MITOR: Jurnal Teknik Elektro

Implementation of Centralized IoT Safety Latching for Class-D Amplifiers: Latency Analysis and OTA Integration

Gaguk Firasanto, Andriani*, Donie Agus Ardianto, Zainin Widadi, Donal Karyano
Faculty of Engineering, Electrical Engineering Program – Pamulang University
Pamulang, Indonesia
*andriani199829@gmail.com

Abstract – *Class-D audio power amplifiers have become the dominant topology in modern high-power acoustic reinforcement systems due to their superior efficiency and compact footprint, yet they remain highly vulnerable to catastrophic failures induced by thermal runaway and output overcurrent. Although conventional passive protection devices and localized active protection systems are capable of isolating such faults at the unit level, these approaches inherently lack centralized remote monitoring capability, statistically grounded latency awareness, and seamless wireless software maintainability — limitations that become increasingly critical as audio infrastructures evolve toward large-scale smart-building deployments. To address these gaps, this study proposes a centralized Internet of Things (IoT)-based safety latching protection system that employs an ESP32 microcontroller as a telemetry node integrated with an INA219 digital current monitor and an LM35 precision thermal sensor. In contrast to decentralized architectures, the main safety latching algorithm based on digital OR logic is deliberately offloaded to a Python-based Graphical User Interface (GUI) server, with bidirectional command and telemetry exchange facilitated through the Message Queuing Telemetry Transport (MQTT) protocol. In addition, an Over-The-Air (OTA) firmware update mechanism using a secure cloud-hosted repository is integrated to enable wireless software maintenance and threshold reconfiguration without requiring physical hardware intervention. The experimental results demonstrate consistently high measurement accuracy, with average acquisition errors of less than 1% for thermal telemetry and less than 2% for current telemetry. The centralized safety latching algorithm operated robustly and successfully disconnected the amplifier load at the critical thresholds of 75.1 °C and 3.48 A, effectively preventing destructive power oscillations by enforcing a mandatory LATCHED_OFF state that requires manual operator authentication for restoration. A statistical network latency analysis conducted over 50 test cycles further confirmed mean isolation delays of 34.6 ms under strong signal conditions and 85.4 ms even under weak signal conditions — both well below the 200 ms safety margin required to prevent semiconductor degradation. Furthermore, the OTA mechanism was successfully validated for remote firmware deployment without interrupting the primary telemetry loop. In conclusion, the proposed centralized IoT framework significantly improves the diagnostic reliability, operational safety, and long-term maintainability of high-power audio systems, providing a scalable foundation for next-generation smart audio infrastructures.*

Keywords – *Class-D Amplifier; Centralized IoT; Safety Latching; MQTT Latency; OTA Update.*

I. Introduction

MODERN audio reinforcement systems have become a fundamental component of contemporary acoustic infrastructure, ranging from large-scale concert venues and conference auditoriums to public address installations in transportation hubs, houses of worship, and industrial facilities. In each of these deployments, the audio power amplifier represents the most critical electronic stage, because it is responsible for converting low-level line signals into high-current waveforms capable of physically driving electrodynamic loudspeaker transducers. Over the past decade, Class-D amplifier architectures have achieved widespread adoption, progressively displacing traditional linear topologies such as Class-A and Class-AB designs. This paradigm shift is primarily attributed to the superior power conversion efficiency, significantly lower thermal dissipation, and compact physical footprint offered by switching-mode designs [1]. By leveraging high-frequency pulse-width modulation (PWM) techniques operating at carrier frequencies typically between 200 kHz and 1 MHz, Class-D modules can attain operational efficiencies exceeding 90%, while simultaneously minimizing the volume and mass of associated heat dissipation hardware. However, this high power density and aggressive switching behavior also intro-

The manuscript was received on May 28, 2026, revised on May 30, 2026, and published online on July 31, 2026. Emitor is a Journal of Electrical Engineering at Universitas Muhammadiyah Surakarta with ISSN (Print) 1411 – 8890 and ISSN (Online) 2541 – 4518, holding Sinta 3 accreditation. It is accessible at https://journals2.ums.ac.id/index.php/emitor/index.

duce critical vulnerabilities. The sensitive metal-oxide-semiconductor field-effect transistors (MOSFETs) embedded within the output H-bridge stage remain highly susceptible to catastrophic failures triggered by rapid thermal runaway, output overcurrent anomalies, inductive flyback transients, and sudden short-circuit conditions across the speaker load [2, 3].

