The Dam Gate Cybersecurity Testbed

Chen-Yu Lee
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Meng-Wei Chang
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Jung-Shian Li[*]
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan
E-mail: cylee@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, mwchang@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw[*]
www.ncku.edu.tw

Abstract

The testbeds are very important for cybersecurity research on critical infrastructure. In today's drastic climate change, the dam gate control system is a very important part of the critical infrastructure for people's livelihood. In traditional research, because the real control system cannot be used directly, most of the research can only be carried out in a simulation way. The research based on simulation alone lacks practical value due to too many assumptions. This research was supported by the Water Resources Agency, Ministry of Economic Affairs and National Science and Technology Council in Taiwan. The gate control cybersecurity testbed was built with a blueprint of the real world.

Keywords: Cyber Security, ICS Security, PLC, Dam Gate Testbed

1. Introduction

In the era of rapid development of modern network communication and industrial control, large-scale key infrastructures have also been built by various countries, aiming to activate the industrial economy, develop an all-around industrial environment that benefits the country, and gradually improve the industry to meet the needs of the people.

There are many elements in the Industrial Control System (ICS)[1] such as the Industrial Internet of Things or the Supervisory Control and Acquisition System (SCADA), etc. Among them, the Programmable Logic Controller (PLC) is a key operating component. It can not only communication between the device's signals, and can be directly connected to the computer for signal transmission.

And because PLC is concerned with the physical behavior of the infrastructure, it will also face the information security crisis of cyber-attacks[2]. Russian hackers launched a data destruction attack on a Ukrainian power plant on April 8, 2022, and related companies cooperated with Ukrainian authorities to successfully prevent this attack[3].

In order to maintain the network security of critical infrastructure, this paper designs a set of testbeds that simulate water resource basins and connects PLC and other physical devices to build a set of physical testbeds for the implementation of new technologies for key infrastructure.

2. Background

In this section, we mainly discuss the components based on the critical infrastructure testbed. In traditional critical infrastructure, there are always problems, whether it is production efficiency or information security attack and defense[4], but in practice, it is impossible to directly implement new research or technology to critical infrastructure, because if there is a problem with its operation, it will cause serious problems. The country suffered great harm. Therefore, based on various considerations, most research will first be established and analyzed on a testbed, and then implemented in critical infrastructure.

2.1. *Programmable logic controller (PLC)*

PLC can control commands through memory access, and can also use various modules for customized functions. In recent years, the PLC in the industrial environment has gradually developed into a microcomputer. Whether it is digital and analog output and input, or directly building a human-machine interface (HMI), PLC has played a pivotal role in the industrial environment.

2.2. *Modbus/TCP*

Modbus is currently a communication protocol widely used in PLCs and has also been extended to become the communication protocol standard of the entire industrial environment. And because of the convenience, the current industrial environment gradually relies on Ethernet as a connection, so Modbus TCP is often used in industrial environments. However, with the advantages of such convenience and flexibility, Modbus is also vulnerable to unauthorized writing and packet analysis because it is transmitted in plain text, so it will be subject to behaviors such as penetration attacks.

2.3. *Critical infrastructure testbed*

The establishment of the testbed can cooperate with the supervisory control and data acquisition system (SCADA) [5] and can be classified by many aspects, mainly divided into three categories: information technology, communication, and operation technology, and there will also be different settings for each research. Key infrastructure testbed such as water conservancy and power generation. The establishment of the testbed is mainly aimed at the fact that if various tests are directly carried out on key infrastructures, it may cause them to be shut down or damaged, and the country will suffer huge losses. Therefore, it is very important to set up a testbed that meets its own needs and conduct tests on it.

3. Design of Dam Gate Testbed

Due to the cybersecurity issues of critical infrastructure, this paper designs a testbed for simulating the dam gate system. Because each gate is driven by the PLC, and the PLC has registers to access related instructions and data. Therefore, this information can express various values of the current industrial environment such as water pressure

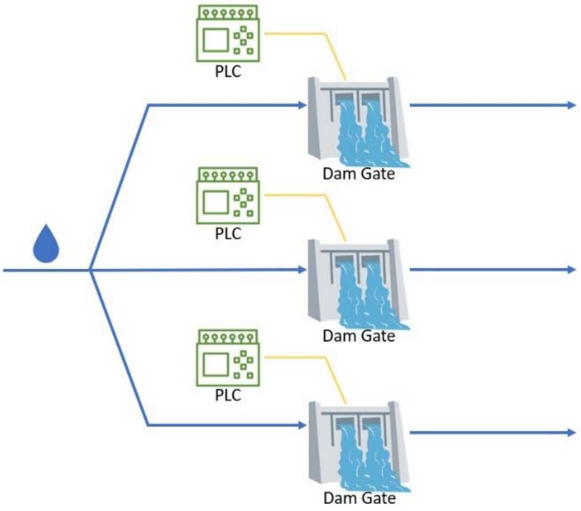

Fig. 1. Dam Gate Testbed Framework

and current. Taking Modbus/TCP as an example, a testbed for simulated dam gates in the computer is designed, and the gates are all connected and transmitted by physical PLC. In order to facilitate users to conduct research related to industrial control.

