The Detecting Abnormal Operations in ICS Using Finite-State Machines

Pei-Wen Chou
Department of Electrical Engineering / M.S. Degree Program on Cyber-Security Intelligence,
National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Nai-Yu Chen
Department of Electrical Engineering / M.S. Degree Program on Cyber-Security Intelligence,
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: pwchou@cans.ee.ncku.edu.tw, nychen@cans.ee.ncku.edu.tw, jsli@ cans.ee.ncku.edu.tw,
*ihliu@cans.ee.ncku.edu.tw**
www.ncku.edu.tw

Abstract

In 2021, a water treatment facility in Florida, USA, fell victim to an external malicious attack. In this incident, malicious actors attempted to manipulate the quantities of specific chemicals to impact water quality and safety. Given the intricacies of abnormal operation detection in Industrial Control Systems and the advantages of finite-state machine, we endeavored to apply this approach for the detection of abnormal ICS (Industrial Control System) operations. We conducted a series of tests using the dam control system cybersecurity testbed established by TWISC@NCKU, Taiwan. The results indicate that our approach effectively enhances the efficiency of identifying non-standard operational behaviors, enabling maintenance personnel to promptly identify anomalies.

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

1. Introduction

In 2021, a water treatment facility in Florida, USA, faced an external malicious attack, where attackers attempted to manipulate the quantities of specific chemicals, severely jeopardizing water quality and safety. [1] How to effectively detect abnormal operation of ICS has become an important challenge?

The integration of FSM methods involves comprehensive monitoring and analysis of system states [2], such as utilizing finite state machines. Taking equipment malfunction as an example, the awareness that its operation may deviate from normalcy prompted the design of a method for detection, employing FSM to monitor changes in PLC states. This amalgamation of state and anomaly detection enables swift identification and response to potential issues, ensuring the stable operation of the system.

This research focused on applying FSM methods to detect abnormal operations within ICS, aiming to enhance detection efficiency and accuracy. This research uses the dam control system cyber-security testbed built by TWISC@NCKU to conduct relevant research and verification. The results show that the scheme is feasible and effective, and the method can be effective at a very low cost. It can identify non-standard operating behaviors and help personnel identify abnormal situations immediately.

2. Methodology

2.1. *Programmable Logic Controller*

A Programmable Logic Controller (PLC) [3] automates control by executing instructions stored in its memory. Crucial in industries, it interfaces with systems like Finite State Machines (FSM) for more efficient monitoring.
PLC states indicate its operations during automation. "DI" and "DO" signify Digital Input and Output, reflecting signal statuses (e.g., switches). "AI" and "AO" represent Analog Input and Output, detailing continuous signal conditions. Together, they showcase the PLC's performance across various inputs and outputs.
Its architecture consists of a CPU, input, and output modules. The CPU processes logic and manages device communication. Inputs gather data from sensors, while outputs control actuators. This robust design ensures stable operation in demanding industrial environments.

2.2. *Finite-State Machine*

In recent years, Finite State Machines (FSMs) have been widely applied in various fields, including software development [2] and machine learning [4]. The strength of FSM methodology lies in its intuitive system model, aiding in the comprehension, design, and testing of intricate system behaviors. Its simplicity and scalability render it an effective tool for describing and controlling system behaviors.

In the context of anomaly detection, FSMs are employed for modeling normal system behavior by defining states and transitions. (Fig.1) This approach involves monitoring system operations, detecting state transitions deviating from expected behavior, and providing real-time alerts. The integration of FSM-based anomaly detection is widely adopted to enhance the efficiency of system behavior modeling and anomaly detection [5], highlighting the pivotal role of FSMs in comprehending system behavior and addressing challenges in anomaly detection.

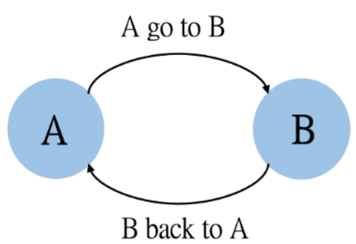

Fig. 1. Finite-State Machine

2.3. *Modbus/TCP*

Modbus is widely employed as a communication protocol in industrial environments, facilitating information exchange among industrial devices such as PLCs and sensors [6]. Despite the convenience of plaintext data transmission provided by Modbus/TCP, it inherently poses potential security risks, making it susceptible to unauthorized access and cyber attacks.

