Propositions for Effective Cyber Incident Handling

Jung-Woon Lee*, Jae-Gu Song, Jun Young Son, and Jong-Gyun Choi
Nuclear ICT Research Division, Korea Atomic Energy Research Institute, Daejeon, Republic of Korea
**Corresponding author: leejw@kaeri.re.kr*

1. Introduction

Digital technologies have been applied expansively to nuclear instrumentation and control (I&C) systems. This application has raised cyber security issues. U. S. NRC published the regulatory guide 5.71 (RG 5.71) in 2010 [1]. Korea Institute of Nuclear Nonproliferation and Control (KINAC) has prepared the regulatory standard RS-015 [2] based on RG 5.71. Korean nuclear facilities submitted their cyber security plan (CSP) and have implemented the elements of CSP.

According to regulatory documents [1] & [2], the cyber security plan must include incident response and recovery measures by describing how to:

- maintain the capability for timely detection and response to cyber attacks,
- mitigate the consequences of cyber attacks,
- correct exploited vulnerabilities, and
- restore affected systems, networks, and equipment affected by cyber attacks.

Nuclear I&C systems have a form of industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures [3]. Typically, ICS consists of field devices, such as Remote Terminal Units (RTU), PLCs, and Intelligent Electronic Devices (IED), control servers, engineering workstations, data historian, human-machine interface (HMI), and network communication devices [3]. These are the components that also can be found in nuclear I&C systems.

Stuxnet in 2010 was the first malware to specifically target SCADA systems and PLCs [4]. There have been many other prominent cyber attacks against ICS [5]. From these incidents, it can be known that well-prepared cyber incident response capability is important to detect and respond to cyber incidents in a timely manner.

In this paper, models of cyber incident handling process are surveyed. Based on this survey, a model of cyber incident handling process is proposed and research and development (R&D) activities to establish effective incident handling capabilities are suggested.

2. Models of Cyber Incident Handling Process

In this section models of cyber incident handling process in both Information Technology (IT) environments and ICS environments are reviewed. The phases and tasks in the models are analyzed in consideration of their application in Korean nuclear facilities.

2.1 Models in IT Environments

The cyber incident analysis process guide by Korea Internet and Security Agency (KISA) [6] is a guidance for incident response in the domestic IT environments. It describes the seven steps of cyber incident response process including 1) preparation, 2) detection, 3) initial response, 4) response strategy development, 5) incident investigation, 6) reporting, 7) recovery & resolution, as illustrated in Fig. 1.

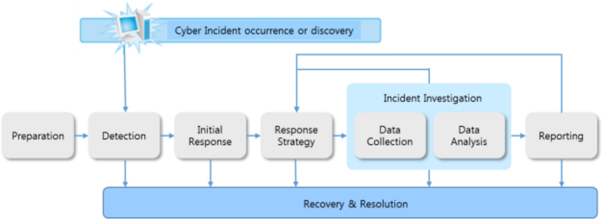

Fig. 1. Seven steps of cyber incident response [6]

NIST SP 800-61 [7] depicts the incident response process consisted of phases: 1) preparation; 2) detection & analysis; 3) containment, eradication & recovery; 4) post-incident activity. NIST SP 800-86 [8] provides a guide to integrate forensic technologies with incident response. The forensic process in this report includes data collection, examination, analysis, and reporting. The cyber incident handling program by U.S. Department of Defense [9] describes cyber incident handling process grouped into the following phases: 1) detection of events; 2) preliminary analysis and identification of incidents; 3) preliminary response actions; 4) incident analysis; 5) response and recovery; and 6) post-incident analysis. Fig. 2 shows these phases.

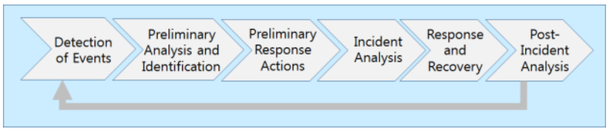

Fig. 2. Cyber incident handling process [9]

2.2 Models in ICS Environments

According to [10], planning, incident prevention, and post-incident analysis/forensics (top three ones in Fig. 3) are the elements for cyber incident response capability that are proactive in nature to prevent an incident or better allow the organization to respond when one occurs. Detection, containment, remediation, and recovery and restoration (bottom four ones in Fig. 3) are the elements for detecting and managing an incident once it occurs.

