SAND2020-1298C

COMPUTER AND INFORMATION SECURITY TRAINING AND AWARENESS PROGRAMMES FOR NUCLEAR FACILITIES

N. AGBEMAVA
Nuclear Regulatory Authority
Accra, Ghana
Email: n.agbemava@gnra.org.gh

J.W. LEE
Korean Atomic Energy Research Institute
Daejeon, Korea, Republic of.

M.T. ROWLAND
Sandia National Laboratories
Albuquerque, New Mexico, USA

P. GYEKYE
Nuclear Regulatory Authority
Accra, Ghana

1. ABSTRACT

The risk to nuclear facilities from cyber-attacks is a growing concern due to entrance of new adversaries and the advancement of capabilities of existing adversaries such as criminal organizations and nation states. Recent sophisticated attacks have targeted instrumentation and control (I&C) systems having significant potential consequences for security and safety. This increasing risk has resulted in the recognition that cyber security is an essential element of the overall security framework of nuclear facilities and is a pressing priority for facility operators and national regulators.

A critical computer security measure is the provision of cyber security awareness and specialist training for all facility personnel. Provision of training is an administrative control measure within the Computer Security Programme (CSP) and is implemented in the organization's training programme. All personnel require cyber security awareness training with additional specialist training required for those roles and responsibilities associated with the greatest risks.

When considering the requirements for training, it is important to understand the work tasks and activities that are dependent upon knowledge, skills, and abilities that are specific to cyber security. This understanding begins with the assignment of personnel to roles and responsibilities to address risk associated with cyber security.

This paper provides evidence that the importance and urgency of cyber security awareness and training is underestimated at present. Recommendations are also provided for training programme development to guide nuclear facility operators, with international assistance and cooperation, to deliver effective cyber security training.

2. INTRODUCTION

Cyber-attacks are proving an effective means by which adversaries can target organizations, employees, and their critical assets and information. This requires organizations to adopt defensive strategies and implement preventive and protective measures. One significant measure is a comprehensive cyber security training

programme to provide the necessary knowledge, skills, and abilities for personnel to identify, manage, and mitigate risks associated with cyber-attacks[1].

The Verizon 2019 Data Breach Investigations Report (DBIR) [1], reported that 94% of malware was delivered via email, and that social engineering techniques were involved in 33% of attacks leading to breaches. This 2019 DBIR reflects DBIRs from previous years showing that email remains the most attractive (e.g. likely) attack vector by which adversaries engage with target organizations and that social engineering remains a very effective technique.

The importance of protecting against these techniques is further noted in the Centre for Internet Security's (CIS) Controls v.7.1 [3] which includes "Control#7 – Email and Web Browser Protections" and "Control #17 Implement a Security Awareness and Training Programme" as key security measures to protect against breaches. CIS further states that:

> Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering. [3]

Therefore, the training programme must consider all personnel to provide an effective first layer or defence. A training programme providing awareness training on cyber security is essential to enhance cyber security culture for all facility personnel. Specifically CIS states "for all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs[3]."

Given the unique potential consequences associated with nuclear material and facilities, it is imperative for both State and operator organizations to develop a comprehensive training programme to protect against the harmful effects of compromise. Further, it is essential for international support and cooperation in training and capacity establishment to ensure that global nuclear security demands are universally met.

3. CYBER SECURITY TRAINING

Nuclear facilities and the organizations that operate, regulate, and supply them require nuclear security. Nuclear security is defined by the IAEA as "The prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities [4, 5]." Cyber security is a critical and integral part of nuclear security.

Cyber security is necessary to ensure that information and digital systems continue to provide significant functions necessary for the safe and secure operation of nuclear facilities. Since these systems may be targeted by adversaries using cyber-attacks, a formal programme is required to provide Cyber security awareness and training to all personnel having a role in the safety and security of the facility.

These roles demand specific knowledge, skills, and abilities (KSAs) which the NICE framework defines as follows:

- Knowledge is "a body of information applied directly to the performance of a function [6]."
- Skills "… Skills needed for cybersecurity rely … on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual [6]."
- Ability is "competence to perform an observable behaviour or a behaviour that results in an observable product [6]."

[1] This paper builds upon Study on Nuclear Facility Cyber Security Awareness and Training Programs [8] from the Korea Atomic Energy Research Institute (KAERI), and incorporates guidance from the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education NICE [6] [14] and IAEA [4][5][7][10][13]. This is intended to be applied to Ghana and African regions as a whole.

