FRAMEWORK FOR CYBER INCIDENT RESPONSE TRAINING

HIDEKAZU HIRAI, TOMOMI AOYAMA, DAVAADORJ NYAMBAYAR & ICHIRO KOSHIJIMA
Industrial Management Engineering, Nagoya Institute of Technology, Japan

ABSTRACT

In recent years, the possibility of cyberattacks against industrial control systems (ICSs) has increased; therefore, ICS owners need to ensure they have suitable cyberattack countermeasures. Even though there are many Internet Technology (IT) tools available to counter known threats to ICS operating systems and application software, behind-the-scenes attackers may still find system vulnerabilities through constant effort. In this paper, the following topics are examined: 1. Cyber incident response methods, 2. Departments/people responsible for cyber incident responses and 3. Cyber incident response training. Since cyber incidents threaten ICSs, concerned departments are generally familiar with safety responses, which are indispensable. However, since cyber incidents can be malicious, such safety responses may be insufficient. Therefore, additional security measures are also necessary. In this paper, the authors clarify the relationship between safety responses and security responses when faced with cyber incidents to ensure that appropriate responses are implemented at the appropriate time. As cyber incident IT response processes cannot generally be applied to ICS-specific cyber incidents, an ICS cyber incident response process and an associated training program were developed to: 1. Ensure trainees understood the framework, 2. Allow trainees to develop correspondence with the specific steps. The training program was conducted for Japanese companies in December 2016, from which the effectiveness of the cyber incident response framework and the training program were confirmed.
Keywords: ICS, security, safety, incident response, training.

1 INTRODUCTION

In 2011, since Stuxnet was discovered in Iran's uranium enrichment facility [1], many cyber incidents have been reported around the world. In 2014, parts of a plant were destroyed, and a plant was stopped by cyberattacks, in German's steel mill [2]. Also in 2015 Ukrainian substation, a power outage occurred due to cyberattacks and exerted an enormous influence on residents [3]. To date, there have been no cases where serious accidents occurred due to cyberattacks in Japan's Critical Infrastructure (CIs). But, the Tokyo Olympic Games are being held in 2020, and every time the Olympic Games are held, possible cyberattacks are widely discussed.

At the 2012 London Olympic Games, there was a possibility that the opening ceremony could have been blacked out because of cyberattacks [4]; therefore, Japan's CIs must implement security measures to counter cyberattacks against Industrial Control System (ICS) for the Tokyo Olympic Games in 2020.

2 PROBLEM SETTING

As cyberattacks can threaten process safety of plants and cause plant outages, companies need to have appropriate cyber incident response mechanisms detailed in specific cyber incident response plans. To develop these plans, companies need to be aware of which response methods to use to effectively thwart the range of possible cyberattacks. Therefore, it has become imperative that companies have appropriate training. However, because of the rapid development of technology, it is often unclear as to how to respond effectively to cyberattacks and the organizational requirements necessary to initiate an effective cyber

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170251

incident response. These details, therefore, need to be clarified before any training is developed.

To develop effective training, the following points need to be determined:

1. Cyber incident response method
2. Department/people responsible for cyber incident response
3. Cyber incident response training.

3 CYBER INCIDENT RESPONSE METHOD

3.1 Cyber incident response based on a safety response

Plant abnormalities depend on the characteristics of the control system. Therefore, cyberattacks can cause the same abnormalities as equipment failure or poor operator control. As safety incidents have occurred many times in the past, organizations that have ICS (hereinafter, an ICS organization) are familiar with responding appropriately to safety incidents. In this paper, abnormalities caused by equipment failure or poor operator control are called safety incidents. Given the above, if safety responses to cyberattacks are properly implemented, the safety of a plant is not immediately threatened; therefore, cyber incident responses based on safety responses should be implemented.

