STUDY OF A SAFETY AND SECURITY FRAMEWORK BASED ON RESILIENCE ENGINEERING

Nyambayar Davaadorj [1] and Ichiro Koshijima [2]

[1,2] Department of Architecture Civil Engineering, Nagoya Institute of Technology, Gokiso-Cho, Showa-Ku,
Nagoya City, Japan

[1] cjv18504@ict.nitech.ac.jp

[2] koshijima.ichiro@nitech.ac.jp

Abstract

Manufacturers are subject to legal requirements for protecting the health and safety of the personnel inside and around the workplace and of those who are directly exposed to workplace activities. Although it might be difficult to manage a situation in which complete safety is ensured, efforts must be made to consider the ways of removing and mitigating potential hazards. Recently, based on the rapid development of IT applications, manufacturers are additionally charged with identifying cybersecurity hazards within the production environment as well as ensuring employee safety. So far, safety and security have been addressed separately within the IT security and production-safety domains, respectively. However, rapidly developing IT and network technologies have made sophisticated cyberattacks widely possible. Hence, there exists a practical need for simultaneously achieving industrial safety and security in the workplace.

In this research, a proactive analysis based on IEC 62443 (internationally applied standard for the manufacturers and operation of industrial management security) and occupational safety and health management system (OSHMS) is proposed. We present a methodology based on a global standard for combining the safety and security operations to maximize resiliency against a potential cyberattack scenario.

1. INTRODUCTION

Chemical manufacturers are subject to legal requirements for protecting the health and safety of the personnel who are inside and around the workplace and of those who are directly exposed to workplace activities. Although it might be difficult to manage a situation wherein a complete level of safety is ensured, efforts must be made to consider ways of removing potential dangers to workforces within an organizational setting. Such an organization should therefore perform a programmatic-level risk assessment for understanding the specific hazards that may exist within their specific processing areas. After the risk assessment, the organization should summarize the discovered information and then communicate it to downstream importers, distributors, and customers. Moreover, the organization should ensure that viable safety and security risks are determined and controlled. The term “safety” refers to a state of being “safe,” whereas production hazards are recognized and controlled to an acceptable level.

Based on the rapidly developing IT technologies, manufacturers are continually charged with identifying hazards related to cybersecurity and employee safety. The term “security” in the production field pertains to the risk created by cyberattacks to an industrial control system (ICS). ICSs are typically employed in industries when connections to the internet are made for data analysis purposes. So far, safety and security have generally been addressed as separate tenets within the IT security and production safety domains. However, the rapidly developing IT and network technologies, have made sophisticated cyberattacks a real possibility. A cyberattack is a huge risk for the safety and security of production processes; therefore, there is a practical need for embracing simultaneous achievement of safety and security from a business continuity standpoint.

In this research, a discussion is set forth based on the global standards for safety and security, which refer to IDEF0 for function modeling [National Institute of Standards and Technology, 1993] and the derived organizational matrix (referred to as the “resilience matrix”) presented within. The global standard for security is IEC 62443 (internationally applied standard for the manufacturers and operation of industrial management security) [IEC Central Office, 2010], while the global standard for safety is the occupational safety and health management system (OSHMS), an internationally applied standard that has been notably implemented for reducing potential risks within production/processing facilities [OHSAS Project Group, 2007]. Finally, this research discusses a methodology for combining the safety and security aspects to maximize resiliency levels against potential cyberattacks.

2. ANALYSIS OF GLOBAL STANDARD FOR SAFETY AND SECURITY

2.1 Setting up the issue from the global standard

For simultaneously achieving safety and security, an analysis is required to accurately characterize both the safety and security standards. For the safety standard, the OSHMS has previously been assessed [Davaadorj Nyambayar, 2016].

For the security standard, IEC 62443 has been previously analyzed by a worldwide organization for standardization, which comprises all national electrotechnical committees [IEC Central Office, 2010].

