International Journal of Modern Developments in Engineering and Science
Volume 5, Issue 4, April 2026
www.ijmdes.com | E-ISSN: 2583-3138 | RESAIM Publishing | www.resaim.com

IoT Safety Ecosystem for Electrical Hazard Mitigation

Virendra Swaroop Sangtani[1], Abhishek Kumar[1*], Kanishka Choudhary[1], Khushi Chouhan[1], Kuldeep Gurjar[1]
[1]*Department of Electrical Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, India*

***Abstract*: Conventional electrical protection relies on basic overcurrent detection, leaving low-voltage networks vulnerable to unseen hazards like localized thermal degradation and stray voltage. This research introduces a multi-parameter hazard mitigation system based on the Internet of Things (IoT) to overcome this significant deficiency. The architecture employs an ESP32 microcontroller along with sensors for current (ACS712), temperature (DHT11), flammable gas (MQ-2), and a custom electromagnetic field probe for non-contact stray voltage detection. This design's primary benefit is its dual- layer protection: local control logic functions autonomously from the Blynk IoT cloud, ensuring rapid circuit isolation during internet disruptions. MATLAB/Simulink validations confirm that the system reliably identifies asymmetrical short circuits and dangerous enclosure voltages, issuing a control trip command in approximately 4 milliseconds, initiating rapid physical disconnection to prevent equipment damage and fatal injuries.**

***Keywords*: Internet of Things (IoT), Electrical Hazard Mitigation, Overcurrent Protection, Stray Voltage Detection, Embedded Monitoring Systems, ESP32.**

1. Introduction

The electrical system of our homes and businesses is critically important to everyday life, while many potential dangers lurk within that very system, such as faulty insulation, unaccounted-for stray voltage, and gas leaks gradually working their way into our living and working areas. If not corrected, these minor issues can lead to major structural fires and thousands of deaths due to electrical shock every year across India [10].

Finding these dangers early is crucial. Despite this, most facilities still depend almost entirely on basic fuses and circuit breakers. Since these devices are built to trigger only during massive power failures, they are essentially blind to slow, low-intensity threats. Engineers are trying to fix this visibility gap by putting smart Internet of Things (IoT) sensors into power grids to monitor systems remotely and lower electrical losses [2], [9], [12], [16]. Furthermore, the integration of embedded microcontrollers has proven highly effective in localizing automated safety and control tasks [11], [13], [14]. The issue is that most current IoT setups only watch one metric at a time, like temperature or current alone. Tracking just one variable misses the bigger picture, allowing complex, combined hazards to quietly escalate.

To tackle this flaw, this project introduces a multi-parameter IoT Electrical Hazard Mitigation System that spots threats before they spiral out of control. To monitor these diverse risk factors, a set of hardware components work together: a Current Sensor (ACS712), a humidity/temperature sensor (DHT11), and a flammable gas sensor (MQ-2). To detect any stray or non-contact voltage on metal surfaces, the hardware design integrates a custom antenna specifically for electromagnetic field detection [4]. This design function is primarily ignored in most commercial designs, which contributes to undetected shock hazards. The transmitting unit uses a central microcontroller to gather information from all of the hardware sensors. Once all of the information is collected, it is then sent to the Blynk Cloud for the generation of a real-time display and immediate notifications via smart device to the user. A combination of environmental sensing and electrical monitoring provides a high level of preventive protection against a severe electrical accident.

2. Literature Review

As electrical networks undergo many threats, there are three particular structural threats; degraded insulation, overloaded circuits and deteriorating physical connections. Many of today's electrical fires and electrical shock events are caused by one or more of these three structural issues. Recent research by Thai et al. [1] has shown that excess current and corroded wire insulation are primary factors in determining the fire risk associated with our electrical systems. The time has come for power companies to have continuous monitoring of their power grid's performance on a proactive basis vs reactive basis of circuit protection devices (fuses) only.

