A Study on Introducing Cyber Security Incident Reporting Regulations for Nuclear Facilities

Chaechang Lee

Korea Institute of Nuclear Nonproliferation and Control
Daejeon, Republic of Korea
Email: chiching@kinac.re.kr

***Abstract*—Industrial control systems have recently become easy prey for cyber attacks as they expand to the Internet, beyond data communication through the network. Among industrial control systems, the systems used by nuclear facilities are especially at high risk against cyber attacks because their dangerous assets are used in managing nuclear materials. Most of the nuclear licensees have recently established cyber security response plans to protect their critical systems from cyber threats. To enable the response plans, effective incident reporting procedures should also be established and notified to personnel who has responsibilities to discover and report an undesired event in a timely manner. This study presents ongoing work, which is part of the study for establishing a cyber security incident response framework for nuclear facilities, and to introduce cyber security incident reporting regulations at nuclear facilities in the Republic of Korea.**

Keywords–Cyber Security; Incident Response; Nuclear Facilities; Reporting Regulation.

I. Introduction

Cyber security threats to industrial control environments have increased significantly because industrial control systems (ICSs) have changed from proprietary, isolated systems to PC-based open architectures and standard technologies interconnected with other networks and the Internet [1].

If a cyber attack occurs and results in damage, infrastructures such as public transportation, water, gas, as well as general IT systems incur financial losses or inconveniences to public amenities. However, cyber attacks on nuclear facilities threaten public safety and life by causing adverse effects on the safety functions of nuclear facilities. Therefore, in order to respond quickly and properly to cyber security incidents, nuclear licensees are required to have a more detailed cyber security incident response system than any other environmental licensees and to prepare incident reporting regulations to enable this. This paper, as a part of the research on building a cyber security incident response system for nuclear facilities in the Republic of Korea (ROK), presents the essential considerations of a regulatory authority in the process of developing and introducing incident reporting regulations.

It also uses practical contexts derived from consultations between regulators and nuclear licensees. In Section 1, the related works and contributions of this paper are presented. In Section 2, the paper describes the difference between incident reporting regulations for nuclear facilities compared to other critical infrastructures or general IT systems. Considerations to introduce incident reporting regulations at nuclear facilities are also presented in Section 2. Section 3 concludes the paper.

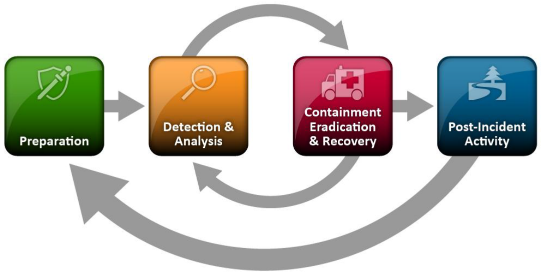

Figure 1. Incident Response Life Cycle [2]

A. Related work

There are several related standards and documents that guide cyber security incident response and reporting.

The National Institute of Standards and Technology (NIST) suggests the standard process to response cyber security incidents [2] and the International Atomic Energy Agency (IAEA) also cites it as the computer security incident response phases [3]. Figure 1 shows the process of incident response. NIST also demands the establishment of an incident report mechanism that permits people to report incidents anonymously [2].

The European Network and Information Security Agency (ENISA) describes good practices guide for the management of network and information security incidents on incident handling [4]. The main topic of the guideline is the incident handling process. The guide includes the formal framework for Computer Emergency Response Teams (CERTs, also known as CSIRTs), roles, workflows, basic CERT policies, cooperation, outsourcing, and reporting. However, the report guideline of the publication is presented for senior managers on how to manage incidents, and not for incident responses. ENISA also presents proposals for incident reporting to public authorities, private organizations and trust service providers, trying an introduction of a new reporting scheme or an improvement of standing procedures, under Article 19 of the electronic IDentification, Authentication and trust Services (eIDAS) regulation [5][6]. Guidelines for managing and reporting cyber security events presented by ENISA cover general IT environments. However, responding to and reporting of cyber security incidents that apply to nuclear facilities are distinct from general IT environments and other critical infrastructures. A detailed analysis is provided in Section 3.