Using the IDEF0 modelling response [5], we now clarify a cyber incident response based on a safety response. Fig. 1 shows a response model that implements safety responses for equipment failures. Rules and standard responses are then added to control the safety responses and ICS organizations, materials, and tools are added to the safety response mechanism. As shown in Fig. 1, if safety responses for equipment failure are properly implemented, the plant remains safe.

Fig. 2 shows a response model for cyberattack safety. It is already clear that safety responses can be effective against cyberattacks; however, these responses assume that the systems or people are in a secure state, which is often not the case.

In this paper, a non-secure state indicates a system state in which people may be affected by cyberattacks.

Examples of non-secure states are as follows:

a) Human machine interface (HMI) states that may be hidden
b) Control device states in which the control programs may have been falsified
c) States of the people who know that the HMI information may be hidden.

Since safety responses do not take into account the non-secure states shown in Fig. 2, the latter are an output from the safety responses. In Fig. 1 and Fig. 2, safety responses are described as one block; however, the process consists of many safety responses. Therefore, the non-secure states that are output from the safety responses indicate that the safety response process is executed in states that are encumbered by non-secure states.

Therefore, as there is a high probability that the safety responses are unable to be appropriately implemented if there are cyber incidents, the responses must be implemented to exclude all non-secure states that may encumber the safety response process. In this paper, responses to non-secure states are called security responses.

Fig. 3 shows a response model structure for cyberattacks based on the above discussion. Safety responses must first be implemented against cyberattacks. As safety responses do not account for non-secure states, these are output from the safety responses. Security responses to the non-secure states are implemented, and secure states are input to the safety responses. Consequently, it is possible to implement appropriate safety responses that take account of non-secure states.

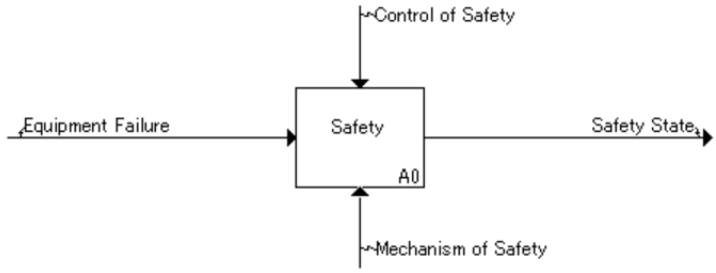

Figure 1: Response model showing the safety responses for equipment failure.

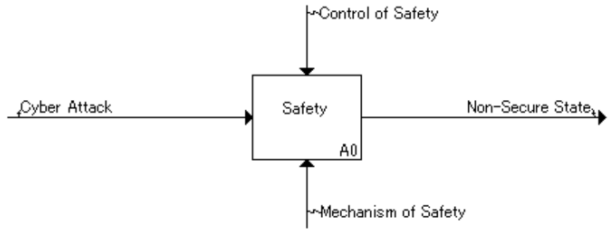

Figure 2: Response model for the implementation of safety responses against cyberattacks.

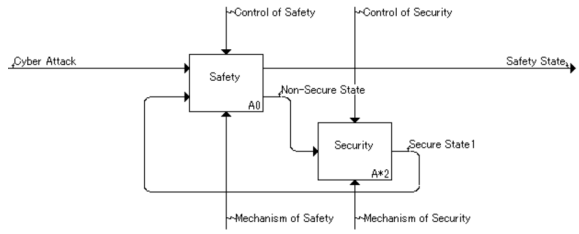

Figure 3: Effective response model against cyber-attacks.

3.2 Cyber incident response step

In 3.1, we demonstrated how security responses are added to the safety responses. However, to implement safety responses, the departments/people responsible for the responses must be aware of the occurrence of any abnormality. Further, to add security responses to safety responses, the departments/people responsible for the responses must realize that the cause of the abnormality is a cyberattack. Therefore, to ensure plant safety at the time of a cyber incident, it is necessary not only to respond to make the plant safe but also to detect the abnormality and specify the cause of that abnormality.

