SUGISAKA MASANORI

Journal of Advances in Artificial Life Robotics
Vol. 4(2); September (2023), pp. 106–109
ON LINE ISSN 2435-8061; ISSN-L 2435-8061
https://alife-robotics.org/jallr.html

Research Article

Cyber-Physical Security Testbed for Dam Control System

Meng-Wei Chang, Jung-Shian Li, 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

ARTICLE INFO

Article History
Received 08 October 2022
Accepted 30 October 2023

Keywords
Critical infrastructure
CPS
ML-Ask
Testbed
Machine learning
Dataset

ABSTRACT
As critical infrastructure has seen substantial growth in recent years, the security of its Cyber-Physical Systems (CPS) has gained greater significance. The rapid evolution of machine learning technology is being harnessed to detect and prevent these threats. Accordingly, this study establishes a Testbed for gathering pertinent datasets to aid machine learning needs, including model training and attack analysis.

1. Introduction

Over the years of development, critical infrastructures have significantly enhanced our quality of life. The introduction of the industry 4.0 concept [1] in 2011 marked a pivotal moment, prompting various industries to prioritize the establishment of secure Cyber-Physical Systems (CPS) [2]. CPS, which integrate computation, networking, and physical processes, empower us to monitor the system's physical processes and network traffic, enhancing overall system performance and resource allocation.

However, vulnerabilities persist in the infrastructure's CPS, potentially endangering lives. Dam facilities, in particular, experience annual failures and security breaches. Some failures result from abnormal inflows triggered by extreme weather conditions, such as the Loas Dam collapse due to heavy rainfall in 2018 [3]. On a different note, the cyberattack on the Bowman Avenue Dam in 2013 [4] exposed the system's vulnerability to potential hacker-induced crises.

Fortunately, the progress in machine learning and neural networks has paved the way for a multitude of novel detection models to counter these threats. For example, J. Goh and their team [5] have leveraged the capabilities of Recurrent Neural Networks (RNN) to develop models for the identification of cyberattacks, utilizing datasets in the training process. Similarly, J. Inoue and their colleagues [6] have dedicated their efforts to pioneering anomaly detection methodologies in the domain of water treatment, adding another layer of security to critical infrastructure.

While the two methods mentioned above center on water treatment, the importance of addressing the security of dam Cyber-Physical Systems (CPS) can no longer be understated in light of global incidents. Consequently, this study places a strong emphasis on the development of a testbed that encompasses both physical and network data components within a dam environment, marking a primary objective of this research

Corresponding author's E-mail: ihliu@cans.ee.ncku.edu.tw, mwchang@cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw URL: www.ncku.edu.tw

2. Research Background

Our research delves into the principles of Industrial Control Systems (ICS) [7] and the SWaT testbed developed in Singapore [14]. Constructing our system in alignment with existing industry standards lends credibility to our data. As such, we will provide a concise overview of these frameworks before diving into the specifics of our testbed.

2.1. *Industrial Control System*

An Industrial Control System (ICS) is a comprehensive network designed to automate industrial processes, comprising various elements such as Human Machine Interfaces (HMI) [8] and Supervisory Control and Data Acquisition (SCADA) [9] systems. These components work together with Master/Remote Terminal Units (MTU/RTU) to transmit commands, Programmable Logic Controllers (PLC) [10] to execute these commands, and a Data Historian for logging historical operational data. While ICS variations cater to specific applications, their primary role is to manage and integrate both Information Technology (IT) and Operational Technology (OT) aspects within the system.

2.2. *SWaT*

The iTrust SWaT (Secure Water Treatment) testbed replicates a water treatment plant, serving as a research facility for cybersecurity in industrial control systems (ICS). It allows controlled experiments and vulnerability assessments, aiding the development of security solutions to protect critical infrastructure from cyber threats and enhance ICS security.

Similar to SWaT, we need to record information like water flow and gate status. However, our architectural focus lies in simulating and recording dam gate controls, hence emphasizing the status and command messages of the gate.

