Cyber Security of Critical Infrastructure Protection Overview in Taiwan's Water Resource Domain

Pei-Yuan Chung, Jung-Shian Li, I-Hsien Liu, Quan-Ru Song, Chu-Fen Li, and Gui-Lin Huang

***Abstract*—Many countries are beginning to promote green energy, hydropower is one, and hydropower is closely related to the critical infrastructure (CI) of the water field. With the rise of hack events, critical infrastructure (CI) and industrial control system (ICS), security becomes more important to the government. Resources and regulations are necessary to prevent possible threats. This research aim at CI of water resource domain. By the process of practical interview, we propose some management and protection guides for ICS information security. The results can be the guideline for related domains.**

***Index Terms*—Critical infrastructure, industrial control system, water resources, cyber security.**

I. Introduction

In recent years, many countries have experienced major hacking attacks on critical infrastructure, resulting in the disruption of public services and even the damage to life and property. According to a research report [1] released by the Dragos Security Team in 2017, it is pointed out that 64% of industrial control system (ICS) components are designed to be insecure, resulting in possible risks even if patches are installed. If the industrial control system (ICS) vulnerability is attacked or exploited by a person with a heart, the impact and loss may be difficult to estimate.

In view of the increasing trend of critical infrastructure attacks, the National Qualifications Security Strategy Report (2018) proposes that “Information Security is a National Security Promotion Strategy”, for the eight critical infrastructure such as government, high-tech parks, energy, water resources, communications, transportation, banking and finance, emergency rescue and hospitals, we are actively pursuing four major aspects: early warning, continuous control, notification and improvement. Continue to promote the safety and security measures of the capital [2].

This paper is based on the national laws and regulations on the critical infrastructure security protection and conducts on-the-spot investigation and analysis of our national water resources field stations, understands the current status of its operations. Analyze and evaluate the degree of compliance with laws and regulations, and collect and develop recommendations for the ICS information security protection.

Manuscript received February 24, 2020; revised May 9, 2020.

P.-Y. Chung, J.-S. Li, I-H. Liu, and Q.-R. Song are with the Institute of Computer and Communication Engineering, Department of Electrical Engineering, National Cheng Kung University, No. 1 Univ Rd., Tainan City, 701, Taiwan (e-mail: jsli@mail.ncku.edu.tw).

C.-F. Li is with Department of Finance, National Formosa University, No.64, Wunhua Rd., Huwei Township, Yunlin County 632, Taiwan (e-mail: chufenli@gmail.com).

G.-L. Huang is with Water Resources Agency, MOEA, 9-12F No. 41-3 Sec.3 Xinyi Rd. Da’an Dist., Taipei City, 106, Taiwan (e-mail: a210010@wra.gov.tw).

II. Literature Review

A. Critical Infrastructure Protection Recommendations

According to the "Basic Policy on Critical Infrastructure Protection", the Executive Yuan of Department of Cyber Security has developed a "Critical Infrastructure Protection Proposal" [3] to provide an important reference for the assessment and implementation of critical infrastructure assessments in the country. This protection proposal is the first safety protection benchmark for industrial control systems in critical infrastructure areas.

Its content includes ICS network architecture, access control, audit and accountability, contingency planning, identification and authentication, system and communications protection, system and services acquisition, physical and environmental protection, system and information integrity, configuration management and organization management 11 categories of safety areas and 41 types of requirements, and an industrial control system checklist is provided as a critical infrastructure self-assessment tool.

This protection recommendation is also the main reference for the study of ICS security protection operations and requirements for critical infrastructure in the water resources.

B. Critical Infrastructure Protection Recommendations

NIST SP 800-82 [4] was published by the National Institute of Standards and Technology of the United States, which describes the recommendations and guidelines for the relevant ICS field, and distinguishes 221 protection requirements in 18 categories of safety. Table I shows [4].

