International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 1, pp 103-112, January-2026

https://doi.org/10.47001/IRJIET/2026.101012

IoT-Based Overcurrent Protection in Substations: A Case Study of New Enma Substation, Aden

[1]Ali Khaled Alshurmani, [2]Taha Mahmoud Radman, [3]*Mohammed Fadhl Abdullah

[1,2,3]Faculty of Engineering, Aden University, Aden, Yemen
[3]University of Science and Technology, Aden, Yemen
Authors E-mail: [1]alshourmani2013@gmail.com, [2]taharadman2014@gmail.com
*Corresponding Author's E-mail: m.albadwi@ust.edu

***Abstract* - The increasing integration of Internet of Things (IoT) technologies into modern power systems has introduced new possibilities for flexible, scalable, and intelligent protection schemes. This paper presents the design and implementation of an IoT-Based overcurrent protection system that emulates the functional behavior of numerical protection relays while leveraging software-based processing and industrial communication technologies. The proposed scheme implements ANSI 50/51 overcurrent protection functions using the Node-RED platform combined with industrial IoT edge devices for real-time data acquisition and control. The protection architecture follows a layered IoT framework, starting from field-level current measurements, through edge data acquisition and communication layers, to software-based protection logic execution and circuit breaker actuation. A two-stage overcurrent strategy is employed, comprising a high-set definite-time element and a low-set inverse-time element based on IEC standard characteristics. The proposed system is validated through multiple operating scenarios, demonstrating reliable fault detection, accurate operating times, and secure tripping behavior. The results confirm that IoT-Based software protection can serve as an effective and low-cost complementary or backup solution to conventional protection relays, particularly in developing power networks and smart substation applications.**

Keywords: Internet of Things, Overcurrent Protection, Node-RED, IoT-Based Overcurrent Protection, Aden Substations.

I. INTRODUCTION

Electrical substations are essential for maintaining the stability and reliability of power systems, as they represent the main points where electricity is transmitted and distributed to consumers. In many developed countries, substations are already supported by advanced digital protection schemes combined with real-time monitoring systems, which allow operators to detect abnormal conditions quickly and even predict possible faults before they occur.

In Aden, the situation is different. Although most substations are equipped with digital protection devices, these devices usually operate in isolation and are not connected to real-time monitoring platforms. This makes it difficult to track the overall performance of equipment or to anticipate failures in advance. Furthermore, there are still several substations that completely lack modern digital protection and any form of real-time monitoring. In addition, the operation of substations in Aden network remains largely traditional, relying on on-site operators to monitor feeder loads and manually read fault events occurring on the electrical equipment. These gaps in the system increase the weakness of the network to unexpected breakdowns, longer blackout periods, and slower recovery after major faults.

Through my work in managing Aden's transmission lines and substations, I have observed several operational challenges arising due to the absence of real-time monitoring systems. A notable incident occurred in July 2024, when a lightning arrester exploded in a main substation (Betro-Hiswa substation). This fault caused a complete shutdown of the system, resulting in increasing the system voltage in 132 kV network to approximately 145 kV and in 33 kV network to nearly 40 kV. The sudden overvoltage damaged several transmission lines (cables), leading to a widespread power outage that affected large portions of the city for more than 24 hours. The consequences of this event extended beyond technical damage. Critical services such as hospitals and water supply systems were disrupted, commercial activities were halted, and many households experienced prolonged lack of electricity. This incident underscores the urgent necessity to implement enhanced protection and real-time monitoring systems in Aden's substations to ensure system reliability, prevent equipment failure, and reduce the socio-economic impact of similar events in the future.

The integration of Internet of Things (IoT) technology into Aden's substations considers a promising solution to these challenges. IoT enables real-time monitoring of equipment and network conditions, providing early detection of potential faults before they develop into serious failures.

This capability allows operators to respond quickly, reducing system downtime and minimizing the risk of equipment damage. In addition, by predicting maintenance needs and preventing major outages, IoT can significantly lower operational costs and improve the overall efficiency and reliability of the power network. Implementing such technologies is therefore essential for modernizing Aden's substations and ensuring a more stable and resilient electricity supply for the city.

This paper presents the design, implementation, and experimental validation of an IoT-based overcurrent protection system for substation applications. The main contributions include the development of a layered IoT protection architecture integrating conventional current transformers, industrial IoT edge devices, and a software-based protection platform, as well as the implementation of a two-stage ANSI 50/51 overcurrent protection scheme using the Node-RED platform with IEC normal inverse and high-set definite-time characteristics. The proposed system was practically deployed and validated at the New Enma Substation using secondary current injection tests, demonstrating accurate pickup detection, stable timing behavior, and reliable tripping performance. The results confirm that the proposed framework provides a flexible and low-cost backup protection solution suitable for developing power networks and smart substation applications.

II. OVERCURRENT PROTECTION

A. Traditional Overcurrent Protection

Overcurrent protection is one of the most fundamental protection functions in electric power systems. Its primary role is to protect generators, transformers, feeders, transmission lines, and associated equipment against excessive currents caused by short-circuit faults or prolonged overload conditions. Failure to detect and isolate such abnormal conditions within acceptable time limits can result in severe thermal and mechanical stresses, leading to equipment damage, reduced service life, and compromised system reliability.

