SAFETY AND SECURITY INTEGRATION FOR THE PRODUCTION INDUSTRY UNDER THE RESILIENCE MATRIX

NYAMBAYAR DAVAADORJ & ICHIRO KOSHIJIMA
Industrial Management Engineering, Nagoya Institute of Technology, Japan

ABSTRACT

Plant Owners must protect a legal requirement that specifies the occupational health and system safety of people in the workplace. Furthermore, it is essential to continue to maintain a safer production site together. Industrial control systems (ICS) are connected to the internet for purposes such as information exchange and data analysis for business-oriented operations and labour saving remote maintenance. ICS is also subject to cyber-attacks as a result of using commercial IT equipment, PC, OS to connect to the internet. In this situation, each manufacturer is charged to identify hazards related to the cyber-security as well as the employee's safety. The term "Cyber-Security" in the production field refers to the risk created by cyber-attacks to the ICS. There is a practical need to adopt global standards for safety and security systematically as a baseline for protecting production environment. Before integrating safety and security standards simultaneously, it is necessary to analyze both specified processes shown, in the clauses of the standard documents. In this paper, the authors would like to discuss a method for implementing IEC 62443 (internationally applied standard for the Owner and operation industrial management security) systematically to integrate into the corporate's safety protection profile specified by OHSAS: 18001.

Keywords: safety, security, IEC 62443.

1 INTRODUCTION

In a production site, machines, and equipment that aren't properly maintained become a possible danger for human operators. Plant owners must prepare to meet legal requirements that specify the health and safety of people in the workplace. Furthermore, it is essential to continue to maintain safer production site.

Industrial control systems (hereafter called ICS) [1] are connected to the Internet for purposes such as information exchange and data analysis for business oriented plant operations and remote maintenance. ICS are installed in many industries such as electric, water-supply and sewage, oil and gas, chemical, pharmaceutical, and assembly and manufacturing.

There are many different types of ICS with variety levels of potential risks and impacts. ICS are also subject to cyber-attacks as a result of using commercial IT equipment, PC, OS to connect to the Internet based on rapidly developed IT technologies. The owners are charged to identify hazards of the production system's cyber-security as well as the employee's safety. (In this paper, "cyber security" at the production site refers to the risk of cyber-attack against ICS.)

Recently, the APT (Advanced Persistent Threat) [2], attack is targeting IT network and allows an unauthorized person to gain access to a corporate LAN and stay there undetected for a long period. The intention of the APT attack is mainly to steal corporate information rather than to cause physical damage to equipment. However, Stuxnet (malicious computer worm) targeted Iran's nuclear facility by corrupting ICS. Keeping security of ICS, therefore, becomes a critical issue, because current cyber attackers finally acquired the ability to break upper network layers of the ICS network.

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170191

Up to now, safety and security have been discussed separately in the production safety society and the IT security society. To achieve safety and security at the same time, it is realistically necessary to systematically adopt the separated global standards for integrating activities.

In this paper, the authors would like to discuss a method for implementing IEC 62443 [3], standard systematically where the safety standard OHSAS 18001 (Occupational Health and Safety Assessment Series) [4], is already installed in the production site. In here we are like to introduce our previous paper.

In Nyambayar et al. [5], authors discussed on OHSAS18001, an internationally applied standard for the construction and operation of occupational health and safety management systems, by using IDEF0 for Function Modelling (IDEF0) and the Resilience Matrix (RM) that can be defined as a cycle to develop new operational procedures to maintain and increase organizational resilience. RM covers activities that occur during establishment, implementation, and maintenance. Accordingly, it seems to be appropriate to place the IDEF0 [6] model of the OHSAS18001 standard into the RM in order to specify the structure of the organizational activity cycle and identify inherent activities.

In this previous study, we discussed a method for evaluating a manner in which OHSAS18001 systematically functions within corporations. Based on the findings, this study clarifies the potential structural objection for corporations when implementing and operating the OHSAS18001 standard.

2 ANALYSIS OF GLOBAL STANDARD FOR SECURITY

Many new international standards have been created in the world of industrial engineering. Most of the used for the occupational safety of the production site is OHSAS 18001. The control system is adopting IEC 62443 [3], standard for cyber security. These global standards provide the main checklist of issues that should be addressed in the qualitative evaluation and countermeasure. The standards also define performance measures against which quantitative reliability and safety calculations can be compared. Also, the global standard provides explanations and examples of how the system can be designed to maximize safety and security reliability.

