Cape Peninsula
University of Technology

SMART MONITORING OF LOW VOLTAGE NETWORKS TO COMBAT ILLEGAL POWER CONNECTIONS

by

THULANI SOLANI

Dissertation submitted in partial fulfilment of the requirements for the degree

Master of Engineering: Electrical Engineering

in the Faculty of Engineering and the Built Environment

at the Cape Peninsula University of Technology

Supervisor: **Dr. C Kriger**
Co-supervisor: **Dr. YD Mfoumboulou**

Bellville Campus
Date submitted: November 2025

DECLARATION

I, Thulani Solani, declare that the contents of this dissertation represent my own unaided work, and that the dissertation has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **November 2025**
Date

ABSTRACT

The power system has continually been evolving with the integration of sophisticated software and hardware. This evolution has focused on medium- and high-voltage networks with a state-of-the-art level of automation, while automation for low-voltage (LV) distribution grids remained relatively unchanged. The current LV distribution infrastructure still contain many legacy devices and systems that require intervention to enhance efficiency and address issues such as non-technical losses (NTLs). NTLs are not technical shortcomings but are attributable to electricity theft, meter tampering, administrative inefficiencies, and non-payment of bills. The demand for an optimized, resilient and sustainable power supply necessitates the development of intelligent methods for the production, storage, and distribution of electricity. Currently, government strategies include the adoption of smart grids in place of conventional electrical grids. Smart grids allow for the distribution of electricity to consumers using digital communication networks, thus enabling continuous monitoring and analysis of the electrical supply.

This research study addresses the global imperative to reduce losses in electricity networks by designing and implementing a smart low-voltage (LV) distribution network grounded in an Internet of Things (IoT) architecture. As the world shifts toward a green-energy future, optimizing power grids to operate efficiently becomes essential for sustainable energy resilience, with electricity theft identified as a significant threat to grid security and performance. Smart grid technologies, underpinned by Internet of Things (IoT) capabilities, offer continuous monitoring and analysis of electrical supply by delivering electricity through digital communication networks. The primary objective of is to design, develop, and implement a smart low-voltage (LV) distribution network monitoring and control system anchored in IoT architecture to mitigate electricity theft and enhance protection, automation, and control of LV networks.

The study posits a gap in the literature: while numerous solutions focus on detection, they often rely on time-consuming utility-led inspections and disconnections, imposing substantial resource burdens. There is a need for scalable, proactive, and automated interventions that minimize direct utility involvement while effectively reducing non-technical losses and improving grid resilience. The research study proposes a framework that leverages real-time data and theory-driven algorithms to enable rapid detection of faults and illicit connections, thereby enhancing observability, fault detection, and proactive maintenance.

The thesis findings and deliverables contribute to the expansion of the knowledge base in the field of smart grids in different ways:

1. The provision of a novel scalable, proactive and automated solution at the low-voltage distribution level, that minimizes direct involvement of the power utility while effectively reducing not-technical losses and improving grid resilience.
2. The development of an integrated IoT-based framework with current and voltage sensors deployed at strategic locations within the LV network in order to identify any anomalies.
3. The construction, design and development of a lab-scale prototype smart LV network solution with validation of operation by means of Proteus software simulations.
4. A pilot-ready solution with the capability for deployment within a LV network of the South African power utility, ESKOM.

The thesis findings and deliverable contribute to extending the knowledge base within academic institutions and other research institutions.

Keywords:
IoT; smart grids; low-voltage distribution; electricity theft; Kirchhoff's Current Law; Proteus simulation; pilot deployment; non-technical losses; grid resilience; automation.

ACKNOWLEDGEMENTS

I wish to thank:

- My supervisor Dr Carl Kriger and co-supervisor Dr Y. D. Mfoumboulou for their support, advice, guidance, and contribution to this Dissertation. Thank you very much for the time you have taken to assist me in this journey.
- My colleagues at Eskom who gave me the opportunity to present my research and subsequently approving funding for it to be implemented as a pilot project.
- My lovely wife Nolukho Mayile Solani for her support, encouragement, understanding, and patience during my time studying. Thanks for the support and taking care of our boys whilst I was always busy with my studies.
- Myself for not giving up on my studies as difficult as it got sometimes.

DEDICATION

This dissertation is dedicated to my late Father Mthuthuzeli Gogobala, I love you Mbotho, Thoyane, Nyawo Zibomvu even though I never had a chance to meet you, I have no doubt you would have been a proud father. To my mother Nomboniso Solani who struggled raising me as a single parent and to my grand Mother Vivian Yalezo who stepped in to raise me to be the man I became. To my siblings for their love

And lastly to my wife and kids for their patience with me during all the hours I was away from them busy with my studies.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym

AC	Alternating Current
ADC	Analog-to-Digital Converter
ADMD	After Diversity Maximum Demand
AMI	Advance metering infrastructure
API	Application Programming Interface
BAN	Building Area Network
CE	Chip Enable
CIU	Customer Interface Unit
DMS	Distribution Management System
DSL	Digital Subscriber Line
EDA	Electrical Design Automation
FAN	Field Area Network
GDP	Gross Domestic product
GSM	Global System for Mobile Communications
HAN	Home Area Network
IAN	Industrial Area Network
IDE	Integrated Development Environment
IoT	Internet of Things
KCL	Kirchhoff's Current Law
LPUs	Large Power users
LV	Low Voltage
MCB	Miniature Circuit break
MISO	Master In Slave Out
MOSI	Master Out Slave In
MPPT	Maximum Power Point Tracking
MV	Medium Voltage
NAN	Neighbourhood Area Network
NTLs	Non-technical losses
PCB	Printed Circuit Board
PLCC	Power Line Carrier Communication
PMUs	Phasor Measurement Units
RF	Radio Frequency
RMS	Root Mean Square
RTC	Real-Time Clock
SCADA	Supervisory Control And Data Acquisition
SDGs	Sustainable Development Goals
SPI	Serial Peripheral Interface
SS	Slave Select
UART	Universal Asynchronous Receiver/Transmitter
USD	United States Dollar
VSM	Virtual System Modelling
WAN	Wide Area Network

1. CHAPTER 1

INTRODUCTION

1.1 Introduction

Over recent years, the development and integration of sophisticated software and hardware into electricity grids have predominantly targeted medium- and high-voltage networks. As a consequence, medium- and high-voltage distribution grids have achieved a state-of-the-art level of automation, while automation for low-voltage (LV) distribution grids remains in its infancy (Hauer and Bartonek, 2016). It is increasingly evident that the current LV distribution infrastructure, often characterized by legacy systems, requires intervention to enhance efficiency and address inherent issues, notably non-technical losses (NTLs). NTLs are losses attributable not to technical shortcomings but to electricity theft, meter tampering, administrative inefficiencies, and non-payment of bills. According to Penn Energy, globally, approximately 96 billion USD is lost to NTLs. Electricity theft ranks third among the most stolen commodities worldwide (Louw and Boroko, 2019).

Despite the rollout of Smart Meters and Advanced Metering Infrastructure (AMI) to customer premises to improve LV grid intelligence and to provide essential measurements, addressing illegal connections remains challenging and may require data analysis that is contingent upon the availability of utility resources (Dudek et al., 2018). In response, this project proposes a system—the Smart LV Networks—that aims to improve the management of non-technical losses, protection, and automation in LV networks. The proposed system will integrate embedded systems and communication technologies to deliver a fully automated, self-healing, and intelligent LV distribution network. Key capabilities include the detection of electricity theft, specifically illegal connections, to prevent unauthorized engagement with the grid. Upon detection, the system will automatically isolate the segment of the network associated with illegal connections, minimize the number of affected customers by rerouting services to legally connected customers, and simultaneously notify both the utility and the affected customers of the event.

The proposed system is designed to complement, rather than replace, smart meters, thereby contributing to more efficient, economical, and safer LV distribution grids. The introduction laid out in Section 1.1 establishes the foundation for the proposed work. The remainder of the chapter is organized as follows: Section 1.2 discusses the awareness of the research problem; Section 1.3 presents the research problem statement; Section 1.4 outlines the research aims and objectives. Research questions are addressed in Section 1.5, with hypotheses presented in Section 1.6. The delimitations of the study are discussed in Section 1.7, followed by the motivation in Section 1.8. Assumptions are described in Section 1.9, and the methodology is

discussed in Section 1.10, while Section 1.11 discusses the outline of the dissertation. The chapter concludes with Section 1.12.

1.2 Awareness of the Research Problem

NTLs in power systems are typically categorized into three main forms: (i) meter tampering by prepaid customers, (ii) non-payment by large power users (LPUs), and (iii) illegal connections where consumers physically connect to the grid without authorization (Romero, 2012). Among these, the present study concentrates on illegal connections as the core problem to be addressed.

NTLs are disproportionately prevalent in underdeveloped countries, where persistent inequalities in living standards and limited affordability for basic necessities—including electricity—create incentives for illicit energy access. South Africa's rural areas and townships exemplify this dynamic. Louw and Boroko (2019) note that socio-economic distress, driven by high unemployment, contributes to substantial urban migration, rapid urban expansion, and the growth of informal settlements. In such contexts, the demand for electricity and the absence of formal service provision drive electricity theft, thereby intensifying NTLs.

The World Bank reports that electricity theft in southern Africa is substantial, with estimates reaching 50% of generated capacity in some regional segments, and NTLs potentially accounting for up to 1.2% of GDP in several countries (World Bank, cited in Louw and Boroko, 2019). PennEnergy further situates NTLs within a global revenue loss framework, estimating annual worldwide losses in the hundreds of billions of dollars and ranking electricity theft among the top forms of theft (Louw and Boroko, 2019). Pauline et al. (2020) add that in certain underdeveloped countries, approximately half of generated capacity is attributed to losses, underscoring the inefficiencies and financial strain imposed on utility providers. For paying consumers, the cascading effects include increased generation costs and higher electricity prices, which further entrench the affordability gap and expand the incentives for illicit access.

1.3 Problem Statement

This research addresses the problem of illegal connections as a major contributor to non-technical losses in electricity distributions. The study posits that while meter tampering and non-payment by LPUs are relevant, illegal connections present the most tractable and impactful target for policy and technical interventions, given their direct impact on system losses and revenue leakage.

NTLs place a double burden on both utilities and consumers. For utilities, unrecovered revenue undermines investment capacity, compromises maintenance, and necessitates higher tariffs

for compliant customers. For consumers who do pay, electricity prices rise to compensate for losses, reducing affordability and potentially widening energy poverty. Additionally, elevated losses strain grid infrastructure, impede reliable service, and hinder economic development by dampening productivity and growth. The international literature (e.g., World Bank statistics and industry reports) corroborates the significant macroeconomic implications of NTLs, reinforcing the urgency of targeted interventions in high- prevalence regions.

1.4 Research Aim and Objectives

1.4.1 Aim

The aim of this study is to design, develop, and implement a smart LV distribution network monitoring and control system grounded on an Internet of Things (IoT) architecture. The primary goals are to mitigate electricity theft and to enhance protection, automation, and control of LV networks.

Specifically, the work seeks to:

- Architect an integrated IoT-enabled monitoring framework capable of real-time data acquisition, communication, and analytics across LV feeders;
- Implement robust anti-theft mechanisms through advanced metering, anomaly detection, and secure data credentials; and
- Improve protection coordination and automated control strategies to increase reliability, efficiency, and safety in LV distribution systems.

The anticipated outcome is a validated prototype and accompanying methodological framework that can be deployed to reduce non-technical losses and bolster grid resilience.

1.4.2 Objectives

The aim is attained through theoretical derivations and practical implementation.

1.4.2.1 Objectives: Theoretical analysis

- To conduct a literature review on existing solutions for combating illegal connections
- To investigate the implementation of an IoT architecture
- To develop a mathematical model for the proposed system

1.4.2.1 Objectives: Practical implementation

- To simulate the proposed system with the Proteus simulation software
- To analyse the working of the proposed system on the simulation using cases
- To build a lab scale prototype of the proposed system
- To test the working of the proposed system using cases

- To test and validate the prototype with the simulated results by comparing the responses on the cases

1.5 Research Question

The project seeks to address the following questions:

- Is it feasible to leverage developments in smart grid technology to construct a smart LV network capable of automatically detecting illegal connections and selectively disconnecting the supply to eliminate unauthorized electricity usage?
- How can the LV network be modernized to achieve enhanced efficiency, real-time monitoring, and improved safety through smart technologies?
- Is it feasible to simulate the proposed Smart LV network and construct a physical prototype to evaluate its performance under real-time operating conditions?

1.6 Hypothesis

The following statements constitute the hypotheses guiding this research:

- It is feasible to leverage advancements in smart grid technology to construct a smart low-voltage (LV) network capable of automatically detecting illegal connections and disconnecting supply to eliminate illegal electricity usage.
- Modernization of the LV network to a smart configuration will enhance efficiency, enable real-time monitoring, and improve safety.
- The smart LV network can be simulated and constructed to evaluate its performance in real-time.

1.7 Delimitations of the research

The following are the delimitations of the research:

- The literature review will be conducted only on the electricity theft and existing ways available in the market to combat this problem.
- The developed system will be simulated on the Proteus software.
- The proposed system will only be built on a lab scale prototype for the purpose of this report. Further implementation on the real network like the piloting phase is not part of the project.

1.8 Motivation for the research

The primary motivation for the research is the substantial impact of NTLs on revenue collection and energy security within South Africa’s power systems. The existing literature documents that NTLs—including electricity theft, meter tampering, and unauthorized connections—pose significant challenges not only to developing economies but also to more advanced contexts. Anecdotal and empirical evidence indicate that users may ascend utility poles to establish live

and neutral connections on bare conductors, subsequently consuming electricity without payment or accountability. Once these illegal connections are established, the resulting unmetered consumption tends to be sustained, undermining accurate load profiling and revenue realization.

Reducing NTLs is critical for alleviating strain on electricity grids. Diminished losses can translate into improved grid reliability and a reduced need for defensive measures against load shedding—an ongoing challenge in South Africa. Load shedding arises when total electricity demand outstrips generating capacity, a discrepancy exacerbated by illegal connections that elevate unaccounted-for consumption, thus affecting generation planning and reserve margins. When load shedding is implemented, all consumers—legitimate paying customers included—experience interruptions, eroding trust in the utility and potentially reducing demand-side responsiveness.

Moreover, illegal connections impose mechanical and financial stresses on distribution infrastructure. Overload conditions decrease the lifespan of distribution transformers, increasing maintenance and replacement costs for the utility. The financial implications of transformer degradation are non-trivial, influencing tariff design, capital expenditure budgeting, and overall system reliability. Against this backdrop, the proposed system aims to provide an enhanced framework for managing transformer overload and extending transformer life, thereby contributing to more resilient grid operation.

1.9 Assumptions

The study assumes the adoption of an IoT architecture that inherently depends on robust communication infrastructure. In this context, the following assumptions are posited:

- For each LV distribution transformer, there exists at least GSM (Global System for Mobile Communications) coverage within the geographic region where the transformer is deployed. This assumption ensures reliable mobile connectivity for data transmission and remote monitoring of transformer telemetry.
- The maximum distance from the transformer to the furthest customer connected to it does not exceed 1 kilometre. This constraint implies a bounded communication length for end-user devices and facilitates feasible network latency and signal quality within the deployment area.

1.10 Design and methodology

1.10.1 Research approach/philosophy

The study adopts a quantitative methodology. This choice reflects the experimental nature of the research, wherein iterative design, testing, and modification are conducted within a

controlled environment. Data is collected in numerical form and subjected to comparative analyses across successive iterations until the predefined objectives are achieved.

1.10.2 Research question/Objectives

This study adopts a methodology aimed at addressing the problem of illegal connections in LV distribution networks, with the objective of developing a novel system that can be implemented on LV distribution networks worldwide. The research questions that guide the adopted methodology are as follows:

- Is it feasible to leverage developments in smart grid technology to construct a smart LV network capable of automatically detecting illegal connections and selectively disconnecting the supply to eliminate unauthorized electricity usage?
- How can the LV network be modernized to achieve enhanced efficiency, real-time monitoring, and improved safety through smart technologies?
- Is it feasible to simulate the proposed Smart LV network and construct a physical prototype to evaluate its performance under real-time operating conditions?

1.10.3 Research Design

This study adopts an experimental, iterative design to develop a fully smart, LV distribution network. Initially, a representative model of the current legacy LV network is constructed within a simulation environment to replicate existing conditions, including illicit connections. The objective is to observe and quantify the electrical behaviour—currents and voltages—under faulty conditions in order to understand their impact on various network components. Following the observation phase, the design is augmented with IoT devices comprising sensors and microcontrollers, strategically deployed to detect the identified fault conditions. Data collected by these IoT devices are centralized for subsequent processing.

The next phase involves modifying the simulated network to incorporate actuators and switches governed by the detected conditions. After integrating IoT devices, sensors, and switching logic, the faults are re-simulated individually to verify whether the IoT system can reliably detect prevailing conditions, trigger appropriate control actions, and isolate affected sections of the LV network based on fault type and location.

Proteus Virtual System Modelling (VSM) software is selected as the platform for its accessibility and its ability to simulate power lines across multiple voltage levels while incorporating electronic components such as sensors and microcontrollers essential for IoT devices. The choice of Proteus is grounded in its robust capabilities for modelling, simulating, and analysing complex systems. The Proteus environment offers libraries that support interaction with microcontrollers and with any analogue or digital peripherals connected to them, thereby enabling integrated hardware–software co-design and verification (Pauline N. et al., 2020).

This interoperability facilitates the seamless integration of IoT devices into the low-voltage (LV) network within the simulation.

Upon completion of the simulation and verification that all IoT devices operate as intended, the project proceeds to hardware realization. All electronic components used in the IoT devices are procured to construct a lab-scale, real-life replica of the LV network. The prototype mirrors the tests conducted in the simulation, and similar procedures are executed to collect data for comparison. Data is recorded from both the simulated experiments and the prototype to assess the extent to which simulated results align with real-world performance.

In terms of data collection and analysis, the study compares electrical measurements (voltages, currents), fault detection rates, and the responsiveness of switching actions between the simulation and the physical prototype. The overarching aim is to validate the feasibility and effectiveness of a smart LV network architecture that utilizes IoT-driven detection and automated isolation to improve reliability and safety in low-voltage power distribution.

1.10.5 Data collection

The experiments gather numerical measurements of current magnitudes and voltages at various strategically placed locations on the simulated LV network using current and voltage sensors. The collected data is used to evaluate the system's ability to process and leverage these measurements to control the network.

1.10.6 Data analysis

Data is collected from both the simulated experiment and the constructed prototype. These two data sets are then compared to determine whether the prototype confirms the results of the simulation. The observations arising from the comparative analysis are discussed.

1.10.7 Ethical considerations

This study constitutes experimental research conducted within a controlled environment and poses no potential harm to humans, animals, or the environment. The primary ethical concern pertains to the management of bias and the integrity of data handling. Measures were implemented to ensure that data is collected and recorded accurately, maintaining transparency and preventing any manipulation intended to distort findings or to propagate a predetermined narrative in support of the hypothesis.

1.10.8 Limitations

The experimental setup is designed to closely emulate the behaviour of a real-world low-voltage distribution network. However, the study is conducted at a small scale using low voltages and compact sensors, which constrains the generalizability of the findings. Consequently, the data and results obtained from this experimental framework are limited to a

laboratory environment and do not fully capture the complexities of a live LV network. In particular, real-world conditions such as high-voltage surges, lightning events, and adverse weather can introduce dynamics not represented in the laboratory tests.

As a result, there remains a need to transition the developed system to real-life piloting in an operational network to observe its performance under all pertinent conditions. Although the South African Power utility company Eskom has approved piloting for the proposed system and preparatory work has commenced, the outcomes of the pilot phase lie outside the scope of this report. They are not included in the requirements for the completion of the current research due to time constraints and the extended duration required to conduct a thorough pilot observation.

1.11 Chapter breakdown

The dissertation comprises six chapters. The following sections provide concise summaries of each chapter's content.

1.11.1 Chapter One

Chapter 1 introduces the thesis by articulating the problem awareness and the central research problem to be addressed. It subsequently presents the hypotheses, and clearly states the study's aims and objectives. The chapter also defines the scope and boundaries of the investigation, along with the assumptions underpinning the research. A concise overview of the research design and methodology is provided, outlining the chosen approach, data sources, and analytic techniques. Finally, the chapter highlights the anticipated contributions of the work and briefly describes the organization of the remainder of the thesis.

1.11.2 Chapter Two

This chapter presents a literature review of electricity theft, with particular emphasis on illegal connections. It analyses the drivers of electricity theft, its impacts on stakeholders and utility systems, and surveys the proposed solutions as reported in the extant literature.

1.11.3 Chapter Three

This chapter provides an overview of the legacy electrical grid, with particular emphasis on the current state of LV distribution networks and the intrinsic deficiencies that give rise to issues such as energy theft and a range of faults impacting reliability and efficiency. The discussion subsequently analyses current flow within LV networks through the framework of Kirchhoff's current law, illustrating how network topology governs observed behaviour. Building on this theoretical foundation, the chapter develops a concept for smart low-voltage networks that integrates IoT devices into LV infrastructures to realize a fully automated, intelligent distribution

system. The proposed approach aims to enhance monitoring, control, and protection, thereby improving the security, reliability, and efficiency of LV networks.

1.11.4 Chapter Four

This study reports the development of a laboratory-scale smart low-voltage prototype designed to evaluate the functionality of the proposed system prior to piloting it in a larger distribution network. In this chapter, a simulation of the smart low-voltage network is also presented, conducted using Proteus simulation software to verify the prototype results and to compare them with the expected performance.

1.11.5 Chapter Five

This chapter presents the testing of both the smart LV prototype and the simulated network implemented in Proteus. It assesses the feasibility of implementing a smart LV network based on the results obtained from these tests. The discussion analyses the findings from the experimental tests and simulations to evaluate the viability, performance, and potential challenges of the proposed system.

1.11.6 Chapter Six

This concluding chapter synthesises the dissertation's findings, providing a concise overview of each chapter's contributions and articulating the principal takeaways and their implications for theory, practice, and future research.

1.12 Conclusion

This chapter has introduced the dissertation by framing the central problem and outlining the foundational components of the research. It presents the awareness of the problem, articulates the problem statement, and enumerates the aims and objectives. A hypothesis is proposed, alongside potential research questions, explicit assumptions, and the overall research design and methodology. Additionally, the chapter provides a comprehensive outline of the structure of the dissertation, detailing the sequence and scope of each forthcoming section.

Chapter Two offers a literature review focused on illegal connections and prior efforts aimed at mitigating or eradicating such practices. The review synthesizes existing literature on the phenomenon and surveys the methodological approaches employed in related studies. By examining prior research methods, the literature identifies effective strategies and potential gaps that inform the current study's methodological choices.

2. CHAPTER 2
LITERATURE REVIEW ON ELECTRICITY THEFT AND EXISTING SOLUTIONS

2.1 Introduction

Amidst appeals for rapid and urgent action on climate change, as underscored by the recently concluded COP29 in Baku, the United Nations Sustainable Development Goals (SDGs) 7 and 13 explicitly encourage all stakeholders to ensure access to clean and sustainable energy for everyone (Arora, 2025). Moving forward, most countries and intergovernmental organizations have prioritized sustainable development by placing affordable, clean, and reliable energy availability at the centre of their efforts. However, efforts to reduce population dependence on finite fossil fuels for conventional energy have coincided with an overall increase in energy demand. Consequently, utility firms are compelled to reinvest profits in alternative forms of renewable electricity generation. This trend is not evident in developing nations however, where electricity theft remains a major challenge. Countries such as South Africa, Ghana, and India are illustrative examples (Williams et al., 2023).

A principal cause of non-technical losses in power systems is electricity theft, including fraud, non-payment, pilferage of prepaid cards from vending machines, and illicit electrification schemes. Today, most power utilities worldwide view electricity theft as a critical concern, with substantial financial costs borne by governments and power companies alike (Zulu and Dzobo, 2021). Electricity theft accounts for a substantial portion of distribution-line losses—estimates exceeding 50% in some contexts. Notwithstanding its severe and often lethal consequences for small businesses, utilities, the public, and the perpetrators, electricity theft continues to rise, as evidenced by data from 102 countries (Williams et al., 2023).

Therefore, it is imperative to implement adequate measures to reduce power losses attributable to electricity theft, thereby mitigating financial losses for power utilities and their broader economic impact. Such measures include the development of systems that automatically detect and monitor instances of electricity theft within the power system grid.

The principal objective of the study is to develop a system capable of mitigating illegal power connections in low-voltage networks. Accordingly, a literature review is warranted to survey prior publications and prior works addressing this problem. The sections for this chapter are outlined as follows; Section 2.2 outlines the literature search methodology. Section 2.3 presents the literature on illegal power connections; Section 2.4 offers a comparative analysis of developments in the existing literature; Section 2.5 presents discussion; and section 2.6 concludes the chapter.

2.2 Literature search

A comprehensive search was conducted using accumulative databases that aggregate information from multiple publishers, employing two key phrases: “electricity theft” and “illegal electricity connections.” The initial search for “electricity theft” retrieved 575 publications whose metadata matched the search terms. Upon screening the results, it became evident that these publications encompassed a wide range of study types related to electricity theft in general, without narrowing to the specific type and problem this study seeks to address. To reduce the breadth of results, the second search was conducted using the phrase “illegal electricity connections,” yielding approximately 43 publications. A review of the publication descriptions identified 36 papers appearing relevant to the study. Further analysis of the documents’ contents refined the corpus to about 22 papers that are pertinent to the research aims. Of these, 13 studies offered solutions targeted at addressing the problem, while the remaining works comprised studies of the problem, theoretical analyses, and statistical assessments. Consequently, 22 studies are included in the literature analysis.

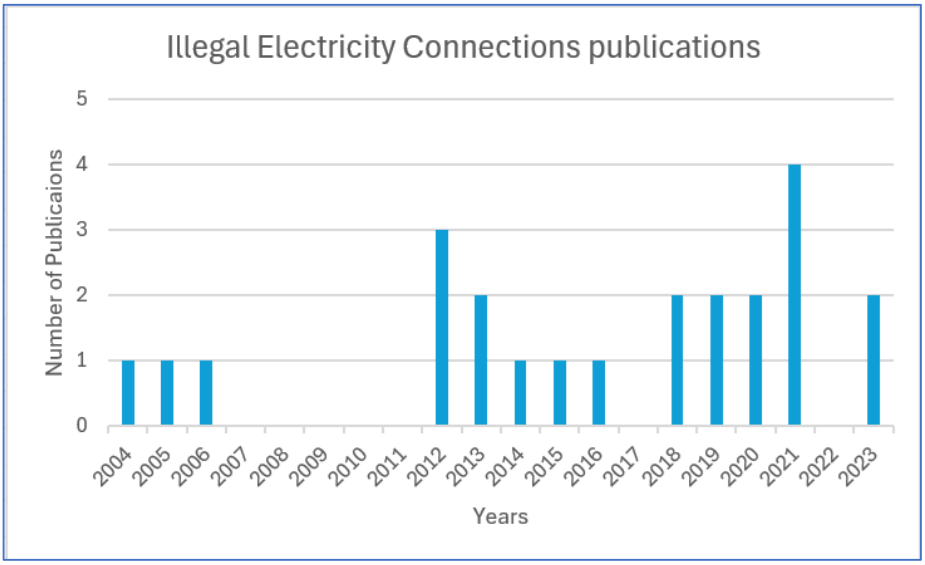

Figure 2.1: **Bar graph showing the number of publications per year**

Figure 2.1 presents the temporal distribution of publications addressing illegal connections. The figure indicates that scholarly activity on this topic began in 2004, with one publication per year through 2006, after which scholarly output appears to have declined. A notable resurgence occurred in 2012, with three publications, followed by a reduction to two in 2013 and one in 2015 and 2016, respectively. There were no publications in 2017; however, the topic reemerged in 2018 with two publications and remained pertinent through 2021, with two publications per year and a peak of four in 2021 alone. Following a brief gap in 2022, two additional publications were recorded in 2023. This analysis suggests an ongoing need for

research on unlawful electrical connections, given the relatively sparse number of publications proposing globally applicable solutions, indicating that the issue persists without a widely implemented innovative remedy.

2.3 Literature review on electricity theft

2.3.1 Power System Overview

The electric power system comprises three principal components: generation stations, the transmission system, and the distribution system. The primary objective of this system is to generate, transfer, and distribute electrical energy with maximum efficiency, ensuring that consumers receive electricity at reliable voltages and frequencies (Babu et al., 2012).

Generation and transmission facilities are typically situated outside densely populated regions, which can impede public access. The distribution subsystem begins at the substation and directs electricity to structures within urban and rural areas for end use. This system can be subdivided into two main elements: (a) primary distribution, which commences at the distribution substation and terminates at the distribution transformer. It generally encompasses voltage levels of 22 kV, 11 kV, 6.6 kV, and 3.3 kV; and (b) secondary distribution, which starts at the distribution transformer and ends at the consumer and predominantly involves single-phase 230 V and three-phase 380 V systems (Khan et al., 2013).

Within a power-system grid, numerous operational losses occur and can be categorized as technical and non-technical. Technical losses arise from power dissipation in transmission lines, transformers, generators, and other components of the grid. These losses can be quantified rapidly and accurately using the technical characteristics of the grid, such as sending-end voltage and current and the impedance of transmission lines. In contrast, non-technical losses are more challenging to quantify precisely, as they originate from external sources and must be estimated by comparing the total energy billed to the total energy supplied to electrical consumers (Williams et al., 2023; Zulu and Dzobo, 2021).

2.3.2 Electricity Theft and Non-Technical Losses in Power Distribution System

Non-technical losses (NTLs) in power systems are typically categorized into three main areas: meter tampering by prepaid customers, non-payment or evasion by large power users (LPUs), and illicit connections that bypass authorized metering and supply arrangements (Babu & Sushma, 2013; Louw and Bokoro, 2019). Meter tampering compromises the integrity of metering infrastructure, while illicit connections directly undermine the revenue stream of distribution utilities. In addition, large power users may evade payments, exacerbating financial losses and contributing to unstable power supply.

The distribution network serves as the essential bridge between generation and end-use loads. It comprises feeders, distributors, service mains, and associated control and protection equipment (Babu et al., 2012). A central issue arises from the distribution system's expansive reach within densely populated areas, where low and easily accessible voltage levels can enable direct connections to electrical appliances, circumventing proper metering. Such practices increase technical losses and are prohibited (Khan et al., 2013). As utilities migrate toward more sophisticated architectures, the distribution infrastructure is increasingly adopting smart-grid concepts, characterized by two-way communication between devices, particularly within Advanced Metering Infrastructure (AMI) (Bastos et al., 2023; Neagu et al., 2018; Sharma et al., 2021).

The evolution toward smart grid infrastructure offers opportunities for improved detection and mitigation of NTLs. Enhanced monitoring, real-time data analytics, and automated fault and anomaly detection can strengthen supervisory control and data acquisition (SCADA) systems and AMI. However, despite these advances, electricity theft remains a pervasive challenge for utilities worldwide, with substantial financial implications for governments and energy companies (Sharma et al., 2021; Raggi et al., 2020).

In developing nations such as India, electricity theft constitutes a major impediment to reliable power delivery and systemic financial health. Theft manifests in various forms, including fraud, non-payment, pilfered vending mechanisms, prepaid schemes exploited through illicit means, and unauthorized electrification schemes (Williams et al., 2023). The economic impact is compounded by degraded service quality and increased system losses, which necessitate robust policy intervention and technological modernization.

2.3.3 Causes of Electricity theft

Electricity theft is a problem that disproportionately affects underdeveloped and developing countries, where significant inequalities in living standards constrain access to basic services, including reliable electricity. In these contexts, large segments of the population cannot afford official electricity supply, which fosters illegal connections and non-technical losses. For example, in South Africa, rural areas and townships experience substantial impacts from such losses.

Louw and Bokoro (2019) attribute the pronounced non-technical losses observed in South Africa to underlying socio-economic problems, chief among them a high unemployment rate. This unemployment drives considerable rural-to-urban migration as individuals seek employment opportunities. The resultant rapid urbanization accelerates the growth of informal settlements established by migrants, where energy demand outpaces formal infrastructure provision. The combination of unemployment, limited access to affordable electricity, and the

informal nature of housing in these settlements creates a milieu in which electricity theft becomes a practical response to constrained legitimate supply. Consequently, unauthorised connections and power theft emerge as adaptive strategies within these communities, exacerbating non-technical losses and complicating efforts to ensure equitable and reliable electrical supply.

2.3.4 Impact of Electricity theft

Electricity theft in southern Africa is reported by the World Bank to be as high as 50% of generated capacity in certain regions, with non-technical losses potentially amounting to as much as 1.2% of Gross Domestic product (GDP) in several countries worldwide. Unauthorized consumer connections, which are not properly qualified, generate accidents requiring substantial repair work, cause abrupt voltage surges, and accelerate premature deterioration of the electrical network. These incidents, along with early wear of equipment, adversely affect both electricity providers and the paying consumers who fund the system (Basak et al., 2019; Korovkin et al., 2021).

Recent studies indicate that energy theft imposes annual global costs of approximately US$89.3 billion, of which US$58.7 billion are borne by developing nations such as South Africa. The cascading effects of theft—most notably pronounced electricity shortages and potential load shedding—have a deleterious impact on national economic growth (Pealy and Matin, 2021; Williams et al., 2023; Zulu and Dzobo, 2021). The Ridge Times reports that South Africa faces six forms of electricity theft, resulting in average losses of up to ZAR20 billion (about US$1.5 billion) per annum: theft of cables, extraction of oil from substations, damage to utility equipment, non-payment of power bills, and the sale and use of illegally obtained prepaid vouchers from pilfered vending machines (Zulu and Dzobo, 2021).

A 2015 Eskom report estimated that illicit connections accounted for 6% of South Africa’s GDP in revenue loss, with approximately ZAR1.5 billion in electricity revenue lost between July 1, 2012, and June 30, 2013. The EThekwini Municipality in Durban, KwaZulu-Natal, allocates around ZAR300 million annually to anti-electricity-theft initiatives, including programs that promote lawful, safe, and economical electricity use by detecting and prosecuting electricity thieves (Zulu and Dzobo, 2021). According to Penn Energy, global non-technical losses amount to US$96 billion, with electricity theft ranking as the third most stolen commodity worldwide (Louw and Bokoro, 2019). Pauline N. et al. (2020) suggest that some underdeveloped countries experience losses equivalent to approximately 50% of generated capacity, imposing added strain on electrical grids as utilities must generate double the necessary energy to satisfy demand and ensure service to paying customers. This dynamic elevates generation costs and, consequently, electricity prices for consumers.

2.3.5 Papers reviewed

The body of related work addressing power usage and the reduction of electricity theft within electrical distribution systems is summarized below. Table 2.1 presents an overview of the evaluated literature. Key features highlighted in the table include the authors' objectives, the hardware and/or software employed, and the corresponding conclusions.

Table 2.1: Comparison of papers published on proposed solutions to address electricity theft

Paper (Reference)	Aim of the project	System overview	Hardware/Software required	Authors Conclusion
Illegal Connection Location on Main Power Cable (Pavic et al., 2004) And, Reduction of non-technical losses based on Time Domain Reflectometer (TDR) principles and function (Trupinic et al., 2005) These two papers are written and published by two writers but in essence proposing the same solution.	The primary objective is to establish a foundational mechanism for identifying potential energy theft and for accurately determining the precise length and location of illicit electrical connections.	The theoretical foundation and operational principles of the Time Domain Reflectometer (TDR) underlie the methodology described herein. Analogous to radar systems, the central concept of the TDR is pulse reflection. Upon connection to a pair of conductors at one terminus of a cable, the device generates a brief incident pulse. In accordance with transmission-line theory, this pulse propagates along the conductor and, at points of impedance discontinuity—such as cable damage, an opposing termination, or other alterations in geometry—splits into reflected pulses. The distance to the impedance discontinuity is determined by measuring the elapsed time between emission of the incident pulse and the return of the reflected pulse, combined with knowledge of the propagation velocity within the cable. The composite impedance of the cable is a function of its intrinsic resistance, inductance, and capacitance per unit length, as well as any external loading. The system is designed to address scenarios in which cable connections are obscured by operators or other actors in private environments, such as yards, where utility personnel lack direct access during routine inspections.	The authors employ a Time Domain Reflectometer (TDR) to perform the diagnostic tests associated with the method. The TDR setup comprises a standard oscilloscope and a sinusoid signal generator.	For all unauthorized connection types located on the primary home power supply, the described technique is advised. A primary household power cord can be tested for approximately 30 minutes. When testing the same main power cables in the future, the transmission and reflected pulses of the cables are stored on a personal computer and subsequently compared and analysed using the TDR's internal memory. It should be noted that, in order to perform the test, the consumer's main cable must be disconnected from the power supply. These types of tests can be conducted concurrently with other scheduled maintenance tasks.
Use of the Shunts Detecting Equipment for	To develop and evaluate an authorized investigative methodology for	A portable apparatus designated as a "lines and shunts detector" has been developed for commercial	Shunt detector equipment is used to demonstrate the	The recognition of an unlawful connection when indicated by an energy-balance

the Identification of Illegal Power Outlets (Parra and Calderon, 2006)	identifying clandestine electrical connections within a facility's distribution network. The objective is to deploy a vetted, legal instrument capable of locating unauthorized taps with sufficient precision (in terms of distance and depth) to inform corrective actions, thereby reducing time and resources spent on inspections while ensuring compliance with relevant safety and regulatory standards.	deployment to locate metallic pipework (e.g., gas, water, or cable television conduits), pipe valves, electrical service lines, and related derivatives. The device operates by injecting a low-power signal at a predetermined alternating frequency directly into the target pipe or electrical conductor, or by employing inductive coupling via a clip-on coil. The injected frequency is deliberately chosen to be distinct from the standard operating frequency of the system under investigation; for example, it differs from typical power line frequencies such as 50 Hz or 60 Hz. The detection system comprises two principal components: a transmitter and receptors. Transmission modality is contingent upon several factors, including whether the conductor is energized, whether it forms a closed loop or a bow when endpoints are connected, and whether access to the conductor is available to the transmitter for signal injection. The transmitter may introduce the signal through one of three modalities: conductive injection, inductive coupling, or purely inductive induction, with the selection guided by prior information about the conduit and its environment. After selecting the appropriate injection or induction method, the receptor is employed to trace the primary conducting pathway and to identify and monitor potential derivatives of the transmitted signal. This methodology facilitates the identification of all alternatives to the primary pathway, including illicit tap points, by analysing the detected conduction paths.	effectiveness of the proposed system	discrepancy remains contingent on further scrutiny to identify the precise cause. Nevertheless, the employed method has demonstrably reduced detection time by at least 50%. Furthermore, relative to the resources typically required for personnel teams and material supplies in such operations, the costs associated with shunt placements—including labor and materials—have been reduced by 80%.
Parameter Identification of Unknown Radial Grids for Theft Detection (Weckx et al., 2012)	This study offers a method for detecting electricity theft (double feeding) by extracting a linearized load flow model from smart meter data.	When precise distances between residences or the cable length connecting a smart meter to the distribution feeder are not available, this work proposes an algorithm capable of locating the grid section and identifying customers who either double-feed or tamper with the meter. The proposed algorithm rests on the assumption that, for	The study employs a simulation-based methodology to evaluate and illustrate the functioning of the proposed system. Specifically, a three-phase, four-wire radial low-voltage distribution network with a TT earthing configuration for residential	In the expanding domain of smart grid applications, accurate knowledge of the grid topology is essential. The proposed linearized model yields information on both the location and the phase of each customer, enabling a granular representation of the system. The results indicate that the errors associated with

		each customer, both active power (P) and reactive power (Q), as well as voltage magnitude (V), are measured by a smart meter. To determine the time instances of theft, the system operator can compare the substation-measured power with the aggregate measured consumption. This information may be stored within a database for traceability and forensic analysis.	customers is modelled and tested within the simulation environment. The choice of simulation software is not specified in the report.	the linearization are negligible for the purposes of topology identification and state estimation within radial networks. A notable application of the linearized load-flow model is its potential to address electricity-theft detection and mitigation in radial grids, where unauthorized consumption poses a major challenge to reliable power delivery.
HVDS approach for reducing the Technical and non-technical losses to enhance the Electrical Distribution System performance (Babu et al., 2012) And, Operation and Control of Electrical Distribution System with Extra Voltage to minimize the Losses (Babu and Sushma, 2013) These two papers are written by the same writers, with the later paper using a software for simulation to reproduce the result for verification of the study.	In order to improve the distribution system performance, this study proposes a new methodology that minimizes both non-technical and technical losses.	The proposed system aims to improve the voltage profile and reduce losses in the distributor phase by elevating the distribution voltage from its nominal level (100%) to a higher level (approximately 152%), corresponding to an increase from 230 V to around 350 V at the distribution point. A dedicated voltage-regulation device is then employed to step the voltage down to the conventional customer-side voltage of 230 V. The methodology achieves substantial reductions in both technical and non-technical losses, with reported total system power savings of up to 49.12%. variability.	A prototype of the proposed system was constructed using a three-phase distribution transformer rated at 11 kV / 415 V / 230 V, in conjunction with a voltage booster (230 V to 350 V) connected to the transformer's secondary winding. To indicate an unauthorized connection, a 16 W compact fluorescent lamp is connected between the R-phase and neutral at the secondary side of the voltage-boosting transformer. In addition, three compact fluorescent lamps are connected across the secondary side of a specialized voltage regulator device (SVRD) located at the consumer end. The three SVRD units, each with a rating of 350 V / 230 V, are inserted across the corresponding phase–neutral pairs of the voltage booster. A simulation of the same setup is constructed on MATLAB Simulink.	The proposed approach offers a low initial cost and, by reducing both technical and non-technical losses while enhancing the voltage profile at the distal end of the network, is expected to yield a substantial improvement in overall system performance. Moreover, this approach supports a strategic shift toward postponing the development of new power plants and delaying the procurement of electricity from nearby states, thereby influencing longer-term planning and resource allocation in the power sector.
Payback Analysis in Identification and Monitoring of Commercial Losses in Distribution Networks (Evaldt et al., 2012)	A low-cost power meter prototype for identifying commercial losses in distribution networks is presented in this research.	The Intelligent Electronic Device (IED) constitutes the foundational component of the system architecture. Predetermined locations are designated for the placement of the IEDs, which in turn supply power to a defined group of consumers. Power meters are distributed across the distribution network using a wireless channel arranged in a cascade communication mode. The	A Hall effect sensor, which operates linearly for electric current measurements and provides an output voltage proportional to the current passing through it, is employed. For preliminary experimentation, a low-current sensor with a 30 A peak rating is utilized; in the final prototype,	The project demonstrated favourable behavioural characteristics during circuit testing and showed potential for favourable return on investment, which supports considerations for its implementation. It should be noted that, although the circuit cannot entirely eradicate fraud, it constitutes a highly effective mechanism for the rapid

		disparity between measurements recorded by successive IEDs within the same network segment serves as an indicator of commercial losses in that segment. A computing system located at the distribution control centre processes and analyses the data received from the IEDs and employs the network model to identify billing inconsistencies. At the conclusion of a specified period (e.g., monthly), the utility can compare the volume of electricity delivered to residences by the IEDs against the aggregate total recorded by each customer's individual meters.	this sensor is replaced by a 550 A peak model. To monitor the system voltage, a voltage transformer is incorporated. The digital data processing is performed using a microcontroller from the Microchip RF PIC family, which includes an integrated RF transmitter. Since the central processing unit (CPU) contains only a transmitter module, an RF receiver module is added to enable bidirectional communication. The antenna system is implemented on a printed circuit board (PCB) forming a loop configuration to support the RF propagation characteristics required for the experiment.	identification of irregularities. In practice, this capability could contribute to reducing the frequency of on-site inspections. However, it is important to acknowledge that such reductions are not the primary objective of the system and are accompanied by substantial maintenance costs, which can undermine prudent allocation of time and financial resources.
Intelligent modelling Scheme for Detection of Line Losses in Power Distribution System (Khan et al., 2013)	This paper's main aim is to provide a method for electricity theft detection and prevention.	The proposed system enables a real-time comparison of power consumption at the consumer's terminal with the power delivered by the transformer. This interface is implemented through GSM communication and microcontroller-based monitoring within the low-voltage (LV) network. By juxtaposing the electricity supplied by the distributor and the electricity consumed by the end user, the system facilitates the detection of electricity theft. The principal modifications to the power distribution framework associated with this approach are as follows: (a) Real-time power statistics measurements conducted between the distributor and the consumer; (b) continuous comparison of power delivery and actual utilization; and (c) expedient notification of power mismatches to the appropriate authorities	There is no software or hardware used on the study. This paper is a theoretical-based paper. Micro controllers and GSM modules are proposed hardware that could be used.	This study rests on theoretical and ideological assumptions regarding its implementation. Accordingly, it is advisable that extensive empirical research be conducted to address any technical challenges associated with electronic devices used in the proposed system. Presently, the power-theft detection equipment is connected only to the secondary distribution network; however, future work should explore extending monitoring to the entire power system to facilitate the effective management of excessive line losses. Additional investigation is warranted into a mechanism by which a microprocessor can restrict the electricity usage of unauthorized users without adversely impacting the usage of legitimate customers.
Equipment for monitoring and combating of non-technical losses in distribution networks Penner et al., 2014)	The aim of the project is to develop an affordable Distribution Transformer Monitor (DTM).	The device measures, stores, or transmits, via GSM, the power consumption recorded at the transformer to the utility company. The utility provider compares this transmitted data with the consumer's reported or	The system prototype is constructed utilizing components comprising a microcontroller (Arduino ATmega168), an SD card module, an	Several utilities that provided funding for the project across multiple Brazilian states installed the Digital Telemetry Modules (DTMs). The data collected by these systems are subsequently utilized by

		monitored power usage to detect inconsistencies. Any notable discrepancies between the measured consumption and the consumer's usage indicate potential electricity theft.	LCD display, a real-time clock (RTC), as well as voltage sensors and clamp-on current sensors. Software development for the microcontrollers was performed using the Arduino Integrated Development Environment (Arduino IDE). of the prototype.	the ongoing non-technical loss (NTL) detection program, which is currently under development.
Non-Technical Losses in Power System and Monitoring of Electricity Theft Over Low-Tension Poles (Chauhan, 2015)	The aim of the project is to develop a monitoring methodology for detection of electricity theft over low tension distribution lines.	The proposed approach involves positioning contemporary monitoring devices along the transmission path between the two poles in order to enable theft detection over long-distance (LT) lines. Under the assumption that no load is connected between the poles, the current flowing between them remains approximately equal when the supply voltage is constant. A measurable deviation in this current is observed when an unlawful load is introduced between the poles. Moreover, the location of the theft or unauthorized load insertion can be precisely identified, as the corresponding current perturbation is captured and recorded by the monitoring infrastructure.	A working prototype is built using the following electronics components: Microcontroller, Analog-to-Digital Converter (ADC). Current transformers. Liquid Crystal Display (LCD).	The suggested system's disadvantage is that it can only be used for pole sections with no load linked between them.
Illegal connection location on distribution lines using traveling waves method (Medrado et al., 2016)	The aim of the project is to develop a method for identifying unauthorized, clandestine connections in distribution lines based on the regular and known load of a network sections of 13.8 kV with extension 15.55 km.	The traveling-wave method for fault localization relies on precise timing of the transient voltage or current wave as it propagates from the fault location to the line terminals where monitoring locators are installed, together with the known propagation speed of the wave along the transmission or distribution line. The method exploits the highly transient signal generated by the sudden change in load or fault condition at the point of disturbance. The proposed locator architecture incorporates an alternative technique that requires two network analysers, each installed at the terminal of the respective transmission/distribution line. By determining the difference between the arrival times of the initial transient wave at the two analysers, the location of the fault or load within the	A computer model is developed using the ATP / EMTP (Alternative Transients Program / Electromagnetic Transients Program) software	It is recommended that a novel product be developed to implement this technique within operational distribution networks. Such a product would mitigate financial losses associated with power distribution and enhance the precision with which covert connections in distribution networks can be identified. By enabling practical deployment in real-world systems, the proposed solution holds promise for improving overall network efficiency, reliability, and security.