Conventional overcurrent protection is typically implemented using electromechanical or numerical protection relays that operate based on predefined pickup settings and time–current characteristics. While these devices offer high reliability, their configuration flexibility, scalability, and integration with modern monitoring platforms may be limited, particularly in legacy substations and developing power networks.

Recent advancements in IoT technologies and industrial communication systems have enabled the deployment of software-based protection and monitoring solutions. By combining real-time data acquisition, networked communication, and flexible processing platforms, IoT-Based protection schemes offer new opportunities for adaptive, modular, and cost-effective protection system design.

This paper proposes an IoT-Based overcurrent protection system implemented using the Node-RED platform. The main contribution of this work lies in the development of a layered IoT protection architecture that integrates conventional measurement devices with software-based protection logic, while preserving the fundamental operating principles of numerical overcurrent relays. The proposed approach is particularly suitable for use as a backup or supervisory protection system and as a research-oriented platform for smart grid and substation automation studies.

B. Fundamentals of Overcurrent Protection

Overcurrent protection operates by continuously comparing the measured line current with predefined pickup thresholds. When the measured current exceeds the pickup value, a trip command is issued either instantaneously or after a calculated time delay, depending on the selected protection characteristic.

According to ANSI/IEEE device numbering standards, overcurrent protection is classified into instantaneous or high-set overcurrent protection (ANSI 50) and time-delayed overcurrent protection (ANSI 51). Instantaneous elements provide rapid fault clearance for high-magnitude short-circuit currents, while time-delayed elements allow selective coordination between upstream and downstream protection devices.

Inverse-time overcurrent characteristics are widely adopted in practical protection systems. In such characteristics, the operating time decreases as the fault current magnitude increases, enabling effective discrimination between faults occurring at different locations in the power system. The International Electro-Technical Commission (IEC) has standardized several inverse-time curves, including normal inverse, very inverse, and extremely inverse characteristics, which are extensively implemented in modern numerical relays.

III. LITERATURE REVIEW

Recent research has increasingly explored the integration of Internet of Things (IoT) technologies into power system monitoring and protection; however, the degree to which IoT is effectively combined with overcurrent protection logic in substations varies significantly across the literature. Among the most directly relevant studies, the work presented in [2] proposes a wireless IoT-Based overcurrent relay for transmission line protection. This study demonstrates the feasibility of replacing conventional wiring with wireless communication while implementing definite-time overcurrent protection. Despite its relevance, the protection logic remains simplified and does not address inverse-time characteristics, relay coordination, or standard-compliant setting methodologies.

A similar protection-oriented approach is presented in [4], where an IoT-Based overcurrent protection system is developed for low-voltage distribution networks. The proposed system detects overcurrent faults using fixed threshold values and communicates fault information via GSM technology. Although effective for basic fault detection and isolation, the system lacks multi-stage protection, coordination, and applicability to substation environments.

The work in [3] advances beyond basic monitoring by introducing an open-architecture microprocessor-based relay protection device using Industrial IoT concepts. This study focuses on modular relay design and processing speed, highlighting the potential of IoT-enabled protection platforms. However, overcurrent protection characteristics and coordination requirements are not addressed in detail, limiting its use as a complete protection solution.

Protection coordination enabled by IoT communication is investigated in [5], where IoT is employed to enhance information exchange among protection devices in smart substations. Simulation results indicate improvements in fault detection latency and coordination speed. Nevertheless, the study does not implement explicit overcurrent relay algorithms or detailed setting calculations, positioning it more as an architectural contribution than a protection design reference.

In [9], the integration of IoT with Edge Artificial Intelligence is explored for real-time grid protection and control. The proposed framework demonstrates improved fault response under various operating conditions using simulation-based validation. However, protection decisions are treated primarily as an AI-based classification task, without formal modeling of overcurrent protection curves or coordination principles.

Several studies emphasize IoT-Based monitoring while incorporating limited protection-related functionality. In [1], a smart IoT-Based system is proposed for monitoring and controlling substation equipment, including basic overcurrent detection and control actions. While the system demonstrates practical monitoring capabilities, the protection functions are simplified and serve mainly as proof-of-concept implementations. Transformer fault detection using IoT is further explored in [10], where temperature, voltage, and current measurements are employed to identify abnormal operating conditions. Although overcurrent and differential protection concepts are mentioned, the study does not address detailed protection characteristics such as slope compensation, coordination, or standard-based relay design.

Cloud-based monitoring and analytics for substations and transmission lines are presented in [6], where IoT is used to support condition monitoring and fault detection. The focus of this work is primarily on data acquisition and health assessment rather than structured protection logic. Similarly, [7] introduces an Android-based IoT system for monitoring the 110 V DC auxiliary supply in substations. While this system contributes to improving substation reliability, it does not address protection functions directly.

Additional IoT-Based monitoring and control frameworks for substations and smart grids are discussed in [11], [12], and [13]. These studies demonstrate the effectiveness of IoT for real-time data visualization, remote supervision, and operational awareness. However, they do not incorporate detailed overcurrent protection logic or relay coordination strategies, and thus provide only indirect support for protection-oriented research.

Overall, the reviewed literature indicates that although IoT-Based monitoring of power systems is well established, only a limited number of studies directly address IoT-Based overcurrent protection, and those that do often rely on simplified threshold-based algorithms without comprehensive coordination or standard-compliant design. This reveals a clear research gap in developing an IoT-Based overcurrent protection scheme for substations that integrates real-time monitoring with robust, coordinated, and practically deployable protection logic, which the present study aims to address.

