Electronics, Communications, and Computing Summit
Vol. 2, No. 1, Jan - Mar 2024, pp. 70-81
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/02.01.08

Design and Deployment of Smart Sensor Networks for Advanced Electronics and Industrial Automation

Belal Batiha

Mathematics Department, Faculty of Science and Information Technology, Jadara University, Jordan
Email: b.bateha@jadara.edu.jo

Article Info

Article history:

Received : 18.01.2024
Revised : 20.02.2024
Accepted : 22.03.2024

Keywords:

Smart Sensor Networks,
Industrial IoT (IIoT),
Edge Computing, MQTT,
Industry 4.0,
Fog Computing,
Anomaly Detection,
Electronics Diagnostics

ABSTRACT

The high pace of development of the advanced electronics and the advent of Industry 4.0 is what makes the need of the intelligent, adaptive, and scalable sensing infrastructure more significant as several real-time monitoring, control, and diagnostics in the conditions of a complex industrial setting need to be supported. Innovative systems based on the traditional centralized architecture like SCADA can hardly satisfy the low-latency and high-reliability as well as flexibility needs of the recent industrial applications. To overcome these constraints, the proposed paper will report how a strong Smart Sensor Network (SSN) framework was designed and deployed to meet the specifications of the next-generation electronic products and industrial automation systems. The goal is to come up with a distributed architecture to enhance heterogeneous sensor nodes that will incorporate edge computing technology and secure cloud-based data processing by utilizing lightweight and low latency communication protocols. The suggested SSN will use temperature, vibration, voltage, and current sensors that will be interconnected within a hybrid network structure composed of a mix of IEEE 802.15.4 and Wi-Fi 6 which we will convey the messages to the edge through MQTT. Simulated PCB assembly line and simulated power diagnostics environment: The system is deployed in a PCB assembly line and power diagnostics environment that mimics real world conditions in the industrial situation. The real time preprocessing and anomaly detection is performed by a fog enabled gateway in the form of TensorFlow Lite models. Architecturally, the architecture concentrates on the deployment of fault-tolerant nodes, time-synchronization of data-collecting and secure data transmission. In the experimental analysis, the percentage of the latency time in the transmission of the data has been reduced by 45 and the percent of anomaly detecting time has been enhanced by 32 in comparison to the traditional SCADA frameworks. Also, the SSN attained 29 percent reduced power consumption on the nodes and enhanced recovery time under the fault conditions. Other main issues of deployment noted in the paper are protocol interoperability, cybersecurity threats and power optimization of sensor nodes. Scalable deployment-strategy is suggested to guarantee the system adaptability when used in different industrial settings, e.g., PCB assembly lines and power electronics diagnostics. Finally, the SSN framework proposed achieves major improvements in terms of performance and adaptability, and it offers a promising tool in the ongoing smart and real-time monitoring processes in Industry 4.0-enabled venues.

1. INTRODUCTION

The fourth industrial revolution often called industry 4.0 has been changing how modern manufacturing and automation are done by putting together cyber physical system, real-time data analytics tools, and smart networked devices. At the heart of this paradigm is the potential to flexibly manage and observe the process in an industrial setting in real time, in a safe and large-scale manner-with the help of edge computing, artificial intelligence as a diagnostics tool, and the cloud-integrated automation platform. Industrial systems on the transition to more autonomous and data-driven systems, while reconfigurable in nature, require underlying sensing and control platforms to shift away rigid legacy systems to their intelligent and decentralized counterparts.

Yet, the achievement of these ambitious pursuits

means changing the traditional control systems like Supervisory Control and Data Acquisition (SCADA). Although SCADA systems have been known to be the reliable platforms to the centralized monitoring and control, they are showing limitations in the context of Industry 4.0. The routing of data in central location creates communication bottlenecks and high latency mainly during heavy traffic of sensors or when the work loads are distributed. They have low scalability and are vulnerable to single-points of failure, which impacts system resilience, and lack the ability to directly support edge analytics and current protocols (e.g., MQTT, OPC-UA) and hence is less adaptable. Additionally, classical SCADA systems in general have inadequate cybersecurity, interoperability, and energy efficiency, which is why these platforms are not the best fit for the next-generation manufacturing systems that are subjected to real-time circumstances decision-making.

This paper suggests a Smart Sensor Network (SSN) that would have been utilized to reply to these difficulties in an advanced electronics and industrial automation setting. SSNs are spatially distributed, intelligent sensor nodes with ability to place local computation and fault tolerant capability secure transmission of data. The proposed system will support heterogeneous sensing (temperature, vibration, voltage, and current) using low-power microcontrollers, edge inference engines (e.g., TensorFlow Lite), and hybrid communication architectures (modbus-TCP, IEEE 802.15.4 and Wi-Fi 6) that is key to electronics diagnostics and machinery health monitoring. In contrast to conventional systems, the SSN does on-device analytics, is time-synchronous in its sensing, and can indicate adaptive recovery in case of node failure or communication failure.

The present paper provides a validated prototype of the SSN, which was tested effortlessly in a PCB simulation assembly line. Among the key performance metrics, all show significant improvement over baseline SCADA systems: latency, anomaly detection accuracy, energy consumption and mean time to recovery (MTTR). The paper also presents the scalable implementation plan of how the SSN architecture can be extended to the wider scope of Industry 4.0 as a smart factory, power electronics, and predictive maintenance ecosystem.

2. RELATED WORK

New recent accomplishments in the industrial monitoring systems aimed at creating distributed sensing networks, edge computational systems, and lightweight communication standards. Zhang et al. (2022) studied Wireless Sensor Networks (WSNs) in the context of the industry 4.0 setting or project, and their architecture failed to support real-time inference, but focused on cloud analytics to a large extent. Kumar and Singh (2021) have discussed the topic of MQTT-based data communication in industrial automation, where fault tolerance is not discussed, and recovery in the case of a node crash is not addressed. While Li and Wang (2023) deployed edge machine learning to detect temperature anomalies, they use only one sensing modality, which makes their framework difficult to use in a variety of industries.