While new cloud analytics solutions provide valuable insight regarding long-term performance trends, researchers such as Ahmed et al. [6] have identified a fundamental flaw with their use; that is the reliance on the internet results in significant latencies which will delay any response to dangerous events until after they occur. Therefore, there is an immediate need to develop and integrate localized high-speed mitigation technologies to quickly respond to hazardous situations.

To build these localized safety nets, engineers are increasingly turning to isolated sensor architectures. Recent physical implementations heavily favor combining

*Corresponding author: akdoriya5401@gmail.com

microcontrollers with dedicated measurement modules. For instance, new developments in induction motor protection [8] and smart circuit breaker actuation [15] demonstrate how pairing an ESP32 chip with an ACS712 current sensor creates a highly reliable, isolated monitoring loop. Catarinucci et al. [3] and Zhang et al. [9] have similarly validated this approach, showing that mixing specific electrical and environmental sensors allows a system to catch complex, multi-variable faults early without interfering with the main power lines.

Despite these advances, a major blind spot in traditional monitoring remains the physical risk of the measurement itself. Attaching sensors directly to live wires degrades insulation over time and puts operators in danger. Haberman and Spinelli [4] addressed this exact problem by exploring noncontact voltage measurement techniques. Their work proves that using capacitive coupling to read alternating electric fields is both highly accurate and inherently safer. This contactless philosophy directly supports the inclusion of custom electromagnetic field (EMF) probes to detect stray enclosure voltage without physical wire tapping.

Finally, catching a fault locally is only half the battle; the end user actually needs to know about it. Early foundational work by Cagno et al. [7] emphasized that industrial safety setups must be user-centered to be effective. Building on this concept, Razzaque et al. [2] introduced smart energy frameworks that push real-time electrical parameters straight to cloud dashboards, drastically improving remote situational awareness. More recently, Vaheedha et al. [5] demonstrated the immense practical value of utilizing platforms like Blynk to send instant mobile push alerts. By keeping humans in the loop with accessible, readable data, these IoT interfaces trans- form raw sensor readings into immediate, actionable safety warnings.

3. System Architecture and Methodology

Our proposed system for mitigating electrical hazards, built using the internet of things (IoT) features a multi-layer modular design [9]. Even if there is no internet or Wi-Fi gets disconnected our system still works and trips the relay with millisecond-level latency, completely eliminating the unpredictable delays of cloud communication. The methodology is divided into three primary functional layers: real-time data acquisition, protection logic and circuit isolation, and IoT telemetry. To validate its real-world performance under severe faults, the architecture was further modeled using MATLAB/Simulink.

A. Real-Time Data Acquisition

The Central node of our multi-node architecture is ESP32-WROOM-32 microcontroller which integrates dual-core processing capability and built-in Wi-Fi communication [5]. It continuously collects data from our sensor network, evaluates safety conditions and then executes the mitigation commands when the safety threshold exceeds and also sends the real time data through WIFI through cloud to our IoT bylniot platform where live dashboard with clear visual charts is visible and alerts are received. To ensure comprehensive hazard detection, the system monitors four critical electrical and environmental parameters:

For physical isolation, the Strip = 0 command triggers an electromechanical relay module. Acting as an ideal switch, the relay instantly breaks the 230 V AC supply line. Since this decision bypasses cloud servers, the logic processing delay is evaluated via simulation to be approximately 4 ms, followed by the physical relay's electromechanical clearing time.

1) Overcurrent & Fault Detection: The ACS712 current sensor is used to track the load current passing through the electrical circuit. In proportion to the magnetic field created by the conductor current, the apparatus generates an analog voltage. This voltage signal is sampled by the analog- to-digital converter of the microcontroller to estimate the effective load current and identify abnormal overcurrent conditions [8].

2) Thermal Monitoring: To detect unusual thermal conditions, the DHT11 sensor measures the ambient temperature close to electrical wiring. Temperature variations are transformed by the sensor into a digital output signal that the controller can process directly. By continuously checking, the device can find overheating that is caused by damaged insulation or bad electrical connections [8].

