# MiniDAM: A Dam Cybersecurity Toolkit

**Tzu-En Peng**
*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*

**Yun-Hao 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*

**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*
*E-mail: tepeng@cans.ee.ncku.edu.tw, mwchang@cans.ee.ncku.edu.tw, yhchang@cans.ee.ncku.edu.tw,*
*jsli@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw*[*]
*www.ncku.edu.tw*

**Abstract**

Testbeds, serving as simulations of real-world scenarios, are of paramount importance for research in cybersecurity related to critical infrastructure. In this paper, we aim to offer a comprehensive exploration of the MiniDAM and our testbed, introducing its physical settings based on real dam operational standards. Furthermore, a comparative analysis between the Secure Water Treatment (SWaT) testbed, MiniCPS, our testbed, and MiniDAM is presented. This paper also includes insights into dataset generation and the integration of other functionalities. The exposition of MiniDAM's features and capabilities serves as a foundation for enhancing resilience and provides valuable support for advancing research within the broader field of dam-related studies.

*Keywords*: Dam Testbed, Critical Infrastructure, Industrial Control System, Cyber-Physical System, Cybersecurity

## 1. Introduction

Critical infrastructures [1] have significantly enhanced our quality of life over years of development. Since the introduction of the Industry 4.0 [2] concept, ensuring the security of Cyber-Physical Systems (CPS) [3] has become a primary objective across various industrial sectors. CPS involves the seamless integration of computation, networking, and physical processes. Through CPS, we gain the capability to monitor both the physical processes and network traffic within a system, thereby enhancing overall system performance and resource allocation.

However, despite the advancements, numerous vulnerabilities persist within the CPS of critical infrastructures, posing potential risks to public safety [4]. Dam facilities, in particular, experience failures and security breaches annually. The cyberattack on the Bowman Avenue Dam in 2013 underscored the potential crisis posed by malicious actors targeting these systems. Conversely, Some failures are attributed to anomalies in inflow, often triggered by extreme weather conditions. For instance, the collapse of the Laos Dam and the Sandford Dam failure in 2018 were both consequences of heavy rainfall.

The security of dam CPS can no longer be ignored after the tragedies that happened around the world. As a result, a testbed with a toolkit that contains both physical and network aspects of data for further research in a dam scenario is needed.

## 2. Research Background

Our research is primarily based on the concept of Cyber-Physical Systems (CPS), focusing on the investigation of the widely referenced SWaT Testbed [5] and MiniCPS [6]. Subsequently, we compare their features with our own testbed and toolkit.

### 2.1. *Cyber-Physical System*

CPS represents an innovative paradigm that integrates computational algorithms and physical processes to create intelligent and interconnected systems. These systems enable seamless communication and collaboration between the digital and physical worlds, allowing for real-time monitoring, control, and optimization of diverse applications.

R. Alguliyev et al. [7] illuminated the principle of CPS operation and philosophical issues of CPS raised, and also proposed a tree of attacks on CPS. J. Shi et al. [8] described and summarized the features of CPSs, then three classic cases were given with research challenges and suggestions for future work.

### 2.2. *SWaT Testbed & MiniCPS*

When it comes to testbeds and toolkits in the field of CPS, the SWaT Testbed and MiniCPS are frequently referenced.

#### 2.2.1. *SWaT Testbed*

Secure Water Treatment (SWaT) is a water treatment testbed for research in the field of cybersecurity. SWaT consists of a six-stage process of water treatment with frequently used industrial components, such as Programmable Logic Controllers (PLCs) made by Allen-Bradley, Human Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) workstation, Historian, etc. The SWaT Dataset systematically generated from the testbed is also provided for CPS researchers to do further analysis and other related works.

#### 2.2.2. *MiniCPS*

MiniCPS is a toolkit built on top of Mininet [9] to provide an extensible, reproducible research environment for network communications, control systems, and physical-layer interactions in CPS. MiniCPS was also used to model the communication and control aspects of SWaT while illuminating example applications.

MiniCPS focuses on high-fidelity network emulation and being a framework for all fields of CPS. However, the full-fledged physical process simulation was considered to be out of the scope of MiniCPS since it does not aim to be a performance simulator. Furthermore, MiniCPS can only run on Linux operating systems due to its reliance on Mininet. MiniCPS also put very little emphasis on Visualization, such as Graphical User Interface (GUI).