		monitored segment can be inferred.		
The method of detecting illegal electricity consumption using the AMI system (Dudek et al., 2018)	The aim of the project is to compare 3 analytic techniques of detecting electricity theft using an Advance Metering Infrastructure (AMI) system and suggests the more accurate method.	The 3 analytical techniques are methods based on voltage drops, Kirchhoff's laws and loads. The study is trying to find which of these 3 methods are more accurate so that it can be suggested for deployment in the real world	Simulations are carried out for a MV/LV station, supplying power to 20 users with AMI meters. The software used is the Advanced Metering Infrastructure (AMI) software.	This study describes three analytical techniques for identifying the use of unauthorized electricity. Due to insufficient measurement accuracy, both the Kirchhoff's law-based approach and the voltage-drop method exhibit errors that are too large for practical, real-world application. While the load-based approach has not yet been validated under real-world conditions, it appears more promising in establishing the foundational framework for illicit electricity consumption detection.
Influence of Outliers on Transformer Power Losses Estimation Using a Statistical Based Data Mining Approach (Neagu et al., 2018)	The study offers a novel data mining-based method that applies the fundamentals of Knowledge Discovery on Databases (KDD) with a particular focus on identifying outliers detected by smart meters.	Human analytical capability, when deployed without automation, is markedly outstripped by the potential for extensive database analysis. Modern computer memory enables the storage of large volumes of data, and with appropriately calibrated algorithms, anomalous or atypical data patterns can be identified. Consequently, an operator can supervise automated procedures designed to detect aberrant data trajectories. Data mining, as an approach, serves to reduce measurements to variables that are most informative, while discarding extraneous, unknown, or potentially salient information. Concurrently, data mining extracts knowledge from the databases generated by software tools, uncovering implicit insights that were not previously evident but may prove valuable in a given context.	MATLAB is utilized to apply the data mining technique.	This study proposes a novel data-mining approach, grounded in statistical and information-theoretic techniques derived from smart-meter data, to detect anomalous usage. A real-world database comprising 300 rural substations was employed to evaluate the method. The results indicate that the proposed approach effectively identifies and removes outliers, which in turn enhances the accuracy of energy-loss estimation. The analysis reveals that certain factors exert a disproportionately large influence on the assessment of power losses, while others have comparatively smaller effects. By applying the methodology to compute energy losses, a more precise quantification is achieved. Notably, the removal of outliers corresponds with a demonstrable reduction in active energy losses; however, the specific study context exhibits low loading on power transformers, which may influence the generalizability of the findings.
IoT Based Drone Operated Monitoring of Distribution Transformers and Terminating Illegal Power Connections	The purpose of this study is to suggest an Internet-of-Things (IoT) based drone system for monitoring distribution transformers and cutting off unauthorized power connections.	A drone has been deployed as a surveillance instrument within this project. The aircraft is preconfigured with a Global Positioning System (GPS) module to monitor the electrical distribution pathway and to detect any unauthorized connections.	Solar powered drone with a camera, motorised telescopic extension and a solenoid valve operated cutter are some of the hardware mentioned for the proposed project.	This study presents an architecture in which unmanned aerial vehicles (UAVs) are integrated into a control loop for power-industry applications, whereby UAVs are responsible for real-time data collection. The envisioned

(Basak et al., 2019)		Upon detecting such connections, the drone utilizes a built-in telescopic-extension cutter to sever them promptly. In addition, a thermographic (infrared) camera and a current-measurement device are employed to monitor the temperature of distribution transformers and the current drawn from them. If abnormal temperature or current conditions are observed, the transformer-associated alarm is triggered, and the local operating station is notified. The implementation of this surveillance system is anticipated to substantially reduce losses within the power sector and to mitigate adverse effects associated with transformer fault conditions.		paradigm—real-time data acquisition, autonomous analysis, and responsive action—constitutes a significant advancement toward a theft-resistant power sector. The deployment of UAVs offers notable economic benefits for a country like India, where the electricity sector has suffered substantial losses due to illegal connections and inadequate transformer maintenance. When combined with a sensor network, drones have the potential to transform, and possibly supplant, traditional Supervisory Control and Data Acquisition (SCADA) systems in the future. Further research should address security, reliability, and scalability considerations to ensure robust integration within existing power-system infrastructures.
An Alternative technique for the detection and mitigation of electricity theft in South Africa (Louw and Bokoro, 2019)	The aim of the project is to investigate the application of zero-sequence current-based detection as a mitigation strategy to deal with illegal connections by ground surface conductors.	In a three-phase power distribution network, an earth fault condition leads to the establishment of a zero-sequence current (ZSC). This study employs monitoring of ZSC at the star-point node of the distribution transformer as a secondary method for detecting energy theft associated with exposed conductors in contact with the ground. Furthermore, the work proposes point-of-distribution isolation as a means to mitigate revenue losses, power-quality disturbances, and risks to human safety. Results indicate that the underlying theory supports the proposed alternative technique as both a mitigation and detection mechanism for non-technical losses (NTL) arising from ground-lying bare conductors that contribute to electricity losses.	The DigSILENT software package version 15 is used to perform simulations of a simplified network. Furthermore, a laboratory experiment is created to verify the DigSILENT results.	Ongoing studies are being conducted to elucidate the impact of ZSC (Zero-Sequence Current) in real-world settings. The primary objective of this study is to ascertain the fundamental characteristics of ZSC components through the compilation of field data collected over time. Building on these empirical insights, the researchers design and implement an algorithm that is integrated into a custom measurement device. The intended function of this system is to provide alerts and, if necessary, isolate the affected supply node in situations where unauthorized connections are introduced by bare-ground surface conductors.
Embedded Power System Monitoring of Illegal Power Connections in Kenyan Domestic Supply (Pauline N. et al., 2020)	The objective of this project is to develop an embedded-system device capable of remotely locating users who attempt to tap power at the service head without being billed.	Through Global System Communication (GSC), the system immediately notifies the utility company of the status of the affected electrical connection. This capability is intended to reduce the cost of power by protecting Kenya's distribution network from high non-technical losses (NTLs) associated with unauthorized connections. The system operates on	MATLAB/Simulink is utilised in conjunction with Proteus Virtual System Modelling (VSM) for the development of the embedded system model. The approach encompasses the collection of monitored information and the analysis of detected	The study successfully designs and simulates an embedded power-system prototype capable of tracking and identifying unauthorized electricity connections in Kenya. The automated system offers utility companies a means to reduce domestic electricity theft by remotely monitoring illicit connections and issuing SMS alerts whenever

		real-time current measurements. The hardware configuration comprises two sensor modules installed at strategic points: one placed upstream (before the cut-out) and one downstream (after the cut-out) of the service line, in addition to a 240-volt service line. The configuration supports three interconnected loads (lamps), an interrupting switch, an LCD display for user interface, and several key electronic components, including a microcontroller for data processing. The system incorporates two current-sensing devices: one to monitor the incoming supply current and another to monitor the current drawn by the load. Data collected by these sensors are transmitted via a linked serial monitor to the utility provider.	data. Proteus is employed due to its robust capabilities in modelling, simulating, and analysing complex systems. The Proteus environment provides libraries that facilitate interaction with a microcontroller and any analogue or digital peripherals interfaced with it, enabling integrated hardware–software co-design and verification.	aberrant readings are detected at the customer intake point. The device incorporates an automatic interrupting switch, enabling remote disconnection of power to users attempting to establish unauthorized connections. Consequently, this design obviates the need for manual inspection and its associated time-consuming procedures.
Non-Technical Loss Identification by Using Data Analytics and Customer Smart Meters (Raggi et al., 2020)	The study's goal is to present a novel method for identifying non-technical losses using the customer's smart meter and data analytics.	This approach constitutes a data-analytic technique derived from a three-phase state estimator, tailored for the detection and localization of NTLs through data obtained from smart meters. The method adopts a Weighted Least Squares (WLS) formulation and incorporates principles of faulty data analysis to enhance robustness against measurement anomalies. To locate and identify NTLs, the authors introduce a novel index based on the correlation of measurement residuals. It is important to emphasize that, in contrast to conventional state estimation (SE) tools, the proposed approach is designed for offline application and does not aim to estimate the overall operating state of the distribution system in general terms. Rather, the conceptual framework is developed as a specialized application technique for the localization and detection of NTLs.	The suggested algorithm is validated using simulations, however the program used is not mentioned.	The customer smart meter represents a tool with potential benefits for distribution system management, contingent upon the development of methods capable of converting the substantial data generated by these devices into actionable information. In this context, the present work proposes a novel data-analytic approach for non-technical loss (NTL) localization and detection, addressing illicit connections that arise from prior deficiencies in data analysis.
Tackling Energy Theft in Smart Grid-A Comprehensive Review and Framework (Pealy and Matin, 2021)	This article focuses on the detection and control of energy theft from smart meters, with the goal of aiding utility companies in identifying unlawful connections and taking appropriate action.	This study describes a microcontroller-enabled system configured to monitor and log the energy consumption of a residence. Specifically, the microcontroller is programmed to display the House's regular energy usage and to persist this	Proteus simulating software is used to simulate the proposed system	To fully harness the benefits of smart grids, it is essential to reduce their vulnerabilities. This paper tackles the issue of electricity theft and proposes a preventive measure to curb energy theft through the deployment of smart

		data in non-volatile memory for subsequent retrieval and analysis. The smart meter portion of the system interfaces with the microcontroller to enforce a load-control mechanism: when the total electrical load exceeds the established baseline, a blockage message is displayed to indicate an overage condition. In a manner analogous to standard utility installations, the smart meter is connected to the power provider's infrastructure; upon detecting a stoppage condition at a particular meter ID, the provider is alerted through their system with a corresponding notification. The integrated configuration thereby enables real-time display, local data storage, and external signalling of abnormal load events, contributing to improved monitoring and management of residential energy consumption.		meters. The proposed architecture enables utility companies to monitor consumer electricity usage on a regular basis and addresses theft by integrating a smart meter's microcontroller. This technology facilitates the detection of anomalous power consumption by both the customer and the power provider, enabling prompt notification to investigate potential theft or misuse of power. Overall, the approach aims to enhance grid reliability and security by improving theft detection and enabling timely corrective actions.
Design of Electric Meter with Double Connected Data Capture System for Energy Theft Monitoring (Zulu and Dzobo, 2021)	This paper's primary goal is to create a real-time monitoring system that can identify instances of power theft in distribution networks.	This study proposes a double metering system capable of tracking, identifying, and pinpointing electricity theft from the transformer's distribution point to each distribution pole, as well as to individual residences supplied by the network. Each house meter and distribution pole meter incorporate current and voltage sensors as part of the envisioned configuration. To achieve precise power measurements across the entire distribution grid and to facilitate real-time monitoring and theft detection, the system measures and records the power transferred and delivered at each point within the distribution network. Every ten minutes, Arduino Uno microcontrollers are configured to read data from the voltage and current sensors. The infrastructure comprises a sequential communication chain: the main distribution transformer's meter communicates with the first distribution pole meter, which in turn communicates with the second distribution pole meter, continuing along the chain to subsequent pole meters. Each	For this research Proteus Design Suite v.8.10 SP3, has been used to simulate the proposed real-time monitoring system.	The global revenue losses experienced by a substantial portion of power utilities are largely attributable to electricity theft. In the context of unauthorized connections and meter manipulation within the power system grid, the proposed real-time monitoring and detection framework for electricity theft demonstrates favourable outcomes in simulations. In the South African setting, the implementation of the proposed system is anticipated to play a critical role in mitigating theft, aiding in the identification of illicit usage, and assisting power companies and local authorities in the recovery of funds. Given that the current work remains at the simulation stage, the immediate next step involves the development of a laboratory-tested prototype to validate performance prior to pilot deployment within an actual town's portion of the power system grid.

		distribution pole meter, connected to the supply to each household, also interfaces with the corresponding house smart meter to assess the balance between power supplied by the distribution pole and power consumed within the house.		
Determination of Consumer Powers by Measurements at the Supply Feeder Ends (Korovkin et al., 2021)	This paper seeks to develop a method for identifying and locating unapproved power take-off points within residential electrical networks.	The study investigates a measurement-based approach to determining the capacities of multiple consumers supplied by a single feeder, using data acquired solely at the feeder's beginning and end points. Furthermore, the technique provides robust control and precise accounting of both supply and consumption, while enabling the detection of nodes associated with illicit connections.	No software and no hardware are used for this study	This study presents a method for estimating the power consumption of multiple customers connected to a common feeder by utilizing readings from metering devices located at the feeder's origin and terminus. The computations and derived ratios demonstrate that the end-point and start-point meter readings can be employed to determine each individual consumer's power usage and to identify power take-off locations with accuracy. By obviating the need for installing discrete control devices for each customer, the proposed approach facilitates a reduction in capital expenditures during the design and deployment phases of automated electricity metering systems.
An Efficient IoT Based Electricity Theft Detecting Framework for Electricity Consumption (Sharma et al., 2021)	The methodology is intended to help energy trading businesses identify instances of electricity theft.	The initial phase involves the analysis of historical consumption data for a designated location, which may correspond to the feeder level, the distribution-transformer level, or any other segment of the electrical distribution system where electricity theft is suspected. In the second phase, IoT devices are integrated with the metering units of individual sources within the area of interest, enabling real-time aggregation of all power delivered to that sector. Subsequent IoT devices are deployed across various components of the power supply network, including additional segments of the electricity distribution path, to enhance monitoring granularity. These devices collect data in real time and transmit it to a central server housed within a data centre or, where applicable, a cloud storage environment, leveraging Global System for Mobile Communications (GSM)	The hardware and software used include, an Arduino based microcontroller, GSM Module, Wi-Fi Module, Bluetooth Module, RF Module, ACS712 Current Sensor, LM35 temperature sensor, IIC OLED Display, 3.7 V Battery, Camera Module, Cent OS Linux, Apache Web Browser, PH, MySQL, cURL, Cloud Storage/Server at Data Centre	The proposed system demonstrates the capability to detect electricity theft over a substantial portion of the power supply, with a hierarchical identification process that first flags the larger affected area and subsequently localizes the precise location or premises where the theft occurs. Utilities and distribution operators can further mitigate such illicit activity by deploying the enhanced version of the real-time coverage device, customized to their operational requirements. In the experiment described in this work, the IoT-based framework installed at Premises 4 successfully identified theft from 04:00 to 21:00 hours. For a more precise analysis of the suspected segment, IoT 4 correlated actual consumption data with meter readings, noting instances where the meter displayed zero usage while the

		technology. Through the analysis of this real-time data, the framework aims to pinpoint the precise location of electrical theft. To augment surveillance and deter theft, an auxiliary IoT-enabled vigilance device is employed to capture images of the surrounding environment, thereby monitoring exposed wiring and other potential vulnerabilities. Alerts generated by the vigilance device are relayed to representatives of the power distribution utility in real time, enabling prompt investigative and remedial actions to mitigate energy losses associated with theft.		graphical display indicated consumption, thereby highlighting discrepancies suggestive of tampering or theft.
Mitigating Electrical Losses Through a Programmable Smart Energy Advanced Metering Infrastructure System (Williams et al., 2023)	This study describes a method for reducing electricity theft using programmable smart energy meters.	The proposed approach involves integrating interrupt-based signaling into smart energy meters to detect input signals originating from an auxiliary current sensor installed at the terminal point of the service line. This location corresponds to where unauthorized connections typically occur between the sensor and the meter. The Advanced Metering Infrastructure (AMI) framework under consideration provides several essential smart services, including the computation of energy consumption in kilowatt-hours (kWh) and the generation of customer bills that are subsequently transmitted to the utility facility. In addition, the AMI system is capable of executing a power shutdown to the meter when required.	Proteus software is utilized to simulate and illustrate the efficacy of the suggested approach.	The proposed approach introduces deliberate perturbations to smart energy meters to detect input signals from an auxiliary current sensor installed at the service-line terminal point, the location where unauthorized connections are typically established between the sensor and the meter. Among the smart services provided by the proposed AMI system are (i) the computation of energy consumption in kilowatt-hours (kWh) and (ii) the generation of bills delivered to the utility operator. The AMI system can subsequently interrupt the power supply to the meter. The effectiveness of the proposed method is demonstrated by programming and validating the expected functions of the smart energy meter using Proteus, illustrating the method's efficacy.
Energy Frauds Characterizatio n based on Information Theory Quantifiers (Bastos et al., 2023)	The aim of the research is to propose an energy fraud characterisation study based on Information Theory Quantifiers (ITQ).	A three-step characterization framework is employed. First, the Bandt–Pompe (BP) non-parametric transformation is applied to electricity consumption time series to produce a histogram that preserves causal temporal information. Second, from this histogram, statistical measures—Fisher Information (FI), Statistical Complexity (SC), and Permutation Entropy (PE)—are computed to describe potential fraudulent activities. Finally, these descriptors	Python software is utilized to implement and analyse the fraud characterisation results with the use of quantifiers from ITQ. The data analysis techniques are implemented using Ordpy, a pure Python package that is based on the BP symbolic encoding approaches	Based on ITQ, this study presents an accurate categorization of fraudulent users. By integrating ordinal patterns, ITQ, stochastic processes, and causal information planes, the proposed framework effectively identifies fraud. In summary, the approach demonstrates the capability to classify fraud instances with precision while enabling examination of user behaviour. Moreover, it reveals commonalities among fraudulent actors, thereby providing a more

		are mapped onto the Fisher–Shannon (FS) Plane and the Complexity–Entropy Causality Plane (CECP), where their positions correspond to a spectrum of canonical states. This visualization facilitates characterization of diverse fraudulent patterns as they converge within the CECP and FS planes. The analysis utilizes a dataset from the Irish Smart Metering Energy Project, comprising over 5,000 residential and commercial power users.		robust characterization of fraudulent activity. Consequently, certain fraud patterns can be linked to underlying compatibilities among them, which may be useful for modelling random patterns across diverse datasets in future research. The proposed methodology warrants further evaluation across varied fraud scenarios and data types to assess its generalizability and potential limitations.

2.4 Comparative analysis of the developments in the existing literature

The issue of unauthorized electricity connections has persisted for a considerable period, prompting researchers to devise innovative strategies to curb and ultimately resolve it. Discussed below is a comparative examination of the developments within the current literature, drawing on publications identified from 2004 to 2023. The aim is to synthesize and contrast the progression of methodological approaches, theoretical perspectives, and empirical findings across this body of work.

The cited works by Pavic et al. (2004) and Trupinic et al. (2005) advocate a uniform remedial strategy for illicit utility connections. The proposed methodology targets connections concealed by offenders within private premises, areas inaccessible to utility personnel during routine inspections. The authors recommend the deployment of time-domain reflectometers (TDRs) to address such illicit connections. This approach relies on testing a line in a dead (de-energized) condition to detect impedance variations along the line that may indicate cable breakages or illicit taps. To enable meaningful comparisons between initial measurements and those obtained during subsequent random inspections for suspected theft, the system is optimally operated by performing an initial cable test to determine the full length of the cable free of illegal connections, with the resulting data subsequently stored.

Operationally, a wave generator emits a brief pulse into the cable under investigation. The incident pulse propagates along the conductors and encounters a bifurcation into transmitted and reflected pulses; if a fault such as a break, a second disconnected cable end, or any geometric alteration along the conductors changes the impedance, additional reflections occur. The distance to the impedance anomaly is computed from the pulse's travel time and the known wave speed, using both the incident and reflected signals. At a given point, an oscilloscope records the incident, transmitted, and reflected pulses. This pulse-reflection mechanism is analogous to radar operation and constitutes the fundamental operating principle of the TDR technique. The authors illustrate the method with experiments employing

a TDR consisting of a sinusoidal signal generator and a basic oscilloscope. The principal advantage of the TDR approach lies in its potential to pinpoint the exact location of illicit connections, thereby guiding investigators.

However, several limitations are noted. A primary drawback is that the technique is constrained to application during scheduled power outages, since it requires dead-line conditions to function. The approach is outdated, it might have been effective in contexts where electricity thieves concealed their illicit connections and needed early detection. This is no longer the case, looking at countries such as South Africa in the townships, where illicit connections are often evident without concealment, this method would not even be needed. The broader challenge is the allocation of utility resources, which are constantly expended to disconnect illicit connections, only for offenders to reconnect within the same day, frequently without concealment. Consequently, modern power infrastructures and the prevalence of readily detectable illicit connections render the described TDR-based method largely inapplicable in present-day contexts.

According to Parra and Calderon (2006), shunt detection technology can be employed to identify unauthorized power connections. Their paper introduces a portable device, referred to as the “lines and shunts detector,” developed for commercial use to locate metallic pipework, electrical service wires, pipe valves, and related derivatives. Examples of such pipework include gas, water, and cable television systems. The device operates by either inducing a very low-power signal through a clasp-type coil or by injecting a present alternating frequency directly into the pipe or electric conductor. This frequency differs from the standard operating frequency of the system under inspection (e.g., 50 Hz or 60 Hz for electrical systems). The detection system comprises two primary components: receptors and a transmitter. The method by which the transmitter introduces the signal depends on several factors, including whether the conductor is electrified, whether it forms a loop or a bow when the ends are connected, or whether the conductor is not directly accessible to the transmitter. Depending on the preceding information, the transmitter can inject the signal in one of three ways: conductively, through inductive coupling, or by induction. The receptor serves to monitor the principal conducting pathway and to identify and track potential derivatives of the injected or induced signal after the chosen procedure has been determined. By mapping the detected pathways, the system aids in locating unauthorized cables that are tapping into the network. The efficacy of the proposed system is demonstrated using shunt-detection equipment. The “lines and shunt detector,” designed to locate illicit connections concealed beneath underground cables, shares similarities with the time-domain reflectometry (TDR) method. A notable advantage of this approach is its applicability to live networks, eliminating the need to wait for scheduled power outages to commence investigations. Furthermore, it can identify illicit connections on

subterranean cables with high accuracy. However, a drawback is its susceptibility to misidentifying other nearby metallic objects as unlawful tap connections. Additionally, like the TDR method, the system requires resources to investigate, identify, and disconnect illicit connections. In many regions of South Africa, neither method proves effective for uncovering overt illicit links.

The study by Weckx et al. (2012) contributes an algorithm designed to identify illicit electricity connections that steal power in smart-grid environments where cable lengths are ambiguous or unknown. The authors advocate the use of a load-flow algorithm to locate theft and propose a methodology capable of pinpointing both the grid location and the customer responsible for double-feeding or meter tampering in scenarios lacking precise distances between residences or between the smart meter and the distribution feeder. The proposed algorithm rests on the premise that every customer is equipped with a smart meter that records voltage as well as active and reactive power. By comparing the substation-measured power with the aggregate power consumed, the system operator can determine the times at which theft occurs. To illustrate and evaluate the functionality of the proposed approach, the authors conduct simulations using a three-phase, four-wire radial low-voltage network with a TT earthing configuration typical of residential systems; however, the manuscript does not specify the simulation software employed. A key advantage of the approach is its operational efficiency: it reduces the amount of equipment required within the grid to detect theft, thereby lowering implementation costs. The methodology relies solely on data from smart meters, which may already be stored within existing databases. Yet, the proposed solution has notable limitations. Like other approaches discussed in the literature, it can only alert the utility company to theft events occurring at particular customer locations, necessitating subsequent investigation and resource allocation to identify and disconnect the responsible parties. A further drawback is that the method is tailored to illicit connections through double-feeding by customers who are already connected to the grid and does not address cases involving illicit connections by customers who have never previously accessed the grid.

A low-cost power meter prototype is proposed by Evaldt et al. (2012) to detect commercial losses within distribution networks. The approach adopts an Intelligent Electronic Device (IED) framework, deploying meters in pre-selected regions to monitor power delivery to a subset of customers. A wireless cascade communication topology disseminates meter data across the distribution network. Commercial losses in a given segment are inferred from the discrepancy between readings of consecutive IEDs within that segment. Data aggregated from the IEDs are processed at a central distribution control centre, where the network model facilitates the identification of billing anomalies. Periodically, utilities compare the sum of individual customer meters against the total energy delivered as indicated by the IEDs. An experimental prototype

employs a Hall Effect Sensor to generate an output voltage proportional to the measured current, demonstrating linear response for electric current measurements. A low-current sensor with a 30 A peak is used for testing, while the final prototype utilizes a higher-capacity 550 A peak sensor. Voltage measurement is performed via a voltage transformer. Digital data processing is implemented on a Microchip RF PIC microcontroller, which integrates an RF transmitter. To enable bidirectional communication, an RF reception module is added, given that the CPU provides only a transmitter. The antenna system is implemented in a loop configuration on a printed circuit board.

Commercial losses are identified by comparing distributed energy measurements with invoiced energy. The system can thus reveal energy losses attributable to unauthorized connections or metering discrepancies. A notable limitation is the requirement for field personnel to investigate and physically remove illegal connections when energy theft is detected. This investigative process can be time-consuming and resource-intensive, potentially leaving some illicit connections unaddressed. The proposed prototype demonstrates a practical, low-cost solution for detecting commercial losses in distribution networks using IEDs and wireless cascade communication. Its strengths lie in the end-to-end architecture, from sensor-level measurements to centralized anomaly detection. However, the reliance on on-site verification to remediate illegal connections represents a significant operational bottleneck.

The authors (Babu et al., 2012; Babu and Sushma, 2013) describe a system in which the distributor phase voltage is temporarily increased from its nominal level (for example, from 100% to 152%, or from 230 V to approximately 350 V), and subsequently stepped down to the standard operating voltage (230 V) at the customer premises via a specialised voltage regulator device. The methodology purports to reduce both technical and non-technical losses, reporting potential savings of up to 49.12% of the total power delivered within the distribution system. Accordingly, improvements to the voltage profile are associated with reductions in I^2R losses. The recommended approach maintains distributor phase voltages up to 350 V, which aligns with the observation that most domestic appliances operate at 230 V. Consequently, the technique is presented as having no inherent risk of power theft or unauthorized connections in the distribution network.

The rationale posits that operating the distributor at voltages above the normal level diminishes I^2R losses. A voltage booster (capable of 230 V to 350 V) is connected to the secondary of a three-phase distribution transformer (ratings 11 kV/415 V/230 V) to prototype the proposed system. A 16 W compact fluorescent lamp is connected across the R-phase and neutral on the secondary side of the booster transformer to denote an unlawful connection. Three additional compact fluorescent lamps are connected across the secondary side of the special

voltage regulator device (SVRD) at the consumer end. The three SVRDs (350 V/230 V) are then placed across the voltage booster's phases and neutral. The authors propose High Voltage Distribution System (HVDS) as an effective approach for reducing electricity theft in low-voltage networks, with the additional purported benefit of marginally decreasing technical losses.

However, the system presents notable drawbacks. Foremost among these is a significant public safety concern: elevating operating voltages could increase the risk of electric shock and harm to individuals attempting illicit connections. Given the prevalence of illegal wiring practices—such as twin flex cables strung across streets and sometimes within reach of children in townships—even modest voltage increases may pose substantial hazards to the general public. Another limitation concerns the feasibility of integrating such an HVDS approach within a flexible smart grid framework for distributed energy resources in low-voltage networks. While 230 V remains the most common operating voltage for many household appliances, many inverters designed to integrate distributed energy resources (DERs) are also standardized for 230 V. Implementing the proposed scheme would thus require reverse voltage regulator or inverter designs that conform to the 350 V standard rather than the 230 V standard, potentially impeding alignment with ongoing smart grid advancements in LV networks.

The study by Khan et al. (2013) proposes an intelligent modelling framework for detecting line loss in power distribution systems. The methodology involves a comparative assessment of the transformer's supplied power and the corresponding power consumption by end users. Implementation considerations include the use of microcontrollers within the low-voltage (LV) network and Global System for Mobile Communications (GSM) communication to facilitate data collection and reporting. The central objective is to identify electricity theft by contrasting the distributor's delivered energy with the consumer's consumption. Accordingly, the principal modifications to the power distribution system are identified as: (a) continuous comparison of power delivery and utilization; (b) real-time measurement of power statistics between the distributor and the consumer; and (c) timely reporting of power mismatches to relevant authorities. The authors emphasize that the work is theoretical in nature and does not employ hardware or software implementations. They suggest GSM modules and microcontrollers as possible hardware options, noting that the proposed intelligent modelling scheme remains a conceptual framework requiring further investigation. The concept holds potential but shares a common limitation with other techniques cited: the need for utility companies to investigate and disconnect connections deemed illegal.

In the study by Penner et al. (2014), the proposed apparatus is designed to monitor and mitigate non-technical (theft-related) losses within distribution networks. The system gauges the transformer's power consumption, recording either to local storage or transmitting the data to the utility via GSM. The utility then compares customer consumption against this transformer-level data, with discrepancies interpreted as indications of power theft. In response, the utility dispatches system operators to investigate and disconnect the implicated locations. The prototype hardware comprises Arduino ATmega168 microcontrollers, an SD card, an LCD display, a real-time clock (RTC), voltage sensors, and clamp-on current sensors, and it is programmed using the Arduino Integrated Development Environment (IDE). The proposed configuration aligns with the low-cost power-meter prototype previously described, as well as the related intelligent modelling framework. Collectively, these approaches rely on measuring transformer-level energy use and transmitting the data to the utility for reconciliation with customer-metered energy invoicing; any variances are construed as evidence of power theft. A common limitation across the three proposed methodologies is their dependence on utility-company involvement to verify and physically disconnect the suspected electricity theft sites.

Chauhan (2015) propose a monitoring system for identifying power theft along low-tension distribution lines. The central premise is that theft detection is feasible by deploying current monitoring devices between adjacent poles, under constant voltage conditions. When no illicit load is connected between poles, the current measured between them remains approximately equal. Introduction of an unauthorized load results in a detectable alteration of this current, enabling theft identification. The proposed design employs a comparator in conjunction with two current sensors positioned near each pole to verify current parity across the span; any discrepancy between the two sensor readings may indicate electrical theft occurring between the poles. By recording the observed changes in current, the system can facilitate localization of the theft site or the insertion point of an unauthorized load.

The prototype implementation utilizes several electronic components: an analog-to-digital converter (ADC), a microcontroller, current transformers for current measurement, and a liquid crystal display (LCD) to present warnings. Notable limitations of the concept include: (i) applicability restricted to scenarios lacking legally connected consumers between the poles; (ii) practical deployment challenges arising from wiring requirements, given that spans between poles can extend to approximately 100 meters. In this configuration, the comparator and associated wiring would be situated in the mid-span, with a current sensor installed at the initial pole and another sensor located up to 100 meters away, raising concerns about feasibility and reliability. A final drawback, common to prior proposals, is the continued necessity for utility operators to intervene in disconnecting any unauthorized connections.

The traveling wave method, as proposed by Medrado et al. (2016), offers a technique for identifying illicit connections on distribution lines. This fault-location approach relies on the propagation speed of voltage or current transients along the line and the path from the failure site to the line terminals integrated into the locating devices. The system described leverages the highly transient signal generated at the moment of load connection. Unlike some methods, this locator requires the installation of two network analysers, with one unit placed at each end of the transmission and distribution lines. By comparing the arrival times of the first transient wave at each analyser, the location of the load within the monitored segment is determined. Precise time synchronization between the two analysers is essential for accurate measurement; thus, ensuring that both analysers share an identical time base is crucial. A practical synchronization strategy includes integrating a GPS module into each analyser or transmitting synchronization signals via the power line.

The ATP/EMTP (Alternative Transients Program / Electromagnetic Transients Program) software is employed to develop a computer model of the system. The proposed approach is conceptually akin to time-domain reflectometry (TDR), in that it estimates the distance to the illicit connection by evaluating the traveling-wave speed generated by the unauthorized connection. The principal advantage of this method is its capability to detect illicit connections and estimate their distance from the two measurement points (analysers). However, the approach imposes a burden on utility providers due to the potentially high data volume and the need for personnel to inspect and disconnect illicit connections, especially in areas with limited resources. Regions with infrequent illicit connections and adequate workforce may benefit more readily from the method.

Dudek et al. (2018) compare three analytical paradigms—load-based analysis, Kirchhoff's current-balance method, and voltage-drop analysis—to determine which offers superior accuracy for identifying unauthorized usage. The study also outlines the limitations and practical constraints associated with each method in real-world deployments.

1) Voltage-Drop Based Method

   Principle: For a given line section, calculate current from the measured voltage drop and compare it with the current inferred from active and reactive power flow. Since voltage drops reflect the aggregate consumption of all users, any discrepancy between the voltage-drop–derived current and the meter indication signals potential illegal usage.

   Operational Steps:

   - Measure voltage drops along a line segment starting at the line's terminus.

- Compute current from voltage drop data and from power-flow data.
- Flag deviations beyond predefined thresholds as suspected theft.

Assumptions and Limitations: Assumes accurate voltage and power-flow measurements; susceptible to measurement errors and does not quantify reactive power fully in practice.

2) Kirchhoff's Current Balance Method

Principle: Verify that the total current delivered by a substation equals the sum of currents observed at customer connections, in accordance with Kirchhoff's laws.

Operational Steps:

- Sum the currents received by all customers and compare to the supply current from the station.
- A mismatch indicates potential theft, though it cannot identify the specific culpable customers.

Assumptions and Limitations: Requires synchronized measurements at a fine temporal resolution; precise individual identification is not possible; 15-minute interval measurements may be impractical in networks with static meters, and reactive power is not explicitly quantified.

3) Load-Based Method

Principle: Detect illicit use by analysing per-customer load patterns rather than aggregate measurements.

Operational Steps:

- Monitor daily/weekly energy usage profiles for individual AMI-enabled customers.
- Establish a weekly baseline and compute the daily discrepancy between observed usage and the weekly average.
- Identify customers whose usage diverges significantly from the baseline.

Assumptions and Limitations: Requires reliable per-customer load data and long observation periods; measurement errors can confound results; efficacy depends on the selection of appropriate baselines and thresholds.

The load-based method demonstrated notable potential for detecting unlawful consumption at the individual customer level, particularly when leveraging weekly baselines to accommodate daily and weekly usage patterns. The voltage-drop method provides a direct, system-wide check but hinges on measurement accuracy and may yield false positives in the presence of measurement noise or unmodeled network changes. The Kirchhoff's current balance approach

offers a broad validation of system integrity but lacks granularity for pinpointing individual violators and is sensitive to measurement synchronization and data resolution.

The comparative analysis indicates that determining illegal electricity consumption on the basis of individual household loads constitutes the most accurate approach. This approach is analogous to the previously discussed algorithmic method for identifying electricity theft. Both methodologies rely on statistical analyses to detect households that engage in illegal electricity use via double feeding. A notable drawback shared by all proposed solutions is the necessity for frequent utility intervention to execute disconnections.

In order to identify outliers detected by smart meters, Neagu et al. (2018) propose a novel data mining–based approach grounded in Knowledge Discovery in Databases (KDD). The authors argue that human engineers, in the absence of automation, are unable to perform comprehensive database analyses at the necessary scale; advances in storage capacity allow more data to be recorded, thereby enabling anomaly detection through appropriate algorithms. Consequently, an operator can oversee an automated process that identifies anomalous data. Data mining can reduce measurements to include only meaningfully relevant or previously unidentified information, while simultaneously extracting implicit, potentially actionable knowledge from databases produced by software applications. The implemented data mining method is executed within the MATLAB environment. The proposed technique computes the current rate of electricity theft in distribution networks by leveraging outliers in smart-meter data, enabling the identification of theft instances and their locations. As with other methods described in the literature, the utility remains responsible for dispatching operators to perform disconnections when warranted.

An IoT-based drone system for monitoring distribution transformers and curtailing illicit electrical connections has been proposed by Basak et al. (2019). In this framework, a drone serves as a surveillance instrument that is preconfigured to trace the electrical routes and detect unauthorized connections, utilizing a GPS module for navigation. The system incorporates a telescopic extension-equipped cutter, enabling rapid disconnection of detected illicit links. In parallel, the drone monitors transformer health through thermal imaging and current measurements, employing a thermographic camera and a current sensor. Upon identification of anomalies in temperature or current, the system triggers an alarm and notifies the local operating station. The envisaged surveillance capability is posited to reduce losses in the power sector while mitigating adverse effects on transformer assets. The hardware components of the proposed design include a motorized telescopic extension, a solenoid-valve actuated cutter, and a solar-powered drone integrated with a camera. Notably, this approach is the first on the reviewed literature to advocate autonomously cutting and removing illicit

connections following detection via drone surveillance, thereby potentially reducing the need for direct utility intervention and lowering non-technical losses. According to the system design, deployment would ostensibly require a drone for each transformer zone, with operation conducted within the respective zone and powered by solar energy for charging. The routine inspection and responsive capabilities are anticipated features of the system. A salient drawback acknowledged in the discussion is the substantial capital cost associated with deploying a drone network across all transformer zones, which may impede wide-scale implementation.

Louw and Bokoro (2019) propose ZSC-based detection as a means to counteract unlawful ground surface connections. Zero-sequence current (ZSC) emerges in three-phase electrical systems under earth fault conditions and can reveal leakage paths to the ground. This research applies ZSC monitoring at the distribution transformer's star point as a secondary safeguard to identify energy theft associated with exposed wiring on the ground. The proposed strategy includes isolation at the distribution point node to mitigate revenue losses, supply-quality issues, and human safety hazards. The study explores whether ZSC monitoring, coupled with node isolation, can function as a preventative mechanism and a detector of non-technical losses (NTL) caused by bare, surface-deployed conductors. A condensed electrical network was modelled using DigSILENT Power Factory, Version 15, to simulate earth faults and ZSC phenomena. A laboratory test was designed to validate DigSILENT results. The scope of the ZSC-based system is limited to conductors that form unauthorized connections across roadways, lie on the ground, and frequently lack adequate insulation or exhibit insulation damage. In many scenarios, uninsulated conductors permit current flow to ground, precipitating ground faults that can generate detectable ZSC signals. The study notes a critical limitation: illicit connections may remain undetected if conductors are insulated or if insulation remains intact, thereby blocking ZSC detection.

Simulation results indicate that ZSC signatures at the transformer star point can correlate with ground-plane fault events and intentional ground connections, enabling potential identification of non-technical losses. Laboratory validation corroborates that ZSC increases during ground fault-like scenarios, supporting the concept of using ZSC as a monitoring metric. Distribution point isolation demonstrates potential to reduce the duration and impact of detected faults, contributing to improved revenue protection and system reliability. The proposed ZSC-based scheme provides a supplementary layer of protection against unlawful ground surface connections. Its effectiveness hinges on the presence of earth faults and exposed conductors; insulated conductors may suppress ZSC signatures, limiting detection capabilities.

The authors (Pauline N. et al., 2020) propose an embedded-system device designed to detect and locate customers who attempt to consume electricity without proper billing by monitoring pre- and post-meter current flow. The system identifies attempts to “tap” electricity by illicitly increasing load ahead of the service head and provides real-time notifications of the status of the affected connection to the utility via Global System for Mobile Communications (GSM). The overarching objective is to protect Kenya’s distribution network from high non-technical losses (NTLs) associated with unlawful connections, thereby reducing overall power costs. The device operates by measuring current values from two sensor modules: one installed before the cut-out (pole side) and another after the cut-out (meter side). The experimental configuration comprises three linked loads (bulbs), an interrupting switch, an LCD display, a microcontroller for data processing, a current sensor to monitor the load current, and a sensor for the incoming supply current. Data to be transmitted to the utility provider are generated through a connected serial monitor. The embedded-system model is developed and observed, and detected data is analysed using Proteus and MATLAB/Simulink. Proteus is employed for its capability to model, simulate, and analyse electrical systems, and its libraries support communication with microcontrollers and other analog/digital components. The proposed system aims to identify electricity theft perpetrated by consumers who connect supplemental loads ahead of the electricity meter. Two current sensors are implemented in the system: one at the distribution pole and one beneath the meter. A microcontroller, receiving data from the current sensors, continuously compares the current entering the meter with the current drawn by the consumer. If a discrepancy arises—i.e., the current between the two sensing points does not match—the device alerts the utility to a potential instance of electricity theft prior to the meter. The method targets only the specific category of theft involving evasion of electricity metering and excludes theft occurring between the distribution transformer and the legitimate customer’s point of connection.

The authors (Raggi et al., 2020) propose Non-Technical Loss Identification through Data Analytics and Customer Smart Meters. This work proposes a data-analytic method designed specifically for NTL detection and localization, utilizing publicly accessible or operator-provided smart meter data. Unlike traditional state estimation (SE) procedures, which aim to infer the operating state of the network in real time, the proposed approach operates offline, focusing on the localization and identification of NTL events. The central contribution is a discrete, three-phase estimator integrated into a WLS framework, augmented by a residual-correlation based index for localization. Smart meter measurements are aggregated to construct a suitable dataset for analysis. Data quality issues, including missing or corrupted measurements, are addressed prior to model application. A three-phase state estimator is formulated within a Weighted Least Squares (WLS) context. The estimator is adapted to operate in an offline mode, distinct from conventional online SE objectives. A novel index, derived from residual

correlation, is proposed to detect and localize NTLs. The index leverages the relationship between measurement residuals across meters to identify anomalous patterns consistent with non-technical losses. The residual-correlation index is mapped to network topology to infer the probable location of NTLs. The method emphasizes localization accuracy while acknowledging potential ambiguities due to data limitations.

The proposed approach is not intended to replace physical inspection or disconnection processes. It serves as a diagnostic tool to prioritize investigative resources and guide offline analyses. The methodology is demonstrated on simulated or real-world smart meter datasets (as available), illustrating the detection and localization capabilities of the residual-correlation index within a WLS-based offline framework. The study discusses sensitivity to measurement noise, data gaps, and model inaccuracies, and outlines robustness measures to mitigate false positives/negatives. The results underscore how distribution system management can leverage smart-meter data to identify suspicious consumption patterns and strategically allocate manual inspection resources.

Pealy and Matin (2021) propose a framework for Tackling Energy Theft in Smart Grids. The study aims to demonstrate the energy consumption profile of a residence using a microcontroller configured to record data in memory. When the aggregate load exceeds a predefined typical load, the microcontroller transmits a signal to the smart meter to enact a block, accompanied by a blockage notification. Given that each smart meter is inherently connected to the electricity supplier, the supplier's system receipts indicate when a particular meter ID is halted. The article concentrates primarily on the detection and management of energy theft associated with smart meters, with the objective of aiding utility providers in identifying illegal connections and taking appropriate actions. The principal goal of the study is to mitigate power theft resulting from meter bypassing, excluding scenarios where users connect to the network without authorization and consume electricity.

Design of an Electric Meter with a Double-Connected Data Capture System for Energy Theft Monitoring is proposed by Zulu and Dzobo (2021). The study proposes a double metering configuration capable of monitoring, detecting, and locating power theft from the transformer distribution point to each distribution pole and to every dwelling connected to the electrical grid. As part of the system, current and voltage sensors are installed at each distribution pole meter and at each household meter. The system measures and records the power transferred and distributed from each point within the distribution network to provide accurate power measurements across the entire grid and to enable real-time monitoring and theft detection. Arduino Uno microcontrollers are configured to read data from voltage and current sensors every ten minutes. The first distribution pole meter, linked in sequence to the second, third,

and so on, ultimately connects to the main distribution transformer's meter. Each distribution pole meter connected to a household supply is also linked to a smart meter within the residence to assess the balance between power consumed by the home and power supplied by the corresponding distribution pole. While presently in the simulation stage, the proposed system demonstrates potential for addressing meter bypassing and illegal connections. Because power transfer is monitored from pole to pole up to the end user, it becomes feasible to identify the specific structure associated with an illegal connection.

A notable drawback of the proposed approach is its implementation cost, given that each distribution pole must accommodate a current sensor, a microcontroller, and a GSM module. GSM modules are comparatively expensive; deploying one at each distribution pole could unnecessarily elevate the overall cost. Moreover, the cost of GSM communication is high due to the need for SIM cards for every pole within the LV distribution network, with messages transmitted at ten-minute intervals. This elevates communication costs and raises questions regarding the project's feasibility. Although the system can detect instances of electricity theft and report them to the utility, it still requires the utility to undertake physical disconnections, which incurs additional expenses for power companies. This limitation is consistent with limitations already discussed with other solutions.

Authors Korovkin et al. (2021) propose a method for determining consumer power by measurements taken at the supply feeder ends. The study advocates using data from metering devices located at the beginning and end of a feeder to estimate the power consumption of multiple users connected to the same feeder. Specifically, the authors describe a procedure to compute the capacities of several consumers powered by a single feeder based on measurements collected at feeder respective start and end points. The accuracy of determining consumer energy consumption and the location of power take-off points is validated by the calculations and ratios presented in the article. The proposed approach enables the development and implementation of automated power metering systems with reduced capital expenditure, as it obviates the need to install control devices for each individual customer. Additionally, the method facilitates the identification of nodes with unauthorized connections and ensures precise accounting of electricity supply and consumption. The study advises installing a metering device at the transformer, with data from customer smart meters subsequently used to correlate the power consumed by the customers with the power drawn from the transformer feeder's starting point. The authors demonstrate that unauthorized connections on feeders can be located using computations based on information supplied by each meter. Like many prior studies, the work has the limitation of identifying instances of unauthorized connections to the power provider, while still requiring resources for disconnections.

Sharma et al. (2021) present their work, An Efficient IoT-Based Electricity Theft Detecting Framework for Electricity Consumption. The framework leverages Internet of Things (IoT) techniques to monitor and detect electricity theft across customers assigned to specific geographic areas. The initial stage analyses historical consumption data for a given site, which may correspond to the distribution-transformer level, the feeder level, or any other segment of the electrical supply where theft may occur. In the second stage, IoT devices are deployed at individual source metering units, which provide real-time measurements of all power supplied to a particular location. Additional IoT devices are incorporated at various points of the network that delivers power. The analysis of real-time data collected by these IoT devices is performed at a central server located in a data centre or, where appropriate, cloud storage, using GSM technology to support communications. This process enables the precise localization of the electrical theft site. To monitor the exposed line and deter electricity theft, an extra IoT monitoring device is employed to capture photographs of the surrounding area, with real-time notifications transmitted to representatives of the power distribution company to take the necessary actions to mitigate losses due to energy theft.

The study is grounded in comparing actual consumption with invoiced consumption through IoT-enabled measurements. This framework is well-suited for deployment in regions where illicit connections are concealed. The study's foundation lies in analysing IoT-collected data to contrast billed versus actual consumption, which is particularly advantageous in locales where illegal connections remain hidden, as opposed to scenarios where the illicit connections are visible, and the primary challenge is mobilizing resources to disconnect them.

The authors Williams et al. (2023), present a strategy for mitigating electrical losses through a programmable, smart energy Advanced Metering Infrastructure (AMI) system. The approach includes detecting input signals from an additional current sensor installed at the service-line terminal point, where illicit connections may be formed between the sensor and the meter; to this end, interrupts are incorporated into the smart energy meters as part of the proposed mitigation strategy. One of the key services provided by the proposed AMI system is the generation of invoices for the utility operator and the calculation of energy consumption in kilowatt-hours (kWh). The AMI system is designed to disable the meter's power supply when anomalies are detected.

The study centres on meter-bypassing forms of electricity theft. In cases of discrepancy between the supplied power to the meter's feeder cable and the power registered by the meter, the system recommends penalizing the offending meter by disconnecting its power and notifying the utility provider. The methodology involves a comparison between the power

delivered to the service line and the actual power passing through the meter. It should be noted that illegal connections are not within the scope of this study.

Bastos et al. (2023) propose an Energy Frauds Characterization framework grounded in Information Theory quantifiers. The study employs data from the IQT to develop a quantifier-based classification of energy fraud. A three-step characterization procedure is implemented as follows. First, the electricity consumption time series are transformed into a histogram using the Bandt-Pompe (BP) approach, a non-parametric method that preserves causal temporal information. Second, to characterize fraudulent actions, the authors extract three information-theoretic measures from the histogram: Permutation Entropy (PE), Statistical Complexity (SC), and Fisher Information (FI). Finally, the locations of these measures delineate a range of canonical states on both the FS Plane and the Complexity–Entropy Causality Plane (CECP). This facilitates the identification of distinct fraudulent patterns where intersections occur in the FS and CECP representations. The study utilizes the Irish Smart Metering Energy Project dataset, comprising over 5,000 residential and commercial customers. Results indicate that Information-Theoretic Quantifiers (ITQs) effectively characterize a variety of fraud patterns. The analysis emphasizes statistical methods to identify the regions where power fraud occurs based on observable patterns. As with many prior studies, the research attributes the responsibility for disconnections following detection of unauthorized connections to the utility company.