3. Testbed Architecture

The objective of our testbed is to is to mimic a real dam's CPS in the data we collect, achieved by replicating a retired dam in Taiwan. We will delve into the architectural specifics in the following section, outlining how this goal is accomplished.

3.1. *Dam Environment*

The testbed's structure is visually represented in Fig.1, featuring the simulation of seven spillways within the dam, each managed by PLCs.

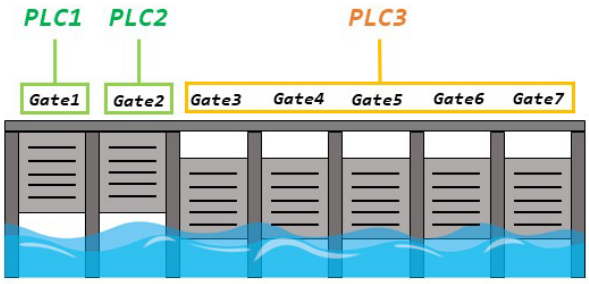

Fig. 1. The dam scenario within the testbed, featuring seven spillways, which are controlled by three PLCs

The water level within the dam is subject to fluctuation due to factors including the inflow from upstream, rainfall, and the discharge of water downstream. There are seven gates in total, the first two representing the regular discharge which is controlled by two PLCs; and the others will be the backup spillways that only rise up by a same PLC simultaneously when needed.

The primary objective of the spillways is to regulate the water level within the dam to accommodate a range of purposes, including agricultural and domestic water supply. Conversely, any gate control behaviors that result in either excessively high or low water levels are classified as non-normal operations. Such deviations from normal operations have the potential to lead to serious dam failures or an inability to meet water supply demands.

3.2. *CPS framework*

As depicted in Fig.2, the Human Machine Interface (HMI) maintains a constant query to the connected PLCs for gateway status updates and possesses the capability to transmit commands to the PLCs via Modbus TCP [11] packets. Furthermore, it communicates with the linked SQL server to log the operational data.

The Arduino boards are used to serves as the primary interface for on-site dam management. In actual dam operations, workers commonly engage with the facility's controls by physically pressing buttons on the control panels, a practice necessitated by security considerations. This design choice is motivated by the

potential occurrence of Man-in-the-Middle (MITM) attacks [12] between the PLCs and HMI, posing a risk of delivering counterfeit data to the SQL server. Additionally, we will separately capture and store the transmitted packets within both the OT and IT networks using Wireshark [13] hosts.

Inflow data for the dam is sourced from historical records of a retired dam system. Gate control behavior includes typical operations for positive samples and irregular events, such as incorrect gate control, creating non-standard gate statuses as negative samples. Our future plans involve adding more attack scenarios to enhance dataset diversity.

4. Testbed Implementation

To put the testbed architecture depicted in Fig.2 into practice, we've assembled an array of components from a retired dam system. These include the Schneider TWDLCAE40DRF PLCs [15], the HMI, and a Windows 10 PC serving as the database.

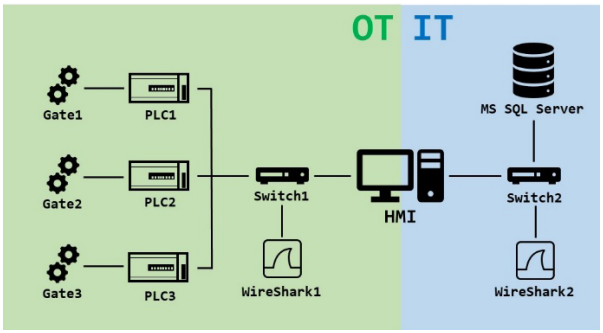

Fig. 2. The testbed's CPS framework comprises both the IT and OT elements within the system

In addition, we've incorporated two extra Windows 10 PCs dedicated to the task of recording packets using Wireshark. Furthermore, the network infrastructure features the Cisco IE 4000 [16] for Switch 1 and the HP 1810-8G [17] for Switch 2.