3) Gas & Smoke Detection: Our MQ2 sensor detects smoke and flammable gases produced when insulation burns, and any abrupt increase in these gases warns of an impending fire threat. The detecting element changes its electrical resistance in the presence of flammable gases such as methane, hydrogen, and LPG. In order to detect possible fire hazards, the controller processes the measurable analog signal produced by these resistance variations [6].

4) Stray Voltage & Shock Protection: A specially designed non-contact electromagnetic field probe with a copper antenna is used to identify stray voltage risks. Through capacitive coupling, the antenna detects alternating electric fields generated by energized conductors [4]. The con- troller detects the induced signal when metallic equipment surfaces become inadvertently energized, allowing for the identification of possible electric shock conditions.

B. Protection Logic and Circuit Isolation

The actual fault isolation is handled purely at the local hardware level for maximum reliability. The microprocessor keeps checking the data it gets against strict safety limits. These limits are an RMS current (IRMS) of more than 10 A, an ambient temperature (T) of more than 60◦C, a gas detection state (G) of 1 or more, or a stray voltage (V_{stray}) of more than 30 V (a conservative safety margin well below the typical 50 V AC touch-safe limit defined in international standards). If any parameter violates its limit, the system launches an immediate trip sequence guided by the following Boolean equation for the active-low trip signal (S_{trip}):

$$S_{trip} = \begin{Bmatrix} 0\ if\ (I_{RMS} > 10)\ \vee (T > 60) \\ \vee\ (G = 1) \vee \left(V_{stray} > 30\right) \\ 1\ Otherwise \end{Bmatrix} \quad (1)$$

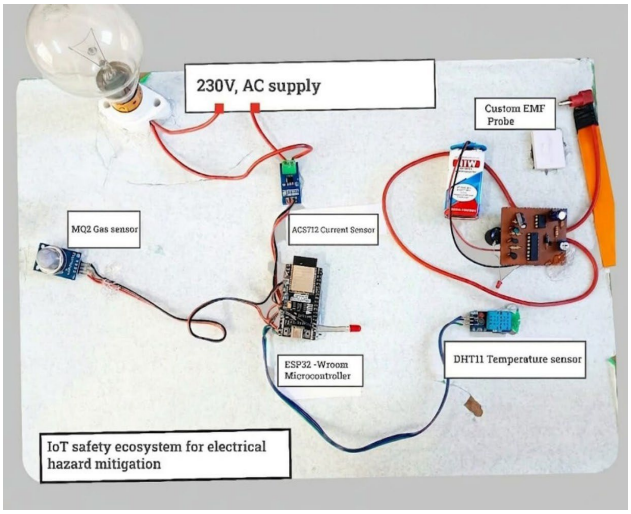

Fig. 1. Hardware architecture of the proposed IoT-based multi-layer hazard mitigation system

C. *IoT Telemetry and Remote Supervision*

The remote supervisory framework operates synchronously with the localised tripping mechanism. Current, temperature, and gas condition are among the real-time sensor data that our main node, ESP32, transmits via Wi-Fi from our sensor network. In addition to guaranteeing that primary hazard mitigation is independent of internet connectivity, our system instantly notifies the user via a mobile device or monitor of the type of fault state, alerting them to the need for prompt maintenance intervention [5].

D. *Simulation-Based Validation*

A mathematical model was created in MATLAB/Simulink (shown in Fig. 2) to thoroughly verify this protective logic under severe fault conditions.

A series R-L branch that represented a realistic distribution line impedance was used to mimic a 230 V, 50 Hz single-phase home supply. The continuous power system transients were modeled using the ode23t solver, which is optimised for stiff AC power systems, while discrete calculation blocks were used to mimic the ESP32's digital RMS processing. The physical relay was modelled as a controlled ideal switch. Two worst-case situations were assessed by the simulation: an independent stray voltage fault and an asymmetrical overcurrent fault. The mathematical findings validated the system for low-voltage danger reduction by confirming that the suggested architecture effectively identifies aberrant parameters and starts quick isolation.