IV. IOT-BASED OVERCURRENT PROTECTION SYSTEM ARCHITECTURE

4.1 Layered System Architecture

The proposed IoT-Based overcurrent protection system is designed using a multi-layer architecture that integrates conventional power system measurements with modern IoT technologies. The overall system architecture is illustrated in Figure 1.

4.1.1 Field Measurement Layer

At the field level, current transformers (CTs) installed on the protected feeder provide secondary current signals proportional to the primary line currents. These secondary currents are converted into standardized 4–20 mA analog signals using industrial current transducers to enhance noise immunity and ensure reliable signal transmission within the substation environment.

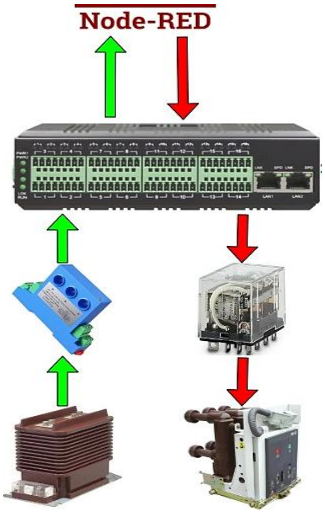


Figure 1: IoT-Based Overcurrent Protection Framework Overcurrent Protection Framework

4.1.2 Edge IoT Device Layer

The processed analog signals are acquired by an industrial Ethernet-based AI/AO/DI/DO server, which functions as the edge IoT device. This device aggregates real-time measurements, provides digital input/output interfaces, and serves as the gateway between the physical power system and the software-based processing environment.

4.1.3 Communication Layer

Data exchange between the edge IoT device and the processing platform is achieved using standard industrial communication protocols, such as Modbus, MQTT, HTTP or other protocols. For geographically distributed substations, cellular communication technologies can be employed to enable remote connectivity. This communication layer ensures reliable and scalable data transfer for protection and monitoring purposes.

4.1.4 Processing and Protection Logic Layer

The Node-RED platform is used as the core processing environment for implementing the overcurrent protection logic. Real-time current measurements received from the IoT device are processed by the protection algorithm, which evaluates pickup conditions, calculates operating times, and determines faulted phases.

4.1.5 Operation and Control Layer

Upon detection of a fault condition, the protection logic issues a trip command that is transmitted back to the field (substation) via the IoT device. An auxiliary relay is energized and closes its NO contact to operate the circuit breaker trip coil, thereby isolating the faulty section of the power system. The overall architecture ensures electrical isolation between the low-voltage IoT system and the high-voltage switching equipment.

4.2 System Specifications

To ensure clarity, reproducibility, and engineering completeness, the main hardware components, communication interfaces, and protection parameters of the proposed IoT-Based overcurrent protection system are summarized in Table 1. The specifications include the transformer rating, current transformer ratio, transducer characteristics, IoT edge device configuration, communication protocol, and protection settings used during experimental validation at the New Enma Substation. These parameters form the basis for the implementation of the ANSI 50/51 protection functions and the associated timing characteristics.

Table 1: System Specifications of the Proposed IoT-Based Overcurrent Protection Scheme

Component	Specification
Protected Equipment	20 MVA Power Transformer (New Enma Substation, Aden)
Primary Voltage Level	11 kV Distribution Side
Current Transformer (CT) Ratio	1800 / 1 A
CT Secondary Rating	1 A
Current Transducer Output	4–20 mA Analog Signal
Analog Input Range (IoT Device)	4–20 mA
Edge IoT Device	Industrial Ethernet AI/AO/DI/DO Server
Communication Protocol	Modbus TCP/IP
Processing Platform	Node-RED
Sampling Interval	Real-time continuous acquisition
Low-Set Pickup Current (I_{set1})	0.5 A (Secondary)
High-Set Pickup Current (I_{set2})	0.8 A (Secondary)
IEC Curve Type	Normal Inverse
Curve Constants	(K = 0.14), (\alpha = 0.02)
Time Multiplier Setting (TMS)	0.05
Stage-2 Definite Time Delay	200 ms
Trip Output Interface	Digital Output via IoT Device
Circuit Breaker Trip Method	Auxiliary Relay Contact
Electrical Isolation	Opto-isolated digital output
Protection Functions	ANSI 50 (Instantaneous), ANSI 51 (Inverse Time)

4.3 Block Diagram Representation

To provide a high-level functional overview of the proposed IoT-Based overcurrent protection system, a block diagram representation is illustrated in Figure 2. The block diagram highlights the main functional components of the system and the logical flow of information between them, starting from current sensing and ending with circuit breaker operation.

The block diagram clearly shows the interaction between the field measurement devices, the edge IoT layer, the communication network, the Node-RED processing environment, and the final actuation stage. This representation emphasizes the layered IoT framework and clarifies the role of each subsystem in the overall protection scheme.

