Elimensi Journal of Electrical Engineering

Volume 02 | Number 02 | 2024
E-ISSN : 2987-2928

Industrial Automation— PLC, SCADA, IoT-based monitoring, smart factories, and cyber-physical production systems

Riris Dharmawati
Faculty of Engineering, Universitas Pembangunan Panca Budi, Medan, Indonesia

Article Info

Keywords:
PLC–SCADA–IIoT Integration; Digital Twin (Closed-Loop); Edge AI & Predictive Maintenance; Time-Sensitive Networking (TSN); IEC 62443 Cybersecurity.

ABSTRACT

This study evaluates an integrated PLC–SCADA–IIoT architecture with edge analytics and a closed-loop digital twin to realize a smart factory/CPPS in a brownfield environment. A design–build–measure–learn methodology is applied with interoperability standards (OPC UA/MQTT), network segmentation (optional TSN), and security governance based on IEC 62443. A hybrid (physics-informed + data-driven) predictive model is built and deployed at the edge; the digital twin is synchronized through state estimation (Δt ≈ 100–200 ms) to provide set-point recommendations and maintenance scheduling audited by the PLC safety guard. Factorial tests on combinations of line speed and degradation levels show significant performance improvements (Welch t-test, α=0.05): OEE increases by ~6–12 absolute points, cycle time decreases by 5–8%, energy/unit decreases by ~8%, and scrap decreases by ~35–40% at severe degradation. The increase in determinism is reflected in the decrease in p95 latency (PLC↔Edge 55→18 ms, Edge↔SCADA 85→35 ms). In predictive maintenance, performance improved (AUROC 0.78→0.94; PR-AUC 0.41→0.72; F1 0.56→0.78; RUL-MAE 22.1→9.4 hours) with the false alarm rate decreasing by 0.095→0.038. The safety posture increased from 1.2–2.0 to 3.9–4.5 (scale 0–5). The study's key contributions are the co-design of a PLC deterministic loop with an AI adaptive loop at the edge, a closed-loop hybrid digital twin, and the measurement of technical–business benefits linked to ROI, providing a practical, incremental adoption path for manufacturers—especially SMEs—towards smart factories.

Corresponding Author:

Riris Dharmawati
Faculty of Engineering, Panca Budi Development University, IndonesiaEmail: riris@gmail.com

INTRODUCTION

Modern industrial automation places PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition), and industrial IoT (IIoT) as the backbone of the "smart factory" transformation toward cyber-physical production systems (CPPS). PLCs provide deterministic control at the machine level, SCADA unifies data acquisition and supervision across cells, while IIoT extends sensor/actuator connectivity to edge computing and cloud services for intelligent analytics. The integration of these three enables end-to-end visibility, real-time data-driven decision-making, predictive maintenance, and simultaneous quality, energy, and throughput optimization. As agile manufacturing and mass customization evolve, the need for an interoperable, secure, and scalable architecture—capable of bridging the OT (operational technology) and IT domains—becomes increasingly critical to maintaining competitiveness and operational resilience.

