International Journal of Smart Home
Vol.8, No.2 (2014), pp.115-122
http://dx.doi.org/10.14257/ijsh.2014.8.2.13

Analysis of Common Security Factor on Energy Industry

Sanghyun Park, Sangkyo Oh and Kyungho Lee

Center for Information Security Technologies, Korea University, Seoul, Korea
{parksh1, darkapple, kevinlee}@korea.ac.kr

Abstract

The energy industry has several industry group such as nuclear, thermal, hydro, gas, electricity. There are evident the common ground and differences among nuclear, thermal, hydro, gas, electricity. The common grounds of them are originated in energy industry group and the differences are divided from each energy control system.

At the present, the issue is not there are many papers indicated each characteristic of nuclear, thermal, hydro, gas, electricity but there isn't paper indicated common ground as a single energy industry. The other issue is that the analysis data used to evaluate and analyze in such papers was not the specialized data but the general IT data. Not considering the difference between general IT environment and environment of the energy group probably bring out the distortion in the analysis data.

This paper solved the problems previously indicated and presented the common ground as the energy industry and prove them through statistical analysis. To put it concretely, this paper will present the sub domains that the whole energy industry groups always carry out and prove them through statistical analysis.

The result of this paper is expected to be important data available reference to being planned and managed the policy applicable to the whole energy group by the policy maker.

Keywords: *Energy Industry group, Common grounds, Common Security factor*

1. Introduction

Energy industry of the country is important and generally people agree and empathize for importance of energy industry. If the energy industry is important, management and evaluation of the energy industry should also detail and achieve effectiveness of management and evaluation. However, assessment and management for energy industry in the field is not detail and does not achieve effectiveness. Because energy industry groups are evaluated as general information security checklist not specific energy industry checklist. Such a common criteria can make the evaluation result unsuitable for each energy group. Therefore it is difficult to find the common ground of the whole energy industry group by using the basic common criteria to evaluate and analyze. Although they find the common ground, most of them are not accurate.

For this reason, this paper evaluates the energy industry groups as specific energy industry checklist to obtain meaningful results and then analyzes to find common security factors on energy industry that is nuclear, thermal, hydro, gas, electricity and so on.

Prior to beginning this paper, the controls and survey questions suitable for each energy group are made and sent to the each groups. And then that questionnaires are gathered as a unit of individual group and compare and analyze, and we find the common security factor by checking on the controls observed in common. After that we analyze them and prove the significance as the common security factor by using statistical analysis.

ISSN: 1975-4094 IJSH

The common security factor presented in this paper is not the characteristics of the individual energy group but the characteristics of the whole energy industry. And the characteristics of the individual energy group contains the main value relevant to the industry. Through the results of this paper, the government can get efficient and effective result in order to implement and manage the whole policy in the energy field.

2. Analysis Preparation

Evaluation conducted by using specific check list for ICS(Industrial Control System) basically. The checklist was created based on the NIST Special Publication 800-53 that include security guidance and recommended check list for ICS. The evaluation sheet is the same as the next and the answer to each item is classified Yes, No, Partial and N/A.

Current status questionnaire of security management system

Domain	Contents
D.1	Access Control
D.1.2	Access Control Account Management
Description of controls	◑ The control system can not manage the account (e.g., remote terminal) is required 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.1.2.2	Using, form(Individuals, groups, and guests) for each account information has been identified in specific?	√				Identification is based on the command center information security rules	the command center information security rules	the command center information security rules Article 8. Access control system No 43. User accounts management
		Cycle						
		Once a year						
		Opinion						

Figure 1. Example of Evaluation Sheet

All results are mapped as follows.

Table 1. Control Status Level's Definition and Point

	Definition	Point
Yes	Yes is in compliance with a document and related grounds control items	3
Partial	Partial is have a portion of the document or evidence related to the control items or the compliance level is incomplete	2
No	No is not fulfill control and article and rationale associated with the control item does not exist	1
N/A	N/A is does not related with control and business processes	Except

In addition, description of controls is added explanation for the detail situation of ICS for the answers and Answer basis, Evidence and Location of evidence are an item for reliability evaluation.

The check list configured main domain, Sub domain, and control. Total number of main domain is 14 domains and total number of sub domain is 90 domains. Total number of control is 186 pieces. Configure for main domain and Sub domain are as follows.

