Journal of Robotics, Networking and Artificial Life
Vol. 11(3); March (2026), pp. 196-199
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

Enhancing ICS Situational Awareness: A Passive Network Traffic Analysis Approach

I-Hsien Liu[1], Chien-Wen Tseng[2], Jung-Shian Li[3]*, Chu-Fen Li[4]

[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] *M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[3] *Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[4] *Department of Finance, National Formosa University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
*Email: ihliu@cysec.ee.ncku.edu.tw, cwtseng@cysec.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw**, *chufenli@gmail.com*
*Corresponding Author

ARTICLE INFO

Article History

Received 10 November 2024
Accepted 10 December 2025

Keywords

Industrial Control Systems
Packet Analysis
Process monitoring
Event Extraction

ABSTRACT

Monitoring the operational integrity of industrial control systems (ICS) is a fundamental concern in modern infrastructure environments. While previous studies have primarily relied on direct access to controllers' data for system observation, this study adopts a passive network-based approach to minimize potential disruptions. By analyzing communication traffic within a simulated dam control system, the research investigates how network-observable information exchanged between devices can reflect system-level operational behavior. Through detailed inspection of packet-level data, including protocol usage, register values that reveal PLC operational states, the study aims to enhance situational awareness without interfering with system operations.

© 2022 The Author. Published by Sugisaka Masanori at ALife Robotics Corporation Ltd.
This is an open access article distributed under the CC BY-NC 4.0 license
(http://creativecommons.org/licenses/by-nc/4.0/).

1. Introduction

Industrial Control Systems (ICS) play a pivotal role in operating today's infrastructure, including energy networks, manufacturing plants, and water systems. Recent incidents, such as the 2024 cyberattack on a Texas water facility [1], have highlighted the vulnerability of ICS environments and the need for continuous monitoring to safeguard operational integrity. Traditional approaches to analyzing ICS behavior often rely on direct access to Programmable Logic Controllers (PLCs) or engineering logs. However, such access is frequently restricted due to security policies, vendor constraints, or operational risks.

ICS monitoring approaches predominantly focus on single-device analysis through direct controller access or individual sensor monitoring. While effective for detecting localized failures or anomalies, these approaches face limitations when addressing system-wide issues or complex operational sequences involving multiple devices. Initial efforts have emerged to tackle these broader challenges, as demonstrated by system-wide integrity frameworks [2]. A key limitation is the absence of explicit semantics for state transitions and system-level workflows. As a result, bridging the gap between raw traffic and system-level behavioral understanding remains an open challenge.

This research addresses the gap between single-device monitoring and system-level behavioral understanding. We propose a process that analyzes packet exchanges among multiple devices in a distributed ICS and converts them into structured descriptions of operational behavior.

Extending prior work, we perform an exploratory study of the CANS RT dataset [3][4], which was generated from a simulated dam control system. The dataset reflects communication patterns commonly found in critical-infrastructure operations. By passively inspecting packet-level traffic, we identify characteristic operational flows present in the system's communication patterns. These observations form the foundation for constructing reference models that describe normal operational behavior and support the design of future anomaly-detection methods.

2. Background

2.1. Industrial Network

Industrial Control Systems (ICS) are critical for managing infrastructure such as dams, power grids, and manufacturing plants. In SCADA-based environments, Programmable Logic Controllers (PLCs) function as the control bridge from the field to supervisory systems [5], executing both digital I/O for discrete operations and analog I/O for continuous sensing and actuation. While this hierarchical architecture ensures reliable process control and device I/O traces validate local operations, system-wide dynamics such as flow regulation or load balancing emerge only from PLCs and operator coordination.

2.2. Device-Level Monitoring

Traditional ICS monitoring often relies on single-device information sources such as direct PLC access, engineering logs, or sensor data. These approaches are valuable for identifying localized failures and validating device-level correctness. However, when extended to distributed environments, they may provide only a partial view of the system. Operations such as flood discharge or load balancing embody behaviors that emerge at the system level, requiring holistic observation beyond individual device monitoring.

To complement device-level information, passive observation of network traffic offers a non-intrusive perspective on system behavior. Modbus TCP [6] as one of the most widely used industrial protocols, enables visibility into device interactions through its function codes and register exchanges. Because sensor values and actuator-related data are routinely transmitted over the network, analyzing packet-level traffic provides opportunities to observe multi-device operational activity and system-level behavioral context that are not visible from single-device monitoring alone.

