Education Method for Simultaneous Achievement of Safety and Security in the IoT Era

Nyambayar Davaadorj, Yuitaka Ota, Akihiro Tsuchiya and Ichiro Koshijima
Department of Architecture, Civil Engineering and
Industrial Management Engineering
Nagoya Institute of Technology, Nagoya, Japan
Nyamaa0727@gmail.com

ABSTRACT

The manufacturing industry is obligated to ensure its employees' health and safety. However, employees in a manufacturing plant are exposed to constant safety hazards. Therefore, ensuring worker safety in the plant is difficult. Moreover, the manufacturing industry in recent times has adopted control systems for plant management. Therefore, it is imperative to respond to the threat of cyber-attacks in a production environment. Hence, simultaneously safeguarding the control system against cyber-attacks and ensuring the safety of employees is necessary. However, the safety of employees and cyber-security are dealt with independently by the production safety division and the IT security division, respectively. Such a scenario may lead to a delayed response in case of an emergency and may increase the seriousness of the damage caused. Therefore, in this paper, a PDCA cycle that combines safety and security in the IoT era is presented, and an educational method is proposed that Safety-II and Security-II implementation together.

KEYWORDS

Safety, Security, Cyber-attack, IoT, ICS.

1 INTRODUCTION

With the diversification of production processes, complications and international standardization of on-site machine tools are increasing. Moreover, with the introduction of new mechanical equipment and chemical substances, the causes of occupational accidents are diversifying. Therefore, the greatest obligation of the manufacturing industry is to safeguard workers' health and to ensure the safety of its employees [1].

However, workers in a manufacturing plant are exposed continuously to health hazards. With the recent introduction of control systems by the manufacturing industry for management, it has become necessary to respond to the threat of cyber-attacks in a production environment. Therefore, securing the control systems against cyber-attacks while ensuring the safety of employees at the same time at a given site has become necessary [2]. However, up until now, worker safety and cyber security have been dealt with separately by the production safety division and the IT security division, respectively. Safety and security divisions work independently, and they may lead to more severe damage caused by a delayed response in case of an emergency [3].

Therefore, in this paper, a PDCA cycle that combines safety and security in the IoT (Internet of Thinking) era is presented, and an educational method is proposed to implement Safety-II and Security-II the organization, simultaneously.

2 SAFETY AND SECURITY

In the IoT era, control systems are significantly involved in the planning, design, operation, and marketing of the manufacturing industry. In particular, IoT is often used to achieve improvements in productivity and to reduce the production costs of plants and manufacturing industries.

Therefore, the manufacturing industry needs to ensure employee safety and industrial control system (ICS) safety simultaneously. For that purpose, we define the following two problems.

ISBN: 978-1-941968-46-8

1. Discovering effective interactions between safety and cybersecurity: It is necessary to propose an analysis method based on global standards. Find out about effective PDCA cycle to continuously implementing.
2. Maximizing organizational resilience against uncertain and unexpected cyber-attacks: It is necessary to access PDCA cycles implementation based on global standards.

2.1 Safety-based production

Deciding to standardize each of task for work manuals and advancing work according to the manual can reduce defects. First, it is necessary to arrange work procedure manual properly. Figure 1 shows indispensable relationships between safety and production tasks.

When tasks are designed using a procedure manual, and when work is carried out according to the guidelines in a procedure manual, the following is achieved.

1. Machinery can be run without incurring mechanical damage.
2. Machinery can be run without incurring environmental damage.
3. Machinery can be run while ensuring employee's health and safety.

The above three operations ultimately result in smooth operations in a manufacturing business. Also, the work is devoid of mechanical and environmental damage, and a safe work environment for employees is ensured, which leads to continuity in the company's management.

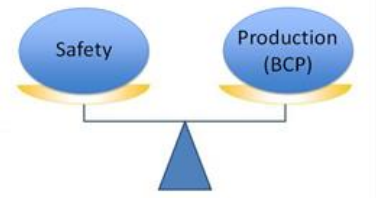

Figure 1. Relationship between safety and production.

2.2 Security-based production

A standardized operating procedure of the control system allows the operation of the control system to proceed normally. ICS is involved in the planning, design, and operation of the processing system. In particular, an information network can be used manufacturing industry utilizes IoT to improve productivity, thereby contributing to reduced costs and some human resource requirements.

Therefore, designing a procedure manual for the control system and utilizing the procedure manual affects the following three aspects (Figure 2).

1. Operation of the ICS network without incurring safety damage.
2. Operation of the ICS network without incurring production damage.
3. Operation of the ICS network without information loss

The above three operations ultimately lead to a smooth functioning of the manufacturing business. Moreover, the work is devoid of mechanical and environmental damage, and a safe work environment for employees is ensured, which leads to continuity in the company's management.

