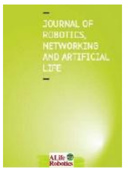
SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 11(1); May (2025), pp. 73–77
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html



Research Article

MiniDAM: A Comprehensive Toolkit for Dam Cybersecurity

I-Hsien Liu, Tzu-En Peng, Meng-Wei Chang, Yun-Hao Chang, Jung-Shian Li
National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan

ARTICLE INFO

Article History
Received 31 October 2023
Accepted 19 March 2025

Keywords
Critical
Infrastructure
Testbed
Cybersecurity
ICS
CPS

ABSTRACT

Testbeds play a crucial role in cybersecurity research for critical infrastructure by simulating realistic environments. This paper presents an in-depth examination of the MiniDAM toolkit and our developed testbed, which is modeled on actual dam operation standards. We provide a detailed overview of its functionalities. Additionally, a comparative study is conducted between MiniDAM, our testbed, MiniCPS, and the Secure Water Treatment (SWaT) testbed. This work further discusses the process of generating datasets and incorporating additional features. The capabilities of MiniDAM are demonstrated as a robust platform, significantly contributing to the advancement of research in dam cybersecurity.

1. Introduction

Critical infrastructures [1] have played a pivotal role in enhancing societal well-being over the years. With the emergence of Industry 4.0 [2], securing Industrial Control Systems (ICSs) and Cyber-Physical Systems (CPSs) has become a crucial focus. ICSs are widely deployed across critical infrastructures, including power grids, water treatment plants, and dams. ICSs are designed to automate and control complex industrial processes, facilitating real-time monitoring and decision-making to ensure operational stability. However, the interconnection of these systems with external networks making their security a top priority. CPS represents the fusion of computational, networking, and physical elements, enabling the monitoring and optimization of both physical processes and network activities within a system. This integrated approach offers significant improvements in system efficiency and resource management.

Although CPS has made significant progress, critical infrastructure remains vulnerable, presenting substantial threats to society. Dams, specifically, are susceptible to operational failures and cybersecurity breaches, with incidents occurring annually. Certain failures are linked to abnormal inflow conditions, often resulting from severe weather events. For instance, in 2018, the collapses of the Sandford Dam and Laos Dam were triggered by intense rainfall.

Given the impact of such incidents worldwide, ensuring the security of dam-related CPS is imperative. To meet this requirement, an extensive testbed that incorporates both operational and communication data specific to dam environments is crucial for advancing research efforts.

2. Research Background

This research centers around ICSs and CPSs, with a emphasis on researching the well-known SWaT Testbed [3] and the MiniCPS [4]. Our work involves a comparison of these established testbeds with the design and functionalities of our own testbed and toolkit.

2.1. *Industrial Control System*

ICSs play a vital role in the automation and supervision of intricate industrial processes within critical infrastructure. These systems often incorporate Distributed Control Systems (DCS) to distribute control across multiple components and Supervisory Control and Data Acquisition (SCADA) systems to collect and monitor real-time data. Additionally, Programmable

Corresponding author E-mail: jsli@cans.ee.ncku.edu.tw

Logic Controllers (PLCs) are fundamental to automating tasks and processes, ensuring the efficiency and safety of operations.

D. Bhamare et al. [5] analyzed the evolving landscape of ICSs and examined key contributions from both industry and academia in advanced technologies. They believe that testbeds play a critical role in addressing security challenges by offering deeper insights into the management of industrial processes.

2.2. *Cyber-Physical System*

CPS provide a framework that merges computational algorithms with physical processes, allowing for the creation of smart, interconnected systems. This integration facilitates seamless interaction between the digital and physical worlds, enabling real-time monitoring, data exchange, and system control. By linking sensors, controllers, and actuators with advanced computing technologies, CPS enhances the ability to optimize performance, increase automation, and respond dynamically to changing conditions, making these systems highly effective in critical applications such as industrial automation, transportation, and smart infrastructure management.

J. Shi et al. [6] provided a detailed overview of CPS characteristics, illustrating their functionality through three representative case studies. They also identified key research challenges and proposed directions for future studies to enhance the resilience and effectiveness of CPS.

2.3. *SWaT Testbed and MiniCPS*

The SWaT Testbed and MiniCPS are often cited as key references for testbeds and toolkits in the realm of CPS research.

2.3.1. *SWaT Testbed*

SWaT serves as a dedicated testbed for conducting cybersecurity research related to water treatment systems. It features a six-stage water treatment process utilizing commonly used industrial components, including Allen-Bradley PLCs, Human Machine Interfaces (HMIs), SCADA workstations, and a Historian. The SWaT Dataset, produced systematically from this testbed, is provided to researchers in the field of CPS for comprehensive analysis and further study.

