CYBER INCIDENT EXERCISE FOR SAFETY PROTECTION IN CRITICAL INFRASTRUCTURE

YUITAKA OTA, TOMOMI AOYAMA, DAVAAADORJ NYAMBAYAR & ICHIRO KOSHIJIMA
Industrial Management Engineering, Nagoya Institute of Technology, Japan.

ABSTRACT

Many companies, especially those that own critical infrastructure (CI), must prepare processes to cope with serious incidents before they happen. Conventional safety countermeasures already developed a priori to deal with expected problems, such as machinery malfunction, natural disasters and human errors. Field operators also are well trained against such problems. In recent years, however, cyber-attacks have emerged as a 'clear and present danger' and have rendered CI uncertain and unsafe through industrial control systems (ICSs). Thus, CI owners should now prepare countermeasures to ensure the safety and security of ICSs. Unfortunately, responding to situations without experience and developing adequate countermeasures is a difficult challenge. A certain resilience must be developed that gives the actors the ability to flexibly cope with a crisis and quickly recover to a safer state. In CI systems, field operators are the most important element for dynamically managing ICS emergency response.

In this paper, the authors would like to discuss the following two problems:

1. Simultaneous achievement framework of safety and security in ICSs
2. Personnel training methodology based on the above framework

Also, we present an illustrative example of the proposed framework and methods based on exercises in which almost 200 CI personnel and security experts participated.
Keywords: cyber-incident, personnel training, ICS-SIRT

1 INTRODUCTION

1.1 Background

The threat of cyber-attack to industrial control systems (ICSs) has been increasing since Stuxnet was discovered in Iran's uranium enrichment facility in 2010[1]. As a result, companies are obliged to compromise by increasing resilience against such sophisticated cyber-attacks through ICSs. In 2016, a blackout due to a cyber-attack occurred in Ukraine [2]. In this case, restoration was rapidly achieved (about 1 hour) by manual operations. In this case, restoration was rapidly achieved (about 1 hour) by manual operations learned from a previous attack in 2015 [3]. This case suggests that (i) cyber-attacks are a real threat for most ICSs and (ii) the human contribution is essential for responding to a cyber-attack.

It is essential to enhance security to protect companies from cyber-attacks. However, even if companies improve cyber security, preventing all cyber-attacks is impossible. Also, companies holding ICSs, especially Critical Infrastructures (CIs), support our everyday lives. Shutting down for the safety of CIs being threatened by cyber-attacks has a significant impact on social and business activities. In fact, the result of such a shutdown often satisfies the intention of the attackers. Therefore, companies involved with CI must consider not only plant safety but also business continuity.

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N2-246-257

1.2 Problem Statement

Companies holding ICSs have taken various countermeasures to ensure and maintain plant safety. These countermeasures are prepared considering malfunction of equipment, natural disasters, human errors, etc. as threatening plant safety. Not only have the factors that have been examined until now, but also cyber-attacks need to be considered as threatening plant safety. However, Japanese companies have not been seriously considering a cyber-attack as a cause of ICS malfunction. If a cyber-attack occurs, it may propagate not only cyber damage through the ICS network but also physical damages through the plant's physical structure. Thus, owners of CI should prepare countermeasures to ensure the safety and security of ICSs.

In Ref. [4], E-ISAC makes the following implications:

'The attacks highlight the need to develop active cyber defenses, capable and well-exercised incident response plans and resilient operations plans to survive a sophisticated attack and restore the system'.

As an example of such an approach, for the 2020 Olympic and Paralympic Games, the Japanese Ministry of Economy, Trade and Industry has promoted the 'Cybersecurity Management Guideline,' which includes human resource development in the industrial sector [5].