In earlier studies, J. J. Gonzalez introduced a cyber security reporting system to share cyber security data, such as intrusion

ISBN: 978-1-61208-605-7

attempts, successful intrusions, and incidents of all types. He urged that it could lead to a more comprehensive and effective cyber data collection and analysis [7]. C. W. Johnson identified some of the challenges that frustrate the exchange of lessons learned from cyber security incidents in safety-related applications. He then argued for the integration of reporting mechanisms for cyber attacks on safety-critical national infrastructures [8]. R. Leszczyna and M. R. Wrobel proposed an approach to developing a data model for security information sharing platform for the smart grid [9]. All these previous research were focused on information sharing of security data. They however did not introduce reporting regulations for instant incident responses.

Especially at nuclear facilities, the IAEA states the goal and challenges of reporting during the computer security incident response process [3]. Additionally, the IAEA states that the goal of reporting is to ensure that everyone who needs to know about a computer security incident is informed in a timely manner. The IAEA further presents that the determination of the frequency of reporting and the level of detail required is a challenge to organizations [3]. However, it focuses on phases of incident response at nuclear facilities and analysis of the incident, and reporting is only briefly mentioned as one of the phases.

The United States (US) and Nuclear Regulatory Commission (NRC) have already introduced and applied cyber security event notification in the form of Code of Federal Regulations (CFR). [10] and [11] classify the cyber security events and set a time limit for reporting according to its severity. They also describe the process and method to notify the events in detail. However, they are based on the incident response infrastructure and systems in the US, and it is difficult to apply it in a country where the well-organized environment is not prepared.

This paper presents the essential items, based on experience of practical regulation and policy introduction, to be considered by the countries and regulatory agencies that intend to introduce reporting rules of responding to cyber incidents at nuclear facilities.

II. Considerations to introducing the policy

Cyber security incident response and reporting at nuclear facilities are different from the ordinary IT environments and other critical infrastructure.

- Unlike a typical IT environment, when a cyber security incident occurs at a nuclear facility, the personnel who discover and respond to the incident must consider the radiation effects. The activities that need to be done between report and response depend on the nature of the radiation effects, the content to report, and the status of the person or extent of the organization receiving the report. Hence, subsequent reporting of the situation is required whenever circumstances change.
- Systems at nuclear facilities, such as PLC, DCS, and HMI have a variety of accessible users: operators, maintenance personnel, security personnel, auditors, and contractors. Therefore, if anyone with access to the system discovers an undesired event, a standardized reporting form is required to accurately communicate the situation. Additionally, because the physical space of the facility is large, compared to an IT environment and, additionally, because there are dangerous areas where CERTs have restrict access, it may be difficult to directly assess the situation and notify the appropriate authorities or experts. Therefore, it is necessary to establish a clear reporting method for all accessible users to report the situation to the experts, and periodical training should be carried out.
- Some systems at a nuclear facility may be out of date, need to be updated, or run security programs such as an antivirus software. In such a case, it may be difficult for the user to notice a malicious access to the systems. If no security programs are run and no security policies are set, it may be difficult to detect a malicious intrusion. The operator may suspect the possibility of a compromise of the system only after finding an abnormality in the operation of the facility. Therefore, in order to confirm a cyber attack, it is necessary to consider not only notifications of cyber threats but also notifications of an abnormal situation related to the operation of the facility, such as rapid pressure or temperature change.
- In IT systems, data confidentiality and integrity are typically the primary concerns. For an ICS, human safety and fault tolerance in preventing loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products, are the primary concerns. Therefore, incidents that should be reported in the IT environment may not be necessary to report because of their low severity at a nuclear facility. Conversely, incidents that are overlooked in an IT environment may be a serious incident that must be reported at a nuclear facility.

Depending on the mission and nature of the organization that is responsible for introducing cyber security incident reporting policy, the purpose of creating the reporting requirements is different. Accordingly, the considerations in developing and introducing reporting regulations may vary. This section presents the considerations that the organizations should address to establish cyber security incident reporting regulations.