When an operational fault occurs, such as a low-impedance short circuit between the output terminals, a saturated audio waveform driven into clipping, or an excessive thermal spike accumulating within the chassis, an uncontrolled flow of destructive energy is delivered directly to the speaker load. This unregulated power transfer frequently causes permanent and irreversible damage to expensive voice coils, melting the copper windings or deforming the suspension assembly of the transducer. To safeguard high-power audio transducers from such failure modes, traditional engineering frameworks have predominantly relied on passive protection devices, including bimetallic thermal switches, polyswitch resettable fuses, and electromechanical sacrificial fuses installed in series with the speaker line [4]. Although these legacy components are highly economical, mechanically simple, and widely available, they suffer from inherently delayed response times in the order of hundreds of milliseconds, which are often too slow to interrupt instantaneous transient overcurrent spikes before semiconductor degradation begins to propagate. Furthermore, passive components operate blindly in the sense that they lack the intrinsic capability to capture, quantitatively process, or chronologically record the diagnostic telemetry associated with the fault event itself. As a direct consequence of this informational opacity, system technicians face significant difficulties during post-incident troubleshooting, because no empirical time-series data is available to determine whether a particular failure was caused by sustained thermal overload, mechanical resonance of the loudspeaker chassis, an electrical short circuit, or an upstream power supply anomaly. Recent engineering developments have therefore moved toward microcontroller-based active circuit breakers in an effort to overcome these diagnostic limitations. However, early active variants still frequently encounter floating analog signal noise, ground bounce artifacts, and a pronounced lack of synchronized data-logging infrastructure, which collectively undermines their forensic value in production environments.

Specifically addressing these constraints, a prior foundational study successfully implemented a localized active protection framework driven by an Arduino Nano microcontroller [5]. The reported system integrated an LM35 precision thermal sensor for heatsink temperature monitoring and an INA219 digital current monitor for high-side load current measurement, both of which were validated through software calibration routines and further enhanced by a hybrid moving-average filtering technique designed to isolate raw sensor telemetry from electromagnetic interference (EMI) generated by the amplifier switching stage [5]. A digital OR-logic gate algorithm was executed locally on the microcontroller, ensuring that the output relay would instantly disconnect the speaker load whenever the predefined safety thresholds for temperature or current were breached [5]. Although this hardware-centric approach proved to be highly precise and robust for single-unit fault isolation, its architectural reliance on localized hardware processing and short-range wired serial communication introduced a fundamental limitation in terms of scalability and remote observability. As modern audio infrastructures rapidly transition into large-scale smart buildings, distributed event venues, and multi-zone commercial complexes, a fully decentralized approach becomes increasingly insufficient to support multi-zone remote surveillance, wide-area diagnostic grouping, coordinated cross-channel shutdown, and rapid centralized operator intervention during emergencies.

The progressive convergence of the Internet of Things (IoT) paradigm into industrial automation provides an attractive opportunity to elevate audio hardware protection from a stand-alone safety circuit into a fully cloud-integrated monitoring ecosystem [6–8]. By leveraging high-performance microcontrollers equipped with native wireless connectivity, such as the dual-core ESP32 platform, physical telemetry signals can be wirelessly transmitted across networked environments and consolidated within a centralized supervisory dashboard [9]. Nevertheless, transitioning a safety-critical real-time protection mechanism from local microcontroller pins to a centralized IoT architecture inevitably introduces a new class of complex network-layer challenges. Offloading the decision-making safety logic to a centralized server or an interactive dashboard inherently introduces additional network latency, occasional packet loss, and transmission jitter over wireless communication layers such as the Message Queuing Telemetry Transport (MQTT) protocol operating over TCP/IP [10, 11]. In a centralized environment, excessive delay in transmitting a “Cut-Off” command from the central server back to the actuator node could allow an overcurrent state to persist long enough to inflict permanent thermal damage on the output MOSFETs. Therefore, a rigorous and statistically valid evaluation of round-trip network latency becomes a strict safety requirement rather than a mere quality-of-

service metric [12, 13]. Furthermore, long-term deployment of remote IoT nodes introduces software sustainability challenges, because manual firmware flashing through physical USB or UART cables becomes highly inefficient, time-consuming, and operationally expensive once the units have been installed inside sealed amplifier racks, embedded ceiling panels, or distributed across geographically distant venues [14–16].

To systematically bridge these identified research gaps, the present study proposes the implementation of a *Centralized IoT Safety Latching Protection System* for Class-D power amplifiers, built around the ESP32 microcontroller and the MQTT communication protocol. Departing from the previous localized processing paradigm reported in [5], this research deliberately shifts the computational execution of the digital OR-logic algorithm to a centralized Python-based server, while simultaneously optimizing the edge node solely for high-frequency telemetry acquisition and command actuation [17]. The primary contributions and novelties of this research are threefold and may be summarized as follows:

1. **Centralized Safety-Latching Architecture.** This study designs a centralized safety-latching framework that structurally prevents the occurrence of dangerous power oscillations and auto-reclosing loops by enforcing a mandatory *LATCHED_OFF* state, which can only be cleared through a manual operator-driven reset issued from the graphical user interface (GUI).
2. **Empirical MQTT Latency Characterization.** This study provides a comprehensive network latency performance analysis, including statistical metrics such as mean, standard deviation, and 95% confidence intervals, in order to map the empirical timing boundaries of MQTT-driven protection commands under varying network signal strength conditions [18, 19].
3. **OTA Firmware Lifecycle Integration.** This study integrates an Over-The-Air (OTA) firmware update lifecycle management system using secure cloud-hosted repositories, ensuring that wireless software maintenance, threshold reconfiguration, and security patching can be performed remotely throughout the operational lifetime of the device [20–22].