At the time of the cyber incident, it is also important not only to ensure plant safety but also to continue business operations. However, when a plant is in an unsafe state, it is

necessary to give priority to ensuring plant safety. Therefore, the response to business continuity should be implemented after ensuring plant safety.

Given the above, as it is important that appropriate responses be implemented in the event of a cyber incident, it is necessary to clarify the appropriate response procedure (hereinafter the cyber incident response steps.)

The requirements for the cyber incident response steps are as follows;

1. Detect abnormalities: Plant operations staff members are unlikely to notice abnormalities when under a cyberattack as the attackers may hide the HMI screens used to monitor the plant. As a result, despite suspicious behaviour, operations staff members monitoring the plant using HMI may not notice any abnormality. Therefore, it is important to first detect an abnormality.
2. Immediately act to ensure plant safety after detecting the abnormality: Cyberattacks threaten plant safety. Therefore, after confirming the abnormality, the top priority is to ensure plant safety.
3. Immediately identify whether the cause of the abnormality is a cyberattack or equipment failure: As cyberattacks can cause situations that seem similar to safety incidents, the departments/people responsible for the response may believe that the situation is a safety incident and implement only safety responses. However, when under a cyberattack, both safety and security responses must be implemented. Therefore, to quickly implement security responses, it is necessary to immediately identify that the cause of the abnormality is a cyberattack.
4. Investigate the cause in a way that does not disturb the responses to ensure plant safety: As described in point III, the cause of the abnormality must be immediately identified. However, in the initial response, the priority is to ensure plant safety. Therefore, investigating the cause of the abnormality must be implemented in a way that does not disturb the responses to ensure plant safety. As a full-scale investigation of the cause may disturb the responses to ensure plant safety, it should not be conducted until plant safety is assured. While ensuring plant safety, it is necessary to only investigate whether a situation is a cyber incident or a safety incident.

These are the requirements for the cyber incident response steps. Reference [6], stated that the following six steps should be implemented in response to cyber incidents on an information system:

- Step1: Detection of Event
  - Detect any unusual network activity.
- Step 2: Preliminary Analysis and Identification
  - Determine whether the unusual activity is a cyber incident.
- Step 3: Preliminary Response Action
  - Collect data for the initial defense to prevent any expansion of the damage and to analyze the possible causes.
- Step 4: Incident Analysis
  - Analyze the technical details, root cause, and potential impact of the cyber incident.
- Step 5: Response and Recovery
  - Recover the affected part (soft, hard) of the system to prevent further damage, restore normal operations, and prevent recurrences.

- Step 6: Post-Incident Analysis
    - Confirm the effectiveness and efficiency of the incident handling

The response step in reference [6], detecting abnormality, was Step 1. This satisfies requirement I of the cyber incident response steps. In the response step in reference [6], Step 2 judged whether to assess the situation as a cyber incident from the preliminary cause analysis, and Step 3 implemented provisional responses to prevent the spread of the damage, which satisfies requirements II and III in the cyber incident response steps.
In the response steps in reference [6], in Step 4, a full cause investigation is implemented to investigate the root cause. This satisfies requirement IV of the cyber incident response step.

Therefore, the response steps proposed in reference [6], are also effective as cyber incident response steps for the control system. However, the response steps proposed by reference [6], did not include any safety responses; therefore, safety responses have to be added to the response steps proposed by reference [6].

The safety response items to be added to each step are as follows:

- Step 1: Detection of event
    - Detect unusual plant behavior.
- Step 2: Preliminary analysis and identification
    - Determine whether the behavior is a normal abnormality or equipment failure.
- Step 3: Preliminary response action
    - Collect data for the initial response to ensure safety and generate data to prevent an insecure state and for further cause analysis.
- Step 4: Incident analysis
    - Analyze the technical details, root cause, and potential impact of the unsafe plant conditions.
- Step 5: Response and recovery
    - Restore the systems of the affected equipment, prevent further damage, and return to normal operations.
- Step 6: Post: Incident analysis
    - Confirm the effectiveness and efficiency of the safety response.

