SUGISAKA MASANORI

Journal of Advances in Artificial Life Robotics
Vol. 4(3); June (2025), pp. 146–149
ON LINE ISSN 2435-8061; ISSN-L 2435-8061
https://alife-robotics.org/jallr.html

Research Article

Identifying Industrial Control Systems Anomalies Operation Based on Finite-State Machines

I-Hsien Liu[1], Pei-Wen Chou[1], Nai-Yu Chen[1], Jung-Shian Li[2]
[1]*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*
[2]*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

ARTICLE INFO

Article History
Received 30 November 2023
Accepted 15 May 2024

Keywords
FSM
ICS security
Dam control systems
Anomaly detection

ABSTRACT

I During 2021, a facility responsible for treating water in Florida, USA, experienced a cyberattack orchestrated by external malicious entities. These attackers sought to tamper with the levels of certain chemicals in an attempt to compromise the integrity and safety of the water supply. Recognizing the complexity of detecting abnormal operations in Industrial Control Systems (ICS), we sought to leverage the benefits of finite-state machine technology to address this challenge. To evaluate our approach, We performed a series of assessments utilizing the cybersecurity testbed for dam control systems developed by TWISC@NCKU in Taiwan. Research results show that improved detection of irregular operational behaviors, empowering maintenance staff to swiftly pinpoint anomalies.

1. Introduction

During 2021, a facility responsible for treating water in Florida, USA, encountered a malicious external attack, during which hackers sought to manipulate the levels of certain chemicals, posing a significant threat to the quality and safety of the water supply [1]. Effectively identifying abnormal operations within Industrial Control Systems (ICS) has emerged as a significant challenge.

Using FSM techniques involves carefully monitoring and analyzing the states of the system [2]. This study focuses on using Finite State Machine (FSM) techniques to detect anomalies in Industrial Control Systems (ICS), enhancing detection accuracy and efficiency. By applying FSM to monitor Programmable Logic Controller (PLC) states, the system swiftly identifies potential issues, ensuring smooth operation. The research, conducted using the TWISC@NCKU cyber-security experimental platform for dam control, validates the effectiveness of this approach. It demonstrates its ability to promptly detect deviations from normal operations, aiding personnel in recognizing abnormal conditions at minimal cost. rom normal operations, aiding personnel in recognizing abnormal conditions at minimal cost.

2. Methodology

2.1. Programmable Logic Controller

A Programmable Logic Controller (PLC) [3] automates control processes by executing stored instructions, often alongside Finite State Machines for efficient monitoring. PLC states, like "DI" and "DO" for Digital Input and Output, represent signal statuses such as switches, while "AI" and "AO" indicate Analog Input and Output, showing continuous signal states. This structure, consisting of a CPU, input, and output modules, ensures dependable performance in industrial settings by collecting data from sensors and controlling actuators.

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

2.2. Finite-State Machine

Lately, Finite State Machines (FSMs) have found widespread application across various domains, including software development [2] and machine learning [4]. FSM methodology's simplicity makes it easy to understand and design system models, which is effective for testing complex system behaviors. Its adaptability to different scales makes it a powerful tool for illustrating and managing system behaviors. In anomalous behavior detection, FSMs are used to model the typical behavior of the system by defining conditions and changes, Fig. 1. This method entails observing system activities, identifying changes in state that diverge from anticipated behavior, and issuing immediate notifications. The incorporation of FSM-driven anomalous behavior detection is extensively embraced to improve the effectiveness of modeling system behavior and detecting anomalies [5], underscoring the crucial role FSMs play in understanding behavior of the system and tackling anomaly detection challenge

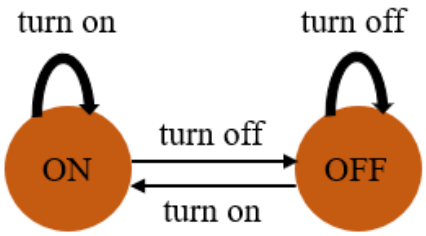

Fig. 1 Finite-State Machine State

2.3. Modbus/TCP

Modbus enables data exchange between PLCs and sensors in industrial settings, but its TCP variant poses security risks due to plaintext transmission. My research stresses the need for robust security measures to safeguard system integrity and confidentiality.

At the same time, leveraging Modbus commands to access the memory locations within PLCs [6], understanding DI and DO states via designated memory variable addresses is possible with Modbus. Real-time visibility into PLC status is facilitated through Modbus queries. It's crucial to manage Modbus communication security carefully to maintain system resilience and mitigate digital security risks in practical scenarios.

2.4. Critical infrastructure testbed

The study, carried out via a sequence of assessments conducted on the Dam Control System Cybersecurity Testbed [7] developed by TWISC@NCKU in Taiwan, established critical findings. Simulation validation confirmed the dam system's effective response to irregular circumstances, ensuring stability during real-world operations. Testing on the testbed enhances dam system security and dependability, improving their ability to handle unexpected incidents during real operations.

3. Build the PLC status set through ongoing exploration.

3.1. System architecture

To address cybersecurity concerns and detection of abnormalities challenges in critical infrastructure, this paper presents creating a test environment to simulate the system designed to detect abnormalities in dam gates Fig. 2. Every gate is regulated by a Programmable Logic Controller (PLC), featuring registers for accessing relevant commands and information. As a result, this data can accurately depict the current environmental conditions, including the necessity before commencing any operations, ensuring that the abnormal indicator light remains off.