2.5 Discussion

The comparative analysis of the reviewed literature suggests that the proposed solutions can be classified into five distinct approaches. These include signal analysis, power consumption comparison, electric current drawn comparison, statistical analysis, distribution modification (which renders the product unusable prior to delivery to the intended customer), and surveillance. Among these, the most frequently employed approach is power consumption comparison, as authors predominantly advocated its use, followed by statistical analyses. The remaining three approaches have received comparatively less attention in the extant literature.

The cited authors (Evaldt et al., 2012; Khan et al., 2013; Korovkin et al., 2021; Pauline N. et al., 2020; Penner et al., 2014; Sharma et al., 2021) propose solutions that share methodological similarities, centering on the comparison of power consumed by legitimate customers with the power supplied, in order to determine potential illegal connections based on power mismatches. While these works converge on the power-consumption paradigm, there are notable differences in their implementation details and approaches to power comparison, as discussed in Section 2.4.

A second cluster of studies (Bastos et al., 2023; Neagu et al., 2018; Raggi et al., 2020; Weckx et al., 2012) employ statistical analyses to address electricity theft. Their strategies rely on mining data from smart meters and applying algorithms and mathematical models to detect anomalies that may indicate illegal connections.

A third group (Parra and Calderon, 2006; Medrado et al., 2016; Pavic et al., 2004; Trupinic et al., 2005) utilizes signal analysis to infer illegal connections by examining the behavior of traveling waves along conductors.

A fourth approach (Babu et al., 2012; Babu and Sushma, 2013) focuses on distribution modification to ensure the product is not usable until it reaches the intended customer's premises, effectively hindering unauthorized connections by design.

Chauhan (2015) and Williams et al. (2023) propose applying Kirchhoff's current law to compare currents drawn by consumers with the current supplied, thereby identifying current mismatches that may signal illicit connections.

Basak et al. (2019) introduce surveillance of electricity networks for illegal connections, incorporating automated actions to eliminate problematic unauthorized connections.

Across the literature, experimental methodologies prevail, with a subset employing simulation software for proof of concept. Proteus simulation software is frequently used, and several studies have built prototypes to demonstrate feasibility.

This proposed research study adopts the electric current comparison approach, leveraging Kirchhoff's current laws to monitor for electricity theft. In contrast to many prior works, this study includes an automated intervention mechanism to mitigate illegal connections and reduce the burden of disconnections on electricity providers. To validate the concept, two experimental modalities are proposed:

(i) A simulation using Proteus Virtual System Modelling (VSM) software, and
(ii) A laboratory-scale prototype to verify the results.

2.6 Conclusion

This chapter surveys the existing literature on electricity theft, emphasizing the various forms of theft, contributing factors, and the consequences for electricity supply and governance. It also reviews mitigation strategies and efforts to eradicate electricity theft within low-voltage (LV) networks. A comparative discussion highlights the range of methods, approaches, software tools, hardware, and simulation platforms employed to address this issue. The

literature indicates that disconnection of illegal users has predominantly been performed through labour-intensive, manual processes, incurring substantial costs for the utility. In response, this research study proposes an approach to detect and interrupt illegal connections as they arise within the low-voltage (LV) distribution network, with the objective of substantially reducing the resources required for disconnection. The work is experimental in nature. It builds on prior research that has employed both prototyping and simulation to validate concepts. These include Evaldt et al. (2012), Panner et al. (2014), Chauhan (2015), and Sharma et al. (2021) who developed experimental prototypes, and Pauline et al. (2020), Pearly and Martin (2021), Zulu and Dzobo (2021), and Williams et al. (2023) who utilized Proteus simulation software for experimentation—this study adopts a hybrid methodology. By combining prototype construction with Proteus-based simulations, the research seeks to verify results and test the proposed hypotheses.

Chapter Three describes the LV network operation, the Proteus-based simulation of the legacy LV network, and the development of the proposed solution for addressing illegal connections.

3. CHAPTER 3
THEORY ON LV NETWORKS AND DEVELOPMENT OF SMART LV NETWORKS

3.1 Introduction

This chapter documents the initial phase of the research, whereby a representative model of the current legacy low-voltage (LV) distribution network is constructed within a simulation environment to replicate existing conditions, including illicit connections. The primary objective is to observe and quantify the electrical behaviour—specifically currents and voltages—under fault conditions in order to assess their impact on various network components. Following the observational phase, the theoretical framework governing the operation is presented, and the design is augmented with Internet of Things (IoT) devices, including sensors and microcontrollers, strategically deployed to detect the identified fault conditions. This integration yields a fully developed smart LV concept, proposed as a solution to the problem of illegal connections.

The ensuing sections provide a progressive build-up to this development: Section 3.2 offers an overview of the South African legacy power system. Section 3.3 discusses the present state of LV distribution networks. Section 3.4 traces the evolution of connecting LV customers to LV networks. Section 3.5 analyses the current flow within an LV network. Section 3.6 outlines smart grid architecture. Section 3.7 details IoT architecture while Section 3.8 presents the developed concept (the smart LV network). Section 3.9 presents the changes to be made on the existing LV networks and Section 3.10 provides the conclusion.

3.2 South African Legacy Power System Overview

The South African electrical network is organized around a generation-transmission-distribution paradigm managed by the power utility company Eskom. Generation occurs at power stations where energy is produced from either coal, nuclear, hydro, diesel sources or renewable energy sources (Solar and Wind). The generated electricity is subsequently transformed to higher voltages to enable efficient long-distance transmission, followed by step-down transformations to deliver suitable voltage levels to end users (Eskom, 2023). This thesis focuses on the residential consumer segment within the broader power system.

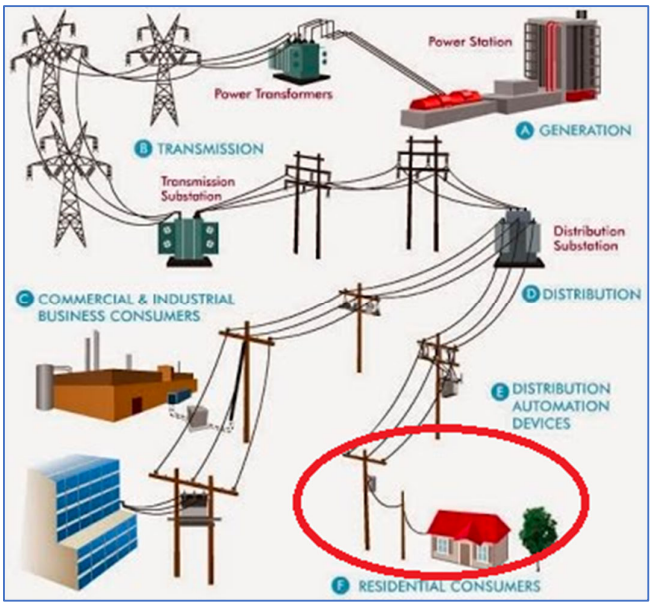

Figure 3.1: **Legacy power system overview from Generation to the consumer (The Electricity Forum, 2023)**

Generation: Electricity generation takes place at multiple power stations using three-phase generators. Energy sources include coal, nuclear, hydropower (water), and diesel. In Figure 3.1, the generation process is denoted by the letter A. The generated electrical energy is then prepared for transmission through step-up transformers, elevating voltages for long-distance transport (Eskom, 2023).

Transmission: High-voltage transmission lines, supported by pylons, convey electricity from generation sites to transmission substations. In Figure 3.1, this phase is labelled B. Transmission voltages are elevated to 765kV 400kV, or 275kV to minimize losses over long distances. Transmission employs a three-phase, 3-wire configuration (Eskom, 2023).

Distribution: From transmission substations, voltage is stepped down through successive transformer networks and distributed via high-voltage distribution lines to distribution substations. In Figure 3.1, this stage corresponds to the Distribution phase and is denoted with the letter D. Substations reduce voltages to 132kV, 88kV, 66kV, 44kV, and 33kV within a three-phase, 3-wire system (Eskom, 2023).

Secondary distribution and end-user delivery: Distribution substations subsequently furnish power to commercial, industrial, and residential customers through medium-voltage (MV) distribution networks. The commercial and industrial sectors are indicated in Figure 3.1 by letter C. To supply low-voltage appliances, voltage is further reduced by LV distribution transformers from 22kV to 400V, 11kV to 400V, 6.6kV to 400V, or 3.3kV to 400V,

corresponding to the Residential Consumers indicated by letter E in the schematic (Eskom, 2023).

3.3 Present state of LV networks

At the residential consumer level, the majority of electricity theft and illegal connections occur. This vulnerability arises where voltages are sufficiently low for consumers to hook their lines and connect their appliances without undergoing voltage transformation. In the distribution system, three categories of LV distribution transformers are employed to serve residential consumers (Brown, 2003).

1) Single-phase transformers: Typically, 16kVA, comprising a single phase and a neutral conductor. Residential Loads are connected between the phase and the neutral conductor.
2) Dual-phase transformers: Commonly 32kVA and 64kVA, containing two phases and a centrally tapped neutral conductor. Each single-phase Load is connected between one phase and the neutral conductor.
3) Three-phase transformers: Rated at 25kVA, 50kVA, 100kVA, and 200kVA, containing three phases and a neutral conductor. Single-phase loads are connected between any phase and the neutral conductor. Three-phase Loads receive all three phases plus the neutral and connect their three-phase loads across the three phases, with single-phase loads distributed between any phase and the neutral conductor.

Maximum customer count per transformer is estimated using the After Diversity Maximum Demand (ADMD). ADMD represents the calculated maximum electrical load for a group of consumers (e.g., a residential area or building) by accounting for the fact that not all individual loads operate at their peak concurrently. In electrical engineering, ADMD is applied to determine the required capacity for distribution networks (such as substations and wiring); ensuring capacity is sized for realistic usage rather than the aggregated sum of absolute theoretical maxima of every connected device (Brown, 2003).

ADMD varies with settlement type: Rural settlements, rural villages, informal settlements, and townships. A key differentiator among these settlements is average household income, which correlates with the number of electrical appliances within each dwelling. Rural settlements exhibit the lowest ADMD, while townships exhibit the highest (Brown, 2003).

Illustrative example: If the ADMD for rural villages is 1.2kVA, this implies that a typical single household is expected to draw up to 1.2kVA at peak load. Consequently, transformer sizing must reflect this expectation; for instance, selecting a 64kVA transformer yields an approximate capacity to serve about 54 households.

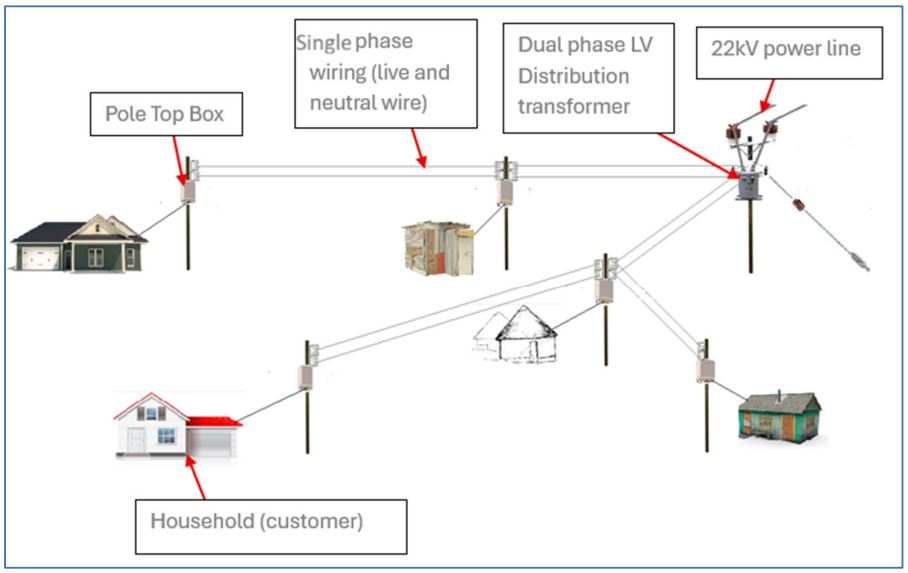

Figure 3.2: A bare wire Low Voltage distribution network (single transformer zone)

Figure 3.2 illustrates a single transformer zone for a bare wire low voltage distribution network setup with five single-phase households connected on the same dual phase LV distribution transformer. This is a type of design that is predominately used in the rural settlement and rural villages. This setup of a dual phase transformer with five households is the general circuit that will be used for simulation and prototyping throughout this research project, any exception will be declared beforehand.

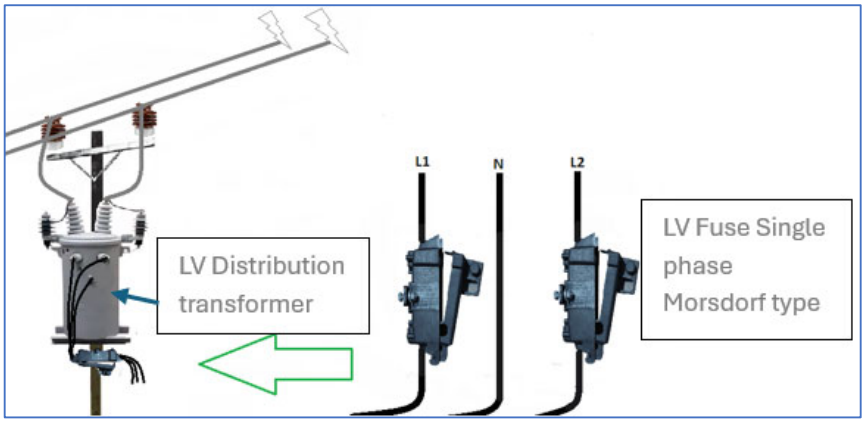

Figure 3.3: LV distribution transformer fuses for protection

Figure 3.3 illustrates an LV distribution transformer and its associated fuses. In contemporary LV networks, LV distribution transformer fuses constitute one of the only two forms of protection employed for safeguarding the transformer. These fuses function as overcurrent

protection devices, responding to both short-circuit and overload conditions (Ventruella, 2020). When an overcurrent or overload event occurs, the fuse operates, isolating the transformer and disconnecting all customers served by that phase. Consequently, customers experience a loss of supply until an operator is dispatched to the site to replace the fuse, a process triggered by consumer reports or by smart meters indicating an outage. This manual restoration procedure introduces delays and negatively impacts supply restoration times.

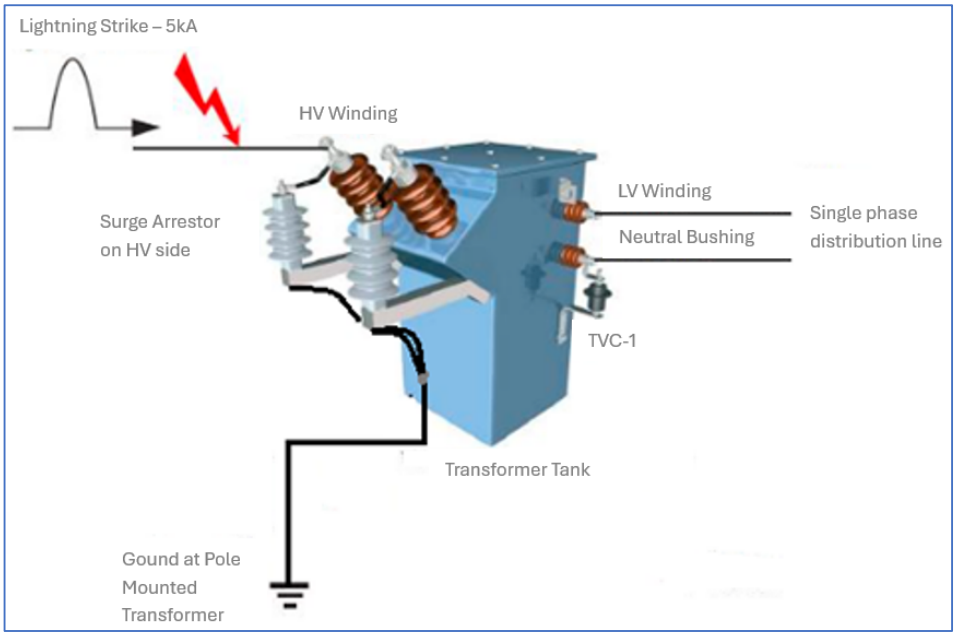

Figure 3.4: LV distribution transformer surge arrestors
(adapted from: Daniel Yapias, 2015)

The second form of protection in LV distribution transformers is provided by surge arrestors. When integrated with transformer earthing, these devices safeguard the transformer against unwanted voltage surges that could cause insulation breakdown and equipment damage, as illustrated in Figure 3.4. A surge arrestor behaves as a semiconductor with a prescribed breakdown voltage. Under normal operating conditions, it acts as an insulator; however, when the line voltage surpasses the breakdown threshold, the arrestor conducts and shunts the surge energy to ground via the earth connection at the base of the device. This discharge mitigates the energy transferred to the transformer, thereby protecting critical components from surge-induced damage (Lanphier et al., 2007).

Despite their protective role, surge arrestors themselves require monitoring and replacement after protective events. Once a surge has occurred and the arrestor has operated, the transformer remains without surge protection until inspection and maintenance are performed. In practice, it takes approximately twelve months for operators to detect damaged surge arrestors during annual line inspections. Consequently, replacement or repair occurs at these

maintenance intervals, often concurrent with identifying transformer faults. The delayed detection and replacement of compromised arrestors impose substantial operational costs on utility companies, given the increased risk of transformer damage during subsequent surges. From an economic perspective, transformers represent a significant capital expense relative to the cost of surge arrestors.

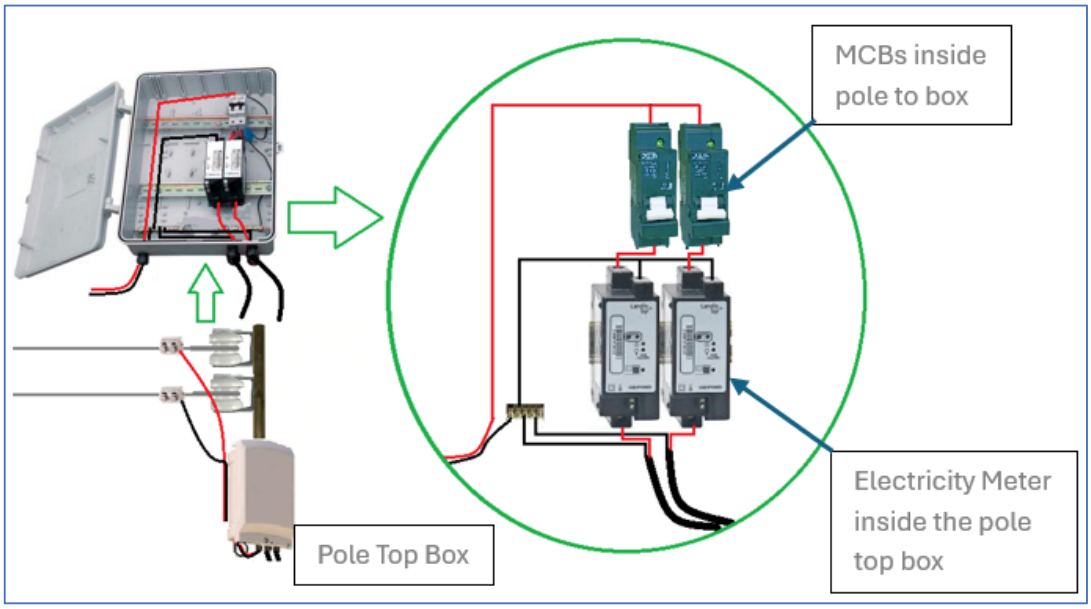

Figure 3.5: LV distribution network pole top box

Figure 3.5 depicts a pole-top box serving as a connection point for an LV distribution network. The connection from the distribution lines is made from bare phase and neutral conductors using insulated wires that enter the pole-top enclosure. Within the enclosure, the live conductor is routed to a circuit breaker before feeding the customer metering equipment, which may be a traditional split-meter or a smart-meter arrangement. The number of meters housed within the pole-top box corresponds to the number of customers served by that particular pole-top box; for example, a 6-way box accommodates six meters and six connected customers, while a 4-way box serves four meters and four customers.

The circuit breaker functions as an overcurrent protection device, designed to interrupt the supply to a customer when their current draw exceeds the breaker's rated capacity or in the event of a short circuit occurring on the service cable (Mennell, 1997). When the circuit breaker operates (trips), the affected customer experiences a temporary loss of supply until a line operator is dispatched to reset the device. This manual intervention introduces delays in the restoration of electricity to the affected customer.

From the given overview, several inherent drawbacks of the incumbent topology become evident. Primarily, the manual operation and limited visibility impede rapid fault detection, isolation, and restoration. These issues highlight the potential benefits of enhanced network visibility, automation, and control. Improvements in these areas can lead to higher customer satisfaction and reduced operating costs for the utility. In alignment with advances in smart grid technology, the present project seeks to address these drawbacks by enhancing visibility, automation, and control within the LV distribution networks.

3.4 Evolution of connecting single phase customers to LV networks

The process and framework for integrating single-phase consumers into the South African electricity grid has developed over time. A principal impetus and driver of this evolution is the persistent challenge of detecting and mitigating electricity theft.

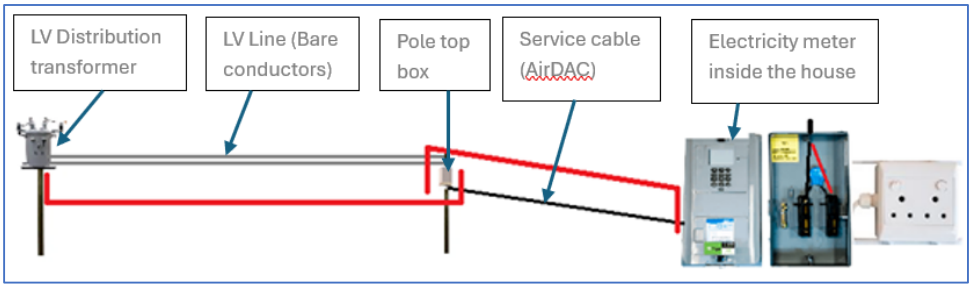

Figure 3.6: Old prepaid meter type

Figure 3.6 depicts the connection of LV customers to the LV network via an LV distribution transformer and a pole-top box leading to an electricity meter installed inside a customer residence. In this configuration, the electricity meter resides within the dwelling, linked to the pole top box by an AirDac (the service cable connecting the customer premises to the distribution line), allowing customers to load electricity tokens directly into the meter. A notable drawback of this arrangement is an elevated susceptibility to meter tampering and bypass. Seals on the meter can be easily compromised, enabling tampering within the confines of the customer's residence. In many cases, customers do not even need to access the meter itself; they can simply connect other appliances on the AirDac above the electricity meter, additional high-power appliances—such as electric stoves and geysers—thereby drawing energy directly from the LV network without measurement. The vulnerabilities in this arrangement create two principal theft vectors within the LV distribution network: (i) the segment from the pole-top box to the interior meter (as indicated by the red line in Figure 3.6) and (ii) the conduit segment between the LV distribution transformer and the pole-top box (as indicated by another red line in Figure 3.6). To mitigate electricity theft resulting from meter bypass, the split metering system was introduced.

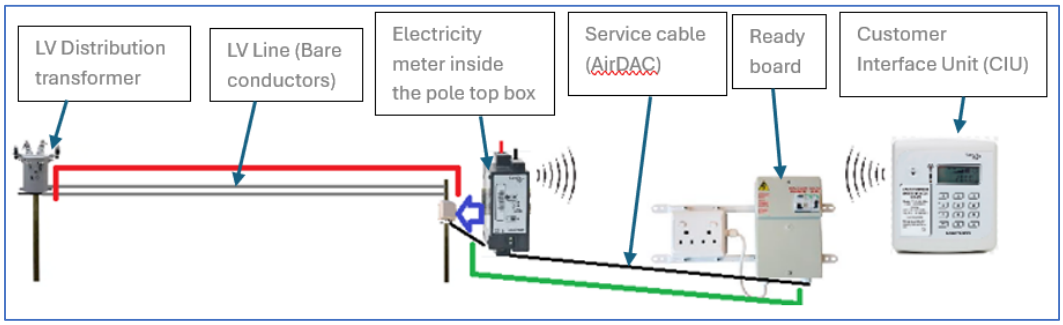

Figure 3.7: Split metering unit

Figure 3.7 depicts the procedure for connecting a customer to the LV network using a split metering configuration. In this arrangement, the electricity meter is separated from the Customer Interface Unit (CIU); the meter is installed in the pole-mounted box outside the dwelling, while an internal “ready board” within the house connects to the distribution board (DB) through an AirDac, to interface the customer’s appliances with the external connection from the pole. Inside the dwelling, the CIU houses the keypad component of the system. The CIU communicates with the external meter via either Power Line Carrier Communication (PLCC) or radio frequency (RF) channels. The customer uses the CIU to load tokens into the external meter. When the meter exhausts its allocated electricity units, a relay situated at the external pole causes a disconnection, thereby interrupting supply to the house and to the main feeder cable entering the residence (as illustrated in Figure 3.7). This configuration has effectively mitigated the problem of customers bypassing the meter from within the dwelling. Even if a customer attempts to connect their appliances directly to the main cable above the ready board (AirDac), all consumption must still pass through the customer-side meter located on the outside pole. Consequently, the only segment of the LV network that remains susceptible to electricity theft after installing split metering units is the remainder of the network from the transformer to the internal meter within the pole box, as indicated by the red line in Figure 3.7. Figure 3.8 below further illustrates the exploitation of this vulnerability.

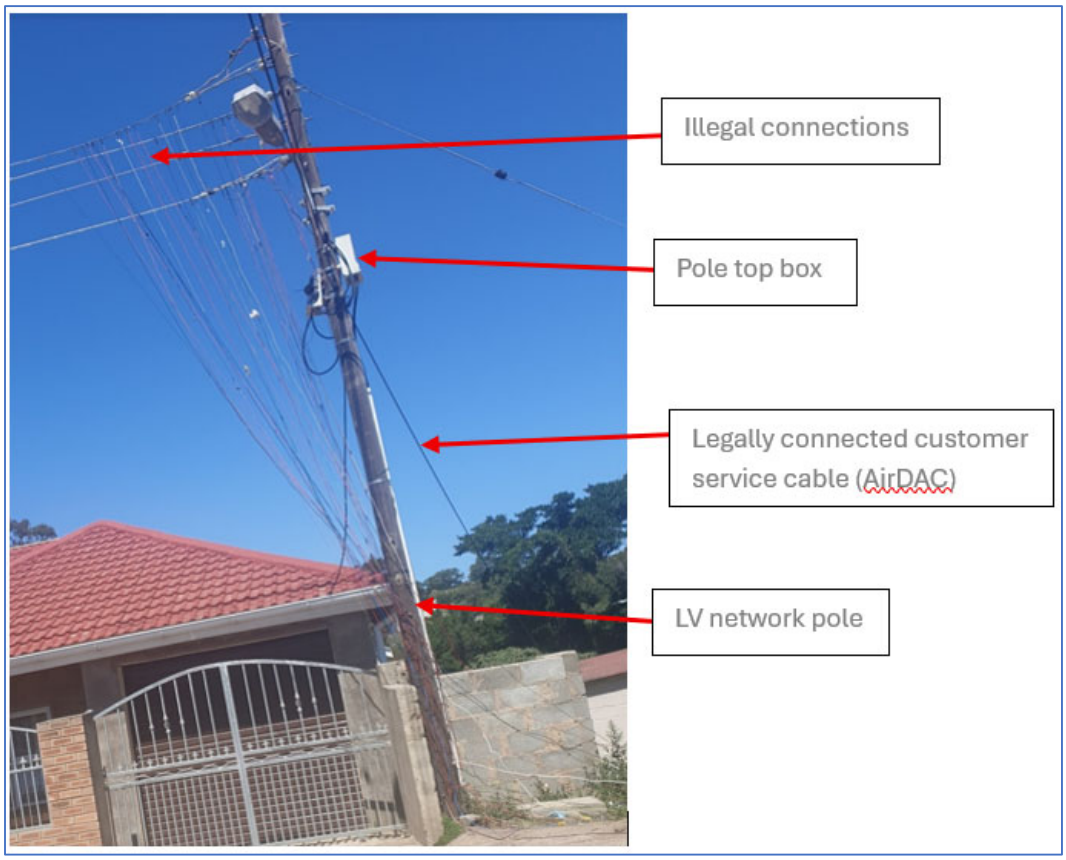

Figure 3.8: Image showing illegal connections
(Image taken in 2023 by the author, in a township in the Eastern Cape)

The proposed system described in this thesis is designed to address this vulnerability, ensuring that no portion of the network remains exposed to electricity theft.

3.5 Current flow in an LV network

3.5.1 Simulation of current flow in an LV network

Figure 3.9 depicts an LV distribution network featuring an illegal connection. The illustration indicates that the illicit hookup increases the number of connected customers from five to six. For ease of spotting the difference, the illegally connected customer is tapping between the poles, whereas legally connected customers have meters installed inside the pole-top box. Since this connection is not metered, it taps directly onto the conductor without any metering device.

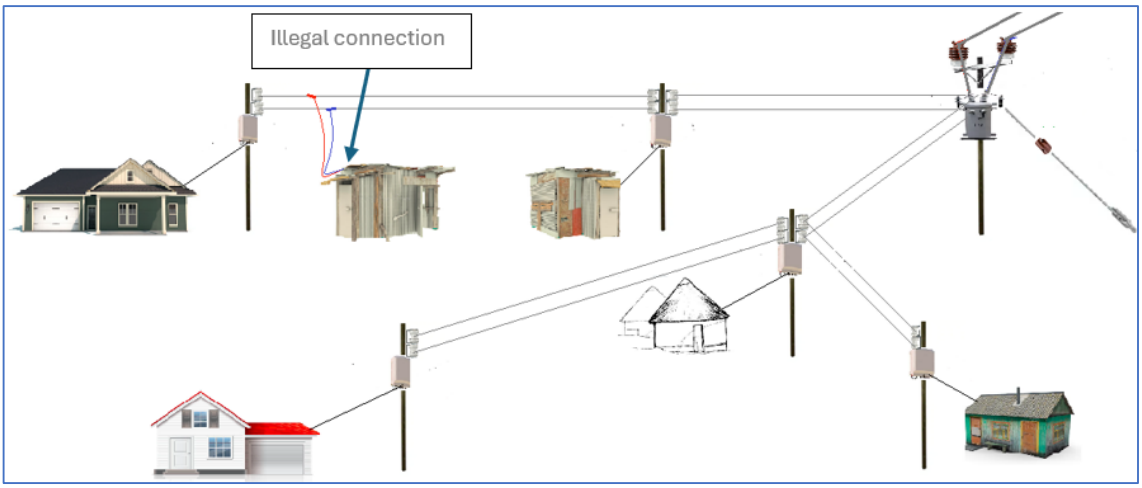

Figure 3.9: LV distribution network with an illegal connection

This LV distribution network is further analysed using Proteus simulation software, as depicted in Figure 3.10. In the simulation, a 22kV/400V centre-tapped LV distribution transformer is employed and connected to an alternating current (AC) source. On the LV side of the transformer, two voltmeters are connected between each phase and the neutral conductor located adjacent to the transformer. Both voltmeters indicate a nominal voltage of 230 V, which corresponds to the supply voltage available at the customer premises. To model the customers on this LV distribution network, light bulbs are used as representative loads, each possessing a resistance of 230Ω. Applying Ohm's law to the network yields:

$$V = IR \tag{3.1}$$

$$I = \frac{V}{R} \tag{3.2}$$

$$I = \frac{230}{230}$$

$$I = 1A$$

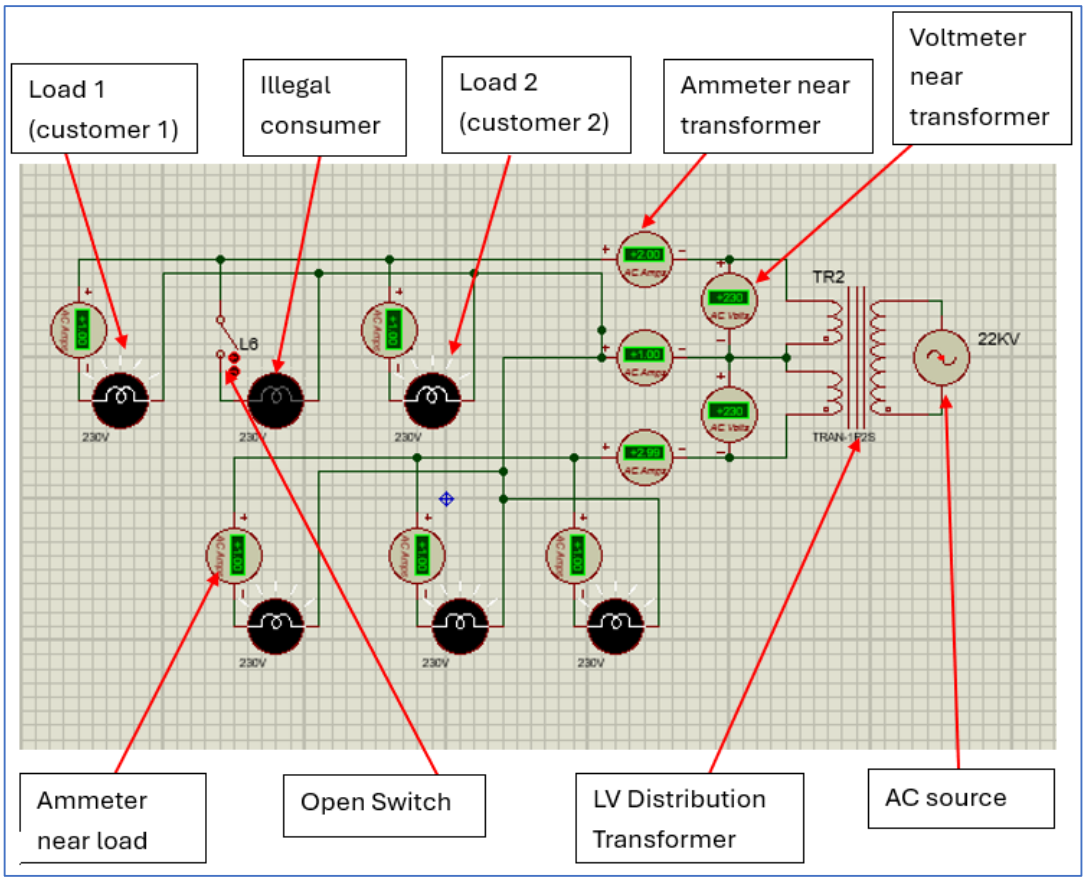

Figure 3.10: **Simulation of the LV distribution network in Proteus simulation software**

Consequently, each bulb draws a current of 1A, where I denotes the current in amperes, V denotes the voltage across the bulb in volts, and R denotes the bulb's resistance in ohms. The calculation shows that each bulb should draw an electric current of 1A when the simulation is run.

In Figure 3.10, each bulb representative of a customer premises is paired with an ammeter to quantify its individual current drawn from the distribution network, effectively serving as a surrogate electric meter for a real-life low-voltage distribution system. As depicted in Figure 3.10, the ammeters adjacent to five bulbs register 1A each. The illustration also includes a sixth bulb that is used to represent an illegal connection. To facilitate rapid identification of the illegal connection, this bulb is not equipped with an ammeter; notwithstanding, it is electrically identical to the other bulbs and thus draws the same current, presuming it is metered. This additional bulb is fitted with a switch to permit controlled introduction and removal of the illegal connection for experimental purposes. When the simulation is executed, all bulbs transition to white colour, except for the illegal-connection bulb, whose colour remains unchanged due to the switch remaining in the off position. In the baseline condition without the illegal connection, the top phase comprises two bulbs, and the bottom phase comprises three bulbs. With two

top-phase bulbs each drawing 1A, the ammeter adjacent to the transformer on the top phase records a total of 2A, while the bottom-phase ammeter records 3A, corresponding to the aggregate current drawn by the three bottom-phase bulbs. Additionally, a current of 1A flows through the neutral ammeter adjacent to the transformer to offset the phase current imbalance.

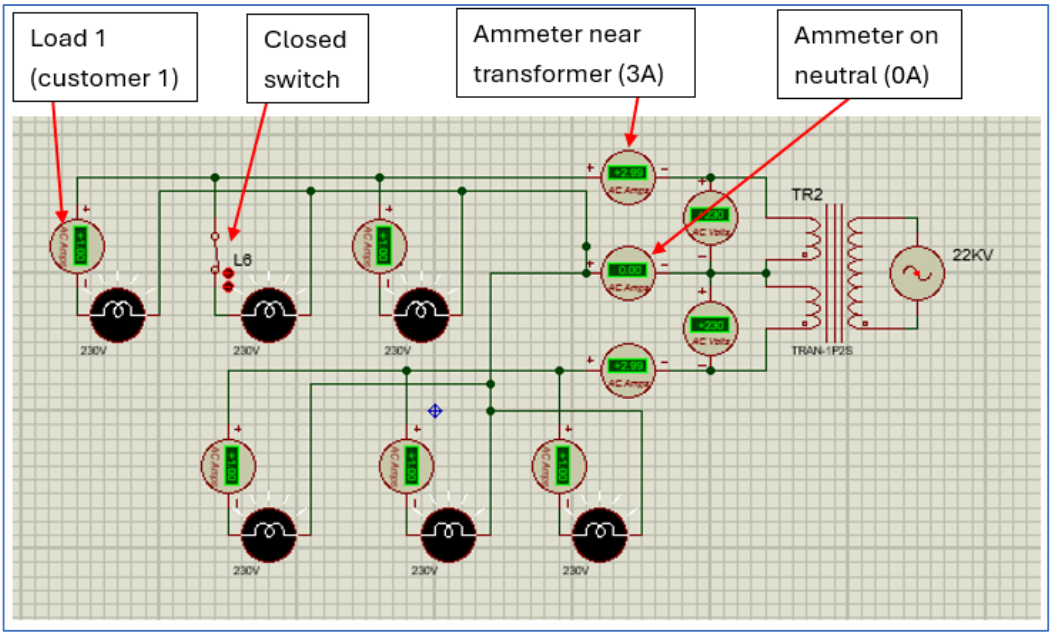

Figure 3.11: **Simulation of the LV distribution network in Proteus simulation software with an illegal connection**

Figure 3.11 depicts the LV distribution network with an illicit connection introduced into the system. The illegal connection initiates a drawing of 1A. The current drawn by the other loads remains unchanged; however, a marked change is observed in the ammeters located proximal to the transformer. Specifically, the current drawn from the affected phase near the transformer increases. Consequently, the total current supplied surpasses the total current metered, indicating that the transformer must supply additional current to accommodate the illegal connection as well. This discrepancy between the supplied and metered currents underscores the impact of unauthorized tapping on network loading and measurement accuracy.

3.5.2 Theory behind the current flow on an LV network

Kirchhoff's current law asserts that the total current entering a junction (or node) is equal to the current exiting the node, given that no charge is accumulated within the node (Zemanian, 1992). This principle underpins the theoretical basis of the proposed system in this study.

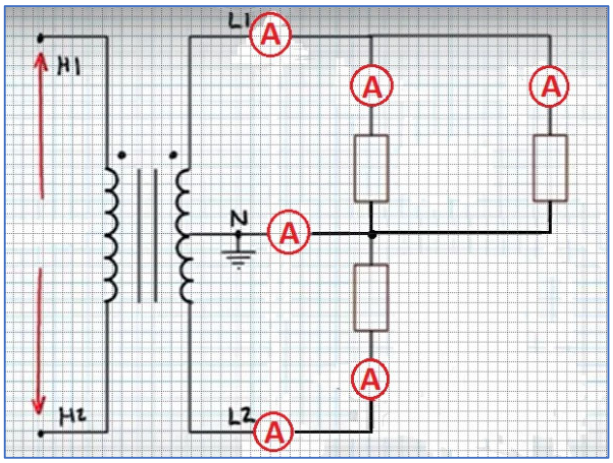

Figure 3.12: Low voltage network schematic diagram

In Figure 3.12, a representative low-voltage network schematic is depicted. The diagram features a single-phase centre-tapped transformer and three loads; each modelled as an individual household. For a transformer with a turn's ratio of 1:1, the line-to-line voltage between H1 and H2 is 460V. Consequently, the phase-to-neutral voltage for each phase (L1–N and L2–N) is 230V. Each load connected to the network experiences a voltage of 230V across its terminals. The current flowing through each load is governed by Ohm's Law (Eq 3.1),

$$V = IR \qquad (3.3)$$

such that I = V/R, where V is 230V for each load and R is the respective load resistance (Glover et al., 2012).

Scenario 1: Refer to Figure 3.13; the combined loads between L1 and N are exactly equal in resistance to those between L2 and N. This condition is characterized as a balanced system.

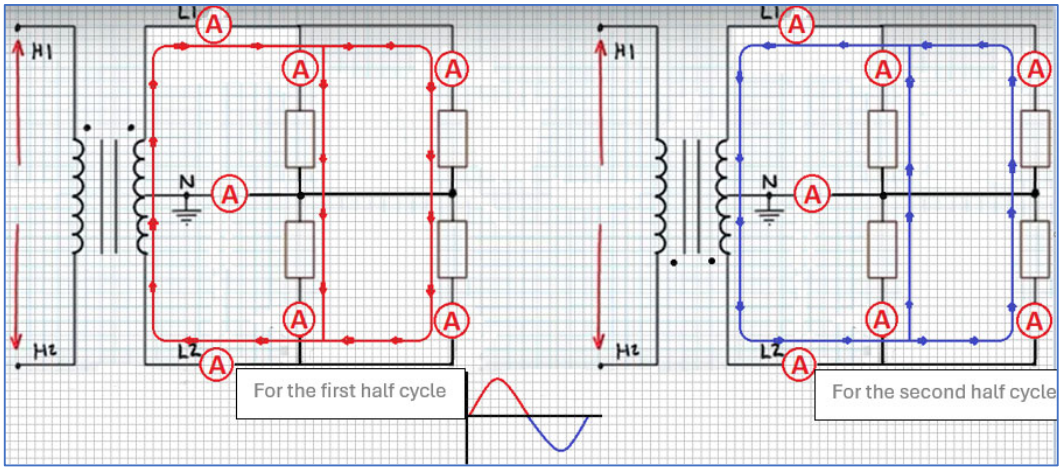

Figure 3.13: Flow of current for balanced system in an LV network, Full cycle broken down into two halves

Figure 3.13 depicts the current flow for a balanced system in an LV network, considering a complete AC waveform divided into two half cycles. In the left-hand illustration corresponding to the first half cycle, current flows from L1 through the loads connected between L1 and N, as well as through the loads connected between L2 and N, as indicated by the red arrows. The current in the branch L1–N is perceived as emanating from the live (L) terminal throughout this half cycle, whereas the current in the branch L2–N is perceived as originating from the neutral (N) terminal. The neutral conductor returning to the transformer carries no current in this half cycle. In the right-hand illustration, corresponding to the second half cycle of the AC waveform, the current flows from L2 through the loads between L2–N and L1–N, as indicated by the blue arrows. No current flows through the neutral conductor back to the transformer during this half cycle. During this half cycle, the loads on L2–N experiences current originating from the live terminal, while the loads on L1–N experience current as if originating from the neutral terminal; this pattern repeats for alternating half cycles.

Scenario 2: In reference to Figure 3.14, the loads connected between L1 and N exceed the load between L2 and N. Consequently, the aggregate current drawn by the two loads between L1 and N is greater than the current drawn by the single load between L2 and N.

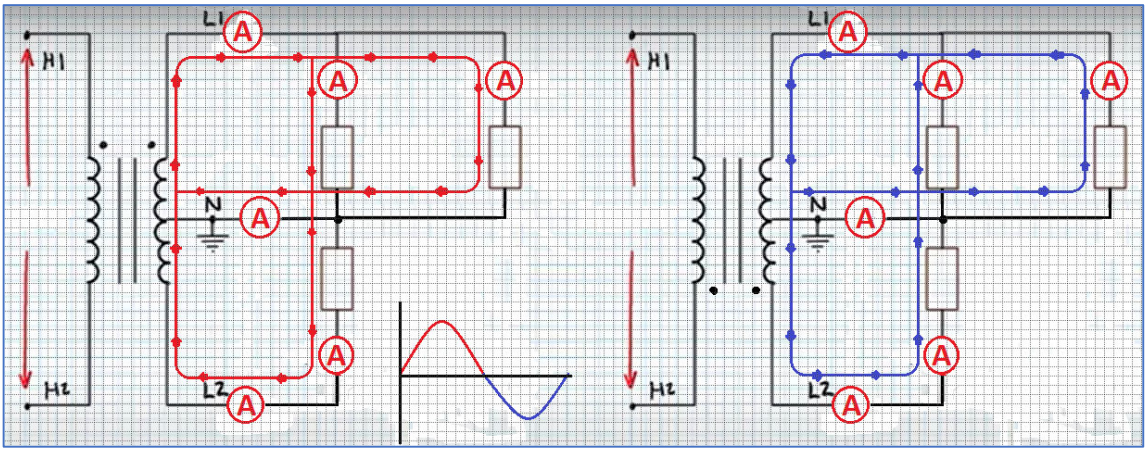

Figure 3.14: **Flow of current in an unbalanced system, Full cycle broken down into two halves**

Figure 3.14 depicts the current flow in an unbalanced system for a full AC waveform divided into two halves. During the first half-cycle, shown on the left, current flows from phase L1 through the loads connected between L1 and Neutral (N). The aggregate current drawn by these loads exceeds the current required by the load between L2 and N; consequently, the load between L2 and N draws only its necessary portion from the combined currents, and any surplus current returns to the transformer via the neutral conductor. In the corresponding depiction in Figure 3.14 (on the right), the current flow for the second half-cycle is illustrated. During this half-cycle, current proceeds from L2 through the load between L2 and N. Since the

current demand of the L2–N load is less than the combined currents of the L1–N loads, the neutral conductor supplies the requisite excess current to augment the L2–N load current so that the total currents meet the requirements of the two loads connected to L1. The described sequence then repeats.

In the final scenario, it is possible to modify the load profile to impose higher loads on the second phase (L2); however, the system will continue to operate in the same manner as the system functions observed in Scenarios 1 and 2. It is important to note that, in both cases, the currents within the closed-loop system sum to zero, in accordance with Kirchhoff's Current Law. This holds notwithstanding the dynamic nature of current flow, which can exhibit substantial variations as individual appliances are powered on and off. Such operational behaviour can cause the loads to transition between balanced and unbalanced states at different times of the day.

The preceding discussion, in reference to Figure 3.14, yields several consistent conclusions regarding phase currents in the described electrical system:

- First, the algebraic sum of the currents through the loads connected between phase 1 (L1) and Neutral (N) is equal to the total current in phase 1, as measured by the ammeter A located at phase 1 proximal to the transformer.
- Second, similarly, the sum of the currents through the loads connected between phase 2 (L2) and Neutral (N) equals the total current in phase 2, as measured by the ammeter A situated at phase 2 near the transformer.
- Third, if there is no current flowing through the ammeter at Neutral, then the current measured at the L1 ammeter must equal the current measured at the L2 ammeter, indicating phase balance (i.e., IL1 = IL2).
- Fourth, if there is current through the Neutral ammeter, then either IL1 equals the sum of IN and IL2, or IL2 equals the sum of IN and IL1; this condition indicates an unbalanced system.
- Finally, deviations from the conditions stated above may indicate a fault within the system, such as a broken conductor or another fault that provides a path for current to ground. Such a fault would disrupt the closed-loop condition and could be exploited to isolate the transformer as a means of fault localization and environmental protection.

The above consistent conclusions are employed to develop a system for monitoring abnormal conditions within an LV distribution network. The approach requires the measurement of current from various segments of the LV network and the establishment of a real-time comparison framework to assess prevailing operational conditions. Based on these comparisons, appropriate decisions and actions are then executed to respond to detected

anomalies. This methodology underpins the monitoring of faults and illicit connections within the LV network analysed in this work.

3.6 Smart grid architecture

Smart grid technology represents a paradigm with a range of important objectives. Key aims include the decentralization of generation within electricity networks, the integration of green renewable energy sources, real-time grid visibility, data acquisition to support informed decision-making, and enhancements in protection, automation, supervisory control, energy efficiency, and energy storage, among others. Collectively, these objectives seek to foster a sustainable energy future and improve grid stability and reliability. Achieving them requires a rapid transformation of the legacy electricity grid, yet implementing all measures simultaneously would be prohibitively expensive. A prudent strategy involves developing and deploying projects that target specific objectives across different levels of the electricity grid, enabling incremental progress while managing costs and risk (Regmi, 2015).