2.3. System -Level Monitoring

Building on the visibility provided by Modbus TCP traffic, passive packet analysis has become an attractive approach for ICS monitoring. Unlike intrusive methods that require controller access, packet captures collected through mirror ports offer system-wide observability without disrupting operations. Prior research has shown that examining packet attributes such as function codes, register addresses, and timing intervals helps to identify device roles, understand communication patterns, and uncover malicious activities like replay or injection attacks [7]. By examining the packet-level data, we can extract Modbus features such as function codes and register values. Converting these packets into structured event sequences allows us to identify and analyze representative operational behaviors within the system.

Most existing approaches analyze packets as individual observations or emphasize statistical anomaly detection methods, such as examining the frequency distribution of function codes or variations in response times [8]. These studies provide valuable insights into device communication behaviors, and further research could build on these foundations to better represent system-level workflows and multi-device coordination. Beyond packet-level statistics, passive analysis of industrial protocols can also reveal higher-level structural information [9]. From request–response pairs, directed communication graph can be reconstructed where vertices represent endpoints and edges describe interaction direction and strength.

3. Industrial Network Traffic Analysis Approach

To effectively observe the operation of ICS, previous studies mainly monitored the PLC register address values [10]. However, this requires interaction with the system and can easily affect its operation. Therefore, this study uses network stream observation as a passive method to obtain relevant data on system operation. The traffic analyzed in this study is collected from a simulated dam gate control system.

To minimize the impact on the observed system, this study utilizes network traffic sniffing technology to reveal the operation of different components in the system by examining Modbus/TCP protocol attributes (such as function codes and register values) within the payload of each packet in the traffic, such as the operational relationship between HMI and PLC connected to a specific gate. This study uses Petri Net [11] to represent state transitions and concurrent operations. By associating transitions with events and using tokens to indicate the current system state, Petri Nets are ideal for ICS modeling, as coordinated operations across multiple devices are common in ICS. Previous studies have used HMI logs or even PLC code to construct Petri Nets or finite state models, enabling structured analysis of control behavior [12]. These works highlight the value of formal models in anomaly detection and workflow verification. Figure 1 presents the process for building an ICS operating model, outlining the steps from network traffic to event log construction and subsequent system-level analysis.

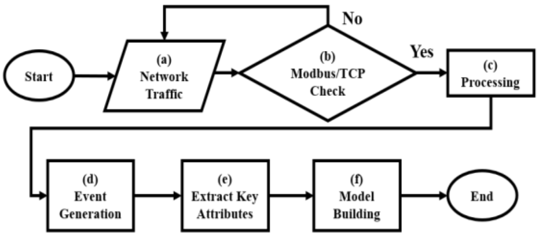

Figure 1. The Building ICS Operating Model Process

The following details the process of establishing an ICS operational model. The analysis begins by capturing raw network traffic in pcapng format through a mirrored port, as shown in Figure 1(a). In Figure 1(b), Modbus/TCP packets are filtered from the capture, and Figure 1(c) decodes protocol fields, including timestamps, IP addresses, function codes, and register values. These decoded packet records form the basis for event construction. The filtered Modbus/TCP packets are transformed into discrete events shown in Figure 1(d). Subsequently, as indicated in Figure 1(e), essential attributes such as DI bitfields and register values are extracted to enrich event semantics. Each event is annotated with a timestamp, assigned to a PLC case according to its IP address, and labeled with an activity representing the underlying control operation inferred from the packet. Finally, with these attributes, the event log becomes suitable for subsequent process discovery, enabling the construction to build an ICS operating model via a Petri net, as shown in Figure 1(f).

4. Experiment

The experimental setup emulates a dam gate control system that closely reflects real industrial operations. In this environment, the PLCs execute control logic, operate actuators, and update sensor readings, while the HMI provides real-time visualization and enables supervisory commands. All devices communicate over an industrial Ethernet network using Modbus/TCP for periodic polling and control exchange. Network traffic is passively collected through a mirrored switch port and serves as the dataset for analysis. Based on this data, the study builds an operational model. The system architecture is shown in Figure 2.