2 CYBER-ATTACKS ON INDUSTRIAL CONTROL SYSTEM

Figure 1 shows a cyber security testbed and a virtual ICS network. The testbed (Fig. 1) heats water with a heater in the lower tank and circulates the heated water through a simple pipeline to the upper tank (using a pump). The testbed is also equipped with actual industrial control devices and controlled automatically. In this ICS network, OLE for Process Control (OPC) Servers collect and exchange process data, and monitor them by using Supervisory Control And Data Acquisition (SCADA) function included in the OPC Servers. OPC Servers receive various parameters from the testbed's sensor, and SCADA gives instructions to the control equipment using the data of the parameters. This ICS network is designed by the secure zoning method proposed by Hashimoto [6] to suppress the damage of cyber-attacks.

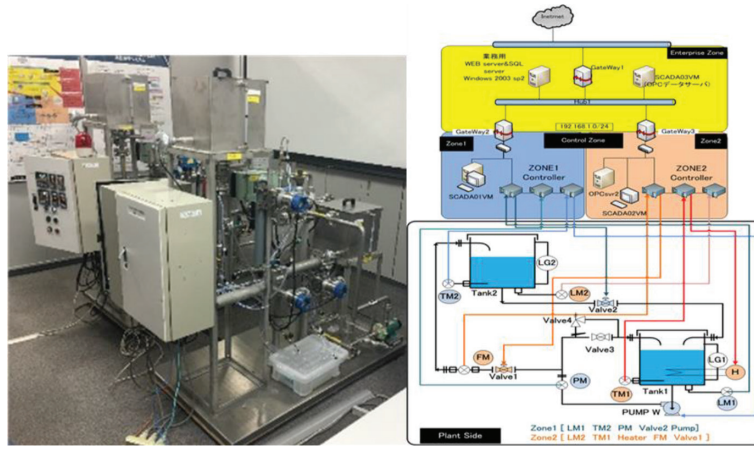

Figure 1: Cyber security testbed and ICS network.

The authors have demonstrated cyber-attacks against the testbed. According to the steps of the anatomy of a cyber-attack [7], the attacking procedure is determined as follows.

1. Attack Step 1: Reconnoitering and enumeration
   The attacker executes the Armitage to launch Metasploit framework [8]. Then, the attacker executes the Nmap, which scans a target network (ICS-2 Network 192.168.12.0/24). After completing the scan, the attacker gets target information.
2. Attack Step 2: Intrusion and advanced attacks
   According to the functions of the Armitage, the attacker ascertains an attack method and vulnerability in the Metasploit framework. The attacker exploits payloads, which execute inappropriate code in the use of the vulnerability. After sending the payloads, the attacker obtains administrator's permission for the OPC2 illegally.
3. Attack Step 3: Malware insertion
   The attacker uploads a malware execution file to an OPC2 background process so as to execute a malware file. The configuration file of OPC2 was rewritten, and then the OPC2 was restarted. Resulting from the attack, the valve controlled by the OPC2 shutdown.
4. Attack Step 4: Clean-up
   The attacker deletes the malware file and the configuration file from OPC2 storage so as not to leave the cyber-attacks evidence, and finish the cyber-attack.

Figure 2 shows monitoring screen shot in operation. As the valve is opened, the stage of the testbed changes. Usually, the state transition of the testbed appears on the monitor of the operator as shown in the left figure. The changing graph shows the liquid level of the upper tank. The liquid level is changing due to malfunction of the valve. The operator can notice the abnormality of the testbed due to the unusual process deviations from the steady state condition through the monitor. However, the attacker conceals the information about cyber-attack in order not to let anyone notice the cyber-attack. The monitoring screen of the testbed is concealed as shown in the right figure, while the cyber-attack causes serious accidents at the testbed.

This demonstration shows a possibility of safety incidents caused by cyber-attacks to ICS.