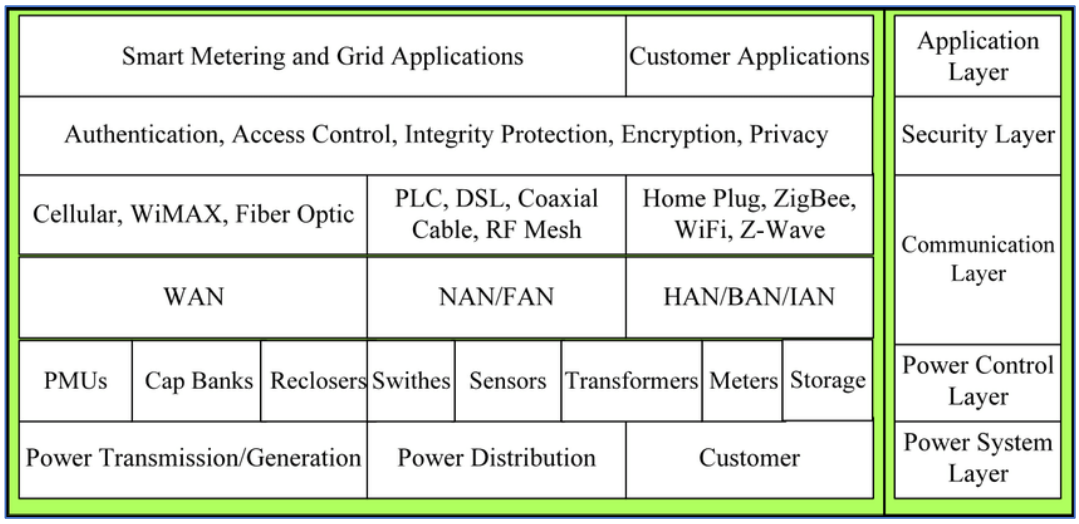

Figure 3.15: Smart Grid Multi-Layer architecture
(Regmi, 2015)

Figure 3.15 depicts a smart grid architecture organized into multiple layers, illustrating how smart grid technologies are implemented and developed. The model comprises five layers: power system, power control, communication, security, and application, with each layer containing distinct elements and functions.

In the power system layer, the key components are power generation, transmission, distribution, and customers. The power control layer focuses on the devices and subsystems used to regulate and manage the grid, including Phasor Measurement Units (PMUs), capacitor banks, reclosers, switches, sensors, transformers, smart meters, and energy storage systems.

The communication layer addresses the configuration of communication networks and media that enable data exchange across the grid. The Wide Area Network (WAN) links devices or gateways across distances ranging roughly from 10 km to 100 km. Potential communication media include cellular, WiMAX, and Fiber optic links. Within the same layer, the Neighbourhood Area Network (NAN) and Field Area Network (FAN) connect more distant devices over intermediate ranges, approximately 100 meters to 10 kilometres. Mediums for NAN and FAN can include PLCC, Digital Subscriber Line (DSL), coaxial cable, or RF mesh technologies. The Home Area Network (HAN), Building Area Network (BAN), and Industrial Area Network (IAN) connect devices within much shorter proximities, from about 1 meter to 100 meters, with communication options such as home plug, ZigBee, Wi-Fi, or Z-Wave. Data transfer among devices can cascade across ranges—for example, substation automation and control may entail linking devices within a FAN and subsequently connecting substations across a WAN. This hierarchical connectivity enables visibility, protection, automation, and control of substations (Regmi, 2015).

Data exchange and device intercommunication require robust security measures. The security layer addresses data protection concerns, including authentication, access control, integrity protection, encryption, and privacy. The final layer, the application layer, provides end users with access to data for enhanced control, management, and application deployment (Regmi, 2015).

3.7 Internet-of-things (IoT) architecture

Smart grid technology can be understood as the application of the IoT principles to electricity grids. The IoT is a broad concept that encompasses numerous aspects of daily life, including transportation infrastructure, home automation, agriculture, healthcare, power systems, and even sports. At its core, the IoT involves deploying sensors and actuators on devices that require monitoring and control, thereby enabling these devices to connect with one another and with the Internet. As a result, such devices continually transmit data regarding their status, which facilitates ongoing monitoring and remote control via the Internet. This interconnected data ecosystem supports enhanced situational awareness, more efficient resource management, and improved reliability within complex systems such as modern electrical grids.

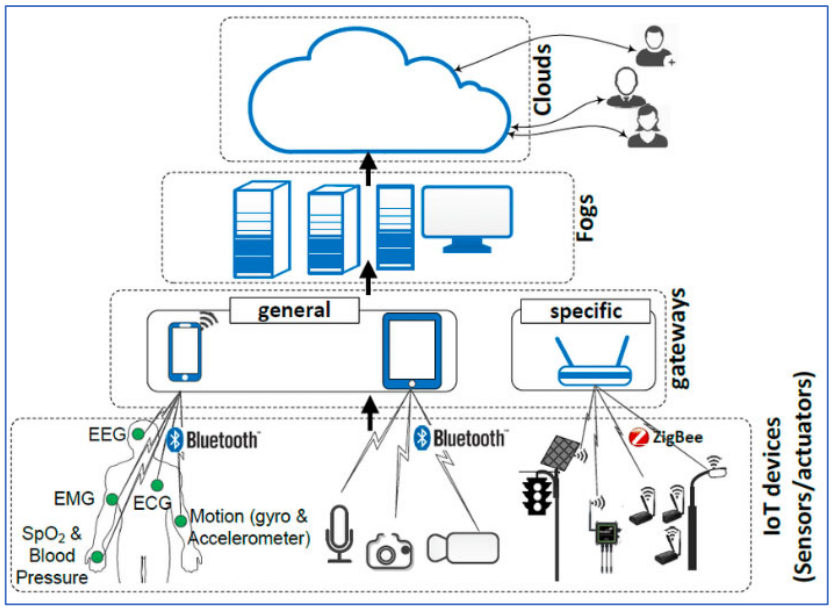

Figure 3.16: Internet of Things multi-layer architecture (Mekki et al., 2019)

Figure 3.16 depicts the IoT multi-layer architecture. At the base layer, sensors and actuators function as IoT devices deployed for monitoring. These devices are interconnected through various communication networks, which may comprise a HAN, NAN, or WAN. The devices communicate with gateways that connect them to Fog computing nodes. Fog computing embodies a distributed architecture in which a succession of nodes processes data from IoT devices in real time. The Fog layer performs computation, and, on occasion, uploads summarized data to the cloud for storage and subsequent retrieval. The IoT enables improved management in several domains: traffic management, autonomous (self-driving) vehicles, and accident prevention in road transportation; health monitoring and management in medicine; energy sustainability, reliability, and stability in power systems; and a wide range of additional applications across diverse sectors (Mekki et al., 2019).

3.8 Developed concept

In this study, an IoT multilayer architecture is applied to an LV distribution network within a transformer zone to develop a smart LV network, drawing on observations presented in section 3.5. The proposed system facilitates the measurement of currents drawn proximal to the transformer as well as the currents drawn by each legally connected customer. These measurements are compared in near real time to monitor for abnormal conditions, including illegal connections and to interrupt them as they arise within the LV network. The approach entails deploying IoT devices on each pole box situated in the transformer zone and installing an additional pole-top box adjacent to the transformer, each endowed with its own IoT device. A communication network is configured so that an IoT device in every pole box executes a predefined sequence of repetitive instructions designed to measure currents and voltages and

to transmit the data to a centralized repository where it can be cross-checked against the currents and voltages measured at the transformer phases and the neutral conductor. The expected outcome is a smart grid project characterized by a fully observable, automated, and controllable smart LV network, as depicted in Figure 3.17, with the capability to detect faults and illicit connections in real time and to interrupt power supply as necessary.

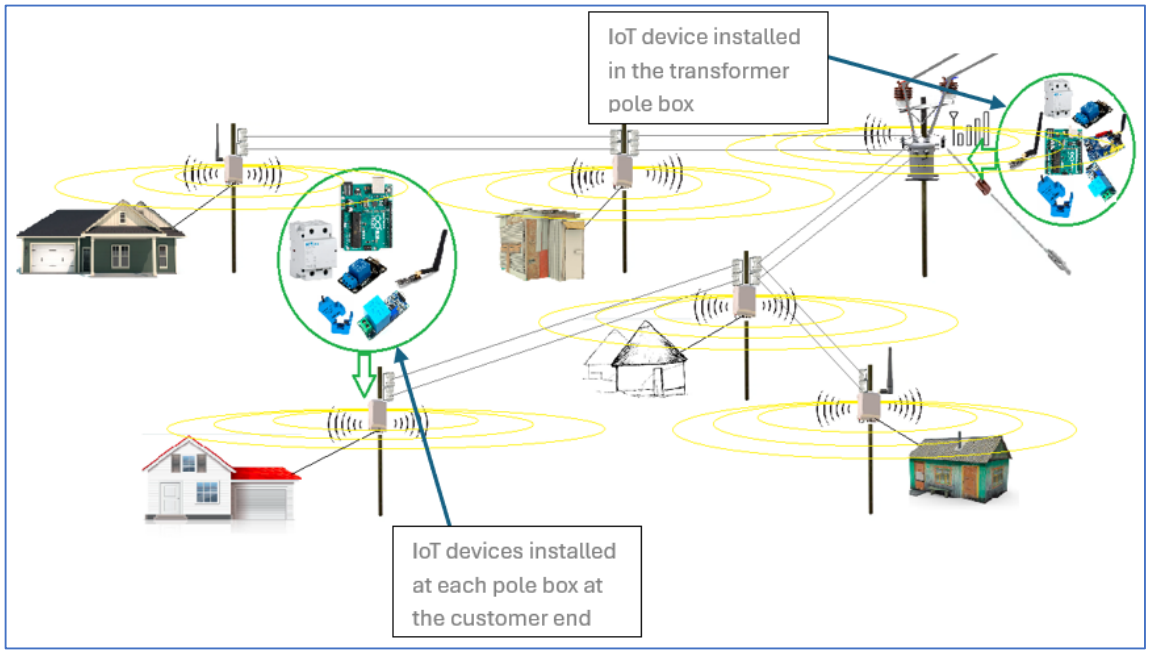

Figure 3.17: **Proposed Smart LV network showing one transformer zone**

Figure 3.17 presents the proposed smart LV network, illustrating a single transformer zone.

The resultant LV network is depicted via the flow diagram in Figure 3.18, which delineates the creation of a NAN that enables communication among the pole-top box located near the transformer and all other pole-top boxes connected to customer premises. This configuration supports near real-time exchange of current and voltage measurements. By incorporating a gateway, a WAN is established to interconnect multiple NANs—encompassing all transformer zones within the MV distribution network—to the utility's control centre or data centre. This WAN facilitates data collection, online monitoring, and automation of the LV network.

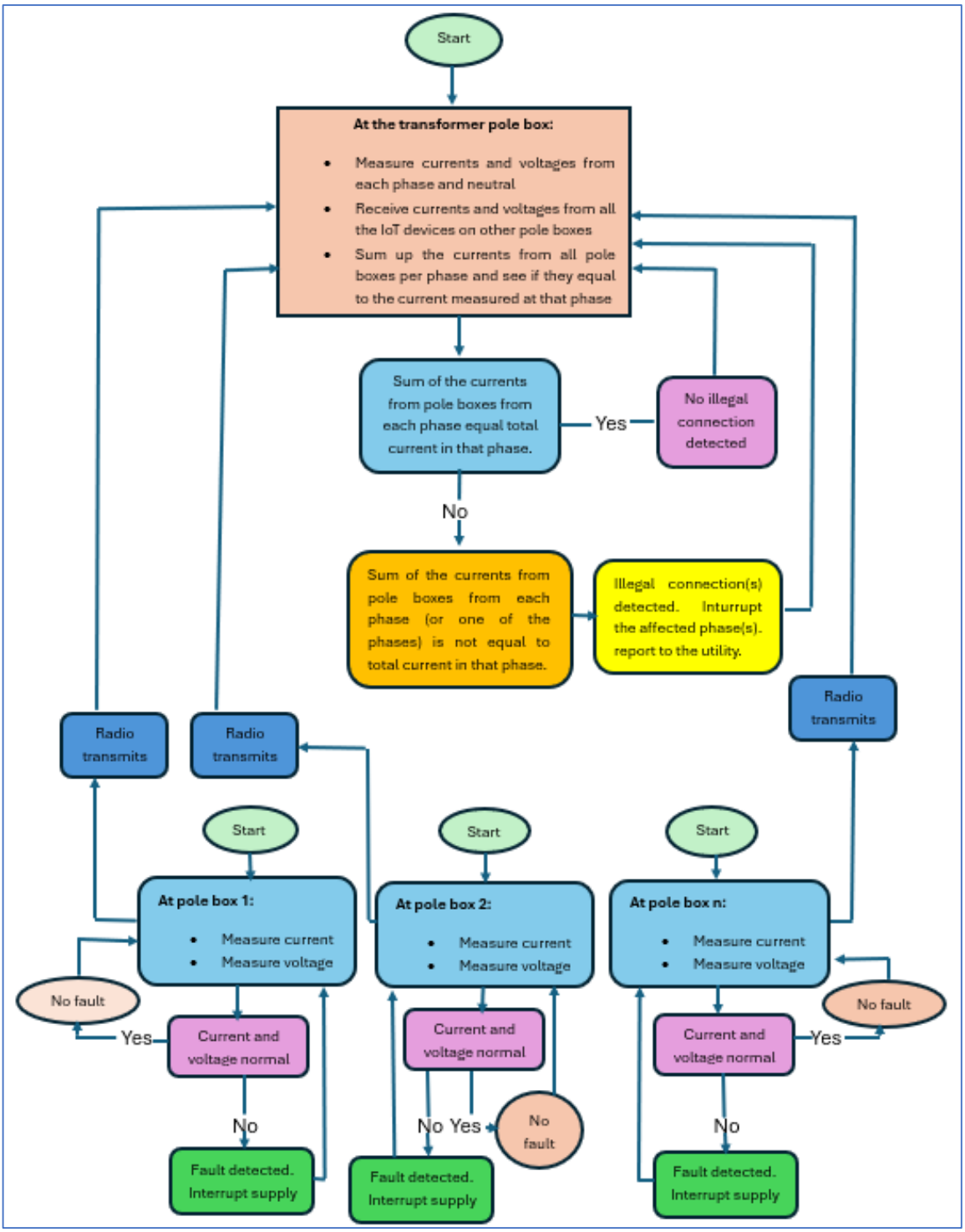

Figure 3.18: Flow diagram for monitoring, detecting and interrupting illegal connections

The diagram depicted in Figure 3.18 presents a composite of multiple flow diagrams integrated within a single schematic, interconnected through communications links. It includes a flow diagram representing the segment of the algorithm responsible for monitoring illegal connections that operates on the IoT device located at the transformer, which possesses a distinct initiation point. Additionally, it contains a flow diagram outlining the segment of the

algorithm that performs monitoring on IoT devices installed at each pole box, where customers are connected, spanning from pole box 1 to pole box n (where n denotes any arbitrary number of pole boxes within the transformer zone).

From the flow diagram starting from the pole boxes at the customer ends (Pole box 1 to Pole box n):
Step 1: The IoT device at the customer pole box measures the current drawn by the customer.
Step 2: The IoT device measures the voltage across the customer meter.
Step 3: The IoT device checks these values against allowable ranges (e.g., Maximum of 20A for a 20A customer, Maximum of 60A for a 60A customer and a voltage within 5% +/- 230V across the customer meter), anything outside these parameters would be treated as an abnormal condition and triggers isolation of the customer power.
Step 4: Only if there is a detected abnormal condition, the IoT device isolates the customer power.
Step 5: The IoT device radio transmit the measured current and voltage values and the status of the relay at this pole box to the IoT device near the transformer.
Step 6: The sequence starts over from step 1.

From the flow diagram at the transformer pole box:
Step 1: The IoT device measures currents from each phase and neutral.
Step 2: The IoT device measures voltages across each phase.
Step 3: The IoT device checks these measured values against the allowable ranges (e.g., maximum allowable currents to be drawn from the transformer per phase). The other checks done in this step is scanning for faults, which is further illustrated in Figure 3.19 below as an extension to Figure 3.18.
Step 4: Only if there is a detected abnormal condition from the measured values, the supply is interrupted on the affected phase(s).
Step 5: Receive the currents, voltages and relay statuses radio transmitted by the IoT devices from other pole boxes.
Step 6: Sum up the currents from all pole boxes connected in one phase for each of the phases.
Step 7: Compare the summed up received current per phase with the current measured in each phase.
Step 8: Only if the summed up received currents per phase are greater than the current measured in that phase, an illegal connection is detected, the affected phase is interrupted.
Step 9: The IoT device reports the interruption to the utility company for further action.
Step 10: The sequence starts over from step 1.

Figure 3.19 presents the flow diagram of the algorithm executing on the transformer IoT device for monitoring faults within the network. This flow diagram is an extension of step 3 on the abnormality checking at the transfomer IoT on figure 3.18.

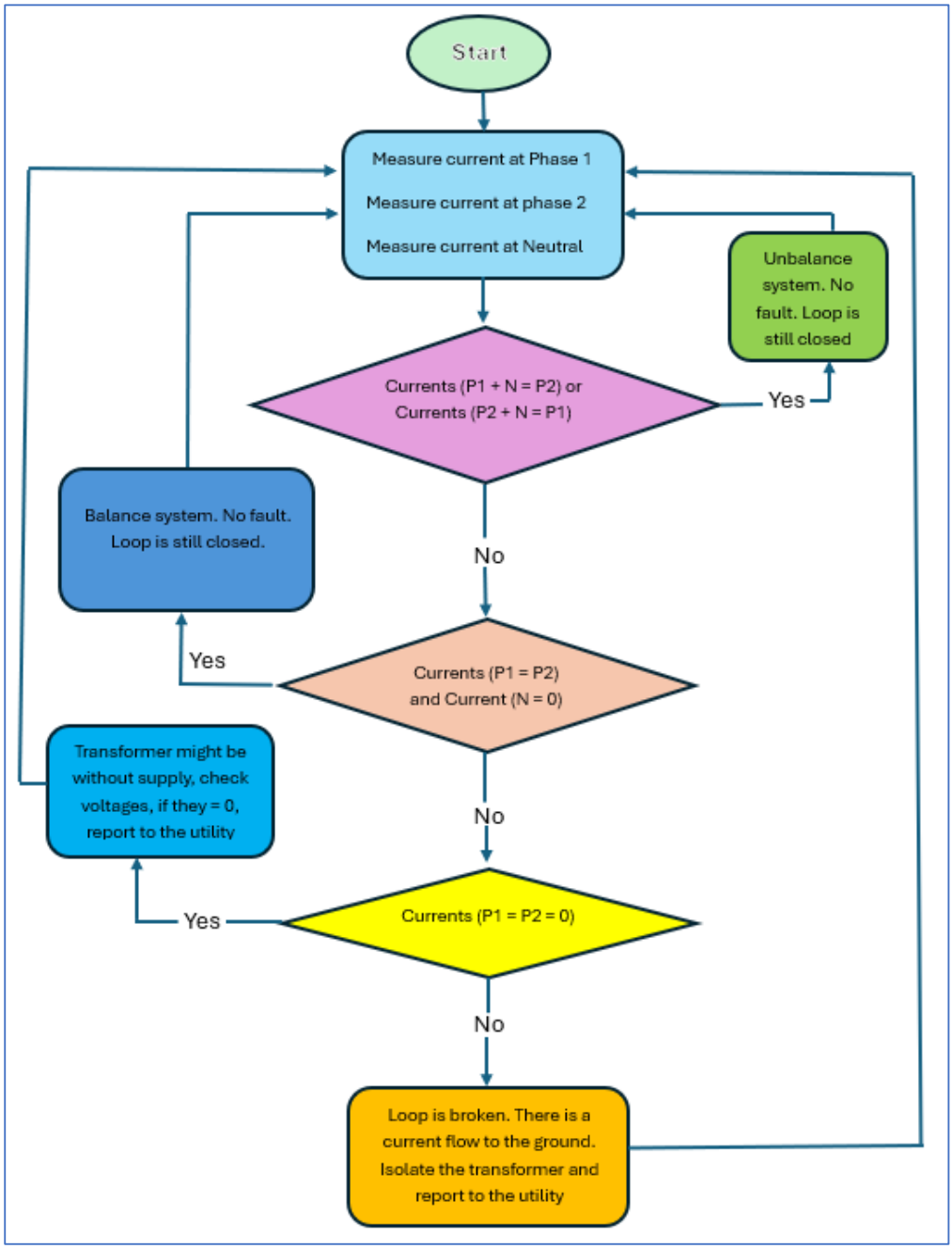

Figure 3.19: Flow diagram for detecting broken conductor on the ground

From the flow diagram at the transfomer pole box:

Step 1: The IoT device measures currents from each phase and neutral.

Step 2: The IoT device checks the currents against the condition: Currrent at phase one plus current at neutral must be equal to the current at phase two, or current at phase two plus current at neutral must be equal to the current at phase one)
Step 3: If the contition on step 2 is true, then there is no fault, the sequence start over on step 1.
Step 4: If the condition on step 2 is false, then check the currents against another condition: Current at phase one must be equal to the current at phase two and current in neutral must be equal to zero.
Step 5: If the contition on step 4 is true, then there is no fault, the sequence start over on step 1.
Step 6: If the condition on step 4 is false, then check the currents against another condition: Current at phase one must be equal to the current at phase two, equal to current in neutral and they must all be equal to zero.
Step 7: If the contition on step 6 is true, then the transfomer might be out of supply. The IoT device checks the voltage, if it is also equal to zero, it reports to the utility company. The sequence start over from step 1.
Step 8: If the condition on step 6 is false, then there is a fault on the transfomer zone, the IoT device isolates the affected phase(s) and report to the utility company.
Step 9: The sequence start over from step 1.

3.9 Changes to be made on the existing LV networks

The smart LV network is realized through the deployment of IoT devices at strategically selected locations within the existing LV distribution networks. Each IoT device is assembled from a heterogeneous set of electronic components. The device architecture centres on a microcontroller that serves as the processor, complemented by an NRFL01 radio module to enable wireless communication, creating a NAN. Integrated sensing elements include current and voltage sensors for monitoring electrical parameters, while relays and contactors provide the means to control the network. For wide-area connectivity, a Global System for Mobile Communications (GSM) module is incorporated to facilitate cellular WAN communication, thereby linking each NAN to the utility company’s information systems, such as the Distribution Management System (DMS).

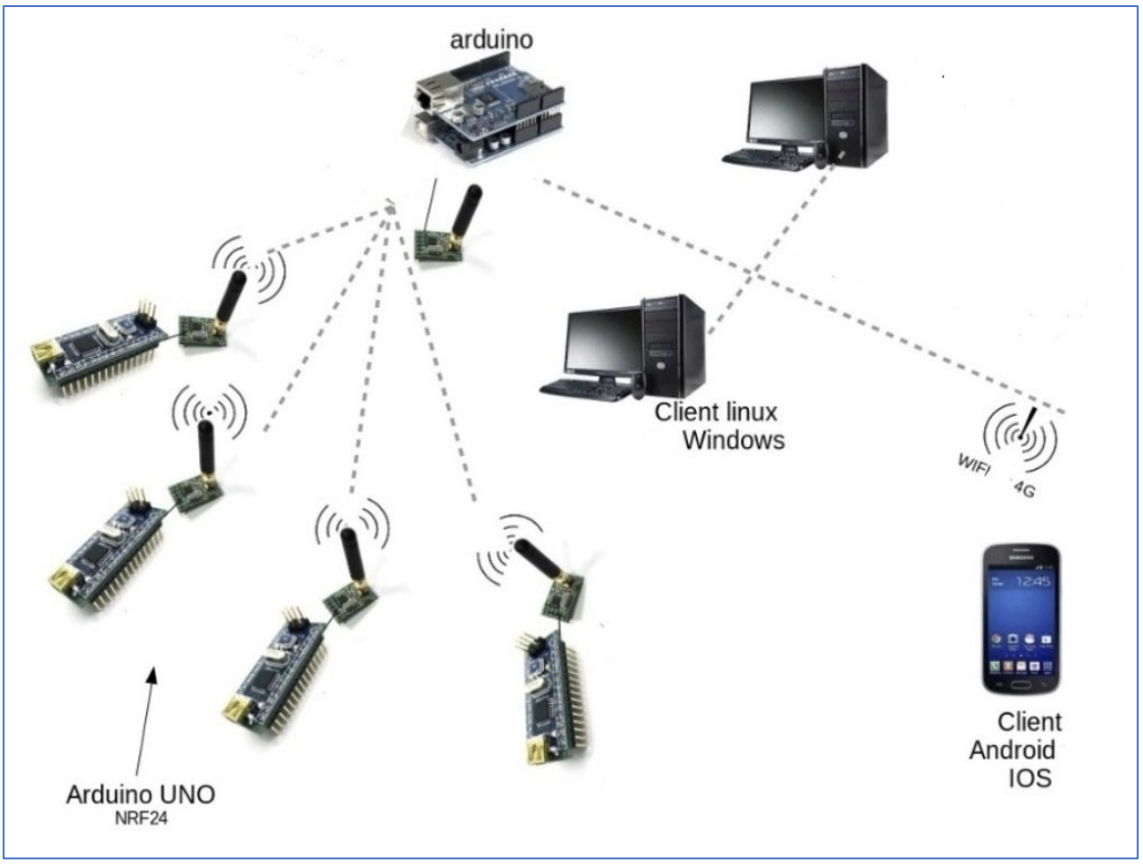

Figure 3.20: **Illustration of the mash network of the proposed system (Ndlovu et al., 2020)**

Figure 3.20 illustrates the proposed meshed network and its deployment, with each module mounted on a pole-top enclosure. In this configuration, network state updates are periodically transmitted, providing continuous situational awareness at predefined intervals. The circuit is capable of receiving commands from a mobile device (cell phone) or an associated distribution management system. This remote-control capability enables remote tripping and resetting of relays and contactors, thereby facilitating centralized operability of the network.

To deploy IoT devices on the existing LV network and to establish a mesh communication network, the following modifications are required for each transformer zone within the LV network.

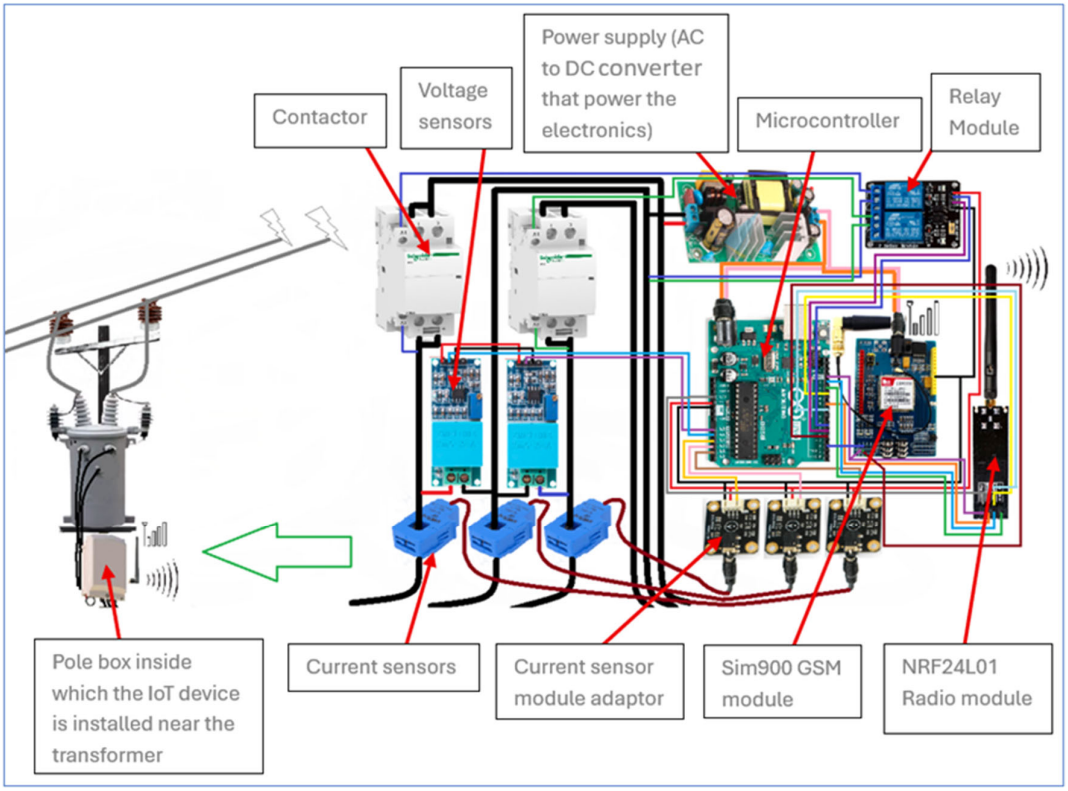

Figure 3.21: IoT device inside a transformer pole top box of a smart LV network

Figure 3.21 depicts the interior of the proposed transformer pole-top box. In the design, the transformer fuses are replaced with a contactor switch to facilitate automation and online control, thereby improving restoration of the supply under fault conditions. From the transformer, two power phases and a neutral conductor pass sequentially through three current sensor modules; these modules measure current and relay the data to the microcontroller. In addition, two voltage sensor modules monitor the voltages and feed the measurements to the microcontroller. Measuring the voltages proximal to the transformer mitigates the risk associated with a broken neutral conductor by ensuring that the voltages between both phases and neutral remain within acceptable ranges prior to delivery to customers. The microcontroller is interfaced with a radio module for data transmission and reception within the transformer zone NAN. It also incorporates a GSM module that serves as a gateway to connect to a WAN, enabling interconnection with other transformer zones. A relay module is employed to actuate the contactors during automation for supply interruption in abnormal conditions and for online control. The circuit is powered by a compact AC-to-DC converter (power supply). Additionally, this system is designed to be powered by small solar panel mounted on top of the pole to maintain functionality in the absence of network supply.

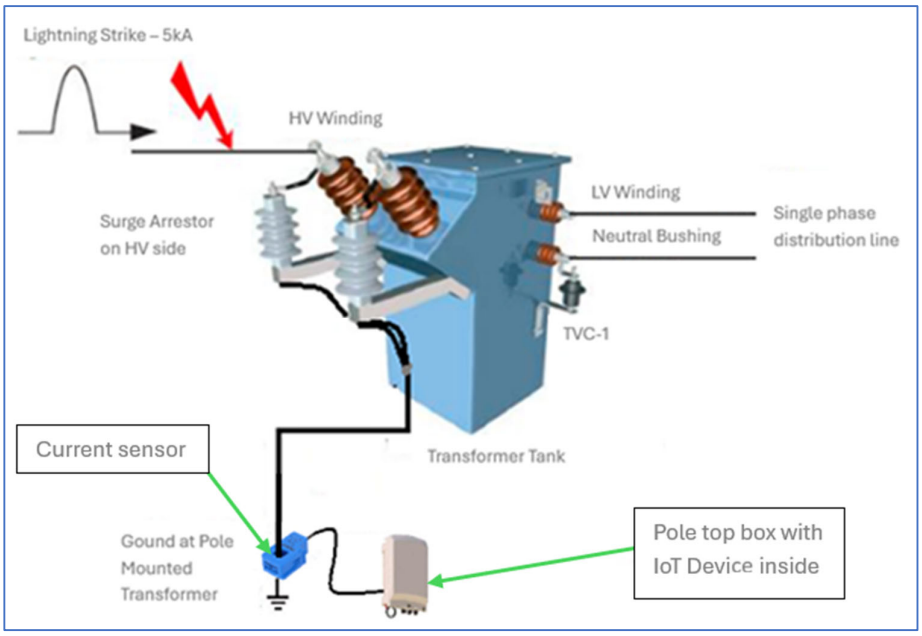

Figure 3.22: **Proposed surge arrestor monitoring**
(adapted from: Daniel Yapias, 2015)

To address the issue of surge arrestors operating and remain undetected for extended periods and thereby reducing transformer lifespan, Figure 3.22 illustrates a proposed surge-arrestor monitoring subsystem integrated into the overall system. Under normal conditions, the earth conductor connected to the surge arrestors should carry no current, with only a negligible leakage current present. When a surge arrestor operates, a substantial current flows to ground, after which the grounding path through the surge arrestor is effectively interrupted. Incorporating a current sensor module on the earth conductor, which is connected to a microcontroller, enables real-time monitoring and notification of surge-arrestor operation. This arrangement allows an operator to be dispatched to replace the surge arrestor prior to subsequent lightning events, thereby eliminating the need to wait for line inspections and contribute to extending transformer life span.

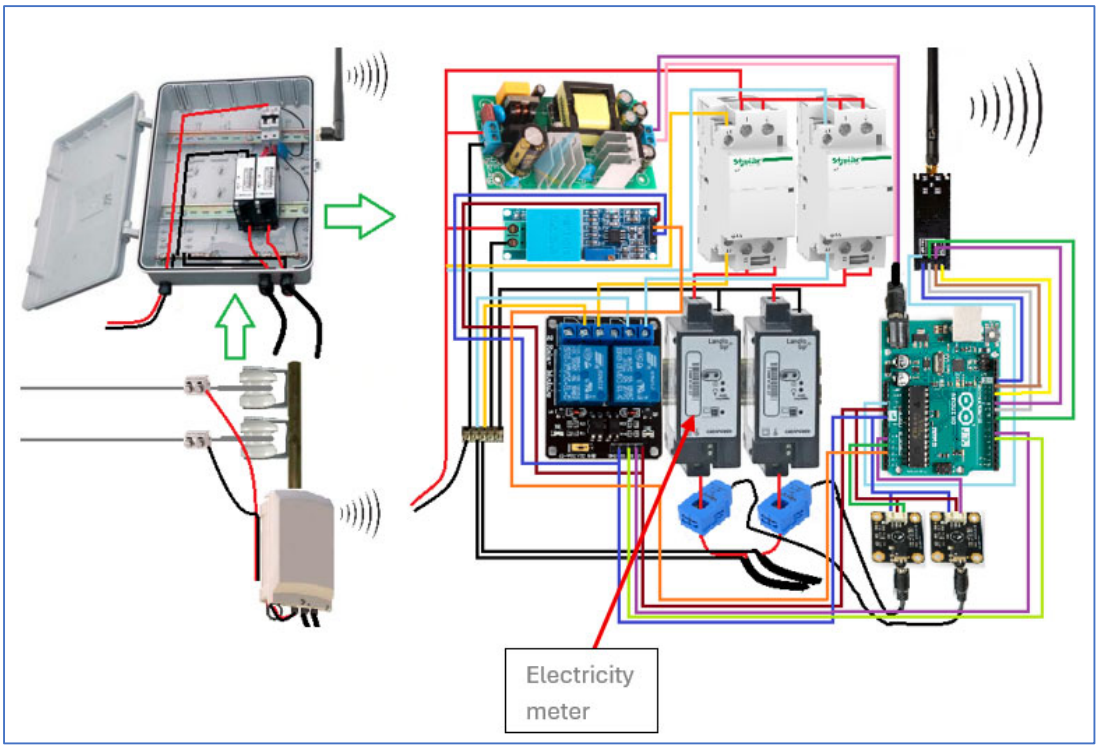

Figure 3.23: **IoT device inside a customer side pole top box of a smart LV network**

Figure 3.23 illustrates the interior configuration of the proposed pole-top utility box, which supplies electricity to customers. In the revised design, the circuit breaker is replaced by contactor switches to facilitate automated control and streamlined automation. Incoming line conductors, consisting of a live conductor and a neutral, connect to a voltage sensor module that delivers data to a microcontroller. Current sensors are positioned downstream of the customer meters along the feeder cable that routes to the customer premises; these sensors quantify the current drawn after passing through the customer meter and likewise feed data to the microcontroller. Consequently, the total number of current sensors in the enclosure is determined by the number of meters installed within the pole-top box. Any current flow that does not traverse one of the designated sensors will trigger an illegal-connection detection event. The relay module serves to operate the contactors for automation and control purposes. A radio module interfaces the pole-top box with a NAN, enabling near real-time transmission of currents, voltages, and relay status. The circuit is powered by a compact power supply and is designed to be concurrently supplied from small solar panel mounted on the top of the pole in the event of a power outage.

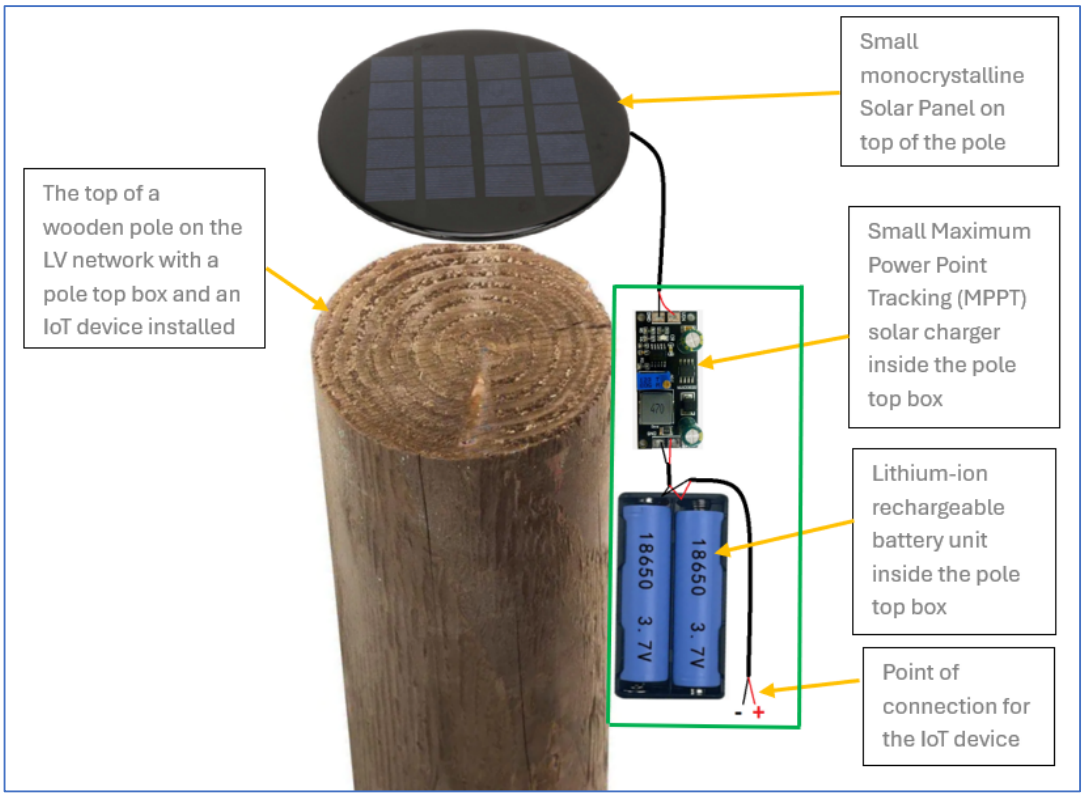

Figure 3.24: Solar energy unit as backup power for the IoT devices

The Smart LV network design, as presented, is complete yet contains a notable vulnerability. The IoT devices employed within the network are currently powered by the same electrical supply they monitor. Consequently, a total power outage would disable these devices, preventing ongoing data recording and hindering reports of power absence. This deficiency can be remedied by the modification illustrated in Figure 3.24: a solar energy unit mounted at the top of each pole, integrated with a pole box, and connected via a conduit along the pole into the pole box. The proposed unit provides a backup power source for each IoT device at every pole box, ensuring continued communication in the absence of grid electricity. The unit comprises a solar panel, a Maximum Power Point Tracking (MPPT) controller (a module that facilitates charging of rechargeable lithium-ion batteries while delivering protection against overcharging, deep discharging, and overcurrent conditions), and rechargeable lithium-ion batteries.

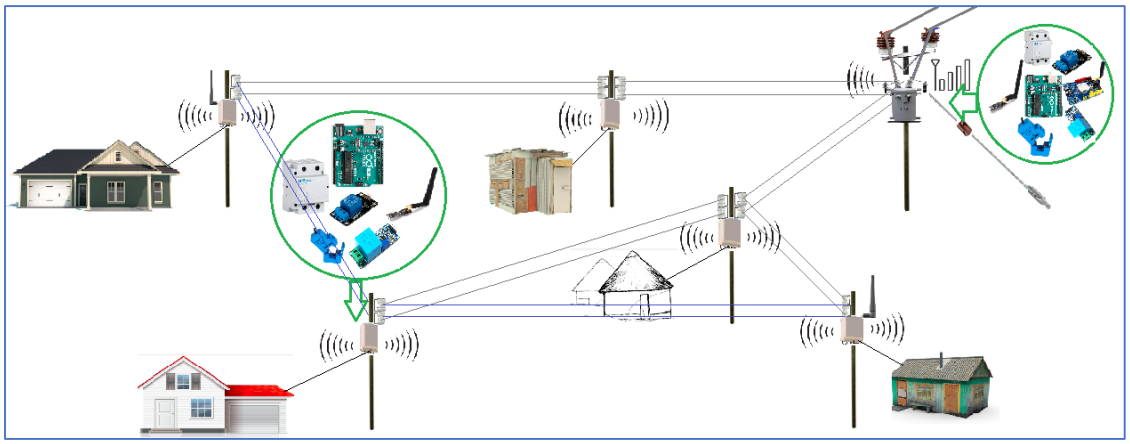

Figure 3.25: Proposed LV network with self-healing capabilities

Figure 3.25 depicts a ring network configured to support self-healing capabilities. In this architecture, if an unauthorized connection is introduced within any segment of a conductor between two poles, the affected span can be isolated autonomously while an alternative span is energized to restore power to the customers served by the isolated segment. Similarly, for faults such as a broken conductor mid-span, the compromised span can be fully isolated from both ends, with power rerouted to affected customers via an alternative pathway. This self-healing process can be executed automatically within a matter of seconds, minimizing service disruption and maintaining reliability.

3.10 Conclusion

This chapter provides an overview of the South African legacy power system and examines the current state of LV distribution networks, with emphasis on the drawbacks inherent in the existing design. It traces the historical evolution of connecting LV customers to LV networks and highlights developments that have already been implemented to mitigate non-technical losses, subsequently highlighting the existing gap that still allows electricity theft. The chapter analyses the current flow within an LV network, yielding observations and conclusions that inform the subsequent development of a smart LV network. It also delineates the smart grid multilayer architecture and the IoT architecture, which establish the theoretical foundations for the developed concept. The chapter introduces the proposed concept—the smart LV network—through the lenses of both the smart grid and IoT architectures. It details the requisite modifications to existing LV networks and presents a step-by-step design to realise a complete smart LV network.

Chapter Four presents a laboratory-scale prototype design and the simulation of the smart LV network for experimentation, with the aim of validating whether the hypothesised and proposed solution functions as intended and yields the expected results.

4. CHAPTER 4
SMART LV NETWORK PROTOTYPE AND SIMULATION DESIGNS FOR EXPERIMENTATION

4.1 Introduction

As global demand for power continues to rise, it is imperative to develop more intelligent methods for the production, storage, and distribution of electricity. At present, government strategies are best served by adopting smart grids in place of conventional electrical grids. Beyond their traditional roles, smart grids offer the capability to deliver electricity to consumers via digital communication networks, enabling continuous monitoring and analysis of the electrical supply. Realizing these advantages requires leveraging the Internet of Things (IoT) capabilities inherent to smart grids (Shahinzadeh et al., 2019).

This chapter details the design of a smart LV network prototype and provides a Proteus-based simulation to test and validate the hypothesis articulated in Chapter 1: that advances in smart grid technology can be exploited to construct smart LV networks capable of automatically detecting illegal connections and selectively interrupting supply to suppress unauthorized electricity usage. The chapter is organized to present the methodological framework underpinning the study. Section 4.2 delineates the prototype design, detailing its core components, architecture, and implementation considerations. Section 4.3 outlines the simulation design, including the modelling approach and parameter choices. Section 4.4 provides the concluding remarks of the chapter.

4.2 Prototype design

In Chapter 3, Section 3.5 introduced an LV network containing 5 customers and an illicit connection connected in a dual face transformer, as depicted in Figure 3.9. This network is subsequently simulated in Figures 3.10 and 3.11 using Proteus software.

In this section, a laboratory-scale prototype that emulates this LV-network model is constructed with the electronic components described in Chapter 3, Section 3.9, to facilitate the development of the required IoT devices. The resulting prototype provides a tangible representation of the smart LV network and enables feasibility testing of the proposed system prior to scaling the design to a real LV network. For the experimental program, both the laboratory-scale prototype and the simulation adopt a consistent network design to simplify the prediction and calculation of expected output voltages and currents.

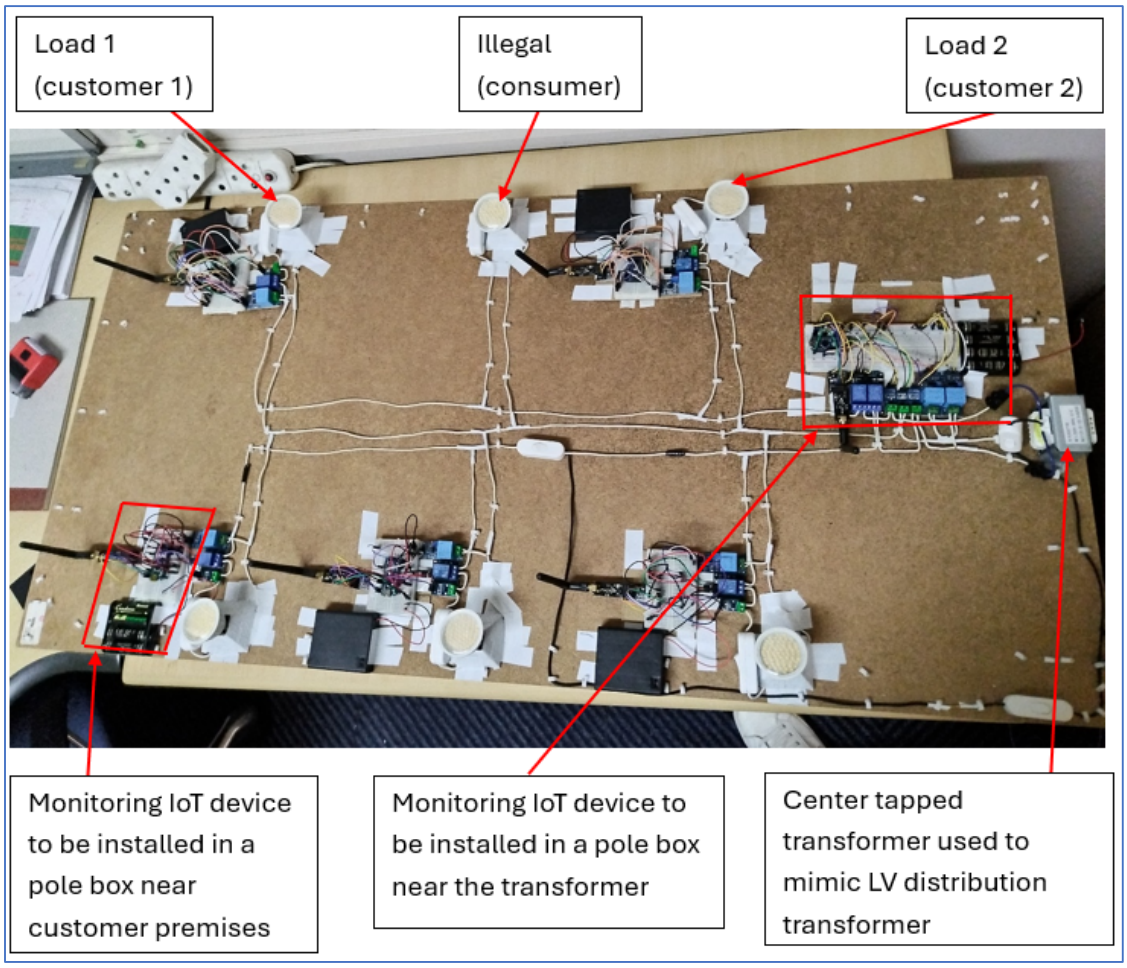

Figure 4.1: Lab scale prototype of the smart LV distribution network

Figure 4.1 presents the laboratory-scale prototype of the smart LV distribution network designed to test the stated hypothesis. The physical setup mirrors the LV distribution topology previously described and simulated in Proteus, comprising six bulbs: five are metered to represent legally connected customers, and one remains unmetered to simulate an illegal connection. All bulbs are identical to ensure uniform current draw under equivalent operating conditions. Five identically configured monitoring IoT devices are positioned proximate to the five legitimately connected bulbs, enabling near real-time measurement of electrical parameters at the customer premises. An additional IoT device is installed adjacent to the transformer to monitor network conditions at the source. Notably, the unmetered bulb lacks an IoT monitor and is equipped only with a switch to simulate disconnection/connection events. The deployed IoT devices facilitate real-time comparison of currents and voltages at the customer premises with those observed at the transformer, enabling the detection of illegal connections and a range of other faults within the LV distribution network.