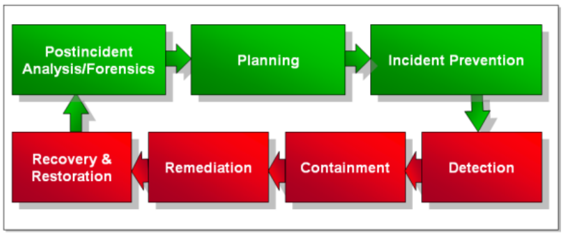

Fig. 3. Incident response key elements [10]

In [11], the core components of cyber incident response with an embedded forensics component are: 1) detection; 2) response Initiation; 3) incident response action/forensic collection, 4) incident recovery/forensic analysis, and 5) incident closure/forensic reporting.

In [12] and [13], the post-incident (forensic) analysis process includes 1) examination, 2) identification of evidence, 3) collection of evidence, 4) analysis of evidence, and 5) documentation of the process and results. In [12], the cyber incident response process quite similar to that in [11] is also described. The ICS incident response process with a forensic approach in [14] consists of 1) preparation of control system baselines, network monitoring, logging, tools, incident response team, incident response plan, and training, 2) volatile and non-volatile evidence preservation, 3) evidence analysis, 4) restoration, and 5) lessons learned. Other incident forensic processes can be found in [15], [16], and [17]. These are illustrated in Figs. 4, 5, and 6, respectively.

An IAEA document for nuclear facilities [18] also describes the phases of computer incident response with a list of tasks and its assignment to incident response team members. The phases are 1) preparation, 2) detection and analysis, 3) mitigation (containment, eradication, and recovery), 4) post-incident activity, and 5) reporting. Most of the tasks described in this document, however, are not specific to ICS environment.

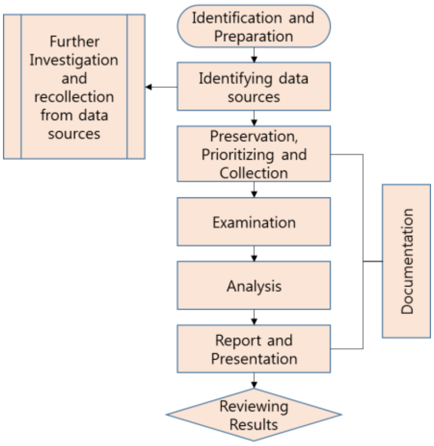
Identification and Preparation
Identifying data sources
Preservation, Prioritizing and Collection
Examination
Analysis
Report and Presentation
Reviewing Results
Further Investigation and recollection from data sources
Documentation

Fig. 4. Incident response forensic process [15]

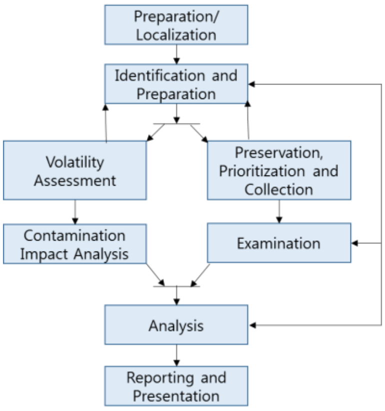
Preparation/ Localization
Identification and Preparation
Volatility Assessment
Preservation, Prioritization and Collection
Contamination Impact Analysis
Examination
Analysis
Reporting and Presentation

Fig. 5. SCADA Incident Response and Forensic Process [16]

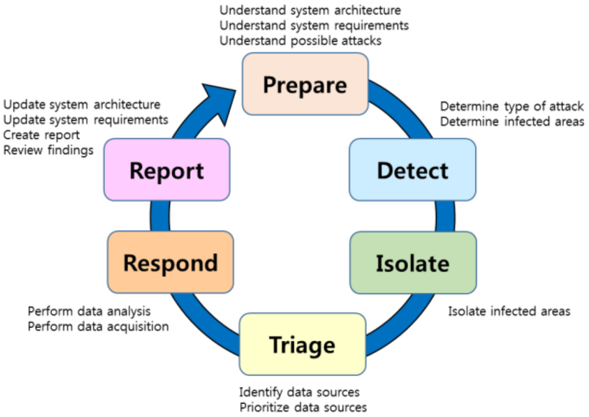

Fig. 6. SCADA forensic incident response model [17]

3. Proposed Model and R&D Suggestions

In this section, a model for cyber incident handling is proposed and R&D activities are suggested to establish effective incident handling capabilities.

3.1 Proposed Model of Incident Handling Process

A model of three stages, which are monitoring, incident response, and forensics as shown in Fig. 7, is proposed in consideration of incident handling capability aspects.