The remainder of this paper is organized as follows. Section II systematically details the embedded hardware integration, the centralized software logic flowchart, the formulation of the MQTT communication topics, and the OTA update mechanism. Section III presents the empirical results of sensor calibration and accuracy validation, the verification of the centralized latching algorithm, and a detailed discussion of the observed network latency characteristics across multiple signal regimes. Finally, Section IV concludes the paper, summarizes the principal findings, and outlines several promising directions for future development, particularly with respect to cryptographic hardening of the OTA channel.

II. Research Methods

This research employs a comprehensive quantitative experimental framework by designing an advanced embedded Internet of Things (IoT) ecosystem. The developed architecture intelligently bridges hardware-level telemetry acquisition with a centralized Python-based analytical server to execute active protection mechanisms for Class-D audio power amplifiers. To provide a systematic understanding of the system operational workflow, the methodology is divided into four primary subsections: hardware architecture, centralized protection logic, network communication protocols, and firmware lifecycle management.

i. Hardware Architecture and Sensor Integration

The fundamental hardware architecture operates on a closed-loop topology that physically separates the low-voltage logic control domain from the high-voltage audio amplification circuit. As illustrated in Figure 1, the core data acquisition and communication node is driven by the ESP32 microcontroller. The ESP32 is specifically selected because of its dual-core processing capability, integrated Wi-Fi transceiver, and robustness in handling continuous IoT data streams in electromagnetically noisy environments [9].

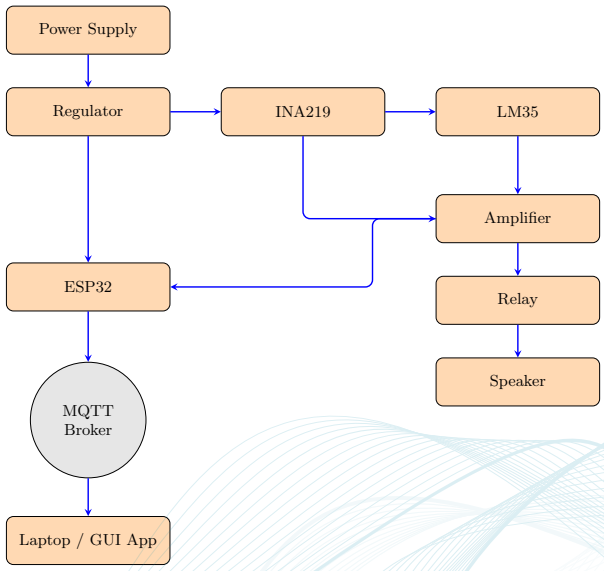

Figure 1: System block diagram of the centralized IoT safety latching protection system.

To ensure high-fidelity telemetry acquisition, the hardware node incorporates two precision sensors powered by a stable LM2596 step-down converter set to 5 V to mitigate potential voltage sag during heavy audio reproduction. For electrical load monitoring, an INA219 digital current and power monitor is deployed in a high-side series configuration. This sensor communicates directly with the ESP32 through the I2C protocol, which is highly resistant to analog signal degradation and electromagnetic interference (EMI) commonly found in high-power audio chassis. Meanwhile, the thermal condition of the amplifier heatsink is continuously monitored using an LM35 precision analog temperature sensor connected to the Analog-to-Digital Converter (ADC) pin of the ESP32.

For electromechanical actuation, a single-channel relay module is employed as an active circuit breaker. Operating in an Active Low configuration, the relay functions as a normally closed (NC) gate that defaults to a cut-off state when the logic control loses power, thereby ensuring a fail-safe operating condition. The complete physical interconnection of these components is presented in Figure 2.

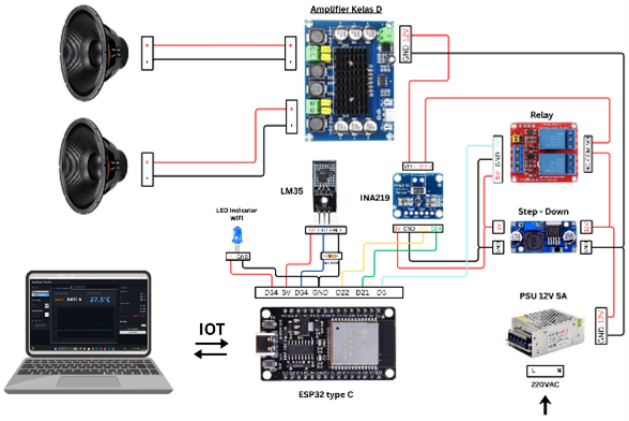

Figure 2: Protection system circuit schematic.

ii. Software Design and Centralized Protection Logic

The raw analog telemetry acquired by the ESP32 must be mathematically converted into readable physical units before transmission. The voltage output from the LM35 thermal sensor, denoted as V_{ADC}, is processed by the 12-bit ADC of the ESP32, which operates using a 3.3 V reference voltage, into a digital temperature value T. The temperature conversion formula is shown in Equation (1).