Table 2. Domain Name and Control Number

Main domain name	Sub domain name	Control number
D.1 Access Control	D.1.1 Access Control Policy and Procedures	2
	D.1.2 Account Management	11
	D.1.3 Separation of Duties	4
	D.1.4 Least Privilege	1
	D.1.5 Unsuccessful Login Attempts	2
	D.1.6 System Use Notification	4
	D.1.7 Concurrent Session Control	1
	D.1.8 Session Lock	3
	D.1.9 Remote Access	6
	D.1.10 Wireless Access	5
	D.1.11 Access Control for Mobile Devices	8
D.2 Audit and Accountability	D.2.1 Audit and Accountability Policy and Procedures	2
	D.2.2 Auditable Events	5
	D.2.3 Response to Audit Processing Failures	3
	D.2.4 Audit Reduction and Report Generation	1
	D.2.5 Audit Generation	4
D.3 Security Assessment and Authorization	D.3.1 Security Assessment and Authorization Policies and Procedures	2
	D.3.2 Security Assessments	5
	D.3.3 Continuous Monitoring	3
D.4 Configuration Management	D.4.1 Configuration Change Control	1
	D.4.2 Security Impact Analysis	1
	D.4.3 Access Restrictions for Change	1
	D.4.4 Configuration setting	1
	D.4.5 Least Functionality	1
D.5 Contingency Planning	D.5.1 Contingency Planning Policy and Procedures	2
	D.5.2 Contingency Plan Testing and Exercises	3
	D.5.3 Alternate Storage Site	3
	D.5.4 Information System Recovery and Reconstitution	1
D.6 Identification and Authentication	D.6.1 Identification and Authentication Policy and Procedures	2
	D.6.2 Identification and Authentication (Organizational Users)	1
	D.6.3 Device Identification and Authentication	1
	D.6.4 Identifier Management	1
	D.6.5 Cryptographic Module Authentication	1
D.7 Incident Response	D.7.1 Incident Response Policy and Procedures	2
	D.7.2 Incident Response Training	1
	D.7.3 Incident Response Testing and Exercises	1

	D.7.4 Incident Handling	1
	D.7.5 Incident Response Plan	1
D.8 Maintenance	D.8.1 System Maintenance Policy and Procedures	2
	D.8.2 Non-Local Maintenance	6
	D.8.3 Maintenance Personnel	1
D.9 Media Protection	D.9.1 Media Protection Policy and Procedures	2
	D.9.2 Media Access	1
	D.9.3 Media Marking	2
	D.9.4 Media Storage	2
	D.9.5 Media Transport	4
D.10 Physical and Environmental Protection	D.10.1 Physical and Environmental Protection Policy and Procedures	2
	D.10.2 Physical Access Authorizations	3
	D.10.3 Monitoring Physical Access	3
	D.10.4 Visitor Control	1
	D.10.5 Emergency Shutoff	1
	D.10.6 Emergency Lighting	1
	D.10.7 Fire Protection	1
	D.10.8 Temperature and Humidity Controls	1
	D.10.9 Water Damage Protection	1
	D.10.10 Location of Information System Components	1
D.11 Planning	D.11.1 System Security Plan	1
	D.11.2 Rules of Behavior	1
	D.11.3 Privacy Impact Assessment	1
D.12 Personnel Security	D.12.1 Personnel Transfer	1
	D.12.2 Personnel Sanctions	1
D.13 Risk Assessment	D.13.1 Risk Assessment	1
	D.13.2 Vulnerability Scanning	6
D.14 System and Services Acquisition	D.14.1 System and Services Acquisition Policy and Procedures	1
	D.14.2 User-Installed Software	1
	D.14.3 Security Engineering Principles	1
	D.14.4 Supply Chain Protection	1
D.15 System and Communications Protection	D.15.1 Application Partitioning	1
	D.15.2 Security Function Isolation	1
	D.15.3 Information in Shared Resources	1
	D.15.4 Denial of Service Protection	1
	D.15.5 Boundary Protection	4
	D.15.6 Transmission Integrity	1
	D.15.7 Transmission Confidentiality	1
	D.15.8 Network Disconnect	1
	D.15.9 Trusted Path	1
	D.15.10 Cryptographic Key Establishment and Management	1
	D.15.11 Use of Cryptography	1
	D.15.12 Public Access Protections	1
	D.15.13 Collaborative Computing Devices	1