2.1 Setting up the issues with IEC 624443

To install the above-mentioned safety and security standards simultaneously, the following questions/issues are posed when a structure of each activity is set up and ensure IEC 624443 into the OHSAS 18001 management process [5].

1. Clarification of activities in IEC 62443 clauses: The actions that should be performed and the precedence orders that should be taken into account while they are performed should be specified based on the clauses.
2. Determination of other actions inherent to the IEC 62443 process: Unspecified actions should be expected to proceed IEC 62443 clauses.
3. Determination of a methodology to provide safety and security for the production site by using its organization structure.

2.2 Analysis of IEC 624443 clauses

The analysis of IEC 62443 was conducted by deconstructing and categorizing clauses from the following perspectives (see Table 1):

1. Sentence
2. Subjects, objects, and verbs within the sentence
3. Category (knowledge, skill and rule) the sentence specified

As an illustration of our proposed method, in this paper, we selected Section 4.2 of the IEC 62443-2-1 (Industrial communication networks - Network and system security – Part 2–1: Establishing an industrial automation and control system security program), however, the method is not bound by this case.

Table 1 shows only risk identification, classification and assessment clauses, which contain directives on activities and requirements to secure ICS network. The result showed that the entity in-charge of risk assessment activity is primarily the "organization," and there is no clear statement t clarifying "who should actually act." Furthermore, when the object was extracted, it was hence not clear what action should be taken within the organization. There are many uncomplete rules included in IEC 62443. Under these circumstances, it is necessary to acquire necessary knowledge and skills by continuously improving corporate activities.

Rasmussen [7] remarked:

> "*When we distinguish categories of human behaviour according to basically different ways of representing the constraints in the behaviour of a deterministic environment or system, three typical levels of performance emerge skill-based behaviour, rule-based behaviour, and knowledge-based behaviour performance*,"

where:

Skill-based behavior: Represents sensory-motor performance during acts or activities which, following a statement of an intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior.

Rule-bases behavior: The composition of such a sequence of subroutines in a familiar work situation is typically controlled by a stored rule of procedure which may have been derived empirically during previous occasions, communicated from other person know-how as instruction or a cook book recipe, or it may be prepared on occasion by conscious problems solving and planning.

Knowledge-based behavior: During unfamiliar situations, faced with an environment for which no know-how or rules for control are available from previous encounters, the control or performance must move to a higher conceptual level, in which performance is goal controlled and knowledge.

2.3 Modelling of activities in IEC 62443 clauses

When a plant owner implements IEC 62443, it follows the relevant clauses in the IEC 62443 standard. The standard requests a PDCA [Plan, Do, Check (Evaluate), Act (review and implementation)] structure, which includes IEC 62443 policy, goal, and ICS industrial security planning. Its operation also includes daily inspections and improvements, update the records and regular review of the system.

This paper revealed the following three areas where information is unclear in the implementation and operation of IEC 62443:

1. The input and output of a given activity
2. The main subject of a person who carries out the activity

Table 1: Analysis of risk identification, classification, and assessment in IEC 62443.

Main activities in the sentences	Subject	Verb	Object	Knowledge, Rule, Skill
The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets.	organization	select assessment	risk assessment	knowledge
The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks.	organization	provide	risk assessment	rule
A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised.	financial and HSE	performed	financial and HSE	knowledge
The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk and group the devices into logical systems.	organization	identify	various IACS	rule
The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk.	physical HSE	integrated	assets overall risk	knowledge
Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement.	organization	conducted	through all stages	rule
The risk assessment methodology and the results of the risk assessment shall be documented.	organization	documented	risk assessment	skill
Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS.	organization	maintained	Comprising the IACS	knowledge

3. The conditions on the limitations and resources that must be taken into account in executing the activity

To identify these elements in the clauses of the IEC 62443, a modeling tool, IDEF0 [6], is used.