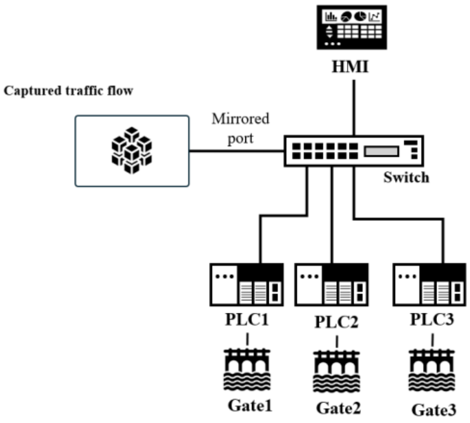

Figure 2. ICS's Passive Data Collection Architecture

As shown in Figure 1(a) and Figure 1(b), the captured packets are examined to obtain the Modbus/TCP fields relevant to the PLC controllers. Using tshark in Figure 1(c), the Modbus/TCP traffic is analyzed to obtain the digital-input values embedded in the register fields. The digital-input (DI) registers are then interpreted at the bit level to derive discrete status signals. These extracted fields collectively provide visibility into both the logical behavior of the controllers and the physical conditions of the system during operation.

Based on the extracted information, Modbus/TCP response is converted into an event as illustrated in Figure 1(d) and Figure 1(e). Each event is defined by three essential attributes: a timestamp, an activity label derived from DI state changes, and a case identifier corresponding to the PLC's IP address. These structured events collectively form the event log used for subsequent analysis. Using the representative operational sequences contained in this event log, a Petri net was discovered using PM4Py's implementation of the Inductive Miner in Figure 1(f).

To illustrate how the mined Petri Net reflects the actual operational behavior of the dam-gate control system, Figure 3 presents three representative segments derived from the event log. These segments come from the activity built from the network traffic in the CANS RT dataset [3][4], which captures the system's operational behavior. From this dataset, the commonly observed opening and closing sequences were taken for illustration in Figure 3.

This study analyzed network traffic from multiple gate monitoring points and a series of gate operations. The circular icons in the figures are called "Places" and are used to represent intermediate states between events. The white rectangular icons are called "Transitions," representing changes in DI combinations; for example, "DI3_OFF" indicates that the state of DI 3 has changed to "OFF." Details are as follows: Figure 3(a) shows the combined operation trajectory of all controllers. It demonstrates how DI changes from different PLCs occur simultaneously in the discovered model. The black transitions inserted by the sensing excavator represent routing structures, such as branches and concurrency, forming a model that shows multiple possible paths and reflects the multi-gate operation of the system. The two transitions in Figure 3(b) and Figure 3(c) represent the gate opening and closing operations, respectively. In Figure 3(b), the first transition indicates that the gate starts to open from a fully closed state, and the second transition indicates that the opening operation ends. Figure 3(c) shows the gate closing operation mode. The first transition indicates that the gate begins to move downwards, and the second transition indicates that the gate is fully closed. These results demonstrate how the system's operational behavior is reflected in the discovered model.

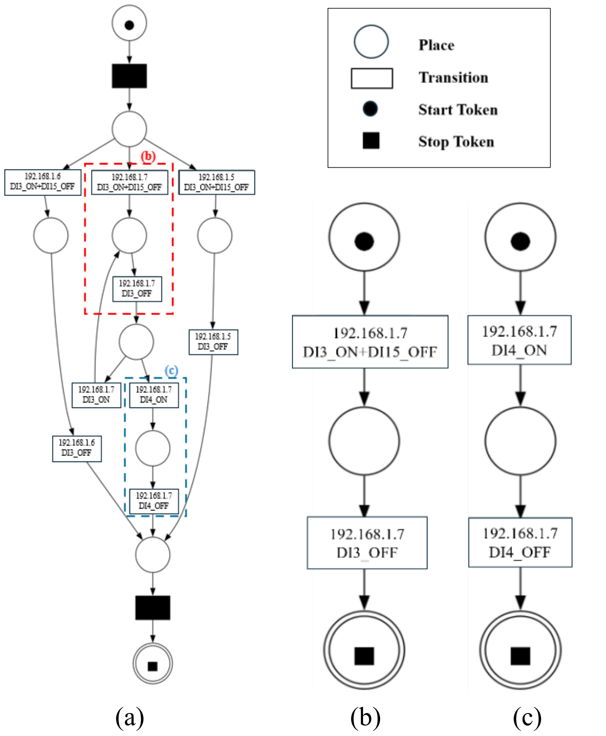

Figure 3. The Operation Models via Petri Net

5. Conclusion

This study introduces a comprehensive process designed to enhance Industrial Control System (ICS) situational awareness. The process covers the key steps from passively capturing network traffic to producing structured event logs. By applying this methodology to ICS environments, it shows that an operation model can be derived from the captured traffic. In this context, the operation petri net model serves as the main result of the analysis process and is used to describe the system's underlying behavioral logic.