The training programme requires an understanding of each role and the necessary KSAs required to competently perform them. This paper will consider the roles common to an operating nuclear facility. These are:

- Non-technical Employees: Custodial, Field Staff, Clerical
- Contractors
- Operations and Maintenance: Technical and Licensed Staff
- System and Design Engineers
- Cyber Security Team
- Management, including leadership

Each of these types require a specific set of KSAs that requires their own curriculum of cyber security training. To minimize the number of curricula, cyber security training can be broadly limited to the four types of training detailed within Annex III of IAEA NSS 23-G [7]. These are: :

- Awareness training which "increases awareness of threats and vulnerabilities and recognition of the need to protect data, information, computer-based systems and the means of processing them (computer and information security awareness) [7]".
- Topical training which "includes courses on specific aspects of security for all staff (classified material handling, CDAs, removable media and portable devices procedures) [7]."
- Professional training which "is typically detailed technical training for staff with particular responsibilities, for example for system administrators, software developers, network administrators, security guards, document classifiers and declassifiers, among others [7]."
- Specialized security training which "is focused and expert level training, usually for management level, in the areas of risk management, incident prevention and incident response, among other things [7]."

KAERI states that cyber security awareness training should be provided to all the facility personnel including contractors and further details two groups:

- "individuals that are involved in the design, modification, and maintenance of critical digital assets (CDAs) [8]", and
- "system managers, cyber security specialists, system owners, network administrators, and other personnel having access to system-level software [8]."

Both groups require topical and professional training, and personnel having roles and responsibilities associated with the greatest risk (e.g. Cyber Security Team members; Cyber Security Incident Response Team members, Cyber Security Officers, Chief Information Security Officer, Risk Acceptance roles) require additional specialized training. Table 1 summarizes the types of training that are recommended for each facility role.

TABLE 1. CYBER SECURITY TRAINING AND TRAINEES [7, 8]

Type of cyber security training	Applicable Personnel
Awareness Training	All employees and contractors
Topical Training	All employees and contractors
Professional Training	Technical and Security Staff (e.g. system administrators, software developers, network administrators, security guards, system engineers)
Specialized Cyber Security Training	cyber security team (CST), cyber security incident response team (CSIRT), Cyber Security Officer, Chief Information Security Officer (CISO), Risk Acceptance Roles)

4. CYBER SECURITY AWARENESS TRAINING

The Verizon DBIR [1] has noted that cyber-attacks continue to target human behaviours through phishing and social engineering. The Secureworks® 2018 Incident Response Insights Report, confirms this, and recommends employee education to address this threat [9].

The CIS Controls V7.1 [2] describes the challenge as follows:

> It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfil important functions at every

stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artefacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions).[3]"

A cyber security awareness programme should contain the following elements. The list is based upon the KAERI study [8] enhanced with recommendations from CIS, IAEA and NIST:

- Organizational Policies, Roles and Responsibilities [8],
  (i) For example, contacts to whom to report suspicious activity, incidents, and violations of cyber security policies, procedures, or practices (introduce attack indicators and reporting system)
- Definitions of confidentiality, integrity, availability (CIA) and potential risks arising from compromising CIA [8, 10]
- Description of attack vectors and how these are used by adversaries to access systems [8, 9, 10]. For instance, the five attack vectors used in the Electric Power Research Institute (EPRI) Threat Assessment Methodology (TAM): network, wireless, portable media and mobile devices, supply chain, and physical access [11].
- General cyber threats, methods, attack techniques (including new threats and techniques, if any) [2, 8]
- Cyber-attacks targeting Nuclear Facilities and/or industrial control systems (ICS) [8]. This includes:
  - Cyber Security Programme Elements [8, 10] such as incident response plans and procedures, and
  - Critical Controls and Measures [3, 8, 10]

5. TOPICAL TRAINING

KAERI also provides recommendations for topical training which '… helps plant system engineers and CST to perform suitably the cyber security activities defined in the CSP [8]." Topical training topics include:

- Identification of critical systems and critical digital assets (CDAs)
- Security level assignment under the defense-in-depth (DID) strategy
- Assessment of CDAs' compliance with security control requirement.
- Application of required security controls
- Performing cyber security activities related to CDAs after the implementation of security controls the operation of technical security controls.
- Supports for cyber security incident response, Incident handling, Incident monitoring, CDA backups, Recovery and reconstitution, etc.