3 INCIDENT RESOPNSE AND ORGANIZATIONAL STRUCTURE

To date, malfunction of equipment, human error, etc. have been considered as causes of ICS malfunction. In addition to this reason, companies need to add cyber-attacks as a cause of ICS malfunction. Abnormal operation of a plant depends on the characteristics of the plant

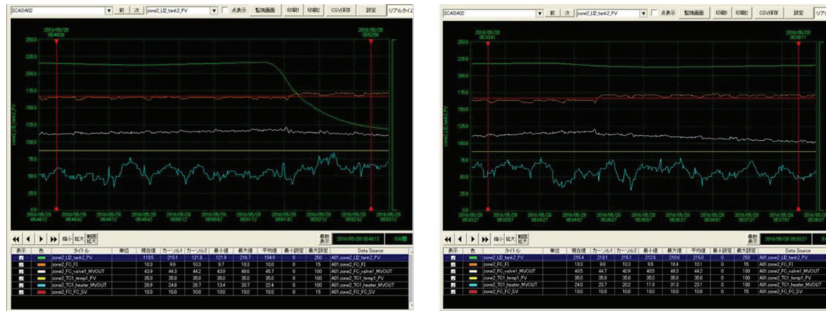

Figure 2: Monitoring screen shot in operation.

regardless of the cause of the ICS malfunction. In other words, the accident that occurs in a plant is the same regardless of whether the cause is a cyber-attack or another reason. Even if it is caused by cyber-attacks, the situation happening at a plant is the same as what has been experienced up to now.

3.1 Incident Response

Companies have made a lot of efforts to ensure the safety of their plants for many years. One of them includes response against plant abnormality. As mentioned previous section, even if plant abnormality caused by cyber-attacks is not different from the situation of the plant that companies have been experiencing until now, they can ensure the safety of the plant threatened by cyber-attacks by using this response (safety response).

Figure 3 shows the structure of cyber incident response. If the plant is operating abnormally caused by the cause considered so far, it is possible to restore plant safety by performing safety response as shown in the left figure. However, there is a possibility that cyber-attacks will interfere with safety response (e.g. concealment of the information of a plant on the monitor). Companies must consider where cyber-attacks interfere safety response. And it is necessary to take the response to eliminate the effect of cyber-attacks (security response) to take safety response as shown in the right figure. Therefore, if a cyber-attack causes abnormal operation of a plant, a response to rectify the situation is required in combination with a structure to add a security response to the safety response.

3.2 Organization Structure Required for Incident Response

In Japanese companies, when an incident happened at a plant, departments and divisions related in places where abnormality is caused have investigated the cause and responded. However, in the case of a cyber-attack (cyber incident), there is a possibility that damage other than the part where the abnormality is happening (infecting other equipment, etc.). In other words, various departments and divisions need to deal with cyber incidents. And if

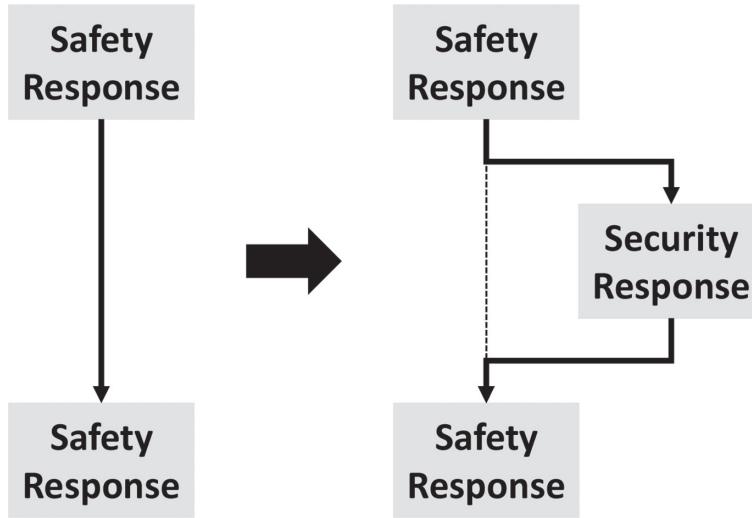

Figure 3: The structure of cyber incident response.

these departments and divisions deal with cyber incidents their own hands, proper response would be delayed, and the damage caused by cyber incidents could be expanded.