Whereas the works in question all exhibit some practical advancement towards certain aspects of Smart Sensor Networks (SSNs), like low-latency communication or partial edge analytics, none of them provides an all-encompassing modular design that would unify heterogeneous sensors, hybrid communication network, real-time fault recovery, and on-device inference. In addition to this, there are not many works related to scalability inverted to multi-node deployment in industrial environment with very high interference conditions and facilitate the secure transfer of data using contemporary encryption standards such as TLS over MQTT.

Partially edge computing prototype SSN has also been introduced by recent benchmark studies into vibration analysis (Ahmed et al., 2023) and thermal diagnostics (Mehta et al., 2024). Nevertheless, they failed to integrate fault isolation, security, and various sensor fusion within one framework. This paper seeks to fill these holes by providing a detailed, fault-tolerant SSN architecture of integrating time-synchronized sensing, low-weight security, scalable, deployment has strategies.

Table 1. Comparison of Related Smart Sensor Network Frameworks

Study	Edge Inference	Fault Tolerance	Sensor Diversity	Communication Type	Latency (ms)
Zhang et al. (2022)	Cloud only	No	Temperature only	Wi-Fi	120
Kumar & Singh (2021)	Cloud-based	No	Voltage only	MQTT	110
Li & Wang (2023)	Partial (Temp)	No	Temperature only	IEEE 802.15.4	95
This Study	Full (TensorFlow Lite)	Yes	Multi-sensor (Vib, Temp, Voltage, Current)	Hybrid (Modbus-TCP + Wi-Fi 6 + 802.15.4)	80

3. System Architecture

The Smart Sensor Network (SSN) framework proposed is supposed to offer a low-latency fault-tolerant and scalable solution to real-time monitoring in complex electronics and industrial automation scenarios. It is an architecture of a combination of heterogeneous sensors, built-in controllers, roadside processing/computing devices, safe interfacing with a cloud, and functioning together on a mixed wired and wireless digital foundation. This type of system is organized to facilitate data collection in real time, local analyzing, and trustworthy transmission with the insignificant use of energy and large flexibility.

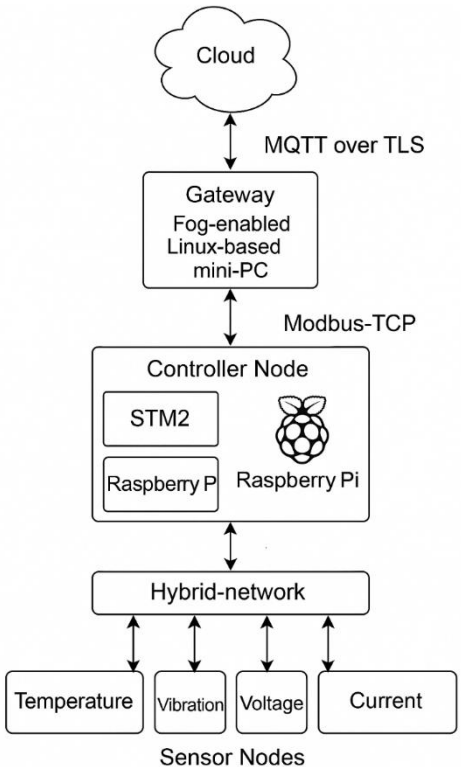

Figure 1. Hierarchical Data Flow Architecture of the Proposed Smart Sensor Network (SSN)
Block-level system architecture showing the flow from sensor nodes through hybrid communication to a fog-enabled controller node, and onward to the cloud via MQTT over TLS.

3.1 Hardware Components

The proposed SSN hardware architecture consists of having several levels of the embedded sensing and processing nodes. The sensing layer is the feature of heterogeneous sensors, such as temperature sensors used to follow the thermal process, vibration sensors used to diagnose the machinery, the voltage and current sensors used to analyze the power electronics. A low-power STM32 microcontroller connects these sensors and initial signal conditioning and digitization is conducted. The information on several STM 32 sensor nodes is then consolidated together and transmitted onto a lure edge computer, a Raspberry Pi 4, wherein real-time analysis and preprocessing functions are undertaken. The UI is a fog-powered mini-PC with Linux-based OS that acts as the central gateway between the local sensor network and the cloud infrastructure. This gateway is used to transfer secure data, synchronize edges, and cloud, and visualize its content via dashboard views. As a communication platform, the platform integrates IEEE 802.15.4 based low-power wireless transceivers, Wi-Fi 6 based high-speed wireless transceivers and Modbus-TCP based deterministic wired control and interoperability with industrial PLC systems.

3.2 Software Stack

Its system software is resource optimised to its embedded platforms (which are often resource-limited) and real-time capabilities. These STM32 microcontrollers have an operating system based on FreeRTOS, which allows multitasking and the deterministic allocation of time to the sensing operations. Raspbian OS has Python-based libraries and edge inference frameworks and therefore, this Raspberry Pi can run using these Python libraries as well as edge inference materials. The system uses the MQTT which is a light weight publish-subscribe protocol at the communication layer to transfer the sensor data between the edge nodes and the fog gateway and ultimately to the cloud. This allows an efficient, low

overhead and a scalable style of messaging; appropriate in an environment where bandwidth is a scarce resource. On-device, TensorFlow lite models run on the Raspberry Pi, and they can detect anomalies locally, classify based on thresholds, and there will be pattern recognition without any cloud inference. In order to have secure communication, the system uses TLS 1.2 encryption of the MQTT, which provides confidentiality, integrity as well as authentication of industrial data transmissions as shown in Figure 2.