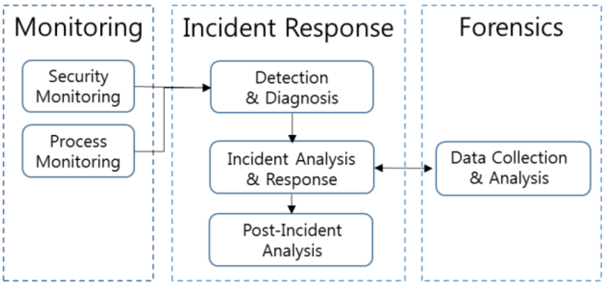

Fig. 7. Proposed incident handling model

Detecting an incident early will help to limit or even prevent possible damage and reduce the downstream efforts to contain, eradicate, recover, and restore the affected systems [10]. Two general approaches can detect an ICS cyber security incident. The first is through user observation of abnormal system or component behavior. The second is through automated detection systems or sensors [6, 9, 10, 18]. Monitoring capability is important for effective detection, allowing to start the incident response process. It is difficult to determine whether or not abnormal symptoms are associated with a malicious attack or usual component malfunction [19, 20]. In this sense, the proposed model incorporates process monitoring as well as security monitoring during the monitoring stage. Depending on incident characteristics, in some cases of incidents, digital forensics technologies may need to be applied by specialist trained forensic examiners during the incident response stage [15]. A link between the incident response stage and the forensics stage is placed in the model.

Based on the survey of the models in section 2, actions to be performed in the three phases of incident response stage are collected and described as follows:

1) Detection & Diagnosis Phase

- Identify suspicious behavior or cyber events of interest
- Prepare to handle the event
  - collect all relevant information about the event, such as design documents, network diagrams, configuration baselines, change logs, and authentication credentials
  - prepare incident analysis hardware and software
- Analyze precursors and indicators
- Look for correlating information
- Determine if the event is a reportable cyber event or incident
- Determine potential infected areas
- Compare the characteristics of digital assets involved in the event to known baselines
- Check the integrity of digital assets involved in the event if possible
- Perform preliminary impact assessment and determine potential damage
- Categorize the event and Classify the security level
- Determine if immediate actions are required to place the facility in a safe and secure condition
- Perform immediate response actions
  - contain the incident
  - identify data sources based on the type of incident
  - safely acquire and preserve the integrity of all data to allow for further incident analysis

2) Incident Analysis & Response Phase

- Assess the impact of volatile data capture against the safety and operation of the system.
- Collect and preserve information
  - collect volatile evidence
  - collect non-volatile evidence
- Perform incident analysis
  - develop a timeline of the incident
  - determine delivery vector(s)
  - determine system weaknesses
  - identify root cause(s)
  - expand previous impact assessment
- Develop a mitigation strategy
- Research and develop course of actions.
- Eradicate the incident
- Identify and mitigate all vulnerabilities that were exploited
- Remove malware, inappropriate materials, and other components
- Recover from Incident.

3) Post-Incident Analysis Phase

- Develop lessons learned.
- Enhance security measures to prevent re-infection.

Non-technical matters such as coordination, reporting, escalation, and documentation are not included in this list of actions. However, these should be considered in the development of site-specific incident response strategies and procedures.

3.2 Research and Development Suggestions

Based on the three stages of the model, R&D activities are suggested. Present nuclear I&C systems have many different types of digital assets from many different vendors. This means the results of development for a plant or a type of asset cannot be effective or applicable to other plants or other types of assets. Hence, the development should be plant-specific and dependent on the characteristics of assets.

1) Development of cyber event monitoring system

For the enhancement of monitoring capability, a cyber event monitoring system should be implemented. Cyber event monitoring technology for IT environments is widely used, but applying this to ICS environments needs adjustments or new developments. Automated detection systems, such as network intrusion detection systems, protocol-based intrusion detection systems, host-based intrusion detection systems, and network and device logging and analysis systems, should be developed and installed.

2) Development of incident response strategies and procedures

For the enhancement of incident response capability, procedures with if-then rule-based and step-by-step description of actions are necessary, especially for the detection and diagnosis phase of the incident response stage.

Existing procedures addressing plant abnormal states, such as abnormal operation procedures and alarm procedures, need to incorporate decision points to identify that abnormal events are cyber-related so that the diagnosis of events can be transferred to the incident response process.

Criteria to determine whether detected suspicious symptoms or anomalies are a cyber incident or not should be developed based on the implemented monitoring capabilities in a specific plant. The criteria should be included in procedures for the detection & diagnosis phase. Experiments on a test-bed to explore system changes that may be incurred by an acceptable list of potential cyber attacks against ICS will help the development of criteria.

Hardware and software configuration baselines should be prepared. The baselines will be used to identify any changes made in systems and assets during the detection and diagnosis phase.

Device and system integrity checking methods and tools need to be developed also for detection and diagnosis purposes.