A. Scope of cyber security incident

First, the scope of cyber security incidents that may arise at a nuclear facility should be defined to apply incident reporting and incident response procedures. This means that assets, in the same manner as systems and network at nuclear facilities, should be identified to protect from cyber attacks by carrying out planned response activities.

Nuclear facilities have various services from enterprise business networks, including e-mail service, web server, and the Internet, to process control instrumentation bus network connected to sensors, actuators, and instrumentation. In addition, there are various systems, such as not only office PCs but also PLCs, DCSs, and HMIs located in the operations zone of nuclear facilities. Licensees should identify and select the essential assets among them to apply the established reporting regulation. For example, the NRC defined systems that perform safety, security, and emergency preparedness functions as critical digital assets that should be thoroughly protected from cyber attacks [12].

B. Subject of report

The person or entity to be responsible for the decision to report an incidence should be taken into consideration. If a reporting entity is not specified, it may result in unnecessary time loss from the time of incidence report to an appropriate response. As a reporting entity, the following persons may be considered: Operators of the nuclear facilities who first discover an undesired event; the team manager of the operators; and cyber security experts at the nuclear facilities who can determine whether the event was caused by digital threats. Because the reporting entity affects the immediacy and the concreteness of the reporting, it may vary according to the mission and nature of the organization.

NIST requires at least one reporting mechanism that allows for anonymous reporting [2].

C. Reportable incidents

It is not easy to damage nuclear facilities and disrupt normal operation with cyber attacks. The control networks of the nuclear facilities are usually separated from the external network such as the Internet. The control systems of the nuclear facilities have different platforms from the ordinary personal computer and requires specialized skills to implement malicious codes with the intent of compromising the control system. Nonetheless, nuclear facilities are an attractive prey to cyber terrorists because of their impact and influence. Attackers would gather the necessary information to carry out cyber attacks and infiltrate the control network based on the collected information. Thereafter, they would attempt to control the targeted systems and damage the nuclear facilities. All these processes are referred to as Advanced Persistent Threats (APT) attack.

When defining the reportable events, the nuclear facilities can categorize the cyber security events possible in the nuclear facility and present them as reportable events according to each stage of the APT attack: Preparation, Access, Resident, Harvest [13].

However, it is difficult for an on-site operator to determine immediately if the undesired events on the systems and networks are caused by the harvest stage of an APT attack, or by other causes such as mechanical or electrical faults, malfunctions due to the lifetime of the device, and human error. Therefore, when creating cyber security reporting regulations, it is necessary to provide a criterion for judging an incident that cannot be clearly determined as a cyber threat as a reportable event.

The most representative event, detectable and reportable at the stage of access or resident in an APT attack process, is a discovery of malicious software, also known as a malware, by an antivirus program. Even if the malicious effect of the malware on the systems and networks of nuclear facilities is difficult to establish immediately upon discovery, it must be reported because of the potential to adversely impact them. Additionally, the malware need to be analyzed to ascertain their infiltration routes and take preventive measures. Any unauthorized activities including creation, deletion, and modification of an account ID/PW, programs, and processes, and the alteration to configurations are also reportable events, which can be discovered at the stage of access or resident stage.

The events that can be discovered and reported during the preparation stage of the cyber attack include the collection of information indicating a planned cyber attack against nuclear facilities, such as a threatening message on SNS or a website posting. Although these events may not yet have been initiated and their severity and immediacy of response are relatively low, they must be reported and a proactive approach should be taken thereafter.

NRC has classified the reportable events into three cases and presents example events for each case [11].

D. Report flow

In cyber security reporting regulations, the organization or agency to which report must be made after the discovery of a cyber security incident should be defined. The IAEA suggests, as part of its goal of reporting, that everyone who needs to know about a computer security incident should be informed in a timely manner [3]. First, if the person who discovers an undesired event cannot determine whether incident responses are required with cyber security approaches, he or she should notify a cyber security team who can determine whether it is a result of cyber threats. The cyber security team should determine whether a professional technical support is needed, and report it to the incident handler or CSIRT. In addition, because similar cyber attacks at other nuclear sites such as cyber terrorism can occur simultaneously, it should be reported to a regulatory authority and the relevant authorities that manage and supervise nuclear facilities. The authorities related to nuclear facilities should collect information about the situation at other facilities and determine whether a national cyber terrorism crisis is ongoing, then report it to a national control center for the cyber crisis response.