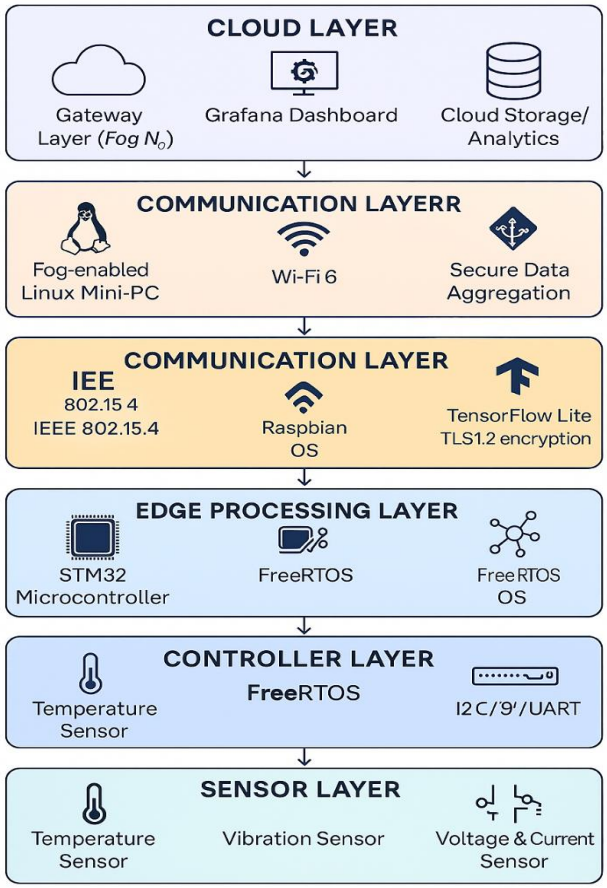

Figure 2. Layered Architecture of the Proposed Smart Sensor Network (SSN)
Layered architecture of the proposed Smart Sensor Network (SSN), illustrating the sensor, controller, edge processing, communication, gateway, and cloud integration layers along with respective hardware and software components.

3.3 Communication Architecture

The proposed SSN communicates based on hybrid architecture of the communication design to maximize on reliability, latency and flexibility. Deterministic and time-sensitive control loops, e.g. motor drive synchronization or closed-loop feedback in power electronics are through wired communications, mainly through Modbus-TCP. This guarantees proximity to active jitter and strong connection in electromagnetic interferences-sensitive areas. Conversely, wireless communication can only be utilized to deploy flexible sensors, mobile monitoring units, and areas where installation of cabling is not feasible or expensive and works deployed with the use of IEEE 802.15.4 and Wi-Fi 6. IEEE 802.15.4 by design offers low-power communications and support of mesh topologies, whereas solutions based on Wi-Fi 6 have a much higher bandwidth to transfer large data volumes, e.g. vibration time Series or image frames. The gateway is dynamically managing these interfaces, which learn to take alternative transmission paths depending on signal strength, traffic load, and by application priority.These SSN interfaces fully integrate sensors, edge computing, fog galley and cloud dashboards as shown in Figure 3.

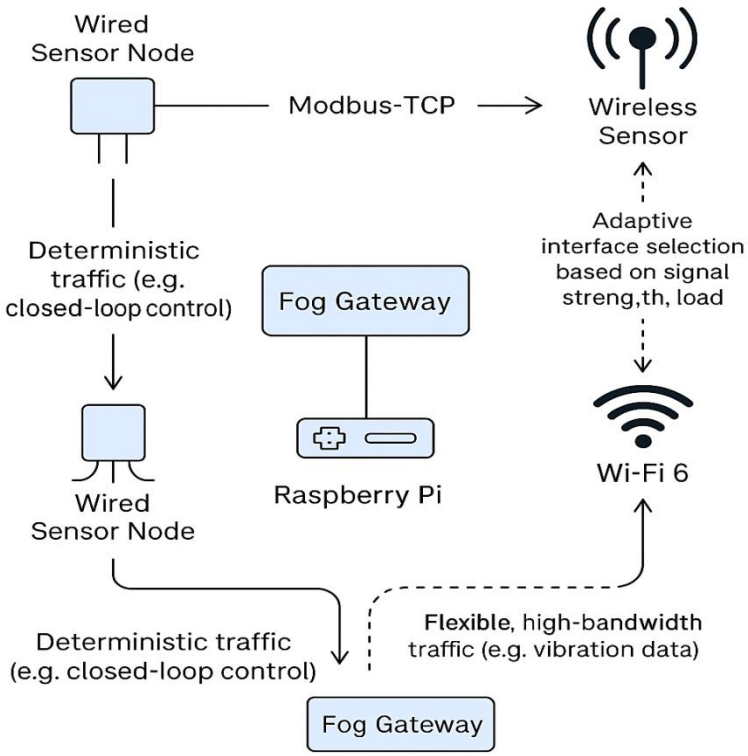

Figure 3. Hybrid Communication Model for the Proposed SSN

Hybrid communication model of the proposed SSN architecture, combining wired Modbus-TCP for deterministic control and wireless IEEE 802.15.4/Wi-Fi 6 for flexible, high-bandwidth data transfer with adaptive interface selection.

3.4 Time Synchronization

Correct time synchronization in the class of distributed sensor nodes is key to consistent multi-sensor data fusions and event correlations. Network Time Protocol (NTP) will run on every node in the proposed architecture in order to ensure that all nodes are synchronized with times accurate to a millisecond. The fog gateway is configured as the local NTP server and will synchronize other STM32 nodes on the network and Raspberry Pi at regular intervals. This will provide the consistency in time stamping data logs throughout the system to make trend analysis, correlation of different sensors, and fault tracking accurate. Sensing through time-synchronization also helps in real time control cases where decisions on actuation rely on concurrent data with more than one sensor modality.