In both these analyses, the global standard(s) pose the following queries/issues when a structure of each activity is set up and evaluated with regard to industrial system resiliency within each organization:

1. Clarification of activities in standard clauses: Based on the safety and security standard clauses, are the actions which should be performed, the order in which such actions are performed, and the considerations to be taken into account for the actions clearly provided?
2. Determination of other actions inherent to the standard process: Are the determined actions that should be performed clearly provided even though they are not sufficiently detailed in the standard clauses?
3. Considering a methodology to determine how a corporation might use an organizational structure to provide safety and security for a business continuity environment.

2.2 Analysis method of risk identification

For each section, global standard risk assessment is discussed and analyzed. All assessed examples in this section consider only risk identification, classification, and assessment, which contain directives on main activities for responding to safety and security. The analysis of global standards was conducted by deconstructing and categorizing the clauses with the following configurations:

1. The main activities in the sentences (for extracting only the sections of recommendations for actions related to the system risk assessment for safety and security)
2. Subjects within the sentences
3. Objects and verbs within the sentences
4. Knowledge, skills, and rules

The result showed that the entity in charge of the risk assessment activity is primarily the "organization," and there is no mention in the standard of "who" should actually "implement" the activities. Furthermore, when the object was extracted during the analysis, very few details were actually mentioned. It was hence not clear what actions should be performed within the organization. The global standard is rule-based. There are many rules inclusive within the safety and security standards. Under these rules, methods and knowledge of other skills are clearly necessary. However, such facets prove difficult within a foreign industrial company's attempt to adopt a global standard with a built-in continuous improvement process due to considerable misunderstanding. According to a previous study [Rasmussen J, 1983], discussions are presented regarding requirements at the skill-, rule-, and knowledge-based levels, along with a review of the different levels associated with signals, signs, and symbols. Rasmussen remarked "When we distinguish categories of human behavior according to basically different ways of representing the constraints in the behavior of a deterministic environment or system, three typical levels of performance emerge: skill-based behavior, rule-based behavior, and knowledge-based performance."

2.3 Clarification of activities in global standard clauses

When a corporation implements the global standard, it follows the relevant clauses in the safety and security standard. The standard uses the main requirement in a plan–do–check (evaluate)–act (review and implementation) (PDCA) structure, which includes policies, goals, safety and security goal planning, its implementation and operation, daily inspections and improvements, record updates, and regular reviews of the system itself. This system of business management is adopted by corporations due to its basic principle of improvement in each cycle, which is caused by traversing the PDCA motions. The safety and security standards require the update of vulnerability assessment records; however, there is no mention of continuous improvement strategies in the literature. Consequently, three areas were resultantly uncovered wherein information is unclear in the implementation and operation of the global standard:

1. The input and output of a given activity
2. The main responsibilities of a person who performs the activity
3. The conditions on the limitations and resources that must be considered for the execution of the activity

For example, to identify these elements in the clauses of the OSHMS standard, an IDEF0 modeling methodology is used.

The activity in IDEF0 can be identified as the verbs in the standard clauses of the OSHMS. 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 implemented by a 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 (particularly the executor of the activity) to execute the activity.

Figure 1 shows the determination of the source of a hazard, a risk assessment, and a decision-making process-flow for an exercised management method based upon the clauses in the risk assessment section of the OSHMS standard. The existing activities are a determination of the source of the hazard and risk assessment and the establishment of steps to determine how to manage, implement, and update the records disseminating those steps.