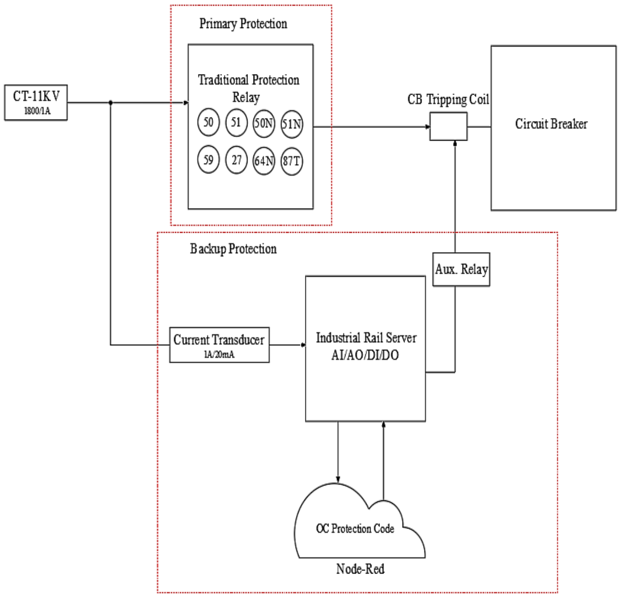


Figure 2: Block Diagram of the IoT-Based Overcurrent Protection System

4.4 Schematic Diagram Representation

In addition to the block-level representation, a detailed schematic diagram of the proposed system is represented in Figure 3. The schematic diagram illustrates the physical and electrical interconnections between current transformers, transducers, IoT edge devices, auxiliary relays, and the circuit breaker trip circuit.

This diagram provides insight into the practical implementation aspects of the proposed architecture, including signal processing, input/output wiring, and isolation between low-voltage control circuits and high-voltage power equipment. The schematic representation confirms the feasibility of deploying the proposed IoT-Based protection system in real substation environments.

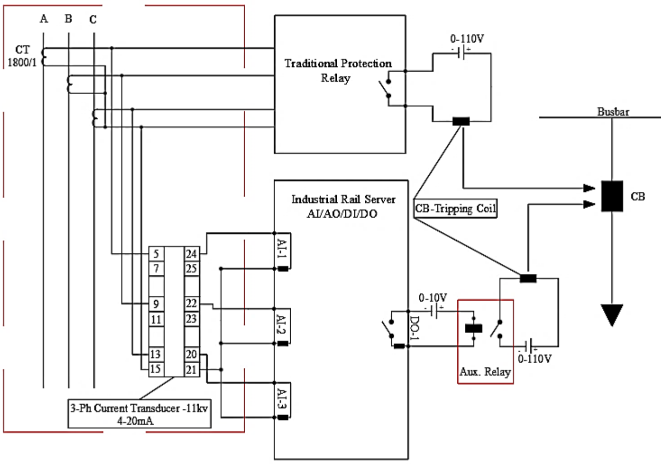


Figure 3: Schematic Diagram of the IoT-Based Overcurrent Protection System

V. ARCHITECTURE OF THE OVERCURRENT PROTECTION SYSTEM USING NODE-RED

The proposed overcurrent protection algorithm is implemented in Node-RED using a set of interconnected nodes that collectively replicate the functional stages of a practical digital protection system. The overall signal flow, as illustrated in Figure 4, follows the sequence of measurement, signal conditioning, protection logic execution, and tripping command issuance. The main nodes used in the implementation and their respective functions are described below.

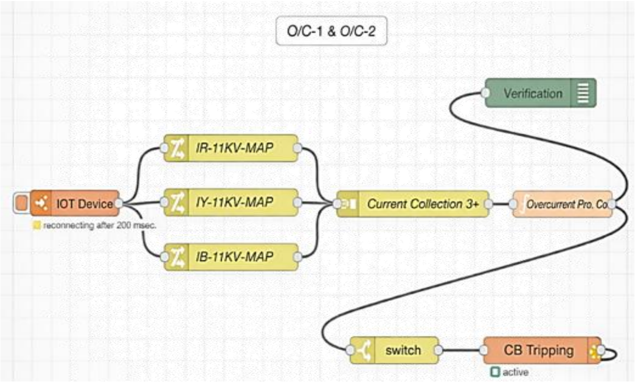


Figure 4: Node-RED Overcurrent Protection Architecture

a. **Modbus Read Node**: This node is used to acquire the real-time three phase current measurements from IoT device installed at the field layer. The device is interfaced with a three-phase transducer that converts the secondary current output of the current transformers (CTs), rated at 1 A, into an analog signal in the range of 4–20 mA. These analog values are digitized and transmitted to the Node-RED environment.

b. **Change Node (Signal Mapping):** It performs signal conditioning and scaling of the measured currents. It maps the received 4–20 mA signals back to their corresponding primary current values in range of 0–1 A. This normalization process ensures that the input data used by the protection algorithm are consistent with the nominal CT ratings.

c. **Join Node:** It is responsible for combining the three independently processed phase currents into a single structured message. Here, the phase currents are defined as individual variables, allowing the Function node to access and process all three phase quantities simultaneously.

d. **Function Node:** It represents the core of the protection scheme. It executes the overcurrent protection algorithm, determines the maximum phase current, identifies the faulty phase, evaluates pickup conditions, and manages the associated time-delay logic.

e. **Switch Node:** It functions as a decision-making element that evaluates the output of the Function node. When a fault condition is detected and a trip signal is generated, this node routes message toward the output stage. Under normal operating conditions, the protection output is blocked, and no tripping command is issued.

f. **Modbus Write Node:** It is used to transmit the trip command to the circuit breaker control system. A control signal is sent to the circuit breaker via the IoT device and an aux. relay, initiating the opening operation and isolating the faulty section of the power system. This step represents the final action of the protection scheme.

g. **Debug Node:** It is utilized for monitoring and validation purposes during system testing and development. It allows real-time observation of the Function node output, facilitating verification of the protection algorithm under both normal and fault conditions.