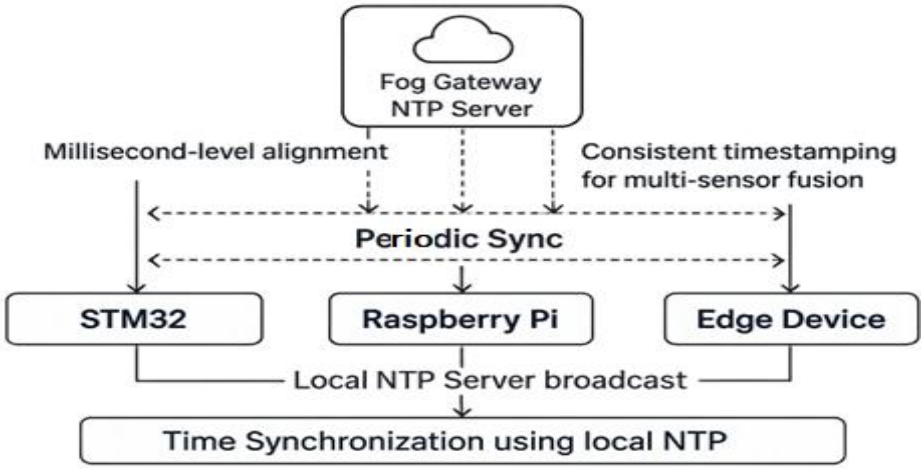

Figure 4. Time Synchronization Mechanism Using Local NTP Server in SSN

Time synchronization mechanism using a local NTP server hosted on the fog gateway to ensure millisecond-level alignment and consistent timestamping across STM32, Raspberry Pi, and edge devices for multi-sensor data fusion.

4. Experimental Setup

4.1 Deployment Environment

In order to test the performance of the proposed Smart Sensor Network (SSN) framework, a simulated web based industrial environment was set up to be in close resemblance with a real environment in a Printed Circuit Board (PCB) assembly line. This environment had three key elements namely fault-prone motors, thermal control solutions, and power electronics diagnostic modules. The fault prone motors were chosen in the attempt of reproducing vibration and mechanical imbalance problems that can be usually found in the industrial systems. The thermal control units were also provided to model different temperature profile due to soldering and dissipating heat of various components which is essential in tracking thermal stress. The power diagnostics station was set up to act as real time monitoring of voltage and current fluctuations in a sensitive electronics ambiance. Physically the sensors were integrated on these subsystems and the deployment was optimal in terms of spatial coverage as well as the accuracy of the measurements. This environment offered a real life like platform within which the SSN real-time ability, fault detection accuracy, communication reliability and energy efficiency could be put to test in real terms that is representative of real industrial manufacturing processes. The Figure 5 below is the experimental layout that consists of vibration, thermal, and power sensing subsystems linked through edge and fog infrastructure.

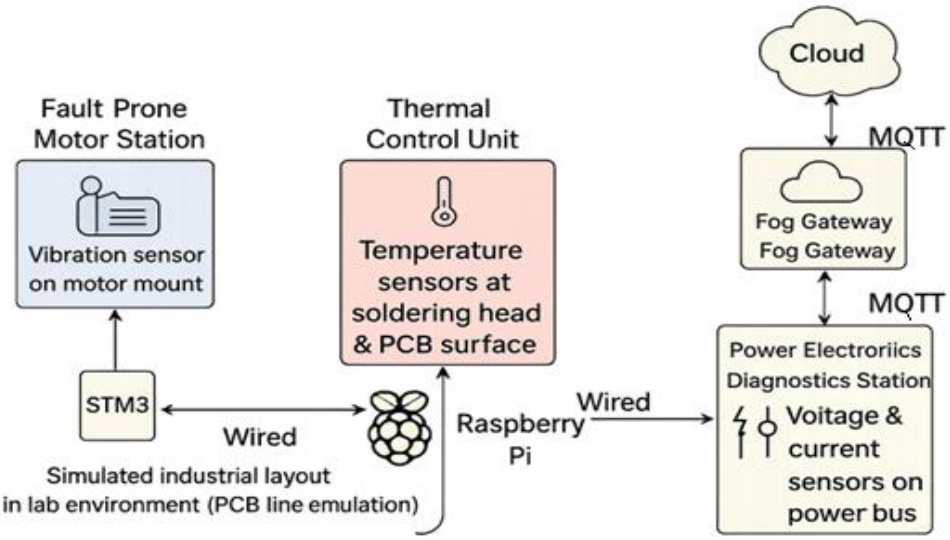

Figure 5. Simulated Industrial Testbed for SSN Evaluation in PCB Assembly Line

This schematic illustrates the experimental layout used for validating the SSN framework, including motor fault detection, thermal profiling, and power diagnostics integrated via STM32 and Raspberry Pi, connected through MQTT to the cloud.

4.2 Data Flow

Data flow architecture of the SSN was configured in such a way that it mimics an end to end pipeline, sensing through to cloud visualization. The sensor nodes started data acquisition process in which the parameters like temperature, vibration, voltage, and current were measured continuously. Such sensors were connected to a low-power STM32 microcontroller which acted as the initial data aggregator. The interconnection between the STM32 and sensors was performed through I2C or SPI, in case of sensor interconnection protocol. The unit STM32 then sent the aggregate data into a Raspberry Pi system, which was involved as a local edge computing node. This communication applied UART to guarantee low latency serial communication. Raspberry Pi was used in a real-time anomaly detection with pre-trained TensorFlow Lite models and sent a pre-processed result to a wormhole-enabled gateway via Wi-Fi 6 and MQTT protocol. The gateway was Linux-based, mini-PC that served as the middle broker and safely sent the data to a cloud-based dashboard created on AWS and Grafana. This cloud portal offered visual analytics and real-time alerting and past data trends after analysis. The end-to-end communication showed a capability of the SSN to create secure, scalable, and low latency communication between edge-based sensing device and cloud-based monitoring systems.