Table 1 shows the safety response items that are added to each step. At the time of the cyber incident, both safety responses and security responses must be implemented in each step.

4 DEPARTMENT/PEOPLE RESPONSIBLE FOR CYBER INCIDENT RESPONSE

As the cyber incident response methods clarified in section 3 are new, there is a possibility that they cannot be implemented within the existing company structure. Therefore, it is necessary to identify the section or department within the company that is to be responsible for executing the cyber incident response methods.

First, the section or department to be responsible for the cyber incident response based on the IDEF0 response model created in 3.1 must be clarified. In the IDEF0 response model, the section or department that has the capability, technology, and authority necessary to respond are added as the response mechanism. In ordinary companies, the ICS is responsible for the safety response mechanism and the IT section or department is responsible for the security

Table 1: Cyber incident response step.

Step	Security response	Safety response
Detection of Events	Detection of activity on network different from usual	Detection of plant behavior different from normal operation
Preliminary Analysis and Identification	Determine whether to treat it as cyber incident	Determine whether to treat it as normal abnormality or equipment failure
Preliminary Response Action	Data collection for initial movement for defense, prevention of damage expansion and further cause analysis	Data collection for initial response for ensuring safety, propagation prevention of insecure state and further cause analysis
Incident Analysis	Understand technical details, root cause and the potential impact of cyber incident	Understand technical details, root cause and the potential impact of plant unsafe conditions
Response and Recovery	Recover the current situation of the affected part (soft, hard), prevent further damage, restore normal operation and prevent recurrence	Restore the current state of the affected equipment, prevent further damage and return to normal operation
Post-Incident Analysis	Confirm the effectiveness and efficiency of incident handling	Confirm effectiveness and efficiency of safety response

response mechanism. However, there may be some crossover influences between the safety responses and the security mechanism, which may make implementation difficult.

Examples of the crossover influences between the safety and security responses are as follows:

a) The security response to isolate the infected devices in a control system means that these devices cannot be used as part of the safety response mechanism
b) The safety response to restart abnormal devices may cause data loss

When there are such crossover influences between the safety responses and the security responses, each response must be implemented with these influences taken into account. To that end, cooperation between the ICS department and the IT department is indispensable.

Fig. 4 shows the IDEF0 response from Fig. 3 with the addition of the crossover influences between the safety responses and the security responses as well as the cooperation between the relevant departments. In Fig. 4, the crossover influences between the safety responses and the security responses are described as the outputs of the safety responses, which are added to the security response control mechanism, and the output from the security responses are added to safety response control mechanism. The cooperation between the relevant departments is described as the security response mechanism added to the safety response mechanism and vice versa.

The safety responses and security responses may also influence business operations. For example, the security responses implemented to isolate infected devices may influence plant operations and result in plant shutdown, which, in turn, may have a serious impact on business operations. Therefore, to isolate the infected devices, cooperation is necessary between the ICS and IT departments as well as with management. If safety responses and security responses influence business operations, each response must only be implemented after the influences have been fully analyzed. To that end, cooperation among the ICS department, the IT department, and management is critical.

