Cyber-Physical Security Testbed for River Basin Gate Control System

Meng-Wei Chang
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University,
No.1 Daxue 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 Daxue 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 Daxue Rd., East Dist., Tainan City, 701401, Taiwan
E-mail: mwchang@cans.ee.ncku.edu.tw, ihlu@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw
www.ncku.edu.tw

Abstract

Due to the flourishing development of critical infrastructures in recent years, increasing importance has been attached to the security of the Cyber-Physical System (CPS) of the infrastructures. Machine learning technology nowadays is evolving rapidly, and is widely implemented in detecting or preventing such attacks. As a result, this research constructs a Testbed to collect relevant data sets to support machine learning requirements, such as training models and analyzing attacks, etc.

Keywords: Testbed, CPS, Critical infrastructure, Dataset, Machine learning.

1. Introduction

Critical infrastructures have improved quality of our life during years of development. After the Industry 4.0 concept been introduced in 2011 [1], a secured CPS [2] has been the main goal of various fields of industry. A CPS are integration of computation, networking, and physical process. With CPS, we can supervise both the physical process and the network traffic of the system, even improve the performance and resource allocation of the system.

Nevertheless, there are many vulnerabilities that exist in the CPS of the infrastructure which may put people in great danger. In the case of dam facilities, there are failures and attack events happening to the dams every year. Some of these failures happened due to the anomaly inflow which can be caused by extreme weather, such as the Loas Dam collapse [3] and the Sandford Dam failure [4] in 2018 were both caused by heavy rains; on the other hand, the cyberattack toward the Bowman Avenue Dam in 2013 [5] had revealed the potential crisis that hackers could do to the system.

Thankfully, the maturity of machine learning and neural networks brings different kinds of detection models to prevent such threats. For instance, J. Goh et al. [6] take advantage of the Recurrent Neural Network (RNN) to train models with datasets to detect

[*] Corresponding author's E-mail: jsli@mail.ncku.edu.tw

cyberattacks. Another example is the anomaly detection for water treatment by J. Inoue et al. [7]

Though the two aforementioned methods both focus on water treatment, the security of dam CPS can no longer be ignored after the tragedies happened around the world. As the result, a testbed that contains both physical and network aspects of data in a dam scenario is needed and became the main goal of this study.

2. Research Background

Our study refers to the concepts of the Industrial Control System (ICS) [8] and ISA-95 [9] framework. Building our system by following the structures that are currently running in the industry makes our data more convincing. Hence, we are taking a brief look at these frameworks before diving into our testbed.

2.1. *Industrial Control System*

An ICS is a set of devices, systems, and networks that operate or automate industrial processes. ICSs usually include some core components, such as Human Machine Interfaces (HMI) [10] and Supervisory Control and Data Acquisition (SCADA) [11] systems that monitor and lead the whole operation; some Master/Remote Terminal Units (MTU/RTU) that send commands; some Programmable Logic Controllers (PLC) [12] that execute the commands by controlling the physical devices; and a Data Historian which record all historical log data of the operation. Despite there are many different ICSs for particular use cases, all of them are managed to control, monitor, and merge Informational Technology (IT) and Operational Technology (OT) aspects of the system.

2.2. *ISA-95*

ISA-95 [9] is an international standard from the International Society of Automation (ISA) that defines the interface between enterprise systems and ICSs. This testbed will be covering the bottom four levels in the five levels of the standard, which includes signals, PLCs, HMIs, and the database.

When collecting the data of our dam testbed, it is important to comply with the proper time scale at each level since time-related features of the data are crucial elements for detecting attacks or anomaly status of the dam system.

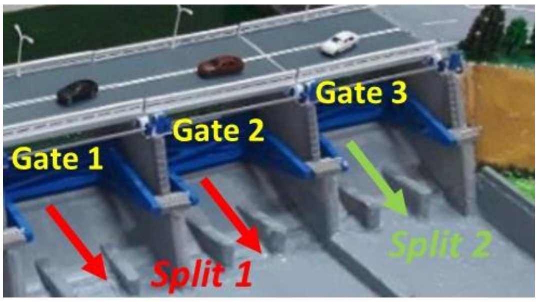

Fig. 1. The three gateways dam scenario of the testbed.

3. Testbed Architecture

The goal of our testbed is to make the data we collect similar to an actual dam CPS, so we build our testbed imitating a retired dam in Taiwan. The details of the architecture will be described in this section.

3.1. *Dam Environment*

The architecture of the testbed is shown in Fig.1, we simulate three gateways of the dam with PLCs, which control the water discharge of the dam.

Water level of the dam is affected by the upstream inflow, the rainfall, and the downstream water discharge. The downstream of the dam will be divided into two splits: *Split 1* controlled by the two gateways representing the main discharge; and *Split 2* is defined as a regular outflow considering some dams contain gateways arranged for the intake of other purposes, such as domestic water supply, agricultural water supply, etc.

3.2. *CPS framework*

As shown in Fig.2, the HMI will not only continuously ask the connected PLCs for the status of the gateways, but also be able to send commands to PLCs through Modbus TCP [13] packets and transmit the log data to the connected SQL server to record the operations.

The control panel is an entity for on-site dam control. After all, in a real dam operation, workers usually interact with the facilities by pressing buttons of control panels on the spot due to the security concerns.