Mitigation strategies for critical digital assets should be developed by considering the configurations of systems under the circumstances incurred by an acceptable list of potential cyber attacks. The strategies should be incorporated into mitigation procedures

3) Development of forensic and incident analysis technology

ICS processes a large amount of data in real time. Data collection and analysis technologies in ICS environments need to be developed, especially for field devices and other assets having characteristics different from those in IT environments. The methods and tools should be fitted into the type of digital assets. Volatile data collection and live incident analysis should be considered in the development.

4) Development of Incident Response Training

Training tools and contents should be developed based on incident response procedures for relevant personnel to practice the incident response process.

3. Conclusions

Establishing and maintaining cyber incident response capabilities is important in nuclear facilities. Based on the survey of cyber incident handling processes, a model consisted of monitoring, incident response, and forensics stages is proposed. R&D activities to establish effective monitoring, incident response, and forensics capabilities in nuclear facilities are suggested.

REFERENCES

[1] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.

[2] KINAC/RS-015, Technical standard for the security of computer and information systems in nuclear facilities, Rev. 1, KINAC, 2014.

[3] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, SP 800-82, Rev. 2, Guide to Industrial Control System (ICS) Security, National Institute of Standards and Technology (NIST), Gaithersburg, MD, United States, May 2015

[4] Barak Perelman, The Rise of ICS Malware: How Industrial Security Threats Are Becoming More Surgical, February 21, 2018. Accessed on July 30, 2018. https://www.securityweek.com/rise-ics-malware-how-industrial-security-threats-are-becoming-more-surgical

[5] Derbyshire, R., Green, B., Prince, D., Mauthe, A., & Hutchison, D. An Analysis of Cyber Security Attack Taxonomies. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, April, 2018.

[6] Cyber Incident Analysis Process Guide, Korea Internet and Security Agency (KISA), 2010.

[7] Cichonski, P., Millar, T., Grance, T., & Scarfone, K., SP 800-61 Rev. 2. Computer Security Incident Handling Guide. Tech. rep., National Institute of Standards & Technology (NIST), Gaithersburg, MD, United States, 2012.

[8] Kent, K., Chevalier, S., Grance, T., & Dang, H., SP 800-86. Guide to integrating forensic techniques into incident response. National Institute of Standards & Technology (NIST), Gaithersburg, MD, United States, 2006.

[9] U.S. Department of Defense, Chairman of the Joint Chiefs of Staff Manual, Cyber Incident Handling Program: CJCSM 6510.01B, 10 July 2012 (Directive Current as of December 18, 2014)

[10] Department of Homeland Security, Recommended practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. Technical report, Department of Homeland security, 2009.

[11] Mark Fabro and Eric Cornelius, Recommended practice: Creating cyber forensics plans for control systems. Department of Homeland Security, 2008.

[12] Pauna, A., Moulinos, K., Lakka, M., May, J., & Tryfonas, T., Can we learn from SCADA security incidents. White Paper, European Union Agency for Network and Information Security (ENISA), Heraklion, Crete, Greece, 2013.

[13] Spyridopoulos, T., Tryfonas, T., & May, J. H. R., Incident Analysis & Digital Forensics in SCADA and Industrial Control Systems. In System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International (pp. 1-6). Institution of Engineering and Technology (IET), 2013. DOI: 10.1049/cp.2013.1720

[14] Folkerth, Lew, Forensic Analysis of Industrial Control Systems, SANS Institute InfoSec Reading Room, September 2015. Accessed on July 6. 2018. https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-industrial-control-systems-36277

[15] Wu, T., Disso, J. F. P., Jones, K., & Campos, A., Towards a SCADA forensics architecture. In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research* (Vol. 12), September 2013.

[16] Betts, M., Stirland, J., Olajide, F., Jones, K., & Janicke, H., Developing a state of the art methodology & toolkit for ICS SCADA forensics. *Int. J. Ind. Control Syst. Secur.(IJICSS)*, *1*(2), 44-56, 2016.

[17] Eden, P., Blyth, A., Jones, K., Soulsby, H., Burnap, P., Cherdantseva, Y., & Stoddart, K., SCADA System Forensic Analysis Within IIoT. In *Cybersecurity for Industry 4.0* (pp. 73-101). Springer, Cham, 2017.

[18] International Atomic Energy Agency, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna, 2016.

[19] Johnson, C. W., Harkness, R., & Evangelopoulou, M., Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems, In Proceeding of the 34th International System Safety Conference, Orlando, USA 8-12 August 2016, International System Safety Society, Unionville, Virginia, USA, 2016.

[20] Takano, M., ICS cybersecurity incident response and the troubleshooting process. In 2014 Proceeding of the SICE Annual Conference (SICE), Sapporo, 2014, pp. 827-832.