$$T\,(^{\circ}\text{C}) = \left(\frac{V_{\text{ADC}}}{4095} \times 3.3\right) \times 100 \tag{1}$$

Meanwhile, the electrical current I is internally calculated by the INA219 module by measuring the voltage drop across a precision shunt resistor R_{shunt} using Ohm's law, as expressed in Equation (2).

$$I = \frac{V_{\text{shunt}}}{R_{\text{shunt}}} \tag{2}$$

To eliminate transient signal noise that could cause false triggering, the processed data are subjected to a hybrid filtering mechanism using a moving average algorithm with a sample size of $N = 10$ before being published to the network [8]. Unlike conventional decentralized systems that process safety instructions locally, this study shifts the computational burden of the protection algorithm to a centralized Python-based Graphical User Interface (GUI) server. The server continuously evaluates the incoming filtered telemetry against strictly predefined safety thresholds, namely a maximum allowable temperature T_{max} of 70°C and a maximum load current I_{max} of 3.0 A.

These thresholds are mathematically and empirically justified. The T_{max} boundary prevents the silicon MOSFETs from exceeding their Safe Operating Area (SOA) to mitigate thermal degradation, while the I_{max} limit ensures that continuous power dissipation across a standard 8-ohm speaker voice coil remains below its physical deformation threshold. The automated decision-making process is governed by a digital OR logic gate structure. The protection state, denoted as $Trip$, is formulated in Equation (3).

$$Trip = (T_{\text{val}} \geq T_{\text{max}}) \vee (I_{\text{val}} \geq I_{\text{max}}) \tag{3}$$

If the condition in Equation (3) evaluates to true, or Logic 1, the Python server immediately transmits a Cut-Off command back to the ESP32 to disconnect the relay. After successful disconnection, the centralized server enters a *LATCHED_OFF* security state. In this critical mode, the system deliberately prevents automatic power restoration or auto-reclosing even when sensor readings return to normal conditions. The system requires a manual RESET command executed by an authorized operator through the GUI to resume operation. This latching philosophy is essential for preventing destructive power oscillations that may damage speaker voice coils during intermittent faults [23, 24]. The complete operational sequence of this centralized safety mechanism is visualized in Figure 3.

iii. MQTT Communication Protocol and Latency Metrics Formulation

The bidirectional data exchange between the ESP32 edge node and the Python centralized server is facilitated by the Message Queuing Telemetry Transport (MQTT) protocol [25]. Operating over the

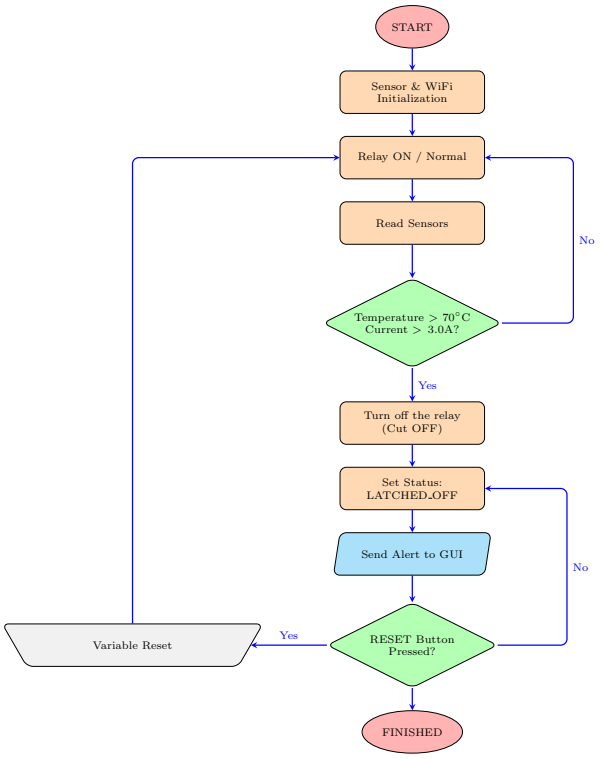

Figure 3: System algorithm flowchart of the centralized safety latching mechanism.

TCP/IP layer, MQTT applies a lightweight publish-subscribe model that minimizes bandwidth consumption and supports efficient communication in IoT infrastructures [6]. The proposed system is structured using hierarchical topic routing. The ESP32 periodically publishes JSON-formatted telemetry to the `smartamp/data` topic, while simultaneously subscribing to the `smartamp/control/relay` topic to receive instantaneous execution commands from the server.

Because the critical safety logic is hosted centrally, evaluating network reliability becomes mandatory. Therefore, this study conducts a rigorous network latency analysis [18]. In this context, latency is defined as the total round-trip time required from the moment a fault is detected by the Python server until the physical relay successfully disconnects the audio load. High network reliability and minimal latency are primary indicators of the feasibility of implementing a centralized protection mechanism over wireless networks.

iv. Firmware Lifecycle Management and OTA Update Mechanism

One of the most persistent challenges in maintaining remote industrial IoT devices is the requirement for physical cable intervention during software troubleshooting. To ensure long-term sustainability and scalability, the proposed system integrates an Over-The-Air (OTA) firmware lifecycle management protocol [14, 21].