The issues mentioned above could pose challenges to the reproducibility of research for researchers in specific domains.

## 3. Dam Cybersecurity Toolkit Architecture

For the physical part of our toolkit, we utilize the PLCs that had been used in a real dam field environment in Taiwan. We also obtained the dam history log which consists of related information during the period, such as water level, opening of the gates, gates inflow, gates outflow, etc.

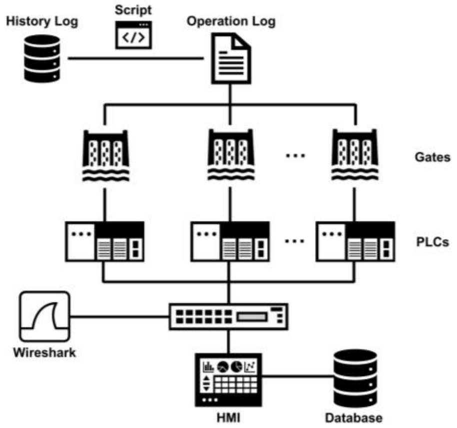
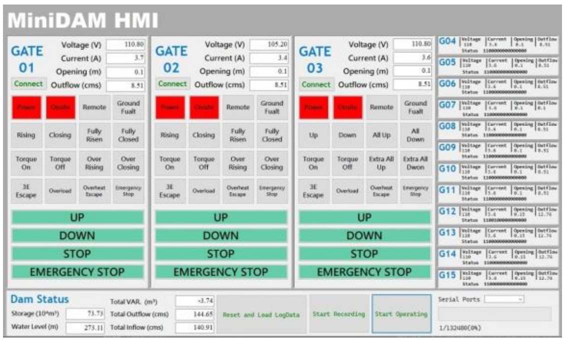


Fig. 1. Architecture of The Dam Cybersecurity Toolkit

The architecture of the dam cybersecurity toolkit is shown in Fig. 1. We further process the history log with the script based on the operational standards of the real dam to generate the operation log which defines how PLCs should work while facing the situation of the corresponding history log. As shown in Fig. 2, we also use our HMI to monitor the states of the PLCs, the overall operation is recorded in the database, and Modbus/TCP packets between HMI and PLCs are simultaneously captured using Wireshark for CPS researchers in the dam field to conduct further analysis and experiments that need related dataset, such as machine learning [10].



MiniDAM HMI

GATE 01 — Voltage (V) 110.80; Current (A) 3.7; Opening (m) 0.1; Outflow (cms) 8.51

GATE 02 — Voltage (V) 105.20; Current (A) 3.4; Opening (m) 0.1; Outflow (cms) 8.51

GATE 03 — Voltage (V) 110.80; Current (A) 3.6; Opening (m) 0.1; Outflow (cms) 8.51

Dam Status — Storage (10⁴m³) 73.73; Water Level (m) 273.11; Total VAR (m³) -3.74; Total Outflow (cms) 144.65; Total Inflow (cms) 140.91

1/132480(0%)

Fig. 2. MiniDAM HMI

## 4. Applications of The Dam Cybersecurity Toolkit

### 4.1. *Dam Environment Simulation*

In contrast to MiniCPS, MiniDAM places a heightened focus on Cyber-Physical Systems (CPS) within dam field environments. Leveraging pertinent Programmable Logic Controllers (PLCs) and historical logs derived from actual usage in dam fields, we meticulously construct a tailored Graphical User Interface (GUI) to facilitate operational tasks. This approach enables us to bridge the gap between theoretical models and real-world dam scenarios. As a result, we generate a diverse array of datasets corresponding to various operational scenarios. These datasets serve as valuable resources for dam domain researchers, offering them rich materials for in-depth analysis and exploration of the intricacies within dam environments.

### 4.2. *Dataset Generation*

In addition to recording related information in the database during operation. Modbus/TCP packets are also captured using Wireshark. As shown in Fig. 3, HMI and PLCs communicate with each other using Modbus/TCP protocol. We can generate datasets for different non-normal scenarios by modifying the logic within the script.