3.1. *System architecture*

First of all, we designed the framework in Fig. 1. according to the actual interaction between PLC and computer and controlled specific gates by sending relevant packet information through PLC. In addition, we have also designed the relevant main control panel to transmit digital signals to the PLC through the switch, which can be more suitable, and the output signal of the PLC can also be controlled by the program without connecting the main control panel to maintain the overall operation flexibility. Finally, we also design a virtual gate system based on packet sending and receiving, and the establishment of the testbed will be described in detail in 3.2.

3.2. *Virtual dam gate testbed*

In this section, we establish a set of virtual dam gate testbed based on Modbus/TCP in Fig. 2. By connecting the computer and the PLC and setting the relevant virtual gate status, you can observe the changes in various values:

- Packet flow
- Gate state change
- Water flow information

It is hoped that this virtual testbed can carry out simulation research such as PLC attack and defense and gate behavior first. In Section 4, we design a set of physical dam gate testbed based on the virtual testbed.

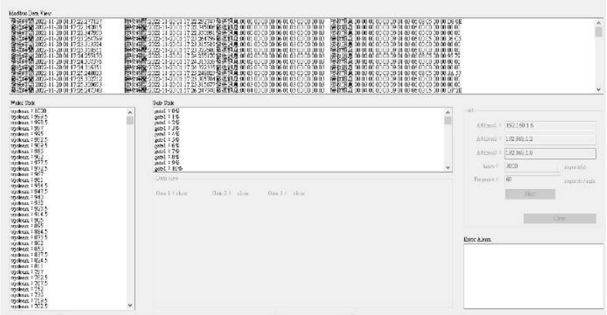

Fig. 2. Virtual Dam Gate Testbed

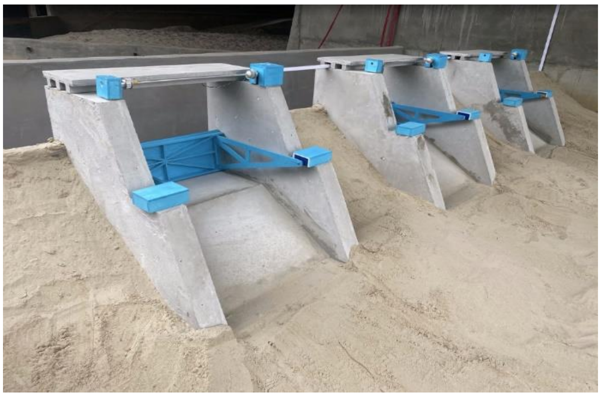

Fig. 3. Physical Dam Gate Testbed

4. Experiment

The team built a set of physical dam gate testbed as shown in Fig. 3. For the sake of reality, the physical gates and terrain heights were also designed to make it fit the practical technology. Moreover, computer equipment is designed for personnel to operate on site, which not only allows on-site personnel to monitor in real-time but also allows operations such as information security offensive and defensive drills or novel technology research.

This research can not only be applied to the research and application of current personnel but it is also expected that the technology and expertise can be further extended to critical infrastructure to improve people's well-being.

5. Conclusion

At present, the development of critical infrastructure is quite rapid, and all countries attach great importance to the development of this facility. However, due to its huge interest in critical infrastructure, it is subject to cyber-attacks. Therefore, the testbed for simulating critical infrastructure is gradually gaining attention.

In order to protect the safety and operability of key infrastructure, this paper designs a virtual dam gate testbed based on PLC and Modbus/TCP protocol. By integrating the physical dam gate system into a virtual testbed, related settings and operations can be completed in a lightweight and flexible manner.

This paper also further realizes the dam gate testbed. In this testbed, research such as PLC packet sending and receiving and gate control, etc., is research with considerable research potential. It is also expected that the research in this paper can be further applied to large-scale critical infrastructure to promote the development of the people and the country.

Acknowledgements

This work was supported by the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) and the National Science and Technology Council (NSTC) in Taiwan under contract numbers 111-2218-E-006-010-MBK.

References

1. W. Knowles, D. Prince, D. Hutchison, Jules Ferdinand Pagna Disso, K. Jones, "A survey of cyber security management in industrial control systems", International Journal of Critical Infrastructure Protection, vol. 9, pp. 52-80, 2015.
2. A. Ghaleb, S. Zhioua, and A. Almulhem, "On PLC network security", International Journal of Critical Infrastructure Protection, vol. 22, pp. 62-69, 2018
3. ESET Research, "Industroyer2: Industroyer reloaded This ICS-capable malware targets a Ukrainian energy company", https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
4. J. Frauenschläger, J. Mottok, " Security-Gateway for SCADA-Systems in Critical Infrastructures", 2022 International Conference on Applied Electronics (AE), 2022.
5. J. Jarmakiewicz, K. Maślanka, K. Parobczak, " Development of Cyber Security Testbed for Critical Infrastructure", 2015 International Conference on Military Communications and Information Systems (ICMCIS), 2015.

Authors Introduction

Mr. Chen-Yu Lee

He was born in Taipei, Taiwan in 1998. He is acquiring the master's degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. He received his B.S. degree from the Department of Communications, Navigation and Control Engineering, National Taiwan Ocean University, Taiwan in 2021. His interests are Cyber-Security , PLC and ICS Security.

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Dr. Meng-Wei Chang

He was born in Pingtung, Taiwan in 1997. He is acquiring the master's degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. He received his B.S. degree from the Department of Physics, National Taiwan Normal University, Taiwan in 2021. His interests are Cyber-Security and ICS Security.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. 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 director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.