The ESP32 microcontroller is programmed with a self-diagnostic routine that periodically queries a designated cloud repository, such as GitHub, through a secure HTTP connection. The ESP32 downloads a plain text versioning file, namely `version.txt`, and compares the remote version string with the currently running firmware build. If a higher firmware version is detected, the microcontroller initiates an automated OTA sequence. The device fetches the compiled `.bin` binary file, verifies the data integrity using checksum validation to prevent corrupted installation, and securely flashes the new program into the secondary OTA memory partition [15]. After a successful writing process, the system automatically restarts and boots from the newly updated partition.

This remote maintenance capability enables engineers to deploy security patches, modify trigger thresholds, and optimize network parameters without dismantling the amplifier chassis. Therefore, the proposed OTA mechanism significantly reduces maintenance costs and operational downtime while improving the long-term maintainability of the centralized IoT protection system.

III. Results and Discussion

This section presents the empirical findings and comprehensive technical analysis used to evaluate the physical and operational performance of the proposed centralized IoT-based protection system. The analysis covers hardware integration, sensor conversion accuracy, centralized logic validation, MQTT network latency characteristics, and wireless firmware sustainability.

i. Hardware Architecture and Sensor Integration

The physical integration of the prototype was successfully realized into a compact, field-deployable protection enclosure. As shown in Figure 4, the ESP32 Type-C core, INA219 digital sensor, LM35 analog temperature sensor configuration, and electromechanical relay assembly were structurally consolidated on a high-density printed circuit layout.

During the integration phase, strict compliance with Electromagnetic Compatibility (EMC) guidelines was enforced. A significant physical separation was maintained between the high-power switching domain, including the Class-D amplifier power supply and speaker output lines, and the low-voltage control domain, including the ESP32 GPIO logic and sensor signal traces. This routing design is essential to prevent high-frequency electromagnetic noise generated by the amplifier output stages from cross-coupling into the

Figure 4: Hardware realization of the centralized IoT protection prototype.

sensitive I2C digital bus or the analog-to-digital converter (ADC) tracks. Consequently, the physical isolation shown in Figure 4 prevents false-triggering anomalies and ensures continuous operational stability under heavy power delivery.

ii. Sensor Calibration and Accuracy Validation

To establish the baseline reliability of the diagnostic telemetry, rigorous calibration and accuracy testing were conducted under varying operational loads. The raw data acquired by the ESP32 and transmitted to the centralized Python GUI were benchmarked against calibrated industrial instruments, namely a True-RMS digital multimeter for current validation and a high-precision digital industrial thermometer for thermal monitoring.

The empirical results for the thermal validation using the LM35 sensor are presented in Table 1. Three critical operational points were monitored, representing cold standby at 30°C, standard operating conditions at 50°C, and an artificially induced overheating state at 75°C.

The quantitative data in Table 1 indicate an excellent linear tracking capability of the LM35 thermal subsystem, maintaining an average measurement error below 1%. The marginal deviation observed is mathematically negligible and remains within the nominal component tolerance. More importantly, at the third test point of 75.0°C, the centralized system immediately detected that the threshold $T_{max} = 70$°C had been exceeded. As a result, the system responsively executed a TRIP state to mitigate potential thermal runaway within the switching transistors.

Table 1: Thermal Acquisition Accuracy and Protection Response. T_{ref}: Reference Temperature; T_{meas}: Measured GUI Temperature; ΔT: Deviation; %Err: Percentage Error.

No.	T_{ref} (°C)	T_{meas} (°C)	ΔT (°C)	%Err	Status
1	30.0	30.2	0.2	0.67	Normal
2	50.0	49.5	-0.5	1.00	Normal
3	75.0	75.1	0.1	0.13	TRIP

Concurrently, the acquisition precision of the high-side INA219 digital current sensor was evaluated by applying dynamic impedance loads to the Class-D output. The current measurement comparison is presented in Table 2.

Table 2: Current Telemetry Precision and Isolation Evaluation. I_{ref}: Reference Current; I_{meas}: Measured GUI Current; ΔI: Deviation; %Err: Percentage Error.