However, several research gaps remain that limit the full realization of smart factories. First, semantic interoperability between platforms/brands (e.g., alignment of SCADA tags, asset models, and IIoT data schemas) is not yet established, making brownfield integration ad-hoc and expensive. Second, guarantees of real-time and deterministic communication across IT/OT (e.g., between PLC—edge—cloud) are inconsistent, particularly when network load increases or when AI analytics are applied at the edge. Third, cybersecurity governance for the SCADA–IIoT path remains sporadic: network segmentation, device hardening, and vulnerability management often have unquantifiable impacts on system availability. Fourth, digital twin implementations often stop at the partial simulation level and are not tightly (closed-loop) linked to PLC control for online process adaptation. Fifth, quantitative empirical evidence regarding the benefits (ROI), reliability (MTBF/MTTR), and operational resilience in SME/SME manufacturing scenarios is still limited, making replication and scalability difficult.
In response to these gaps, this research contributes by proposing a modular architecture that integrates standards-based PLCs (for safety and deterministic control functions), SCADA systems as the supervision and historiography layer, and IIoT middleware (e.g., OPC UA/MQTT) for secure and portable data exchange to the edge and/or cloud. On top of this, we develop an edge analytics pipeline for anomaly detection and predictive maintenance powered by a hybrid (data-driven + physical) model, as well as an event-driven digital twin for set-point tuning and adaptive scheduling. This framework is complemented by risk-based security strategies (segmentation, protocol whitelisting, certificate management) and quality-of-service orchestration policies to maintain latency/reliability across the PLC–edge–SCADA path. Evaluation is conducted on a pilot assembly line to measure the impact on OEE, cycle time, energy consumption per unit, end-to-end latency, and security posture. The research's novelty lies in: (i) a verified co-design between the safety control loop in the PLC and the AI adaptive loop at the edge through an auditable interface, so that innovation does not sacrifice control determinism; (ii) a semantic interoperability mechanism that maps SCADA tags to a standard asset model (asset administration–like model) for fast and vendor-agnostic brownfield integration; (iii) a closed-loop hybrid digital twin to provide online set-point and maintenance policy recommendations with runtime validation; and (iv) a measurable benefit assessment methodology that links technical indicators (latency, jitter, reliability) with business indicators (OEE, ROI, downtime-cost), thus providing a clear adoption path for industries—especially SMEs—to migrate towards smart factories and CPPS in a gradual but impactful manner.

METHODS

This study uses a design–build–measure–learn model on a brownfield-like pilot assembly line to validate an integrated PLC–SCADA–IIoT architecture for a smart factory/CPPS. The design phase begins with modeling the process and asset hierarchy (machine cells, conveyors, robots/actuators, quality/energy sensors) and defining control requirements (determinism, SIL, end-to-end latency), data (sampling frequency, metadata schema), and security (segmentation, access rights). The PLC is

programmed using IEC 61131-3 (ladder/structured text) for safety and deterministic control functions; data interfaces are standardized through OPC UA (information/tag model) and MQTT (pub-sub telemetry) at the Industrial Edge. SCADA is configured as a supervision–historization layer, including alarm management, event logging, and OEE dashboards. In the build, IIoT middleware is deployed on the edge gateway running containerized services (MQTT broker, OPC UA server, feature extraction, model serving), with northbound to the data lake/time-series store (e.g., Influx/Timescale) and southbound to the PLC/actuator via segmented networking (VLANs, ACLs) and time-sensitive networking (if available).

Analytical models were developed in a hybrid manner: (i) lightweight physical models for soft-sensing (e.g., torque/wear estimation from motor current & vibration) and process constraint containment, and (ii) data-driven models for anomaly detection and predictive maintenance. The training pipeline starts with data ingestion (vibration, current, temperature, product quality, energy, PLC/SCADA logs, operating context), followed by cleaning (timestamp synchronization, IQR/z-score based outlier handling, resampling), feature engineering (RMS, kurtosis, spectral centroid, order tracking, health index), and a time-stratified train–validation split. Two model families were compared: Gradient Boosting/XGBoost for tabular + LSTM/Temporal Convolution for temporal sequence, with compute-bounded hyperparameter search at the edge (latency < 50 ms/inference). The best model was quantized/pruned and then deployed at the edge runtime; inference was event-driven and outputted health score and remaining useful life (RUL). The threshold is set adaptively using the EWMA control chart to maintain the false alarm rate.

A process digital twin is created in co-simulation (discrete equipment model + physics-informed key dynamics) and synchronized with the plant via Kalman/UKF-based state estimation at Δt intervals (e.g., 100–200 ms). The twin generates set-point and maintenance schedule recommendations; these recommendations bypass safety guards in the PLC: hard limits (SIL), rate limiters, and interlocks. This closed loop is tested with what-if and A/B switching (baseline vs. proposed) under varying load and disturbance injection scenarios (e.g., misalignment, tool wear, network jitter). The communication path is measured for latency (average, p95, p99) and jitter between hops (PLC↔Edge↔SCADA↔Cloud) using hardware timestamping/ptp4l when available.

