line is organized by $L_k^{TCP}$ and $L_k^{Serial}$. In

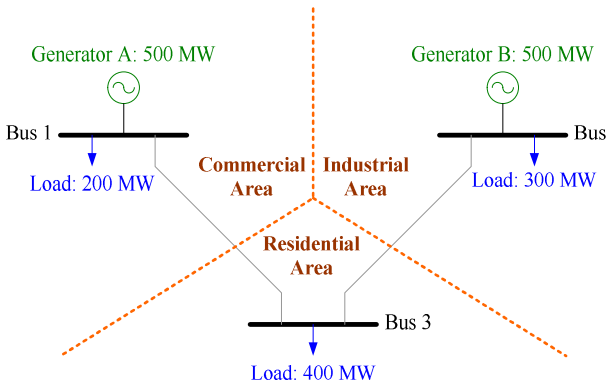


**Fig. 2.** Sample system for case study

this case study, two generators are negligible as they tend to be commonly controlled by the energy management system. If the SCADA server is exposed to the external attacks, the damages may extend over the entire power system. In contrast, when the attacks are limited to a particular RTU, only the probability of power outage at the bus adjacent to this RTU will skyrocket. The regional separation will lend itself to the division of outage cost into the feature of areas or loads [9]. Since the lost value ($LV_n$) of the information asset is, in the power system, extremely less than the outage cost ($OC_n$) from the disabled state, it does not matter to choose only the outage cost as the value of the asset. As per one hour outage [10], the outage cost of residential, commercial, and industrial loads is, respectively, 2.8 [$/kWh], 37.365 [$/kWh], and 127.420 [$/kWh]. The exchange rate for $1 is assumed to be 1,000 [won] in Korean currency. As a result, the asset values are approximately 7,473 [$/h] in commercial area, 38,226 [$/h] in industrial area, and 1,129 [$/h] in residential area.

The risk in monetary value, which each component in area should encounter, is computed by (2). We can draw up a detailed expression for matrix algebra, as depicted by (6). The amounts in Table 6 correspond to a tentative duration of one hour and these will sharply increase when the outage lasts for a length of 24 hours or a few days. It is evitable that long hours of electricity failure would be burst havoc on the community since the outage cost over time may grow exponentially. From Table 6, it is worth highlighting that the greater the risk rate and the asset value are, the higher the risk should be, where the risk rate is explicitly defined by the product of the threat and the vulnerability. The risk in Table 6 is equal to at least an expected damage per hour when threats or attacks are realized.

## 5. Concluding Remarks

Granting that the cyber security in the power system is deserving of much scholarly attention, most research and approaches have ended up with reiterating the threats and ad hoc countermeasures pertinent to the stereotyped information technology system. To overcome this setback, this paper has endeavored to make the security uncertainties in the power system clear. Above all, we put forth a proposal on the assessment structure to quantify the risk, assuming that this risk might be formulated by threats, vulnerabilities, and asset values. In the meantime, the numerical extents of both threats and vulnerabilities were finalized by means of the relative comparisons, which has been prevailed in the analytic hierarchy process of social science, since we have no historical data in relation to them. And the asset value in the power system was determined by the outage cost incurred when this asset happened to be intruded on, which would have immediate and vital implications for operations and reliability of the power system. Though the cyber security risks assessment is worth nothing for unknown threats, this paper could pave the way for a refined follow-up study on the cyber security in the power system by addressing the essential architecture and methodology to

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \\ R_5 \\ R_6 \\ R_7 \\ R_8 \\ R_9 \\ R_{10} \end{bmatrix} = \begin{bmatrix} 0.0179\sum_{j=01}^{15} T_{01j} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.0357\sum_{j=01}^{15} T_{02j} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.0357\sum_{j=01}^{15} T_{03j} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.0357\sum_{j=01}^{15} T_{04j} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.0536\sum_{j=01}^{15} T_{05j} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.0536\sum_{j=01}^{15} T_{06j} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.0536\sum_{j=01}^{15} T_{07j} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0714\sum_{j=01}^{15} T_{08j} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0714\sum_{j=01}^{15} T_{09j} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0714\sum_{j=01}^{15} T_{10j} \end{bmatrix} \begin{bmatrix} 46{,}819 \\ 7{,}473 \\ 38{,}226 \\ 1{,}120 \\ 7{,}473 \\ 38{,}226 \\ 1{,}120 \\ 7{,}473 \\ 38{,}226 \\ 1{,}120 \end{bmatrix} \quad (6)$$