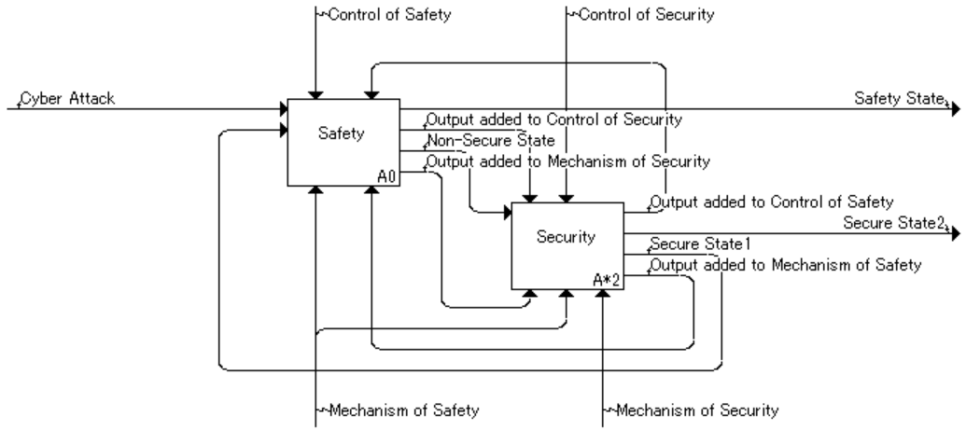

Figure 4: IDEF0 response model Fig 3 with the added crossover influences between the safety responses and the security responses as well as the cooperation between the relevant departments.

As using the IDEF0 response model can cause crossover influences among the safety responses, security responses, and business operations, cooperation between departments is indispensable. However, as incident resolution is time sensitive, there may not be time for the departments to coordinate. Here, therefore, we clarify the departments/people responsible for each cyber incident response step.

Step 1 must be implemented during daily plant operations. Therefore, Step 1 should ideally by implemented by the operations staff routinely involved in plant operations; this means that operations staff must be able to reliably detect any changes in a plant behavior.

In Steps 2 and 3, it is necessary to identify the cause of the abnormalities and implement safety responses. As the time between abnormality occurrence and an accident is generally short, a prompt response is essential. Therefore, at this point, it may not be possible or effective for the ICS and IT departments to cooperate as assumed in the IDEF0 response model. Therefore, the responses at this point must be implemented by the ICS department alone. To that end, ICS departments must have the ability to assess possible cyberattacks as being the cause of an abnormality and must have the ability to implement the security responses after suspecting a possible cyberattack.

In Step 2, when the cause of the abnormality is identified as a possible cyberattack, all devices connected to the network that are in non-secure states may threaten the safety of the plant. Therefore, security responses such as equipment isolation and network shutdown must be promptly implemented. However, these security responses require cooperation throughout the company as outlined in the IDEF0 response model. Therefore, the ICS department needs to have the ability and the authority to implement the security responses and communicate quickly with management.

From Step 4 onward, the parts affected by the cyberattack must be restored. At the time of the cyber incident, as all devices connected to the network were in a non-secure state, all devices related to plant operations must be restored first. However, as it may take time to respond to all non-secured devices, there may be a decline in plant service level, which could have a serious impact on business operations. Therefore, only provisional restoration can be

implemented, such as restoring the plant to a state in which only the minimal devices necessary for secure plant operations are restored to ensure a minimum service standard. As provisional restoration must be implemented company wide, in addition to the safety and security responses, judgments about the minimum plant service level required need company-wide cooperation. However, as provisional restoration must be implemented promptly, the ICS department should take the lead. Therefore, ICS needs to have the ability to implement the necessary security responses until the provisional restoration of the plant as well as have the authority to promptly communicate with management.

After provisional restoration, complete restoration responses must be implemented. Complete restoration means that the state and service level of the plant must return to the normal state. To return the plant service level to a normal state, it is necessary to ensure that all devices in the ICS and IT are secure before reconnecting the IT and ICS networks; therefore, cooperation between the ICS and IT departments is indispensable. Even if all devices in the company are secure and the ICS is returned to a normal state, unless recurrence prevention measures against future cyberattacks are introduced, there is a significant possibility of being attacked again. For this reason, preventive measures must be introduced in both ICS and IT before reconnecting the ICS and IT networks. Preventive measures, therefore, must be introduced on the basis of the root cause identified in Step 4. Because the IT department is responsible for Step 4, they should also implement measures to prevent any future recurrence against the ICS. Therefore, the implementation of complete restoration procedures must involve both the ICS and IT departments.

Given the above, as the department that leads the responses depends on the cyber incident response step being implemented, it is necessary to dynamically switch between the departments that are leading the specific responses. Table 2 shows the department responsible for each cyber incident response step. It needs to be understood, however, that these responses are not independent, as each step requires cooperation with the lead department in the previous and subsequent steps.