VI. FUNCTION NODE ALGORITHM IMPLEMENTATION

The complete overcurrent protection logic is implemented within the Node-RED Function node. The algorithm continuously processes the three-phase current measurements, determines the maximum phase current, identifies the faulty phase, and evaluates the operating conditions of a two-stage overcurrent protection scheme based on ANSI 50/51 standards.

The protection system consists of two coordinated stages:

- **Stage-1 (ANSI 51 – Inverse Time Overcurrent Protection)**:

A low-set inverse-time element based on the IEC Normal Inverse characteristic.

- **Stage-2 (ANSI 50 – Definite Time Overcurrent Protection)**:

A high-set definite-time element for fast clearance of severe faults.

The algorithm operates as follows:

Algorithm 1: Two-Stage Overcurrent Protection Logic

```
Inputs: Three-phase currents: I_R, I_Y, I_B
Parameters:
    • Low-set pickup current: (I_{set1})
    • High-set pickup current: (I_{set2})
    • IEC curve constants: (K, \alpha)
    • Time Multiplier Setting: TMS
    • Definite time delay: (T_{DMT})
Step 1: Current Acquisition and Phase Selection
    1. Acquire real-time three-phase current measurements
       from the IoT edge device.
    2. Compute the maximum phase current:
       [ I_{max} = \max (I_R, I_Y, I_B)]
    3.Identify the faulty phase corresponding to (I_{max}).
Step 2: High-Set Overcurrent Evaluation
(Stage2, ANSI 50)
    4. If (I_{max} \geq I_{set2}), then:
        –Activate the Stage-2 pickup.
        –   Start the definite-time delay timer (T_{DMT}).
        –   After the timer expires, issue a trip command
            classified as:O/C Stage-2 High-Set Trip.
        –   Reset all timers and latch variables.
Step 3: Low-Set Overcurrent Evaluation
(Stage-1, ANSI 51)
    5.   If (I_{max} \geq I_{set1})&( I_{max} < I_{set2} ),
     then:
        –Activate the Stage-1 pickup.
        – Compute the inverse-time operating delay using
          the
           IEC Normal Inverse characteristic :
          [T_{IDMT}                                  =
          \frac{K}{\left(\frac{I_{max}}{I_{set1}}
          \right)^{\alpha} - 1} \times TMS]
        – Start the inverse-time delay timer (T_{IDMT}).
        – After the timer expires, issue a trip command
          classified as:O/C Stage-1 Low-Set Trip.
        – Reset all timers and latch variables.
Step 4: Normal Operation
    6.   If ( I_{max} < I_{set1} ), then:
        – System remains in normal monitoring mode.
        – No protection action is taken.
Step 5: Protection Output
    7. Upon trip decision, a digital output command is
       transmitted via Modbus protocol to the IoT edge
       device.
    8. The edge device energizes an auxiliary relay, which
       operates the circuit breaker trip coil and isolates the
       faulty feeder
```

This structured algorithm ensures reliable fault detection, secure timing behavior, accurate phase identification, and dependable tripping performance under both moderate and severe fault conditions.

VII. OVERCURRENT PROTECTION ALGORITHM FLOWCHART

Figure (5) illustrates the logical flowchart of the proposed overcurrent (O/C) protection algorithm implemented for transformer protection. The protection scheme is based on a two-stage overcurrent strategy, comprising a high-set instantaneous stage DMT (Stage-2) and a time-delayed normal inverse stage IDMT (Stage-1), to ensure fast fault clearance while maintaining selectivity and coordination.

At the beginning of the algorithm, the three-phase currents (IR, IY, and IB) are continuously measured. The maximum phase current (Imax) is calculated, and the faulty phase is identified based on the highest measured current magnitude. This ensures accurate phase selection during fault conditions.

The algorithm first checks whether the maximum current exceeds the high-set pickup threshold (Iset2). If Imax ≥ Iset2, the protection enters Stage-2, which represents the high-set overcurrent element. In this stage, a fixed time delay DMT is applied to enhance security against transient disturbances. After the expiration of the time delay, the relay issues a trip command, classified as **O/C Stage-2 High-Set Trip**, providing rapid fault isolation for severe short-circuit conditions.

If the high-set pickup condition is not satisfied, the algorithm evaluates the low-set pickup criterion (Imax ≥ Iset1). When this condition is satisfied, the protection enters Stage-1, which operates according to a normal inverse time-current characteristic IDMT. In this stage, the operating time is calculated based on the magnitude of the fault current using an inverse-time equation expressed as:

$$T = \frac{K}{\left(\left(\frac{I_{\max}}{I_{\text{set1}}}\right)^{\alpha} - 1\right)} \times \text{TMS}$$

Where $I_{\max}$ is the maximum measured phase current, I_{set1} is the low-set pickup current, K and α are curve constants corresponding to the normal inverse characteristic, and TMS represents the time multiplier setting. This inverse relationship allows higher fault currents to result in shorter operating times, ensuring proper coordination with downstream protection devices. After the calculated operating time elapses, a trip command is issued and identified as **O/C Stage-1 Low-Set Trip**.

