VOL. 10 NO. 5,
NOVEMBER, 2025
E-ISSN 3027-1339
P-ISSN 3026-8257

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Systematic, Evaluation and Diversity Engr. (JSEDE)

A Safety-Critical Edge Intelligence Architecture for Real-Time Fault Diagnosis and Predictive Maintenance in Electronic Systems

John O. Alabi (FNSE)[1]; Gospel Effiong Isangadighi[2]; & Oluwaseun Ade Makinde[3]

[1]Transmission Company of Nigeria, Plot 14 Zambezi Crescent, Maitama, Abuja. [2]Health, Environment, Safety, and Security (HESS) Unit, Department of Environmental Management and Toxicology, Federal University of Petroleum Resources, Effurun, Warri-Port Harcourt Express Way, East-West Road, Delta State, Nigeria. [3]Intelligent Systems and Edge Computing for Electronic Systems, Department of Computer Science, Lagos State University

DOI: https://doi.org/10.70382/ajsede.v10i5.021

Abstract

The safety-critical electronic systems installed in power grids, (industrial) automation, transport, and medical technologies require not only intelligent but also deterministic, explainable, and safety-conformant maintenance solutions. The traditional reactive, preventive, and cloud-centric predictive maintenance methods remain limited by reliance on networks, communication latency, and insufficiently guaranteed runtime safety. The objective of this study is thus to design and test a safety-related edge-wise smart framework that provides real-time fault diagnosis and predictive preventive maintenance at the system edge. A safety-focused design-implementation-evaluation approach was adopted, combining hierarchical edge computing with lightweight deep-learning-based fault diagnosis, hierarchical-logic probabilistic reasoning, and explicit safety techniques such as redundancy, confidence validation, and fail-safe logic control. Several exceptional results were obtained by means of experimental testing in simplicity of fault injection under controlled conditions and high degradation limits: the proposed architecture demonstrated a high fault diagnosis rate of nearly 98%, deterministic end-to-end delays of around 2,308

milliseconds, a low false alarm (2.1) and missed detection (1.3) rates, and high availability (99.94) in operation under fault and unpredictabilities. These findings indicate that edge-deployed intelligence can meet the analytical performance, real-time performance, and functional safety needs simultaneously- something that has not been realised by many centralised approaches. The assertion is that safety-critical edge intelligence is a reflective, scalable paradigm for reliable electronic systems, and it is suggested that future systems adopt edge-centric, confidence-conscious intelligence and that functional safety criteria evolve to explicitly account for the practice of deploying artificial intelligence at the edge.

Keywords: Safety-critical systems, Edge intelligence, Fault diagnosis, Predictive maintenance, Real-time analytics, Functional safety, Reliability engineering

Introduction

The rapid growth of advanced electronics in safety-sensitive industries such as power generation and distribution, industrial controls, transport, aviation, and medical technologies has placed increased demands on their reliable, uninterrupted operation in society. Such systems have the potential to cascade out of control in the event of even a minor malfunction, resulting in substantial economic losses, ecosystem destruction, or loss of human life. As a result, high levels of operational safety, reliability, and availability have become key engineering priorities. Fault diagnostics and maintenance plans are no longer supplementary features of the system design and lifecycle control but integral components [1, 2]. The maintenance of electronic systems has traditionally been conducted in a reactive mode, i.e., corrective measures are implemented once a failure is detected, or preventive measures are performed according to a schedule. Although preventive maintenance minimises the number of unforeseen breakdowns, it often necessitates unnecessary component changes and higher operational expenses. More importantly, both methods are limited in their ability to pre-detect latent failures and gradual degradation processes that typify current electronic parts and subsystems. A large portion of these restrictions has led to increased attention to predictive maintenance, in which condition-monitoring data and advanced analytics are used to predict failures and prevent them.

Recent advances in artificial intelligence (AI) and machine learning (ML) have enabled powerful, data-driven approaches to fault diagnosis and remaining useful life (RUL) prediction in electronic systems. These approaches can also identify complex patterns in sensor data, including subtle performance and degradation patterns that are challenging to model with rule-based and physics-only models [3]. The best thing is that most currently available predictive maintenance systems are cloud-centred, and raw or processed data are sent to collocated servers for analysis. Although effective in non-critical environments, they introduce

communication latency, reliance on network availability, cybersecurity vulnerabilities, and difficulties meeting real-time operational requirements [4,5,6]. These constraints are especially troublesome for safety-related electronic systems, in which diagnostic decision-making must operate within hard, deterministic time constraints. Network congestion or cloud service unavailability can lead to delays, rendering fault detection ineffective and compromising safety assurance. Moreover, the regulatory and certification processes in safety-relevant areas necessitate determinism, reliability, and explainability, which are difficult to establish when decision-making has been delegated to opaque, remotely hosted AI services [7]. This has led to a greater appreciation of the need to deploy intelligence closer to the physical system, where decisions are timely and situationally aware.