In the context of my research, using Modbus/TCP as an example, although it facilitates communication among industrial devices, careful consideration of associated security risks is crucial. The use of plaintext data transmission introduces the risk of information exposure, thereby compromising the integrity and confidentiality of the system. Therefore, during the implementation of Modbus/TCP, robust security measures must be implemented to mitigate potential risks and enhance the resilience of critical infrastructure.

Simultaneously, by utilizing Modbus commands to read the memory addresses of PLCs [7], specific states such as DI and DO can be understood, with these states stored in specific memory variable addresses. Through Modbus queries, real-time insight into the current status of the PLC can be obtained. This underscores the importance, in practical applications, of handling Modbus communication security cautiously to ensure that the system's operation remains resilient against potential risks and cyber threats.

2.4. *Critical infrastructure testbed*

The research through a series of tests conducted at the Dam Control System Cybersecurity Testbed established by TWISC@NCKU in Taiwan [8]. This simulation validation ensures that the dam system accurately and promptly responds to abnormal conditions during actual operations. The simulation of gate control scenarios on the testbed verifies the correct response of gate operations to simulated abnormal events during actual operations, ensuring the stable operation of the dam system under abnormal conditions. This integrated validation on the testbed contributes to ensuring the safety and reliability of dam systems, enhancing the efficiency of responding to abnormal events during actual operations.

3. Construct the PLC status set based on continuous discovery

3.1. System architecture

In response to cybersecurity and abnormal detection issues in critical infrastructure, this paper proposes the design of an experimental platform for simulating the abnormal detection system of dam gates. (Fig. 2) Each gate is operated by a Programmable Logic Controller (PLC), which is equipped with registers for accessing relevant instructions and data. Consequently, this information can reflect the current state of the environment, such as the requirement for the abnormal indicator light to be in the off state before any operations can take place.

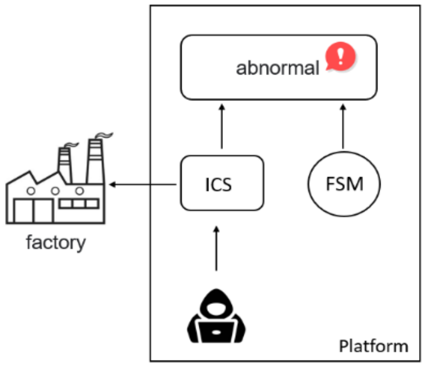

Fig. 2. Anomaly Detection Diagram

3.2. State set construction process Virtual Dam Gate Abnormal Detection testbed

The testing platform employs the Modbus communication protocol to scan the state of Programmable Logic Controllers (PLCs). The scanning interval is set at 0.1 seconds, with a 1-second pause after each scan to simulate real operating conditions. This operation is repeated infinitely to observe changes in two key variables: scan frequency and state variation. Through an infinite number of scans, we will record the results of each observation, laying the foundation for subsequent discussions to thoroughly analyze potential variations and system behaviors. The objective of this testing platform is to gain a comprehensive understanding of the abnormal detection performance of the virtual dam gate system.

```
Start:
  Setting Target PLC

While true:
  # For each iteration
  While PLC’ s Reg is not END:
    Reading Memory Address
  End Loop

  Save PLC’ s State n
  Sleep n

  If n > 1:
    Compare PLC’ s State n & n-1
  End If
End Loop
```

4. Experiment Results

This system effectively communicates the various states and operational stages of the gate through distinct light variations. When the gate is in remote monitoring mode, the remote light is illuminated, indicating normal system operation. However, if floodgate discharge is required, personnel must adhere to regulations and physically attend the site, prompting a switch to on-site mode with the power light activated.

Following the commencement of operations, the ascending light is activated if gate opening is necessary, signifying the gate's upward movement. Upon reaching a specified height while fully opening the gate, the ascending light ceases, and both the on-site and power lights illuminate, denoting complete gate opening. Upon achieving full gate openness at the base, the fully open light illuminates, the ascending light extinguishes, and the descending light activates, indicating an impending gate descent. Operation Process Diagram in Fig. 3.