In the event that the measured current remains below the low-set pickup threshold (Imax < Iset1), the system is considered to be operating under normal conditions. In this case, no protection action is taken, and the algorithm maintains continuous monitoring of the feeder currents.

This structured logic ensures reliable overcurrent detection, fast clearance of high-magnitude faults, and selective operation for lower fault levels, thereby improving the overall protection performance and coordination of the power system.

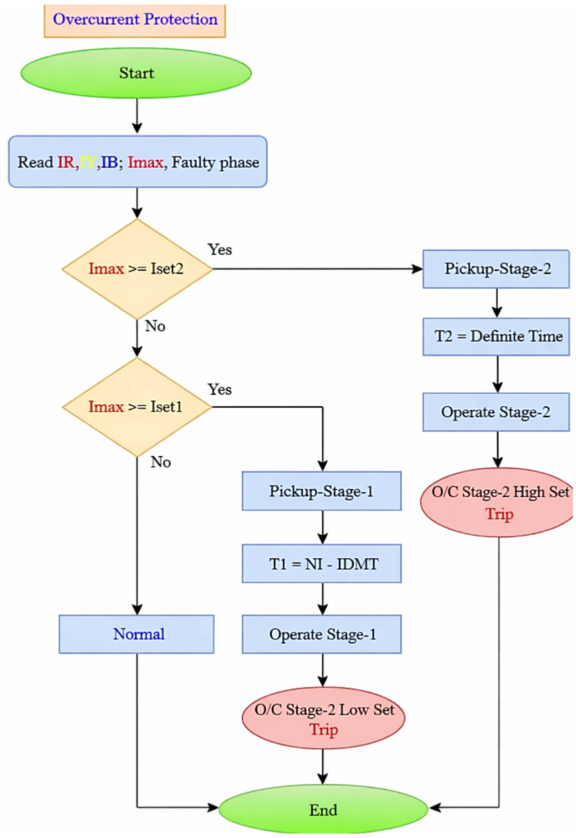


Figure 5: Overcurrent Protection Flow Chart

VIII. EXPERIMENTAL VALIDATION

The experimental validation of the proposed IoT-Based overcurrent protection scheme was carried out at the **New Enma Substation of Aden Electricity Corporation**, as illustrated in Figure (6).

The proposed IoT framework was integrated with one of the **20 MVA power transformers** installed at the substation in order to assess the practical performance of the protection scheme under real operating conditions. The validation process was conducted using a secondary current injection test device by injecting test currents at three different levels, representing normal operating condition, first-stage overcurrent condition (low set) , and second-stage (high set) overcurrent condition.

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 103-112, January-2026
https://doi.org/10.47001/IRJIET/2026.101012

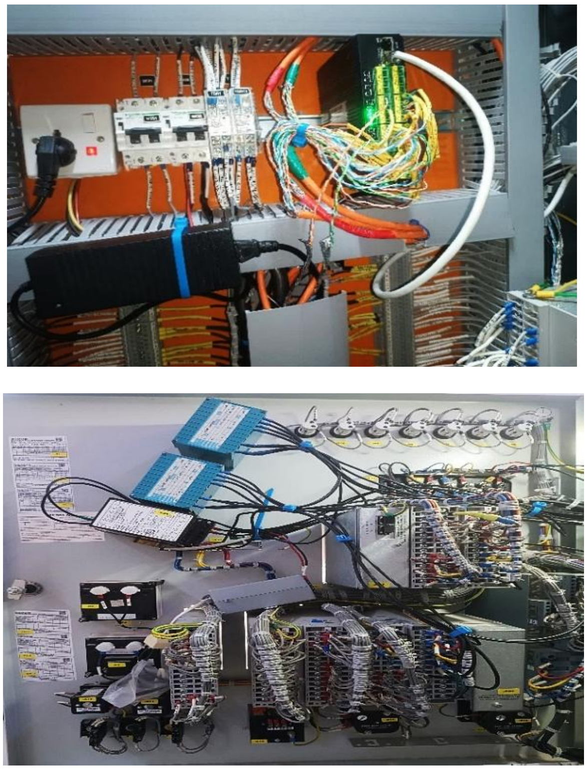
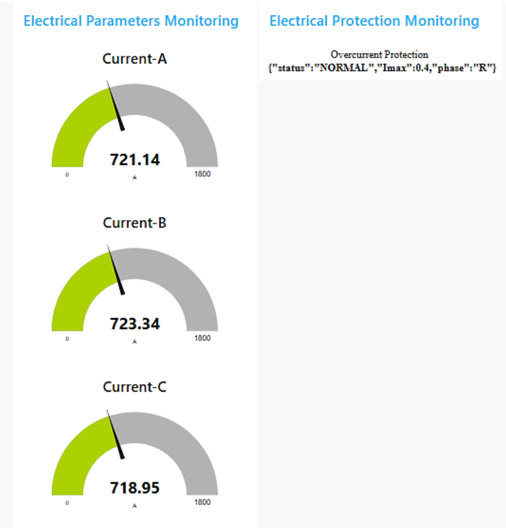


Figure 6: Implemented IoT-Based Overcurrent Protection Scheme at New Enma Substation

8.1 Normal Operating Condition Test

In the first test scenario, a normal current of **0.4 A** was injected on the secondary side, which corresponds to **720 A** on the **11 kV side**. The experimental results showed stable system behavior with no false tripping or unintended protection operation. This confirms the accuracy of the measurement stage and the reliability of the proposed protection scheme under normal operating conditions, as shown in the corresponding Figure (7).