Edge computing has been proposed as a promising paradigm to address these challenges by moving computation and analytics from the central cloud to the network edge, near data sources and actuators. When used with lightweight AI models, edge intelligence enables real-time fault diagnosis and maintenance prediction, reducing latency, lowering bandwidth usage, and revealing sensitive operational information [8]. Despite these benefits, the deployment of AI at the edge of safety-critical applications introduces new challenges, including limited computational resources, robustness under fault conditions, and safety-focused architectural design requirements. Most current research on edge-based fault diagnosis focuses on performance and energy efficiency, whereas formal safety mechanisms (redundancy, fail-safe behaviour, confidence validation, and explainable decision-making) are studied only to a limited extent [9]. This indicates a critical gap in the literature on architectures that integrate edge intelligence with safety assurance principles tailored to electronic systems in real-time, high-risk settings. To address this gap, the proposed study presents a Safety-Critical Edge Intelligence Architecture for real-time fault diagnosis and predictive maintenance of electronic systems. The approach is suggested to include hierarchical edge-smart hybrid artificial intelligence and probabilistic reasoning models, as well as safeguards embedded in the scheme, to provide dependable, interpretable, and low-latency maintenance intelligence. By harmonising edge AI implementation with the high-fidelity demands of safety-critical operations, the work will contribute to a practical, scalable framework that enhances system reliability and underpins future certification and industrial adoption.

Methodologies

This paper primarily follows a safety-oriented, design-implementation-evaluation approach to develop an edge intelligence architecture for real-time fault diagnostics and predictive maintenance in safety-critical electronic systems. Its methodology is designed such that it can be determined, resilient to uncertainty, can be explained, and be shown as safe, as well as can be deployed on resource-constrained edge devices. All the methodological stages are clearly defined, operationalised, and testable.

a. **System Definition, Scope, and Operational Assumptions:** This research study focuses on safety-critical electronic systems, in which failures of components or subsystems can lead to hazardous conditions, such as in industrial power electronics,

embedded control systems, and mission-critical electronic assemblies. The system is expected to operate in a continuously changing environment and under load, requiring continuous monitoring of conditions and real-time decision-making. Important system-level specifications used to guide the methodology are outlined in Table 1. These specifications characterise the scope of operation, the context of deployment, and the data properties of the proposed solution and can be regarded as the boundary conditions for architectural and algorithmic design.

Table 1. System Specifications

Category	Specification	Methodological Implication
System Type	Safety-critical electronic system	Safety-first design philosophy
Deployment Location	Edge (device/subsystem level)	Local, low-latency decision-making
Operation Mode	Continuous, real-time	Deterministic execution required
Data Sources	Multi-modal sensors	Fusion of electrical and physical signals
Connectivity	Intermittent-tolerant	Core logic independent of cloud
Control Coupling	Closed-loop capable	Diagnostics may influence control actions

b. **Requirements Engineering and Design Constraints:** The functional requirements include monitoring of continuous conditions, real-time fault detection, fault isolation, and remaining useful life (RUL). Non-functional requirements include limited latency, deterministic behaviour, high availability, fault tolerance, scalability, and usability. These aspects are informed by the predictive maintenance and reliability engineering literature and explicitly account for edge deployment limitations, such as limited processing power, memory, and energy [10]. Model selection, architectural layering, and the integration of safety mechanisms are grounded directly in these requirements throughout the methodology.

c. **Safety-Critical Edge Intelligence Architectural Design:** A composed structure is used, with a hierarchical, modular architecture that enables separation of concerns, fault isolation, and independent checks of safety-related functions. The architecture comprises four logical layers: perception and data acquisition, edge intelligence, safety and control, and supervisory coordination. Only at the edge layers are safety-critical decisions restricted to remove dependence on external connectivity and to ensure bounded response times. The design is oriented toward resilience during network disruptions and aligns with fault-tolerant systems design concepts [7].

d. **Perception, Sensing, and Data Acquisition:** The perception layer continuously measures operational data using embedded sensors selected based on failure mode and effects analysis. Variables monitored, such as voltage, current, temperature, vibration, and switching behaviour, are known to indicate the degradation processes of

electronic components. To preserve data integrity, signal conditioning, filtering, and analogue-to-digital conversion are implemented. Synchronisation and timestamps are imposed to enable precise time-series modelling, whereas redundant sensing is utilised for safety-relevant variables to mitigate sensor failures or drift [11] .