Acknowledgements

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under Grant No. 114-2634-F-006-001-MBK and 114-2222-E-006-005-.

References

1. Associated Press, "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow," 2024 [Online]. Available: https://www.securityweek.com/rural-texas-towns-report-cyberattacks-that-caused-one-water-system-to-overflow/. [Accessed 15 Oct. 2024].
2. S. Adepu, F. Brasser, L. Garcia, M. Rodler, L. Davi, A.-R. Sadeghi, and S. Zonouz, "Control behavior integrity for distributed cyber-physical systems," ACM/IEEE ICCPS 2020, Sydney, Australia, 21-25 Apr., 2020.
3. CANS, "CANS RT," 2024. [Online]. Available: https://www.cans.ee.ncku.edu.tw/research/cansrt. [Accessed 15 Oct. 2024]
4. 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, 4(2) , pp. 63-66, 2023.
5. D. Upadhyay, S. Ghosh, H. Ohno, M. Zaman, and S. Sampalli, "Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator," International Journal of Critical Infrastructure Protection, 47, p. 100705, 2024.
6. V. Machaka, S. Figueroa-Lorenzo, S. Arrizabalaga, B. Elduayen-Echave, and J. Hernantes, "Assessing the impact of Modbus/TCP protocol attacks on critical infrastructure: WWTP case study," Computers and Electrical Engineering, 126, p. 110485, 2025.
7. L. Rajesh and P. Satyanarayana, "Detection and blocking of replay, false command, and false access injection commands in SCADA systems with Modbus protocol," Security and Communication Networks, 2021, p. 8887666, 2021.
8. I. Burgetová, P. Matoušek and O. Ryšavý, "Anomaly Detection of ICS Communication Using Statistical Models," 2021 17th International Conference on Network and Service Management (CNSM), Izmir, Turkey, 25-29 Oct., 2021.
9. A. J. Akande, C. Fidge, and E. Foo, "Component modeling for SCADA network mapping," 2015 38th Australasian Computer Science Conference (ACSC), Sydney, Australia, 27-30 Jan. 2015.
10. P.-W. Chou, N.-Y. Chen, J.-S. Li, I-H. Liu, "Detecting abnormal operations in ICS using finite-state machines", ICAROB 2024, Oita, Japan, 22-25 Feb., 2004.
11. L. Chen, Y. He, B. Zhang, C. Xia, Y. Qiu, and Z. Yu, "Petri Net-Based Information Enhancement for Quality Monitoring in the Cigarette Manufacturing Process," Measurement, 255, p. 117999, 2025.
12. D. Myers, S. Suriadi, K. Radke, and E. Foo, "Anomaly detection for industrial control systems using process mining," Computers & Security, 78, pp. 103-125, 2018.

Authors Introduction

Prof. I-Hsien Liu

He serves as an assistant professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He earned a Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests include cybersecurity, OT security, and wired and wireless communication.

Ms. Chien-Wen Tseng

She is pursuing her M.S. degree in the Cyber-Security Intelligence Program at National Cheng Kung University, Taiwan. Her current research focuses on passive traffic analysis and anomaly detection in ICS environments

Prof. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering at National Cheng Kung University, Taiwan. He obtained his Ph.D. in Computer Science from the Technical University of Berlin, Germany, in 1999. His research interests include cybersecurity, cloud computing, and network management. He is currently engaged in funded research projects related to cybersecurity and critical infrastructure protection

Prof. Chu-Fen Li

She serves as an Associate Professor in Finance at National Formosa University, Taiwan. She received the Ph.D. degree in information management, finance, and banking from Europa-Universität Viadrina Frankfurt, Germany. Her current research focuses on intelligence finance, e-commerce security, and IoT security management. Her work has appeared in several international refereed journals, including the European Journal of Operational Research, Journal of Systems and Software, and International Journal of Information and Management Sciences, among others.