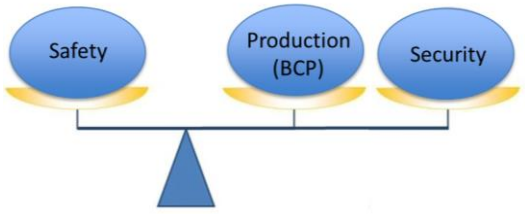

Figure 2. Schematic of the safety and security framework.

2.3 Safety and security-based production

Until now, safety has been implemented for many years for the manufacturing industry in the manufacturing industry. However, realizing a perfectly safe plant is a challenging task. Consequently, the manufacturing industry has attempted to secure the safety of the site using their method for safety. Recently, the big companies have adopted international standards for safety and security. They expect a reduction in risk due to the adoption of global safety standards. In the IoT era, the use

ISBN: 978-1-941968-46-8

of control systems in the production process has become widespread. Figure 3 indicates that the manufacturing industry uses the control system for automation of the production line, stable operations, and reduction in the human resources required.

Also, manufacturing industries collect and analyze data from the control system by connecting to the Internet (for data analysis) for improved marketing functions, management, and line productivity. The analyzed will help the industry adapt to a flexible trading business market and enhance its business efficiency. However, connecting the control system to the Internet increases the risk of cyber-attacks, consequently, increasing risks in the future.

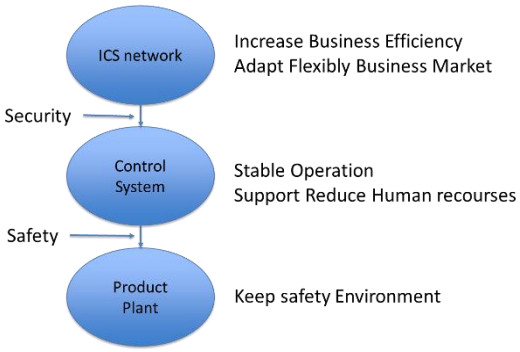

Figure 3. Maintain safe environment.

2.4 Analysis of Safety and Security Integration Standard

In literature [1], [4] the authors discussed the establishment of a cycle for bottom-up that continues to improve, maintain and implement after recognizing the international standard for safety and security standards. For safety, OHSAS18001 (Occupational Health and Safety standard) is analyzed by using IDEF0 and is mapped to a Resilience Matrix (RM) that can be defined as a cycle to develop new operational procedures to maintain and increase organizational resilience. In this matrix skill–rule–knowledge (SRK) model and organizational levels (i.e., individual, group, and organization) are combined in the 3 × 3 chart.

To specify a security standard procedure, IEC62443 (Industry network system standard) [5] is also analyzed by using the approach mentioned above.

The analysis of global standard was conducted by deconstructing and categorizing clauses of the standard from the following perspectives:

1. Chapter titles, subtitles, number, sentence locations
2. Sentences (extracting only the sections on recommendations for actions relating to health and safety)
3. Subjects, objects, and verbs within sentences
4. Verbs, objects, and verbs within sentences
5. Knowledge, skill, rule based on Rasmussen's (Rasmussen, 1983) SRK model [6].

Resilience matrix covers activities that occur during establishment, implementation, and maintenance. Accordingly, it seems to be appropriate to place the IDEF0 model of the global standard into the resilience matrix to specify the structure of the organizational activity cycle and identify basic activities. In this previous study, we discussed a method for evaluating a manner in which PDCA cycle (Figure 4 shows) of OHSAS18001 and IEC 62443 systematically functions within corporations. Based on the findings, this study clarifies the potential structural objection for corporations when implementing and operating the OHSAS18001 and IEC 62443 standard.

According to the OHSAS18001 and IEC 62443 standard analysis, the installation of the PDCA cycles is essential for achieving continuous improvement. Safety and security standard organization structure with section-based PDCA cycle;

- Each section goes through the implementation, maintenance, and improvement processes.
- Subsequently, the improvement must be checked and tested. If it passes the check, one can proceed to the next stage.
- If the improvement fails the check, one goes back to an improvement process, provide safety instructions, and then return to the cycle.

ISBN: 978-1-941968-46-8

- PDCA is repeated in each responding section of the organization.