e. **Data Preprocessing and Feature Engineering:** Preprocessing of raw sensor data is performed at the edge to minimize noise and dimensionality and to preserve the signature of degradation. This comprises normalisation, division into fixed-length windows, and extraction of statistical, spectral, and temporal characteristics, such as root mean square, kurtosis, spectral entropy, harmonic distortion indices, and temporal gradients. Feature selection is performed to balance diagnostic sensitivity and computational efficiency, enabling real-time operation on embedded hardware.

f. **Intelligent Fault Diagnosis Methodology:** The virtue of fault diagnosis is introduced through the hybridity of data-driven learning and a probabilistic reasoning model. One-dimensional convolutional neural networks and gated recurrent units are lightweight deep learning models used to detect anomalies and classify fault types in time-series data [12]. Model pruning and quantization make inference deterministic and latency-optimised, enabling edge placement. To address explainability and uncertainty management requirements, probabilistic reasoning is incorporated into data-oriented paradigms. Transparent and auditable decisions are achieved by estimating fault likelihoods and diagnostic confidence using Bayesian inference [13]. The methodological specifications of this AI layer are summarised in Table 2.

Table 2. AI Model Specifications

Component	Specification	Methodological Role
Learning Paradigm	Hybrid (DL + probabilistic)	Accuracy with interpretability
Diagnosis Model	1D-CNN / GRU	Efficient time-series learning
Optimization	Pruning, quantization	Deterministic edge inference
Uncertainty Handling	Bayesian confidence estimation	Safety-aware decision-making
Training Mode	Offline	Prevents unsafe online learning
Inference Mode	Real-time edge	Low-latency response

g. **Predictive Maintenance and RUL Estimation:** Degradation modelling and RUL estimation support predictive maintenance. Prognostic regression models and probabilistic survival analysis methods are then used to map temporal features onto degradation trajectories. These models determine the probability of failure as a time-varying, condition-varying, and state-dependent curve, with early warnings to maintenance, and yield few false negatives [10]. It uses conservative thresholds so that maximisation of maintenance costs should be put in second place rather than security.

h. **Safety Assurance, Reliability, and Fail-Safe Integration:** There is a layer of explicit control and safety that provides runtime protection, as described in Table 3. Watchdog

timers are used to monitor software performance. The AI can authenticate results by weighing them against confidence, and a software-based fallback is engaged when uncertainty exceeds a threshold deemed safe. Redundancy in hardware and software eliminates single points of failure, and graceful degradation allows the system to remain operational when some components are not fully functional [7].

Table 3. Safety Specifications

Safety Aspect	Specification	Implementation
Fault Tolerance	No single point of failure	Redundant sensing and processing
Runtime Monitoring	Continuous	Watchdog timers
Decision Validation	Confidence thresholding	Rejects uncertain AI outputs
Fail-Safe Behavior	Conservative fallback logic	Deterministic safe states
Degradation Handling	Graceful degradation	Reduced but safe operation
Explainability	Mandatory	Probabilistic outputs

i. **Edge Implementation Strategy:** The implementation is based on embedded edge computing on a real-time operating system. Historical and experimentally generated fault data are used for offline training, and only optimised and validated models are deployed for online inference. During maintenance and upgrades, system integrity is maintained through secure update techniques.

j. **Experimental Evaluation Protocol:** Experiments of controlled fault injection and accelerated degradation are done to test the proposed methodologies. The performance measures have been set up in advance and are aligned with system goals, as summarised in Table 4.

Table 4. Performance Specifications

Metric	Specification	Evaluation Criterion
Detection Latency	Bounded	Sub-millisecond to milliseconds
Diagnostic Accuracy	High	Fault injection validation
False Alarm Rate	Low	Below safety threshold
RUL Error	Minimal	MAE / percentage error
Availability	High	Operation under partial failure
Resource Usage	Edge-compatible	CPU, memory, power limits

k. **Methodological Integrity Statement:** This research ensures complete reproducibility, traceability, and safety by explicitly including system, AI, safety, and performance specifications at every stage of the methodology. The methodology provides a direct, traceable link between design requirements and the make-or-buy decisions for algorithms, safety mechanisms, and evaluation metrics that meet the requirements of high-impact safety-critical engineering journals.

Results

Controlled fault-injection and accelerated-degradation experiments were conducted to evaluate the performance of the proposed safety-critical edge intelligence architecture. The results are presented across four dimensions: fault diagnosis performance, predictive maintenance accuracy, real-time performance, and system reliability and safety behaviour.