	D.15.14 Mobile Code	2
	D.15.15 Voice Over Internet Protocol	2
	D.15.16 Session Authenticity	1
D.16 System and Information Integrity	D.16.1 Flaw Remediation	4
	D.16.2 Malicious Code Protection	5
	D.16.3 Spam Protection	2
D.17 Awareness and Training	D.17.1 Security Awareness and Training Policy and Procedures	2
	D.17.2 Security Awareness	1
	D.17.3 Security Training	1
	D.17.4 Security Training Records	1
		186

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. Analysis of Common Security Factor for Energy Industry Group

This paper will compare and analyze the 6 energy industry target groups (thermal, gas, nuclear, combined cycle, electricity, power exchange) through survey. And then this paper find the common ground of 6 energy industry group that will be proven by logic.

The step of proof is as follows.

First, it compare to survey result of 6 energy industry groups and then extract controls that all energy industry are observed.

Table 3. The Collection of Control that Every Energy Industry are Observed

No	Main domain name	Sub domain name	Question's code	Energy industry groups					
				Power exchange	Electricity	Gas	Combined Cycle	Nuclear	Thermal
1	Access Control	Account Management	1.2.2	Yes	Yes	Yes	Yes	Yes	Yes
2		Separation of Duties	1.3.4	Yes	Yes	Yes	Yes	Yes	Yes
3		Least Privilege	1.4.1	Yes	Yes	Yes	Yes	Yes	Yes
4	Media Protection	Media Access	9.2.1	Yes	Yes	Yes	Yes	Yes	Yes
5		Media Marking	9.3.1	Yes	Yes	Yes	Yes	Yes	Yes
6			9.3.2	Yes	Yes	Yes	Yes	Yes	Yes
7		Media Storage	9.4.1	Yes	Yes	Yes	Yes	Yes	Yes
8			9.4.2	Yes	Yes	Yes	Yes	Yes	Yes
9		Media Transport	9.5.2	Yes	Yes	Yes	Yes	Yes	Yes
10			9.5.4	Yes	Yes	Yes	Yes	Yes	Yes
11	Physical and Environmental Protection	Physical Access Authorizations	10.2.1	Yes	Yes	Yes	Yes	Yes	Yes
12		Monitoring Physical Access	10.3.1	Yes	Yes	Yes	Yes	Yes	Yes
13			10.3.2	Yes	Yes	Yes	Yes	Yes	Yes
14		Visitor Control	10.4.1	Yes	Yes	Yes	Yes	Yes	Yes

15		Emergency Shutoff	10.5.1	Yes	Yes	Yes	Yes	Yes	Yes
16		Emergency Lighting	10.6.1	Yes	Yes	Yes	Yes	Yes	Yes
17		Fire Protection	10.7.1	Yes	Yes	Yes	Yes	Yes	Yes
18		Temperature and Humidity Controls	10.8.1	Yes	Yes	Yes	Yes	Yes	Yes
19		Water Damage Protection	10.9.1	Yes	Yes	Yes	Yes	Yes	Yes
20		Location of Information System Components	10.10.1	Yes	Yes	Yes	Yes	Yes	Yes
21	System and Communications Protection	Denial of Service Protection	15.4.1	Yes	Yes	Yes	Yes	Yes	Yes
22		Boundary Protection	15.5.1	Yes	Yes	Yes	Yes	Yes	Yes
23			15.5.4	Yes	Yes	Yes	Yes	Yes	Yes

As the table above, the total number of main domains are 4 pieces, and sub domains are 23 pieces. These domains are common security factor for energy industry groups.

Second, it make a supposition as below through above result.

"Above 4 main domains and 23 sub domains are common security factor of 6 energy industry groups in total main domains and sub domains."

To prove this point, it distinguish remaining control from 4 main domains and 23 sub domains.