To mimic the behavior of the dam gates, we've integrated Arduino MEGA 2560 boards [18] to emulate the DI/DO values associated with the gates, these values will also be recorded. The Operate behaviors can be executed by two paths: serial communication or PLC digital outputs. Where serial communication emulates on-site gate control, while the PLC digital output serves as the remote control from the HMI.

This comprehensive setup enables us to accurately replicate and record the interactions and operations of the dam control system for further analysis and experimentation.

5. Conclusions and Future Works

In our research, we have developed a comprehensive *CPS testbed that encompasses both OT and IT elements* within a dam environment. This testbed is closely aligned with real dam infrastructures, utilizing components from a retired dam system.

Looking ahead, our plans include the collection of the dataset for different types of operation, or even complete publication of the dataset. We are also exploring the potential integration of additional physical attack and cyberattack scenarios into the testbed.

Our primary focus is on elevating the testbed to enhance the security of critical infrastructure systems.

Acknowledgements

This work was supported by the National Science and Technology Council (NSTC) in Taiwan, under contract numbers 111-2218-E-006-010-MBK and 112-2634-F-006-001-MBK, and the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) in Taiwan.

References

1. Lasi, H., Fettke, P., Kemper, HG. *et al.* "Industry 4.0," *Business and Information Systems Engineering*, Vol. 6, pp. 239-242, 2014.
2. E. A. Lee, "CPS foundations," *Proceedings of the 47th design automation conference*, Anaheim, CA, USA, 13-18 Jun., 2010.
3. BBC NEWS, "Loas dam collapse: Many feared dead as floods hit villages," 2018. [Online]. Available: https://www.bbc.com/news/world-asia-44935495. [Accessed 7 Aug 2022]
4. GARY COHEN, "Throwback Attack: How the modest Bowman Avenue Dam became the target of Iranian hackers," 2021. [Online]. Available: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/. [Accessed 7 Aug 2022]
5. 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)*, Singapore, 12-14 Jan., 2017.
6. 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), New Orlearns, LA, USA, 18-21 Nov., 2017.
7. K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, R2, USA, 2014.
8. 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), Slovakia, 23-25 Aug., 2018.
9. A. Daneels and W. Salter, "WHAT IS SCADA?", 7th International Conference on Accelerator and Large Experimental Physics Control System, Trieste, Italy, 4-8 Oct., 1999.
10. 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.
11. Andy Swales, *Open Modbus/TCP Specification*, R1, Schneider Electric, France, 1999.
12. Avijit Mallik, "Man-in-the-middle-attack: Understanding in simple words", *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, Vol. 2, pp.109-134, 2018.
13. Gerald Combs, "Wireshark", 1998. [Online]. Available: https://www.wireshark.org. [Accessed 7 Aug 2022]
14. iTrust, "Secure Water Treatment (SWaT) Dataset" [Online]. Availabe: https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/. [Accessed 7 Aug 2022]
15. Schneider Electic, "TWDLCAE40DRF," 2022. [Online]. Available: https://www.se.com/ww/en/product/TWDLCAE40DRF/compact-plc-base-twido-100-240-v-ac-supply-24-i-24-v-dc-16-o/. [Accessed 7 Aug 2022]
16. Cisco, "Industrial Ethernet 4000 Series Switches," 2022. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html. [Accessed 7 Aug 2022]
17. HPE, "HPE OfficeConnect 1810 Switch Series," 2022. [Online]. Available: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c02500478
18. Arduino, "Arduino MEGA 2560 Rev3," 2022. [Online]. Available: https://store.arduino.cc/products/arduino-mega-2560-rev3. [Accessed 7 Aug 2022]

Authors Introduction

Mr. Meng-Wei Chang

He is a postgraduate of Cloud and Network Security (CANS) Lab, 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.

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.

Prof. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. 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. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University(TWISC@NCKU).