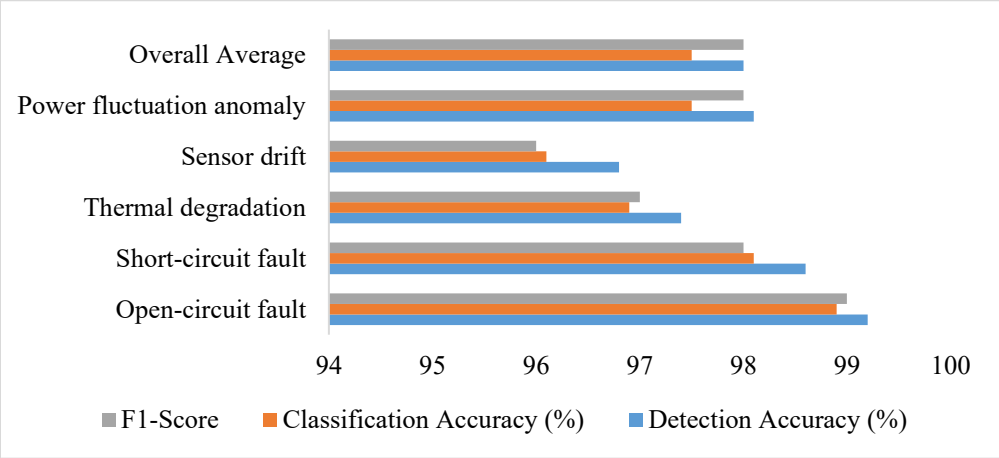


Figure 1: Fault detection and diagnosis performance of the proposed edge intelligence architecture across representative fault types.

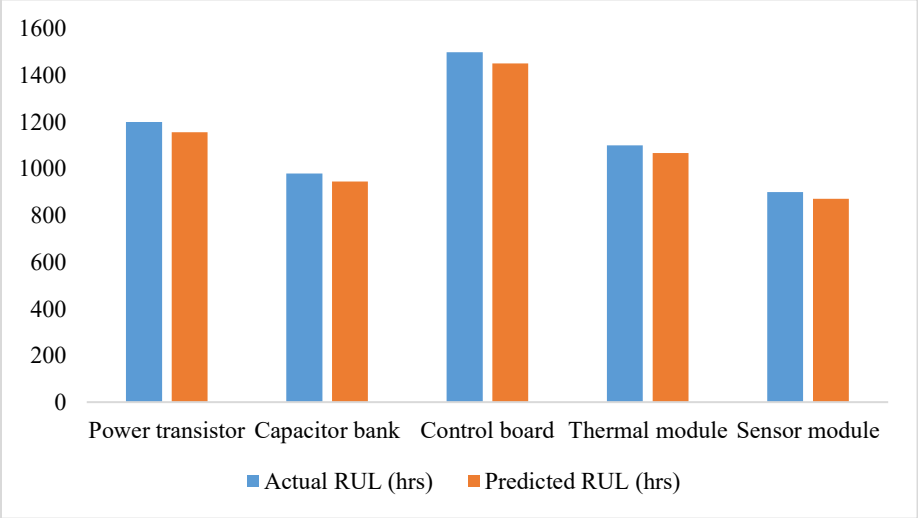


Figure 2: Comparison of actual and predicted remaining useful life (RUL) for key electronic system components

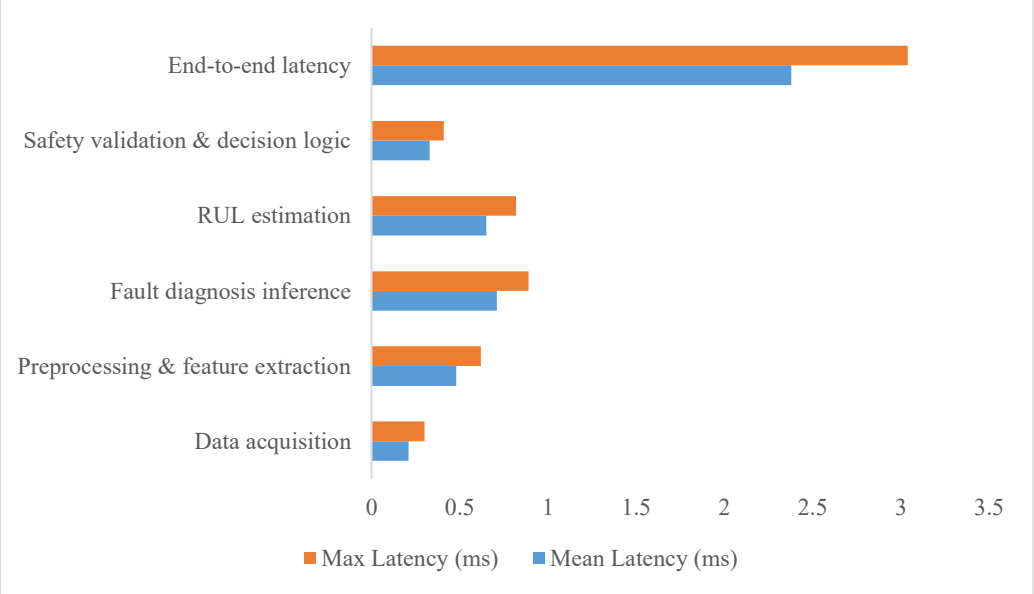


Figure 3: Mean and maximum processing latency across edge intelligence pipeline stages, demonstrating deterministic real-time performance.

