International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 137-142
http://dx.doi.org/10.14257/ijsia.2014.8.3.15

Security Control Analysis of ICS

Dongkyun Seo, YoungIn You and Kyungho Lee

Center for Information Security Technologies, Korea University, Seoul, Korea
{olly, crenius, kevinlee}@korea.ac.kr

Abstract

Industrial control systems (ICS) are computer-controlled systems that monitor and control industrial processes that exist in the physical world. ICS monitors and controls the national infrastructure or industrial process including transportation facilities, water treatment and distribution, electrical power transmission and distribution, and gas pipelines. If a SCADA system is stationary, disaster is inevitable. But, many ICSes were not built to withstand security incidents, such as accidental cyber-related incidents, DoS attacks, and malware infiltrations. Vulnerability of ICS information system becomes clear, security evaluation of the system began to be implemented. Security evaluation for ICS information system has been implemented for all areas, it is performed without considering the characteristics of each field. Control to be applied to all areas, all the same, but the importance of the control is different. This paper has offered the reader a correlation analysis approach which will allow them to grade importance their defensive efforts. Once a prioritized list has been created, a risk management approach to addressing system vulnerabilities may occur. Furthermore, this result based on real data of power generation companies.

Keywords: *ICS, Security indicator, Energy industry, ISMS*

1. Introduction

Energy and industrial sectors are the backbone of the real economy. Cyber- attack attempt for this sector has steadily increased each year. Information security breaches energy to relieve anxiety has emerged the need for about a new concept of security management system. However, Energy industry what has Separate Safety Network is different from IT industry. So, Safety is more important than Confidentiality, Integrity and Availability. Therefore, energy industry security systems should be different form the IT security systems.

In general, the overall IT security management systems that contribute to improving the security level. However, the appropriate security management systems in the energy industry is still many shortcomings. In fact, many management system is still based on an existing IT environment, and applied equally to the energy industry. Thus, there are many unreasonable part. In addition, focus only common standard like NIST SP 800-53, and evaluate by control measures based on the law. As a result, each area, thermal, gas, electricity, nuclear power, etc., do not have to reflect the particular circumstances.

KURM-ISMS, self-developed in KURM (Korea University Risk Management Lab), is to overcome the limitations of existing ISMS, including the risk management procedures. KURM-ISMS is considering ISO / IEC 27000 Series, and NIST standard. In addition, the control-based evaluation method that combines the NIS assessment items and KISMS superset of controls was constructed.

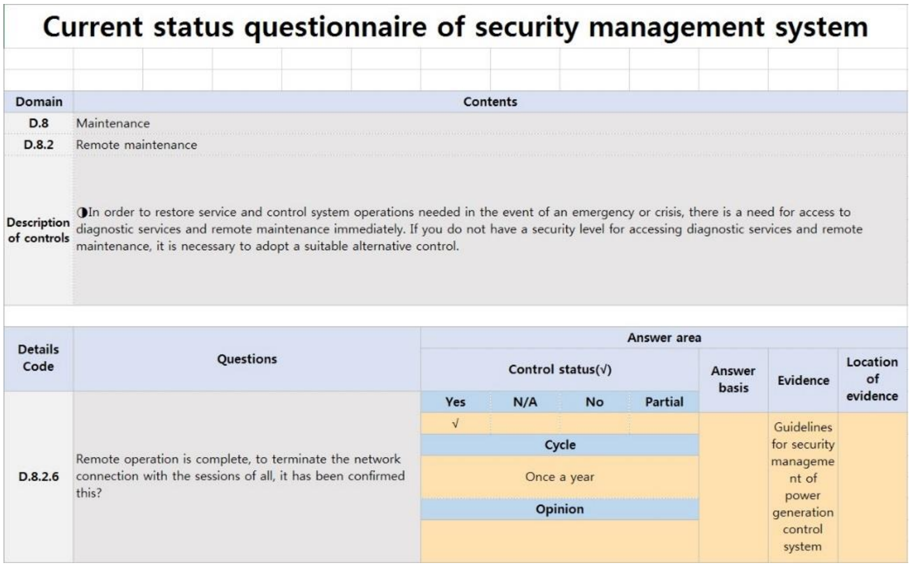
In this study, KURM-ISMS through the control of the questionnaire items constitute a superset. And questionnaire responses were analyzed statistically. Based on the results of

ISSN: 1738-9976 IJSIA

analysis of the importance of identifying in each control item, and thus the weight for step-by-step methods that can be applied to derive reasonable. Through this, the energy industry to configure the appropriate security systems and security management decisions on investment criteria can be established.

2. Evaluation Method

Evaluation conducted by using checklist basically. Checklist was created based on the NIST Special Publication 800-53. This document include security guidance for industrial control system. The evaluation sheet, the same as the next, the answer to each item is classified Yes, No, Partial and N/A.



Current status questionnaire of security management system

Domain	Contents
D.8	Maintenance
D.8.2	Remote maintenance
Description of controls	◑In order to restore service and control system operations needed in the event of an emergency or crisis, there is a need for access to diagnostic services and remote maintenance immediately. If you do not have a security level for accessing diagnostic services and remote maintenance, it is necessary to adopt a suitable alternative control.