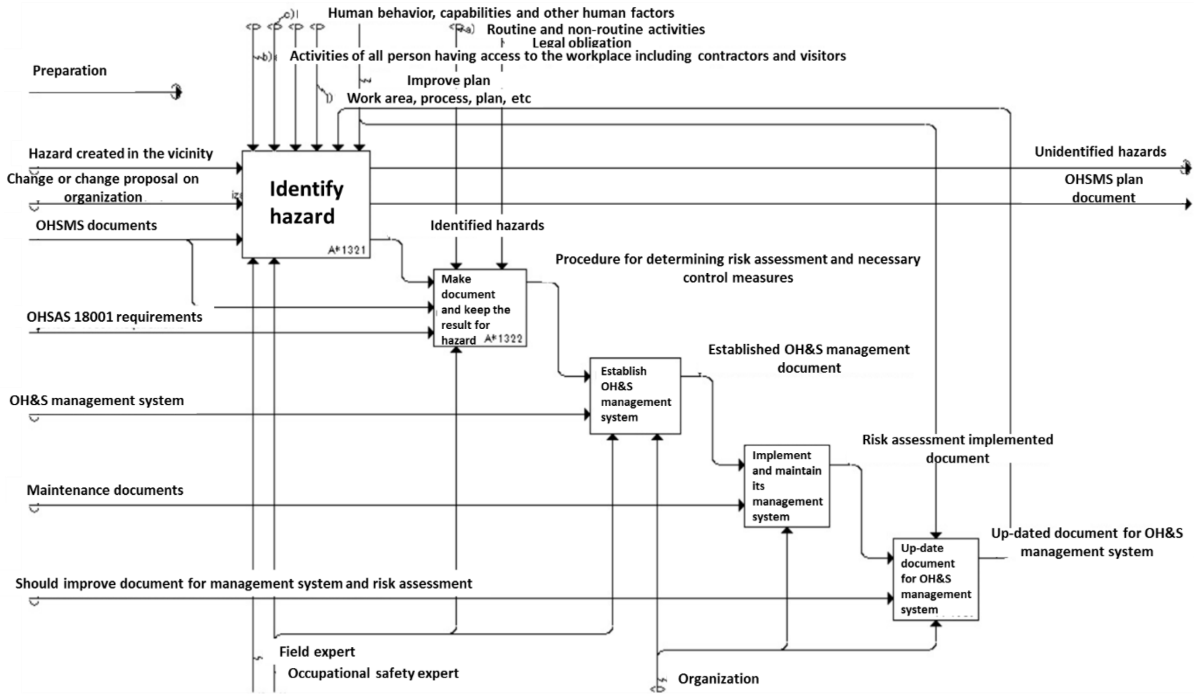
Human behavior, capabilities and other human factors
Routine and non-routine activities
Legal obligation
Activities of all person having access to the workplace including contractors and visitors
Improve plan
Work area, process, plan, etc
Preparation
Hazard created in the vicinity
Change or change proposal on organization
OHSMS documents
Identify hazard
A*1321
Identified hazards
Unidentified hazards
OHSMS plan document
Procedure for determining risk assessment and necessary control measures
OHSAS 18001 requirements
Make document and keep the result for hazard
A*1322
Established OH&S management document
Establish OH&S management system
OH&S management system
Risk assessment implemented document
Implement and maintain its management system
Maintenance documents
Up-dated document for OH&S management system
Up-date document for OH&S management system
Should improve document for management system and risk assessment
Field expert
Occupational safety expert
Organization

Figure 1. IDEF0 modeling of the occupational safety and health management system (OSHMS) risk assessment

3. OPERATION OF RESILIENCE MATRIX

The model of the global standard expressed through the use of IDEF0 is transformed into a resilience matrix (RM) to determine inherent activities. The RM describes a model whose capacity to respond (i.e., resilience) to signals is considered in the context of an organization. The RM is a 3 × 3 matrix comprising nine cells, with the horizontal axis representing the response provider (i.e., individual, group, and organization) to the signals and the vertical axis representing the ease with which the signals change (in three stages from low to high). Each of the nine cells shows that a certain response provider should perform a specific action to enhance resilience within an organization in response to varying signals. In this matrix, Rasmussen's skill–rule–knowledge (SRK) model and organizational levels (i.e., individual, group, and organization) are combined in the 3 × 3 chart.

3.1 Results of the RM OSHMS model

The results of the analysis are projected onto the RM. The RM can be defined as a cycle mechanism to develop new operational procedures so that an individual can implement them and provide feedback regarding their ease of use to maintain and increase organizational resilience. Accordingly, it seems appropriate to place the

IDEF0 model of the OSHMS standard into the RM to specify the structure of the organizational activity cycle and identify inherent activities.