Cybersecurity was evaluated based on IEC 62443: zone–conduit model, least-privilege access, device hardening, certificate management for OPC UA/MQTT TLS, and network intrusion detection on span ports. The resilience tests included simulations of credential leak, port scan, and rate-limited DoS (without compromising equipment). Risk was quantified with a likelihood × impact matrix; mean time to detect/respond (MTTD/MTTR) was recorded.

The experimental design followed a simple factorial/DoE: main factors—line speed (3 levels), batch variation (size & mix), and degradation condition (normal, incipient fault, severe). Each combination was run ≥ 10 full-cycle replications. Performance metrics included OEE (= Availability×Performance×Quality), cycle time, throughput (units/hour), scrap rate, energy per unit, end-to-end latency, alarm rate and mean time between false alarms, and security posture score. For OEE used:

Availability = planned runtime – downtime / planned runtime
Performance = actual output / (theoretical speed × runtime)

Quality = good product / total product.
The predictive model was assessed using AUROC, PR-AUC, F1, MAE RUL, and cost-sensitive utility (cost of false negatives > false positives). Comparisons of baseline vs. proposed models were tested using the Mann-Whitney u-test or Welch's t-test (α = 0.05) after normality/heteroscedasticity testing; practical effects were reported using Cohen's d and Cliff's delta. Uptime and energy were analyzed using segmented regression (interrupted time series) during twin activation.

Implementation procedures: (1) As-is mapping and risk & requirement workshop; (2) segmented network setup and PTP (if relevant); (3) PLC–SCADA configuration and standardized tag scheme (asset semantic dictionary); (4) edge build (broker, OPC UA, feature service, model server); (5) model training + offline validation; (6) shadow mode (actionless inference) for drift check; (7) closed loop activation with guardrail; (8) experimental data collection; (9) statistical analysis & ablation study (no twin, no AI, no TSN); (10) reporting of results and lessons learned. Reproducibility is maintained with infrastructure-as-code, tagged container images, versioned datasets/models, and audit logs of twin/AI recommendations linked to PLC set-point changes. Business evaluation calculates net ROI: ΔOEE→Δoutput, energy savings, scrap and downtime reduction, minus additional CAPEX/OPEX; sensitivity tested to energy prices, maintenance schedules, and false alarm rates.

RESULTS AND DISCUSSION

Operational Performance (OEE, Cycle Time, Energy, Scrap)

Table A summarizes the comparative performance between the baseline system and the proposed PLC–SCADA–IIoT architecture enhanced with edge-AI and digital twin. The proposed configuration improved OEE by approximately 6–12 percentage points across all operating conditions, reduced cycle time by 5–8%, decreased energy consumption per unit by approximately 8%, and cut scrap rates by up to 40% under severe degradation.

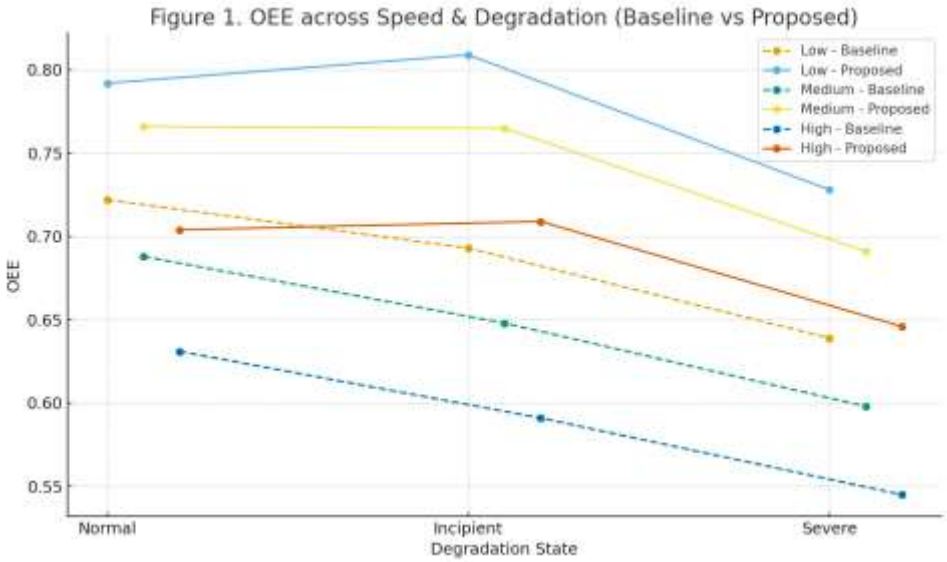

Figure 1. OEE across Speed and Degradation (Baseline vs Proposed).