No.	I_{ref} (A)	I_{meas} (A)	ΔI (A)	%Err	Status
1	0.50	0.47	-0.03	6.00	Normal
2	2.00	2.05	0.05	2.50	Normal
3	3.50	3.48	-0.02	0.57	TRIP

The analysis of Table 2 reveals highly reliable tracking performance from the INA219 module. A higher percentage error of 6.00% was observed at the low-current boundary of 0.50 A. This condition is a known mathematical characteristic resulting from the quantization limits of the internal Programmable Gain Amplifier (PGA) of the INA219 when reading minimal shunt voltages. However, as the current increased toward the critical threshold, the accuracy improved significantly, reaching an error rate of only 0.57% at 3.50 A. Upon reaching 3.48 A, which confirmed the breach of the $I_{max} = 3.0$ A threshold, the system responded immediately by triggering the isolation relay, thereby protecting the speaker voice coil.

iii. Centralized Safety Latching Logic Verification

The core structural novelty of this study lies in verifying the digital OR logic gate algorithm hosted centrally on the Python server. To test the robustness of this architecture, four distinctive operational fault scenarios

were simulated. The behavioral responses of the system logic are summarized in Table 3.

Table 3: Logic Verification Matrix for Centralized Fault Scenarios

Scenario	Temperature State	Current State	Combined OR Output	Centralized System Status
Normal	False ($< 70^{\circ}C$)	False (< 3.0 A)	Logic 0	Online / Safe
Overheat	True ($\geq 70^{\circ}C$)	False (< 3.0 A)	Logic 1	LATCHED_OFF
Overcurrent	False ($< 70^{\circ}C$)	True (≥ 3.0 A)	Logic 1	LATCHED_OFF
Dual Fault	True ($\geq 70^{\circ}C$)	True (≥ 3.0 A)	Logic 1	LATCHED_OFF

The empirical matrix in Table 3 demonstrates that the digital OR gate operating on the server functions effectively. Any individual or combined breach of the safety parameters immediately transitions the system into a secure *LATCHED_OFF* mode. The significant advantage of this centralized latching logic is visually recorded in the GUI monitoring dashboard shown in Figure 5.

Figure 5: TRIP/Cut-off Python GUI dashboard.

As demonstrated in Figure 5, once a fault triggers a trip condition, the relay remains locked in the OFF position indefinitely, even after the physical parameters cool down or the current drops back to zero. By forcing the system to maintain a permanent disconnected state until a manual authenticated RESET command is received from the operator interface, the framework eliminates the risk of destructive power oscillations, namely rapid and unmanaged on-off cycling, which commonly damages audio hardware during intermittent short circuits.

iv. MQTT Network Performance and Latency Analysis

To ensure statistical reliability regarding wireless network behavior, latency testing was expanded to 50 operational cycles across three different network conditions based on the Received Signal Strength Indicator (RSSI): strong signal above -50 dBm, medium signal from -50 to -70 dBm, and weak signal below -70 dBm. The statistical findings, including standard deviation σ and 95% confidence interval, are presented in Table 4.

Table 4: MQTT Round-Trip Latency Performance Based on 50 Test Cycles. Note: RSSI = Received Signal Strength Indicator; N = Sample Size; μ_L = Mean Latency; σ = Standard Deviation; J = Jitter; 95% CI = 95% Confidence Interval of the mean.

Network Condition (RSSI)	N	μ_L (ms)	σ (ms)	J (ms)	95% CI (ms)
Strong (> -50 dBm)	50	34.6	2.1	1.5	[34.0, 35.2]
Medium (-50 to -70 dBm)	50	48.2	4.8	3.2	[46.9, 49.5]
Weak (< -70 dBm)	50	85.4	14.5	11.8	[81.4, 89.4]

The statistical expansion in Table 4 confirms that under optimal and medium network conditions, the centralized system reliably executes a protection cut-off in under 50 ms. Even under weak signal conditions, the observed mean latency of approximately 85.4 ms remains sufficiently fast to isolate the audio load before critical semiconductor meltdown occurs, which typically requires sustained fault exposure exceeding 200 ms.

Finally, to quantitatively establish the novelty and architectural improvement of the proposed system, Table 5 presents a head-to-head comparison with the prior localized hardware study [5].

Table 5: Quantitative Comparison Between Prior Work and the Proposed System

Feature / Metric	Prior Study [5]	Proposed System
Architecture	Decentralized (Local)	Centralized IoT (Cloud/Server)
Microcontroller	Arduino Nano	ESP32 (Dual-Core)
Protection Logic	Embedded hardware level	Python GUI server with OR logic
Remote Monitoring	None (wired data logger)	Real-time MQTT dashboard
Maintenance	Manual physical flashing	Over-The-Air (OTA) wireless update
Isolation Response	≈ 2 ms (hardware interrupt)	≈ 34.6 ms (network latency)

As shown in Table 5, although the centralized architecture inherently introduces a minor network transmission delay compared to direct hardware interrupts, it successfully resolves the scalability limitations of the prior study by enabling wide-area surveillance and wireless maintenance capabilities.

v. OTA Firmware and Sustainability Evaluation

The final scenario focused on testing long-term technology sustainability through the remote Over-The-Air (OTA) firmware lifecycle updater script. During the evaluation, a modified firmware binary file, namely `Firmware_V1.1.bin`, was uploaded to the designated GitHub repository cloud infrastructure.