**Table 6.** Quantified results of risks in monetary value with threats and vulnerabilities considered

| Components in SCADA | Server | $L_1^{TCP}$ | $L_2^{TCP}$ | $L_3^{TCP}$ | $L_1^{Serial}$ | $L_2^{Serial}$ | $L_3^{Serial}$ | $RTU_1$ | $RTU_2$ | $RTU_3$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Threats (T) | 0.3168 | 0.1292 | 0.1292 | 0.1292 | 0.054 | 0.054 | 0.054 | 0.2516 | 0.2516 | 0.2516 |
| Vulnerabilities (V) | 0.0179 | 0.0357 | 0.0357 | 0.0357 | 0.0536 | 0.0536 | 0.0536 | 0.0714 | 0.0714 | 0.0714 |
| Asset Value (A) [k$/h] | 46,819 | 7,473 | 38,226 | 1,120 | 7,473 | 38,226 | 1,120 | 7,473 | 38,226 | 1,120 |
| Risk (R) [k$/h] | 265.50 | 34.47 | 176.32 | 5.17 | 21.63 | 110.64 | 3.24 | 134.25 | 686.70 | 20.12 |

estimate the risks in the SCADA system.

In the near future, we will strive for an outreaching research on the distinct exposition of threats and vulnerabilities applicable to the SCADA system.

## Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(grant number. NRF-2012R1A1A 2007953).

## References

[1] SANS Institute InfoSec Reading Room, *Vulnerability Assessment*, July 2001, http://www.sans.org/reading-room/whitepapers/basics/vulnerability-assessment-421.

[2] Vulnerability Assessment, Wikipedia, http://en. wikipedia.org/wiki/Vulnerability_assessment.

[3] S. Massoud Amin, "Cyber and Critical Infrastructure Security: Toward Smarter and More Secure Power and Energy Infrastructures," *Canada-U.S. Workshop on Smart Grid Technologies at Vancouver*, March 25, 2010.

[4] A. Hussain, C. J. Seok, M. S. Choi, S. J. Lee, and S. I. Lim, "Line Security Evaluation of WANS Considering Protectability of Relays and Vulnerability of Lines," *Journal Elec. Eng. Tech.*, vol. 9, no. 6, pp. 1864-1872, November 2014.

[5] P. Burris and C. King, "A Few Good Security Metrics," *METAGroup Inc.*, October 11, 2000.

[6] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment," *in Proceedings of IEEE Power Tech Conference*, Bucharest, Romania, July 2009.

[7] Analytic Hierarchy Assessment, Wikipedia, http://en. wikipedia.org/wiki/Analytic_hierarchy_process.

[8] Ernest H. Forman, Decision by Objective: Analytical Hierarchy Process, http://www.dept.aoe.vt.edu/~ cdhall/ courses/aoe4065/AHPslides.pdf.

[9] Korea Electrotechnology Research Institute and Incheon National University, A Study to Investigate Industrial Customer Interruption Cost for Power System Planning, Ministry of Commerce Industry and Energy, February 2008.

[10] B. Hu, X. H. He, and K. Cao, "Reliability Evaluation Technique for Electrical Distribution Networks Considering Planned Outages," *Journal Elec. Eng. Tech.*, vol. 9, no. 5, pp. 1482-1488, September 2014.

**Pil Sung Woo** He received his B.S. degree from Pai Chai University, Korea, in 2012, and his M.S. degree in Electronic and Electrical Engineering from the Hongik University, Korea, in 2014. Currently, he is pursuing a Ph.D. degree in Electronic and Electrical Engineering at the Hongik University.

**Balho H. Kim** He received his B.S. degree from the Seoul National University, Korea, in 1984, and his M.S. and Ph.D. degrees from the University of Texas at Austin in 1992 and 1996, respectively. He was with KEPCO (Korea Electric Power Corporation) from 1984 to 1990 and joined Hongik University in 1997 where he is presently a professor of Electronic and Electrical Engineering. His research fields include optimal power flow, public utility pricing, electricity market design & operation, resource planning, and demand management.

**Don Hur** He received B.S., M.S., and Ph.D. degrees in Electrical Engineering from Seoul National University in 1997, 1999, and 2004, respectively. His industry experience includes an internship in 2001 at Burns & McDonnell Engineering Company, Kansas City, MO, USA. After finishing his Ph.D., he spent some time as a post-doctoral research associate at the Engineering Research Institute of Seoul National University and the University of Texas at Austin, TX, USA. He is currently an associate professor in the Department of Electrical Engineering at Kwangwoon University, Seoul, Korea, where he is affiliated with the power and energy systems area. He is a life member of KIEE and author or co-author of over 100 publications, studies, reports, and journal articles. His research interests relate broadly to modeling, analysis, and optimization of electric power and overall energy systems to feature the role and possible evolution of non-conventional energy resources, such as renewable generation and energy storage.