2.3.2. *MiniCPS*

MiniCPS has been utilized to simulate the control elements and communication of the SWaT Testbed. This toolkit, built on the Mininet platform, provides a versatile and replicable research environment for investigating communication networks and system controls in CPS.

While MiniCPS serves as a comprehensive framework for various CPS fields, it does not include full-scale physical process simulation. Moreover, MiniCPS operates exclusively on Linux systems because of its reliance on Mininet and provides only basic support for visualization tools like Graphical User Interfaces (GUIs).

These limitations may present challenges for researchers in certain domains, potentially affecting the reproducibility and accessibility of their studies.

3. Architecture of the Dam Cybersecurity Toolkit

The physical component of our toolkit incorporates PLCs that were previously deployed in an operational dam environment in Taiwan. In addition, we have collected historical logs that provide detailed records of key operational parameters, such as water levels, gate positions, inflow, and outflow data over specific periods.

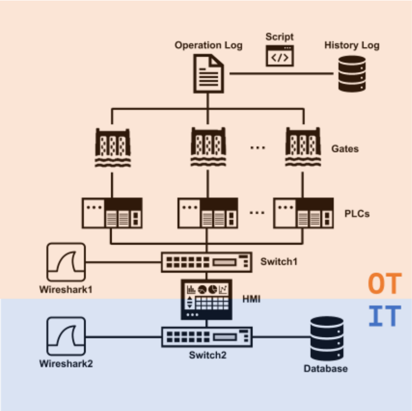


Fig. 1. The Cybersecurity Toolkit Architecture for Dam

Fig. 1 presents a comprehensive overview of the architecture of our toolkit designed for enhancing dam cybersecurity. To create an operation log that dictates the behavior of the PLCs based on the scenarios outlined in the historical data, we utilize a script that processes the history logs in accordance with the operational standards of the real dam. This approach ensures that the simulated conditions closely mirror actual dam operations, providing an accurate representation of how the PLCs should respond under various circumstances. By aligning the operational log with real-world protocols, we enable more precise testing and analysis of both system performance and potential vulnerabilities.

4. Experiment

4.1. *Simulation of the Dam Environment*

Unlike MiniCPS, MiniDAM is specifically designed to address CPS in dam-related environments. We have created a tailored GUI using appropriate PLCs and historical logs from real dam operations to facilitate a range of operational activities. This method effectively connects theoretical models with real-world dam applications.

We conducted a comparative analysis of the statistical characteristics between normal operation experiments and historical records, focusing on capacity variations. As shown in Table. 1, the findings reveal a 58.6% decrease in average storage discrepancies during normal operation experiments compared to historical data. A visual comparison, shown in Fig. 2, further illustrates that storage variations are generally more stable during normal operations compared to historical data for most time periods.

Consequently, we generate a wide range of datasets representing different operational scenarios, providing dam researchers with valuable resources for comprehensive analysis and deeper exploration of complex dam environments.

Table. 1. Comparison between Normal Operation and Historical Record

Statistics		Normal operation	Non-normal operation
Storage Difference (cms)	Average	-0.002	-0.002
	Average absolute deviation	1.869	3.169
	Standard deviation	11.362	17.975
Waterlevel (m)	Average	271.707	271.571
	Average absolute deviation	0.192	0.119
	Standard deviation	0.259	0.243

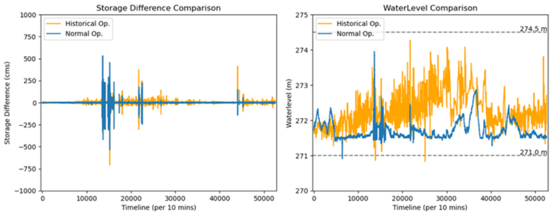


Fig. 2. Data Visualization of Normal Operation and Historical Record

4.2. *Dataset Generation*

In Table. 2, we provide a comparative analysis of several prominent ICS datasets alongside our testbed dataset, CANS RT. Although the widely recognized KDD CUP 1999 and CICIDS datasets have a much larger total number of records, they lack data regarding the states of physical devices, which is critical for understanding the interactions between cyber and physical elements in industrial environments. This limitation makes these datasets less suitable for research focused on CPSs.

On the other hand, our dataset captures a comprehensive range of device state information, which is essential for accurately modeling and simulating real-world industrial scenarios. With a substantial number of records documenting various gate states and other detailed attributes such as voltage and current, our dataset provides a more nuanced view of system behavior.