Figure 2 shows the OSHMS risk assessment clauses expressed in the IDEF0 model and transferred to the RM as well as the relevant inherent activities. The activities in the box cells pertain to the OSHMS clauses according to the RM. With the representation of the IDEF0 version of the OSHMS clauses, the "establishment of procedures" by an "organization" is connected to the inputs and outputs through the "implementation of the procedure" by an "individual."

Figure 2 shows the PDCA cycle for the OSHMS standard. The PDCA cycle ultimately aids in the dissemination of the OSHMS standard throughout the example organization. To execute this company-wide PDCA cycle continuously without failure, it is necessary to establish a section-based PDCA cycle at each stage of the cycle within the individual, group, and organizational levels.

In an organizational structure with a 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.
- This is repeated in each responding section of the organization.

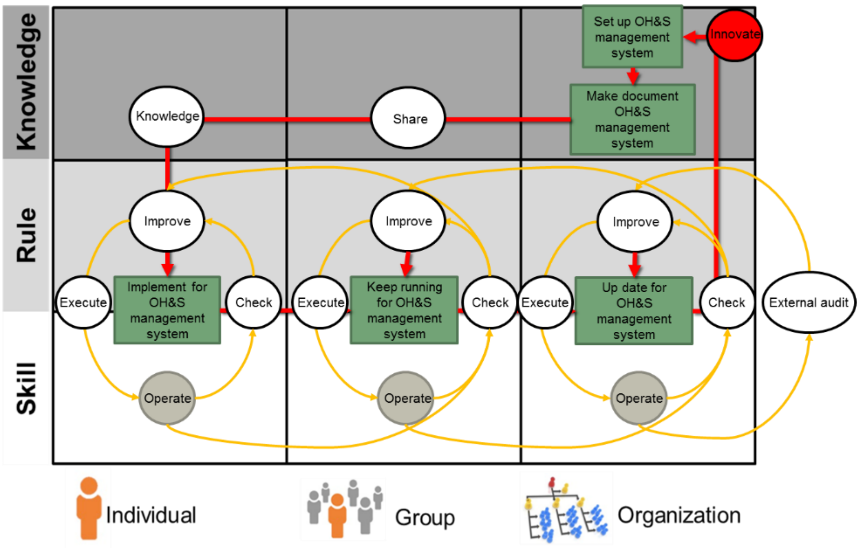
Knowledge
Rule
Skill
Set up OH&S management system
Innovate
Make document OH&S management system
Knowledge
Share
Improve
Improve
Improve
Execute
Implement for OH&S management system
Check
Execute
Keep running for OH&S management system
Check
Execute
Up date for OH&S management system
Check
External audit
Operate
Operate
Operate
Individual
Group
Organization

Figure 2. *Resilience matrix (RM) for the OSHMS based on the IDEF0 diagram*

3.2 Results of the RM-IEC 62443 model

The analysis results of IEC 62443 were projected onto the RM. The RM can be defined as a cycle mechanism for developing new operational procedures, for an individual to implement them, or to provide feedback regarding their ease of use to maintain and increase organizational resilience for the IEC 62443. Accordingly, it seems 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. Figure 3 shows the IEC 62443 risk assessment clauses expressed in the IDEF0 and transferred to the RM as well as the relevant inherent activities. The activities in all steps pertain to the IEC 62443 clauses. In particular, the activities in "Conduct risk assessment throughout the life-cycle of the IACS," "Document the risk assessment," and "Maintain vulnerability assessment record" constitute the main PDCA cycles for the IEC 62443 clauses. The representation of the activities selects a risk assessment and identifies the IACS based on the "organization," which is connected to provide risk assessment information, including methodology training. The activities in the "Prioritize system," "Conduct a detailed risk assessment," and "Identify the reassessment frequency and triggering criteria" sections follow the rule-based activities. Based on these facets, it can be assumed that a resilient organizational model should appear similar to that (should be similar to the RM-OSHMS model) depicted in Figure 3. The PDCA cycle helps disseminating the IEC 62443 standard throughout the example organization. To execute this company-wide PDCA cycle continuously without failure, it is necessary to implement a section-based PDCA cycle at each stage of the cycle. Figure 3 shows where it is possible to establish this PDCA cycle within the individual, group, and corporate levels.