To respond proper response, it is necessary for companies to prepare an organizational structure according to the purpose to be achieved beforehand and to dynamically change the organizational structure in accordance with the trend of the situation (change in purpose).

The authors visualized the state in which the work volume changes over time (Fig. 4). And, we visualized the organizational structure required for incident response as well as the transition of the work volume.

a) Operation Staff
The purpose of this organization is to operate the plant normally and provide company's services. The operation Staff is familiar with the normal operation of the plant, so he/she can detect the behaviour of the plant different from normal operation.

b) ICS-ERT (Emergency Response Team)
The purpose of this organization is to ensure the plant safe whatever the cause is. Instead of focusing on the cause of plant malfunction, ICS-ERT will focus on the state of the plant and take response. Moreover, ICS-ERT do not work in herself, but manage the Operation Staff (including the IT Staff in the field) and ensure the safety of the plant.

c) ICS-SIRT (Security Incident Response Team)
The purpose of this organization is to respond to incidents and return to the state of normal plant for continuity Company's business. In the case of a plant abnormality caused by a cyber incident, it is necessary to respond to IT to ensure the safety of ICS not only for ICS.

d) CSIRT (Computer Security Incident Response Team)
The purpose of this organization is to respond to parts (IT system) other than the ICS-SIRT service (ICS system) and return it to the state of an ordinary enterprise IT system.

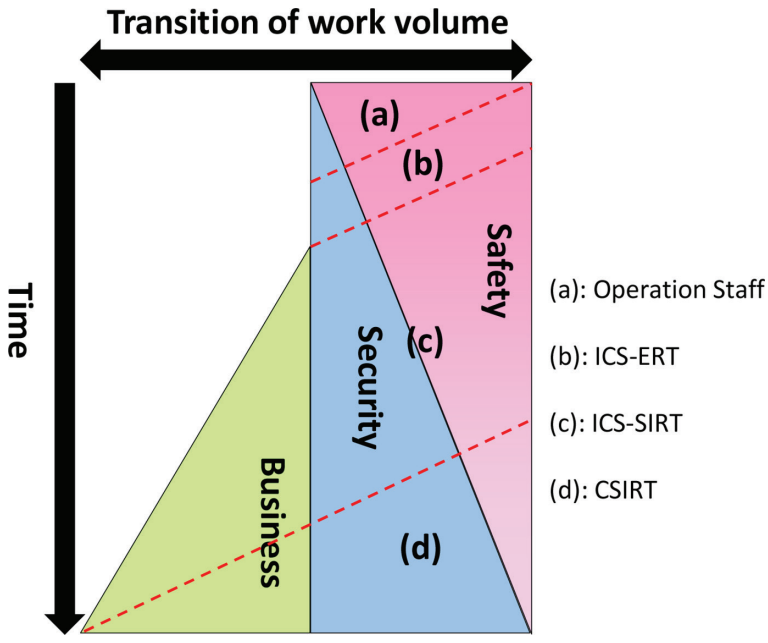

Figure 4: Organization image for cyber incident response.

4 EXERCISE IN BUSINESS CONTINUITY PLANT

To formulate measure to ensure the safety and security of ICS, it is necessary to experience how cyber-attacks affect ICS. By getting those experiences, companies can understand what measure can be taken to remove the effect of cyber-attacks. However, many companies don't have the experience of cyber-attacks to formulate measure against cyber-attacks (companies don't have the ability to detect even if it is cyber-attack). Therefore, to think about the measure of the inexperienced situation, the exercise, which can simulate the cyber-attack, can be effective.