The activity in IDEF0 can be identified as the verbs in the standard clauses of IEC 62443. Concomitantly, whatever is fed to execute this activity is expressed as the input, and the results of executing the input through the activity can be expressed as the output. The control is done by limiting condition in executing the activity, and a mechanism is formed in a manner in which the execution of the activity is supported. This is expressed as the resource (especially the executor of the activity) to execute the activity.

Fig. 1 shows the determination of the source of the select and identifies a risk assessment methodology, provide risk information, integrate physical, HSE, document the risk assessment and maintain information of the IEC 62443 standard document. Exiting activities

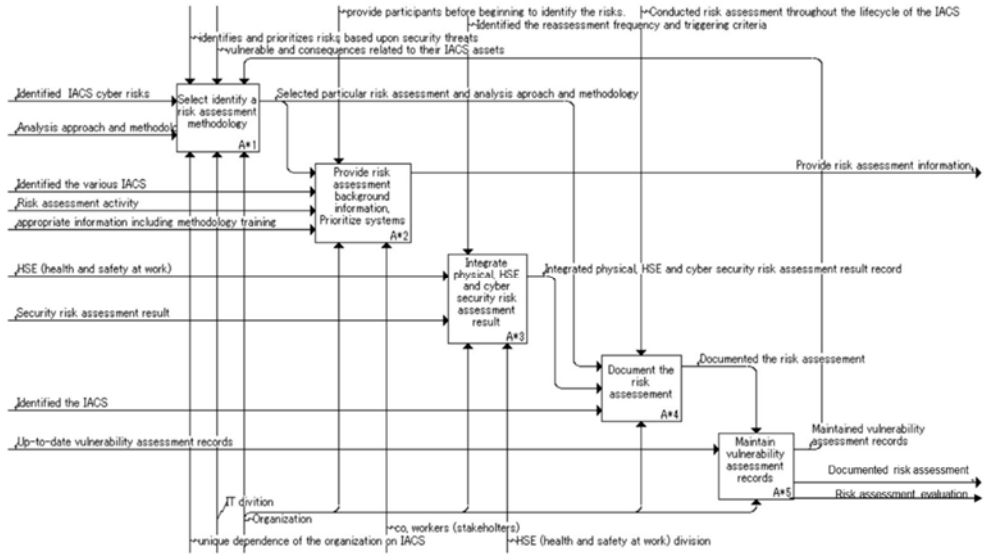

Figure 1: IEC 62443 risk assessment IDEF0 modeling example.

are a determination of the source of the select and identify risk assessment, and the provide information of steps to determine how to manage, implement, update the records disseminate those steps.

3 MAPPING IN IEC 62443 TO ORGANIZATION OPERATION

3.1 Operation steps of resilience matrix

The model of the IEC 62443 standard expressed through using IDEF0 is transformed into a resilience matrix (calling RM) made by own to determine inherent activities. The resilience matrix proposes and is a model where the capacity to respond is considered in the context of an organization. Fig. 1 showing each activity for the mechanism, who should act that activity. For example, standard mention organization, and IT division, the unique dependence of the organization on IACS, Heal and safety division for each activity. This reason can be separate based on organizational level (individual, group, organization). The individual is employed and a small group of the division. The group is division. For example, IT division and health and safety division, ICS divisions including. The organization is a more responsible person and top manager or financial manager.

The RM is a three-by-three matrix consisting of nine cells, with the horizontal axis representing the response provider based on Fig. 1 (individual, group, organization). Each of the nine cells shows that a certain response provider should take a certain kind of action to enhance resilience within an organization in response to varying signals.

3.2 RM-based IEC 62443 model

The RM can be defined as a cycle to develop new operational procedures, for an individual to implement it, and provide feedback regarding its ease of use as a group to maintain and increase organizational resilience. Accordingly, it seems to be appropriate to place the IDEF0

model of the IEC 62443 standard into the RM to specify the structure of the organizational activity cycle and identify inherent activities.

Fig. 2 shows the IEC 62443 risk assessment clauses expressed in IDEF0 and transferred to the RM as well as the relevant inherent activities. The activities cells are from IEC 62443 risk assessment clauses. For example, with the representation of the IDEF0 version of the IEC 62443 clauses "select and identify a risk assessment methodology" by the "organization" is connected to input "provide risk assessment information" action by the group.