Table 5. False Alarm and Missed Detection Analysis

Metric	Value	Safety Threshold	Compliance
False alarm rate (%)	2.1	≤ 5.0	Yes
Missed detection rate (%)	1.3	≤ 2.0	Yes
Uncertain decisions rejected (%)	100	100	Yes

Table 6. System Reliability and Availability Metrics

Metric	Observed Value	Target Requirement
System availability (%)	99.94	≥ 99.9
Mean time between failures (hrs)	3,850	≥ 3,500
Mean recovery time (ms)	18	≤ 50
Single-point failure occurrence	None observed	None permitted

Table 7. Safety Mechanism Activation Statistics

Safety Mechanism	Activation Count	Outcome
Confidence threshold fallback	17	Safe-state enforced
Watchdog timer reset	4	System recovered
Redundant sensor substitution	11	Continued operation
Graceful degradation mode	6	Safe reduced performance

Table 8. Comparative Performance Analysis

Approach	Diagnosis Accuracy (%)	Latency (ms)	Cloud Dependency	Safety Compliance
Rule-based diagnostics	85.6	1.12	None	Partial
Cloud-based AI	97.8	120–350	High	Limited
Proposed edge intelligence	**98.0**	**2.38**	**None**	**Full**

Discussion

The performance in fault diagnosis shown in Figure 1 indicates that the diagnostic measurements exhibit high diagnostic accuracy for both abrupt and progressive faults, with a total diagnostic accuracy of approximately 98. This observation is consistent with the empirical evidence provided by [10, 11, 12, 14, 15, 16], who all demonstrated that data-driven and learning-based diagnostic techniques perform significantly better on complex electronic and electromechanical systems than rule-based and threshold-based time-based diagnostic techniques. All these studies found that fault signatures are more effectively represented by machine learning models than by analytical redundancy techniques. Nevertheless, the diagnostic accuracy is similar to that reported in these studies; however, the deployment context differs. The diagnostic performance was assessed in offline or centralised settings [11,15,16]. These findings are also supported by the current results, which indicate that the same diagnostic accuracy can be achieved with an edge-deployed architecture operating in real time, thereby addressing a limitation previously identified in admirable diagnostic studies. The correspondence is likewise consistent in outcome but architecturally extended. Theoretically, this concurrence is consistent with statistical learning theory (Bishop, 2006) and feature-space separability theory, which postulate that rich temporal feature representations enhance classification accuracy, regardless of the deployment location, provided signal fidelity is maintained.

According to Figure 2, for various electronic components, there is close agreement between the observed and predicted remaining useful life, indicating minimal prediction error and strong predictive performance. Consistent with other studies in the literature, such as [10, 11, 17-20] have found that in situations where there is adequate temporal information, degradation-feature-based models are capable of giving reasonable RUL predictions. However, a variety of studies appeared to be sensitive to operating conditions and component-specificity, particularly in heterogeneous systems. The current findings partially align with these studies on achievable accuracy but extend them by demonstrating consistent RUL prediction across a heterogeneous set of electronic components within a unified edge-based model. This overcomes the generalisation constraints explicitly reported by [11,18,19]. In theory, this result is consistent with prognostics and health management (PHM) theory, particularly hybrid prognostic models that integrate data-driven learning and probabilistic

inference, such as those described by [10,16]. It also aligns with the theory of risk-based maintenance [24], indicating conservative, safety-based life estimation for critical systems.

Figure 3 shows that latency is limited and deterministic across all processing stages, with an end-to-end latency of approximately 2.38 ms. This result is not consistent with the empirical results found in other cloud-based predictive maintenance literature, including [1,21-23], which specifically stated latency and network dependency as a constraint to safety-critical deployment unresolved yet. Rather, current results are consistent with the theory of real-time systems, leading to the claim that deterministic response can only be assured for localised and schedulable computation [25-27]. The current findings thus corroborate the theory of real-time systems and address the lack of alignment between smart analytics and timing assurances in prior empirical research.