Table 2: Department responsible for each cyber incident response step.

Step	Security response	Safety response
Detection of Events	Detection of activity on network different from usual	Detection of plant behavior different from normal operation
Preliminary Analysis and Identification	Determine whether to treat it as cyber incident	Determine whether to treat it as normal abnormality or equipment failure
Preliminary Response Action	Data collection for initial movement for defense, prevention of damage expansion and further cause analysis	Data collection for initial response for ensuring safety, propagation prevention of insecure state and further cause analysis
Incident Analysis	Understand technical details, root cause and the potential impact of cyber incident	Understand technical details, root cause and the potential impact of plant unsafe conditions
Response and Recovery	Recover the current situation of the affected part (soft, hard), prevent further damage, restore normal operation and prevent recurrence	Restore the current state of the affected equipment, prevent further damage and return to normal operation
Post-Incident Analysis	Confirm the effectiveness and efficiency of incident handling	Confirm effectiveness and efficiency of safety response

Operation Staff
ICS-ERT
ICS-SIRT
CSIRT

The following is a description of each responsible department:

a) Operations Staff: Operations staff members are familiar with the normal operating states of the plant and are therefore able to detect unusual plant behavior.
b) ICS-Emergent Response Team (ICS-ERT): This department can implement the initial response to ensure plant safety when a plant abnormality due to a cyber incident is detected.
c) ICS-Security Incident Response Team (ICS-SIRT): This team identifies and isolates the parts affected by the cyberattacks and protects the ICS against any further attacks. This department also ensures the use of minimal devices to ensure continuing operations at the plant and also cooperates with management.
d) Cyber Incident Response Team (CSIRT): This team implements the cyber incident response on the information system to eliminate future cyberattack threats and also cooperates with management.

5 CYBER INCIDENT RESPONSE TRAINING

5.1 Development of cyber incident response training

The training was developed to ensure that the trainees understood the following cyber incident response items and all the mechanisms involved based on the safety response:

a) Cyber incident response based on safety response
b) Cyber incident response step
c) Departments responsible for cyber incident response

The training involved a desk exercise in which the trainees were involved in developing a cyber incident response.

The prerequisites necessary for developing the cyber incident response were as follows:

a) A fictitious company (business contents, organizational structure, and the abilities and authority of each person within the organization)
b) Plant operations at the company (physical plant instrumentation and plant system operation and logistics)
c) A cyberattack scenario for the fictitious company
d) Safety response scenario for the cyberattack scenario

Fig. 5 shows the cyber incident response worksheet that trainees complete. The vertical axis of the worksheet represents time, and the horizontal axis shows the person/department responsible for a specific response. The safety response scenario set as part of the preconditions is also fully described on the worksheet. Trainees then have to create a cyber incident response from the following procedure based on the IDEF0 response model.

1. Identify the non-secure state in the described safety response scenario
2. Consider the security responses against the non-secure states
3. Consider the people responsible for the security responses and the implementation timing and complete the responses on the worksheet

This procedure was based on the IDEF0 response model shown in 3.1.

Through this exercise, trainees come to understand a cyber incident response based on a safety response as well as the people/departments responsible for each step.

The training is divided into three phases: a preliminary phase, an emergency phase, and a recovery phase. Table 3 shows the position of each phase in the cyber incident response process. Trainees must develop an appropriate cyber incident response for each phase on the