The embedded self-diagnostic block within the ESP32 successfully initiated an automated background request, retrieved the cloud-hosted `version.txt` file, and detected the version mismatch without causing any lag or interruption to the primary telemetry loop. The microcontroller then downloaded the updated binary payload, verified its cryptographic checksum integrity,

and flashed the program directly into the secondary partition. After a successful software writing operation, the ESP32 executed an automated warm reboot and loaded the newly updated firmware parameters seamlessly.

This successful deployment confirms that long-term software maintenance, threshold adaptation, and bug patching can be conducted wirelessly, thereby eliminating physical maintenance overhead and machinery downtime in complex commercial installations. However, it is important to acknowledge the current security boundaries of the proposed OTA mechanism. The system currently uses standard HTTP channels and relies solely on cryptographic checksums to ensure data integrity against corrupted downloads. Because the current design lacks digital signature authentication, such as HTTPS/TLS code signing, the architecture remains theoretically vulnerable to malicious firmware injection. Therefore, upgrading the OTA protocol with robust cryptographic authentication remains a critical focus for future development to ensure deployment viability in high-risk industrial environments.

IV. Conclusion

The implementation of a centralized Internet of Things (IoT) safety latching protection system for Class-D power amplifiers has been successfully realized and empirically validated. By shifting the computational execution of the digital OR logic algorithm from a local microcontroller to a centralized Python-based server, the system achieved a robust and remotely accessible diagnostic framework. Experimental results demonstrated high precision in telemetry acquisition, with the LM35 thermal sensor and INA219 current monitor producing average measurement errors of less than 1% and 2%, respectively.

The centralized safety latching algorithm operated reliably, successfully disconnecting the amplifier load when the operational parameters exceeded the predefined critical thresholds, as tested at 75.1°C and 3.48 A. By enforcing a mandatory *LATCHED_OFF* state, the proposed architecture proved effective in preventing destructive power oscillations and auto-reclosing loops, ensuring that power restoration can only occur after a manual authenticated operator reset.

Furthermore, the comprehensive network latency analysis confirmed the viability of this centralized approach. The total round-trip isolation delay averaged 34.6 ms under optimal conditions and remained responsive, with a maximum mean latency of 85.4 ms under weak signal conditions. These results indicate that the system can provide a protective response within the required safety margins to prevent semiconductor degradation over a wireless network.

Finally, the successful integration of the Over-The-Air (OTA) updater validates the long-term sustainability of the system. The proposed framework enables administrators to deploy firmware patches and adjust safety thresholds wirelessly without physical hardware intervention. Overall, this research provides a responsive, data-driven, and maintainable preventive protection solution for modern high-power audio infrastructures.

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Electrical Engineering at Universitas Pamulang for providing the laboratory facilities, technical equipment, and continuous academic support necessary to conduct this research. Special appreciation is also extended to all colleagues and researchers who provided constructive feedback during the development of the prototype and the preparation of this manuscript.

References

[1] J. Altet, X. Aragones, E. Barajas, X. Gisbert, S. Martínez, and D. Mateo, "Aging compensation in a class-a high-frequency amplifier with dc temperature measurements," *Sensors*, vol. 23, no. 16, 2023. https://doi.org/10.3390/s23167069

[2] S. Rubio, S. Bogarra, M. Nunes, and X. Gomez, "Smart grid protection, automation and control: Challenges and opportunities," *Applied Sciences (Switzerland)*, vol. 15, no. 6, 2025. https://doi.org/10.3390/app15063186

[3] B. Paliwoda, W. Krzysztof, and M. Biega, "Challenges and opportunities — a review," *Energies*, vol. 15, no. 1806, 2022.

[4] V. P. Mateichyk and A. V. Navrotskyi, "Systematization of hardware schemes of vehicle operation monitoring systems," *Reporter of the Priazovskyi State Technical University. Section: Technical Sciences*, no. 48, pp. 184–192, 2024. https://doi.org/10.31498/2225-6733.48.2024.310711

[5] G. Firasanto, Andriani, and Kiswanta, "Performance analysis of logic gate-based power amplifier protection with hybrid filtering," *PROtek: Jurnal Ilmiah Teknik Elektro*, vol. 13, no. 2, pp. 110–115, 2026. https://doi.org/10.33387/protk.v13i2.11567

[6] A. Dubey and S. K. Yadav, "Basics of internet of things," *Interantional Journal of Scientific Research in Engineering and Management*, vol. 08, no. 10, pp. 1–6, 2024. https://doi.org/10.55041/ijsrem37970

[7] P. Raja, S. Kumar, D. S. Yadav, and T. Singh, "The internet of things (iot): A review of concepts, technologies, and applications," *International Journal of Information Technology and Computer Engineering*, no. 32, pp. 21–32, 2023. https://doi.org/10.55529/ijitc.32.21.32

[8] H. T. Gaikwad, N. R. Kamble, S. P. Kamble, P. S. Kamble, S. S. Jadhav, and S. V. Kothawale, "Supervisory performance of monitoring of industrial machines and faults monitoring using iot," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*,

vol. 13, no. VII, pp. 425–427, 2025. https://doi.org/10.22214/ijraset.2025.72965

[9] A. P. Pangarkar, S. Shabadi, and P. G. Gawande, "A comprehensive analysis of esp32 microcontroller for iot applications," *International Journal of Novel Research and Development*, vol. 10, no. 10, pp. 501–505, 2025. https://doi.org/10.56975/ijnrd.v10i10.310100