The scope of the people who need to know about a computer security incident can be extended as much as possible according to the determinant of the situation being reported. In particular, if it is deemed that there are possibilities of a radiological damage due to a discovered incident, a radiological emergency must be promptly declared and appropriate the radiological disaster prevention organization, which implements appropriate protective measures, must be notified of the situation.

E. Means and contents of reporting

Various means can be used to report, such as by means of a phone, fax, or e-mail. Telecommunications is a useful reporting tool to deliver the fastest in-the-field situation. However, because of the nature of the information being disseminated verbally, untrained reporters may omit the important information that must be included in the report or may deliver ambiguous semantics. In the case of faxes or e-mails, because the recipients may not be reached in time or be aware of the reporting, they are unsuitable for the initial reporting of incidents. In particular, e-mails that require access to the Internet can be an inappropriate reporting tool in some cases. This is because the location of nuclear facilities where a cyber security incident occurs may be situated far away from the office where the Internet service is available. Additionally, the cyber attacks may have compromised the Internet connection or the e-mail system. The contacts used for reporting should always be kept up-to-date and multiple methods should be prepared in advance [2].

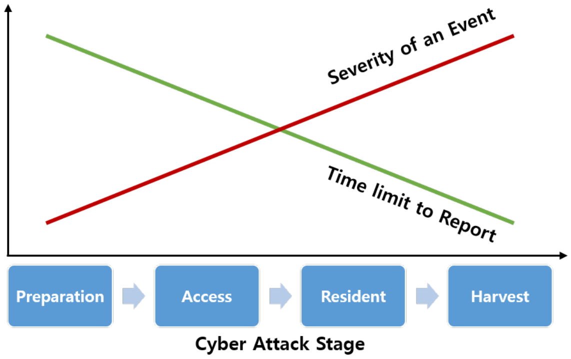

Figure 2. The correlations of the severity of the incident and the time limit to report by the stage of an APT attack

A form of written reports should be prepared in a pre-defined form so that senders know in advance what kind of information needs to be written and reported. The written reports must include the name and contact number of the reporter, the date and time when the event occurred or was discovered, the affected systems and networks of the nuclear facility, the actions that were taken, and the current status of the facility [2][11].

F. Report process

Most reports do not get finalized on the first attempt. After the initial reporting of a discovered situation, follow-up reporting is continuously required, based on changes in circumstances or gathered information. When a cyber security incident reporting regulation is enacted, a 2-step or 3-step reporting procedure can be presented in conjunction with the reporting method. Both processes take verbal reports as the first step in event reporting. When the event is initially discovered, it is important to promptly report through the available telephonic systems, such as by means of a telephone, hotline, or mobile phone.

Thereafter, the 2-step reporting procedure, such as the one implemented by the regulation of NRC, requires a detailed description of the discovered incident and the corresponding response activities in a single written report.

The 3-step reporting procedure requires, additionally, an analysis of the incident, which may take a long time after the licensee’s second report. It also includes a description of corrective plans to take as preventive measures against similar types of incidents. This method is useful for the regulatory authority responsible for assessing and determining whether the incident response activities and their corrective plans are appropriate for the nuclear facilities.

The discovered cyber security incidents should be reported in a timely manner, depending on the severity of the incident to the nuclear facility. Time loss in collecting accurate information can cause delays to a timely response. The more likely an impactful incident on the safety of a nuclear facility, the more desirable a fast report and quick response.

Figure 2 shows the correlations of the severity of the incident and the time limit to report by the stage of the APT attack.