4. Results and Discussion

The operational behavior of the proposed IoT-based Electrical Hazard Mitigation System was examined through dynamic simulations conducted in MATLAB/Simulink, alongside physical validation of the hardware prototype. The primary objective of this analysis was to verify whether the embedded protection logic can recognize hazardous electrical conditions, disconnect the power source within a sufficiently short time interval, and successfully transmit remote IoT alerts to prevent damage or injury.

A. *Overcurrent and Short-Circuit Protection Performance*

The first simulation investigated the system's response to a severe current surge caused by a short-circuit fault. Initially, the system operated under steady load conditions for a duration of two seconds, allowing the current waveform to stabilize and establish a reference operating state. At t = 2 s, a fault condition was purposefully introduced into the circuit to imitate an abrupt short circuit.

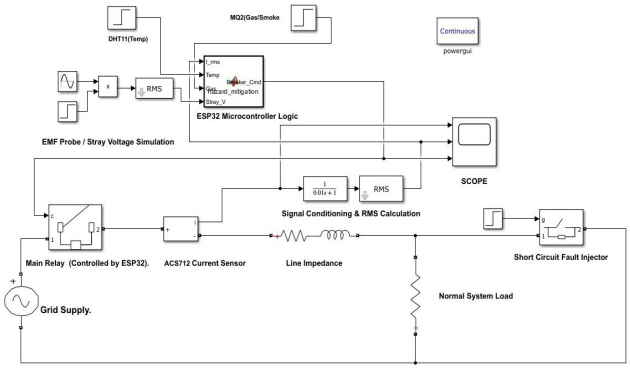

Fig. 2. MATLAB/Simulink model

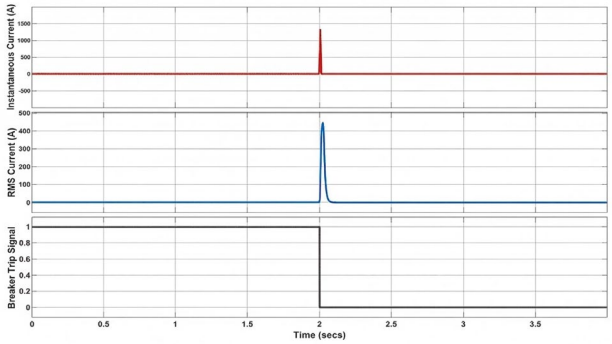

Fig. 3. Simulated current response during short-circuit fault and subsequent system isolation

According to the simulation results (illustrated in Fig. 3), the estimated RMS current exceeded the predefined safety limit of 10 A immediately following the fault occurrence. The control algorithm sent a trip instruction when it detected this threshold violation, which opened the relay switch and stopped power supply to the load. As a result of this activity, the current waveform fell to zero, indicating successful electrical isolation. In addition, a latching mechanism was included within the control logic to keep the disconnection status after the problem occurred. This prevents repeated switching operations that may otherwise occur if the fault condition persists. Such behavior is particularly important for ensuring safe system shutdown and preventing relay wear due to oscillatory switching.

B. *Transient Characteristics of the Fault Event*

A detailed transient analysis was conducted to better understand the instantaneous behavior of the system at the exact moment the fault was introduced.

The waveform (see Fig. 4) shows that the short circuit happened around the supply voltage's zero-crossing point. In these circumstances, the instantaneous peak current is greatly

increased by the DC offset component that inductive circuit parts create in the current waveform. According to the simulation, the current magnitude momentarily reached about 1300 A, which is indicative of the high electrical stress that can occur in low-impedance fault situations.

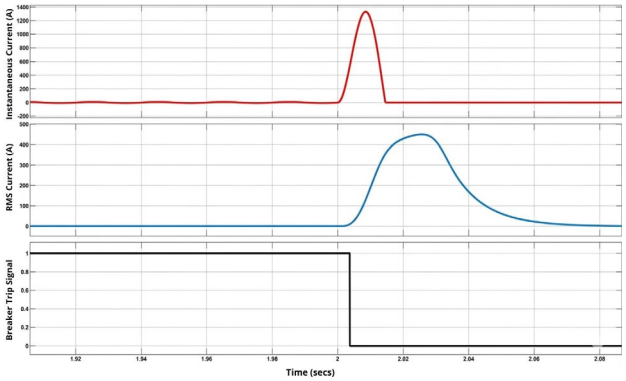

Fig. 4. High-resolution analysis of short-circuit current and controller response delay