Electrical Parameters Monitoring

Current-A

721.14

Current-B

723.34

Current-C

718.95

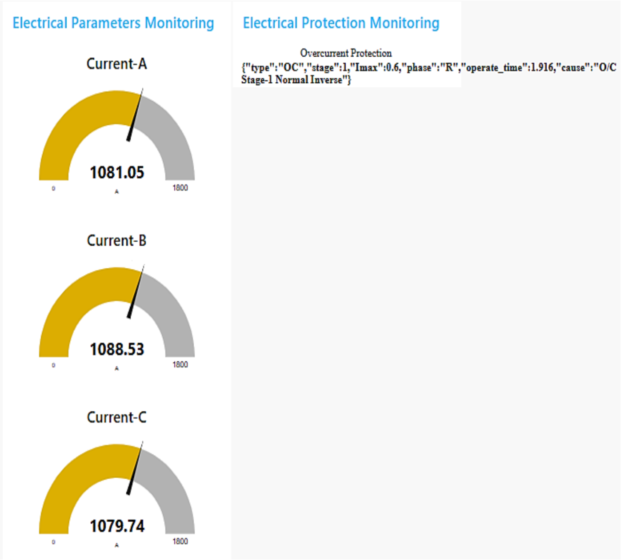
Electrical Protection Monitoring

Overcurrent Protection
{"status":"NORMAL","Imax":0.4,"phase":"R"}

Figure 7: Normal Operating Condition Test

8.2 First-Stage Overcurrent Test (ANSI 51)

In the second scenario, an overcurrent exceeding the pickup value of the first protection stage was injected. The injected current magnitude was **0.6 A**, corresponding to **1080 A** on the **11 kV side**. The inverse-time overcurrent element (**ANSI 51**) was correctly activated, and the operating time followed the predefined inverse-time characteristic. The measured tripping time closely matched the theoretical values, demonstrating correct pickup detection and timer operation, as illustrated in the Figure(8).



Electrical Parameters Monitoring

Current-A

1081.05

Current-B

1088.53

Current-C

1079.74

Electrical Protection Monitoring

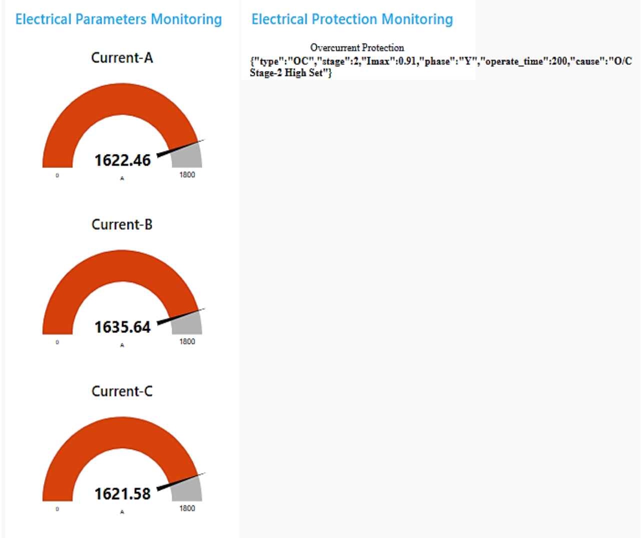
Overcurrent Protection
{"type":"OC","stage":1,"Imax":0.6,"phase":"R","operate_time":1.916,"cause":"O/C Stage-1 Normal Inverse"}

Figure 8: First-Stage Overcurrent Test (ANSI 51)

8.3 Second-Stage High Overcurrent Test (ANSI 50)

In the final scenario, a high fault current of **0.9 A** was injected, which is equivalent to **1620 A** on the **11 kV side**. Under this condition, the high-set overcurrent element (**ANSI 50**) was immediately triggered, and a trip command was issued within the predefined definite-time setting (200ms). These results confirm the fast and reliable response of the proposed protection scheme under severe fault conditions, as shown in the Figure(9).

Overall, the experimental results demonstrate excellent performance of the proposed IoT-Based overcurrent protection scheme. Accurate pickup detection, stable timing characteristics, and reliable tripping behavior were achieved across all tested operating conditions. The close agreement between measured and theoretical operating times confirms the correctness and practical feasibility of the proposed protection approach for real-world substation applications.



Overcurrent Protection

```
{"type":"OC","stage":2,"Imax":0.91,"phase":"Y","operate_time":200,"cause":"O/C
Stage-2 High Set"}
```

Figure 9: Second-Stage High Overcurrent Test (ANSI 50)

IX. DISCUSSION AND LIMITATIONS

The proposed IoT-Based overcurrent protection system demonstrates several advantages, including flexibility, modularity, and ease of integration with modern monitoring platforms. The use of Node-RED enables rapid development and modification of protection logic, making the system particularly suitable for research, education, and backup protection applications.