G. Report on classified information

Cyber security incident reporting regulation should contain the reporting method for sensitive information classified as confidential such as [11]. During the ongoing cyber attack, reporting the incident through an open network, which is an unprotected channel, can result in additional cyber security damage such as information leakage. It is therefore best to prepare a channel for secure communication that uses asymmetric key encryption with a certification for public key verification. However, if the dedicated systems are not prepared for transmission and reception of sensitive information, a guideline should be prepared to indicate the temporary measures for reporting the classified information, such as using a symmetric key to encrypt the file containing the information, and transmitting the key via another channel.

H. Response and follow-up action

When introducing cyber security reporting regulations, it should include the response and follow-up actions that each team and organization received the report should perform.

Because the operator in charge of a system at the nuclear facility always operates and manages the on-site system, he or she has the primary responsibility to find out the cause of the abnormal situation when the undesired event was discovered. The system operator should determine whether there are radiological effects and evaluate the event according to the International Nuclear and Radiological Event Scale (INES) standards, based on the severity of the event, by checking the status of the nuclear facility [14]. If there is no radiological effect, the operator should check whether the undesired event is the result of a simple mechanical or electrical fault, or whether the guaranteed days of the system has expired.

A cyber security team at a nuclear facility has the responsibility of determining whether the abnormal situation of the reported system is the result of cyber threats. Various system logs can be used by the team as reasonable evidence for cyber threats, such as the event log, the status of the executed process, network configuration, antivirus log, and register values. The cyber security team also should determine whether it is possible to deal with the cyber threats using their own response capabilities. In the case of planned cyber attacks, ongoing incidents, or incidents requiring the services of a professional cyber security response team for an initial incident investigation, the situation should be notified to CSIRT.

CSIRT, the special team for cyber security incident responses, protects nuclear facilities by preventing ongoing cyber security attacks and analyzing the incidents. In the case of an intended cyber attack, they find possible suspects and hand over the case to the appropriate law enforcement agencies. The cyber security team and CSIRT should identify the cause of the incident and establish corrective actions to take as preventive measures against similar types of incidents in the future.

Figure 3 shows the report flow with responses and follow-up actions.

III. Conclusion

This paper presented the issues that a regulatory body should consider when introducing reporting regulations for cyber security incidents at nuclear facilities. The regulator should ensure that nuclear facilities not only establish cyber security

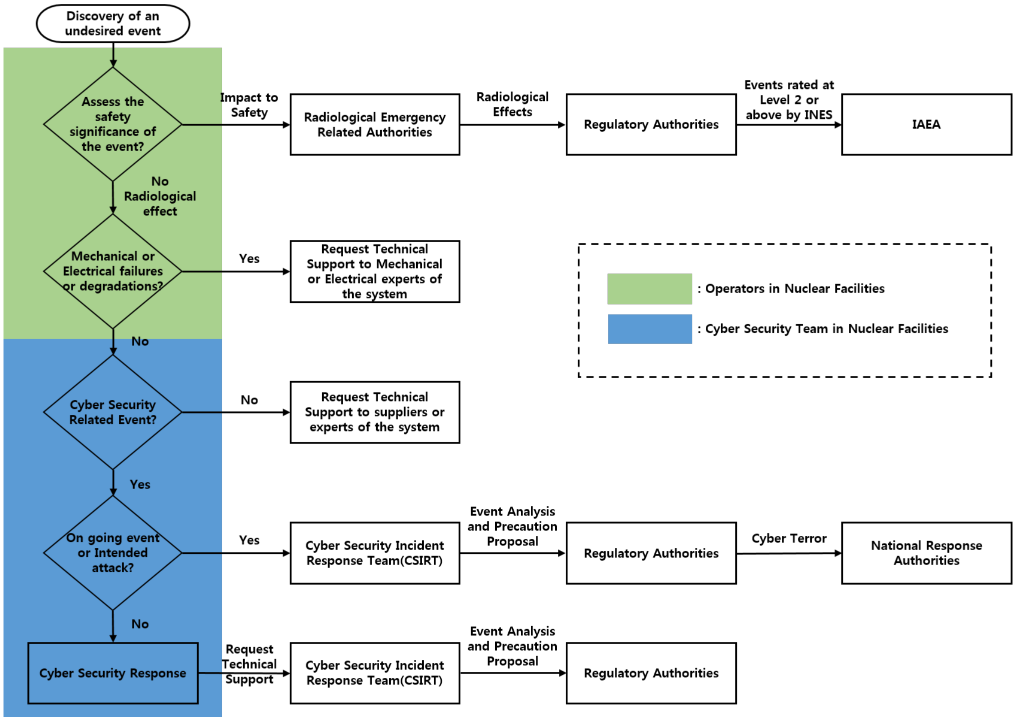
Discovery of an undesired event
Assess the safety significance of the event?
Impact to Safety
Radiological Emergency Related Authorities
Radiological Effects
Regulatory Authorities
Events rated at Level 2 or above by INES
IAEA
No Radiological effect
Mechanical or Electrical failures or degradations?
Yes
Request Technical Support to Mechanical or Electrical experts of the system
🟩 : Operators in Nuclear Facilities
🟦 : Cyber Security Team in Nuclear Facilities
No
Cyber Security Related Event?
No
Request Technical Support to suppliers or experts of the system
Yes
On going event or Intended attack?
Yes
Cyber Security Incident Response Team(CSIRT)
Event Analysis and Precaution Proposal
Regulatory Authorities
Cyber Terror
National Response Authorities
No
Cyber Security Response
Request Technical Support
Cyber Security Incident Response Team(CSIRT)
Event Analysis and Precaution Proposal
Regulatory Authorities