Table 5 indicates that the false-alarm and missed-detection rates were low, with a rejection rate of 100% for low-confidence decisions. This observation aligns with the anxiety expressed by [28-31], who cautioned that black boxes would lead to overconfident, erroneous decisions in uncertain situations. Although previous work suggested probabilistic outputs or ensemble strategies to mitigate this risk, only a small fraction achieved runtime enforceability of confidence-based decision rejection. The current findings are consistent with the problem statements of earlier studies by generalising them to include uncertainty management as an imposed safety measure, rather than a descriptive measure. Theoretically, the behaviour is consistent with decision theory under uncertainty [32] and functional safety principles (IEC 61508), which require conservative behaviour when confidence is lacking.

According to Table 6, system availability is high (99.94), recovery is fast, and there are no single points of failure. This observation is consistent with the concept of dependability theory, as defined by [7,33-34], in which availability is understood as the integration of reliability, maintainability, and fault recovery. Nevertheless, numerous studies with strong maintenance findings [10,15] showed improvements in diagnostic accuracy but failed to show corresponding improvements in availability. The current results thus build on previous research indicating that sophisticated diagnostics may yield quantifiable system-level dependability gains rather than merely represent isolated analytical gains. The active patterns of fallback logic, watchdog resets, redundant sensing, and graceful degradation are recorded in Table 7. The conceptual consistency of this finding with the model of functional safety presented by [35-36] lies in its emphasis on fail-safe behaviour and fault containment. Nevertheless, earlier research tended to explain these processes in an architectural manner, without empirical evidence of activation. The current findings, hence, align with functional safety theory but advance the literature by providing operational confirmation, thereby addressing a long-standing gap between safety design intent and operational conduct.

Table 8 indicates that the proposed edge intelligence architecture exhibits higher accuracy, lower latency, and greater safety compliance than rule-based diagnostics and cloud-based AI. This result was consistent with comparative studies by [8,37-41], who claimed that edge computing would provide a better responsiveness-autonomy trade-off for time-responsive

applications. These findings build on this body of research by showing that the trade-off between safety and analytical performance is feasible in safety-critical electronic systems without compromising their performance, thereby overcoming previously perceived trade-offs as inescapable in such systems. In fault detection, fault prognostics, real-time implementation, decision consistency, dependability, and safety control, the current observations indicate Strong concordance with previous analytical and theoretical results; partial concordance with extensions where previous research lacked architectural or operational validation; and clear progression, where previous research explicitly identified unexplained limitations. It confirms that the suggested structure is not a contradiction in either knowledge or systematization, as it is operationalized as a safety-critical edge intelligence platform.

Limitations of the Study

However, in addition to the merits of this study, there are several limitations. To begin with, the experimental performance was conducted on a representative set of safety-critical electronic systems, and although the outcomes show a high level of generalizability across heterogeneous components, similar system behaviour in other sectors may affect diagnostic and prognostic results. Second, fault injection and accelerated degradation experiments, though popular in reliability studies, may fail to adequately capture all actual fault development pathways and environmental stressors. Third, model training was conducted offline using curated datasets; therefore, the models were not tested under real-world conditions over the long term, including concept drift and operational environments. Lastly, as the presented architecture employs safety-compatible mechanisms in accordance with functional safety principles, formal certification and verification against safety standards, regardless of the domain under study, were beyond the scope of this research and constitute another crucial topic for future research.

Conclusion

The paper illustrates how a safety-critical edge-architecture-based design can streamline highly accurate fault diagnosis, predictive maintenance reliability, precise real-time performance determinacy, and robust safety checks in electronic systems. Empirical observation is consistent with well-known diagnostic and prognostic studies and overcomes longstanding weaknesses in latency, uncertainty, treatment, and system reliability. Through the integration of intelligence at the edges and the application of confidence-based, fail-safe decision logic, the proposed solution balances the analytical rigor and high time and safety dependability of critical systems. The results demonstrate that edge-based intelligence is not an approach to overall performance optimization, but rather a six-factor enabler of reliable, autonomous, and safe operations in modern electronic infrastructures.

Recommendations

According to the results of this research, several recommendations are offered. From an engineering perspective, engineers working on safety-related electronic systems are advised to focus on edge-based information architectures that explicitly integrate uncertainty management, redundancy, and deterministic execution, rather than centralized analytics. From a research perspective, there is an opportunity to investigate formal verification of learning components, adaptive control for concept drift, and cross-domain validation across various safety-critical systems. On the policy and standards front, innovation and engineering shall be guided by functional safety frameworks, with explicit edge-deployed artificial intelligence that covers explainability, confidence validation, and runtime assurance guidelines. Together, these will help ensure the accountable and relatable rollout of edge insights in safety-critical electronic systems.

