A Short Note on Explainable Intrusion Detection for Water Distribution Systems

Jhon K

January 4, 2026

Abstract

Industrial Control Systems (ICS) used in critical infrastructure remain vulnerable to cyber-physical attacks. This short note summarizes an explainable anomaly detection approach for water distribution systems and highlights why explainability is operationally useful for responders and operators.

1 Background

Water distribution systems are a core component of critical infrastructure. Detecting attacks quickly is important, but operators also need actionable signals: which sensors/actuators are implicated and why an alert occurred.

2 Summary of an Explainable WADI-Based Approach

A recent case study proposes an LSTM autoencoder trained on benign windows of WADI telemetry and evaluates anomaly detection with ROC-AUC, while adding explainability via per-feature reconstruction-error changes (e.g., ΔMSE) to identify the tags most responsible for anomalous windows [1].

3 Why Explainability Matters for ICS Operations

Explainability can reduce time-to-triage, support incident scoping, and improve trust in detection systems by connecting alarms to specific process variables.

4 Conclusion

Explainable anomaly detection can make IDS outputs more usable for real-world ICS teams, especially in safety-critical environments like water distribution.

References

[1] S. Shahid, "Xai for intrusion detection in water distribution systems: A case study using the wadi dataset," TechRxiv, Nov. 2025, preprint. [Online]. Available: https://doi.org/10.36227/techrxiv.176404012.26834913/v1