4.1 Purpose of the Exercise

The purpose of the exercise is to 'learn how to think about organizational collaboration to deal with cyber-attacks on ICS.' Therefore, the object of the exercise is as follows;

Organization:	Organization concerned with administration of ICS Organization concerned with administration of business
Response:	Safety management (safety response), response to cyber-attack (security response)

Given the combination of organization and response, exercises must satisfy the following three requirements for participants:

- Appropriate information must be gathered for those who determine the source of the attack. If necessary information cannot be collected, the person determining the source of the attack cannot formulate an appropriate response. As a result, the response may be delayed, and the requisite information. In other words, communication must be smooth. Therefore, the exercise must enable participants to understand the importance of communication when dealing with abnormal situations.
- Many companies in Japan are trying to build CSIRT to respond to cyber incidents. However, CSIRT for IT systems cannot deal with problems related to ICSs. ICS-SIRT and ICS-SIRT are necessary when considering the cooperation of the targeted organization. Thus, the exercise makes it clear to participants the need for ICS-ERT and ICS-SIRT.
- Many companies are preparing safety measures in case of abnormal operation of a plant. This safety response can also be used as a response to cyber-attacks. Thus, participants in the exercise must understand that the safety response is available in the case of a cyber-attack.

4.2 Design of Exercise

It is effective to construct a case-based exercise to satisfy the requirements as mentioned above. The exercise consists of four scenarios: virtual enterprise, cyber-attacks, response to operational situation that becomes unsafe and plant operation during cyber-attack. It is needed to make it possible for participants to use a knowledge obtained through the exercise for their company. Therefore, the exercise scenario was made based on a testbed (Fig. 1). The testbed's structure is kept simple so that participants can focus on the essence of the exercise.

- Virtual enterprise scenario
  In this scenario, participants must think about how organizations can cooperate to handle cyber-attacks. To make it easier for participants to imagine organizational collaboration,

an organizational structure equivalent to that of the real company must be set up to the extent possible.

- Cyber-attacks
  This scenario requires participants to think about how to respond to incidents caused by cyber-attacks. Participants should be as real as possible so that participants gain experience in dealing with realistic cyber-attacks.
  This scenario is created based on the cyber-attack the authors are conducting.
- Response to operational situation that becomes unsafe
  This scenario allows participants to understand how cyber-attacks affect the safety response.
  This scenario simulates an abnormal operation of the testbed. The safety response to the situation is written in the workflow (Fig. 5).
- Plant operation during cyber-attack
  This scenario allows participants to understand the full impact of ICSs malfunction caused by a cyber-attack.
  This Scenario is created by observing the transition of the driving situation of the testbed due to the cyber-attack the authors are conducting.

4.3 Administration of Exercise

During the proposed exercise, participants should think about how it corresponds to a situation caused by a real cyber-attack and how this correspondence evolves over time. In the exercise, participants think about the reaction to the situation caused by the cyber-attack. If there are few coping people, the coping person cannot cope with the lack of resource. The reaction is thereby late. If the response is delayed, the attacker leads. If the attacker leads, the damage spreads. To prevent the damage spreads, it is necessary for a person coping with the

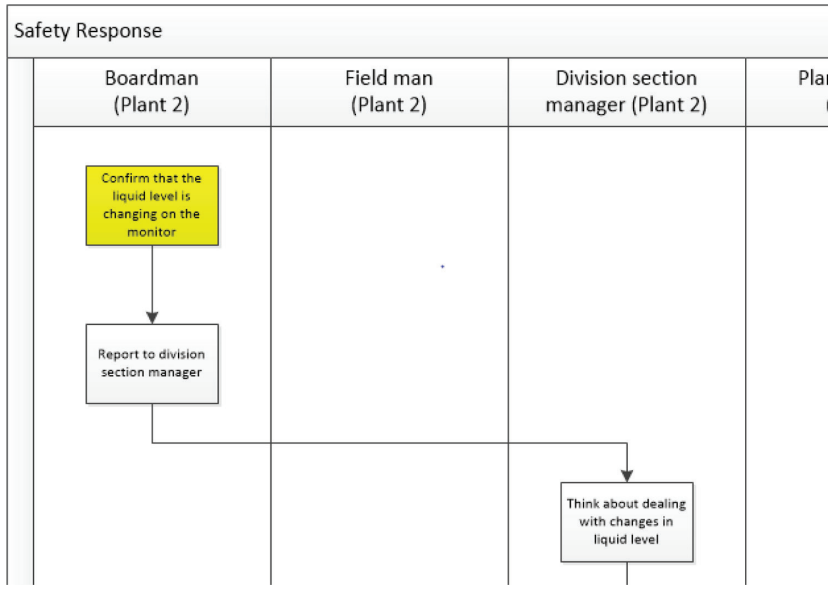

Figure 5: Safety response in the workflow (part).

situation caused by the cyber-attack to reconstitute an organization dynamically to avoid the attacker from leading.