Additionally, the timing analysis sheds light on the control algorithm's reaction time. The switching command was issued at roughly 2.004 s, which corresponds to a control logic reaction latency of almost 4 ms, even though the problem happened exactly at 2.000 s. This small delay depicts the microcontroller's practical computational sequence, which includes signal acquisition, RMS computation, and threshold comparison. Generating a trip signal in 4 ms is extremely quick. Even when accounting for the subsequent mechanical clearing time of a standard electromechanical relay, the total isolation speed functions well within the thermal withstand limitations (I2t) of typical PVC wiring, preventing long-term thermal damage.

C. *Stray Voltage Detection and Shock Prevention*

In addition to overcurrent protection, the system was evaluated for its ability to detect hazardous voltage levels appearing on exposed conductive surfaces. In this scenario, the load cur- rent was maintained at a safe operating value of approximately 1.3 A, representing normal device operation. At t = 2 s, a simulated stray voltage was applied to the equipment enclosure to mimic insulation failure or internal wiring faults.

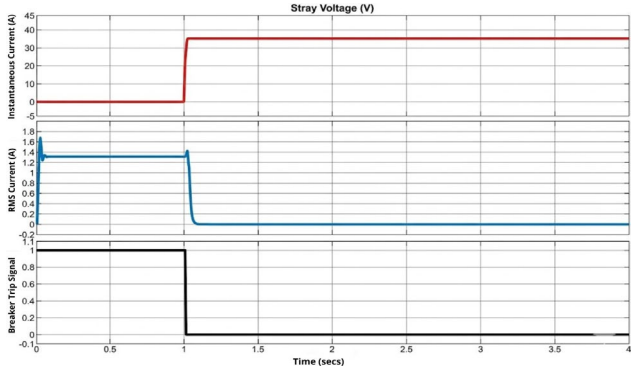

Fig. 5. System response to stray voltage fault during normal load conditions

As observed in Fig. 5, the EMF sensor circuit noticed a sudden increase in enclosure voltage, which reached around 35V. Because the protection algorithm defined 30V as a conservative touch-safe threshold—staying well below the typical 50V AC limit for low-voltage installations to prevent hazardous human exposure—the controller quickly recognized the condition as a potential shock danger. The controller instantly recognized the situation as a potential shock hazard.

The control logic prioritized human safety and ordered an emergency shutdown of the relay, thereby reducing the risk of electric shock, even if the load current was below the overcurrent limit. This experiment shows that the structure we suggested can identify electrical risks that conventional safety systems could miss, especially those caused by hazardous casing voltages rather than excessive current flow [4].

D. *Hardware Prototype and IoT Telemetry Validation*

To complement the mathematical simulation, the physical hardware prototype was tested under controlled conditions to validate the embedded control algorithm and the wireless re- mote supervisory framework. The ESP32 successfully acquired real-time data from the multi-parameter sensor suite, including the ACS712, DHT11, MQ-2, and the custom EMF probe.

Upon deliberate triggering of the safety thresholds (e.g., exposing the MQ-2 sensor to combustible gas limits or inducing a test overcurrent), the local electromechanical relay successfully isolated the 230 V test load, confirming the functional integration and reliability of the localized hardware logic. Concurrently, the remote alerting capabilities of the IoT telemetry module were assessed.

The ESP32 successfully sent the fault data over Wi-Fi to the Blynk loT cloud as soon as a threshold was crossed, as seen in Fig. 6. Instantaneous mobile push alerts were produced by the system, which correctly classified the particular hazard (e.g., noting whether the trip was caused by an overcurrent, a thermal breach, or a stray voltage shock hazard). This physical validation proves that the dual-layer architecture operates exactly as designed: it achieves immediate localized power isolation to protect equipment, while successfully providing remote facility managers with critical situational awareness via the cloud [5].