[10] S. B. Bhaskoro, H. Supriyanto, B. B. Aji, and B. Pamungkas, "Perbandingan performansi latency protokol komunikasi http dan mqtt pada internet of things," *JTT (Jurnal Teknologi Terapan)*, vol. 8, no. 2, p. 82, 2022. https://doi.org/10.31884/jtt.v8i2.309

[11] J. Roldán-Gómez, J. Carrillo-Mondéjar, J. M. Castelo Gómez, and S. Ruiz-Villafranca, "Security analysis of the mqtt-sn protocol for the internet of things," *Applied Sciences (Switzerland)*, vol. 12, no. 21, 2022. https://doi.org/10.3390/app122110991

[12] F. C. Kusuma, N. B. A. Karna, and A. I. Irawan, "Analisis perbandingan quality of services (qos) protokol http dan mqtt pada sistem monitoring berat ayam broiler berbasis iot," *Jurnal Nasional SAINS dan TEKNIK*, vol. 2, no. 1, pp. 16–22, 2024. https://doi.org/10.25124/jnst.v2i1.7987

[13] F. P. E. Putra, F. Muslim, N. Hasanah, Holipah, R. Paradina, and R. Alim, "Analisis komparasi protokol websocket dan mqtt dalam proses push notification," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, pp. 63–72, 2024. https://doi.org/10.60083/jsisfotek.v5i4.325

[14] A. Kesari, "Firmware in flight: A deep dive into ota update mechanisms for iot," *International Journal of Research in Applied Science and Engineering Technology*, vol. 13, no. 5, pp. 1254–1268, 2025. https://doi.org/10.22214/ijraset.2025.69655

[15] M. La Manna, L. Treccozzi, P. Perazzo, and S. Saponara, "Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update," *Sensors*, vol. 21, no. 2, p. 515, 2021. https://doi.org/10.3390/s21020515

[16] A. Bhattacharjee, H. Mahmood, S. Lu, N. Ammar, A. Ganlath, and W. Shi, "Edge-assisted over-the-air software updates," 2023.

[17] A. Jamshidpey, M. Wahby, M. Allwright, W. Zhu, M. Dorigo, and M. K. Heinrich, "Centralization vs. decentralization in multi-robot sweep coverage with ground robots and uavs," *Artificial Life and Robotics*, 2025. https://doi.org/10.1007/s10015-025-01049-7

[18] L. Nurfiqin, Z. Sari, and F. D. S. Sumadi, "Analisis quality of service (qos) protokol mqtt dan http pada sistem smart metering arus listrik," *Jurnal Repositor*, vol. 3, no. 1, pp. 121–130, 2024. https://doi.org/10.22219/repositor.v3i1.31040

[19] F. Palmese, A. E. C. Redondi, and M. Cesana, "Adaptive quality of service control for mqtt-sn," *Sensors*, vol. 22, no. 22, 2022. https://doi.org/10.3390/s22228852

[20] A. Shoker, F. Alves, and P. Esteves-Verissimo, "Scaiota: Scalable secure over-the-air software updates for vehicles," in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2023, pp. 151–161. https://doi.org/10.1109/SRDS60354.2023.00024

[21] Q. Zhang, Y. He, Y. Xiao, X. Zhang, and C. Song, "Ota-key: Over-the-air key management for flexible and reliable iot device provision," *IEEE Transactions on Network and Service Management*, vol. 22, no. 2, pp. 2106–2119, 2025. https://doi.org/10.1109/TNSM.2024.3515212

[22] Z. Fauziah, N. P. Anggraini, Y. P. A. Sanjaya, and T. Ramadhan, "Enhancing cybersecurity information sharing: A secure and decentralized approach with four-node ipfs," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 153–159, 2023. https://doi.org/10.34306/ijcitsm.v3i2.139

[23] P. S. S. T, "Iot based real-time fault detection and protection in power transformers," *International Journal For Multidisciplinary Research*, vol. 7, no. 2, pp. 1–4, 2025. https://doi.org/10.36948/ijfmr.2025.v07i02.42068

[24] M. J. Naikwadi, A. A. Mali, R. S. Gavade, and D. S. Gavali, "Iot-based three phase motor protection system with remote monitoring," *International Journal For Research in Applied Science and Engineering Technology (IJRASET)*, vol. 14, no. III, pp. 2229–2231, 2026. https://doi.org/10.22214/ijraset.2026.78360

[25] A. Kurnianto, J. D. Irawan, and F. X. Ariwibisono, "Penerapan iot (internet of things) untuk controlling lampu menggunakan protokol mqtt berbasis web," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 6, no. 2, pp. 1153–1161, 2023. https://doi.org/10.36040/jati.v6i2.5393