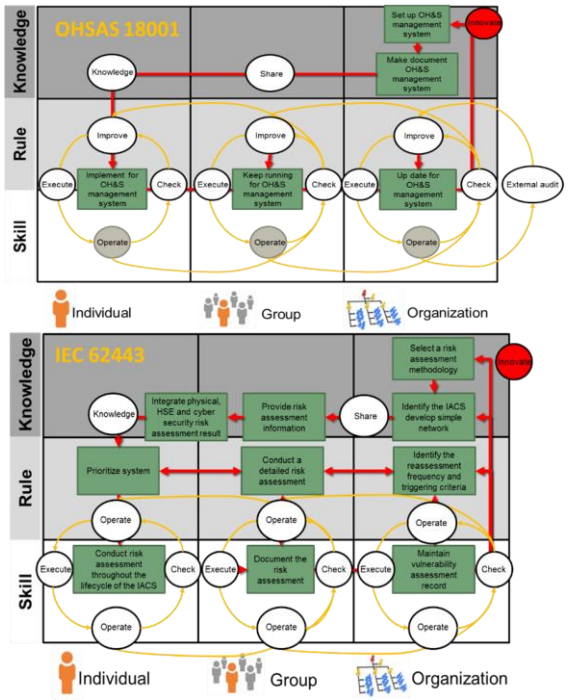

Figure 4. Schematic of the safety and security standard framework.

3 SAFETY AND SECURITY SIMULTANEOUS ACHIEVEMENT FRAMEWORK

In the event of a cyber-attack, it is necessary to have a corresponding structure to add security correspond for safety response. Also, a response process is required to converge the situation. If the control system survives the cyber-attack as an operational abnormality, measures for securing safety must be immediately implemented. Safety response and security correspondence must be realized simultaneously. Figure 5 illustrates a cyber incident correspondence structure that takes into consideration the security correspondence constraint condition. During a cyber incident, the organization (communication, resource, system) and there are constraints on (resources, systems) in the environment, and time constraints due to the urgency in the cyber incident. We explain the relationship between safety, cyber incident response, and the corresponding constraints using the IDEF0 modeling method. Given that cyber-attacks cause unsafe operating conditions in the control system, safety measures are first implemented.

An unsecured state is one of the outputs in the process of looping safety correspondence to safeguard the control system. The non-secure state shown Figure 5 is the state of the control system that is affected by the cyber incident, viz., the human condition (judgment, knowledge). Further, security correspondence is implemented against the outputted insecure state. Security correspondence loop is executed until a secure state is outputted. Even if a secure state is outputted, if the control system is in an all-anxiety status, the safety correspondence loop is executed again, and if an insecure state is outputted in that process, the security correspondence is implemented. Safety response and security correspondence are implemented in this structure until the control system outputs it in a safe and secure state. There exists an extensive roof between the safety and security tree. According to Figure 5 bottom arrow which is control added to perform measures implemented by the organization safely. Non-safety state caused by cyber incidents is implemented by the group and the division. Mechanism added to safety perform measures should be implemented individually.

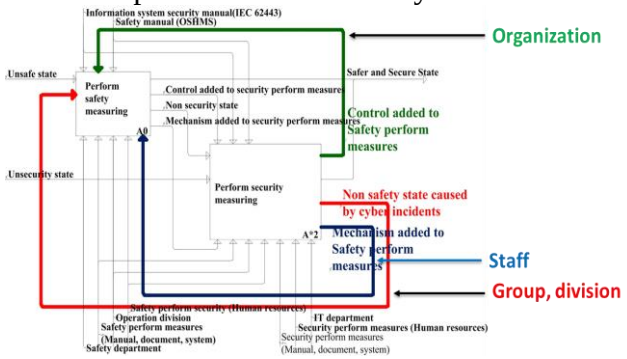

Figure 5. Safe and secure state.

3.1 Approach to integration of safety and cybersecurity

Resilience engineering is a concept proposed by Erik Hollnagel [7]. Hollnagel presented views on Safety-I and Safety-II, which are summarized as follows.

- Safety-I: Avoiding that things go wrong. The Safety-I means a state where things

do not go wrong. The safety I try only to prevent these things from going wrong. This approach assumes that it is possible to attain safety by eliminating all of the contributory factors of adverse outcomes.

- Safety-II: Safety management for responding errors to happen. The safety-II tries to ensure a state where the level of required performance is maintained to be as high as possible and to ensure that things go right under varying conditions. Attention is paid not too rare failure cases but actual routine operational performances.

By the above explanation, Security-I and Security-II are assumed in the same way of thinking.

- Security-I : On the ICS, avoiding that things go wrong Security-I refers to a state where things do not go wrong in the ICS. Security-I attempts to prevent these accidents from happening. This approach assumes that it is possible to attain safety by eliminating all of the contributory factors of adverse outcomes.
- Security-II: Security management for responding errors that are yet to occur Security-II attempts to ensure a state where the level of required performance is maintained as high as possible and to ensure that things go right under varying conditions.

In the system, attention is paid not to infrequent failure cases but instead of actual routine operational performances.