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

- Each section goes through the life cycle of the IACS, documents the risk assessment, and maintains vulnerability assessment records and improvement measures.
- Subsequently, the improvement should 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 the improvement process, provide safety instructions, and then return to the cycle.
- PDCA is repeated in each responding section of the organization.

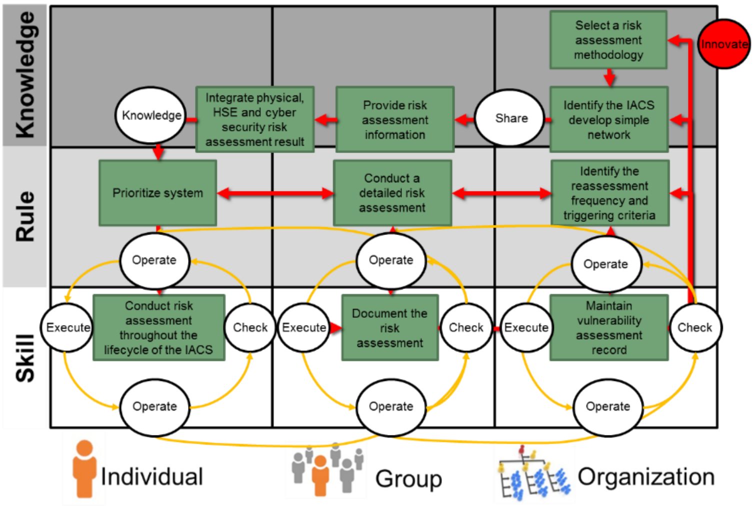
Knowledge
Rule
Skill
Select a risk assessment methodology
Innovate
Knowledge
Integrate physical, HSE and cyber security risk assessment result
Provide risk assessment information
Share
Identify the IACS develop simple network
Prioritize system
Conduct a detailed risk assessment
Identify the reassessment frequency and triggering criteria
Operate
Operate
Operate
Execute
Conduct risk assessment throughout the lifecycle of the IACS
Check
Execute
Document the risk assessment
Check
Execute
Maintain vulnerability assessment record
Check
Operate
Operate
Operate
Individual
Group
Organization

Figure 3. *RM for IEC 62443 based on the IDEF0 diagram*

4. SAFETY AND SECURITY MANAGEMENT FRAMEWORK

An ICS is typically used in industries and in manufacturing, and it conventionally connects the Internet with big data to analyze an appropriate way to improve a production process. The ICS hence presents numerous benefits to consumers and has the potential to enhance the ways in which consumers ultimately interact with each other via technology. However, the ICS is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend, particularly from the security and safety standpoints. As physical objects, dangerous risks to factory workforces inherently exist from regular equipment use and other potential sources.

The reason why it is important to identify ways of successfully integrating the security and safety requirements is that during a cyber incident, there are constraints on an organization (e.g., knowledge limitations and human resources) and the environment (e.g., resources and systems) targeted for the response. In addition, there are time constraints incumbent upon the emergency system during a cyber incident. Figure 4 shows the relationships between safety and security corresponding to a given resource. Since cyberattacks may cause unsafe conditions in control systems, safety measures are a top priority for implementation.

In the course of a safety-corresponding loop, a non-secure state is an output. The non-security state discussed herein refers to the state of the control system under the influence of the cyber incident and thus the state of an individual. Security correspondence is implemented against the output non-secure state. Safety and security's vital tenet of “connection” is the control of the global standard. With regard to safety, the OSHMS is adopted. However, with regard to security, IEC 62443 is adopted. Overall, the global standard requires a fundamental line of response from a safety perspective. As per the global standard analysis, the standard requires the PDCA cycle activities for continuous improvement. This is a practical and methodical approach for simultaneously achieving high levels of safety and security.