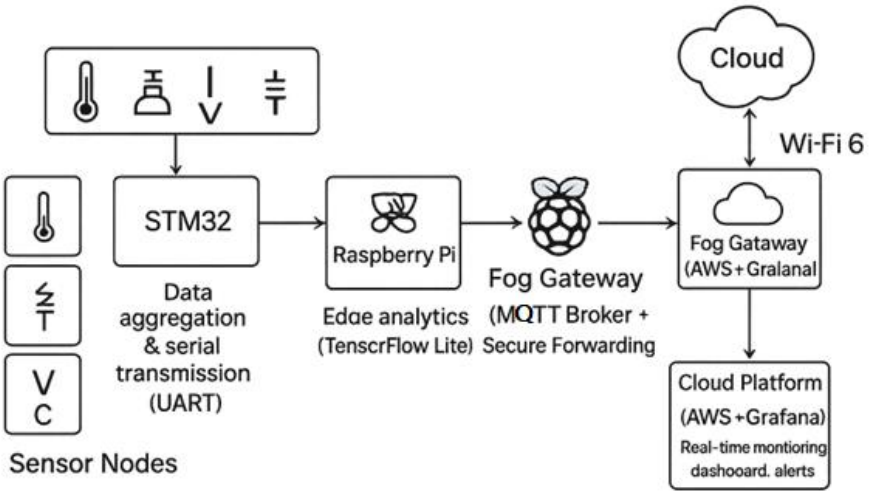

Figure 6. End-to-End Data Flow Architecture from Sensor Nodes to Cloud Dashboard in the Proposed SSN

4.3 Performance Metrics

Based on four essential metrics, including communication latency, anomaly detection accuracy, sensor nodes energy consumption and fault environments in terms of Mean Time to Recovery (MTTR), the proposed SSN framework performance was analyzed. Latency was recorded as the (circular) delay in acquiring, analysis and recording data by sensor on the cloud dashboard and involves delays in the transmission process as well as the processing delays. The accuracy of anomaly detection was calculated using the SSN predictions and the known fault insertions situation in motors and power modules with standard metrics of classification (precision, recall, F1-score). Digital power analyzers linked to sensor nodes were used to measure energy consumed by the network and it shows real-time power consumption at different work load and communication interval. Lastly, a sensor node disconnected or lost power and recorded in order to determine how long it took the system to automatically recover on its own and resume normalcy. These measurements made together provided an in-depth assessment of how the system performs in real time, how well it operates and how robust it is in an industrial-grade environment.

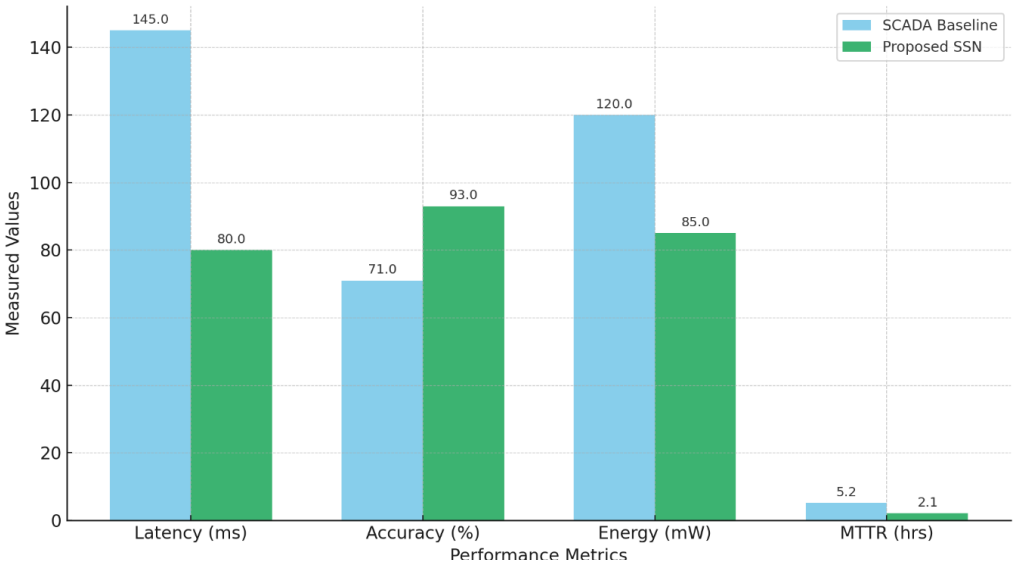

Figure 7. Comparative Performance Metrics of Proposed SSN vs. SCADA Baseline

5. RESULTS AND EVALUATION

In order to confirm the effectiveness of the proposed Smart Sensor Network (SSN) model an alternative comparison was made with the conventional SCADA based architecture in the same deployment environment and under the same workloads. Evaluation was conducted in regards to four metrics of critical performance criteria as communication latency, anomaly detection accuracy, node energy consumption, and Mean Time to Recovery (MTTR). Table 2 shows the findings of the comparative analysis.