Its safety includes access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, personnel security, planning, physical and environmental protection, risk assessment, system and services acquisition, system and communications protection, system and information integrity and program management. It is also commonly cited by internationally relevant standards for critical infrastructure and information infrastructure protection. It is one of the important references for ICS protection and management requirements for this paper.

doi: 10.18178/ijiee.2020.10.2.717

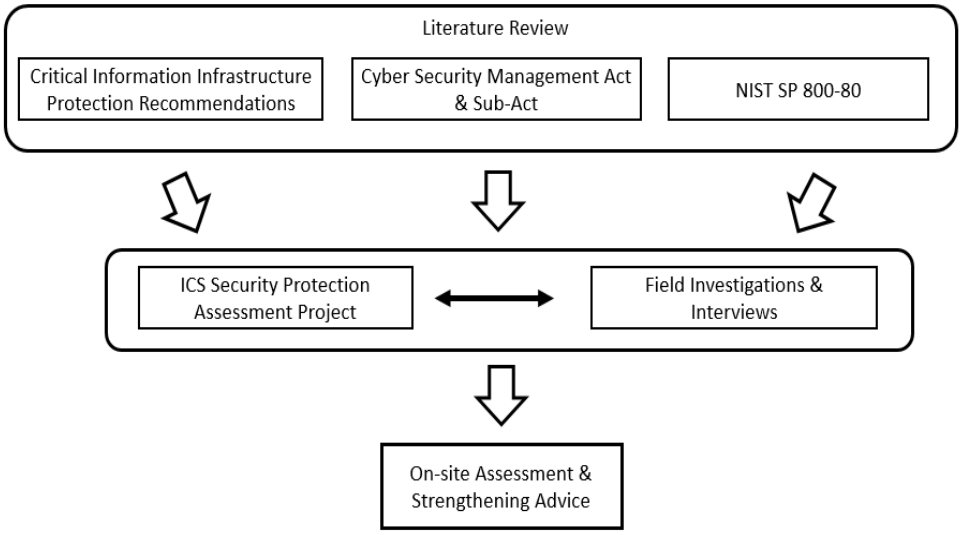

Fig. 1. Research process description.

TABLE I: LIST OF NIST SP 800-82

ID	*Family*	*Class*
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

C. Common Critical Infrastructure Weaknesses

Due to the design and operational characteristics of ICS, it is easy to cause major vulnerabilities. If the station lacks sufficient sense of security and good management, it will be invaded by hackers, and severely cause failure of operation or critical infrastructure functions or loss of life and property. NCCIC/ICS-CERT conducted a common critical infrastructure vulnerability analysis based on the NIST 800-53 control classification project. Among the 638 weaknesses counted in 2015, the top six projects accounted for 35.8%, related lists and descriptions. Table II shows [5].

Based on the results of the above-mentioned literature, this paper through the process of field investigation and personnel interviews, takes the key infrastructure of Taiwan's water resources as the main goal, and evaluates the current situation and needs of the ICS security protection of the station, and proposes a feasible strengthening direction and suggest.

TABLE II: LIST OF SIX MAJOR WEAKNESSES IN CRITICAL INFRASTRUCTURE

Rank	*Weak point project*	*Description*
1	Boundary Protection	1. ICS network lacks border protection 2. Lack of logical separation between ICS network and corporate network
2	Least Functionality	1. Open unneeded services, communications, applications and features 2. Unauthorized access to personal devices
3	Authenticator Management	1. Only rely on passwords for authentication 2. Password complexity is low 3. The authentication process lacks encryption protection
4	Identification and Authentication	1. Lack of account attribution and non-repudiation mechanism 2. Departure account lacks a handler
5	Least Privilege	1. Provide excessive system management privileges
6	Allocation of Resources	2. Manpower is insufficient to respond to security incidents and maintain system security

III. RESEARCH PROCESS

This paper focuses on the critical infrastructure of water resources, conducts ICS security protection assessment, and proposes possible enhancement measures to assist each station to achieve compliance with the safety management law and strengthen the management and control of security risks. The research process is shown in Fig. 1

A. Literature Analysis

In order to carry out the assessment of critical infrastructure security protection in the field of water resources, this paper collects other literatures including the cyber security management act and related sub-Act, “Critical

Information Infrastructure Protection Recommendations", NIST SP 800-82, etc. The main basis for the ICS security protection assessment program.