To represent an LV distribution transformer within the laboratory-scale prototype, a compact single-phase transformer rated at 220 V/24 V is employed. This transformer delivers 12 V

between each active conductor and the center-tapped neutral (0 V). When the voltage is measured between the two active conductors, a total of 24 V is observed, as depicted in Figure 4.2.

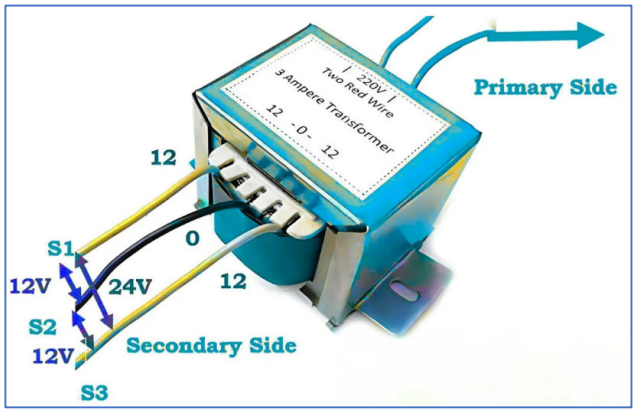

Figure 4.2: Small 220V/24V centre tapped transformer (Rabert, 2024)

The LV transformer depicted in Figure 4.2 may be compact in physical dimensions; however, its design is identical to that of the 22 kV/400 V LV distribution transformer employed in the Proteus simulation environment. Consequently, electrical connections configured in an analogous manner for these two transformers are expected to exhibit equivalent performance in delivering current to the connected loads.

In order to represent the customer's premises on the laboratory-scale prototype, twelve-volt alternating current (12 VAC), 6 W downlight units are employed. These luminaires are specified to operate from a 12 V AC supply, which corresponds to the secondary voltage of the selected single-phase transformer depicted in Figure 4.2. The selection of these downlights is justified by their nominal power rating of 6 W and their operating voltage of 12 V AC. The current drawn from the transformer by each lamp can be determined using Ohm's law,

$$P = VI \tag{4.1}$$

$$I = \frac{P}{V} \tag{4.2}$$

$$I = \frac{6}{12}$$

$$I = 0.5A$$

Where P is the power rating of the down light in Watts (W), V is the Voltage that the downlight will be connected to, and I is the current to be drawn by the downlight from the transformer.

Figure 4.3: 12VAC 6W Downlight (ACDC Dynamics, 2024)

Figure 4.3 illustrates a 12 V AC 6 W downlight configuration employed to model single-phase customers on the laboratory-scale prototype. Each downlight draws 0.5 A, and with six bulbs in total arranged as three bulbs per phase, a single-phase set of three bulbs yields a maximum current of 1.5 A from the transformer. This operating current remains within safe limits for the compact single-phase transformers used in the setup, given that the current rating of the transformer is 2 A.

4.2.1 Measuring of currents on the prototype

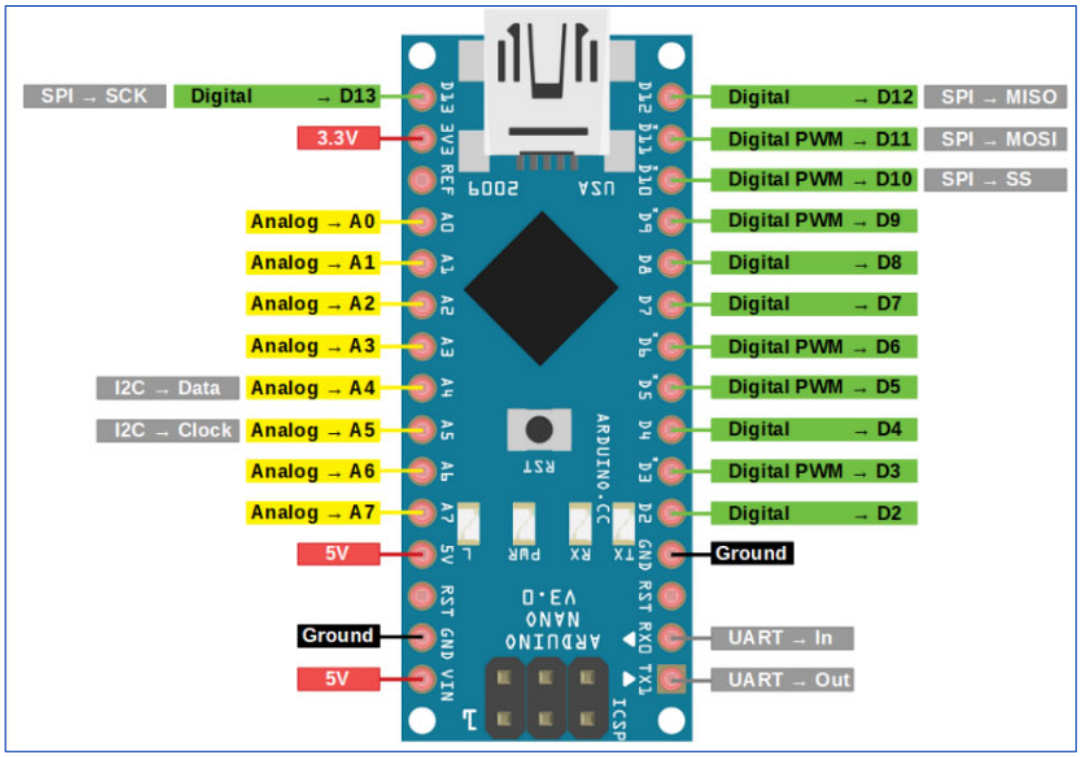

Figure 4.4: Arduino Nano pinout (Dav, 2020)

This study employs an Arduino Nano clone as the microcontroller for a laboratory-scale IoT prototype, with the pin out as indicated in Figure 4.4. The selection is driven by the cost-effectiveness and broad market availability of this device. Notably, these clones remain compatible with the Arduino Integrated Development Environment (IDE), which is used to program all Arduino-compatible microcontrollers. Arduino devices operate by executing a predefined sequence of instructions within a continuous loop; when a program consists of ten instructions, the microcontroller processes these ten instructions in sequence and subsequently restarts the loop, maintaining this cycle until a reset or power interruption occurs.

Among the executable instructions, the microcontroller can read data from its input pins when connected to sensors, and write data to its output pins to control actuators such as relays and LEDs, thereby enabling on/off control. The microcontrollers are capable of performing computations, ranging from simple arithmetic to more complex operations. Programming is conducted using a language that synthesizes elements of C and C++ within the Arduino IDE. The device operates at a clock speed of 16 MHz, translating to an approximate execution rate of 16 million instructions per second under ideal conditions. The nominal operating voltage is 5 V; however, the board can be powered via Vin with an input voltage in the range of 7–12 V. When properly powered, the microcontroller can supply power to low-consumption sensors through its 5 V supply and ground (GND) rails (Dav, 2020).

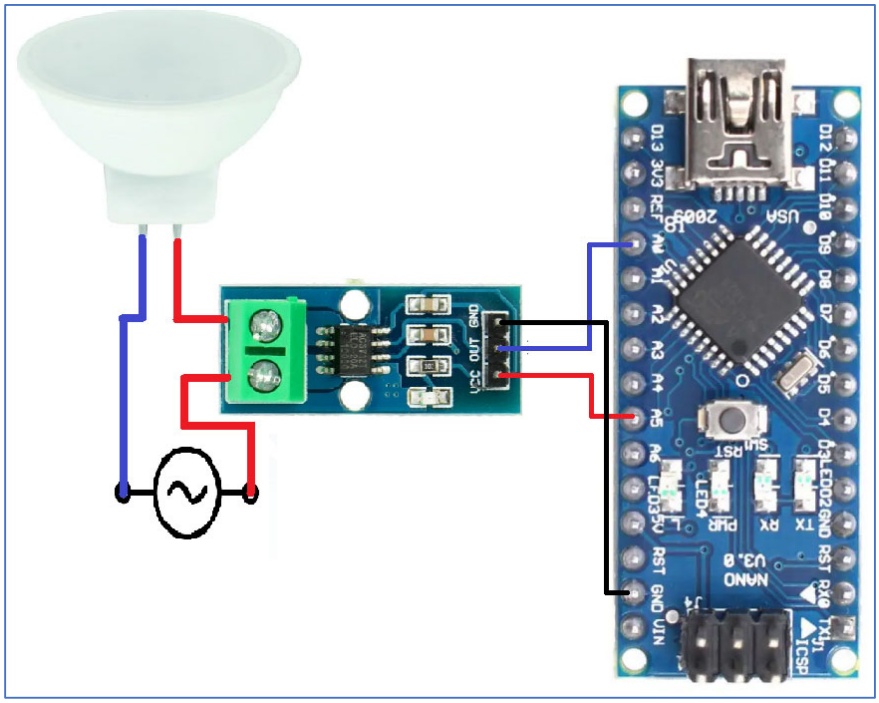

Figure 4.5: Measuring current for the prototype

The prototype employs the ACS712 current sensor, specifically the 5 A variant, for current measurement and connected to the microcontroller as illustrated in Figure 4.5. This selection is justified by the relatively small currents involved, utilizing a larger-current sensor would have introduced accuracy-related challenges. The current sensor is powered from the microcontroller, with VCC and ground connected to the microcontroller's 5V supply and ground, respectively. The sensor's output pin (OUT), which provides the measured signal, is interfaced with the microcontroller's analog input A0. In the experimental setup, the sensor is placed in series with the AC circuit under measurement. Measurement is performed by the microcontroller through repeated sampling of the current flowing in the circuit.

The microcontroller's analog inputs (A0–A7) are connected to a 10-bit analog-to-digital converter (ADC). Any sensor connected to these inputs converts the measured quantity into a small analog voltage proportional to changes in the input, which is then presented to the ADC. The ADC converts this input voltage into a digital value ranging from 0 to 1023. This digital representation is generated by various sensor devices (e.g., humidity, temperature, light, voltage, current, etc.). Although the microcontroller receives these digital values, further processing is often required to render them meaningful in relation to the measured signal. Consequently, a modest amount of mathematical processing is typically applied to interpret the data accurately.

A key consideration is ensuring a stable supply voltage to the ACS712, as fluctuations can directly affect the generated analog signal. The most appropriate approach is to power the microcontroller from a regulated DC source that provides 5 V, or a source capable of maintaining a stable 5 V at the microcontroller's VCC pin. If the supply voltage sags below 5 V, the resultant decrease in the 5 V rail can distort the sensor's output voltage, thereby compromising measurement accuracy (EG Projects, 2023).

When the circuit is powered in order to measure current, and the microcontroller code is executed to initiate AC current measurement on the AC circuit via the ACS712 current sensor, with no current flow on the AC circuit to be measured, the sensor output should indicate 0 A. However, observations of the serial monitor readings reveal fluctuations between 511 and 512, oscillating between these two adjacent values. When a serial plotter is opened within the IDE to visually represent these output values, the resulting plot corresponds to the phenomenon depicted in Figure 4.6.

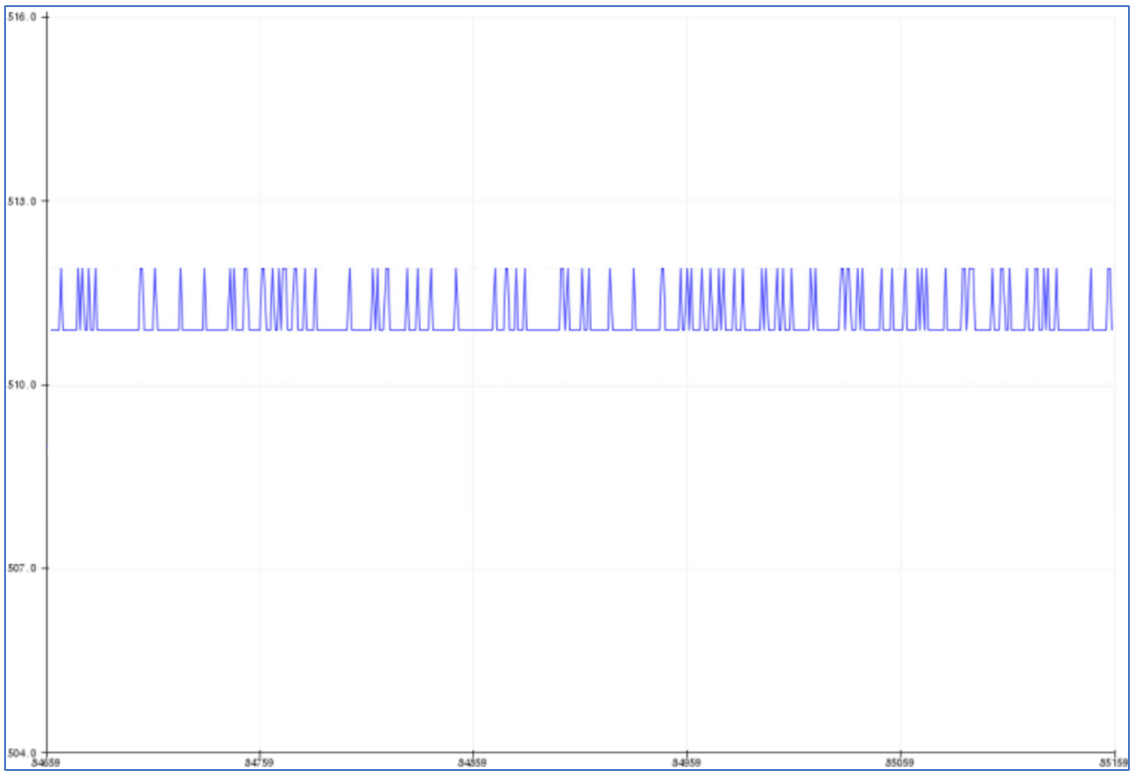

Figure 4.6: Output of the current sensor on the serial plotter measuring 0A

From Figure 4.6, it is observed that the sampled sensor values fluctuate within the narrow range of 511 to 512. These values correspond to the ADC outputs. An ADC reading in the range of 511–512 is interpreted as 0 A of AC current; however, the apparent toggling between these two consecutive codes arises from the sensor's sensitivity. Consequently, the signal does not remain constant at a single code, even though both 511 and 512 accurately reflect zero amperes flowing through the AC circuit. In other words, the two ADC codes represent the same physical quantity (0 A), with the observed alternation attributable to sensor noise and resolution limitations rather than a true variation in current.

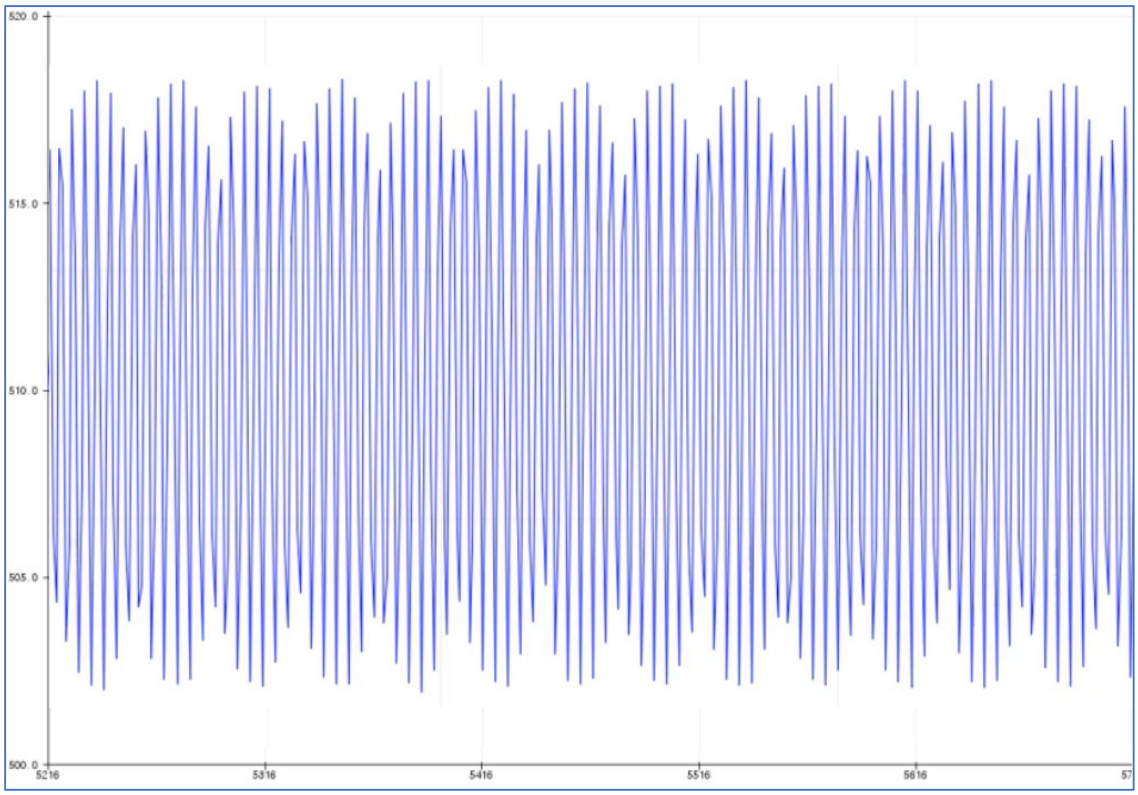

Figure 4.7: **Output of the current sensor on the serial plotter with AC current flow on the AC circuit**

When there is a small AC current flow on the AC circuit, the serial Plotter's waveform transitions to that illustrated in Figure 4.7. Given that the measured current is AC, one would ordinarily expect the plotted signal to conform to an AC waveform. However, the appearance of Figure 4.6 does not resemble the conventional sinusoid, although a close inspection reveals that its average shape approximates a sine wave. This discrepancy arises because the microcontroller samples the AC current at a very high rate. To render the graph as a pure sine wave, the acquisition of the sampled ADC values must be temporally lagged. Introducing a delay of 100 ms in the sampling process yields the sinusoidal waveform depicted in Figure 4.8.

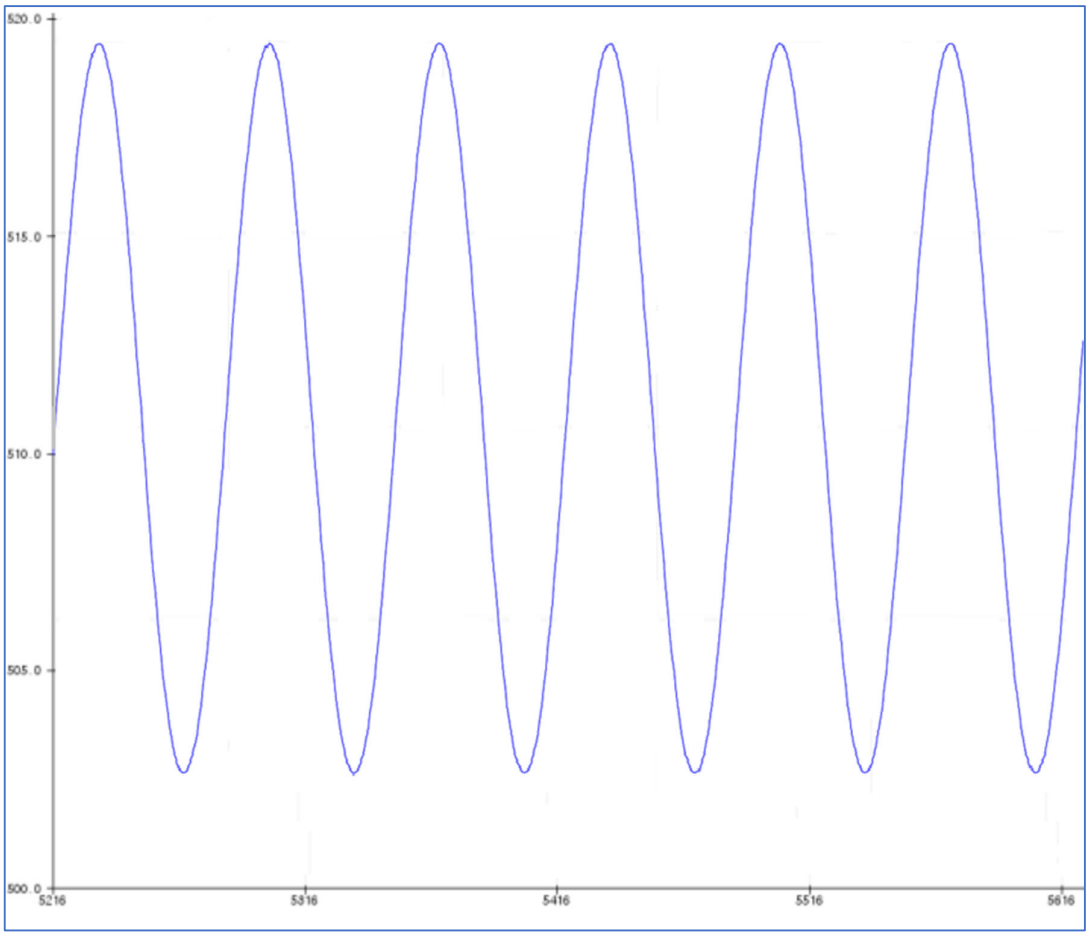

Figure 4.8: **A pure sin wave of the sampled ADC values from the current sensor for the AC current flowing on the AC circuit.**

Figure 4.8 is a complete indication that the current sensor is measuring an AC current from the AC circuit. The subsequent phase involves translating the raw ADC readings into corresponding AC current values that make sense in the context of electric circuits. This translation necessitates a calibration procedure to establish the relationship between the ADC outputs and the actual current.

For calibration, the sensor is connected in series with an AC circuit containing an ammeter to enable current verification. When a nominal current of 5A flowed through the circuit, the recorded digital values exhibited pronounced fluctuations over time, ranging from 0 to 1023 and returning to 0, in a repeating pattern. For the purposes of visualization and to facilitate the conversion from ADC counts to current, a hand drawn sine-wave representation is employed. The sine wave is plotted using the ADC values, which span approximately 0 to 1023, yielding a time–ADC value plot (Figure 4.9). This figure serves as the basis for subsequent calculations to translate ADC measurements into corresponding current values.

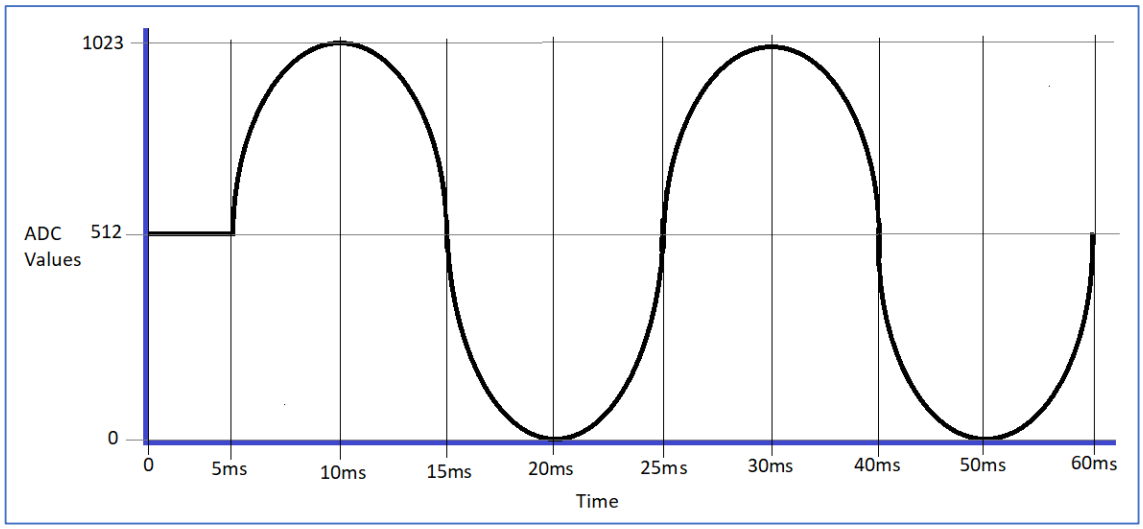

Figure 4.9: A hand-drawn sine wave showing ADC vs time plot

Figure 4.9 depicts the measured ADC values as a function of time. The trace remains constant at 512 for the interval t = 0 to t = 5 ms, corresponding to a period in which there is no current flow in the AC circuit under test. At t = 5 ms, current begins to flow and the ADC values exhibit fluctuations, rising toward the upper limit of 1023 and subsequently returning to 0. It is noteworthy that the complete waveform period observed on the graph is 20 ms. This period reflects the 50 Hz frequency of the measured AC current, a frequency that is preserved in the ADC output values.

$$T = \frac{1}{f} \tag{4.3}$$

$$T = \frac{1}{50}$$

$$T = 20mS$$

In addition, it is important to observe that the digital signal, in the absence of current flow in the AC circuit, is expected to be constant at 511.5, which corresponds to the midpoint between 0 and 1023. However, since the ADC yields only discrete integer values, this midpoint value of 511.5 is rounded to 512. This also explains the toggling between 511 and 512 when there is no current flow.

Figure 4.9 depicts a waveform that resembles the AC current produced by the sensor on the AC circuit. Two notable differences are evident: first, all ADC values are non-negative, so the waveform does not exhibit negative values, thereby failing to convey the bidirectional nature of an AC signal. Second, the digital values range from 0 to 1023 and therefore are not directly interpretable as absolute current values, which may limit their utility for applications such as estimating the current drawn by a kettle. To address these considerations, a hand-drawn

representation of an AC current waveform, as measured by the sensor on the AC circuit, is presented in Figure 4.10.

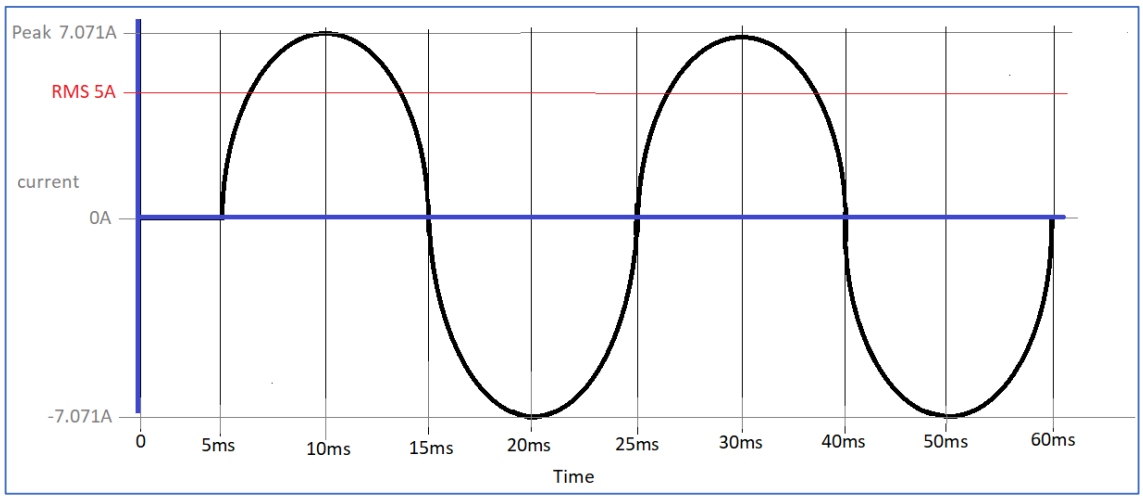

Figure 4.10: **A hand-drawn sine wave showing current vs time plot (Peak to Peak and RMS values)**

From Figure 4.10, the AC circuit current initiates at 0 A for the interval t = 0 to t = 5 ms. Once a 5A current begins to flow, the current waveform develops, commencing at t = 5 ms. The instantaneous current rises to a peak of 7.071A, subsequently decays to 0A, traverses to −7.071 A, and then rises again until the waveform completes, after which it repeats cyclically. The positive and negative portions of the waveform denote both magnitude and direction: positive values indicate current flow from one phase, whereas negative values indicate current flow from the opposing phase in the opposite direction to the initial flow.

Analogous to the ADC value waveform, the period of this current waveform is 20 ms, corresponding to a frequency of 50 Hz. It is worth noting that the current attains a peak of ±7.071 A despite the RMS (root mean square) value of the circuit current being 5 A. This discrepancy arises because the RMS value reflects the effective heating effect (or power-equivalent) of the fluctuatings AC current, whereas the instantaneous peak values reach ±7.071 A. Several methods exist to compute the RMS value from the waveform; one common approach, provided the peak value I_peak is known, is to calculate RMS as I_RMS = I_peak / √2.

$$I_{RMS} = \frac{I_{Peak}}{\sqrt{2}} \qquad (4.4)$$

$$I_{RMS} = \frac{7.071}{\sqrt{2}}$$

$$I_{RMS} = 4.9999 \approx 5A$$

The RMS value of AC is defined as the effective DC value that would produce the same heating effect in a resistor (Electronics Tutorials, 2025). This metric is the quantity displayed by ammeters measuring AC, and it is the sole meaningful parameter for estimating the current drawn by a load such as an electric kettle once it is energized. In essence, RMS current provides a basis for comparing the work performed by an AC current with that of a DC current (Electronics Tutorials, 2025). The current RMS value of 5 A is illustrated in Figure 4.10, where it is indicated by the red line. It is important to note that the objective is to transform the ADC-sampled values on the microcontroller into physically meaningful RMS current values; this constitutes the sole instance in which AC current measurement using the microcontroller and the current sensor would be accomplished.

A comparison of the two waveforms—the ADC values versus time (Figure 4.9) and the current versus time in the AC circuit (Figure 4.10)—reveals a linear relationship between the ADC values and the measured current. Specifically, the peak ADC value is 1023 when the current peak is 7.071, the ADC value is 511.5 (rounded to 512) when the current is zero, and the ADC value is 0 when the current peaks in the negative direction (−7.071). From this description, three coordinates can be plotted to illustrate the linear relationship, as shown in Figure 4.11.

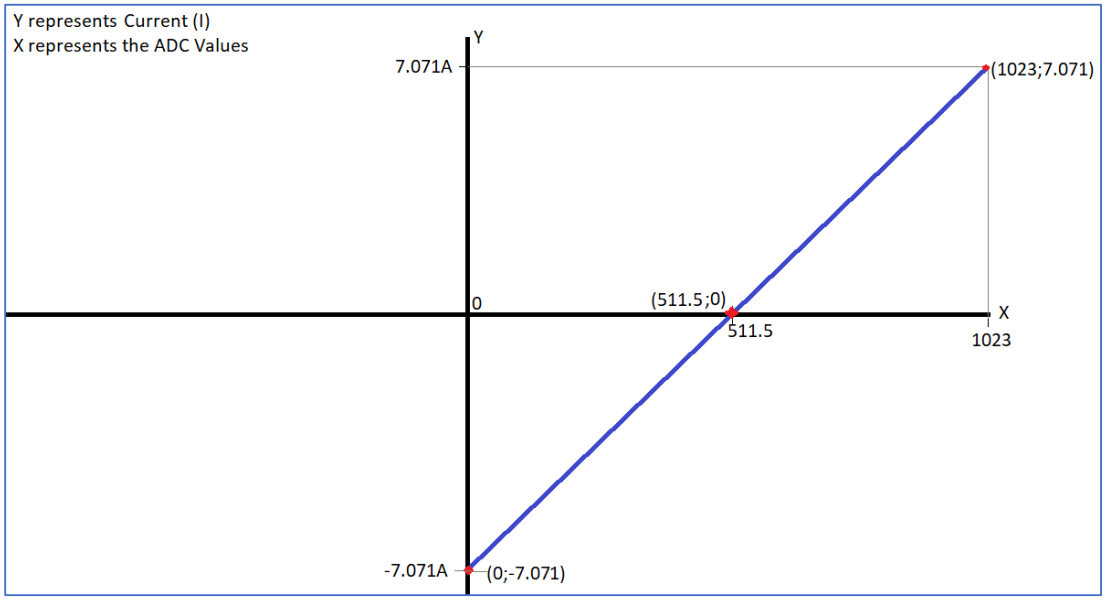

Figure 4.11: **Line graph representing the linear relationship between ADC values and measured AC current**

The linear relationship between measured ADC values and corresponding AC measurements can be expressed by a first-order (linear) equation. Specifically, by applying a straight line, a mathematical linear model can be derived to convert each ADC value into an AC current value. This relationship is described by the equation y = mx + c, wherein y denotes the current values,

m represents the slope (gradient) of the line, x corresponds to the ADC values, and c denotes the y-intercept of the line.

$$y = mx + c \tag{4.5}$$

$$7.071 = m1023 + (-7.071)$$

$$\boldsymbol{m = \frac{14.142}{1023}}$$

Now that the gradient of the slope is found, the full equation is,

$$y = \frac{7.071}{511.5}x - 7.071 \tag{4.6}$$

$$\boldsymbol{I = \frac{7.071}{511.5}ADC - 7.071} \tag{4.7}$$

Where $\boldsymbol{I}$ is the instantaneous current value and $\boldsymbol{ADC}$ is the measured ADC value.

The given equation (4.7) can be used to measusre an instantaneous value of the current equivalent for each ADC value that is sampled by the microcontroller from the current sensor. As an illustrative instance, when the ADC yields a maximum count of 1023, the resulting instantaneous current-equivalent value is computed by substituting this value into the established relationship defined by the equation.

$$I = \frac{7.071}{511.5}ADC - 7.071$$

$$I = \frac{7.071}{511.5}(1023) - 7.071$$

$$\boldsymbol{I = 7.071A}$$

If the measured ADC value is 0, then current is,

$$I = \frac{7.071}{511.5}(0) - 7.071$$

$$\boldsymbol{I = -7.071A}$$

If measured ADC value is 512, keeping in mind that this should be 511.5 but will be converted to 512 by the ADC. Then the current is,

$$I = \frac{7.071}{511.5}(512) - 7.071$$

$$\boldsymbol{I = 0.0069A}$$

As shown, when the ADC reading equals 512, the resulting current value is small but not zero. This nonzero output can be accommodated within the code to be run on the microcontroller. For example, the program can be designed to substitute a value of 511.5 whenever a reading

of 512 is obtained, thereby ensuring that the calculated current converges to zero. If this adjustment is implemented, the subsequent calculation proceeds as follows:

$$I = \frac{7.071}{511.5}(511.5) - 7.071$$

$$\boldsymbol{I = 0A}$$

Lastly, when the microcontroller reads an ADC value of 912, current value is,

$$I = \frac{7.071}{511.5}(912) - 7.071$$

$$\boldsymbol{I = 5.578A}$$

This formula has facilitated the transformation of the ADC values versus time into an equivalent AC current versus time representation. The approach embeds the formula as one of the instructions executed by the microcontroller. The sequence begins with reading the sampled ADC value from the sensor, after which the value is substituted into the formula to compute the corresponding current value. At present, this process yields instantaneous current values, effectively providing samples of the alternating current waveform within the circuit; RMS current values have not yet been computed. To determine the RMS value of the current, the procedure will employ the sampled current values as illustrated in Figure 4.12 below.

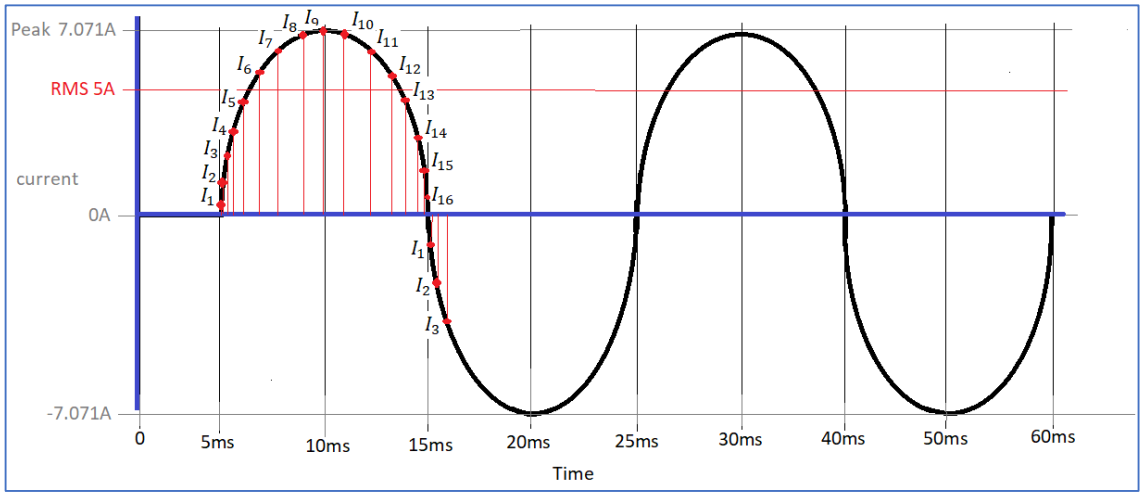

Figure 4.12: **Instantaneous values on the AC current wave**

The RMS value is defined as the square root of the mean of the squares of instantaneous values over a specified period. RMS analysis is not typically employed in DC circuit analysis or in computations where the waveform magnitude remains constant; rather, it characterizes time-varying waveforms—such as sinusoidal currents and voltages—or more complex waveforms in which amplitude changes with time. By sampling equally spaced instantaneous values along the waveform, one can obtain an accurate estimate of the waveform's effective

RMS value. As illustrated in Figure 4.12, the positive half-cycle of the waveform is partitioned into an arbitrary number of n equal segments, and the same partitioning is applied to the negative half-cycle. Increasing the number of instantaneous samples generally improves the accuracy of the RMS calculation, provided that the samples are taken at equal intervals (Electronics Tutorials, 2025).

In this method, each instantaneous point of the current waveform is first squared, meaning it is multiplied by itself, before being summed with the following values. This process corresponds to the "square" component of the RMS current formula. Next, to find the "mean" part of the RMS current, the total squared sum is divided by the count of these instantaneous measurements. Finally, the "root" element is determined by extracting the square root of this mean value. Consequently, the term RMS current (I_RMS) is defined as the square root of the average of the squares of the instantaneous current values, which can be expressed as follows (Electronics Tutorials, 2025):

$$I_{RMS} = \sqrt{\frac{Sum\ of\ the\ sampled\ values(currents)^2}{number\ of\ sampled\ values}} \quad (4.8)$$

$$I_{RMS} = \sqrt{\frac{I_1^2 + I_2^2 + I_3^2 + I_n^2}{n}} \quad (4.9)$$

The RMS formula for I_RMS will facilitate the final stage of AC current measurement using the current sensor in conjunction with a microcontroller, specifically the computation of the current's RMS value. It should be noted that the accuracy of the RMS result improves with the number of instantaneous samples acquired along the waveform; in other words, a higher sampling density yields a more precise estimation of I_RMS. The favourable attribute of this approach is that a microcontroller operates with considerable speed, enabling the acquisition of more than 4,000 sample values within the 20ms period that corresponds to one full cycle of the current waveform. The subsequent sections outline the procedural steps followed by the microcontroller to measure the AC current through the sensor and process the data.

Step 1: Microcontroller takes 1000 ADC sample values at an interval of 0.1ms. This will ensure that the microcontroller samples 200 points per circle and will cover 5 circles for each RMS calculation for a stable reading.

Step 2: Change the ADC values to the instantaneous current values using formula:

$$I = \frac{7.071}{511.5} ADC - 7.071$$

Step 3: Calculate RMS value from the instantaneous values using formula:

$$I_{RMS} = \sqrt{\frac{I_1^2 + I_2^2 + I_3^2 + I_n^2}{n}}$$

Step 4: Process the current and repeat the process.

4.2.2 Measuring of voltages on the prototype

In this prototype, voltage measurement is conducted using a ZMPT101B voltage sensor. This sensor is capable of detecting voltages in the range of 0 V to 250 V AC (Mohammadreza Akbari, 2020). It is suitable for monitoring mains electricity within a domestic environment, where the standard in South Africa is approximately 230 V AC. For the purposes of the prototype, the sensor is also applicable to measurements on the secondary side of the employed single-phase transformer, providing readings of +12 V AC (phase to neutral) and +24 V AC (phase to phase).

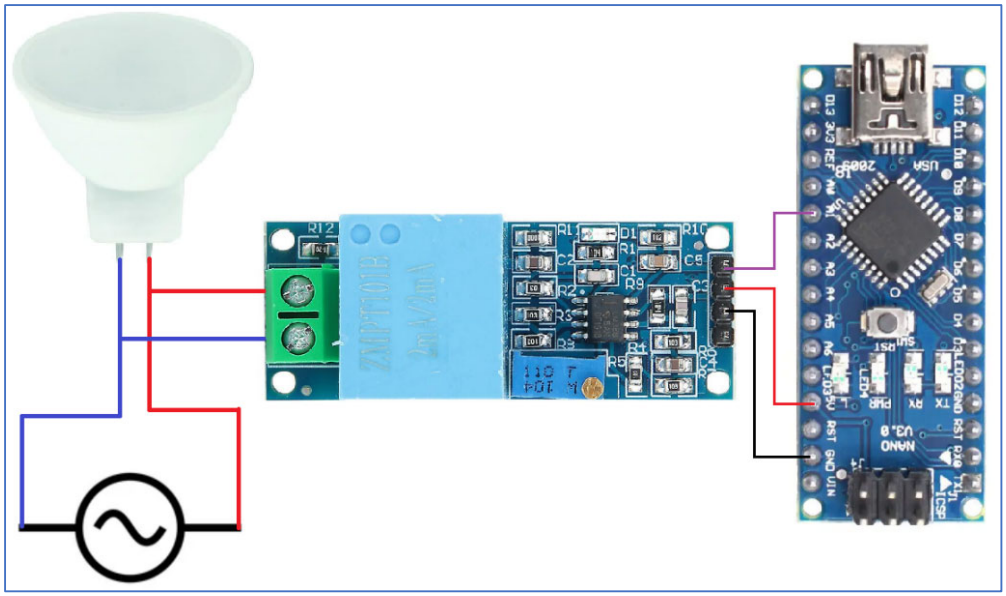

Figure 4.13: Measuring voltage for the prototype

Figure 4.13 illustrates the connection of the voltage sensor to the microcontroller. The VCC pin of the voltage sensor is connected to the 5 V supply of the microcontroller, while the sensor's GND is tied to the microcontroller's ground, and the sensor's OUT output is connected to analog input A1 on the microcontroller. As with the current sensor, the analog output of the voltage sensor is a function of the sensor's supply voltage (VCC); therefore, it is essential to power the sensor from a stable DC source. For the present prototype, the microcontroller is supplied by a 6 V DC source to ensure a regulated 5 V on its 5 V rail. Voltage measurement using the voltage sensor parallels current measurement with the ACS712 sensor that has been previously described. The main distinction is that the ZMPT101B voltage sensor includes a

calibration potentiometer, whereas the ACS712 sensor is factory-calibrated and does not require user adjustment.

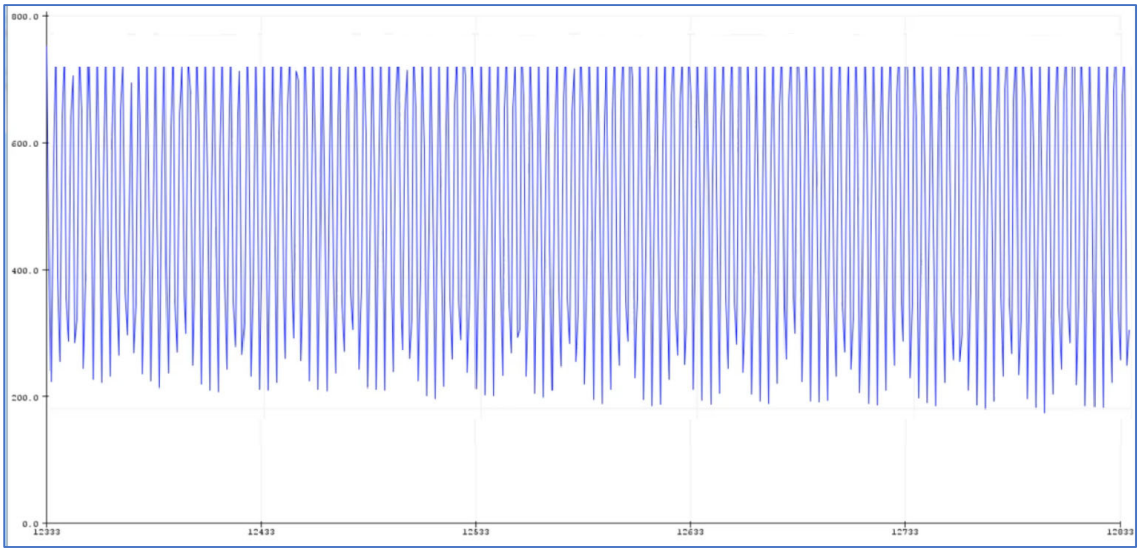

Figure 4.14: **Output of the Voltage sensor from the serial plotter before calibration**

As part of the calibration procedure, the voltage sensor is connected to the 230V AC mains, with a voltmeter connected in parallel to validate the measured voltage. A simple program is executed on the microcontroller to read the analog input from pin A1 and to plot the resulting values via the serial plotter. With the AC voltage supplied to the circuit, and once the program is running, the serial plotter displays the waveform shown in Figure 4.14. The observed waveform exhibits two issues:

1. Distortion in the upper portion of the waveform, and
2. An overall shape that does not resemble a conventional AC (sinusoidal) waveform.

To address the distortion, the calibration potentiometer depicted in Figure 4.15 is employed.

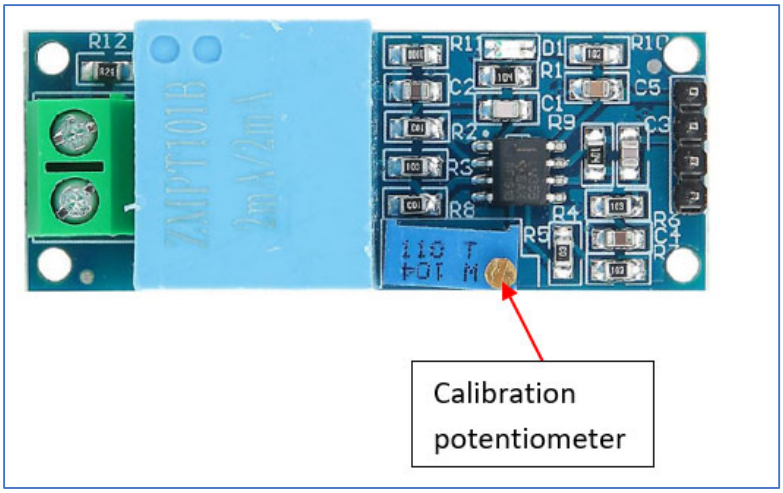

Figure 4.15: ZMPT101B calibration potentiometer
(Mohammadreza Akbari, 2020)

The ZMPT101B voltage sensor is designed to measure voltages across a wide range, from 0 V to 250 V, a specification that has meaningful implications for measurement accuracy. A calibration approach optimized for high-voltage operation may yield diminished precision at lower voltages, while calibration tailored to low voltages can introduce errors when measuring higher voltages. The included calibration potentiometer provides a means to adjust the sensor's response to a chosen range, which is especially important in metering applications where extreme accuracy is required (Akbari, 2020).

By comparison, the ACS712 current sensor employs distinct variants tailored to specific current ranges. For example, a 5 A sensor is not intended to measure 100A within its rated accuracy, whereas a higher-range sensor can handle larger currents but may exhibit reduced accuracy at lower current levels. In this context, the voltage sensor's calibration potentiometer functions as a focus control, enabling the sensor to concentrate on a particular voltage range with minimal degradation in accuracy across that range (Akbari, 2020).