However, certain limitations must be considered. Communication latency, network reliability, and cybersecurity concerns may affect the performance of IoT-Based protection systems if not properly addressed. Consequently, the proposed scheme is suitable as a backup protection solution instead of a full replacement for primary numerical relays in critical protection zones.

X. CONCLUSION

This paper presented an IoT-Based overcurrent protection system implemented using the Node-RED platform. The proposed architecture integrates conventional power system measurements with industrial IoT devices and software-based protection logic to simulate the behavior of numerical overcurrent relays. A two-stage protection strategy based on ANSI 50/51 functions was successfully implemented and validated under multiple operating scenarios.

The proposed system provides a flexible, modular, and low-cost protection solution that is particularly suitable for backup protection, real-time monitoring, and research-oriented deployments in developing power networks. By leveraging industrial IoT technologies, the framework supports the modernization of conventional substations and enables the transition toward smart substation infrastructures.

Future work will focus on extending the proposed platform to include additional protection functions such as earth fault and differential protection, as well as investigating cybersecurity and communication latency mitigation strategies.

REFERENCES

[1] M. S. Hossain, M. S. Rahman, M. S. Islam, and M. A. Matin, "A Smart IoT Based System for Monitoring and Controlling the Sub-Station Equipment," *Internet of Things*, 2019.

[2] M. Hafizi Idris, M. R. Adzman, M. Amirruddin, and I. Md. Amin, "Wireless IoT-Based Overcurrent Relay for Transmission Line Protection," *IEEE Access*, 2021.

[3] A.Neftissov, I. Kazambayev, L. Kirichenko, A. Aubakirova, D. Urazayev, and K. Zhakupova, "Development of Microprocessor Device of Relay Protection Based on Open Architecture Using Industrial Internet of Things Technology," *Procedia Computer Science*, 2024.

[4] R. Andrew and W. S. Boateng, "IoT Based Overcurrent Protection in Distribution Systems," *Preprint*, 2024.

[5] R. Holt, "IoT-Enabled Protection Coordination for Smart Substations," *International Journal of Smart Grid*, 2024.

[6] S.R. Shinde, R. B. Ingle, and P. R. Wankhede, "Cloud-Based Data Analytics and Control of Substation Transformer and Transmission Lines Using IoT," *International Journal of Electrical Power & Energy Systems*, 2021.

[7] E. Dhaniswara, N. Nurholis, and T. Tamaji, "Android-Based Monitoring of 110 Volt DC System in Substations to Improve Maintenance Efficiency," *International Journal of Electrical Engineering and Informatics*, 2022.

[8] A.Bajwa, A. A. R. Tonoy, and M. A. M. Khan, "IoT-Enabled Condition Monitoring in Power Transformers: A Proposed Model," *Review of Applied Science and Technology*, 2025.

[9] V. Writer, "Integrating IoT and Edge AI for Real-Time Grid Protection and Control," *Preprint*, 2024.

[10] Md. S. Hossain, M. S. Islam, and M. A. Matin, "IoT Based Fault Detection and Protection of Power Transformer," *International Journal of Engineering Research*, 2018.

[11] Md. S. Hossain *et al.*, "IoT-Based Monitoring and Control of Substations and Smart Grids," *International Conference on Smart Grid*, 2020.

[12] Md. S. Hossain *et al.*, "IoT-Based Power Monitoring and Management System," *International Journal of Electrical and Computer Engineering*, 2020.

[13] Md. S. Hossain *et al.*, "IoT-Based Real-Time Monitoring and Control System for Distribution Substation," *International Journal of Electrical Engineering*, 2021.

AUTHORS BIOGRAPHY

Mohammed Fadhl Abdullah is currently a Professor of Computer Engineering at Aden University in Yemen. He received his Master and PhD degrees in Computer Engineering from Indian Institute of Technology, Roorkee 1993, Delhi 1998, respectively. He was the editor-in-chief of Aden University Journal of Information Technology (AUJIT). He is a founding member of the International Center for Scientific Research and Studies (ICSRS). His main research interests are in the fields of ML, Parallel algorithms, and Cybersecurity. He can be contacted at email: m.albadwi@ust.edu

Dr. Taha Mahmoud Radman is currently an Assistant Professor of power system protection Engineering at Aden University in Yemen. He received his PhD degree in Electrical Engineering from German Dresden University in 1989. He was the head of electrical department of Faculty of Engineering / Aden university. He is a consultant in public electricity corporation (PEC) of Aden. His main research interests are in the fields of power system protection engineering. He can be contacted at email taharadman2014@gmail.com

Ali Khaled Ali Mohammed Alshurmani is a PhD student in Electrical Engineering at the University of Aden, Faculty of Engineering. He received his Master's degree in power system protection Engineering from the University of Aden, Faculty of Engineering, in 2022, and his Bachelor's degree in power system protection Engineering from the University of Aden, Faculty of Engineering, in 2012, He is a manager of transmission and substations in PEC of Aden. He can be contacted at email: alshourmani2013@gmail.com

Citation of this Article:

Ali Khaled Alshurmani, Taha Mahmoud Radman, & Mohammed Fadhl Abdullah. (2026). IoT-Based Overcurrent Protection in Substations: A Case Study of New Enma Substation, Aden. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(1), 103-112. Article DOI https://doi.org/10.47001/IRJIET/2026.101012

****