On the other hand, the actual DI/DO status of the gateways will be simulated and recorded, the reason behind this design is that Man-in-the-middle (MITM)

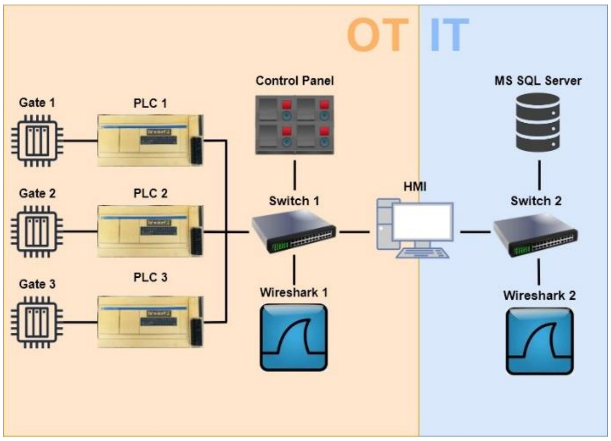

Fig. 2. The CPS framework of the testbed, including IT and OT aspects of the system.

attacks [14] can happen between PLCs and HMI, which makes the SQL server receive fake data.
Finally, the transmitted packets within OT and IT networks will also be recorded separately through Wireshark [15] hosts.

The operations of the three gates and HMI will follow the historical data of a retired dam system as input, the input data contain normal operations of the dam and some non-normal events such as abnormally high rainfall, abnormal gateway operation, abnormally upstream inflow increase, etc. We are also planning to add more attack situations on the testbed to increase the variety of the generated dataset.

3.3. *Data Structure*

Similar to the most used water treatment dataset SWaT [16], the structure of the data will be split into two parts: physical and network.

The physical part of data comes in Comma-Separated Values (.csv) files, which contain a few attributes of each status of dam facilities, such as the open degree of gateways, the inflow values, water level, etc., and the timestamps.

For the network part, all log data will be collected in the form of Packet Capture (.pcap) files through the Wireshark application.

4. Testbed Implementation

To implement the aforementioned testbed architecture in Fig.2, we utilize the devices of a retire dam system, including the Schneider TWDLCAE40DRF PLCs [17] and the HMI and database in the form of Windows 7 virtual machines on a Windows 10 PC. We have also arranged two extra Windows 10 PCs for the Wireshark packets recording, the Cisco IE 4000 [18] for *Switch 1*, and the HP 1810-8G [19] for *Switch 2*; as for the gates of the dam, the Arduino MEGA 2560 boards [20] are utilized to present their DI/DO values.

5. Conclusions and Future Works

In this study, a testbed CPS that covers both OT and IT aspects of a dam environment is established. With all the components of the retired dam system, the testbed is highly associated with the real dam infrastructures.

In the future, we are heading to fully publish our dataset based on historical data, and working on generating our own input data with the features of historical data, or even adding more physical and cyber attack scenarios to the testbed.

After all, the testbed must be continuously improved in terms of reliability and variety to make a greater contribution to the security of critical infrastructures.

Acknowledgements

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

References

1. Lasi, H., Fettke, P., Kemper, HG. *et al.* “Industry 4.0”, Business and Information Systems Engineering, Vol. 6, pp. 151-152, 2015.
2. E. A. Lee, “CPS foundations”, Design Automation Conference, pp. 737-742, 2010.
3. BBC NEWS, “Loas dam collapse: Many feared dead as floods hit villages”, https://www.bbc.com/news/world-asia-44935495
4. WECT, “Sanford Dam fails due to rising waters from Florence”, https://www.wect.com/story/39099087/sanford-dam-fails-due-to-rising-waters-from-florence/
5. GARY COHEN, “Throwback Attack: How the modest Bowman Avenue Dam became the target of Iranian hackers”, https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/

6. J. Goh, S. Adupu, M. Tan and Z. S. Lee, "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks", 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140-145, 2017.
7. J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt and J. Sun "Anomaly Detecion for a Water treatment System Using Unsupervised Machine Learning", 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 1058-1065, 2017.
8. K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn "Guide to Industrial Control Systems (ICS) Security", NIST Special Publication 800-82, R2, 2014.
9. ISA, "ISA95, Enterprise-Control System Integration", https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95
10. P. Papcun, E. Kajati and J. Koziorek "Human Machine Interface in Concept of Industry 4.0", 2018 World Symposium on Digital Intelligence for Systems and Machines (DISA), pp. 289-296, 2018.
11. A. Daneels and W. Salter, "WHAT IS SCADA?", International Conference on Accelerator and Large Experimental Physics Control System, Trieste, Italy, 1999.
12. E. R. Alphonsus, M. O. Abdullah "A review on the applications of programmable logic controllers (PLCs)", Renewable and Sustainable Rnergy Reviews, Vol. 60, pp. 1185-1205, 2016.
13. Andy Swales, "Open Modbus/TCP Specification", Schneider Electric, Vol. 29, pp.3-19, 1999.
14. Avijit Mallik, "Man-in-the-middle-attack: Understanding in simple words", Cyberspace: Jurnal Pendidikan Teknologi Informasi, Vol. 2, pp.109-134, 2018.
15. Gerald Combs, "Wireshark", https://www.wireshark.org
16. iTrust, "Secure Water Treatment (SWaT) Dataset" , https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95
17. Schneider Electic, "TWDLCAE40DRF" , https://www.se.com/ww/en/product/TWDLCAE40DRF/compact-plc-base-twido-100-240-v-ac-supply-24-i-24-v-dc-16-o/
18. Cisco, "Industrial Ethernet 4000 Series Switches" , https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html
19. HPE, "HPE OfficeConnect 1810 Switch Series" , https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c02500478
20. Arduino, "Arduino MEGA 2560 Rev3" , https://store.arduino.cc/products/arduino-mega-2560-rev3

Authors Introduction

Mr. 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. 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.

Prof. Jung-Shain 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 the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.