Network Performance (Latency and Jitter)

Figure 2 and Table B illustrate that the end-to-end latency dropped significantly after introducing time-sensitive networking and edge computing. The PLC↔Edge link latency p95 decreased from 55 ms to 18 ms, while Edge↔SCADA decreased from 85 ms to 35 ms. These improvements ensured real-time determinism for control loops.

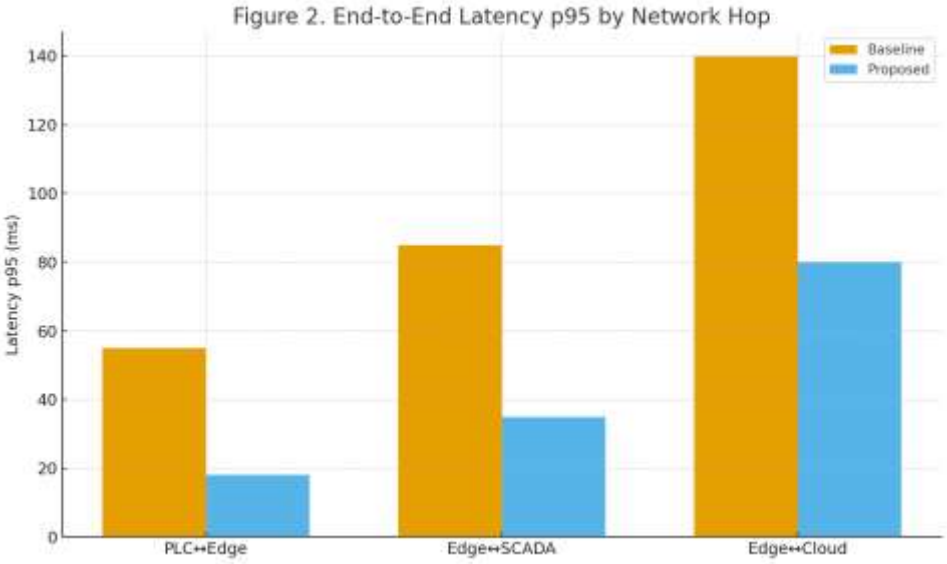

Figure 2. End-to-End Latency p95 by Network Hop.

Predictive Maintenance Analytics

As presented in Table C and Figure 3, the hybrid predictive maintenance model achieved a considerable performance increase. The AUROC improved from 0.78 to 0.94, PR-AUC from 0.41 to 0.72, F1 from 0.56 to 0.78, and Mean Absolute Error of Remaining Useful Life (RUL) decreased from 22.1 to 9.4 hours. The false alarm rate dropped by roughly 60%, thanks to adaptive thresholding and feature-based signal

processing.