To correct the distortion observed in the waveform shown in Figure 4.14, the calibration knob is adjusted until the complete waveform appeared as illustrated in Figure 4.16. This condition confirms that the measured voltage is captured without distortion and with accurate amplitude.

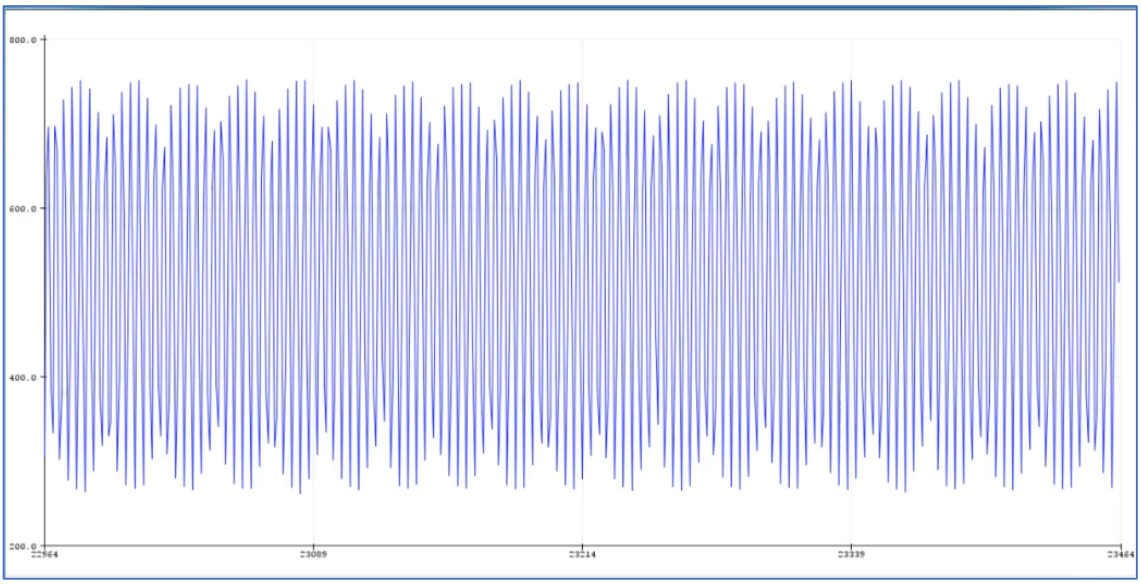

Figure 4.16: Output of the voltage sensor on the serial plotter

Figure 4.16 shows a waveform captured without distortion; however, it does not resemble an ideal sine wave. This discrepancy arises because the microcontroller samples and plots the signal at a high rate, which can cause the displayed trace to depart from a perfect sinusoid even though the underlying signal is sinusoidal. A closer inspection reveals that the waveform does, in fact, follow a sine-wave pattern. To obtain a pure sine wave, the ADC sampling must be delayed a little. Introducing a 100 ms delay in the sampling yields the sine wave depicted in Figure 4.17.

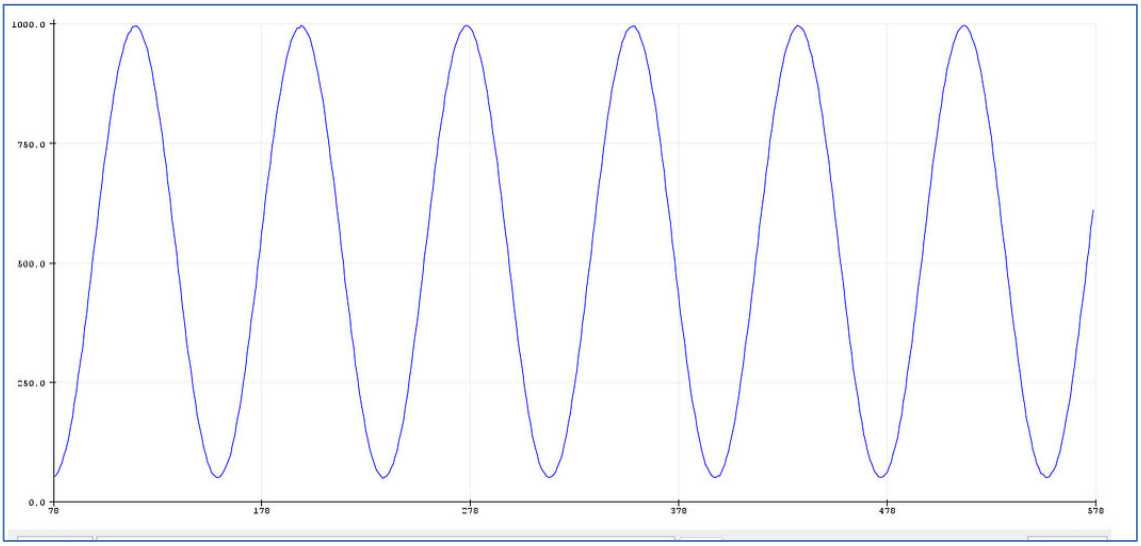

Figure 4.17: A pure sin wave of the sampled ADC values from the voltage sensor for the AC voltage on the AC circuit.

Adjusting the calibration knob alters the observed waveform by flattening its peaks, troughs, or both. This flattening indicates that the waveform is not fully captured by the measurement apparatus, which in turn leads to distortions in the subsequent calculation of the RMS voltage. Consequently, RMS estimates may be biased or inaccurate, depending on the degree of flattening and the underlying waveform shape.

The second step in the calibration process involves deriving the mathematical formula used to convert ADC readings into instantaneous voltage samples. In the absence of voltage on the AC circuit, the microcontroller reads a constant ADC value of 512, which corresponds to mid-scale on a 10-bit ADC (range 0–1023). When a 230 V AC input is applied, the ADC values rise to 982, drop to 41, and then rise again to 982, repeating with the AC cycle. This occurs because the voltage sensor's maximum rating is 250V, exceeding the household mains voltage of 230V. The 250V RMS corresponds to a peak voltage of,

$$V_{peak} = 250\sqrt{2} \quad (4.10)$$
$$\boldsymbol{V_{peak} = 353.55V}$$

The peak of 353.55 means that the voltage sensor reaches 1023 when the voltage peaks at 353.55 and falls to 0 when the voltage peaks at -353.55. The AC mains inside the house peak at,

$$V_{peak} = 230\sqrt{2}$$
$$\boldsymbol{V_{peak} = 325.27V}$$

Similar to measuring the current using the current sensor module, there is a linear relationship between the ADC values and the measured voltage on the AC circuit. Using this relationship, a straight line can be drawn as shown in Figure 4.18.

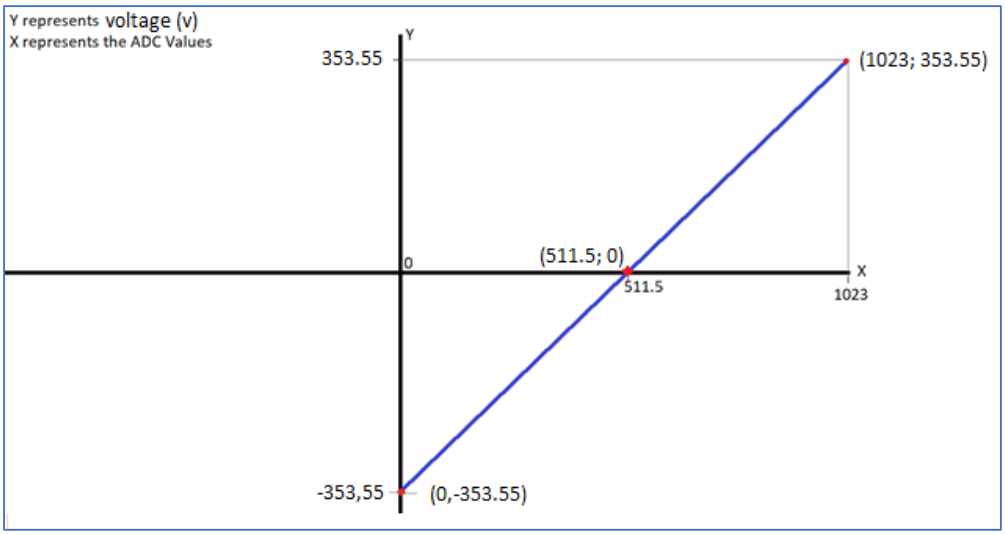

Figure 4.18 Linear relationship between ADC values and the measured AC voltage on the AC circuit

Using the linear equation (4.5),

$$y = mx + c$$

$$353.55 = m1023 + (-353.55)$$

$$\boldsymbol{m = \frac{707.1}{1023}}$$

Substituting the gradient and the y intercept to the equation,

$$y = \frac{353.55}{511.5}x - 353.55$$

$$\boldsymbol{V = \frac{353.55}{511.5}ADC - 353.55} \qquad \textbf{(4.11)}$$

Where $\boldsymbol{V}$ is the instantaneous voltage value and $\boldsymbol{ADC}$ is the sampled ADC value.

The given equation (4.11) can be used to convert the ADC values to instantaneous voltage values. For an example, if the microcontroller reads an ADC value of 982, the instantaneous voltage is,

$$V = \frac{353.55}{511.5}(982) - 353.55$$

$$\boldsymbol{V = 325.21V}$$

When the microcontroller reads an ADC value of 41, the instantaneous voltage is,

$$V = \frac{353.55}{511.5}(41) - 353.55$$

$$\boldsymbol{V = -325.21V}$$

The final phase in determining voltage using a voltage sensor involves computing the RMS voltage based on the instantaneous voltage readings. This process mirrors the previously explained method for deriving RMS from instantaneous measurements. The calculation can be performed using the formula below,

$$V_{RMS} = \sqrt{\frac{V_1^2 + V_2^2 + V_3^2 + V_n^2}{n}} \quad (4.12)$$

The following steps are followed by the microcontroller to measure the voltage using the voltage sensor:

Step 1: Microcontroller takes 1000 ADC sample values at an interval of 0.1ms.

Step 2: Change the ADC values to the instantaneous current values using formula:

$$\boldsymbol{V = \frac{353.55}{511.5} ADC - 353.55}$$

Step 3: Calculate RMS value from the instantaneous values using formula:

$$V_{RMS} = \sqrt{\frac{V_1^2 + V_2^2 + V_3^2 + V_n^2}{n}}$$

Step 4: Process the voltages and repeat the process.

4.2.3 Relay module and a microcontroller

Upon successful measurement and digitization of the instantaneous current and voltage within the microcontroller, subsequent signal processing is performed to extract pertinent electrical information. In the proposed model, beginning with pole-mounted enclosures installed near the customer premises, the remaining task is to verify that the measured signals remain within predefined operating limits, i.e., to detect overcurrent and overvoltage conditions. If either condition is detected, the relay module is actuated to isolate the premises from the electrical supply, thereby providing protection against abnormal electrical events.

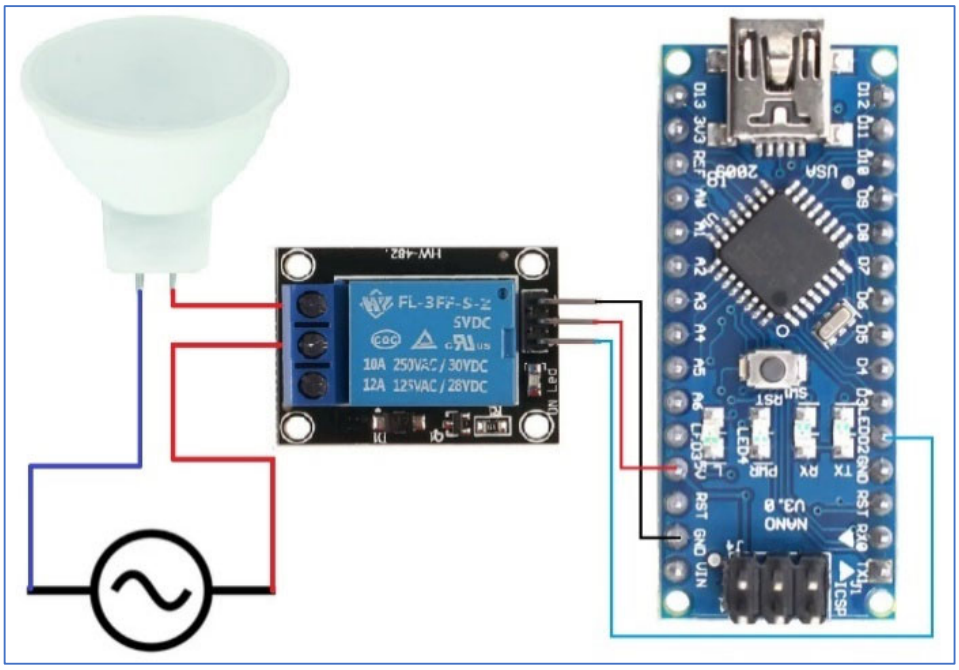

Figure 4.19: **Microcontroller and a relay module to control the AC load**

Figure 4.19 depicts the interconnection between the relay module and the microcontroller. The relay module's VCC and GND pins are connected respectively to the microcontroller's 5 V supply and ground to power the relay coil. The relay's input (IN) is driven by digital pin D2 of the microcontroller. The microcontroller's digital outputs can be set to HIGH (5 V) or LOW (0 V / ground); a HIGH signal energises the relay coil, causing the contacts to close, while a LOW signal de-energises the coil and opens the contacts. On the relay's switched side there are three terminals: COM, NO (normally open), and NC (normally closed). The relay operates as a switch that connects COM to either NO or NC depending on the coil state (Tarantula, 2025).

In this configuration, NO and COM are used to control the AC circuit. When the coil is de-energised, the COM-NO path remains open, and the AC circuit is OFF. Energising the coil (digital HIGH) closes the COM-NO contact, thereby completing the AC circuit. Conversely, if the COM-NC path is used, energising the coil would interrupt the circuit. After measuring the voltage and current in the AC circuit and verifying that they meet the specified limits, any abnormal conditions would prompt changing the relay state from HIGH to LOW to interrupt the AC circuit.

4.2.4 NRF24L01 Radio module and a microcontroller

Further processing of the current and voltage signals, which are measured and stored within the microcontroller, is not limited to determining whether these signals are abnormal. These measurements, together with the relay status, must be radio-transmitted to a separate IoT device located approximately one kilometre away from the sensing site. This requirement is

addressed by employing the NRF24L01 radio module, which provides wireless communication capabilities suitable for medium-range data transmission in IoT deployments.

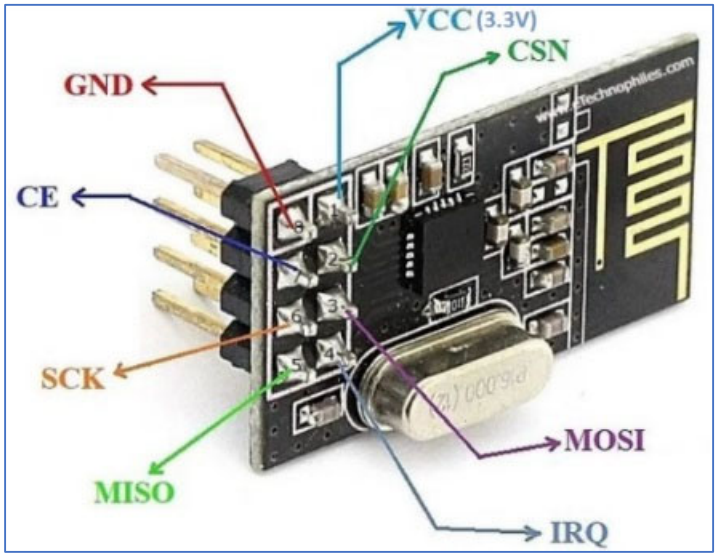

Figure 4.20: NRF24L01 radio module pinout
(Negi, 2024)

Figure 4.20 depicts the pinout of the NRF24L01 module, which requires a 3.3 V DC supply at VCC. Although direct connection to an Arduino is feasible, using an NRF24L01 adapter is preferable for simplifying wiring. The radio transceiver is susceptible to noise, and effective noise mitigation often relies on external circuitry, including a filtering capacitor (Negi, 2024). Utilizing the adapter eliminates the need for this external filtering network, as it incorporates integrated noise-filtering circuitry. Moreover, the adapter includes a voltage regulator that permits operation from input voltages ranging from 5V to 12V, ensuring the module consistently receives the requisite 3.3 V (Last Minute Engineers, 2023).

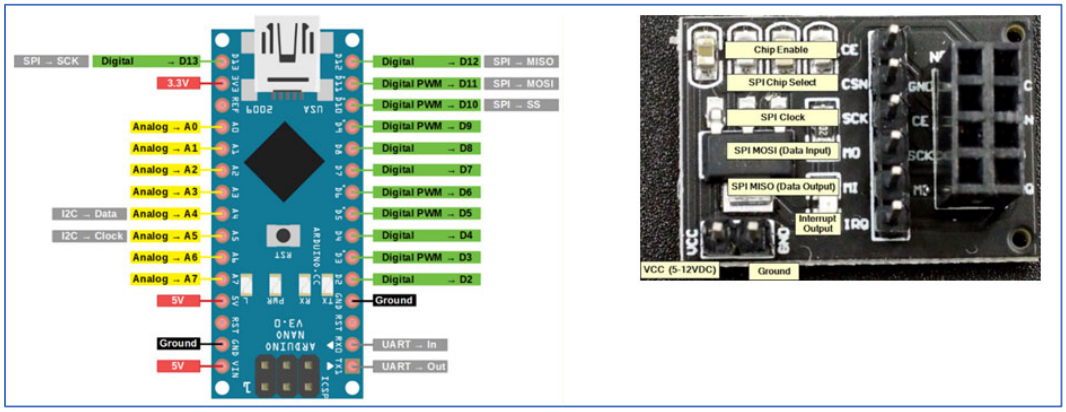

Figure 4.21: Pinout of the Arduino Nano and Pinout of the NRF24L01 radio module adapter side by side (adapted from: Dav, 2020)

Figure 4.21 depicts the pinout of the Arduino Nano alongside the pinout of the NRF24L01 radio module adapter. The adapter is powered from the 5 V supply and the ground (GND) of the microcontroller. The Chip Enable (CE) input of the adapter is connected to digital pin D9 on the microcontroller. The SPI Chip Select (CSN) input is connected to digital pin D10 (SPI Slave Select, SS) of the microcontroller. The SPI Clock (SCK) input is connected to digital pin D13 (SPI SCK) of the microcontroller. The SPI Master Out Slave In (MOSI) input is connected to digital pin D11 (SPI MOSI) of the microcontroller; and the SPI Master In Slave Out (MISO) output is connected to digital pin D12 (SPI MISO) (Last Minute Engineers, 2023).

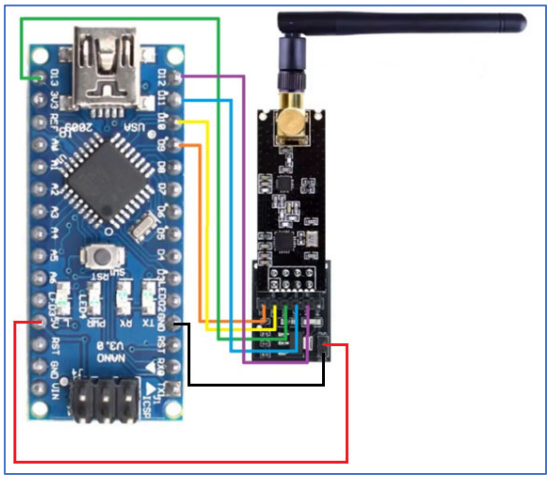

Figure 4.22: **Connection of the NRF24L01 radio module to the microcontroller**

Figure 4.22 illustrates the connection of the radio module and the microcontroller. The microcontroller must transfer the measured current, voltage, and relay status to the NRF24L01 radio module to enable wireless transmission. This data exchange is accomplished via the Serial Peripheral Interface (SPI), a four-wire, synchronous serial communication protocol commonly employed for short-range communication between a master device (controller) and one or more peripheral (slave) devices in embedded systems. SPI is widely adopted due to its simplicity and high data transfer rates. The protocol operates within a master/slave architecture, whereby the master initiates communication and governs the clock, while the slaves respond to the master's commands (Grusin, 2025).

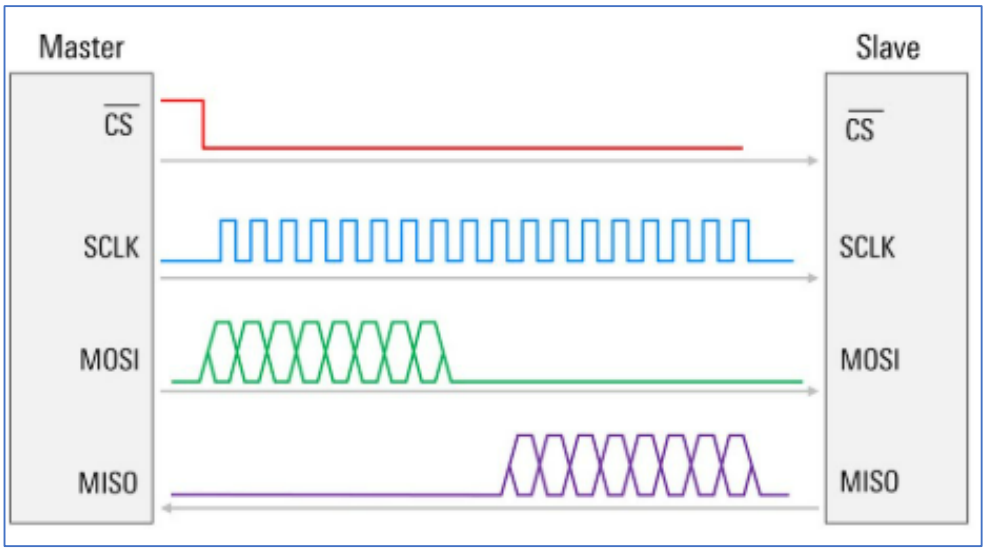

Figure 4.23: **Illustration of an SPI protocol for data exchange between a controller and a peripheral (Grusin, 2025)**

Figure 4.23 illustrates an SPI protocol configuration for data exchange between a controller and a peripheral. The four wires comprise: CS, SCLK (serial clock), MOSI, and MISO. The CS line is held high during idle periods and is pulled low to initiate a transfer, signalling the selected peripheral that data transmission will commence. The controller then provides a clock signal on SCLK to synchronize communication. Data is transmitted from the controller to the peripheral via MOSI, while any data sent from the peripheral to the controller returns on MISO. When the transfer concludes, CS is returned to its high state (Grusin, 2025).

Figure 4.22 shows the connection between the NRF24L01 radio module and the microcontroller, which includes a fifth line, CE (chip enable). The CE line controls the radio module to facilitate power saving (sleep mode) and to switch the module between transmit and receive modes during wireless communication. In the described system, the microcontroller measures current with a current sensor and voltage with a voltage sensor, verifies that these measurements remain within allowable ranges, and uses a relay module to switch an AC circuit under abnormal conditions. After acquiring the measurements and relay status, the controller initiates communication with the radio module to transmit the current value, the voltage value, and the relay status to the radio mesh network, where the data is relayed to the master IoT device. The detailed explanation of how the radio module works and manages data transfer (data packages) is presented on appendix A4.1.

4.2.5 Microcontroller and a GSM Module

Currents and voltages are measured by the microcontrollers integrated in each IoT device. The measured data is subsequently transmitted via a radio mesh communication network to the master IoT device, which is located approximately one kilometre from the peripheral

devices. The master IoT device aggregates the voltages, currents, and relay-status values from all pole boxes and performs further processing, including fault scanning in the low-voltage (LV) network and assessment of illegal connections. When abnormal conditions are detected, the relay is employed to isolate the affected sections of the network. Following these procedures, the status information for the entire LV network is transmitted to a central location where utility personnel can monitor the system and issue control commands back to the network. In this communication chain, the GSM module provides the link to the central facility.

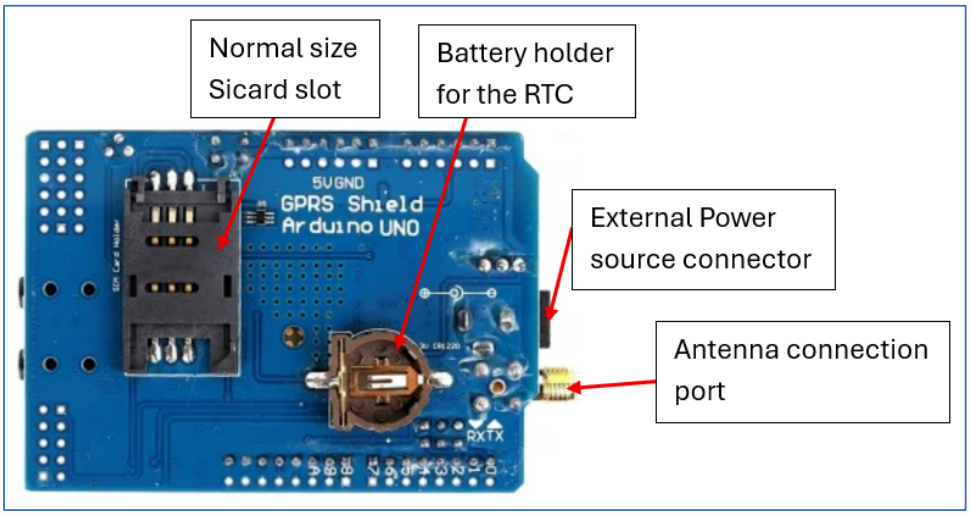

Figure 4.24: Sim900 GSM shield
(Alam, 2022)

An overview of the SIM900 GSM/GPRS shield used in the prototype is provided with reference to Figure 4.24. The module functions as a gateway, linking the low-voltage sensor network to the Internet to enable data loading to the cloud for aggregation, visualization, monitoring, and control. The GSM module includes a standard SIM card slot, a real-time clock (RTC) battery slot, an external power-source connector, and an antenna connection. The SIM card enables cellular connectivity and Internet access. In the present implementation, the ThingSpeak server is used to transmit data through the GSM module. The RTC and its battery allow the module to maintain accurate timekeeping even during power outages, which is advantageous for data collection and transfer because timestamps are essential for interpreting data upon receipt (Alam, 2022).

Operational and power considerations are critical for reliable performance. The GSM module can operate on voltages as low as 5V but may draw up to 2A during active communication. Consequently, powering the GSM module solely from a microcontroller is inappropriate, as a microcontroller can supply 5V but cannot source 2A from its pins. Insufficient power frequently causes the GSM module to reset during communication. To ensure stable operation, the shield

provides a power jack capable of accepting a 5–9 V DC supply. A power source capable of delivering at least 2A should be connected to this external jack to provide the GSM module with adequate power.

Antenna selection and enclosure considerations are also addressed. The antenna is a critical component for establishing cellular connectivity; without it, the GSM module cannot connect to the cellular network. Antenna size and placement depend on the strength of the local cellular signal and whether the module is housed within a metallic or plastic enclosure. For metallic enclosures, it is advisable to position the antenna outside the enclosure to avoid attenuation or shielding of the signal (Alam, 2022).

The communication between the GSM module and the microcontroller is achieved via the UART (universal asynchronous receiver/transmitter) serial protocol, which enables bidirectional data exchange using a two-wire connection in addition to a shared ground reference. UART defines the protocol and electrical interface for serial communication between devices, allowing the microcontroller to transmit data to the GSM module and receive responses. The presence of a ground connection on both ends is illustrated in Figure 4.25 (Peña and Legaspi, 2020).

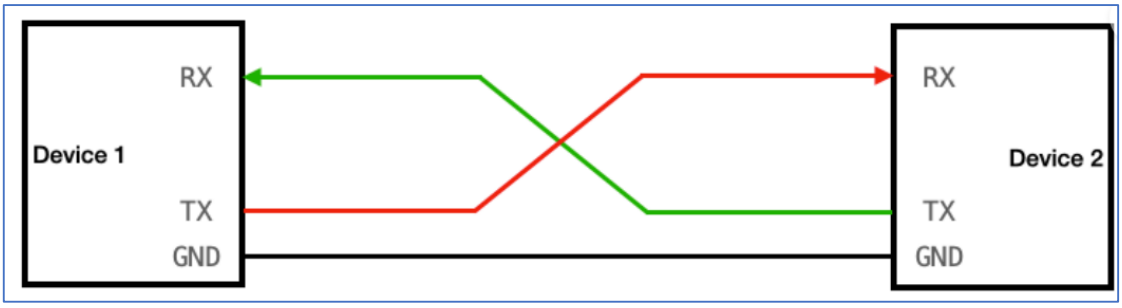

Figure 4.25: **Connection between two devices for UART communication (Peña and Legaspi, 2020)**

UART interfaces use two data lines: a receive (RX) pin and a transmit (TX) pin on each device. The RX pin of one device is connected to the TX pin of the other, enabling bidirectional communication where the transmitting device's data is received by the other. UART supports three communication modes: simplex (unidirectional data flow), half-duplex (transmission in one direction at a time), and full duplex (simultaneous transmission and reception). A key advantage of UART is its asynchronous operation, meaning there is no shared clock between transmitter and receiver. This independence, however, imposes the need for strict coordination: both ends must operate at the same bit timing by agreeing on the baud rate and frame structure, since no clock is shared. Commonly used baud rates include 4800, 9600,

19200, 57600, and 115200 bps; in addition to matching baud rates, both sides must agree on the frame structure and other parameters (Peña and Legaspi, 2020).

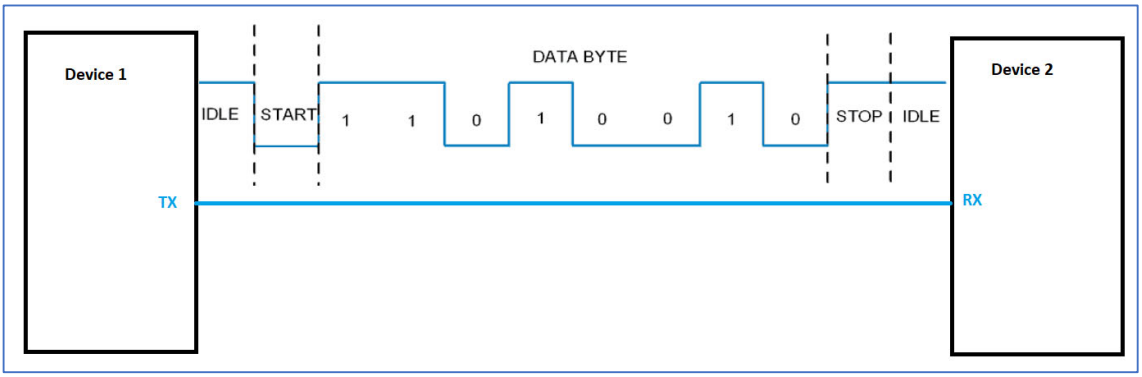

Figure 4.26: Frame structure of UART protocol
(Peña and Legaspi, 2020)

Figure 4.26 depicts the frame structure of the UART protocol. In line with common digital logic conventions, a logical '1' is represented by a high voltage level, while a logical '0' is represented by a low voltage level. The line remains in a high (idle) state when the system is not transmitting, a convention that facilitates fault detection in the event of a damaged transmitter or interconnection. Because UART operates asynchronously, a start bit signals the beginning of data transmission by transitioning the line from idle high to a low level, as illustrated in Figure 4.26. The user data bits follow the start bit, and the stop bit marks the end of the data field. The stop bit maintains the line in the high state for at least one bit duration, though it may also transition back to the high or idle state. In some implementations, an optional second stop bit may be used to provide the receiver with additional time to prepare for the subsequent frame (Peña and Legaspi, 2020).

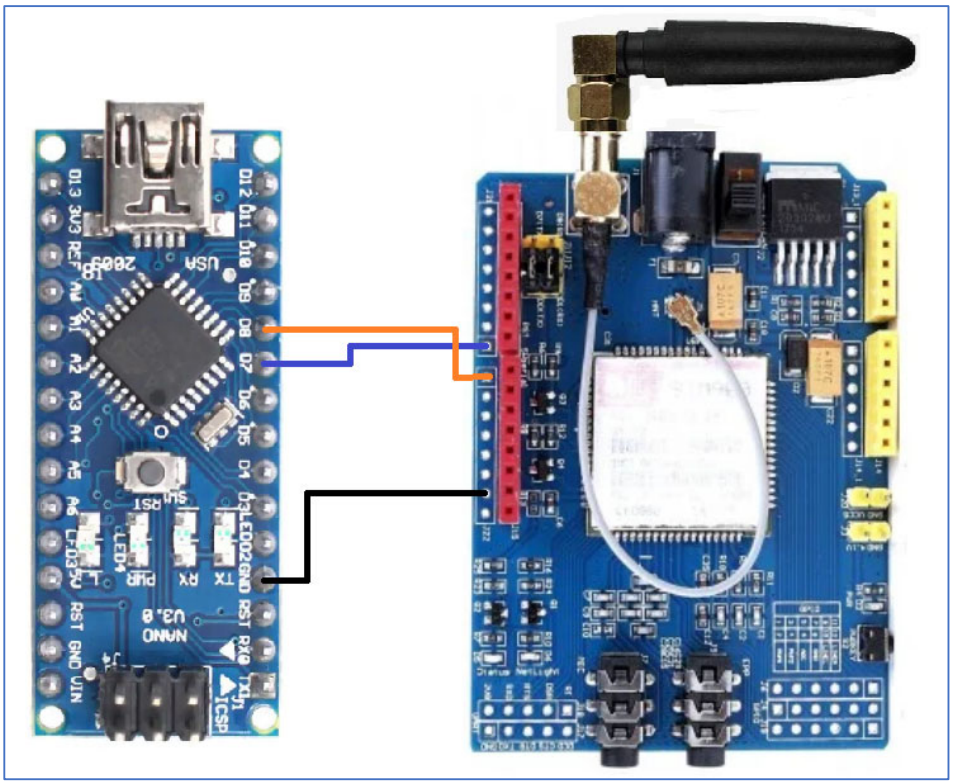

Figure 4.27: Connection of GSM module with the microcontroller

Figure 4.27 presents the wiring scheme for interfacing the GSM module with the microcontroller. The GSM module is powered from an external supply, and, as in Figure 4.26, the interconnection consists of three conductors: the common ground (GND) shared by both devices, and two data lines for UART communication (RX and TX). In the illustrated arrangement, the RX line of the GSM module is connected to the TX line of the microcontroller, and the TX line of the GSM module is connected to the RX line of the microcontroller. To implement this interface without using the microcontroller's native RX and TX pins, the connections are arranged such that microcontroller pin 7 is linked to GSM module pin 7 and microcontroller pin 8 to GSM module pin 8.

Arduino microcontrollers typically communicate with a PC via USB, which provides a UART path for code upload. This USB-based serial communication can interfere with the microcontroller's RX and TX pins whenever the PC communicates with the microcontroller and another UART device (such as the GSM module) is simultaneously in use. To mitigate this issue, UART communication is implemented on alternative microcontroller pins through the use of libraries, thereby enabling UART without occupying the hardware RX/TX pins. In the configuration described here, pins 7 and 8 are employed to realize software UART. The GSM module offers UART selection jumpers with two options: Software UART, which uses the module's D8 (RX) and D7 (TX) pins, and Hardware UART, which uses the module's D1 (RX)

and D0 (TX) pins. Hardware UART is paired with the microcontroller's RX and TX pins, while Software UART utilizes alternative digital pins on the microcontroller, enabled via libraries to function as TX and RX. Consequently, the configuration in Figure 4.27 connects the GSM module's RX to the microcontroller's TX and the GSM module's TX to the microcontroller's RX (Mamtaz Alam, 2022).

4.2.6 IoT device to be installed on the pole box near customer premises

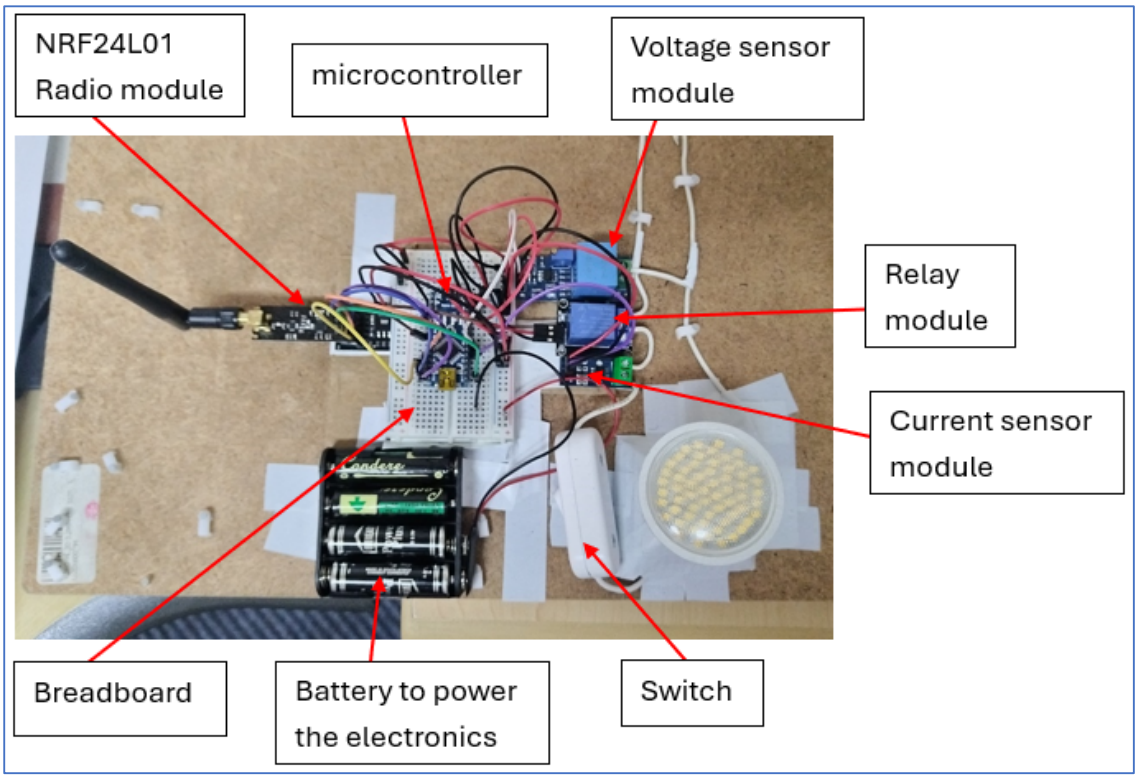

Figure 4.28: The IoT device installed near the customer premises (Near bulb on the prototype)

Figure 4.28 depicts the IoT device designed to represent the installation at the customer premises during the prototype phase. The electronic circuitry is mounted on a breadboard and powered by a 6-V DC battery. A current sensor measures the current in the AC circuit, while a voltage sensor measures the voltage across the lamp in the AC circuit. A relay module provides isolation of the lamp under overcurrent or overvoltage conditions. Finally, a radio module transmits the measured data to a mesh radio network, enabling wireless data communication for monitoring and control. The code running on the IoT device can be seen in appendix B4.2.

4.2.7 IoT device to be installed on the pole box near the transformer

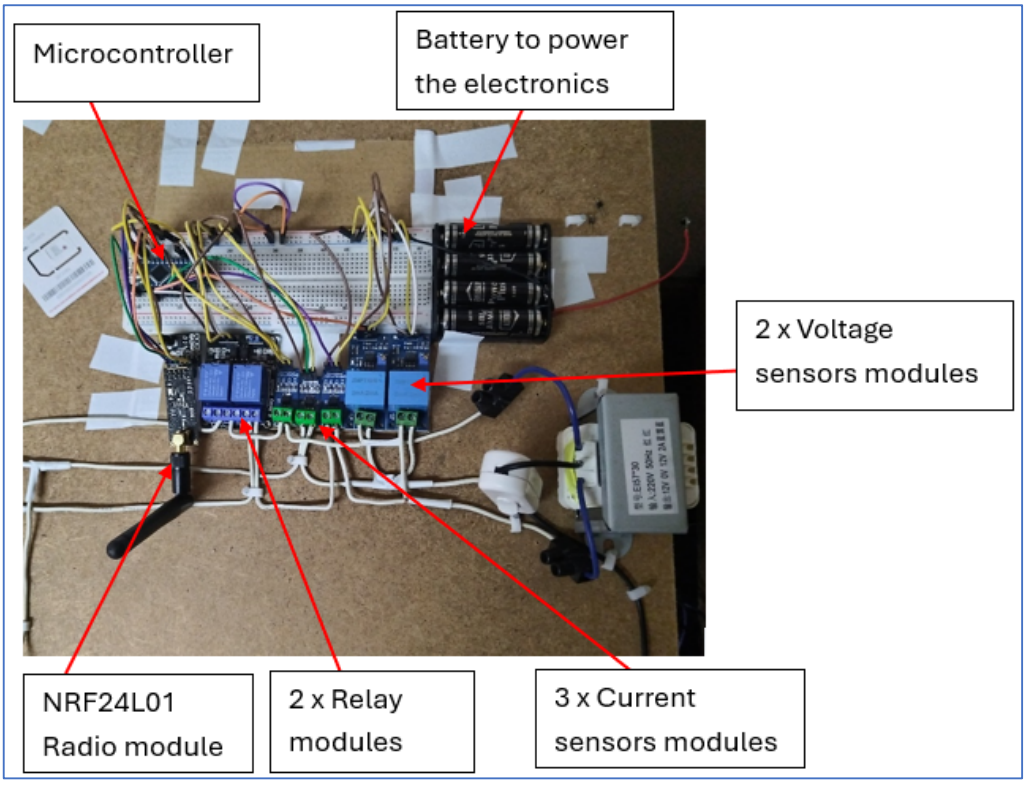

Figure 4.29: The IoT device installed near the transformer on the prototype (master IoT)

Figure 4.29 depicts an IoT device installed near the transformer within the prototype. The circuit is implemented on a breadboard and powered by a six-volt DC battery. All IoT devices in the network are largely similar in hardware and software; however, the device located adjacent to the transformer features a few distinct elements. Specifically, it includes two voltage sensors (one for each phase), three current sensors (one for each phase and one for the neutral), and two relay modules (one per phase). Moreover, this device functions as the master node, running software that listens for data from the other devices, collects and aggregates that data, performs its own measurements, and calculates system losses. Additionally, it contains an extra module not present in the other devices: a GSM module. The GSM module serves as a gateway to connect the transformer zone to the cloud for data collection, aggregation, and online control. The GSM connection is illustrated in Figure 4.30. The code running on the IoT device can be seen in appendix B4.3.

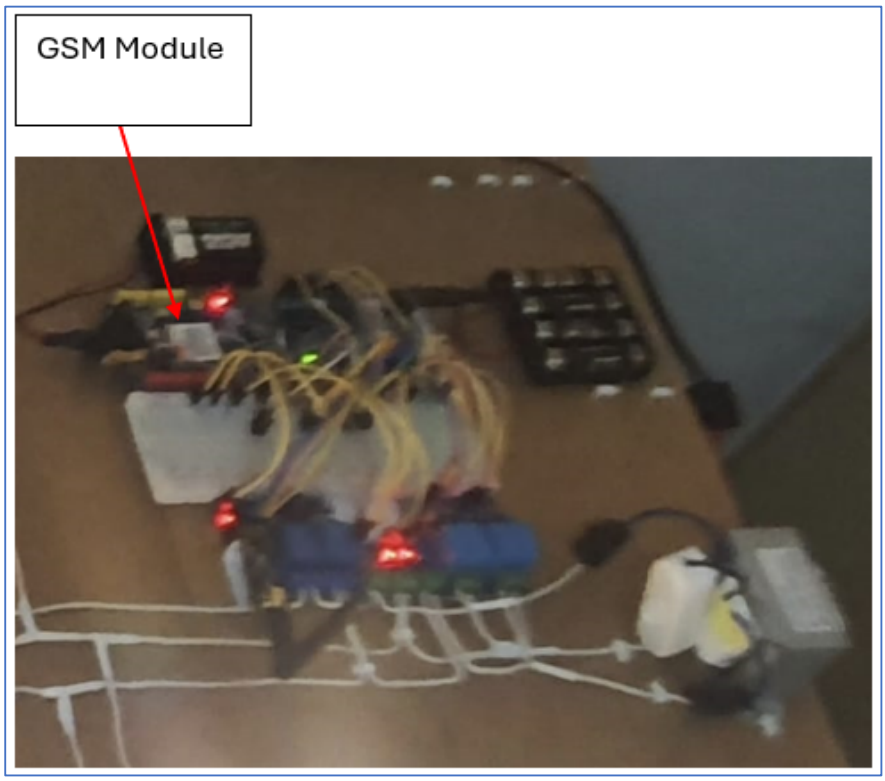

Figure 4.30: GSM module on the transformer IoT

4.2.8 Complete prototype of a Smart LV network

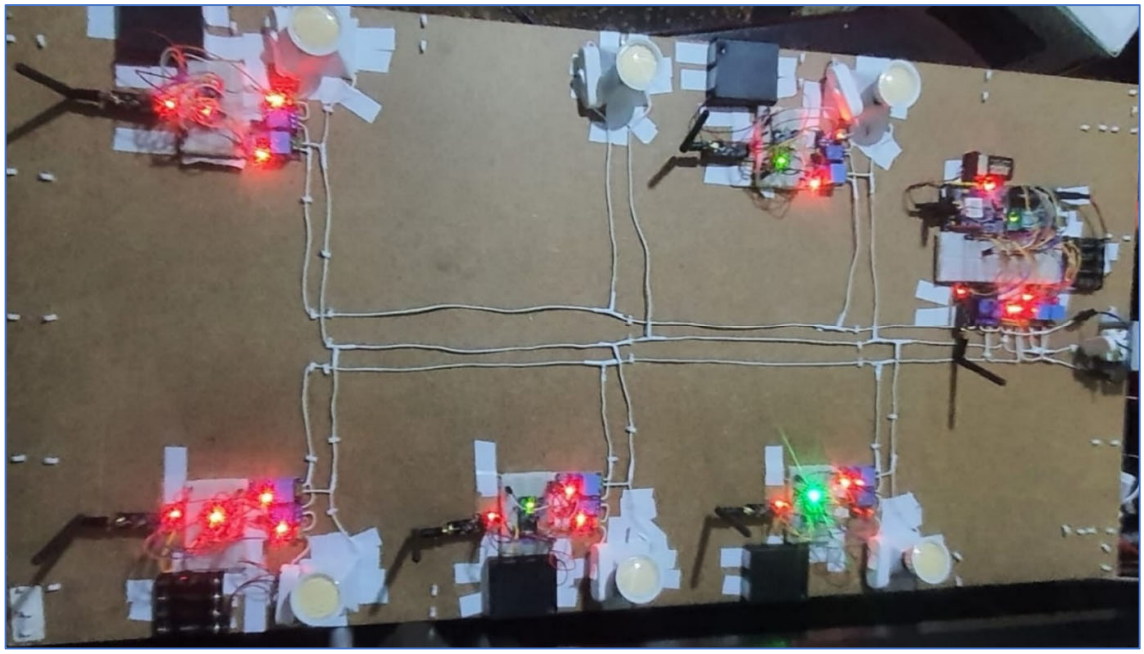

Figure 4.31: Complete prototype of an LV network with IoT devices installed and powered

Figure 4.31 depicts the completed prototype of the LV network with powered IoT devices. With the prototype design finalized, the remaining step is to evaluate whether the prototype operates as hypothesized, including its ability to detect and interrupt illegal connections in the LV network from inception. Before conducting experimental tests and discussing results, the same prototype design is replicated in a simulation environment to reproduce its behaviour and thereby verify the results and conclusions. The simulation design is described in Section 4.3.

4.3 Simulation design

To replicate the behaviour and, where applicable, the results described for the prototype discussed in Section 4.2, a simulation of the same low-voltage (LV) network is constructed using Proteus Design Suite. Proteus is a proprietary electrical design automation (EDA) tool developed by Labcenter Electronics Ltd. in Yorkshire, England. The suite provides an integrated environment for schematic capture, printed circuit board (PCB) layout, and mixed-mode circuit simulation within a Windows operating system, enabling the co-simulation of microcontroller firmware with attached analogue and digital components. By loading a microcontroller program in Hexadecimal or debug format, Proteus enables firmware co-simulation alongside the rest of the circuit, thereby supporting iterative prototyping across multiple application areas.