B. Research and Development of the Security Protection Assessment Project

This paper draws on the "Critical Information Infrastructure Protection Recommendations", NIST SP 800-82 and other literature on the protection of critical infrastructures for water resources, develop a list of ICS security protection assessments based on the characteristics of the water resources. The content includes organizational security, network security, physical security, access security, operational security, system monitoring and protection, event processing and auditing, and operational continuity. As the main basis for the field survey and personnel interviews, and through the feedback of the interviewees, the fine-tuning of the evaluation project was carried out. The description of each security protection is shown in Table III.

TABLE III: EIGHT KEY SECURITY PROTECTIONS DIRECTIONS FOR CRITICAL INFRASTRUCTURE OF WATER RESOURCES

SECURITY PROTECTION	*DESCRIPTION*
Organizational security	Internal and external personnel information security responsibility requirements and protection, as well as ICS risk assessment and improvement procedures
Network security	ICS network management and monitoring behavior
Physical security	Physical protection and monitoring of station area and outbound facilities
Access security	ICS system access control and protection behavior
Operational security	System daily operation control and change management procedures
System monitoring and protection	ICS system abnormal condition monitoring and alarm, as well as system vulnerability protection.
Event processing and auditing	Information security incident notification operations and ICS audits and controls.
Operational continuity	ICS system, equipment operation continuous planning and backup measures.

C. Field Investigations and Interviews

With the cooperation of various stations, this paper will carry out interviews on nearly 20 critical water resources infrastructures in Taiwan from 2018 to 2019, complete field investigations, and use the above-mentioned contents of the eight major security protections to understand the station. Existing controls are used to analyze potential ICS security risks by means of relevant records and feedback from respondents.

D. Status Assessment and Recommendations

In accordance with the principle of security control for various control measures, in line with the implementation status of Taiwan's water resources critical infrastructure and the demand for security, and consider the requirements of various national laws and regulations, and propose the strengthening of ICS security protection as a follow-up plan. And the reference basis for implementing a feasible management and control mechanism.

E. Summary

Through the above research process and the survey of nearly 20 reservoirs, dams and water purification plants, this paper analyzes the current status of critical water resources infrastructure operations in Taiwan, considers its existing security management, and assesses the need for ICS protection. Common recommendations for strengthening are described in the next section.

IV. EVALUATION AND RECOMMENDATIONS

After completing 20 field investigations and personnel interviews on critical infrastructures such as reservoirs, dams and water purification plants, this paper has a very complete understanding of the current situation of station operation and cyber security protection.

In the analysis of the current situation, the critical infrastructure of the water resources surveyed generally has a considerable degree of awareness of the cyber security, and has promoted the implementation of the necessary security protection operations. In addition to the 24-hour shift of personnel to monitor hydrological information, there are also rigorous operational procedures. And regularly carry out flood control drills every year, and prepare for the coming of the flood season. Because the setting of the station needs to be close to the water source, it is often located in the mountainous area or sparsely populated. The hydraulic facilities are widely distributed. The protection and monitoring of physical security is usually the most important item of the responsible personnel; however, due to possible geographical restrictions, Taiwan's water resources critical infrastructure is still using the near-end control mode in the important hydraulic machinery control operations, and avoids the use of manpower-saving remote control. Although the load imposed by the personnel is increased, the control is also strengthened. Respond to the real-time, reducing the risk of misuse and threats from external or Internet attacks.

This paper utilizes the process of field investigations and interviews, and the assessment of the implementation of the critical infrastructure of water resources under the relevant act and regulations, as well as the possible control of threats, and the evaluation of the implementation of the eight major security aspects by researchers. The scores of 1~5 grades are scored, and the scores of all the evaluated stations are averaged. The summary is shown in Fig. 2.