Table. 2. Comparison between Various Well-known Datasets and Our Dataset

Dataset	Type	Features	Number of Records
KDD CUP 1999 [7]	Network Traffic	41	~7,000,000
CICIDS-2017 [8]	Network Traffic	77	2,830,743
SWaT 2015 [9]	Network Traffic	N/A	N/A
	Status Records	53	944,919
CANS RT 2024 [10]	Network Traffic	N/A	N/A
	Status Records	368	1,051,222

5. Conclusion

In this study, we present the physical configuration of MiniDAM, which is designed in accordance with real dam operational standards, and highlight how our toolkit distinguishes itself from MiniCPS.

Specifically, MiniDAM offers advanced capabilities such as simulating the dam environment and generating datasets. We provide a comparative analysis of normal operations and historical records. This comparison illustrates that our testbed can accurately replicate real-world scenarios. Furthermore, we visually represent the data from normal operations and historical records and offer a comparison between several well-known ICS datasets and our dataset generated from MiniDAM.

Overall, MiniDAM's comprehensive dataset and robust simulation capabilities make it an invaluable resource for researchers in the dam domain, enabling them to explore various operational scenarios.

5.1. *Future Work*

Considering the increasing risks that critical infrastructures like dam control systems, may face in the near future, we are actively developing a more advanced toolkit. It is designed to enhance the functionality of the current testbed [11], introducing additional capabilities such as multiple robust anomaly detection and intrusion detection systems. By incorporating these features, we aim to strengthen the resilience of dam operations against cyber threats, enabling early detection of abnormal activities and unauthorized access. This will improve the security posture of dam infrastructures and provide researchers with a platform for exploring innovative security solutions in critical environments.

Acknowledgment

This work was supported by the National Science and Technology Council in Taiwan under contract numbers NSTC 112-2634-F-006-001-MBK and 113-2634-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, p. 106617, 2020.
2. M. Ghobakhloo, "Industry 4.0, digitization, and opportunities for sustainability," *Journal of Cleaner Production*, vol. 252, p. 119869, 2020.
3. 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.
4. 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.
5. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers & Security*, vol. 89, p. 101677, 2020.
6. 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.
7. M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8-10 Jul., 2009.
8. Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection," *IEEE ACCESS*, vol. 8, pp. 132911-132921, 2020.
9. J. Goh, S. Adepu, K. Junejo and A. Mathur, "A Dataset to Support Research in the Design of Secure Water Treatment Systems.," The 11th International Conference on Critical Information Infrastructures Security, Paris, France, 10-12 Oct., 2016.
10. CANS, "CANS RT," 2024. [Online]. Available: https://www.cans.ee.ncku.edu.tw/research/cansrt. [Accessed 3 1 2024].
11. M.-W. Chang, J.-S. Li and I-H. Liu, "Cyber-Physical Security Testbed for Dam Control System," *Journal of Advances in Artificial Life Robotics*, vol. 4, no. 2, pp. 63-66, 2023.

Authors Introduction

Dr. I-Hsien Liu

He serves as an assistant professor in the Department of Electrical Engineering at National Cheng Kung University, Taiwan. He earned his Ph.D. in Computer and Communication Engineering from National Cheng Kung University in 2015. He teaches cybersecurity courses and his interests are Cyber-Security, OT Security, and Wired & Wireless Communication. He holds the position of deputy director at the Taiwan Information Security Center, National Cheng Kung University (TWISC@NCKU).

Mr. Tzu-En Peng

He earned his M.S. degree in Computer and Communication Engineering from National Cheng Kung University in 2024, and a B.S. degree in Electrical Engineering from National Cheng Kung University, Taiwan. His research focuses on Cybersecurity and ICS.

Mr. Meng-Wei Chang

He earned his M.S. degree in Computer and Communication Engineering from National Cheng Kung University in 2024, and a B.S. degree in Physics from National Taiwan Normal University in 2021. His research focuses on Cybersecurity and ICS Security.

Mr. Yun-Hao Chang

He earned his M.S. degree in Computer and Communication Engineering from National Cheng Kung University in 2024, and a B.S. degree in Industrial Engineering from National Tsing Hua University. His research focuses on Industrial 4.0, Cybersecurity, ICS, and blockchain technology.

Dr. Jung-Shian Li

He serves as a full professor in the Department of Electrical Engineering at National Cheng Kung University, Taiwan. He received his B.S. and M.S. degrees in Electrical Engineering from National Taiwan University in 1990 and 1992, respectively. In 1999, he completed his Ph.D. in Computer Science at the Technical University of Berlin, Germany. He instructs courses on communication and his research areas encompass cybersecurity, cloud computing, and network management. He is currently engaged in funded research projects focused on cybersecurity and the protection of critical infrastructures. He holds the position of director at the Taiwan Information Security Center, National Cheng Kung University (TWISC@NCKU).