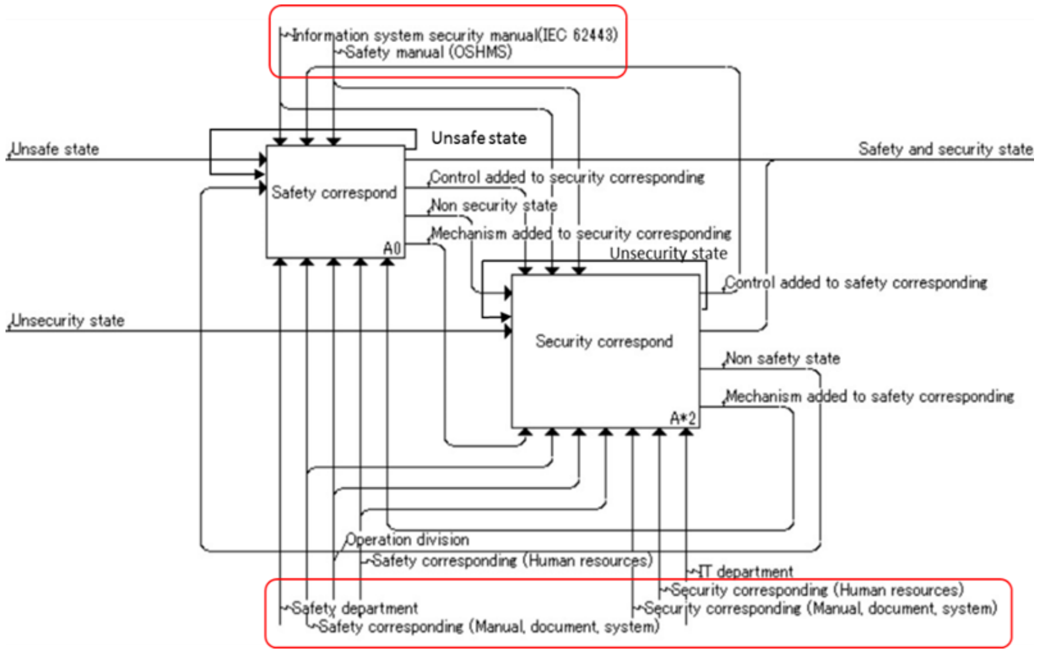
Information system security manual(IEC 62443)
Safety manual (OSHMS)
Unsafe state
Unsafe state
Safety and security state
Safety correspond
A0
Control added to security corresponding
Non security state
Mechanism added to security corresponding
Unsecurity state
Control added to safety corresponding
Unsecurity state
Security correspond
Non safety state
Mechanism added to safety corresponding
A*2
Operation division
Safety corresponding (Human resources)
IT department
Security corresponding (Human resources)
Safety department
Security corresponding (Manual, document, system)
Safety corresponding (Manual, document, system)

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

CONCLUSIONS

In this research, a combined methodology based on IEC 62443 and OSHMS was proposed. Discussions regarding this methodology were provided based on the global standard for combining the safety and security operations to maximize resilience levels against a cyberattack that cannot be perfectly eliminated.

Future perspectives with regard to the safety and security requirements within this domain need continuous education/training of the PDCA cycle. Moreover, personnel training regimens should be adopted based on this framework. Factory operators and IT administrators need to be approached and ultimately evaluated together as a single cohort. In addition, an illustrative example of such a proposed framework and methodology was presented based on exercises wherein nearly 200 CI personnel and security experts had participated.

Acknowledgements

This research is partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No. 16H01837 (2016).

REFERENCES

National Institute of Standards and Technology. (1993). Announcing the Standard for Integration Definition for Function Modeling (IDEF0). National Institute of Standards and Technology, NIST.

OHSAS Project Group. (2007). OHSAS18001: Occupational Health and Safety Management Systems - Requirement. Occupational Health and Safety Assessment Series. pp.90-179.

IEC Central Office. (2010). Industrial Communication Network-Network and system security- Part 2-1: Establishing and Industrial Automation and Control System Security Program. pp.18.

Nyambayar Davaadorj, Ichiro Koshijima, Hajime Eguchi. (2016). A Metric for Quantitative Estimation of Production Unit Based on OSHMS. 29th Symposium of Malaysian Chemical Engineers. pp.37.

Rasmussen J, senior member, IEEE. (1983). Skills, Rules, Knowledge. Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics. pp.257-266.