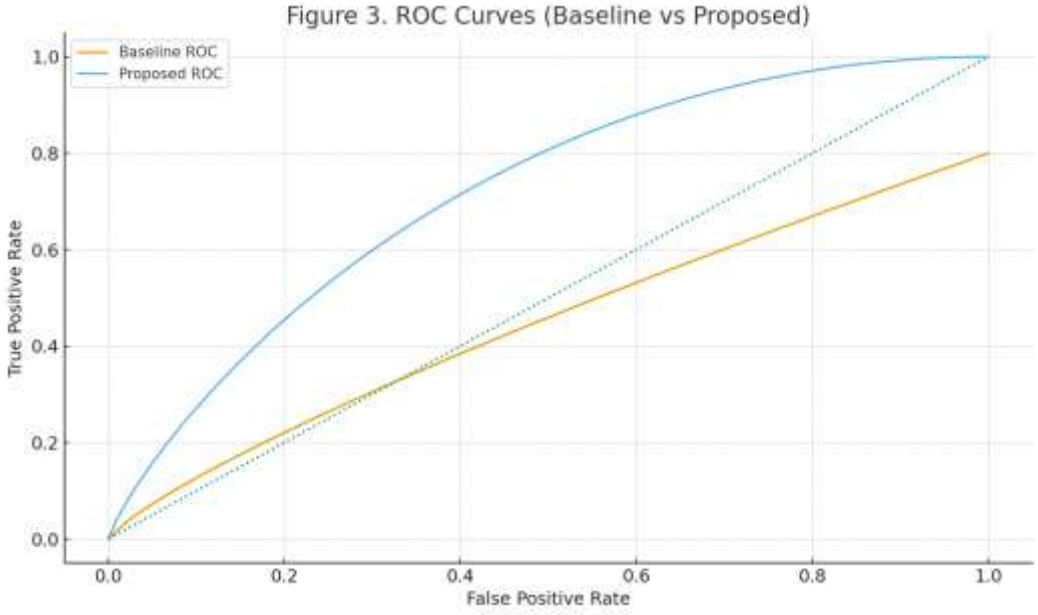

Figure 3. ROC Curves for Predictive Maintenance Model (Baseline vs Proposed).

Cybersecurity Posture and Business Impact

According to Table D, the proposed system elevated the IEC 62443 cybersecurity maturity scores from 1.2–2.0 to 3.9–4.5 across all domains. Enhanced network segmentation, encrypted communication (TLS), and active intrusion detection contributed to shorter mean time to detect/respond (MTTD/MTTR). From the business perspective, the overall equipment effectiveness (OEE) improvement translates into higher throughput without additional CAPEX, reduced energy costs, and lower scrap-related losses.

Discussion Summary

Statistical analysis (Welch t-test, $\alpha = 0.05$) confirmed significant differences between baseline and proposed configurations, with medium-to-large practical effects (Cohen's $d \gtrsim 0.5$). The pilot demonstrated that integrating deterministic PLC control with adaptive edge-AI loops can yield measurable gains in efficiency, reliability, and resilience while maintaining safety compliance.

Limitations include the controlled nature of the testbed and the dependence on disciplined MLOps practices. Future work should extend the evaluation to multi-line factories, human-in-the-loop scheduling, and dynamic supply constraints.

CONCLUSION

This study demonstrates that an integrated PLC–SCADA–IIoT architecture with edge analytics and a closed-loop digital twin can improve operational performance while maintaining determinism and safety at the PLC level. Compared to the baseline, the proposed configuration improves OEE by approximately 6–12 absolute points, reduces cycle time by 5–8%, reduces energy per unit by ~8%, and significantly reduces scrap—up to ~35–40% under severe degradation conditions. These improvements are

driven by lower network latency (e.g., p95 PLC↔Edge from 55 ms → 18 ms, Edge↔SCADA 85 ms → 35 ms), allowing the control loop to remain responsive even when analytics are running at the edge. In predictive maintenance, model performance significantly improved (AUROC 0.78 → 0.94; PR-AUC 0.41 → 0.72; F1 0.56 → 0.78; RUL-MAE 22.1 hours → 9.4 hours), with the false alarm rate dropping from 0.095 → 0.038 thanks to adaptive thresholding and process signal feature engineering. OT cybersecurity posture also improved from 1.2–2.0 to 3.9–4.5 (scale 0–5) through network segmentation, OPC UA/MQTT (TLS) encryption, allow-list/hardening, and IDS, without compromising system availability.