The proposed implement this method and evaluate method the culture of safety and security involves placing activities, which have been specified in manuals in corporations based on global standard on to an RM and determining the necessary activities that the corporation's IEC 62443 had not covered. This methodology can thus develop a structure where a culture and climate safety and security can be organizationally created.

3.3 Non-resilient organization model

By setting and specifying a structure based on the IDEF0 model of the IEC62443 standard through an RM as a resilient organizational model, an organization model that is not resilient can be raised as the following reason.

3.3.1 An issue of having a single response provider complete a response on his/her own

If an organization is not involved in any part of an activity cycle, it is not possible to reflect select and identify a risk assessment methodology, implement document, maintain vulnerability assessment records of a procedure when deciding its security and safety policies. The means that is PDCA cycle meant to assist in improving the organization as a whole does not properly operate. The cycle is rendered non-functional when the "organization" select and identify a risk assessment methodology the procedure, the "individual" implement and integrate physical, HSE and cyber security risk assessment result procedure. "Group" document the risk assessment, provide feedback based on the experience of the individual in

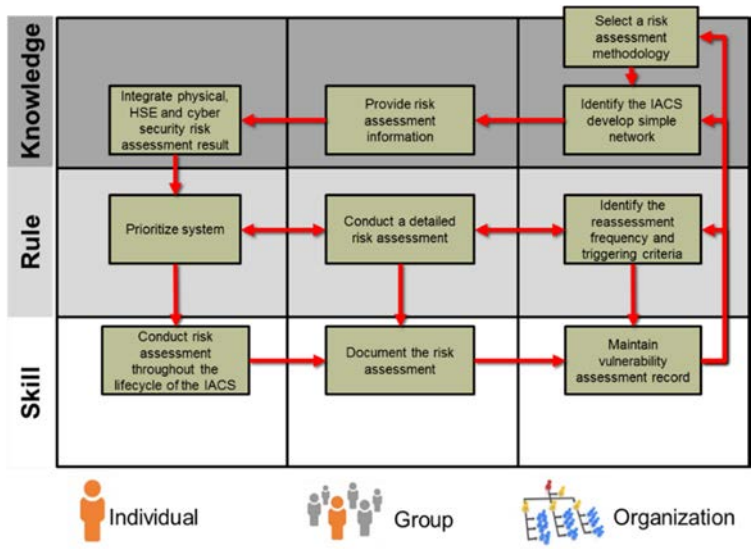

Figure 2: Resilience matrix for IEC 62443 based on IDEF0 diagram.

implementing the procedure to improve and maintain procedure. When this cycle is completed by the "individual," the specific and more appropriate skillset of the "individual," will not be fed back into the "department" and the "organization." Thus, when revising and improving the procedures, those skills will not be reflected in the revision. Furthermore, when the "individual" within each department are left on their own to complete cycles, each department ends up with different procedures. When this happens, the organization finds that a common and organizationally unified framework to respond to signals in not shared across departments, thus making it difficult to flexibly respond to a given situation.

The completion of an activity cycle by a single response provider:

- All activities are carried out by an "individual" response provider, and the activity cycle is completed by the single response provider.
- Individual who belong to multiple departments use their knowledge to develop, operate, and update procedures record, respectively. Improvement in such procedures is brought about only by the department to which those individuals belong.
- The organization uses an organizational model where other response providers, department, and the organizational are not involved in the establishment, implementation or the update of such procedures.

3.3.2 Issue due to the disruption of information dissemination activity

If activities to expand information output are not linked to the following activities, organizational officials cannot decide how to use distributed information under IEC 62443 clause. Therefore, each official of the organization uses his/her discretion in using the disseminated information.

The disruption of information dissemination activity:

- The organizational model where output is based on an activity to disseminate information to other personnel within an organization is disrupted before it connects to any other activity.

3.4 Well-implemented resilient organization model

Based on these issues it can be assumed that a resilient organizational model should look like that shown in Fig. 3. The PDCA cycle is that helps disseminate the IEC 62443 standard throughout the company. To run this company-wide PDCA cycle continually without failure, it is necessary to establish a section-based PDCA cycle at each stage of the cycle. Fig. 3 shows where it is possible to establish its cycle within the individual, group, and at the corporate level.