Details Code	Questions	Answer area						
		Control status(√)				Answer basis	Evidence	Location of evidence
		Yes	N/A	No	Partial			
D.8.2.6	Remote operation is complete, to terminate the network connection with the sessions of all, it has been confirmed this?	√					Guidelines for security management of power generation control system	
		Cycle						
		Once a year						
		Opinion						

Figure 1. Example of Evaluation Sheet

All results are mapped as follows. Yes is in compliance with a document and related grounds control items, three points. Partial is have a portion of the document or evidence related to the control items or the compliance level is incomplete, two points. No is not fulfill control and article and rationale associated with the control item does not exist, one points. N/A is does not related with control and business processes, so except to calculation. Description of controls is added explanation for the special situation of ICS for the query. Answer basis, Evidence and Location of evidence are an item for reliability evaluation. Total number of items is 186 pieces, and is carried out in the field of energy each. It is intended for developers and operation of energy management systems workers and Process Owner. This evaluation was conducted in the energy field of practice and in this paper, we analyze the thermal power field.

3. Methods of Analysis

For each item the evaluation, which was conducted in the fields, classified into each power plant. In this paper, to analyze the relationship between items within total result. Analyze the similarities and differences between in the same field (thermal power field). By utilizing this, to calculate the reasonable weight for each controls. To analysis, using the following table.

Table 1. Concept of Analysis Table

	$\mathrm{w}_{1_i} \times c_1$	$\mathrm{w}_{2_i} \times c_2$	⋯	$\mathrm{w}_{\mathrm{n}_i} \times c_n$	
A ICS					Ave. of $\sum w \times c$
B ICS					Ave. of $\sum w \times c$
⋮					⋮
Yes ratio					
No ratio					
Standard deviation					S.D= $\sum s.d_n$
Ave. of Standard deviation					Ave. of S.D

The ratio of Yes, No is derived from each controls. This ratio is used to calculate weight for each controls. Ratio is divided into 3 levels and each level is given point as 3, 2 and 1. Given a point in a variety of ways (Given a point 3, 2, 1 or 1, 2, 3 depending on Yes or No ratio). The weight are calculated as follows.

$$\mathrm{w}_{\mathrm{n}_i} = \frac{Score\ for\ controls(3{,}2\ or 1\ )}{a_1 \times 3 + a_2 \times 2 + a_3 \times 1}$$

$$a_k\ is\ the\ number\ of\ factor\ in\ each\ level$$

After the weight has been determined, it is applied to controls. The following is the standard deviation for that control. It is intended that the smaller this value is given a weight reasonable for all power plants. Final weight is determined to minimum value by using the average of standard deviation. Security indicator for each area also calculate with this weight.

4. Result of Analysis

Evaluation and analysis is conducted to several thermal power area using by above method. The result is as follow table.

Table 2. Standard Deviation Depending on Weight

	Divide method				Standard deviation
	Interval		Criteria	Sort	
Weigh1	90	70	Yes ratio	forward	**0.00357**
Weigh2	90	70	Yes ratio	reverse	0.004301
Weigh3	70	50	Yes ratio	forward	0.003606
Weigh4	70	50	Yes ratio	reverse	0.004451
Weigh5	60	40	No ratio	forward	0.004202
Weigh6	60	40	No ratio	reverse	0.004009
Weigh7	40	20	No ratio	forward	0.004419
Weigh8	40	20	No ratio	reverse	0.008038

Analysis conduct based on Yes and No ratio. Partial is not used, because it is neutralize the result. The interval divided three level (e.g. 90% or more and 70% or more and the rest). Each level is given a point forward or reverse direction as 1, 2, 3 or 3, 2, 1. As the above, the interval divide into 100%~90%, 90%~70%, 70%~ that shown best result. Because that interval's result is the most minimum value in standard deviation.

Table 3. Standard Deviation Depending on Weight without Dilution

	Divide method				Standard deviation
	Interval		Criteria	Sort	
Weigh9	90	-	Yes/No ratio	forward	0.003965
Weigh10	90	50	Yes/No ratio	forward	**0.003603**
Weigh11	90	50	Yes/No ratio	reverse	0.003846

Survey information is often diluted. So we make weight without dilution. If Yes and No ratio is 50 percent for each, this result excluded from calculation. Then, we can obtain result above. Most minimum value in standard deviation is 0.003603.

This result shows Weight1 is most reasonable weighting method. Because of this standard deviation value (0.00357) is most minimum in this experiment. Furthermore, the calculation without dilution has same result.

5. Conclusion

Evaluation of existing, has not been performed appropriate evaluation according to each field of power generation. So, this study was done in order to assessment appropriate for each field of power generation. It is possible to derive the appropriate security assessment by applying the weight for each control. In this paper, thermal field was taken up, but the extension is possible in all areas of energy, which is in progress actually.

Acknowledgements

This work was supported by the IT R&D program of MSIP/KEIT. [010041560, A development of anomaly detection and a mult-layered response technology to protect an intranet of a control system for the availability of pipeline facilities].

References

[1] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner and G. Rogers, “Guide to industrial Control System (ICS) Security”, NIST Special Publication 800-82.
[2] K. Stouffer, J. Falco and K. Scarfone, “Information Security”, NIST Special Publication 800-53.
[3] ISO/IEC 27001, Information Security Management System.

Authors

Dongkyun Seo, is now a Master Course in Graduate School of Information Management and Security at Korea University since 2013.

YoungIn You, is now a Master Course in Graduate School of Information Management and Security at Korea University since 2013.

Kyungho Lee, received his Ph.D. degree from Korea University. He is now a Professor in Graduate School of Information Security and Security at Korea University, and leading the Risk management Laboratory in Korea University since 2012. He has a high level of theoretical principles as well as on-site experience. He was a former CISO in NAVER corporation, and now he takes as the CEO of SecuBase corporation. His research interests include Information Security Management System (ISMS), risk management, information security consulting, privacy policy, and Privacy Impact Assessment (PIA).