Proteus Design Suite is widely used for design, simulation, and education due to its hardware-free workflow, which makes it suitable for teaching, training, and hobbyist activities as well as professional development. The platform supports co-simulation with a broad range of microcontroller families, allowing users to verify embedded control logic in conjunction with peripheral circuitry before hardware fabrication. The following microcontrollers can be co-simulated within Proteus:

- NXP 8051
- ARM7
- ARM Cortex-M0 and ARM Cortex-M3
- Texas Instruments MSP430
- PICCOLO DSP and ARM Cortex-M3
- Parallax Basic Stamp
- Freescale HC11
- Microchip PIC10, PIC12, PIC16, PIC18, PIC24, dsPIC33
- Atmel AVR (and Arduino)
- 8086
- 8051 and ARM Cortex-M3

4.3.1 Smart LV network components on Proteus

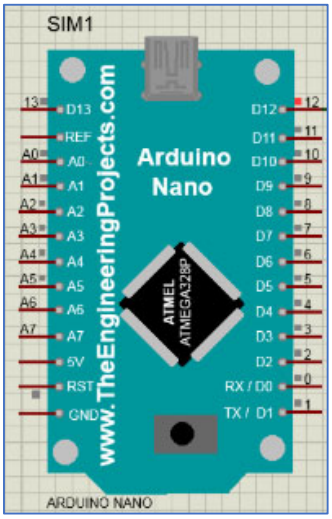

Figure 4.32: Arduino Nano Microcontroller on Proteus simulation platform

Figure 4.32 depicts an Arduino Nano as represented within the Proteus simulation environment. The simulation workflow enables programming of the microcontroller via the Arduino IDE, after which a hex file can be exported and uploaded to the simulated device. When the circuit is simulated, its behaviour is equivalent to that of a real microcontroller-based circuit, providing a valid platform for verifying software–hardware interactions prior to physical prototyping.

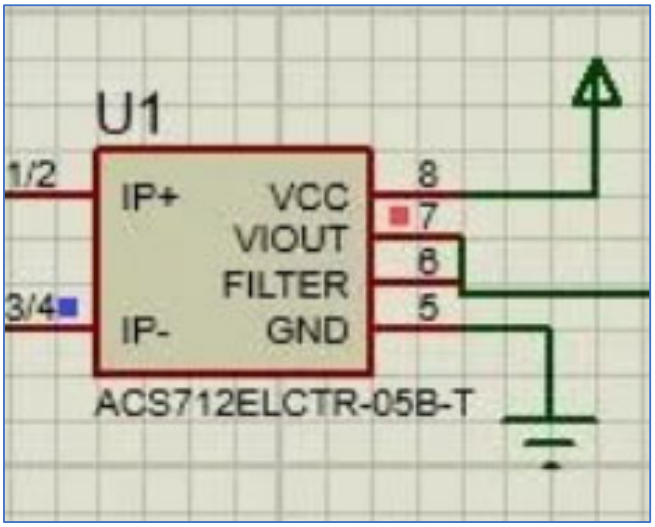

Figure 4.33: ACS712 AC current sensor on Proteus simulation software

Figure 4.33 illustrates the ACS712 current sensor in Proteus simulation software, exhibiting the same operating characteristics as the sensor presented in Section 4.2.

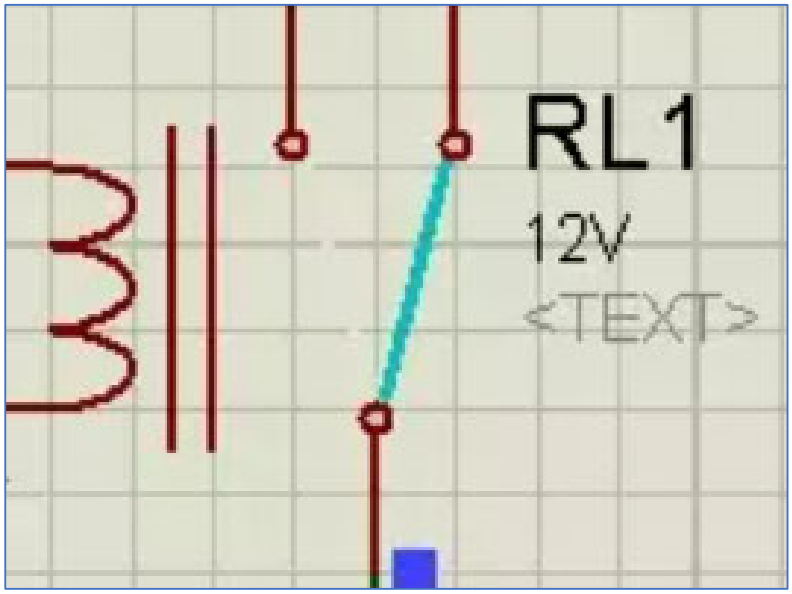

Figure 4.34: Relay on Proteus simulation software

Figure 4.34 depicts the relay within the Proteus simulation software, exhibiting behaviour identical to that of the relay module presented in Section 4.2.

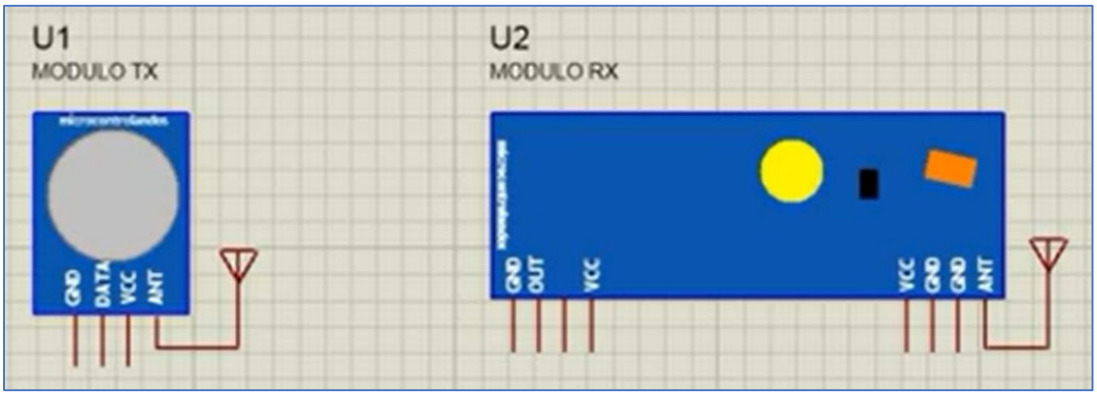

Figure 4.35: Radio frequency transmitter and receiver modules

Proteus simulation software does not include the NRF24L01 radio module within its simulation package. Instead, it provides a generic radio-frequency transmitter–receiver pair. Although this pair does not precisely replicate the NRF24L01's characteristics, it can be configured to meet the simulation's requirements. Consequently, an improvisational workaround is adopted to

enable data transmission in the simulated environment and to proceed with the calculations specified in the design.

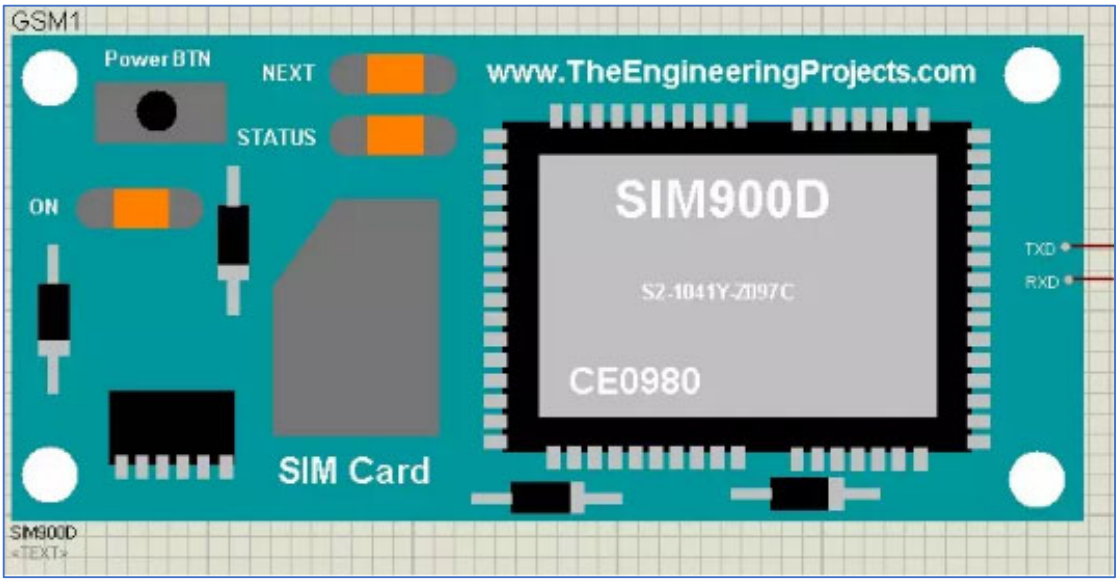

Figure 4.36: Sim900 GSM module on Proteus simulation software

Figure 4.36 depicts the SIM900 GSM module within Proteus simulation software, functioning equivalently to the GSM module described in Section 4.2.

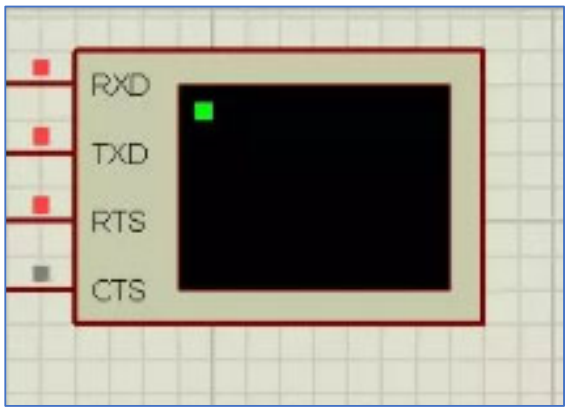

Figure 4.37: Virtual terminal on Proteus simulation software

Figure 4.37 depicts a virtual terminal implemented within the Proteus Design Suite. Because the project is simulated and data exchange occurs across different components of the model, the virtual terminals facilitate observation of the data flow. Specifically, one terminal is installed at the transmitter and another at the receiver to verify that data reaches the receiving end.

4.3.2 Smart LV network simulation on Proteus

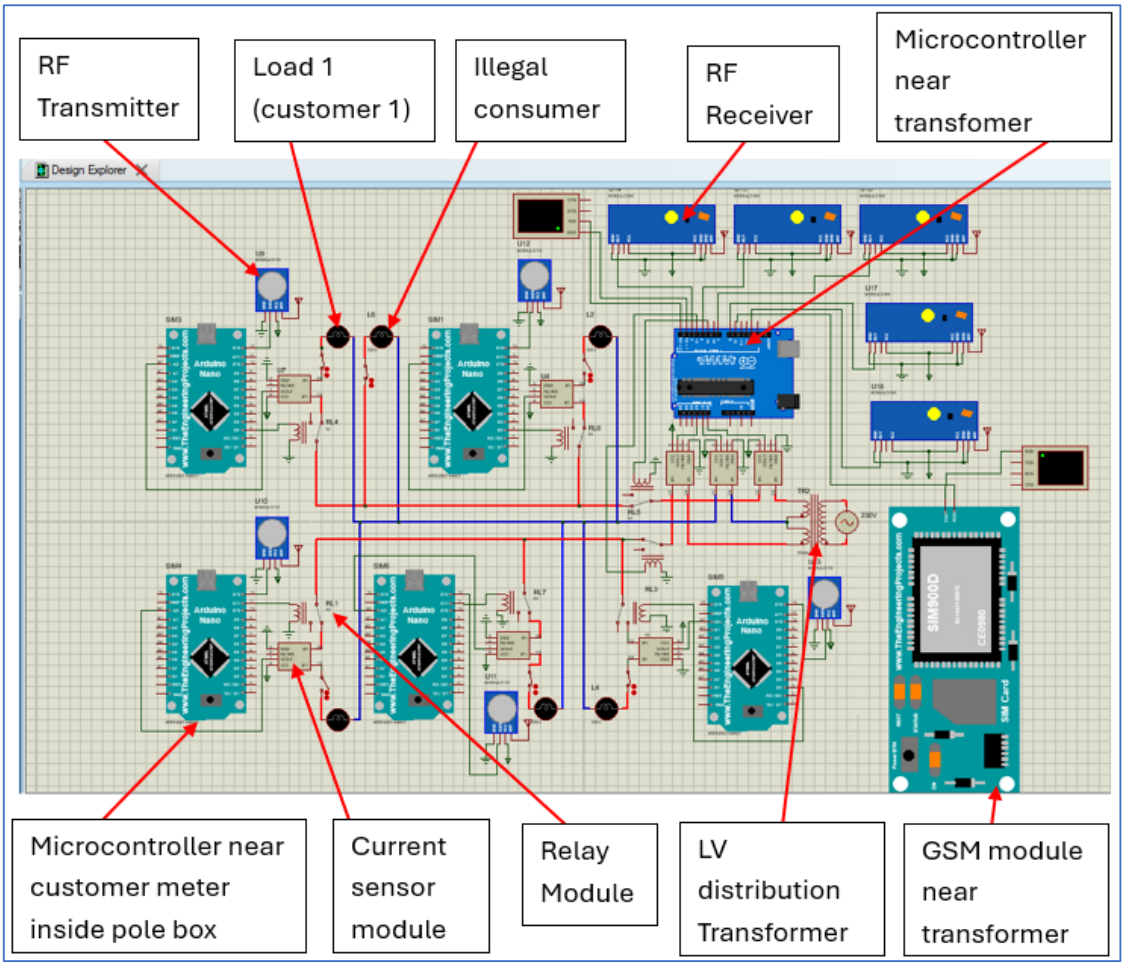

Figure 4.38: Completed version of the simulation with the IoT devices installed on Proteus simulation software

Figure 4.38 presents a completed simulation of the LV network with integrated IoT devices. Relative to the prototype described in Figure 4.2, several differences are evident. First, transformer sizing differs: the simulation imposes no practical size constraints, allowing the use of a full 22kV / 400V transformer. Second, the representation of loads differs: the simulation employs 230V bulbs with a resistance of 230Ω, which yields a current of 1A per bulb according to Ohm's law (I = V/R). Third, the installation of voltage sensors differs: the simulation omits the voltage sensor module, focusing instead on the exchange of current values across the network. Finally, with respect to wireless communication, the NRF24L01 radio module is not available within the software environment; consequently, an improvised arrangement is adopted in which a transmitter is installed on each IoT device and multiple

receivers are installed on the transformer structure. This configuration is sufficient to illustrate the core concept of the project: measuring current at various locations in the LV network, radioing the data to a master IoT device located near the transformer, and performing calculations to identify potential illegal connections.

4.4 Conclusion

This chapter presents a comprehensive design of the proposed smart low-voltage (LV) network prototype, detailing its configuration and the principal parameters governing its operation. Section 2 provides an in-depth exposition of the prototype design, including the selection of components and the methodology for measuring voltage and current with the microcontroller and accompanying sensors, as well as the derivation of the mathematical expressions used to convert ADC readings into instantaneous AC quantities. The discussion also documents the interconnections between each component and the microcontroller and clarifies the communication protocols underpinning the radio module–microcontroller interface and the microcontroller–GSM module interface. Furthermore, the chapter describes a Proteus-based simulation model of the smart LV network, outlining its configuration and the key parameters employed in the simulation to validate and illuminate the design.

Chapter Five presents the testing of both the physical prototype and the simulation, focusing on fault simulations and the observed behaviour of the network. The results of these tests are discussed and interpreted to evaluate the performance and validity of the proposed design.

5. CHAPTER 5
TESTING AND RESULTS DISCUSSION

5.1 Introduction

This chapter outlines the experimental validation and discusses the results obtained from both the hardware prototype and the simulation model. The smart LV network is designed to collect data from multiple points within the LV distribution network in near real-time, employing Internet of Things (IoT) devices operating within a Neighbourhood Area Network (NAN). The collected data is centralized for processing, where the system scans for anomalies, including illegal connections and general faults in the network. Following the detection and remediation of such anomalies, the data is transmitted to a Wide Area Network (WAN) to enable online visibility, monitoring, and control. The validation focuses on demonstrating that each stage—data collection, anomaly elimination, fault detection, and transmission to the cloud—is functioning as intended, with particular attention to the transmission to the ThingSpeak cloud platform.

This chapter is organized as follows: Section 5.2 presents the prototype testing procedures and the corresponding results; Section 5.3 describes the software simulation testing and its results; Section 5.4 discusses the results of both the prototype and the simulation, outlining the key findings and offering recommendations grounded in the evidence; and Section 5.5 concludes the chapter.

5.2 Prototype Testing

Testing commences by powering on the prototype and observing whether the currents and voltages measured at each customer-end IoT device are successfully transmitted to the master IoT device located near the transformer. This verification is accomplished by recording the currents, voltages, and relay statuses at each IoT node and by documenting the data received via the radio link and measured by the master device. The collected measurements are then checked and compared to confirm that all data arrive as intended. Once transmission over the NAN is confirmed to be functioning properly, the unauthorized-connection test proceeds. This test adopts a case-based approach in which network behaviour is assessed in scenarios without the unauthorized connection and in scenarios in which the unauthorized connection is introduced alongside varying combinations of other loads switched on and off to determine whether the unauthorized connection is detected. Similar case-based evaluations are conducted to assess the behaviour of the smart LV network under fault conditions. The network’s behaviour is observed until the data is registered on the cloud via ThingSpeak.

5.2.1 Energising the Smart LV network

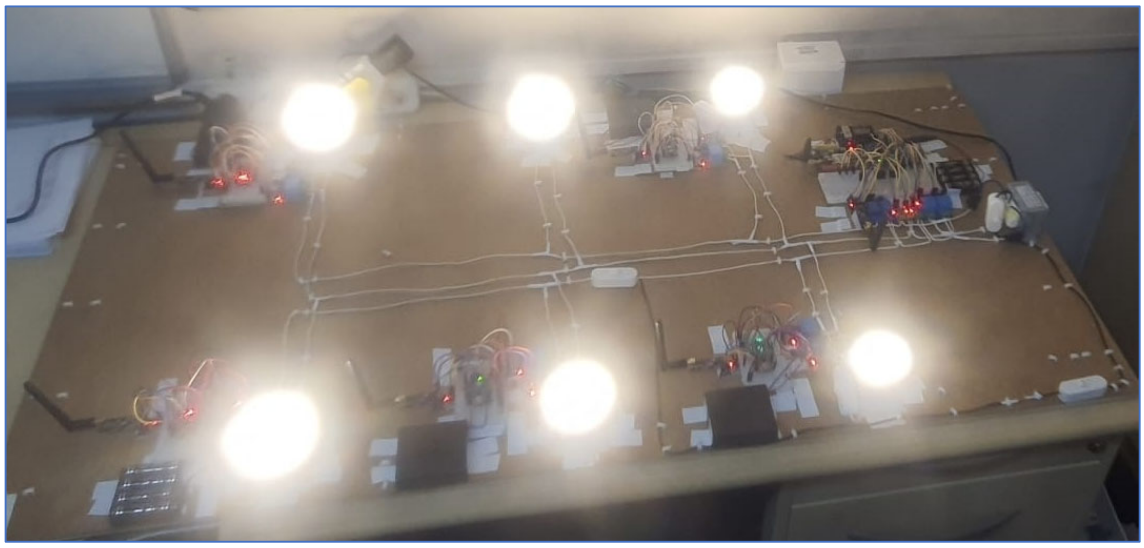

Figure 5.1: Energised smart LV network prototype

Upon programming each microcontroller and energizing the IoT devices, the network commences data exchange relating to currents, voltages, and relay statuses. The on/off switching of different bulbs influences the measured current values near the transformer, as described in Chapter 3, Section 3.8.

Figure 5.1 depicts the smart LV network prototype, in which all IoT devices and bulbs are energised. Following energisation, both relays near the transformer tripped irrespective of the status of the illegal connection, indicating a flaw in the proposed algorithms. The initial step in addressing this issue involved recording the measured values from each IoT device and comparing them as prescribed by the algorithm. Under the transformer-not-energised condition, all bulbs are switched off while only the IoT devices remained energised; the conditional checks and the commands to open the relays are commented out in the code. The resulting data is observed and recorded. Tables 5.1 to 5.6 present the data collected from each IoT device.

Table 5.1: Data measured at the first pole box on phase 1

Pole Box 1 (Phase 1)	
Current	0.0052 A
Voltage	0.310 V
Relay Status	1

Table 5.2: Data measured at the second pole box on phase 1

Pole Box 2 (Phase 1)	
Current	0.0046 A
Voltage	0.321 V
Relay Status	1

Table 5.3: Data measured at the third pole box on phase 1

Current	0.0047 A
Voltage	0.298 V
Relay Status	1

Table 5.4: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0.0050 A
Voltage	0.311 V
Relay Status	1

Table 5.5: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0.0061 A
Voltage	0.301 V
Relay Status	1

Table 5.6: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	0.0062 A
Measured Phase 2 Current	0.0059 A
Measured Neutral	0.0061 A
Measured Phase 1 Voltage	0.320 V
Measured Phase 2 Voltage	0.316 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.0051 A
Received Pole Box 1 Voltage	0.310 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.0046 A
Received Pole Box 2 Voltage	0.321 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.0047 A
Received Pole Box 3 Voltage	0.298 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.0050 A
Received Pole Box 4 Voltage	0.311 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.0061 A
Received Pole Box 5 Voltage	0.301 V
Received Pole Box 5 Relay status	1

Table 5.6 presents the data measured and received at the transformer pole box. From Table 5.6 it is observed that all data recorded at each pole box (Tables 5.1 through 5.5) are

successfully transmitted and received at the transformer pole box. With the transformer OFF, currents and voltages at each pole box should be zero; however, small nonzero values are recorded by the IoT devices. These minor values are then transmitted to the IoT device at the transformer, where they are summed to produce a larger value than that measured at the transformer itself. For example, the current at phase 1 should be the sum of the currents from pole boxes 1, 2, and 3:

0.0051 A + 0.0046 A + 0.0047 A = 0.0144 A,

yet the measured current at phase 1 at the transformer is 0.0062 A.

Because the deployed algorithm checks for a condition in which the current measured near the transformer is not equal to the sum of the currents from each pole box and isolates the phase when these differ, the relays trip immediately upon energising the transformer. This indicates that the pole boxes appear to register a higher current than that delivered by the transformer, although no real current flows in the circuit and all IoT devices should read 0A. The discrepancy and its underlying causes are discussed in detail in Chapter 4. In the absence of current flow on the AC circuit, the ADC value corresponding to 0A should be the midpoint of the 0–1023 range (511.5 for a 10-bit ADC). However, the microcontroller returns integer values, yielding 512, which, when converted to current, does not equal zero. Additionally, the ADC readings at 0 A are not stable, alternating between 512 and 511, neither of which corresponds to zero current.

To address this issue, the code on each IoT device is modified for both current and voltage calculations to ensure that, whenever the ADC reports 512 or 511, the instantaneous current calculation uses the midpoint value of 511.5. This adjustment effectively enforces the true midpoint in the current calculation. As a result, the currents and voltages converge to 0 A when the circuit is completely off. The readings obtained after this modification are presented in Tables 5.7 through 5.12.

Table 5.7: **Data measured at the first pole box on phase 1**

Pole Box 1 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.8: **Data measured at the second pole box on phase 1**

Pole Box 2 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.9: Data measured at the third pole box on phase 1

Pole Box 3 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.10: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.11: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.12: Data measured and received from radio communication at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	0 A
Measured Phase 2 Current	0 A
Measured Neutral	0 A
Measured Phase 1 Voltage	0 V
Measured Phase 2 Voltage	0 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0 A
Received Pole Box 1 Voltage	0 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0 A
Received Pole Box 2 Voltage	0 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0 A
Received Pole Box 3 Voltage	0 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0 A
Received Pole Box 4 Voltage	0 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0 A
Received Pole Box 5 Voltage	0 V
Received Pole Box 5 Relay status	1

Table 5.12 indicates that the currents and voltages received from all other IoT devices are zero, corresponding to the currents measured at each phase. Consequently, when the condition checks and the instruction to open the relay are uncommented, the transformer relays did not trip until the transformer is energised and all bulbs are switched on; the relays

adjacent to the transformer tripped on both phases, indicating partial resolution of the issue. The next step involved re-commenting the condition checks and the instruction to open the relay near the transformer and then observing and recording data at each pole box with the bulbs ON to confirm the presence of voltage and current flow in the circuit. The observed data is presented in Tables 5.13 to 5.18.

Table 5.13: Data measured at the first pole box on phase 1

Pole Box 1 (Phase 1)	
Current	0.498 A
Voltage	12.213 V
Relay Status	1

Table 5.14: Data measured at the second pole box on phase 1

Pole Box 2 (Phase 1)	
Current	0.496 A
Voltage	12.201 V
Relay Status	1

Table 5.15: Data measured at the third pole box on phase 1

Pole Box 3 (Phase 1)	
Current	0.504 A
Voltage	12.198 V
Relay Status	1

Table 5.16: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0.501 A
Voltage	12.211 V
Relay Status	1

Table 5.17: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0.503 A
Voltage	12.203 V
Relay Status	1

Table 5.18: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	1.502 A
Measured Phase 2 Current	1.498 A
Measured Neutral	0 A
Measured Phase 1 Voltage	12.211 V
Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1

Phase 2 Relay status	1
Received Pole Box 1 Current	0.498 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.496 A
Received Pole Box 2 Voltage	12.201 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.504 A
Received Pole Box 3 Voltage	12.198 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.501 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.503 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Observing the data collected at the transformer pole box in table 5.18, the reason for the relays tripping can be easily picked up. Even though the current flow on the circuit is the same because the bulbs have the same resistance, it appears that the current measured at each IoT device is slightly different from the current measured at any other IoT device, the same with the voltages. With the understanding of Kirchoff's current law, the currents should be the same, so why the difference? The source of these discrepancies lies in the accuracy specifications of the measurement modules: the ACS712 current sensor has an error margin of ±1.3%, and the ZMPT101B voltage sensor has an error margin of ±3%. Consequently, a true current of 5A could be reported anywhere within the range of 4.935 A to 5.065 A by the current sensor, and similar tolerance applies to voltage readings, with all readings within these bounds considered acceptable.

To illustrate, using data from IoT devices on the same phase, the current on phase 1 is computed as the sum of the currents from received pole boxes:

0.498A + 0.496A + 0.504A = 1.498A.

In contrast, the IoT device located near the transformer on phase 1 reports 1.502A. Because the integrity check for illegal connections is based on the equality of currents measured at the IoT devices with the current measured near the transformer on the corresponding phase, this difference is interpreted as a fault and triggers the relay.

A practical remedy is to incorporate the sensor error margins into the decision logic. This is achieved by adopting a percentage-based tolerance when testing current equality. The

proposed algorithm is as follows: measure the currents at each pole box and transmit these values to the transformer pole box; at the transformer, receive all radio-transmitted currents and measure the current on each phase; compare the measured phase currents with the currents received from the IoT devices on the corresponding phase. If the IoT-reported currents lie within a ±2% range of the transformer-measured phase currents, the readings are considered acceptable. If, however, the transformer-measured currents exceed the IoT-reported currents by more than ±2%, an illegal connection is deemed present, and the relay on the affected phase is tripped. This approach accounts for sensor inaccuracy and reduces false trips while maintaining the ability to detect actual illegal connections.

This approach completely resolves the previously identified flaw in the algorithm responsible for detecting unauthorized connections within a transformer-based IoT device. The unauthorized connection is introduced at Phase 2 of the transformer. To evaluate the system's ability to detect this intrusion, three tests are conducted, during which data exchanges between the IoT devices are recorded. These tests are done in a form of a case study with three cases.

5.2.2 Case Study: Elimination of illegal connections

Case 1 Illegal connection detection: Case 1 involved switching ON all five bulbs equipped with IoT devices. Subsequently, an unauthorized connection—defined as a bulb without any IoT device in proximity—was introduced. Observations and data collection are conducted to monitor the system's behaviour under these conditions. The data recorded pertain solely to the IoT devices in Phase 2 and to the transformer IoT and are presented in Tables 5.19 to 5.21.

Table 5.19: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0.501 A
Voltage	12.211 V
Relay Status	1

Table 5.20: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0.503 A
Voltage	12.203 V
Relay Status	1

Table 5.21: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	1.502 A
Measured Phase 2 Current	1.498 A
Measured Neutral	0 A
Measured Phase 1 Voltage	12.211 V

Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.498 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.496 A
Received Pole Box 2 Voltage	12.201 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.504 A
Received Pole Box 3 Voltage	12.198 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.501 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.503 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Based on the data recorded in Table 5.21, the following conclusions are drawn. Phase 1: The total current received is the sum of the currents from Pole Boxes 1 to 3: 0.498A + 0.496A + 0.504A, yielding 1.498A. The IoT device near the transformer measured a current on Phase 1 of 1.502A. The difference between the IoT measurement and the received current is 0.004 A (approximately 0.3%), which is below the 2% criterion. Consequently, the Phase 1 relay did not open, and the Phase 1 circuit remains energized. There is no evidence of an illegal connection on Phase 1.

Phase 2: The total current received is the sum of the currents from Pole Boxes 4 and 5: 0.501A + 0.503A, amounting to 1.003A. The IoT device measured a Phase 2 current of 1.498A. The IoT measurement exceeds the received current by more than 2%; applying a 2% threshold to the received current (1.003A × 0.02 = 0.02006A) yields a trip threshold of 1.02306 A. Since 1.498A > 1.02306A, the relay at Phase 2 will trip, cutting the supply to all bulbs on Phase 2. This outcome is attributed to the current drawn by an illegal connection at Phase 2.

Case 2 Illegal connection detection: Case 2 examines a scenario in which one of the two Phase 2 bulbs, each equipped with an IoT device, is deliberately switched OFF, resulting in only a single illuminated bulb, in addition to the bulb that represents an illegal connection. Data collected from the IoT devices on Phase 2 and from the transformer pole box are reported in Tables 5.22 through 5.24.

Table 5.22: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0 A
Voltage	12.203 V
Relay Status	1

Table 5.23: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0.503 A
Voltage	12.203 V
Relay Status	1

Table 5.24: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	1.502 A
Measured Phase 2 Current	1.012 A
Measured Neutral	0.498 A
Measured Phase 1 Voltage	12.211 V
Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.498 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.496 A
Received Pole Box 2 Voltage	12.201 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.504 A
Received Pole Box 3 Voltage	12.198 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.503 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Based on the data recorded in Table 5.24, the following conclusions are drawn:

Phase 1 total current received is the sum of currents from Pole Boxes 1 to 3:

I_received, P1 = 0.498A + 0.496A + 0.504A = 1.498A.

The IoT device proximal to the transformer measured a Phase 1 current of

I_meas, P1 = 1.502A.

The relative difference between measured and received currents is

(1.502 − 1.498) / 1.498 ≈ 0.003, or approximately 0.3%,

which is below the 2% threshold. Therefore, the relay at Phase 1 does not open, and the Phase 1 circuit remains energized. There is no indication of an illegal connection on Phase 1.

For Phase 2, the total current received is the sum of currents from Pole Boxes 4 and 5:

I_received, P2 = 0A + 0.503A = 0.503A.

The IoT device measured a Phase 2 current of

I_meas, P2 = 1.012A.

This measured value exceeds the received current by 0.509 A, corresponding to a relative increase of:

(1.012 − 0.503) / 0.503 ≈ 1.01, i.e., about 101%.

As a result, the relay at Phase 2 tripped, cutting the supply to all bulbs on Phase 2. This increased current is attributed to the current drawn by an illegal connection at Phase 2.

Case 3 Illegal connection detection: Case 3 involved deactivating both IoT-enabled bulbs on Phase 2, while only the bulb representing the illicit connection remained illuminated. The data measured between the Phase 2 pole boxes and the transformer pole box are recorded and are presented in Tables 5.25 to 5.27.

Table 5.25: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0 A
Voltage	12.211 V
Relay Status	1

Table 5.26: Data measured at the fifth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	0 A
Voltage	12.203 V
Relay Status	1

Table 5.27: Data measured and received from radio communication at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	1.502 A
Measured Phase 2 Current	0.501 A
Measured Neutral	1.012 A
Measured Phase 1 Voltage	12.211 V
Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.498 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.496 A
Received Pole Box 2 Voltage	12.201 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.504 A
Received Pole Box 3 Voltage	12.198 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Based on the data recorded in Table 5.27, the following conclusions are drawn:

Phase 1: The total current received is the sum of currents from Received Pole Boxes 1, 2, and 3, yielding 1.498A. The IoT device near the transformer measures a Phase 1 current of 1.502A. The difference between the measured and received currents is 0.004 A, which corresponds to approximately 0.27%, well below the 2% threshold. Consequently, the relay for Phase 1 does not trip, and the Phase 1 circuit remains energized. There is no evidence of an illegal connection on Phase 1.

Phase 2: The total current received is the sum of currents from Received Pole Boxes 4 and 5, equal to 0A. The IoT device near the transformer measures a Phase 2 current of 0.501A. The measured current on Phase 2 exceeds the received current by more than 2%, triggering the

relay to trip and cutting the supply to all bulbs on Phase 2, which is attributed to the presence of an illegal connection.

Collectively, these cases demonstrate the capability of the smart LV network to eliminate illegal connections. The described algorithms are effective for any instance of an illegal connection within the network, provided the illicit current drawn surpasses the 2% differential threshold. The author made a video testing the prototype for illegal connection detection, the video is uploaded on YouTube on the link (copy the link and paste in on a web browser):
https://www.youtube.com/watch?v=RL1xsyupy-w&list=PLvjyFh-Tzzs8zX4j36n9xgtcuTztk9GFI&index=1

5.2.3 Fault detection on the network

Low-voltage distribution networks are susceptible to a range of fault types that compromise public safety and system reliability. Notable examples include broken conductors that may fall to ground and pose risks to humans and animals, as well as broken neutral conductors at transformers, which can induce over-voltage and under-voltage conditions throughout the network. Such faults can result in property damage and give rise to liability claims against electricity distributors. To address these risks, smart LV networks are designed with capabilities to detect and mitigate these faults promptly, thereby enhancing safety, reducing outage durations, and limiting liability exposure through timely fault management.

5.2.3.1 Case Study: Broken conductor on the ground

The current flow in a dual-phase LV distribution network is predictable and can be described by three normal operating configurations. In the first configuration, the current in Phase 1 equals the sum of the current in Phase 2 and the current in the neutral conductor ($I1 = I2 + IN$). In the second configuration, the current in Phase 2 equals the sum of the current in Phase 1 and the current in the neutral conductor ($I2 = I1 + IN$). in the third configuration, the current in Phase 2 equals the current in Phase 1 with no current in the neutral conductor ($I2 = I1$ and $IN = 0$). These three conditions define the normal operating regime for the LV network, as discussed in detail in Chapter 3. The designed smart LV network facilitates the testing of these conditions via three current sensors located near the transformer.

If there is no current flow on all phases and the neutral, this may indicate that there is no power supply at the transformer; voltage measurements should be checked, and a no-supply condition should be reported. If $I1 + IN \neq I2$ or $I2 + IN \neq I1$, leakage current is present, meaning that some current is flowing to ground. Given the deployment of IoT devices across the network, devices affected by a broken conductor will report zero current, providing a clear indication to the transformer IoT device regarding which phase should be isolated.

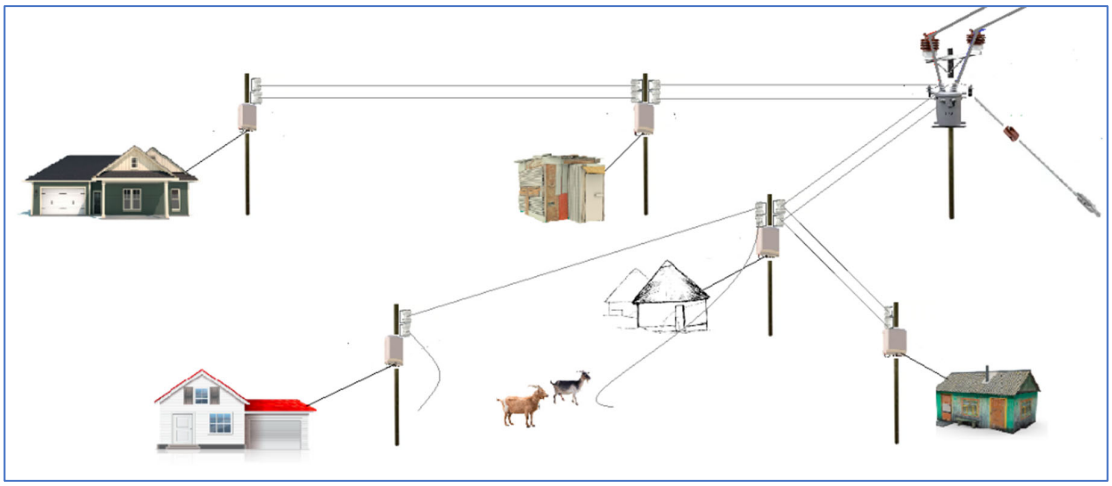

Figure 5.2: Low voltage network showing a broken conductor fault

Figure 5.2 illustrates a low-voltage distribution network subjected to a broken-conductor fault. This fault diverts current to the ground, disrupts the closed conducting loop, and results in a nonzero algebraic sum of the currents in the two-phase conductors and the neutral conductor near the transformer.

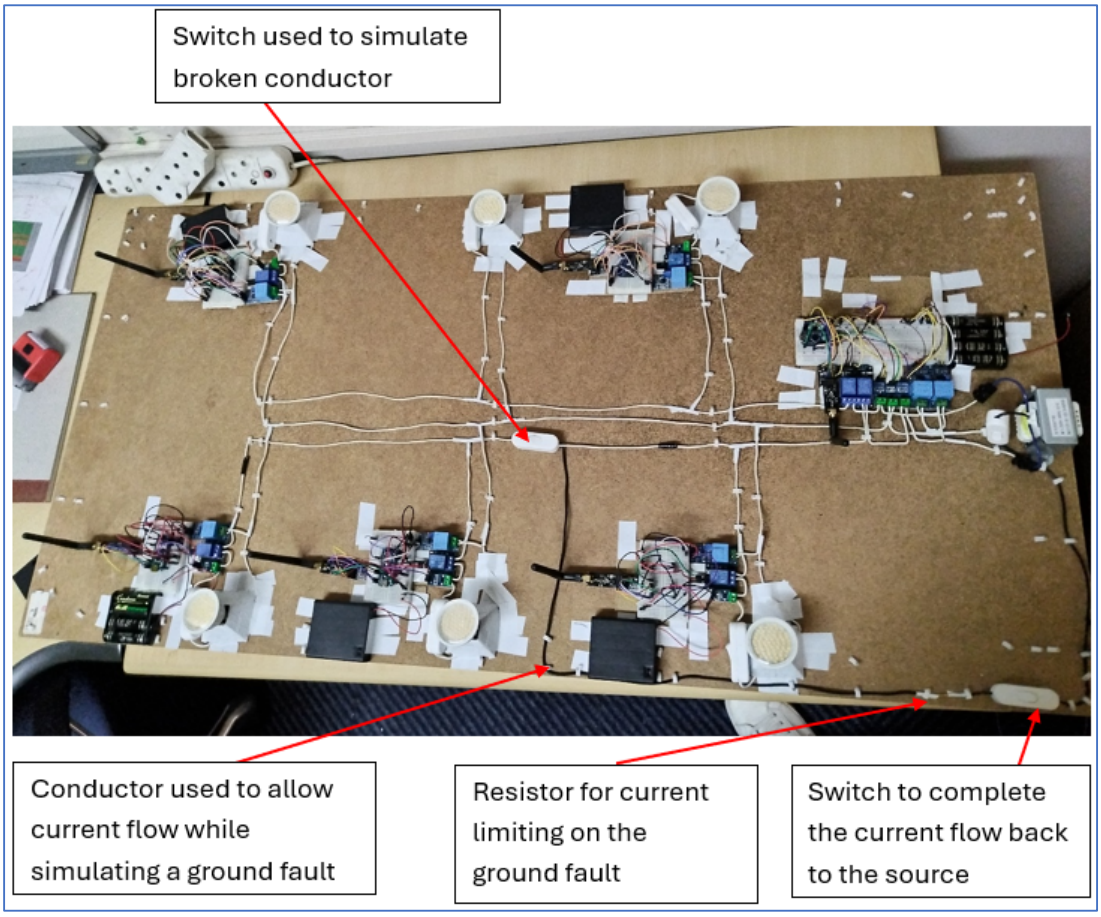

Figure 5.3: Smart LV network prototype showing the simulation of the broken conductor

Figure 5.3 presents the smart LV network prototype and the fault-simulation design used to test the algorithms for detecting and isolating faults. The prototype incorporates two switches. Switch S1 is placed on phase 1 and serves to cut power to two of the three bulbs on that phase. A black interconnection cable runs from this switch back to the transformer on the neutral conductor, bypassing the current sensors. A second switch completes this circuit through a current-limiting resistor placed on the black interconnection conductor to prevent a short circuit. With a 12V supply across the 100Ω resistor, a current of 0.12A is expected to flow through this branch.

To emulate a broken conductor that falls and contacts the ground, Switch S1 on phase 1 is opened, disconnecting power from the remaining two bulbs. Subsequently, Switch S2 on the black interconnection is closed to complete the circuit via the 100Ω resistor. This configuration causes current from the transformer to flow through only one of the three bulbs, with approximately 0.12A traveling through the black branch back to the transformer neutral and not passing through the three sensors located near the transformer. Two tests are conducted to observe the circuit's behaviour under this fault condition and to evaluate the fault-detection and isolation algorithms.

Case 1 Fault detection: All five bulbs, each with an associated IoT device, are energized, with the bulb representing an illegal connection remaining de-energized. Subsequently, a broken-conductor condition is simulated on Phase 1. The data collected during this broken-conductor simulation is presented in Tables 5.28 through 5.31 below.

Table 5.28: **Data measured at the first pole box on phase 1**

Pole Box 1 (Phase 1)	
Current	0.498 A
Voltage	12.213 V
Relay Status	1

Table 5.29: **Data measured at the second pole box on phase 1**

Pole Box 2 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.30: **Data measured at the third pole box on phase 1**

Pole Box 3 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.31: **Data measured and received from radio communication at the transformer pole box**

Transformer Pole Box	
Measured Phase 1 Current	0.619 A
Measured Phase 2 Current	1.012 A
Measured Neutral	0.498 A
Measured Phase 1 Voltage	12.211 V
Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.498 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0
Received Pole Box 2 Voltage	0
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0
Received Pole Box 3 Voltage	0
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.501 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.503 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Under normal LV network operation, the currents are expected to satisfy the relation that the measured Phase 1 current plus the measured Neutral current equals the measured Phase 2 current (within ±2%), or equivalently that the measured Phase 2 current plus the measured Neutral current equals the measured Phase 1 current (within ±2%). From Table 5.27, the following deductions are obtained:

Measured Phase 2 Current = 1.012A;

Measured Phase 1 Current plus Measured Neutral Current = 0.619A + 0.492A = 1.111A,

which differs from the measured Phase 2 current by more than 2%. Similarly,

Measured Phase 1 Current = 0.619A

Measured Phase 2 Current plus Measured Neutral Current = 1.012A + 0.492A = 1.504A

which differs from the measured Phase 1 current by more than 2%. These two discrepancies indicate the presence of leakage current.

Phase 1 total current received is the sum of currents from Received Pole Box 1, 2, and 3:

0.498A + 0A + 0A = 0.498A.

The IoT device near the transformer records Phase 1 current as 0.619A, which exceeds the received Phase 1 current by 0.121A, a deviation greater than 2%, indicating a leakage condition. Consequently, the relay on Phase 1 tripped to cut the supply to the faulty conductor.

Phase 2 total current received is the sum of currents from Received Pole Box 4 and 5:

0.501A + 0.503A = 1.004A.

The IoT device near the transformer records Phase 2 current as 1.012 A, a difference of 0.008 A (approximately 0.8%), which is not greater than 2%; therefore, the Phase 2 relay did not trip. Taken together, the last two tests clearly identify Phase 1 as the leakage phase, warranting isolation of the affected conductor.

Case 2 Case 1 Fault detection: Only the two bulbs on Phase 2, along with the neighbouring IoT devices, are energized; the bulb representing an illegal connection remains de-energized. All bulbs on Phase 1 remain off. Subsequently, a broken-conductor fault is simulated on Phase 1. The data collected during this simulation are presented in Tables 5.32 to 5.35 below.

Table 5.32: Data measured at the first pole box on phase 1

Pole Box 1 (Phase 1)	
Current	0 A
Voltage	12.213 V
Relay Status	1

Table 5.33: Data measured at the second pole box on phase 1

Pole Box 2 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.34: Data measured at the third pole box on phase 1

Pole Box 3 (Phase 1)	
Current	0 A
Voltage	0 V
Relay Status	1

Table 5.35: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	0.121 A
Measured Phase 2 Current	1.012 A
Measured Neutral	1.011 A
Measured Phase 1 Voltage	12.211 V
Measured Phase 2 Voltage	12.197 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0 A
Received Pole Box 1 Voltage	12.213 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0
Received Pole Box 2 Voltage	0
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0
Received Pole Box 3 Voltage	0
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.501 A
Received Pole Box 4 Voltage	12.211 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.503 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

From Table 35, the following values are recorded:

Phase 2 current (I2) = 1.012A,

Phase 1 current (I1) = 0.121A, and

Neutral current (In) = 1.011A.

It follows that

I1 + In = 0.121A + 1.011A = 1.132A,

which exceeds I2 by more than 2%. Conversely,

I2 + In = 1.012A + 1.011A = 2.023A,

which far exceeds I1 (0.121A) by more than 2%. These two discrepancies indicate the presence of leakage current.

Further data assessment shows the phase currents entering the system via the pole boxes. Phase 1 total current received equals the sum of currents from Pole Boxes 1 to 3:

0 A + 0A + 0 A = 0A.

In contrast, the IoT device located near the transformer records Phase 1 current as 0.121 A, indicating that the measured current on Phase 1 exceeds the received current by at least 2%. Consequently, the relay associated with Phase 1 tripped.

For Phase 2, the total current received is the sum from Pole Boxes 4 and 5:

0.501A + 0.503A = 1.004A.

The IoT device near the transformer reports Phase 2 current as 1.012A, a difference of 0.008A (approximately 0.8%), which does not exceed the 2% threshold; as a result, the Phase 2 relay did not trip.

The last two tests confirm that the leakage current is localized to Phase 1. Given this, and the certainty that only Phase 1 is affected, supplying isolation to the defective conductor is warranted. The author made a video testing the prototype for fault detection, the video is uploaded on YouTube on the link (copy the link and paste in on a web browser):
https://www.youtube.com/watch?v=y6M70InU4bU&list=PLvjyFh-Tzzs8zX4j36n9xgtcuTztk9GFI&index=2

5.2.3.2 Case Study: Broken neutral conductor near the transformer

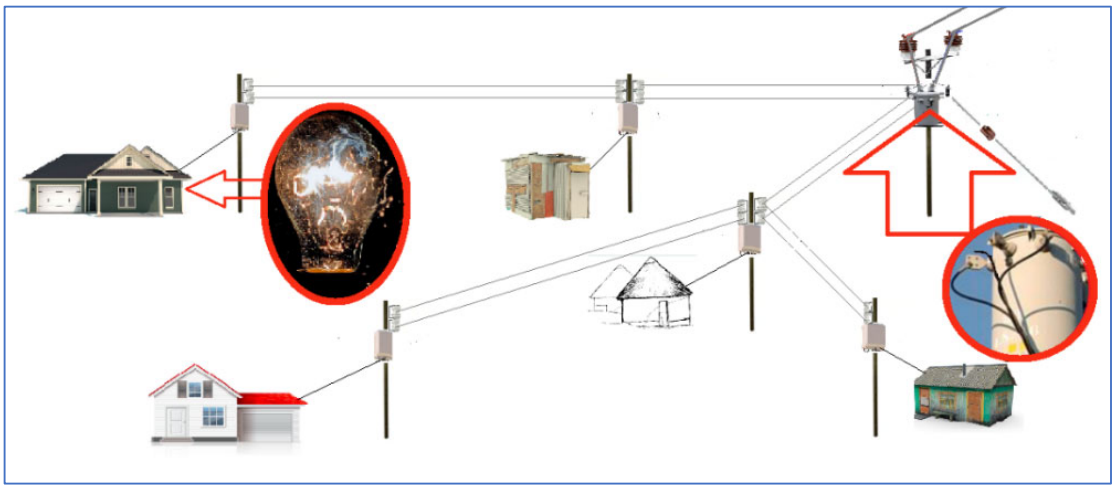

Figure 5.4: LV network with a neutral wire broken near the transformer

Figure 5.4 depicts an LV distribution network in which the neutral conductor is broken proximal to the transformer. This fault represents a particularly troublesome condition for electricity distribution operators, as it can cause damage to appliances connected to the network and may expose the operator to liability claims. The proposed smart LV network is engineered to detect and isolate this fault condition proactively, thereby preventing damage to customer equipment.