Most of the stations have a certain amount of control procedures and implement relevant control measures, but most of them are based on the safety considerations of water supply operations. Although they are consistent with the concept of cyber security, the details of implementation still differ. Therefore, even if the station does not have an immediate risk of cyber security, it should still make necessary adjustments and responses in order to face the various requirements after the implementation of the cyber security management act.

In assessing the cyber security management act and related supporting measures promoted by our government, and considering the evolution of ICS technology and the attack

cases of critical infrastructures in foreign countries in recent years. In order to assist the domestic water resources critical infrastructure security management and protection promotion, this paper proposes the following suggestions for the project with a score of 3 points in the direction of the eight major security protection.

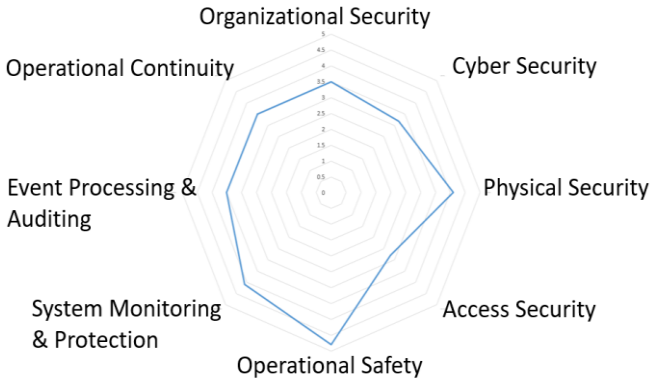

Fig. 2. Radar analysis chart for the implementation of eight key security protections for critical infrastructure of water resources.

A. Consolidation of ICS Network Boundaries

At present, the critical infrastructure of water resources adopts the principle of physical isolation in the architecture of ICS networks, avoiding mixing with administrative network segments or information devices, and minimizing possible network attack. However, after all, the inherent geographical location of the station is limited, the external station facilities are numerous and the communication lines are not easy to set up. It is recommended to maintain the integrity and update of the network topology, maintain and mark the communication lines, and strengthen the network access control, improve the consolidation of ICS network boundaries.

B. Enhancement of Access Control Measures

Common access control principles may not be appropriate for ICS operations, such as password setting principles, such as password setting principles. Due to the 24-hour staff duty system and the equipment that can be used for ICS control, it is strictly controlled, the possibility of account theft or unauthorized access is not high. However, in order to strengthen the division of authority and access records, it is recommended to consider the division of important authority and account allocation, and to evaluate feasible supporting control measures, such as account logout, to make existing access control more perfect.

C. Preservation of Important Logs and Audit records

The critical infrastructure of water resources generally has manual copying of real-time hydrological information, and the ICS system also has related recording functions. It is recommended to consider the functions of the ICS system, enable the necessary system audit mechanism, and back up and save important log files and audit records as a reliable basis for future investigation.

D. Development of an Cyber Security Related Operation Continuity Plan

In response to the annual flood season, the station has fixed flood control drills, but most of them rely on natural disaster prevention and treatment as the main situation. At present, less continuous consideration is given to the operation and maintenance related to the cyber security issues. It is suggested that the situation based on the cyber security incidents can be planned, and the feasible response can be deduced and designed. The operational continuity plan should be drawn up, and the flood prevention exercise schedule will be implemented together to strengthen the emergency response of critical infrastructures.

E. Continued Promotion of the Requirements of the Cyber Security Act

In the past, the critical infrastructure of water resources, due to the focus on the maintenance of the station, is relatively unfamiliar to the issue of cyber security. In the face of the implementation and requirements of the security management act, it is still actively understanding the state of efforts. The proposal can encourage relevant colleagues to participate in education and training related to security, and obtain licenses and qualifications that meet the requirements of the regulations, and continue to promote and strengthen the security protection in the station.