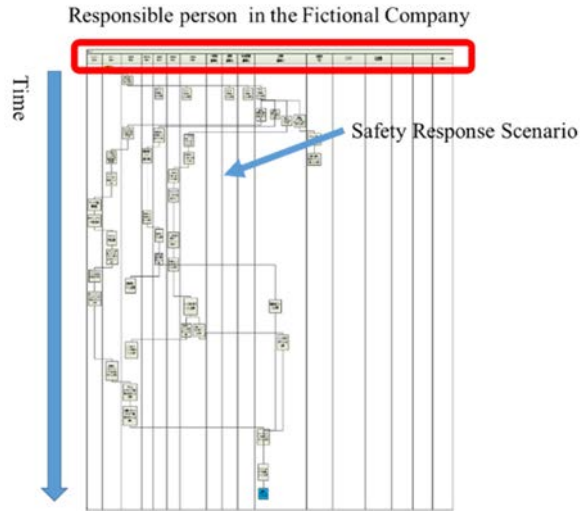

Figure 5: Worksheet provided to trainees.

Table 3: Position of each phase in the cyber incident response process.

	Step	Security response	Safety response
Predictive phase	Detection of Events	Detection of activity on network different from usual	Detection of plant behavior different from normal operation
Emergency phase	Preliminary Analysis and Identification	Determine whether to treat it as cyber incident	Determine whether to treat it as normal abnormality or equipment failure
	Preliminary Response Action	Data collection for initial movement for defense, prevention of damage expansion and further cause analysis	Data collection for initial response for ensuring safety, propagation prevention of insecure state and further cause analysis
Recovery phase	Incident Analysis	Understand technical details, root cause and the potential impact of cyber incident	Understand technical details, root cause and the potential impact of plant unsafe conditions
	Response and Recovery	Recover the current situation of the affected part (soft, hard), prevent further damage, restore normal operation and prevent recurrence	Restore the current state of the affected equipment, prevent further damage and return to normal operation
	Post-Incident Analysis	Confirm the effectiveness and efficiency of incident handling	Confirm effectiveness and efficiency of safety response

basis of the cyber incident response step, which allows them to gain a deeper understanding of each cyber incident response step and the people/departments responsible.
The outlines of each phase are as follows:

1. Preliminary phase: The point at which an abnormality occurs in the plant is set as the start point. Trainees develop responses to ensure plant safety and responses to specify a cause for the abnormality
2. Emergency phase: The point at which it is determined that the cause of the abnormality was a cyberattack is the start point. Trainees develop an initial response after a cyberattack is determined as the cause
3. Recovery phase: The point at which the plant stops is set as the start point. Trainees have to create responses to restore a plant that has stopped because of a cyberattack

5.2 Cyber incident response training results

The cyber incident response training was conducted for companies at the end of 2016.
To measure the degree of mastery of the cyber incident response training, the training deliverables were evaluated using the following:

a) Whether the non-secure states in the described safety responses were identified
b) Whether an appropriate security response was developed for the specified non-secure states
c) Whether the people/departments responsible for the security responses were appropriately specified
d) Whether the developed responses were suitable for the response purpose in each phase based on the cyber incident response process

For most deliverables, the above items were implemented properly. Therefore, it can be said that the trainees understood the cyber incident response methods and the people/departments responsible for the responses.

CONCLUSION

This research developed cyber incident training for companies with ICS. To that end, cyber incident response methods and the people/departments responsible for the cyber incident responses were first clarified. After that, training was developed to help staff understand the safety and security response logistics. The feedback from the training confirmed that the trainees understood the cyber incident response methods and people/departments responsible for the specific cyber incident responses.

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] file:///C:/Users/deveroper/Downloads/20110210-oguma.pdf. Accessed on: 27 May 2017.
[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=2. Accessed on: 27 May 2017.
[3] file:///C:/Users/deveroper/Downloads/20160217_CSC-JPCERT01%20.pdf. Accessed on: 27 May 2017.
[4] http://www.bbc.com/news/uk-23195283. Accessed on: 27 May 2017.
[5] IDEF0 function Modelling Method; University Dr. College Station Texas 77840 United states, Online, http://www.idef.com/idefo-function_modeling_method. Accessed on: 3 Jan. 2017.
[6] 21st Century U.S. Military Documents Cyber Incident Handling Program, US Government, Department of Defence, US Military, US. Air Force, 2013.