To make effective responses, participants have to understand attacker's scenario. To ensure that participants understand the attacker's intention, the exercise is divided into three phases according to the attacker's scenario (Fig. 6).

1. Predictive phase
   The purpose of this phase is to ensure the safety of plants threatened by cyber-attacks. In this phase, the participants examine the safety response obstructed by a cyber-attack.
   After detecting suspicious communication in a section that monitors the network, the exercise begins with an alert for the status of the liquid in the plant. In this phase, the participants must ensure the safety of the plant. Once safety is ensured, participants must investigate the abnormal operation. In this phase, participants can recognize how different causes can influence the safety response.
2. Emergency phase
   The purpose of this phase is to continue business. The participants consider about the security of the plant and how the exercise implicates to a real cyber-attack. They must also take into account how their business will be affected by the cyber-attack. In this phase, the participants consider practical measures taken to ensure business continuity throughout the company.
   This phase begins after the abnormal operation of the plant reveals a cyber-attack. In this phase, participants can recognize that the entire company must be mobilized to treat a situation caused by a cyber-attack.

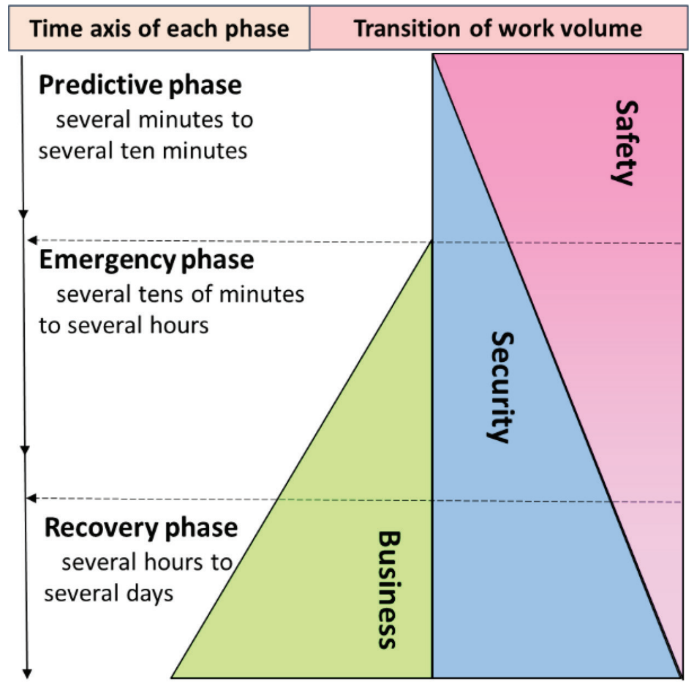

Figure 6: The structure of exercise with workload image for safety, security and business continuity activities.

3. Recovery phase
   The purpose of this phase is to restore own business to normal operation rapidly. The participants must find a way to nullify the influence of the cyber-attack so that the plant can return to normal operation. In addition, they must consider how business is affected by the temporary plant shut down. In this phase, the participants examine the start-up procedure of a plant crippled by a cyber-attack. In addition, the participants examine methods to prevent the recurrence of similar cyber-attacks.
   This phase begins after the plant is stopped by a cyber-attack. In this phase, participants think about how to restart the plant. In this phase, participants can see how different causes affect the restoration of normal plant operation.