First, the global standard determines activities based on risk assessment, which can be considered as the countermeasures of Safety-I and Security-I. Second, Safety-II and Security-II define the maintenance and improvement of a safe environment, which can be considered as the countermeasures of Safety-II and Security-II; these require a continuous execution of the improvement cycle.

Therefore, one company can simultaneously achieve safety and security by maintaining Safety-I, Safety-II, Security-I, and Security-II continuously, as described in Figure 6.

Figure 6. Safety-I, security-I and safety-II, security-II framework

3.2 Global Standard Approach for Integration Respond

International standards correspond to Safety-I and Security-I. Also, it is important to identify and continuously maintain a cycle for a bottom-up approach that can be continuously improved, maintained, and executed after recognizing the international standards for safety and security. As shown in Figure 7 one factory needs care about safety (Safety-I, Safety-II) and security (Security-I, Security-II), human approaches to Safety-II and Security-II are indispensable. In the event of accidents or cyber incident, it is human beings who make the final making decision. Therefore, it is necessary to continuously develop a human resource development training and PDCA of Safety-II and Security-II in case of an emergency.

Figure 7. Safety and security integration framework.

3.3 ICS-BCP training Exercise to Implement the Integrated Response

Safety-II and Security-II involve taking safety measures at the early stages of an emergency. However, cyber-attacks and cyber incidents do not always happen, and cannot be predicted. Therefore, it is necessary to implement correspondence training when Safety-II and Security-II occur. Training for cyber incident handling is aimed at

ISBN: 978-1-941968-46-8

understanding the framework for handling cyber incidents. Therefore, depending on the organizations that are trained, it is necessary to consider the organizational (organizational involved in the operation of the business) and correspondence to cyber-attacks (response to security).

In this exercise (calling ICS-BCP) training, we will consider an organization's response to a cyber-attack. The purpose of the correspondence changes with the passage of the correspondence changes with the passage of time. The following types of activities should be considered according to the purpose of correspondence. (Figure8) the typical deliverables of the exercise are workflow which becomes plants by considering "who" performs an action and "when."

1. Activities to regain plan safety when attacks are disturbed.
2. Activities to maintain production activities that are obstructed by attacks at a specified service level.
3. Activities to deter further attacks.
4. Activities to preserve evidence of attacks.

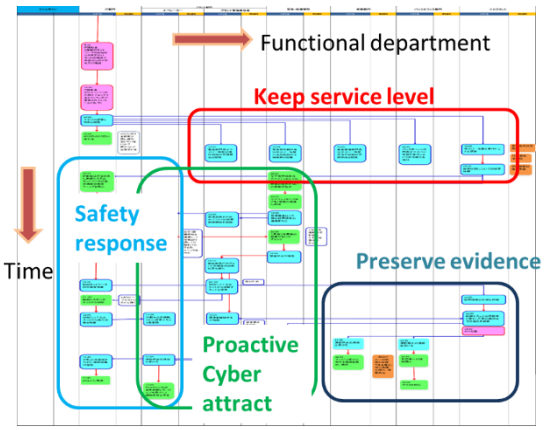

Figure 8. Schematic of the safety and security framework.

4 CONCLUSIONS

In this paper, the author proposed two problems, viz., discovering effective interactions between safety and cyber security and Maximizing organizational resilience against uncertain and unexpected cyber-attacks. Discovering an effective interactive linkage between safety and cybersecurity is necessary.

To that end, we need to maximize the resilience of the organization to cyber-attacks that cannot be predicted reliably. First, the PDCA cycle necessary to combine Safety-I and Security-I was extracted using the IDEF0 modeling method. To build a PDCA cycle between Safety-II and Security-II, an exercise framework to maximize organization resilience was suggested.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] D. Nyambayar, H. Eguchi, and I. Koshijima, "A Matric for Quantitative Estimation of Production Unit Based On OSHMS," IOP Conf.Series:Materials Science and Engineering. 012009 doi:10.1088/1757-899X/206/1/012009.

[2] SANS: Industrial Control Systems Security Blog, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid. Accessed January 29, 2017.

[3] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, and I. Koshijima, "Safety Securing approach against cyber-attacks for process control system," Computers & Chemical Engineering, vol.57, no.15, pp.181-186, October 2013.

[4] D. Nyambayar, and I. Koshijima, "Study of a Safety and Security Framework Based on Resilience Engineering," REA symposium.

[5] IEC Central Office, Industrial Communication Network, and System Security-Part2-1: Establishing and industrial automation and control system security manual, online, www.iec.ch. Accessed on: online user accessed by Yoshihiro Hashimoto.

[6] J. Rasmussen, "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.

[7] E. Holnagel, "Safety-I and Safety-II," Ashgate Pub Co. The Past and Future of Safety Management.