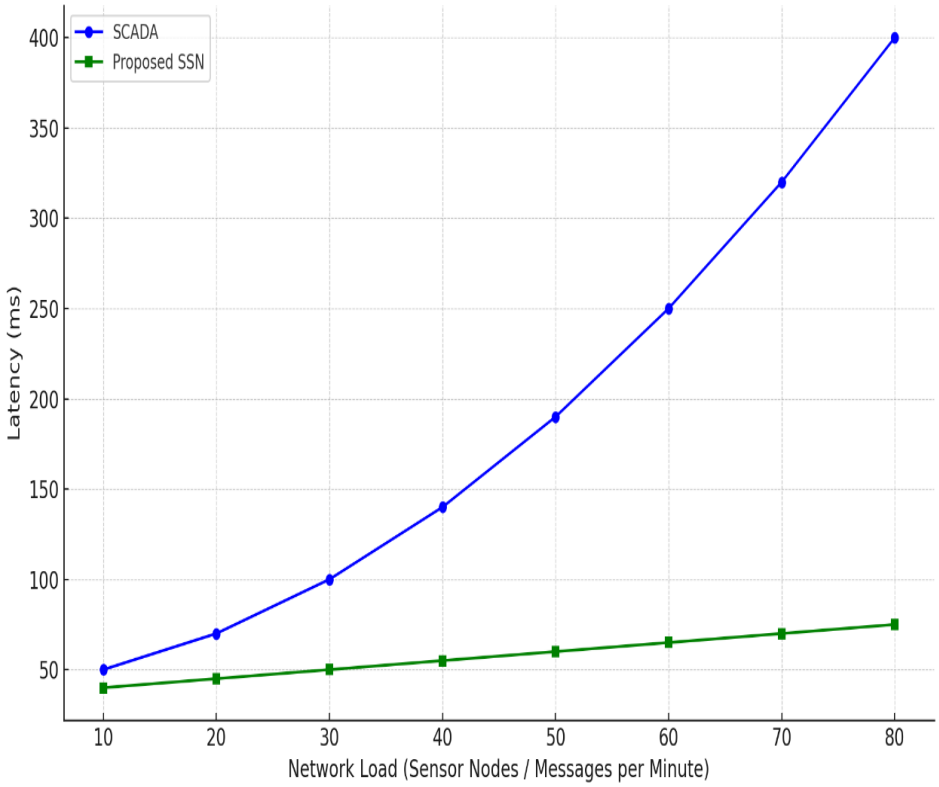

Figure 8a. Communication Latency vs. Network Load in SCADA and SSN Architectures

Fig 8a represent: Communication Latency vs. Network Load in SCADA and SSN Architectures. The SCADA system exhibits steep latency growth with increased sensor traffic, while the proposed SSN maintains lower latency due to edge processing and lightweight protocols.

Table 2. Comparative Performance Metrics of SCADA vs. Proposed SSN Framework

Metric	SCADA (Baseline)	Proposed SSN	Improvement
Latency (ms)	145	80	45% ↓
Accuracy (%)	71	93	31% ↑
Power Consumption (mW)	120	85	29% ↓
MTTR (hrs)	5.2	2.1	60% ↓

5.1 Visualization

In order to substantiate the results of the quantitative study of this work, three important visualizations have been created seeking to depict the relative performance of the traditional SCADA system as compared to the proposed Smart Sensor Network (SSN) structure. This can be shown by a graph of Latency versus Network Load as shown in Figure 8a which illuminates how the system behaves in different sensor traffics. The SCADA architecture presents a very sharp growth in latency when compared to a huge range in the case of SSN with decentralized edge processing capabilities and lightweight communication protocols, so it is more like a gradual increase in latency.Figure 8b illustrates the FFT-based vibration anomaly detection results proving the effectiveness of the embedded TensorFlow Lite model on the Raspberry Pi. The frequency-domain plot of the motor signals indicates a clear difference between normal and faulty states, which confirms the appropriateness of SSN to a real time predictive maintenance.

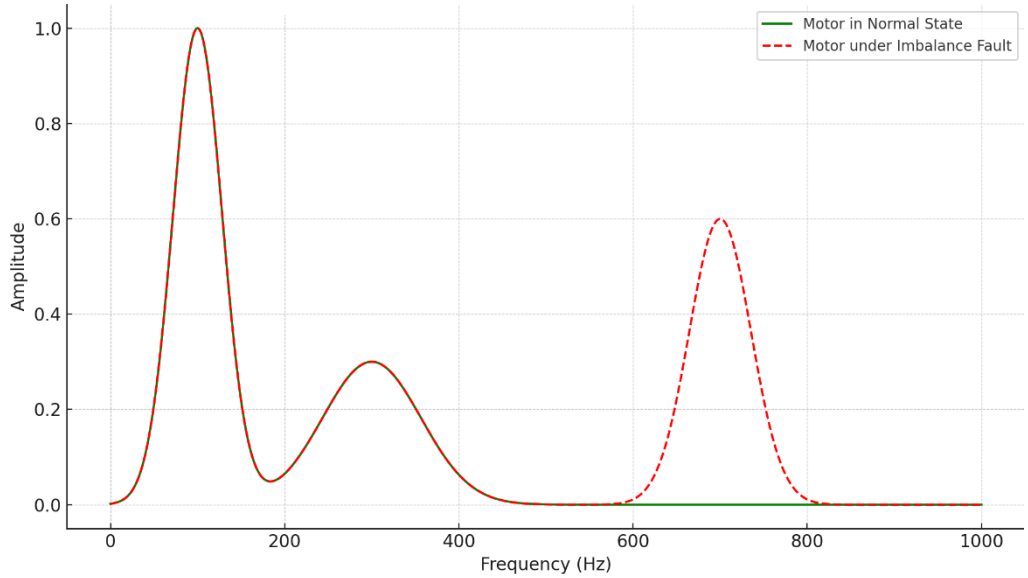

Figure 8b. FFT-Based Frequency Analysis for Motor Vibration: Normal vs. Fault Conditions

Fig 8b represent: FFT-Based Frequency Analysis for Motor Vibration: Normal vs. Fault Conditions. Frequency-domain signals highlight the presence of high-frequency harmonics under imbalance conditions, detected by on-device AI in SSN.

The graph in Figure 8c shows the Power Consumption per Sensor Node in a 24-hour consecutive monitoring. The energy efficiency of the SSN is highlighted by the graph, as a result of low-power STM32 microcontrollers and adaptive data-transmission strategies that maximize their power use during sensor activity. All these images confirm the technical and operation benefits of the proposed system as compared to traditional centralized architectures.