Figure 3. The report flow with responses and follow-up actions

incident response plans or procedures as preparatory measures against increasing terrorism threats, but also pay attention to prepare reporting regulations so that the prepared response systems can be activated in a timely manner. The reporting regulations should be created through thorough discussions by the relevant personnel and authorities on the presented considerations according to the role and nature of the organization introducing the reporting regulation. In addition, established regulations should be a practical guideline with continuous cyber security education and incident response training. For this, the subsequent study will discuss how incident reporting regulations can be implemented effectively and how regulators can identify unforeseen loopholes in the reporting system.

REFERENCES

[1] “Cyber Risks for Industrial Control Systems,” 2015, URL: https://www.if-insurance.com/ [accessed: 2017-06-08].

[2] P. Cichonski, T. Mllar, T. Grance, and K. Scarfone, Computer Security Incident Handling Guide: NIST Special Publication 800-61, Revision 2, National Institute of Standards and Technology, Ed. USA, 2012.

[3] International Atomic Energy Agency(IAEA), Ed., Computer Security Incident Response Planning at Nuclear Facilities. IAEA, 2016.

[4] M. Maj, R. Reijers, and D. Stikvoort, Good practice guide for incident management. ENISA, 2010.

[5] D. V. Ouzounis, Good practice on Reporting Security Incidents. ENISA, 2009.

[6] C. K. Dr. Konstantinos Moulinos, Dr. Marnix Dekker, Proposal for Article 19 Incident reporting. ENISA, 2015.

[7] J. Gonzalez, “Towards a cyber security reporting system–a quality improvement process,” Computer Safety, Reliability, and Security, 2005, pp. 368–380.

[8] C. Johnson, “Tools and techniques for reporting and analysing the causes of cyber-security incidents in safety-critical systems,” 2014.

[9] R. Leszczyna and M. R. Wrobel, “Security information sharing for smart grids,” network, vol. 1, 2014, p. 3.

[10] U.S Code of Federal Regulations, Ed., Physical Protection of Plants and Materials, part 73, chapter 1, title 10. USA, 2015.

[11] U.S Nuclear Regulatory Commission(NRC), Ed., Regulatory Guides 5.83, Cyber Security Event Notifications. USA, 2015.

[12] NRC, Ed., Regulatory Guides 5.71, Cyber Security Programs for Nuclear Facilities. USA, 2010.

[13] M. Li, W. Huang, Y. Wang, W. Fan, and J. Li, “The study of APT attack stage model,” in 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS). IEEE Computer Society, June 2016, pp. 1–5.

[14] IAEA, Ed., The International Nuclear and Radiological Event Scale User’s Manual. IAEA, 2008.