In an organizational structure with a section-based PDCA cycle:

- Each section goes through the select and identifies a risk assessment methodology – prioritize systems and conduct risk assessments throughout the lifecycle of the IACS – document the risk assessment – implement – maintain vulnerability assessment records.
- Subsequently, the improvement must be checked and tested. If it passes the check, one can move on to the next stage.
- If the improvement fails the check, one goes back to an improvement section, provides safety instructions, and return to the cycle.
- The cycle is repeated in each responding section of the organization.

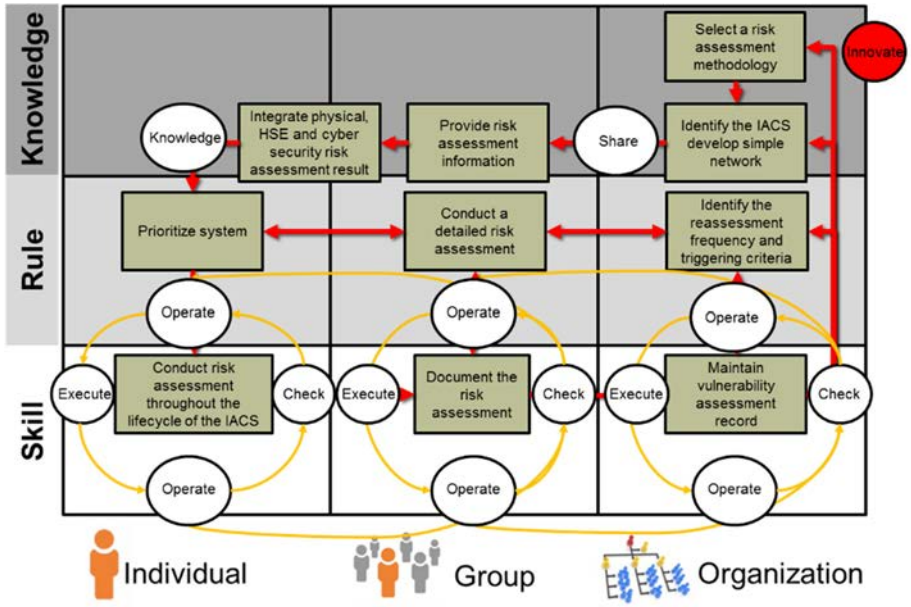

Figure 3: Resilience matrix for IEC 62443 based on IDEF0 diagram.

4 CONCLUSION

In this paper, we proposed a framework and method to enhance security standard in an organization that has adopted IEC 62443 standard. Also, we designed a cyber security exercise by applying the proposed framework and methodology and had positive responses from almost 200 critical infrastructure's personnel and security experts participated. A method for integrating the safety and security standards will be presented in elsewhere.

ACKNOWLEDGEMENT

This research is partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No.16H01837 (2016); however, all remaining errors are attributable to the authors.

REFERENCES

[1] Cheminod, M., Durante, L. & Valenzano, A., Review of Security Issues in Industrial Networks. *IEEE Trans. Ind. Informatics*, **9**, pp. 277–293, 2013.

[2] Brahim, I., Messaoud, D., Guennoun, K., Wahbi, M. & Sadik, M., *Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges*, 2016. IEEE, DOI: 10.1109/ACOSIS.2016.7843932.

[3] IEC Central Office, Industrial communication network – Network and system security – Part 2–1: Establishing and industrial automation and control system security program, Online. www.iec.ch. Accessed on: Nov. 2010.

[4] OHSAS Project Group, *OHSAS18001: Occupational Health and safety management systems – Requirement*, pp. 90–179, 2007.

[5] Nyambayar, D., Koshijima, I. & Eguchi, H., A Metric for Quantitative Estimation of Production Unit Based on OSHMS. *Proceedings of the 29th Symposium of Malaysian Chemical Engineers (SOMChE) 2016 Miri*, Sarawak, Malaysia, Dec. 1–3, 2016.
[6] IDEF0 function Modelling Method; 1408 University Dr. College Station Texas 77840 United states, Online. http://www.idef.com/idefo-function_modeling_method/. Accessed on: 10 Mar. 2017.
[7] Rasmussen, J., Skills, rules, knowledge. signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man and Cybernetics*, pp. 257–266, 1983.