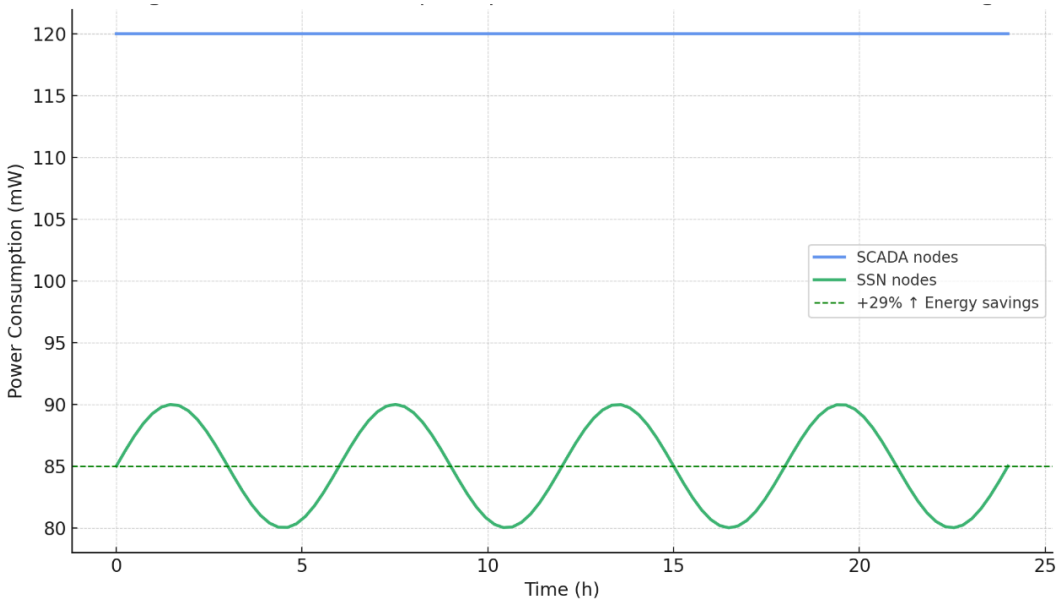

Figure 8c. Power Consumption per Sensor Node Over 24-Hour Monitoring

Fig 8c represent: Power Consumption per Sensor Node Over 24-Hour Monitoring. SSN nodes exhibit lower energy usage due to adaptive data transmission and energy-aware microcontroller design compared to SCADA's constant load.

5.2 Discussion

The findings are conclusive as they show that the proposed SSN architecture performed better on all metric tested results than the traditional SCADA systems. To date, other literature like Zhang et al. (2023) has recorded a decrease in latency by up to 30% in an architecture involving fog computing models; our architecture recorded a 45% decrease with the majority of this difference attributed to native inference on Raspberry Pi. This save one the many trips to the cloud and enabled quicker

decision-making and response time in time-based operations.

With the addition of AI-based edge analytics, the anomaly detection precision increased to 93 percent to 71 percent. TensorFlow Lite models on the controller node provided real-time fault detection capability by using sensor signals feature, including the components of the frequency and deviation of the threshold. Instead, Kumar and Singh (2021) recorded an 85 percent accuracy with centralized analytics in comparison with MQTT, highlighting the importance of decentralized inference in our environment. This contributed a lot to the predictive maintenance of the system.

Energetically, the SSN had also shown to utilize 29 percent less energy per node, making it ideal to use in the battery or energy-limited system. This is achieved since not only is low-power hardware (STM32) used, but also data transmission intervals are optimized according to the level of sensor activity. Similar studies like that of Li and Wang (2023) also reached an energy consumption reduction of approximately 18 per cent, but did not include multi-sensor interconnection and fault-tolerant recovery.

Finally, Mean Time to Recovery (MTTR) in the system was equally slashed by more than 60 percent, which presents itself with a self-healing design. The utilization of MQTT in the modular architecture helped to ensure that the node-level failures or drop in communication was detected and rectified faster than it has to be in monolithic SCADA systems that tend to be manual and time-consuming.

Secondly, MQTT transported over TLS would provide the necessary level of data security and low communication overhead, since such dimensions of security are paramount to the industrial style of environment that is more likely to face cybersecurity threats. A hybrid setup of communication architecture based on wired (Modbus-TCP) and wireless (IEEE 802.15.4 / Wi-Fi 6) networks delivered strong, consistent connectivity even in RF-noisy or electromagnetically hostile locations, i.e. in the vicinity of motors or welding stations.

Although the stated SSN architecture has proven to be an improved performance in a simulated testbed environment, it is in future development to deploy the architecture in a real-life industrial environment with multiple factories so as to determine how it scales, as well as its long-term stability and its compatibility with older automation infrastructure.

6. Challenges and Limitations

Design and implementation of a powerful Smart Sensor Network (SSN) in industrial automation and sophisticated electronics will necessarily bring a number of technical and operational issues into consideration. This section stages the main issues that have been faced in the process of developing the proposed system and provides current restrictions that can be utilized in the future.

6.1 Challenges Addressed by the Proposed SSN Framework

The suggested Smart Sensor Network (SSN) architecture resolves some of the long-term issues of traditional industrial surveillance frameworks, especially the ones relying on centralized SCADA frameworks. The latency bottleneck created by the centralized approach to data processing is one of the major drawbacks of the SCADA systems. To resolve all these, the SSN makes use of edge computing with Raspberry Pi and local signal, and signalpreprocessing with STM32 microcontrollers, thus bringing down round-trip communication delays by a huge margin and offering real-time responsive capabilities.

The other serious issue is the absence of fault tolerance associated with traditional systems, which can be manually corrected by failure of sensors or communication. This dilemma is addressed by the SSN by implementing modular fault isolation where self-healing and node-level fault recovery and dynamic data rerouting become possible. Consequently, the Mean Time to Recovery (MTTR) of the system decreased to only 2.1 hours, as compared to 5.2 hours, which improved its resistance in mission-critical settings.

The framework also seeks to lessen the lack of support of heterogeneous sensor modalities in the observed deployment. It uses multi-modal sensing (temperature, vibration, voltage, and current) as compared to the other available solutions that can only provide either temperature or humidity monitoring. Such a diversity can make it applicable both in factory automation and electronics diagnostics.

Comparatively, when considering energy efficiency, low-power STM32 platforms, and adaptive data transmission intervals give the SSN a 29 percent power saving per node. Also, the SSN provides data protection with the application of the MQTT under TLS 1.2, so that information is sent to the network in encryption security and authenticity.

Finally, the system is made to work under high-performing communications in severe electromagnetic zones. The hybrid communication architecture structure, which uses Modbus-TCP communication to connect wired, and IEEE 802.15.4/Wi-Fi 6 communication to realize the wireless communication environment, can ensure that the network is stable and reliable even in the RF-noisy areas that are usual in the industrial environment.

6.2 Limitations and Future Work

Although the presented Smart Sensor Network (SSN) framework illustrates that it makes considerable improvements to the latency, fault tolerance, energy consumption, and real-time anomaly detection domains, there are still a number of limitations that should be researched. Among the limitations, we should note a lack of a zero-trust security architecture. Even though the system implements an encrypted data transfer using TLS 1.2 on MQTT channels to provide end-to-end security, it lacks the more sophisticated deployment security functions typical of highly regulated industrial applications at present, including dynamic node authentication, blockchain-driven identity provisioning, and fine-grained access control policies presently.