E. *System Performance Evaluation*

The combined simulation and physical hardware study confirms the robust characteristics of the proposed safety architecture. With response times on the order of milliseconds, the system effectively carried out quick threat detection and isolation, well within typical safety margins. Additionally, the incorporation of fault-latching logic prevented dangerous re-energization by guaranteeing stable shutdown behavior.

The architecture offers complete protection against both localized shock threats and high-current electrical fires by utilizing multi-parameter sensing. When compared to conventional single-parameter protection devices, these capabilities show that combining simultaneous IoT-enabled monitoring with embedded deterministic logic greatly increases electrical safety [2], [9], [13], [14].

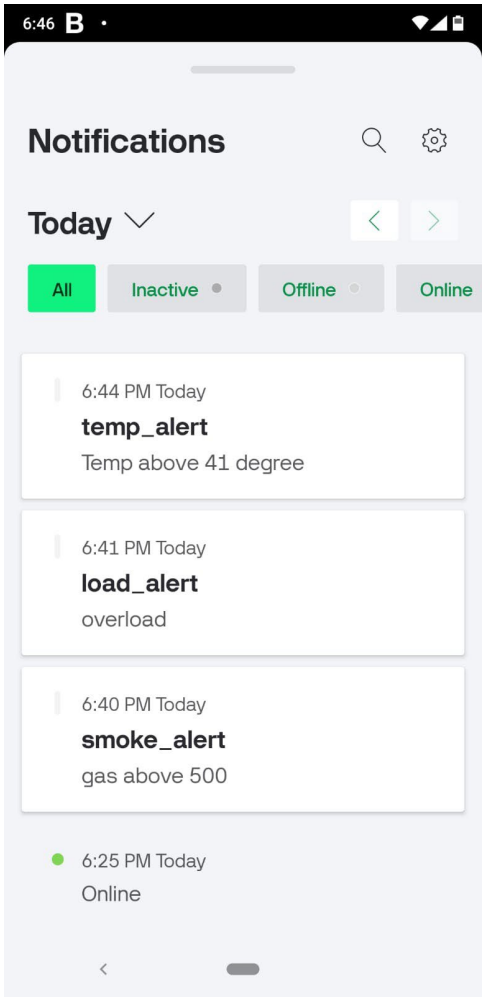

Fig. 6. Real-time IoT dashboard and mobile push notifications categorized by specific fault conditions

5. Conclusion

In order to overcome the shortcomings of traditional single-parameter protection devices, this work demonstrated the design, simulation, and hardware implementation of an Internet of Things-based electrical hazard mitigation system. In order to monitor electrical and environmental safety parameters, such as load current estimation, temperature conditions, the presence of combustible gases, and stray voltage detection using a custom electromagnetic field probe, the proposed architecture combines a ESP3 2–WROOM– 32 microcontroller with a multi-sensor framework. The suggested threshold-based protection logic's dependability was confirmed by simulation simulations conducted with MATLAB and Simulink. The findings show that, with a control logic processing latency of about 4 ms, the controller can identify potentially dangerous electrical situations and issue the trip command, initiating the physical isolation mechanism. Because of its quick reaction, the system can cut off the electrical load in the case of a serious short circuit or dangerous enclosure voltage conditions before serious harm or damage is done.

A key advantage of the proposed design is the separation of safety-critical mitigation logic from cloud-based monitoring. The protection algorithm operates locally within the hardware controller, ensuring that circuit isolation occurs even in the absence of network connectivity. At the same time, remote monitoring through the Blynk IoT platform provides real-time system visibility and fault notifications. This dual-layer architecture therefore combines deterministic hardware protection with IoT-based situational awareness for improved electrical safety.

6. Future Scope

Although the proposed prototype demonstrates the feasibility of the multi-parameter protection architecture for single- phase low-voltage systems, several opportunities exist for further development and large-scale deployment.

Future research may extend the protection framework to high-power electrical systems such as EV charging infrastructure and DC microgrids, where additional hazards such as DC arcing and battery thermal runaway must be considered. Integration with lightweight edge-based machine learning algorithms could also enable predictive fault detection by analyzing current waveform anomalies associated with insulation degradation or loose electrical connections.