Table 2 provides an example of KSAs, using the NICE Specialty Areas and Work Role matrix [12] as a reference list for KSAs for each of the above training topics.

TABLE 2. TOPICAL TRAINING TOPICS: KNOWLEDGE, SKILLS AND ABILITIES

Work Task/Activity [8]	Knowledge [10]	Skill [6]	Ability [6]
CS and CDA identification and analysis	Definition of CS and CDAs Methods and Procedures	*S0367* -To apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). *S0006*-To applying confidentiality, integrity, and availability principles.	*A0123*-To apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). *A0019*-To produce technical documentation.

Work Task/Activity [8]	Knowledge [10]	Skill [6]	Ability [6]
		S0282-Skill in technical writing. *S0171*-To performing impact/risk assessments.	*A0013*-Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means. *A0056*-To ensure security practices are followed throughout the acquisition process. *A0159* -To interpret the information collected by network tools (e.g. nslookup, ping, and Traceroute).
Defense in depth strategy	Meaning of DID strategy Security level assignment criteria • Identification of connections violating • DID rules and possible solutions for those connections	*S0124*-To troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution. *S0171*-To performing impact/risk assessments. *S0027*-Skill in evaluating the adequacy of security designs.	*A0001*-Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. *A0123*-To apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). *A0008*- Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]). *A0027*-Ability to apply an organization's goals and objectives to develop and maintain architecture.

Work Task/Activity [8]	Knowledge [10]	Skill [6]	Ability [6]
Assessment of security control requirements	Introduction of security controls. Assessment methods and procedures Criteria for the applicability of the requirements in CDAs Criteria for compliance	*S0001*-To conducting vulnerability scans and recognizing vulnerabilities in security systems. *S0110*-To identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements. *S0023*-Skill in designing security controls based on cybersecurity principles and tenets.	*A0061*-Ability to design architectures and frameworks. *A0076*-Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development. *A0094*-Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.
Application of required security controls	Methods and procedures for the selection of candidate security control designs How to evaluate the applicability, suitability, and effectiveness of security controls	*S0374*-To identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations. *S0007*-Skill in applying host/network access controls (e.g., access control list).	*A0123*-To apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). *A0065*-Ability to monitor traffic flows across the network. *A0066* -To accurately and completely source all data used in intelligence, assessment and/or planning products. *A0027*-Ability to apply an organization's goals and objectives to develop and maintain architecture.
Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	*S0001*-To conducting vulnerability scans and recognizing vulnerabilities in security systems.	*A0001*-Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. *A0015*-Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. *A0123*-To apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). *A0120*-To share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.
Cyber Investigation (INV)	Knowledge of electronic devices (e.g., computer	*S0068*-To collecting, processing, packaging,	*A0010* -To analyze malware.

Work Task/Activity [8]	Knowledge [10]	Skill [6]	Ability [6]
	systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, etc) Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. *S0047*-To preserving evidence integrity according to standard operating procedures or national standards.	*A0175*-To examine digital media on multiple operating system platforms.

Table II: Contents of technical training

For most of the activities, training materials should be developed based on the facility cyber security procedures. Elements of technical training programs can be developed individually as the activities to be performed.

6. PROFESSIONAL TRAINING

Professional training consists of certifications and other formal and on-the-job training courses and programmes. Certifications for cyber-security (not nuclear specific) include Certified Information Systems Security Professional (CISSP) granted by the International Information System Security Certification Consortium $(ISC)^2$; Global Information Assurance Certification (GIAC) such as Secure Software Programmer .NET or Critical Infrastructure Protection; or industry specific certifications such as Cisco Certified Security Professional.

However, external professional training can range from hundreds (e.g. CISSP) to thousands of dollars (e.g GIAC), not to mention the hours required for study and exam preparation. The cost of professional training as well as limited resources to provide this training internally, demands that training programme needs are supported through international organizations and support.

The contribution of professional training within the programme is to build skills but also verify abilities.

7. EXAMPLE – SPECIALIZED TRAINING – INCIDENT RESPONSE AND RECOVERY

Both IAEA-TDL-005 [13] and NIST sp800-61 [13] provide guidance on cyber security incident response. TDL-005 lists the stages of incident response as (1) Preparation; (2) Detection and Analysis; (3) Containment, Eradication, and Recovery; and (4) Post-Incident Activity [13]. The relationship between these phases is shown in Fig. 1.