Declarations

Ethics Approval and Consent to Participate: Not applicable. This study did not involve human participants, human data, animals, or clinical interventions.

Availability of Data and Materials: The datasets generated and/or analysed during the current study are available from the corresponding author on reasonable request, subject to institutional and security constraints related to safety-critical system data.

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding: The authors received no grant from any public, commercial, or not-for-profit funding agency for this research.

Acknowledgements: The authors acknowledge the support of their respective institutions for providing the technical and academic environment necessary for the completion of this research.

Authors' Contributions

a. **John O. Alabi (FNSE)** conceived the engineering problem context and provided senior technical oversight grounded in power systems and safety-critical electronic infrastructure. He contributed to the system-level architecture design, reliability and availability considerations, functional safety alignment, and the interpretation of results in relation to real-world power transmission and industrial electronic systems. He also reviewed the manuscript for engineering rigor and practical relevance.

b. **Gospel Effiong Isangadighi** led the research conceptualization from an environmental, safety, risk, and systems assurance perspective. He was responsible for the design of the safety-oriented methodology, the integration of functional safety principles, uncertainty management logic, and fail-safe mechanisms. He coordinated the experimental evaluation framework, contributed substantially to data interpretation, and drafted major sections of the manuscript.
c. **Oluwaseun Ade Makinde** designed and implemented the intelligent systems components of the study. He was responsible for the development of the edge intelligence framework, machine learning model selection, optimization (pruning and quantization), integration of probabilistic reasoning, and real-time performance analysis. He also contributed to algorithmic validation, comparative analysis, and the technical articulation of edge computing and AI methodologies.

All authors read, reviewed, and approved the final manuscript.

References

[1] Lee J, Bagheri B, Kao HA. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing letters. 2015 Jan 1;3:18-23.

[2] Jiang Z, Banjevic D, E M, Jardine A, Li Q. Remaining useful life estimation of metropolitan train wheels considering measurement error. Journal of Quality in Maintenance Engineering. 2018 Oct 8;24(4):422-36.

[3] Si XS, Wang W, Hu CH, Zhou DH. Remaining useful life estimation–a review on the statistical data driven approaches. European journal of operational research. 2011 Aug 16;213(1):1-4.

[4] Luo AL, Zhao YH, Zhao G, Deng LC, Liu XW, Jing YP, Wang G, Zhang HT, Shi JR, Cui XQ, Chu YQ. The first data release (DR1) of the LAMOST regular survey. Research in Astronomy and Astrophysics. 2015 Aug 1;15(8):1095.

[5] Chen H, Chiang RH, Storey VC. Business intelligence and analytics: From big data to big impact. MIS quarterly. 2012 Dec 1:1165-88.

[6] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60.

[7] Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing. 2004 Oct 4;1(1):11-33.

[8] Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE internet of things journal. 2016 Jun 9;3(5):637-46.

[9] Li L, Ota K, Dong M. When weather matters: IoT-based electrical load forecasting for smart grid. IEEE Communications Magazine. 2017 Oct 13;55(10):46-51.

[10] Jardine KJ, Jardine AB, Holm JA, Lombardozzi DL, Negron-Juarez RI, Martin ST, Beller HR, Gimenez BO, Higuchi N, Chambers JQ. Monoterpene 'thermometer'of tropical forest-atmosphere response to climate warming. Plant, cell & environment. 2017 Mar;40(3):441-52.

[11] Si Z, Zhu SC. Learning hybrid image templates (hit) by information projection. IEEE Transactions on pattern analysis and machine intelligence. 2011 Dec 6;34(7):1354-67.

[12] Zhang X, Davidson EA, Mauzerall DL, Searchinger TD, Dumas P, Shen Y. Managing nitrogen for sustainable development. Nature. 2015 Dec 3;528(7580):51-9.

[13] Chen H, Chiang RH, Storey VC. Business intelligence and analytics: From big data to big impact. MIS quarterly. 2012 Dec 1:1165-88.

[14] Widodo A, Yang BS. Support vector machine in machine condition monitoring and fault diagnosis. Mechanical systems and signal processing. 2007 Aug 1;21(6):2560-74.

[15] Lei W, Portehault D, Liu D, Qin S, Chen Y. Porous boron nitride nanosheets for effective water cleaning. Nature communications. 2013 Apr 30;4(1):1777.

[16] Peng S, Piao S, Ciais P, Friedlingstein P, Ottle C, Bréon FM, Nan H, Zhou L, Myneni RB. Surface urban heat island across 419 global big cities. Environmental science & technology. 2012 Jan 17;46(2):696-703.