Further improvements may include replacing mechanical relay switching with solid-state circuit breaker technologies based on wide-bandgap semiconductor devices such as silicon carbide or gallium nitride, enabling significantly faster fault isolation. Finally, the sensing and protection architecture can be expanded for three-phase industrial systems, enabling monitoring of induction motors and distribution networks through advanced current analysis techniques.

References

[1] H. D. Thai, N. B. V. Le, D. Lee, and J. H. Huh, "A survey of electrical fire causes assessment technology," *IEEE Access*, vol. 12, 2024.

[2] M. A. Razzaque *et al.*, "IoT-based smart energy monitoring system for smart homes," *IEEE Internet of Things Journal*, vol. 8, no. 3, 2021.

[3] L. Catarinucci *et al.*, "A smart IoT-based system for electrical fault detection and monitoring," *Sensors*, vol. 22, 2022.

[4] M. A. Haberman and E. M. Spinelli, "A noncontact voltage measurement system for power-line voltage waveforms," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 9, 2020.

[5] V. Sayyad *et al.*, "Smart energy meter with real-time monitoring and predictive bill calculation," *International Journal of Creative Research Thoughts*, 2025.

[6] M. F. Ahmed, M. R. A. Khan, and M. N. Islam, "Wearable and IoT-integrated solutions for electrical hazard prevention in industrial environments," *Journal of Artificial Intelligence General Science*, vol. 8, no. 1, 2025.

[7] E. Cagno, A. Neri, M. Macchi, and D. Accordini, "Safety++: Designing IoT and wearable systems for industrial safety through a user-centered design approach," in *Proc. Int. Conf. Safety in Industrial Plants*, 2017.

[8] E. A. Feukeu and S. Mbuyu, "Design and implementation of an IoT-based induction motor protection and control system using Arduino and ESP32," *Journal of Electrical Systems*, vol. 21, no. 1, 2025.

[9] Y. Zhang, Y. Chen, and H. Wu, "Smart electrical safety monitoring using IoT sensor networks," *Sensors*, vol. 22, no. 14, p. 5210, 2022.

[10] National Crime Records Bureau, *Accidental Deaths and Suicides in India 2023*. New Delhi, India: Ministry of Home Affairs, Government of India, 2024.

[11] V. S. Sangtani *et al.*, "Arduino-based smart solar mower," *International Journal of Engineering and Management Research*, vol. 14, no. 2, pp. 111–116, 2024.

[12] S. R. Dogiwal, P. Dadheech, A. Kumar, and L. Raja, "Internet of Things based real-time monitoring system for grid data," in *Cognitive Computing and Intelligent IoT (ICETCE)*, Springer, 2022, pp. 236–247.

[13] M. M. Bahar, A. Sabril, and M. Riska, "Internet of Things (IoT)-based overcurrent protection and detection device for household electrical safety," *Journal of Embedded Systems, Security and Intelligent Systems (JESSI)*, vol. 6, no. 4, pp. 754–766, 2026.

[14] C. L. C. Arque, J. E. M. Jinez, and R. R. S. Torres, "Design and implementation of an ESP32-based electronic module for monitoring and protecting industrial electrical panels using the Modbus TCP/IP protocol," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 12, no. 10, pp. 123–135, 2025.

[15] M. Singh, S. Kumar, Y. Kumar, A. Raj, A. Raj, and K. Gupta, "Advanced technology-based circuit breaker acknowledgement through PZEM-004T module," in *Proc. IEEE North-East India Int. Energy Conversion Conf. and Exhibition (NE-IECCE)*, Silchar, India, 2025, pp. 1–6.

[16] S. S. Nimbekar, B. R. Chakole, A. B. Malewar, S. P. Hinge, T. V. Wanjari, and G. R. Panchbudhe, "Smart energy monitoring and safety system," *International Journal of Scientific Research and Engineering Development*, vol. 9, no. 1, pp. 2057–2061, Jan.–Feb. 2026.