However, during operation, anomalies such as short circuits or system malfunctions might occur, potentially causing gate loosening or jamming during ascent, leading to an overload condition. In such instances, the system should promptly react, for instance, by activating the corresponding warning light to alert operators to perform maintenance or emergency procedures.

In summary, this system proficiently communicates the diverse statuses and phases of gate operations through distinctive light cues. Additionally, it promptly issues warnings during abnormal situations, ensuring operational safety and manageability. Experimental results as shown in Fig .4.

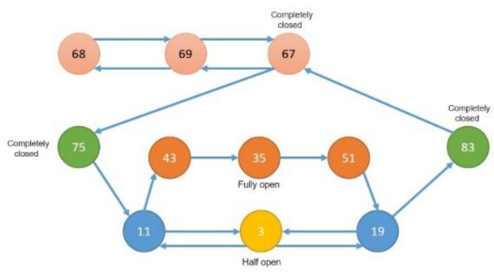

Fig. 3. Operation Process Diagram

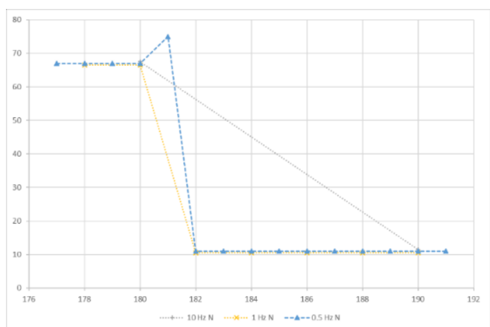

Fig. 4. Experimental results

5. Conclusion

Given the complexity of abnormal operation detection in industrial control systems (ICS), we opted to employ the Finite State Machine (FSM) method for anomaly detection in ICS operations. Through a series of tests conducted at the Dam Control System Cybersecurity Testbed established by TWISC@NCKU in Taiwan, our results demonstrated the effectiveness of our approach in improving the efficiency of identifying non-standard operational behaviors, enabling maintenance personnel to promptly recognize anomalies. This study not only constitutes a technical exploration but also emphasizes addressing potential anomalies in unique scenarios. In summary, this research provides a comprehensive and effective approach to ICS security, particularly in the realm of abnormal operation detection.

Acknowledgements

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. CNN, “Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says,” 2021. [Online]. Available: https://www.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison. [Accessed 30 Oct. 2023].
2. I. Y. Smolyakov and S. A. Belyaev, “Design of the Software Architecture for Starcraft Video Game on the Basis of Finite State Machines,” 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 28-30 Jan., 2019.
3. T. Imanto, and A. Adriansyah. “Performance analysis of profinet network in plc-based automation system,” 2nd 2020 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), Yogyakarta, Indonesia, 28-30 Sep. 2020.
4. S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, “Machine learning in network anomaly detection: A survey,” *IEEE Access*, vol. 9, pp. 152379-152396, 2021.
5. F. Farahmandi and P. Mishra, “FSM anomaly detection using formal analysis,” 2017 IEEE 35th International Conference on Computer Design (ICCD), Boston, USA, 5-8 Nov., 2017.
6. Y. Wang, Y. Wang, Z. Zhu, and Q. Wang, “Modbus TCP protocol in industrial control system Research on anomaly detection method,” 2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT), Qingdao, China, 2-4 Jul., 2021.
7. X. Li, F. Meng, and X. Zheng, “Automatic Control System of Sluice Based on PLC, MCGS and MODBUS Communication,” 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC), Guiyang, China, 23-25 Jul., 2021.
8. 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

Ms. Pei-Wen Chou

She is a postgraduate of Cloud and Network Security (CANS) Lab, Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Department of Healthcare Administration and Medical Informatics, Kaohsiung Medical University, Taiwan in 2022. Her interests encompass network security, blockchain, and industrial control systems.

Ms. Nai-Yu Chen

She was born in Taichung, Taiwan in 1998. She is acquiring the master’s degree in Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Bachelor of BioBusiness Management, National Chiayi University, Taiwan in 2021. Her interests are ICS Security, Network-Based Intrusion and PLC.

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).

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.