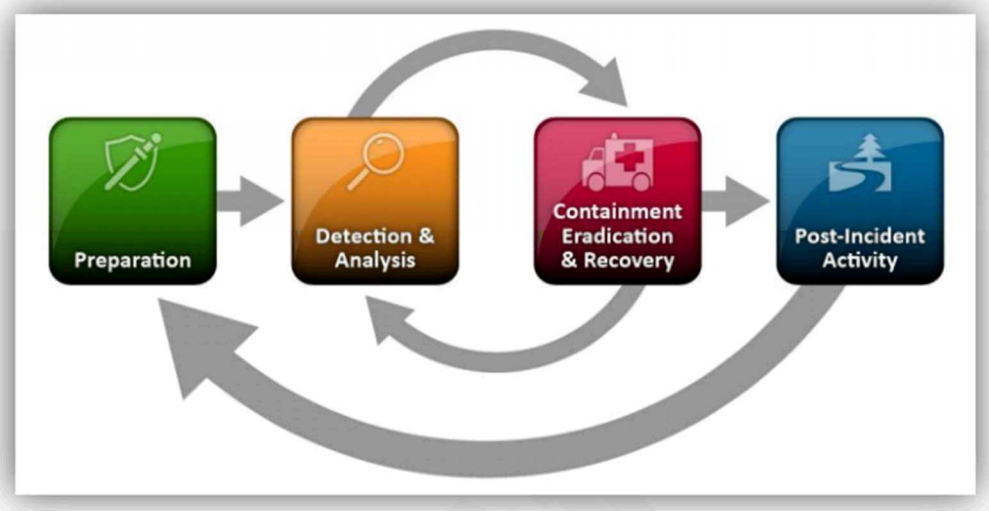

FIG. 1. Computer Security Incident Response Phases [12, Figure 3-1]

Specialized training for incident response should be developed in accordance with the facility's incident response plans and procedures. Incident response training should include hands-on and table-top exercises that progress through the various stages of the incident response plan. To provide realistic exercises, they should be based upon attack scenarios that are facility-specific.

TDL-005 states that "[c]omputer security incident response is not a single action but an approach that supports not only the detection of a computer security incident, but also mitigation and recovery from such an incident." Given the potential for a large number of incidents that could impact an organization, it is difficult to provide effective training that is limited to knowledge aspects only. The scope limitation of IAEA-TDL-005 to planning supports this assumption; compliance to plans, procedures, and processes can be well-supported through enhancing knowledge and awareness of them. This argument can also be extended to efficient communication and coordination, which also needs to be supported by skills and abilities.

For effective incident response, especially in the Analysis, Containment, Eradication, and Recovery stages, skills and abilities have primary importance. This requires specialized training that builds capacity through skills development and ability verification. This training also increases the demands on both the student and the trainer, and also upon the tools, technology, assets, and environments that need to be available.

Specialized training is dependent upon access to environments that allow for realistic hands-on, scenario-based exercises that are representative of nuclear facility environments and that accurately depict the impacts of compromise will ensuring safety and security. These environments include virtual environments/digital twins that provide realistic behaviours, but do not have the potential to result in actual consequences. The need for international support and cooperation in skills building and capacity establishment is vital to ensure that such specialized environments are available in countries that cannot resource these internally.

8. RESOURCES

Educators and Trainers: The NICE Framework [6, 11] provides a reference for educators to develop curriculum, certificate or degree programs, training programs, courses, seminars, and exercises or challenges that cover the KSAs and Tasks. Human resource staffing specialists and guidance counsellors can use the framework as a resource for career exploration.

Education and Training of Cybersecurity Workforce Members: The identification of tasks in work roles allows educators to prepare learners with the specific KSAs from which they can demonstrate the ability to perform cybersecurity tasks. Academic institutions are a critical part of preparing and educating the cybersecurity workforce.

Collaboration among public and private entities, such as through IAEA courses, US Department of Energy (DOE) cyber security training courses, online courses (eLearning), University and Professional Development / GNRA internal training program, would enable such institutions to determine common knowledge and abilities that are needed. In turn, developing and delivering curricula that are harmonized with the lexicon allows institutions to prepare the workforce with the skills needed by work.