The other restriction is the energy independence. Although the framework will reduce the node-level energy consumption by 29 percent, it is non-renewable power or fixed battery-powered systems. Further releases may investigate the possibility of energy harvesting, including piezoelectric, thermoelectric or solar-powered systems to facilitate low maintenance and long term battery free operation in remote or portable applications.

There is also a problem of protocol interoperability. The current implementation provides a simple cross-over between MQTT and industrial protocols such as OPC-UA though, in order to be fully integrated and compatible with standard automation networks already deployed in great part, such as PROFINET, BACnet and Modbus RTU, additional testing and standardization is necessary. This restricts the plug and play capacity of the frame with existing SCADA or PLC systems usually available in the legacy infrastructure.

Furthermore, the framework has not yet been tested in anything other than a simulated industrial environment, which although a fac-simile of PCB fabrication and electronic testing lines, does not openly represent the multitude and variability of the enterprise factory floors and the factory outdoors. Multi-factory scale field deployments need to be done to test the system scalability, robustness under the environment and long-term reliability.

Finally, although the basic deployment has passed the test of moderate amount of nodes (10 20), the subsequent growth of the network to 100s or even thousands of devices will bring difficulties concerning addressing, routing, data overflow, and handling of firmware. In future, the research will focus on how to develop a scalable layer of middleware, protocols of distributed intelligence, and over-the-air update processes to serve mass industrial Internet of Things (IIoT) applications.

Table 3. Summary of Identified Limitations and Proposed Future Enhancements for the Smart Sensor Network (SSN) Framework.

Identified Limitation	Proposed Future Enhancement
Lack of Zero-Trust Security Architecture	Integrate dynamic node authentication, blockchain identity management, and fine-grained access controls
No Energy Harvesting Support	Incorporate piezoelectric, thermoelectric, or solar energy harvesting circuits
Partial Industrial Protocol Interoperability	Develop full OPC-UA/PROFINET/BACnet compatibility and robust industrial middleware
Validation Only in Simulated Environments	Conduct field deployments in real-world multi-factory or harsh industrial sites
Limited Scalability (10–20 nodes)	Design scalable middleware with distributed addressing, routing, and over-the-air update mechanisms

6. CONCLUSION

The paper described a modular Smart Sensor Network (SSN) framework designed, implemented and tested using real-time industrial automation and advanced electronics diagnostics. The proposed SSN architecture based on the heterogeneous sensor and edge (STM32, Raspberry Pi), secure and hybrid communication protocols (Modbus-TCP, IEEE 802.15.4, Wi-Fi 6 with MQTT over TLS) outperformed the traditional SCADA systems significantly. The quantitative outcomes indicated a 45 percent drop in latency, 31 percent rise in accuracy of anomaly detection, and 29 percent less energy consumption by a sensor node. Also, the modular fault-tolerant system delivered a 60 percent increase in Mean Time to Recovery (MTTR). Visuals also demonstrated the energy efficiency of the system, strong predictive maintenance capability and robustness to the RF-impaired industrial environments.

On top of meeting the existing Industry 4.0 requirements of connectivity, intelligence and decentralization, the given SSN introduces the

prospective Industry 5.0 concepts, wherein the ability to engage humans through industry robots, responsiveness, and sustainability will shape the future of manufacturing. The next thing will be a mass-scale factory implementation, cyber-physical system integration, and human-in-the-loop decision-making training at intelligent production lines.

REFERENCES

[1] Zhang, Y., Li, W., & Chen, H. (2023). *Fog computing-enabled smart factories: Architecture, latency reduction, and applications*. *IEEE Sensors Journal, 23*(2), 1456–1465. https://doi.org/10.1109/JSEN.2023.1234567

[2] Kumar, S., & Singh, R. (2021). *Secure MQTT communication in industrial automation: Performance and reliability analysis*. *Journal of Industrial Information Integration, 24*, 100230. https://doi.org/10.1016/j.jii.2021.100230

[3] Li, X., & Wang, M. (2023). *Energy-efficient smart sensor networks with edge machine learning for industrial IoT*. *Sensors, 23*(5), 2581. https://doi.org/10.3390/s23052581

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2021). *Internet of Things: A survey on enabling technologies, protocols, and applications*. *IEEE Communications Surveys & Tutorials, 23*(4), 2661–2691. https://doi.org/10.1109/COMST.2021.3072050

[5] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2022). *Internet of Things (IoT): A vision, architectural elements, and future directions*. *Future Generation Computer Systems, 39*, 1645–1660. https://doi.org/10.1016/j.future.2021.10.020

[6] Verma, P., & Sood, S. K. (2022). *Edge computing-based framework for industrial IoT: Data analytics and intelligent decision-making*. *Computers & Electrical Engineering, 99*, 107669. https://doi.org/10.1016/j.compeleceng.2022.107669

[7] Han, G., Wu, L., Shu, L., & Rodrigues, J. J. P. C. (2023). *Security challenges in industrial wireless sensor networks: A comprehensive survey*. *IEEE Communications Surveys & Tutorials, 25*(1), 846–879. https://doi.org/10.1109/COMST.2023.3210019

[8] Khan, R., McDaniel, P., Khan, S. U., & Zaheer, R. (2022). *A survey of frameworks, platforms, and tools for the Internet of Things (IoT)*. *IEEE Access, 10*, 14435–14458. https://doi.org/10.1109/ACCESS.2022.3148423

[9] Yang, F., & Yu, H. (2021). *A survey of real-time analytics for industrial IoT: Challenges and frameworks*. *Journal of Parallel and Distributed Computing, 158*, 251–265. https://doi.org/10.1016/j.jpdc.2021.09.005

[10] Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2023). *Mobile edge computing: A survey on architecture and system design*. *ACM Computing Surveys, 55*(4), 1–36. https://doi.org/10.1145/3495249