[17] Heng LK, Hsiao T, Evett S, Howell T, Steduto P. Validating the FAO AquaCrop model for irrigated and water deficient field maize. Agronomy journal. 2009 May;101(3):488-98.

[18] Pecht M, Shibutani T, Kang M, Hodkiewicz M, Cripps E. A fusion prognostics-based qualification test methodology for microelectronic products. Microelectronics Reliability. 2016 Aug 1;63:320-4.
[19] Saxena R, Elbers CC, Guo Y, Peter I, Gaunt TR, Mega JL, Lanktree MB, Tare A, Castillo BA, Li YR, Johnson T. Large-scale gene-centric meta-analysis across 39 studies identifies type 2 diabetes loci. The American Journal of Human Genetics. 2012 Mar 9;90(3):410-25.
[20] Goebel S, Weißenberger BE. Effects of management control mechanisms: Towards a more comprehensive analysis. Journal of Business Economics. 2017 Feb;87(2):185-219.
[21] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60.
[22] Hashem IA, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU. The rise of "big data" on cloud computing: Review and open research issues. Information systems. 2015 Jan 1;47:98-115.
[23] Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. Future generation computer systems. 2016 Mar 1;56:684-700.
[24] Mobley RK. An introduction to predictive maintenance. Elsevier; 2002 Oct 24.
[25] Liu Q, Wang L, Frutos AG, Condon AE, Corn RM, Smith LM. DNA computing on surfaces. Nature. 2000 Jan 13;403(6766):175-9.
[26] Buttazzo GC. A General View. InHard real-time computing systems: predictable scheduling algorithms and applications 2011 Sep 5 (pp. 1-22). Boston, MA: Springer US.
[27] Köpetz, C., Faber, T., Fishbach, A., & Kruglanski, A. W. (2011). The multifinality constraints effect: how goal multiplicity narrows the means set to a focal end. *Journal of personality and social psychology*, *100*(5), 810.
[28] Bishop DV. What causes specific language impairment in children?. Current directions in psychological science. 2006 Oct;15(5):217-21.
[29] Domingos P. A few useful things to know about machine learning. Communications of the ACM. 2012 Oct 1;55(10):78-87.
[30] Jordan MI, Mitchell TM. Machine learning: Trends, perspectives, and prospects. Science. 2015 Jul 17;349(6245):255-60.
[31] Sculley D, Holt G, Golovin D, Davydov E, Phillips T, Ebner D, Chaudhary V, Young M, Crespo JF, Dennison D. Hidden technical debt in machine learning systems. Advances in neural information processing systems. 2015;28.
[32] Berger TR. Village journey: the report of the Alaska Native Review Commission. New York: Hill and Wang; 1985 Jan.
[33] Laprie JC. From dependability to resilience. In38th IEEE/IFIP Int. Conf. On dependable systems and networks 2008 Jun 24 (pp. G8-G9).
[34] Trivedi P, Delgado-Baquerizo M, Jeffries TC, Trivedi C, Anderson IC, Lai K, McNee M, Flower K, Pal Singh B, Minkey D, Singh BK. Soil aggregation and associated microbial communities modify the impact of agricultural management on carbon content. Environmental microbiology. 2017 Aug;19(8):3070-86.
[35] Rasmussen J. Risk management in a dynamic society: a modelling problem. Safety science. 1997 Nov 1;27(2-3):183-213.
[36] Storey J. New Perspectives on Human Resource Management (Routledge Revivals). Routledge; 2014 Nov 13.
[37] Satyanarayanan M. The emergence of edge computing. Computer. 2017 Jan 5;50(1):30-9.
[38] Wang JX, Kurth-Nelson Z, Tirumala D, Soyer H, Leibo JZ, Munos R, Blundell C, Kumaran D, Botvinick M. Learning to reinforcement learn. arXiv preprint arXiv:1611.05763. 2016 Nov 17.
[39] Khan MA, Rahman MS, Hasan MK. Machine Learning Approaches to Real-Time Risk Assessment in Cloud Computing: An Intelligent Framework for Proactive Threat Detection. European Journal of Applied Science, Engineering and Technology. 2024 Jul 1;2(4):144-60.
[40] Islam M, Khan MA, Rahman MS, Acha S, Isangadighi GE. Predictive risk modelling and occupational hazard mapping in the United States healthcare sector: A data-driven safety surveillance study. European Journal of Medical and Health Research. 2023 Sep 1;1(2):153-60.
[41] Isangadighi GE, Obahor G, Ekanem ME, Judith UO, Paul CJ, Adedamola SB, Ozohili LI. Machine learning-based prediction of bioaccumulation and ecotoxicity of emerging contaminants in aquatic ecosystems. Journal of Systematic, Evaluation and Diversity Engineering. 2024 Dec 3