For specialized training, there are several offerings, but these are largely out of the reach of countries and organizations with limited resources. These are listed in [8] as SANS ICS cyber security training courses [15] and ISA cyber security training courses [16]. The Black Hat Conference training programs [17], Infosec Institute SCADA/ICS Security Boot Camp [18], and Cybati Control System Cybersecurity Course and Training Kit (CybatiWorks™) [19] can also be considered as candidates.

9. CONCLUSION

Cyber security awareness and training programs need to be based upon the KSAs necessary for personnel to competently perform work tasks and activities necessary to provide nuclear security and specifically protection against compromise (i.e. cyber-attack). These programmes can benefit from use of NIST framework [6] but this requires an in-depth understanding of the roles and responsibilities found within the organization. These Roles and Responsibilities once understood, can be further assigned work tasks and activities that can be taken or adapted from [6].

Once these work tasks are assigned, the NICE Specialty Areas and Work Role matrix [12] can be used to link the necessary KSAs that are required to be delivered by the training programme. The next step would be to link these KSAs to the four types of training identified above. For example, awareness training will largely support only knowledge elements, while specialist training will support skills building and ability verification.

The analysis also revealed that free or publicly available resources that can be leveraged for the training programme are mostly limited to use in awareness training. This places a significant strain on training programmes with very limited resources to provide the necessary professional and/or technical training. It is imperative that international cooperation and support be engaged to fill this gap to ensure global nuclear security needs are addressed.

10. REFERENCES

[1] VERIZON, 2019 Data Breach Investigations Report, USA, 2019

[2] UNITED STATES OF AMERICA OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), A Common Cyber Threat Framework: A Foundation for Communication, https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf , USA, 2018

[3] CENTER FOR INTERNET SECURITY (CIS), CIS Controls v7.1, http://www.cisecurity.org/controls/

[4] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Nuclear Security Series, Recommendations, Nuclear Security Recommendations on Radioactive Materials and Associated Facilities, NSS No. 14, IAEA, Vienna, 2011.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Nuclear Security Series, Recommendations, Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control, NSS No. 15, IAEA, Vienna, 2011.

[6] NATIONAL INITIATIVE FOR CYBER SECURITY EDUCATION (NICE)/NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Cybersecurity Workforce Framework, NIST Special Publication 800-181, U.S. Department of Commerce, August 2017.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Nuclear Security Series, Implementing Guide, Security of Nuclear Information, NSS No. 23-G, IAEA, Vienna, 2015.

[8] LEE, J-W., SONG, J-G., LEE, C-K., Jung-Woon Study on the Development of Nuclear Facility Cyber Security Awareness and Training Program, Transactions of the Korean Nuclear Society Autumn Meeting, Gyeongju, Republic of Korea, (2016).

[9] SECUREWORKS, Cybersecurity Awareness Training: Threats and Best Practices, https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices, 2018.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Computer Security Techniques for Nuclear Facilities, Draft Technical Guidance, NST047, IAEA, Vienna (Draft 2017).
[11] ELECTRIC POWER RESEARCH INSTITUTE (EPRI), Cyber Security Technical Assessment Methodology, Risk Informed Exploit Sequence Identification and Mitigation, Revision 1, Product Id: 3002012752, USA, 2018.
[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Excel Worksheet: Supplemental NICE specialty areas and work roles KSAs and tasks, https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx, USA, 2019
[13] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Computer Security Incident Response Planning at Nuclear Facilities, TDL-005, IAEA, Vienna, 2016.
[14] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Computer Security Incident Handling Guide (Draft) NIST Special Publication 800-61 Revision 2, Gaithersburg, MD, 2012.
[15] SYSADMIN, AUDIT, NETWORK, SECURITY (SANS) INSTITUTE, https://www.sans.org/course, 2019.
[16] INTERNATIONAL SOCIETY OF AUTOMATION (ISA), https://www.isa.org/training-and-certifications/isa-training/top-tier-training-for-top-notch-protection/, 2019.
[17] CMP MEDIA, https://www.blackhat.com/us-16/training/index.html, 2019.
[18] INFOSEC INSTITUTE, https://www.infosecinstitute.com/courses/scada-security-boot-camp, 2019.
[19] CYBATI, https://cybati.org/index.php/home/cybatiworks-for-applied-research, 2019

ACKNOWLEDGEMENTS

This work [8] on which this paper is based has been supported by a grant from the Korea Ministry of Strategy and Finance.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.