As illustrated in Fig. 4, due to significant variations in water flow in Taiwan during the summer season, a comparison of the history log and dataset regarding the water capacity difference over the period of the summer of 2017 was conducted within a normal scenario defined according to operational standards. We observed that the dataset and history log exhibit similar characteristics, demonstrating the validity of our operation log and the similarity between the dataset and the actual field.

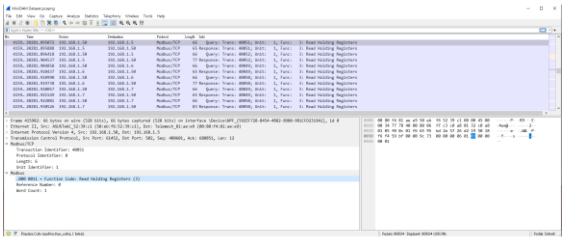


Fig. 3. Modbus/TCP Packets Dataset

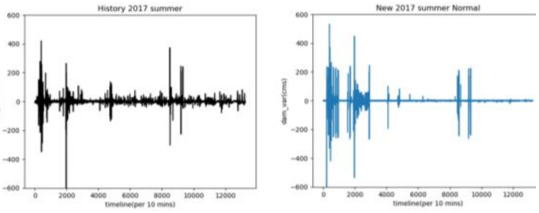


Fig. 4. Comparison of The History Log and Dataset regarding The Water Capacity Difference over The Period of 2017 Summer in a Normal Scenario

## 5. Conclusion

In this study, we introduce MiniDAM's physical settings based on the real dam operational standards and how our toolkit differs from MiniCPS. Furthermore, we illustrate the features of MiniDAM, including dataset generation.

In the future, we are heading to build a comprehensive CPS interface for the dam operations to extend the testbed's [11] functions. Thoroughly define how virtual and physical devices interface with our toolkit, taking into account hydrological information for broader watershed analysis.

## Acknowledgment

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract number 112-2634-F-006-001-MBK.

## References

1. W. Liu and Z. Song, “Review of studies on the resilience of urban critical infrastructure networks,” *Reliability Engineering & System Safety*, vol. 193, 106617, 2020.
2. M. Ghobakhloo, “Industry 4.0, digitization, and opportunities for sustainability,” *Journal of Cleaner Production*, vol. 252, 119869, 2020.
3. E. A. Lee, “CPS foundations,” DAC '10: Proceedings of the 47th Design Automation Conference, Anaheim, California, USA, 12-18 Jun., 2010.
4. J. M. Taylor and H. R. Sharif, “Security challenges and methods for protecting critical infrastructure cyber-physical systems,” 2017 International Conference on Selected Topics in

Mobile and Wireless Networking (MoWNeT), Avignon, France, 17-19 May, 2017.
5. A. P. Mathur and N. O. Tippenhauer, "SWaT: a water treatment testbed for research and training on ICS security," 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), Vienna, Austria, 11-11 Apr., 2016.
6. D. Antonioli and N. O. Tippenhauer, "MiniCPS: A Toolkit for Security Research on CPS Networks," CPS-SPC '15: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, Denver, Colorado, USA, 12-16 Oct., 2015.
7. R. Alguliyev, Y. Imamverdiyev and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212 - 223, 2018.
8. J. Shi, J. Wan, H. Yan and H. Suo, "A survey of Cyber-Physical Systems," 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 09-11 Nov., 2011.
9. Mininet, "Mininet: An Instant Virtual Network on your Laptop (or other PC)," 2023. [Online]. Available: http://mininet.org/. [Accessed 10 12 2023].
10. O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11-14 Dec., 2017.
11. M.-W. Chang, J.-S. Li, I-H. Liu, 2023, "Cyber-Physical Security Testbed for Dam Control System", *Journal of Advances in Artificial Life Robotics*, Vol. 4, No. 2, pp. 63-66.

## Authors Introduction

Mr. Tzu-En Peng

He is acquiring a master's degree in the Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. He obtained his B.S. degree from the Department of Electrical Engineering, National Cheng Kung University, Taiwan in 2022. His interests are Cyber-Security and Industrial Control Systems.

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.

Mr. Yun-Hao Chang

He is acquiring a master's degree in the Department of Electrical Engineering /Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. His interests are blockchain technology and Industrial Control Systems.

Prof. 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 cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. 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. He teaches cybersecurity courses and 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).