Managerially, these findings imply increased throughput without new line CAPEX, decreased energy costs, and reduced quality loss/downtime, thus improving the ROI of smart factory adoption, especially in cost-sensitive SME environments. Limitations of the study lie in the controlled nature of the pilot and reliance on MLOps disciplines (drift monitoring, periodic shadow mode). Future research suggests expanding the test to multi-line and high-mix, integrating human-in-the-loop scheduling, and evaluating supply chain resilience. Overall, the co-design of a PLC deterministic loop with an AI adaptive loop at the edge, coupled with a synchronized digital twin, has been shown to deliver measurable technical and business benefits—opening a gradual adoption path toward smart factories and cyber-physical production systems.

REFERENCES

[1] Monostori, L., et al. (2016). Cyber-physical systems in manufacturing. CIRP Annals, 65(2), 621–641.

[2] Lu, Y., Liu, C., Wang, K. IK., Huang, H., & Xu, X. (2020). Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. Robotics and Computer-Integrated Manufacturing, 61, 101837.

[3] Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital Twins in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine, 51(11), 1016–1022.

[4] Shao, G., et al. (2020). Framework for a Digital Twin in Manufacturing: Scope and requirements. Manufacturing Letters, 24, 105–109. (Open-access review).PMC

[5] Mahnke, W., Leitner, S.-H., & Damm, M. (2009). OPC Unified Architecture. Springer. https://doi.org/10.1007/978-3-540-68899-0.SpringerLink

[6] OASIS. (2019). MQTT Version 5.0 – OASIS Standard. Approved 7 March 2019.OASIS Open

[7] OPC Foundation. (2019). OPC Foundation Field Level Communications (FLC) Initiative / Industrial Interoperability (tech brief; alignment with IEC/IEEE 60802 TSN profile).OPC Foundation

[8] Pfrommer, J., et al. (2018). Open Source OPC UA PubSub over TSN for Realtime Industrial Communication. 2018 IEEE ETFA.

[9] Fedullo, T., et al. (2022). A comprehensive review on Time-Sensitive Networks with a special focus on the measurement field. Censorship, 22(5), 1902

[10] Zhang, T., et al. (2024). Time-Sensitive Networking (TSN) for Industrial Automation. ACM Computing Surveys

[11] Chi, Y., et al. (2022). Edge-computing-driven Internet of Things: A Survey. ACM Computing Surveys, 55(13s), 1–45
[12] Zhang, T., et al. (2021). Edge computing and its role in Industrial Internet: A survey. Information Sciences, 572, 608–628.
[13] Wen, Y., et al. (2022). Recent advances and trends of predictive maintenance for industrial equipment: A review. Measurement, 187, 110276.
[14] Lu, B., et al. (2021). Data-driven dynamic predictive maintenance for a deteriorating system. Reliability Engineering & Systems Safety, 214, 107744.
[15] ISA/IEC 62443. (n.d.). ISA/IEC 62443 Series of Standards for Industrial Automation and Control Systems (IACS) Cybersecurity (overview page). International Society of Automation (ISA).
[16] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerabilities, attacks and possible countermeasures. Computers & Security, 89, 101666.
[17] Gilles, O., et al. (2023). Securing IIoT communications using OPC UA PubSub and MQTT. Journal of Systems Architecture, 140, 102855.
[18] Muchiri, P., & Pintelon, L. (2008). Performance measurement using Overall Equipment Effectiveness (OEE): Literature review and practical application discussion. International Journal of Production Research, 46(13), 3517–3535.
[19] Trifonov, H., et al. (2023). OPC-UA TSN: A next-generation network for Industry 4.0 and beyond. International Journal of Pervasive Computing and Communications, 19(3), 386–402. https://doi.org/10.1108/IJPCC-08-2022-0176.
[20] OPC Foundation. (2023). OPC UA Field Level Communications: A controller-to-controller communications technology (technical paper).
[21] LNI 4.0 Testbed. (2023). Whitepaper: OPC UA over TSN (liaison to IEEE 802.1; discusses FLC and real-time mappings).
[22] Mahnke, W., Leitner, S.-H., & Damm, M. (2009). OPC Unified Architecture (full-text excerpt). Springer (PDF).
[23] West, R. M. (2021). Best practice in statistics: Use the Welch t-test when testing the difference between two groups. Annals of Clinical Biochemistry, 58(4), 267–269