4.4 Administration Method of Exercise

This exercise is done in groups that consist of four to six people. To consider organizational correspondence, participants come from different departments. The exercise requires participants to think about systematic countermeasures and collaborative communication. Therefore, no specific role is given to group members.

4.4.1 Exercise method

The exercise is conducted among members who have different backgrounds. The exercise is a discussion-based exercise for discussion will be active, compare participant's views on a common problem (cyber security) and achieve the purpose of the exercise.

4.4.2 Deliverables of Exercise

The typical deliverables of the exercise are workflow diagrams (Fig. 7), which become plans by considering 'who' performs the action and 'when.' Therefore, the horizontal axis of the worksheet corresponds to the department that does the action and the vertical axis of the worksheet corresponds to the timeline.

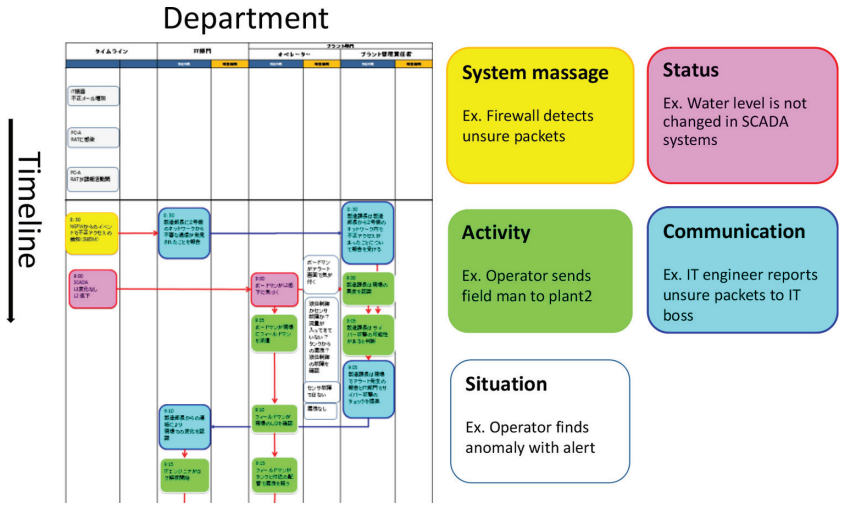

Figure 7: Sample workflow diagram.

4.4.3 Implementing Method

This exercise consists of five steps: an introduction, explanation of preconditions, group work, presentation of results and open discussion. As mentioned in the previous section, the exercise is divided into three phases. Of the five steps, explanation of preconditions, group work and presentation of results occur in each phase as one cycle.

1. Introduction
   The facilitator explains the purpose of the exercise and how to proceed. The general scenarios of the exercise are introduced to the members. At this step, members understand the importance of the exercise and should, therefore, be motivated to apply themselves fully in the exercise. By doing so, members can increase the benefit of the exercise.
2. Explanation of Preconditions
   Preconditions are set for each phase. Preconditions include the state of the plant, the state of the IT network, and the company situation. At the beginning of each phase, the facilitator explains the preconditions. At this point, members watch a video to understand the preconditions (the authors created the video and reproduced the preconditions).
3. Group Work
   The group work consists of workflows that add a security response to the safety response. An A0-size worksheet, colored sticky notes, and a marker are distributed to each group. A precondition and safe response are printed on each worksheet. After understanding the precondition and safety response written in the worksheet, the members do the group work. In group work, if a safety response is deemed insufficient, members add a response by writing the response on a sticky note and sticking it to the worksheet. The meaning of each sticky note depends on its color, so members should use sticky notes of the same color to express similar activities. Next, consider the relationship between the added response and the safety response and draw a line with a marker between the two. Through this exercise, members can visualize the response to cyber-attacks and the structure of the organization collaboration. Members can debate about the various departments involved based on the worksheet (Fig. 8).

Figure 8: An example of team discussion in group work.