V. Conclusion

This paper considers the promotion and regulation of Taiwan's cyber security management act, as well as the government's emphasis on the protection of critical infrastructure. Therefore, it conducts a survey of critical infrastructures for water resources, and combines other normative Literature to consolidate the eight major security protection aspects. Evaluate and understand the existing operational and protective operations of the station ICS, in accordance with the requirements of the act, and the relevant methods of the cyber security attack case, In view of possible risk issues and control actions, it proposes feasible and strengthened recommendations, and hopes to serve as a reference for the continuous promotion of security control and protection in the relevant fields in Taiwan. In the future, this paper will continue to conduct research on act and regulatory requirements, ICS security and management, and expand the framework and content of critical infrastructure security protection to provide more information on critical infrastructure information security protection and promotion issues.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Prof. Jung-Sung Li, Dr. Liu, and Mr. Chung conceived of the presented idea. Dr. Liu, Mr. Chung, and Mr. Song developed the survey. Prof C.-F. Li and Dr. Liu verified the analytical methods. Mr. Huang has helped the survey. Prof. Jung-Sung Li supervised the findings of this work. All authors discussed the results and contributed to the final manuscript.

ACKNOWLEDGMENT

This work was supported in part by the MOST (Ministry of Science and Technology), Taiwan under contracts numbers MOST 108-2218-E-006-035- and MOST 108-2221-E-006-110-MY3.

Thanks to the Ministry of Science and Technology for the project "Information Security Monitoring and Management Technology Development", project number: MOST 108-2218-E-006-035-, and the "Water Resources Critical Facilities Upgrade and Safety Management Ensuring Flagship Project" of the Water Resources Agency of the Ministry of Economic Affairs Provide funding to support this study.

REFERENCES

[1] Dragos, Inc. (2018). 2017 key findings. [Online]. Available: https://dragos.com/resource/2017-key-findings/
[2] National Security Conference National Security Office, National Qualification Security Strategy Report, September 2018.
[3] *Administration of Insurance Administration, Critical Information Infrastructure Protection Proposal*, vo1. 4, January 2019.
[4] NIST Guide to Industrial Control Systems (ICS) Security, NIST SP800-82, Revision 2, 2015.
[5] NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report, NCCIC/ICS-CERT, 2015.

Copyright © 2020 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).

Pei-Yuan Chung is a project manager in Taiwan Information Security Center at National Cheng Kung University. He graduated from I-Shou University, Taiwan with MS degrees in 2005 in information management. He is currently involved in funded research projects dealing with Critical Information Infrastructure Protection (CIIP)

Jung-Shian Li is a full professor in the Department of Electrical Engineering of National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan. He got his BS in 1990 and MS degrees in 1992 in electrical engineering. He obtained his PhD in 1999 in computer science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, cloud security and resource allocation, and IP QoS architectures. He is the deputy director general of National Center for High-performance Computing (NCHC), National Applied Research Laboratories. He serves on the editorial boards of the International Journal of Communication Systems.

I-Hsien Liu is a researcher fellow in the Taiwan Information Security Center at National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering of National Cheng Kung University, Taiwan. He got his master degrees in the Department of Information Management from National Kaohsiung University of Applied Sciences, Taiwan. He obtained his PhD in 2015 in computer and communication engineering from the National Cheng Kung University. He interests are cloud security, wireless network, group communication and reliable transmission in mobile ad hoc networks.

Quan-Ru Song was born in Tainan in 1996. He received the B.S. degree in computer and communication engineering from National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan in 2017 and the M.S. student in computer and communication engineering from National Cheng Kung University (NCKU), Tainan in 2019.

Chu-Fen Li is an associate professor in the Department of Finance at the National Formosa University, Taiwan. She received her Ph.D. in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.

Gui-Lin Huang is a director of Information Management Office in Water Resources Agency, MOEA, Taiwan. He is in charge of different water resource programs, such as IOT application and security protection.