Table 4. The Number of Control for Every Group's Common Security Factor

Main domain name	Sub domain name	Sub domain control number (all question)	Common control number (all energy industry group)	Remain control number
Access Control	Account Management	10	1	9
	Separation of Duties	4	1	3
	Least Privilege	1	1	0
Media Protection	Media Access	1	1	0
	Media Marking	2	2	0
	Media Storage	2	2	0
	Media Transport	4	2	2
Physical and Environmental Protection	Physical Access Authorizations	2	1	1
	Monitoring Physical Access	3	2	1
	Visitor Control	1	1	0
	Emergency Shutoff	1	1	0
	Emergency Lighting	1	1	0
	Fire Protection	1	1	0
	Temperature and Humidity Controls	1	1	0
	Water Damage Protection	1	1	0
	Location of Information System Components	1	1	0
System and Communications Protection	Denial of Service Protection	1	1	0
	Boundary Protection	4	2	2
			23	

As the table above, the number of remaining control is 18 pieces on 23 sub domains.

Third, this paper analyze control that any 5 target groups perform well to prove supposition as follow.

Table 5. The Number of Control for Almost all Group's Common Security Factor

Main domain name	Sub domain name	Remain control number (all energy industry group)	Common control number (5+1 energy industry group)	Remain Control number (5+1 energy industry group)
Access Control	Access Control Policy and Procedures		2	
	Wireless Access		1	
	Account Management	9	6	3
	Separation of Duties	3	3	0
	Unsuccessful Login Attempts		1	
	System Use Notification		1	
Physical and Environmental Protection	Physical and Environmental Protection Policy and Procedures		2	
Risk Assessment	Risk Assessment		1	
	Vulnerability Scanning		4	
System and Communications Protection	Application Partitioning		1	
	Boundary Protection	2	1	1
	Trusted Path		1	
System and Information Integrity	Flaw Remediation		3	
	Malicious Code Protection		4	
	Spam Protection		2	
Configuration Management	Security Impact Analysis		1	
Contingency Planning	Information System Recovery and Reconstitution		1	
Maintenance	Non-Local Maintenance		1	
Media Protection	Media Protection Policy and Procedures		2	
	Media Transport	2	2	0
			40	

3. Result of Analysis

(a) The total number of control on survey is 186 pieces. Among them, the number of control and sub domain that every(6 groups) target groups perform well is 23 pieces and 18 pieces. And then control remain 163 pieces.

(b) In 163 pieces, the number of control that almost all(5 groups) target groups perform well is 40 pieces. Therefore, The above general probability is 24 percent on case that almost all(5 groups) target groups perform well.

(c) In 163 pieces, the number of control that included (a)'s 18 domain is 18 pieces.

Therefore, the more (c)'s 18 pieces include in (b)'s 40 pieces, the more Assumption may be true.

In conclusion, (c)'s 18 pieces include 12 pieces in (b)'s 40 pieces. If (c)'s 18 pieces is strongly affected, 4.3 pieces should include in (c)'s 18 pieces. In other words, the probability that (c)'s 18 pieces include 12 pieces in (b)'s 40 pieces is higher about 3 times than above general probability.

3. Conclusion

This paper presented the common security factor that is Account Management, Separation of Duties, Least Privilege, Media Access, Media Marking, Media Storage, Media Transport,

Physical Access Authorizations, Monitoring Physical Access, Visitor Control, Emergency Shutoff, Emergency Lighting, Fire Protection, Temperature and Humidity Controls, Water Damage Protection, Location of Information System Components, Denial of Service Protection and Boundary Protection.

As above proof, the common security factor is not characteristic from only each specific energy field but common characteristic. And it could be preferentially managed important domain overall energy industry

To put it concretely, this paper is presented that Energy groups are generally manage the preferentially protection of external access, data flow, environment (temparature, humidity) parts.

Through the results of this paper, the government can get efficient and effective result in order to implement and manage the whole policy in the energy field.

Acknowledgements

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2013-H0301-13-3007) supervised by the NIPA(National IT Industry Promotion Agency)

References

[1] National Institute of Standards and Technology "NIST SP 800-55", **(2007)** September.
[2] National Institute of Standards and Technology "NIST SP 800-82, **(2011)** June.
[3] National Institute of Standards and Technology "NIST SP 800-53, **(2009)**, August.
[4] International Organization for Standardization, "ISO 27004", **(2009)**.

Authors

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

Sangkyo Oh, 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).