4. Presentation
   Each group presents their work flow created in the group work while displaying their worksheet to all participants. In this presentation, each group explains not only the added responses but also why they were added.
5. Open-Discussion
   Members share among themselves the knowledge gained through the exercise. Sharing the knowledge through discussion increases the benefit of the exercise for all participants. Also, the administration and the members discuss whether the exercise was useful and whether the administration of the exercise was appropriate.

4.4.4 Administration Staff

The participants in this exercise are supposed to be about 30 to 40 members. The size and complexity of this exercise require a lot of help from the person to progress the exercise smooth. However, even if there are many people, the exercise does not proceed smoothly. For a smooth administration of the exercise, the role of administration staff divided as follows: facilitator, advisor and supporter.

a) Facilitator: The facilitator guides participants through the exercise. He/she explains purpose and method of the exercise at the introduction and the precondition at each phase. During the group work, the facilitator pays attention to each group's progress and manage the time of group work. After the group work is finished, the facilitator will ask questions of each group's deliverables so that the discussion will become active.
b) Adviser: the advisor participates in each group and supports members. The advisors don't actively support, but instead answer questions raised in the group work, explain preconditions in detail and provide advice on creating the workflow.
c) Supporter: The supporter is not directly involved in the exercise. However, it's hard to exercise without this role. The supporter sets up the exercise meeting place before exercise begins and distributes necessary tools for the group work.

4.5 Trial Exercise

To date, a total of 200 professionals has participated this exercise. They expressed a mostly positive opinion about the exercise method and the administration method. Figure 9 shows the level of satisfaction of the participants. According to this figure, the members were mostly satisfied with the exercise.

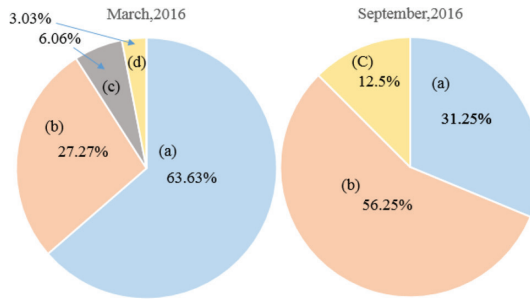

Figure 9: Satisfaction of exercise participant.

Participants understood the purpose of the exercise and recognized its importance. However, this exercise differs in many ways on a real company. Thus, many problems can be expected if this exercise is applied to a real company.

5 CONCLUDING REMARKS

In this paper, the authors explain the incident response and organization for incident response for the safety and security of ICS and examine exercises developed to train employees how to respond in the case of cyber-attacks.

In the future plan, by analyzing the deliverables obtained in the trial exercises, we will be able to improve the exercise. We derive the organizational structure and communication method for dynamical transformation of organizational structures. And we will develop a generic exercise package to be customized to extend this ICS-BCP exercise to various CI companies.

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) and Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), 'Cyber- Security for Critical Infrastructure' (Funding Agency: NEDO), however, all remaining errors are attributable to the authors.

REFERENCES

[1] Symantec Stuxnet – Modus Operandi, available at https://www.sans.org/summit-archives/file/summit-archive-1493844778.pdf (accessed 4 July 2017).

[2] The Center for Strategic Cyberspace + Security Science, available at: http://cscss.org/CS/2017/01/19/ukraine-confirms-december-kiev-blackout-was-cyber-sabotage/ (accessed 4 July 2017).

[3] SANS Industrial Control Systems Security Blog, available at https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (accessed 4 July 2017).

[4] E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid (March 18, 2016).

[5] Japanese Ministry of Economy, Trade and Industry, available at http://www.meti.go.jp/english/press/2015/1228_03.html (accessed 4 July 2017).

[6] Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Hamaguchi, T., Jing, S. & Koshijima, I., Safety securing approach against cyber-attacks for process control system. *Computers & Chemical Engineering*, **57**(15), pp. 181–186, 2013. https://doi.org/10.1016/j.compchemeng.2013.04.019

[7] Dell Sonicwall, Anatomy of a cyber-attack, Dell software, 2012.

[8] Metasploit Framework, available at http://www.metasploit.com/ (accessed 4 July 2017).