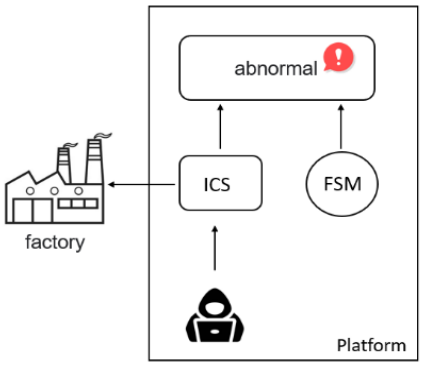

Fig. 2 Abnormality Identification Diagram

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

The testing platform utilizes the Modbus communication protocol to rack the status of Programmable Logic Controllers. It utilizes a scanning interval of 0.5 seconds, followed by a 1-second pause after each scan, mimicking real-world operational scenarios. This process repeats indefinitely to monitor alterations in two crucial factors: scanning rate and state variability. Through an endless series of scans, we will record the outcomes of each observation, providing a basis for in-depth analysis of potential variations and system behaviors. The primary objective of this testing platform is to thoroughly evaluate the virtual dam gate

system's ability to detect anomalies. The flowchart is as shown in Fig. 3.

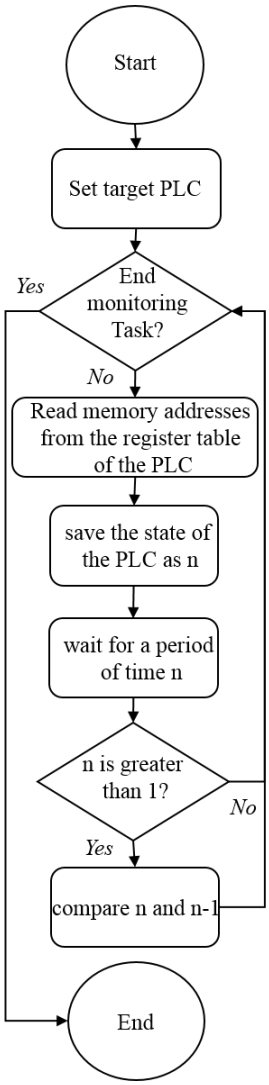

Fig. 3 Detection Process

4. Experiment Results

The system efficiently conveys gate conditions and phases through lighting changes. In remote monitoring mode, the remote indicator light signals regular operation. For flood discharge, personnel must switch to on-site mode (A to B), triggering the power indicator light. On-site operations (C) are necessary, followed by gate opening (D to E). When fully opened (F), both on-site and power indicator lights illuminate. Fully open status is indicated by the fully open light (G). As the gate descends (H to I), the descending indicator light illuminates. See Fig. 4 for the Operation Process Diagram.

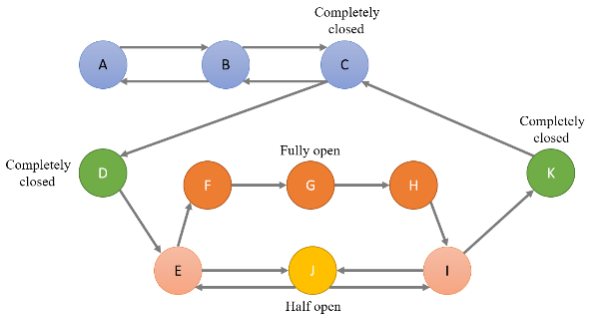

Fig. 4 Process Flow Diagram

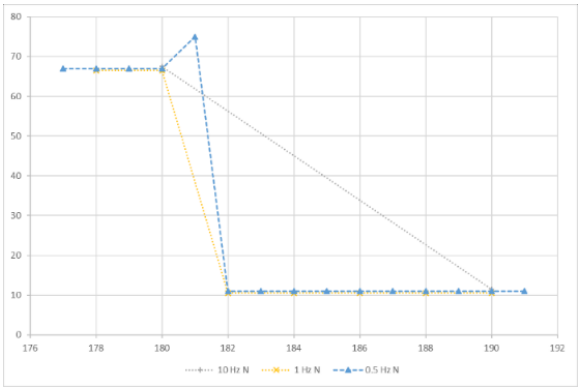

Fig. 5 Test Findings

During operation, unforeseen events like short circuits or malfunctions may cause the gate to jam, leading to overloading. Rapid response is crucial, activating warning lights to alert operators for maintenance or emergencies.

According to the experimental results shown in Fig. 5, experimentation shows that querying every 0.5 seconds uncovers unique states, highlighting potential intrusion opportunities. Thus, it's the optimal frequency for detection. The system communicates gate operations via light indicators, issuing alerts in abnormal situations, ensuring operational safety and ease of management.

5. Conclusion

We implemented Finite State Machine approach to detect abnormalities in ICS operations, addressing challenges in identifying unusual activities. Experiments conducted at TWISC@NCKU's Dam Control System Cybersecurity Testbed in Taiwan validated our

approach's effectiveness in recognizing atypical patterns, enabling swift identification by maintenance staff. Our research underscores the significance of handling abnormalities and offers a robust strategy to bolster ICS security, particularly in 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. 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.
7. 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 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).

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.

Dr. 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. His research interests include cybersecurity, cloud computing and network management.