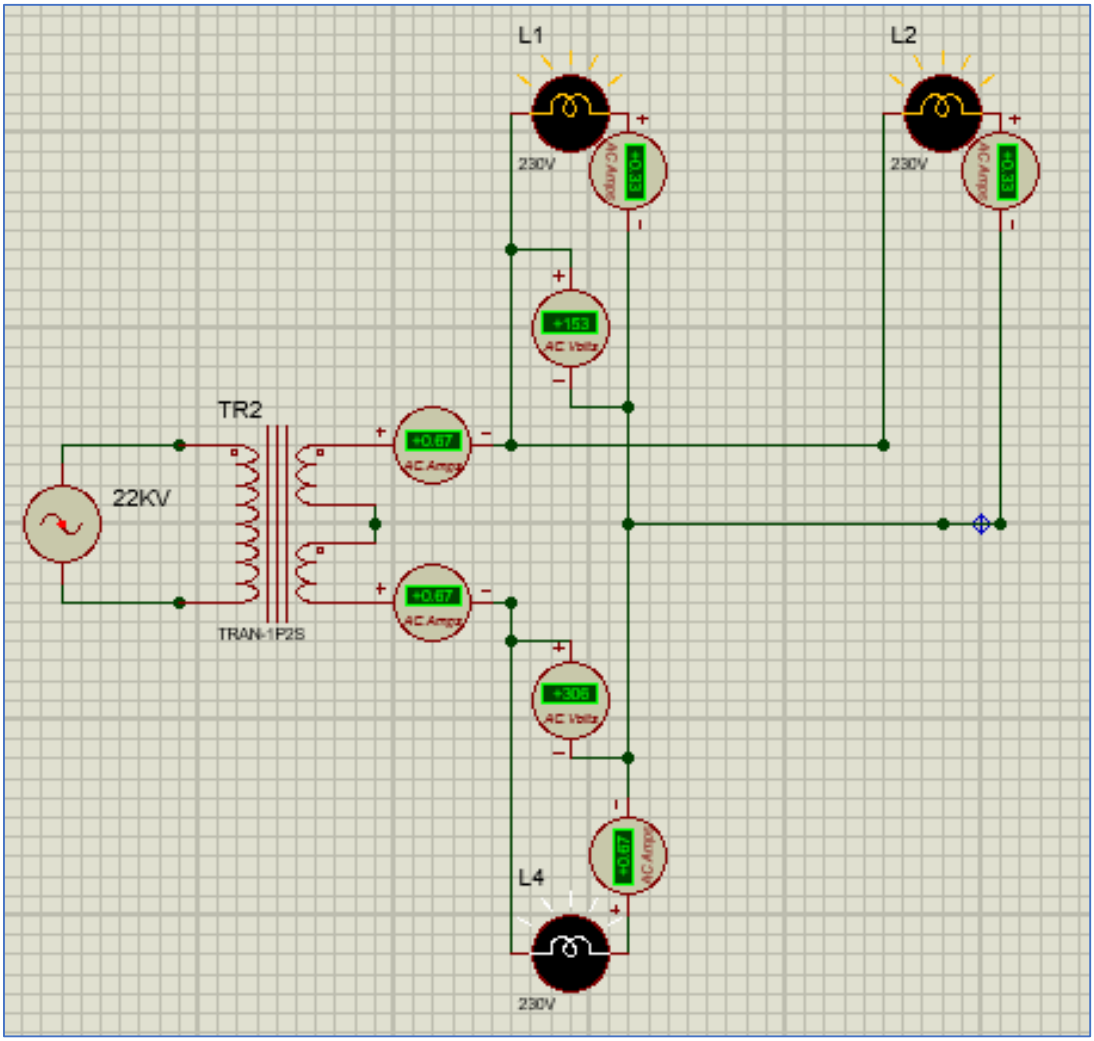

Figure 5.5: Simulated broken neutral on Proteus software

Figure 5.5 depicts a simulated scenario in which a damaged neutral conductor near the transformer on an LV distribution network is used to illustrate its consequences for the network and for customer appliances. Under normal operation, all customer appliances connected to an LV network are effectively wired in parallel across a phase-to-neutral voltage of 230 V, and the current drawn by each device is determined by its power rating through the relation,

$P = V \times I$ or

$I = P / V$

For example, in a typical household, a 2000W kettle and a 150W television connected in parallel both experience 230V, yielding $I_{kettle} \approx 8.7A$ and $I_{TV} \approx 0.65A$.

If the neutral conductor is broken at the transformer, the circuit topology changes. Appliances on one phase remain in parallel with one another but become in series with the appliances on the other phase; the resulting series–parallel network is exposed to a higher overall supply voltage (approximately 400+ V across the combined loads), and the voltage across individual appliances is determined by the voltage-divider rule.

The bulbs in Figure 5.5 are identical with equal resistances, when connected on a normal electric circuit (LV network) they should be experiencing equal voltages across each one of them, and be drawing currents of equal magnitudes, but because of the broken neutral in Figure 5.5, they are observable to be experiencing different voltages and thus drawing unequal current magnitudes. In the specific case of a TV and an electric kettle connected on opposite phases with no other loads, the two form a series circuit. In a series circuit, the same current flows through all components and is determined by the total resistance; consequently, the current through the kettle would also flow through the TV, potentially exceeding the TV’s design current and leading to damage.

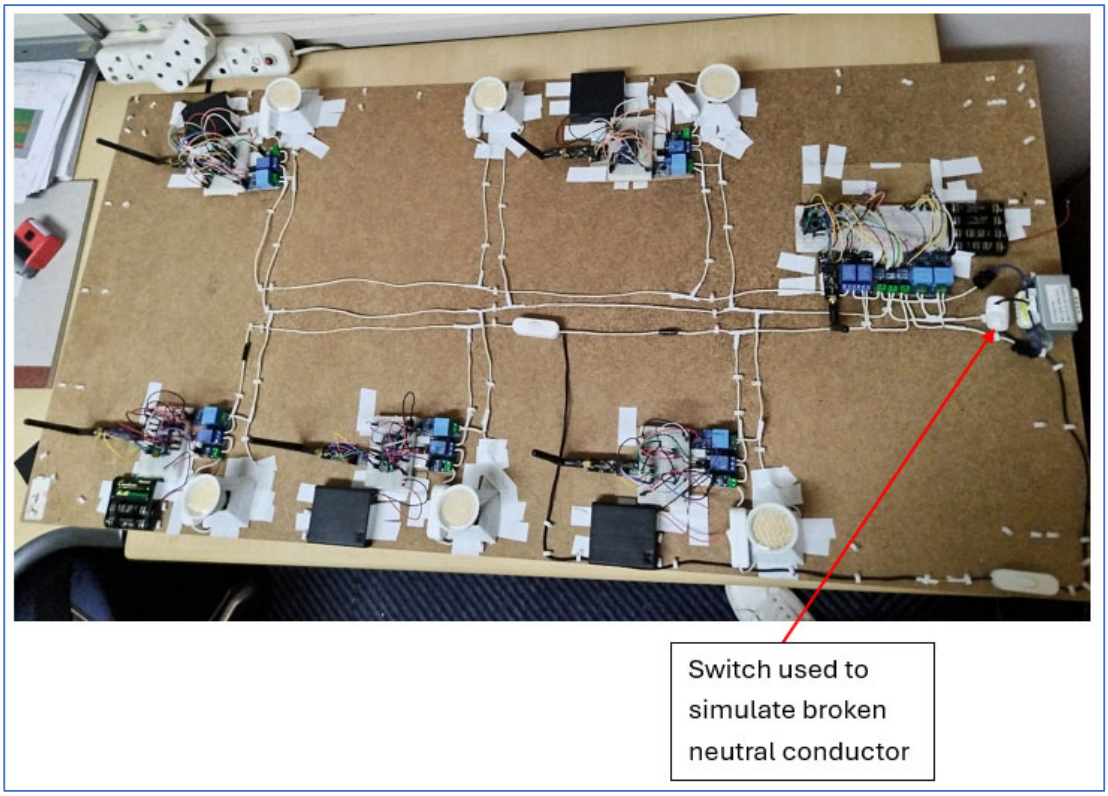

Figure 5.6: **Design of the simulation for broken neutral wire on the smart LV prototype**

Figure 5.6 illustrates the simulation design for a broken neutral conductor in the smart LV network prototype. The prototype incorporates a switch on the neutral wire near the transformer, and when this switch is opened, the neutral path for that transformer is effectively removed. It is noteworthy that a broken neutral does not pose an issue when the loads on the two phases are equal, as the voltage and current are shared symmetrically and no current flows through the neutral. However, in real LV networks, the loads on the two phases are rarely balanced; under such unbalanced conditions, the neutral remains essential for the safety of appliances. Consequently, the voltage dynamics change when the neutral is broken and the phase loads are unequal. To mitigate this fault, the most straightforward approach is to monitor voltage variations. For example, Eskom, the electricity distributor in South Africa, supplies electricity at 230V with an allowable variation of ±5%. This criterion is applied to check the phase voltage near the transformer using voltage sensors. If voltages outside this range are detected, both phase relays are opened, thereby protecting all appliances in the network.

Simulation:

To simulate a broken neutral conductor at the transformer, two bulbs equipped with IoT devices are energized on Phase 1, while one bulb with an IoT device is energized on Phase 2. This configuration created an unbalanced load condition that necessitated a neutral conductor. Subsequently, the switch on the neutral conductor near the transformer is opened to emulate

a broken neutral. Measured data from all IoT devices are recorded in Tables 5.36 to 5.41, and network behaviour is monitored throughout the experiment.

Table 5.36: Data measured at the first pole box on phase 1

Pole Box 1 (Phase 1)	
Current	0.335 A
Voltage	8.010 V
Relay Status	1

Table 5.37: Data measured at the second pole box on phase 1

Pole Box 2 (Phase 1)	
Current	0.334 A
Voltage	8.032 V
Relay Status	1

Table 5.38: Data measured at the third pole box on phase 1

Pole Box 3 (Phase 1)	
Current	0 A
Voltage	8.021 V
Relay Status	1

Table 5.39: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	0.668 A
Voltage	16.021 V
Relay Status	1

Table 5.40: Data measured at the fifth pole box on phase

Pole Box 5 (Phase 2)	
Current	0 A
Voltage	16.023 V
Relay Status	1

Table 5.41: Data measured and received from radio communication at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	0.667 A
Measured Phase 2 Current	0.666 A
Measured Neutral	0 A
Measured Phase 1 Voltage	8.003 V
Measured Phase 2 Voltage	16.012 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.335 A
Received Pole Box 1 Voltage	8.010 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.334 A
Received Pole Box 2 Voltage	8.032 V
Received Pole Box 2 Relay status	1

Received Pole Box 3 Current	0 A
Received Pole Box 3 Voltage	8.021 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.668 A
Received Pole Box 4 Voltage	16.021 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0 A
Received Pole Box 5 Voltage	16.023 V
Received Pole Box 5 Relay status	1

Observations from Table 5.41 show that, although all bulbs have identical resistance and would be expected to draw equal current under normal conditions, the simulated broken-neutral condition results in the bulb energised on phase 2 experiencing a voltage that is double that of the phase-1 bulbs. Consequently, the current through the phase-2 bulb is twice that in each phase-1 bulb, while the two phase-1 bulbs share the current equally. The glow of the bulbs is not uniform, which may lead to damage to the phase-2 bulb. Voltages measured across all IoT devices are abnormal, deviating by ±5% from the nominal 12 V; as a result, all relays tripped, including the two relays on the transformer IoT device, all indicating abnormal voltages.

5.2.4 Data logging to the ThingSpeak platform

The above sections document the completed validation of a smart LV distribution network, including full data exchange on the NAN and demonstrable automation for detecting and isolating abnormalities. The final demonstration focuses on data logging within the ThingSpeak environment, which enables the aggregation, visualization, and analysis of live data streams in a cloud-based platform. ThingSpeak supports the creation of a channel containing up to eight data streams (fields), allowing real-time streaming from up to eight sensors within a single channel (project). Although the LV network contains more sensors, it is not necessary to stream data from every sensor; prioritising data from the sensors located on the transformer pole box suffices, while the remaining fields may be allocated to collect other critical information about the network. The most essential information for assessing the LV distribution network is load profiling, which tracks transformer loading over time to determine whether a transformer should be replaced by a higher-capacity unit or de-loaded to another transformer, a consideration that is crucial for extending the lifespan of LV distribution transformers. Additional fields could be employed to capture the statuses of all relays within the network, enabling monitoring of customers with or without supply due to isolated abnormalities.

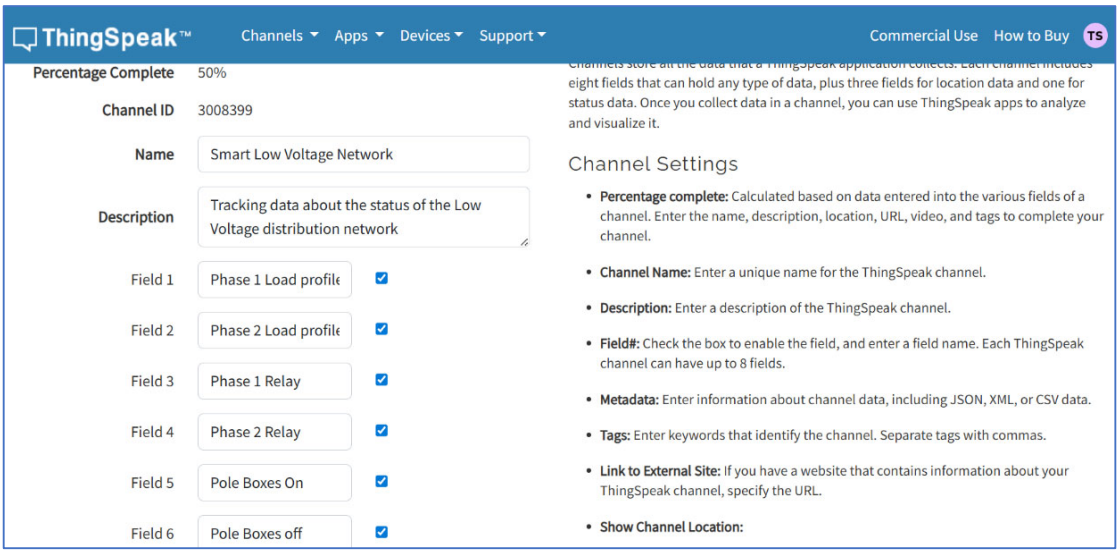

Figure 5.7: ThingSpeak platform demonstrating created fields

The following fields are created (see Figure 5.7): Phase 1 Load Profile; Phase 2 Load Profile; Phase 1 Relay Status; Phase 2 Relay Status; Pole Boxes On; Pole Boxes Off.

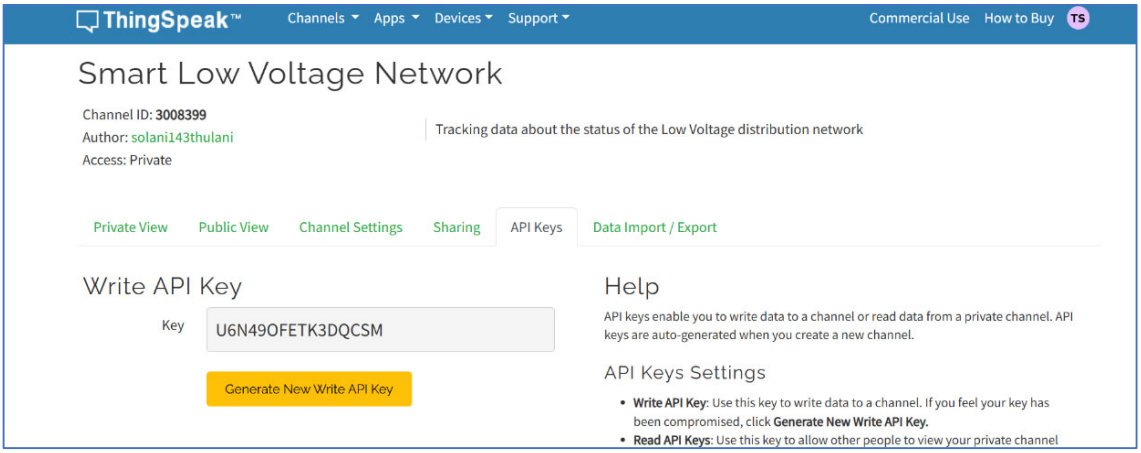

Figure 5.8: API key for writing data into the channel fields

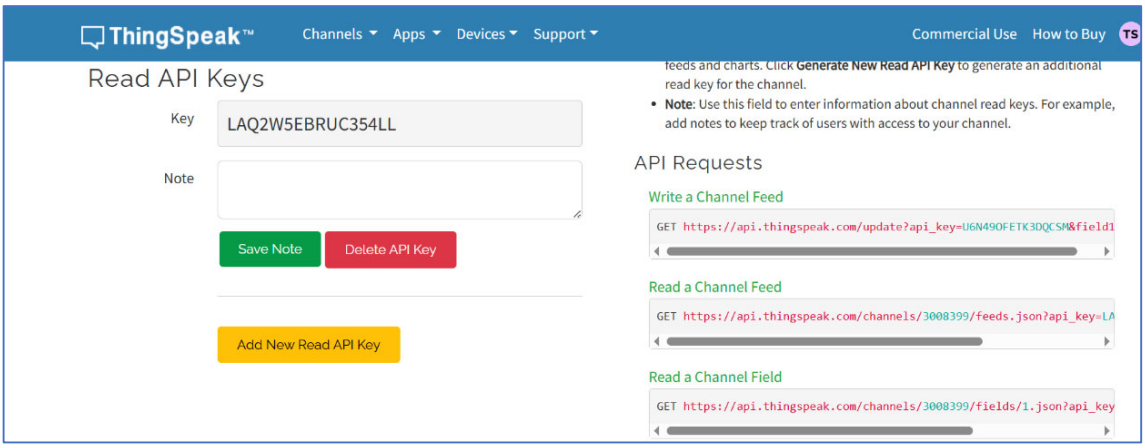

Figure 5.9: API Key for reading data from the channel fields

Figure 5.8 and Figure 5.9 depict the Application Programming Interface (API) keys generated by the ThingSpeak platform for the channel designated to write data to and read data from its fields. APIs function as critical intermediaries that enable interaction and data exchange among disparate software systems. Put simply, an API specifies a set of rules and conventions that govern how software components communicate with one another. These interfaces abstract the complexities of underlying implementations, allowing developers to access functionalities and resources from external systems without needing a detailed understanding of their internal workings. This abstraction supports modularity, reusability, and interoperability—core principles in contemporary software engineering. The widespread adoption of APIs has driven the development of interconnected and extensible software ecosystems, fostering innovation and enabling the creation of novel applications and services (Khazanchi et al., 2020). Within the context of this test, the write API key is the most critical. To transmit data collected at the Transformer IoT device to the ThingSpeak platform, the code running on the transformer must incorporate this write API key. By copying the “Write a channel feed” URL and invoking it in the code with the correct field name, data is continuously streamed from the LV network to the ThingSpeak platform.

5.2.4.1 Case Study: Data logging

Case 1 Data logging: An experimental test is conducted to evaluate data streaming to ThingSpeak. For the test, one IoT-enabled bulb is energised on each electrical phase, resulting in two bulbs being illuminated—namely the bulb connected to Pole Box 1 and the bulb connected to Pole Box 4. Data from the transformer IoT is recorded in Table 5.42, and the corresponding measurements are also observed on the ThingSpeak platform to verify real-time streaming.

Table 5.42: Data measured and received from the radio communication link at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	0.490 A
Measured Phase 2 Current	0.492 A
Measured Neutral	0 A
Measured Phase 1 Voltage	12.549 V
Measured Phase 2 Voltage	12.456 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.492 A
Received Pole Box 1 Voltage	12.476 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0 A
Received Pole Box 2 Voltage	12.543 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0 A
Received Pole Box 3 Voltage	12.489 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.491 A
Received Pole Box 4 Voltage	12.532 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0 A
Received Pole Box 5 Voltage	12.403 V
Received Pole Box 5 Relay status	1

Table 5.42 presents the data measured and received via radio communication at the transformer pole box of the smart LV network prototype. The load profile is derived from the measured phase current and the measured phase voltages at the transformer pole box (see Table 5.42). The power is calculated using the standard formula:

$P = VI$

where P denotes power, V denotes voltage, and I denotes current. The information required for streaming into the designated fields is available from the transformer IoT device, as recorded in Table 5.42. For the purposes of the test, focusing on Phase 1,

$P = V \times I,$

with V = 12.549V and I = 0.490A, yielding:

$P = 6.14901W.$

This represents the power consumed from Phase 1 by the single bulb energised on that phase.

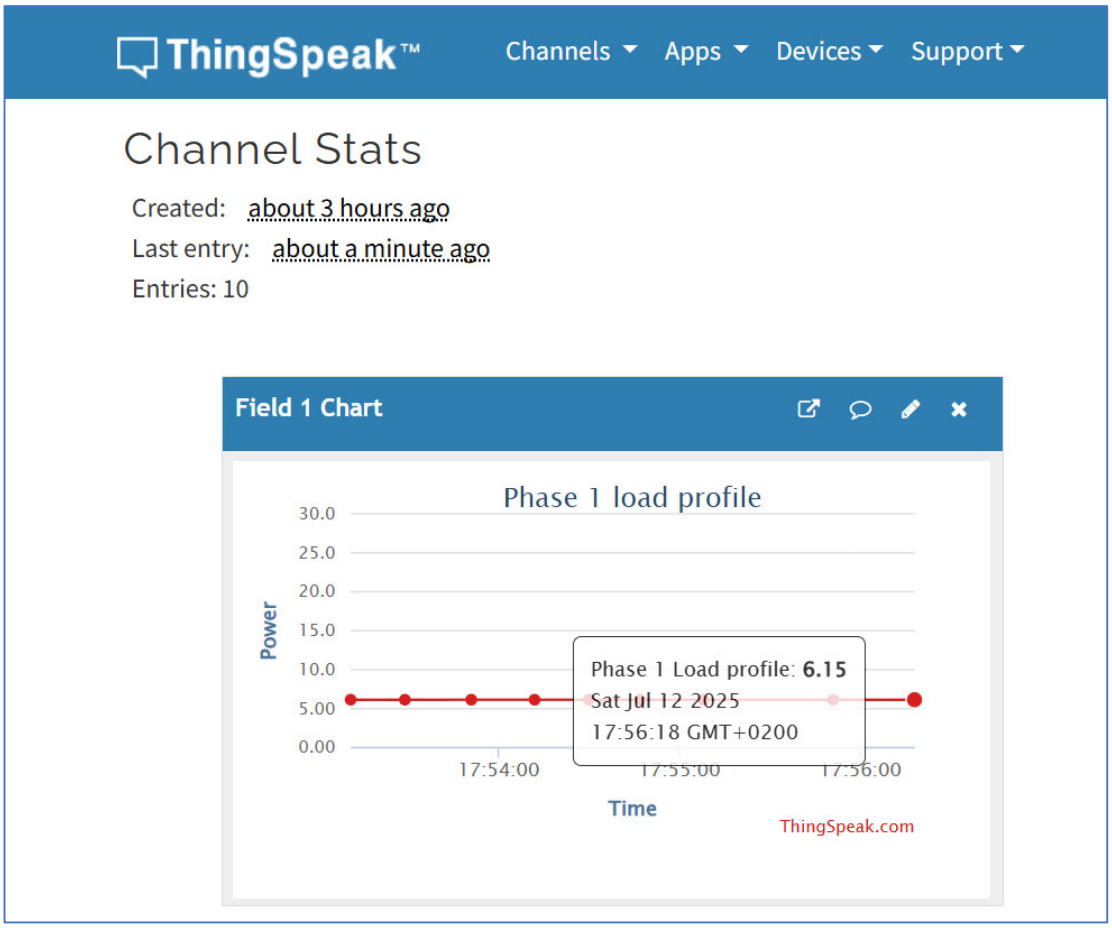

Figure 5.10: Phase 1 load profile loaded on ThingSpeak
(Power consumption for 1 bulb)

Figure 5.10 presents the data uploaded to the ThingSpeak platform and illustrates a graphical load profile of the transformer during Phase 1. The figure comprises ten data entries recorded by the transformer's IoT device and stored in ThingSpeak. The results indicate that the measured power remains constant at 6.15 W over the specified period.

Case 2 Data logging: During the second experimental run, data streaming to ThingSpeak is evaluated for a configuration comprising five IoT-enabled bulbs energized on both electrical phases, with one unauthorized (illegal) connection left de-energized. Data pertaining to the transformer IoT subsystem is recorded in Table 5.43 and subsequently validated on the ThingSpeak platform.

Table 5.43: Data measured and received from radio communication at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	1.502 A
Measured Phase 2 Current	1.023 A
Measured Neutral	0.493 A
Measured Phase 1 Voltage	12.549 V

Measured Phase 2 Voltage	12.456 V
Phase 1 Relay status	1
Phase 2 Relay status	1
Received Pole Box 1 Current	0.492 A
Received Pole Box 1 Voltage	12.476 V
Received Pole Box 1 Relay status	1
Received Pole Box 2 Current	0.491 A
Received Pole Box 2 Voltage	12.543 V
Received Pole Box 2 Relay status	1
Received Pole Box 3 Current	0.501 A
Received Pole Box 3 Voltage	12.489 V
Received Pole Box 3 Relay status	1
Received Pole Box 4 Current	0.492 A
Received Pole Box 4 Voltage	12.532 V
Received Pole Box 4 Relay status	1
Received Pole Box 5 Current	0.501 A
Received Pole Box 5 Voltage	12.203 V
Received Pole Box 5 Relay status	1

Table 5.43 presents the measurements obtained via radio communication at the transformer pole box for the smart LV network prototype. Focusing on the Phase 1 load profile for the test, the real power is computed as

$$P = V \times I$$

with V = 12.549V and I = 1.502A, yielding:

$$P = 18.8485W.$$

This P denotes the real power consumed from Phase 1 by the three bulbs energised on that phase.

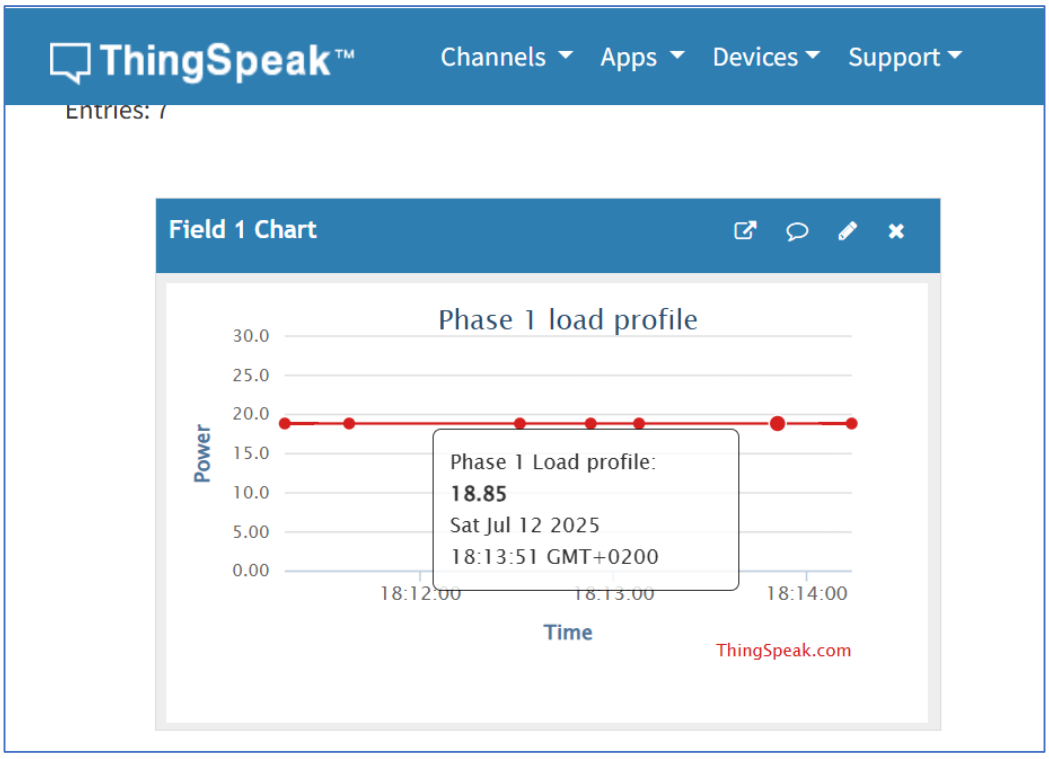

Figure 5.11: **Phase 1 load profile loaded on ThingSpeak (power consumption for 3 bulbs)**

Figure 5.11 below shows the data loaded on ThingSpeak platform, a graphically visualised load profile for the transformer only at phase 1. As can be seen, the Power measured is constant at 18.85W at the given period.

From the 2 demonstrated cases, it is shown that the data from the smart LV network prototype is live streamed into the ThingSpeak platform, through which a graph is drawn to visualise the load profile. This creates a complete visibility of the smart low voltage network prototype.

5.3 Software Simulation testing

Throughout the design and implementation of the smart low-voltage network prototype, simulations and testing of the network are continually conducted using Proteus software to verify the results.

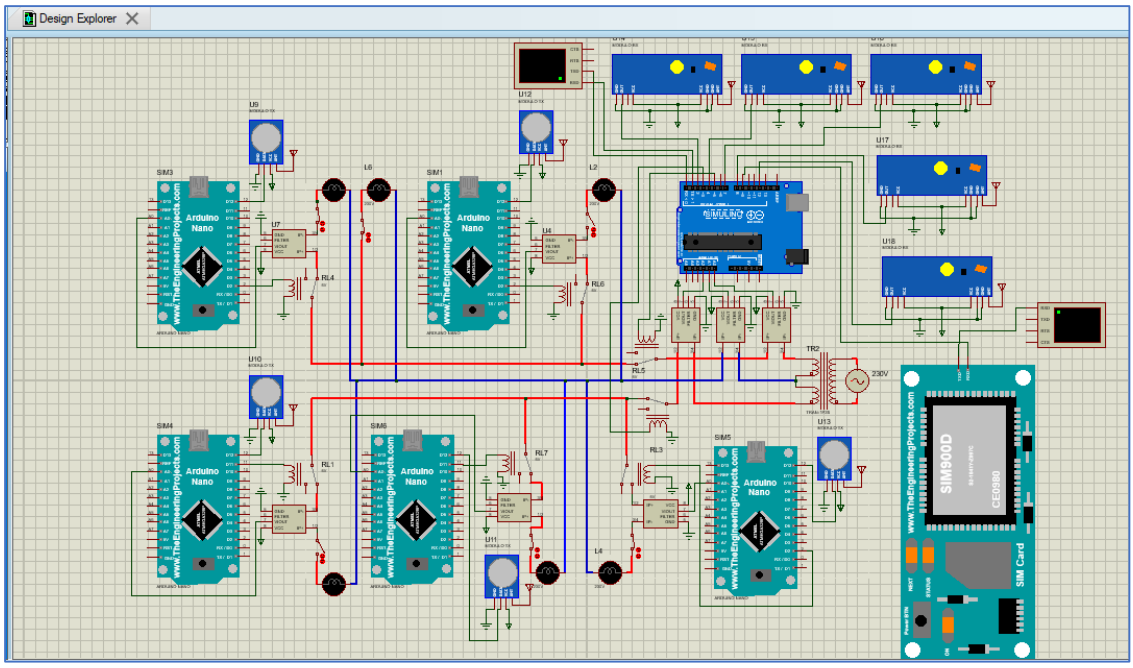

Figure 5.12: Simulation of the Smart low voltage network prototype

This simulation served to verify the underlying assumptions prior to purchasing the components required to build the prototype. A full replica of the prototype is shown in Figure 5.12. All tests conducted on the prototype are replicated and validated using the simulated version implemented in Proteus software. For demonstration purposes, the simulation includes only the current sensors, the relay, and the radio modules; a voltage sensor is not included. Unlike the prototype, the simulated version transmits only current through radio; voltage and relay status are not transmitted.

The transmission of current is demonstrated below. In the final experiment, all five IoT-enabled bulbs are switched on, and an unauthorized connection is introduced. The data is recorded from Tables 5.44 to 5.49.

Table 5.44: Data measured at the first pole box on phase 1

Pole Box 1 (Phase 1)	
Current	1 A

Table 5.45: Data measured at the second pole box on phase 1

Pole Box 2 (Phase 1)	
Current	1 A

Table 5.46: Data measured at the third pole box on phase 1

Pole Box 3 (Phase 1)	
Current	1 A

Table 5.47: Data measured at the fourth pole box on phase 2

Pole Box 4 (Phase 2)	
Current	1 A

Table 5.48: Data measured at the firth pole box on phase 2

Pole Box 5 (Phase 2)	
Current	1 A

Table 5.49: Data measured and received from radio communication at the transformer pole box

Transformer Pole Box	
Measured Phase 1 Current	3 A
Measured Phase 2 Current	3 A
Measured Neutral	0 A
Received Pole Box 1 Current	1 A
Received Pole Box 2 Current	1 A
Received Pole Box 3 Current	1 A
Received Pole Box 4 Current	1 A
Received Pole Box 5 Current	1 A

According to Table 5.49, all currents are successfully transmitted from the pole boxes to the transformer base IoT. The total current at phase 1 equals the sum of currents from pole boxes 1, 2, and 3, i.e.,

1A + 1A + 1A = 3A,

and the current measured at phase 1 near the transformer is 3A.

For phase 2, the total current from pole boxes 4 and 5 is:

1A + 1A = 2A,

while the current measured at phase 2 near the transformer is 3A. The 1 A difference arises due to an illegal connection introduced on phase 2; as a consequence, the relay near the transformer trips and isolates phase 2.

The recorded results indicate that both the simulated version and the prototype behave similarly, with only a minor difference. The simulated version does not incorporate the measurement instrument's error margins. The current measured by the instrument near the transformer in the simulated version matches exactly the current measured by another instrument near the bulbs. The prototype demonstrates that these are ideal conditions; in real life, current sensors cannot always provide identical measurements even when measured

concurrently at the same time and place. Nevertheless, this minor difference does not significantly affect the overall findings of the project.

5.4 Discussion

This study evaluates the design, simulation, and physical prototyping of a smart LV network capable of automatically detecting and disconnecting illicit connections, while also enabling real-time monitoring and enhanced system performance. Testing of both the prototype and its simulated version demonstrated that the smart LV network can detect illegal connections as they arise in LV networks and disconnect the supply to prevent unauthorized electricity usage. Moreover, prototype testing showed that the system can identify a range of other fault types within the LV network. These findings align with the hypotheses articulated in Chapter 1, which stated that:

(i) it is feasible to leverage advancements in smart-grid technology to construct a smart LV network capable of automatically detecting illegal connections and disconnecting supply to eliminate illegal electricity usage;
(ii) modernization of the LV network to a smart configuration will enhance efficiency, enable real-time monitoring, and improve safety; and
(iii) the smart LV network can be simulated and constructed to evaluate its performance in real time.

The design and testing of both the prototype and the simulated version thus support the Chapter 1 hypotheses, indicating that advances in smart grids can be leveraged to develop a smart LV network capable of combating illegal connections. Beyond addressing illegal connections, the implementation of a smart LV network offers a multifaceted approach to enhancing the efficiency, reliability, and safety of LV electricity distribution. Several key benefits are realized through this transition:

Mitigation of Non-Technical Losses (NTL): Smart LV networks provide enhanced monitoring capabilities that enable the identification and remediation of electricity theft, thereby improving revenue collection and grid stability.

Extended Transformer Lifespan: Continuous monitoring of transformer loading and surge arrestor performance allows for proactive identification of potential overload or stress conditions, enabling timely intervention and extending the operational life of transformers.

Enhanced LV Network Fault Management: Automation of LV network functions reduces the frequency of faults and outages by minimizing the need for manual circuit breaker resets, improving service continuity and reducing downtime.

Reduced Liability and Improved Appliance Protection: Proactive monitoring and detection of neutral-wire integrity mitigate voltage imbalances and overvoltage conditions, protecting customer appliances and reducing liability claims associated with damaged equipment.

Improved Customer Satisfaction: Real-time fault reporting, proactive fault detection, and enhanced communication channels contribute to a more transparent and responsive customer experience.

Enhanced Safety and Fault Isolation: Automated systems improve safety by detecting and isolating broken wires in real time, reducing electrical hazards and enhancing overall network safety.

Facilitation of Efficient Fault Finding: Comprehensive performance data and advanced analytics support rapid fault localization and diagnosis, shortening troubleshooting time and improving restoration efforts.

Data-Driven Decision Making: Rich, granular network data enable informed decision-making for future grid planning and optimization, guiding targeted upgrades and improvements for more efficient and sustainable operations.

5.5 Conclusion

This chapter reports the empirical evaluation of the smart LV network prototype and the validation of its corresponding simulation model. The experimental sequence begins with energising the prototype, followed by systematic testing of the implemented algorithms and remediation of observed deficiencies. It then presents a series of case studies designed to assess (i) the detection and elimination of illegal connections, (ii) the detection and isolation of a broken conductor fault, (iii) the detection and elimination of a broken neutral conductor at the transformer, and (iv) the logging of LV-network data on the ThingSpeak platform. A parallel version of the LV network was also simulated and tested using Proteus software, with the results discussed subsequently. The empirical results demonstrate the prototype's operational efficacy, thereby supporting the principal hypothesis articulated in Chapter 1. Specifically, the findings illustrate the feasibility of leveraging advances in smart-grid technology to develop a comprehensive smart LV network capable of mitigating the incidence of unauthorized electrical connections. Beyond this primary objective, the implementation yields ancillary benefits, including improved monitoring and data analytics, enhanced reliability, and potential scalability and integration with broader grid-management systems.

Chapter Six presents the dissertation's final conclusions, including the objectives achieved, the deliverables produced, and the overarching conclusions.

6. CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Introduction

The current power grid is relatively “smart” given the amount of intelligent devices with communication and computation capabilities. However there is a need for an even “smarter grid” with better energy production methods, storage capacity for renewables sources and distribution of electricity. The world is moving toward a green-energy future underpinned by environmentally friendly power generation, which heightens the importance of optimizing power grids to operate as efficiently as possible for a sustainable energy future. A major component of grid optimization and efficiency initiatives is the reduction of losses in electricity networks. Among these losses, electricity theft represents one of the most significant challenges to grid security and efficiency. This smart grid technology project aims to address these problems by optimizing the electricity grids and enhancing their overall efficiency. Currently, governmental strategies are best served by adopting smart grids in place of conventional electrical grids. The digital communication networks form the backbone of the Smart grid, as without them it would be impossible to continually monitor and analyse the power system. Leveraging the Internet of Things (IoT) capabilities provides added functionality to existing smart grids. The purpose of this research is to design and implement a smart low-voltage distribution network to combat electricity theft by exploiting an IoT architecture.

This chapter presents the deliverables and conclusions of the dissertation. Section 6.2 outlines the aims of the research as described in Chapter 1. Section 6.3 details the deliverables and the objectives that are achieved. Section 6.4 discusses future work on the project. Section 6.5 presents publications related to the study. Section 6.6 provides the conclusion to this work.

6.2 Aim and Objectives

6.2.1 Aim of the dissertation

The aim of this study is to design, develop, and implement a smart low-voltage (LV) distribution network monitoring and control system grounded in an IoT architecture. The primary goals are to mitigate electricity theft and to enhance protection, automation, and control of LV networks.

Specifically, the work seeks to:

- Architect an integrated IoT-enabled monitoring framework capable of real-time data acquisition, communication, and analytics across LV feeders;
- Implement robust anti-theft mechanisms through advanced metering, anomaly detection, and secure data credentials; and
- Improve protection coordination and automated control strategies to increase reliability, efficiency, and safety in LV distribution systems.

The anticipated outcome is a validated prototype and accompanying methodological framework that can be deployed to reduce non-technical losses and bolster grid resilience.

6.2.2 Objectives

The aim is attained through theoretical derivations and practical implementation.

6.2.2.1 Objectives: Theoretical analysis

- To conduct a literature review on existing solutions for combating illegal connections
- To investigate the implementation of an IoT architecture
- To develop a mathematical model for the proposed system

6.2.2.1 Objectives: Practical implementation

- To simulate the proposed system within Proteus simulation software
- To analyse the working of the proposed system on the simulation using cases
- To build a lab scale prototype of the proposed system
- To test the working of the proposed system using cases
- To test and validate of the prototype with the simulated results by comparing the responses on the cases

6.3 Dissertation deliverables

This dissertation deliverables are further discussed in the following sections.

6.3.1 Literature Review

The literature review examined electricity theft, with particular emphasis on illegal connections, and surveyed the causes, impacts, and countermeasures described in the extant body of research. The synthesis reveals that, despite considerable attention to the problem, there is no widely utilized method to combat electricity theft that substantially reduces the resource burden on utility companies. Most proposed solutions focus on detection but still require utility-led inspections and disconnections, processes that are both time-consuming and resource-intensive. Consequently, the literature indicated a gap in scalable, proactive, or automated interventions that minimize reliance on direct utility involvement while effectively curbing theft and its broader consequences.

6.3.2 Overview of the current state of the low voltage networks

The thesis provided a brief overview of the current state of LV distribution networks. It highlighted the principal problems arising from the networks' current design, including electricity theft and other general faults. The analysis emphasized the need for a redesign or rapid development of the LV distribution system to align with the latest smart-grid developments, thereby improving reliability, efficiency, and resilience.

6.3.3 Theoretical development behind the current flow in an LV network

The current flow in LV distribution networks is analysed in detail. This analysis relies on Kirchhoff's Current Law (KCL) to establish the theoretical framework. From these findings, conclusions are drawn that proved instrumental in the development of algorithms for designing smart LV networks. The conclusions reveal a considerable degree of predictability in LV current flow under normal operating conditions. When monitored in real time, this predictability enables the rapid detection of faults, including instances of illegal connections.

6.3.4 Developed smart low voltage network concept

An integrated concept is developed outlining a system in which IoT devices are deployed at strategic locations within LV distribution networks. Through these IoT devices, currents and voltages on LV networks can be monitored for abnormal conditions, leveraging algorithms derived from theory discussed previously, which demonstrated the predictability of current and voltage behaviour in LV networks under normal operating conditions. The proposed framework enhances observability, fault detection, and proactive maintenance, with the aim of improving reliability and efficiency of the LV distribution system.

6.3.5 Prototype and simulation design

Building on the developed concept, a lab-scale prototype of a smart low-voltage network is designed and constructed, complemented by a simulation of the network conducted in Proteus software. Through the integrated use of the prototype and simulation, the objective is to observe the concept in operation and to determine whether the system functioned as hypothesized in the report.

6.3.6 Testing and results

An empirical evaluation of both the prototype and its corresponding simulation is conducted. The results indicate that the smart LV network prototype operates as intended and aligns with the hypothesized objectives. The findings demonstrate the feasibility of deploying the system on a large scale and suggest that its implementation can yield substantial improvements in the performance and modernization of existing low-voltage distribution networks. These outcomes support the potential for broader deployment and warrant further pilot studies to validate long-term performance under real-world conditions.

6.4 Future work

Following the presentation of the smart low-voltage network prototype at the Eskom Distribution Innovation and Excellence Conference, held at the Eskom Academy of Learning (EAL) in Johannesburg in July 2024, the South African power utility company Eskom expressed interest in providing funding for further development and pilot implementation within its distribution infrastructure. Consequently, a subsequent meeting was scheduled with the Eskom Funding Committee in June 2025 for a second presentation and demonstration. During this meeting, Eskom formally approved funding for the development and construction of the network, thereby enabling a pilot program within one of Eskom's existing low-voltage networks.

6.5 Publications related to the thesis

- Solani T., Kriger C., Mfoumboulou Y.D, (2025). “Smart monitoring of low voltage networks to combat illegal electricity connections”. The Institution of Engineering and Technology (IET) Smart Grid (submitted for publication)
- Solani T., Kriger C., Mfoumboulou Y.D, (2025). “The unintended consequences of smart prepaid split meters: The Eskom maintenance and operations Case Study”. Submitted to the Southern African Universities Power Engineering Conference (submitted for publication).

6.6 Conclusion

This chapter outlines the aim and objectives of the dissertation and demonstrates how they are achieved. It also documents the deliverables produced by the research. The discussion looks ahead to prospective future developments of the project, centred on the development of a pilot deployment in collaboration with Eskom, the South African electricity public utility. Submitted publications emanating from this research work are presented. Finally, the conclusion is presented.

BIBLIOGRAPHY/REFERENCES

A. A. Chauhan, "Non-Technical Losses in Power System and Monitoring of Electricity Theft over Low-Tension Poles," 2015 Second International Conference on Advances in Computing and Communication Engineering, 2015, pp. 280-284, doi: 10.1109/ICACCE.2015.106.

A. H. Zemanian, "The validity of Kirchhoff's laws for a class of nonlinear transfinite networks," in IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 7, pp. 477-482, July 1993, doi: 10.1109/81.257303.

A. Regmi, “Wireless Communication Solutions for Smart Grid and Industrial Environments,” PY - 2015/07/3, research gate.

A. Shah, W. Mesbah and A. T. Al-Awami, "An Algorithm for Detaching Technical Losses from Non-Technical Losses in Distribution Systems," 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2021, pp. 1-5, doi: 10.1109/ISGT49243.2021.9372255.

Acevedo Parra, J., & Sainchez Calderon, E. (2006). Use of the Shunts Detecting Equipment for the Identification of Illegal Power Outlets. 2006 IEEE/PES Transmission & Distribution Conference and Exposition: Latin America, 1–4. https://doi.org/10.1109/TDCLA.2006.311412

Ankit Negi. (2024). nRF24L01 pinout, features, specs, working and Arduino connections. https://www.etechnophiles.com/nrf24l01-pinout-features-specs-working-and-arduino-connections/

Arduino. (2025). Arduino - Home. https://www.arduino.cc/

Arora, P. (2025). COP29: achieving net zero through financial sustainability. Environmental Sustainability, 8(1), 121–126. https://doi.org/10.1007/s42398-025-00337-z

Babu, P. R., & Sushma, B. (2013). Operation and control of electrical distribution system with extra voltage to minimize the losses. 2013 International Conference on Power, Energy and Control (ICPEC), 165–169. https://doi.org/10.1109/ICPEC.2013.6527643

Babu, P. R., Sushma, B., & Ashwin, K. B. (2012). HVDS approach for reducing the Technical and Non-technical losses to enhance the electrical distribution system performance. 2012 IEEE 5th India International Conference on Power Electronics (IICPE), 1–5. https://doi.org/10.1109/IICPE.2012.6450382

Basak, R., Pal, I., Bandyopadhayay, A., & Guha, T. (2019). IOT Based Drone Operated Monitoring Of Distribution Transformers and Terminating Illegal Power Connections. 2019 3rd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), 1–5. https://doi.org/10.1109/IEMENTech48150.2019.8981224

Bastos, L., Martins, B., Medeiros, I., Rosário, D., Aquino, A., & Cerqueira, E. (2023). Energy Frauds Characterization based on Information Theory Quantifiers. 2023 International Wireless Communications and Mobile Computing, IWCMC 2023, 1196–1201. https://doi.org/10.1109/IWCMC58020.2023.10182829

c3controls. (2025). Basics of Contactors: Comprehensive Guide | c3controls - c3controls. https://www.c3controls.com/white-paper/basics-of-contactors/

Cameron Hashemi-Pour, & Ben Lutkevich. (2024). What is a Microcontroller? | Definition from TechTarget. https://www.techtarget.com/iotagenda/definition/microcontroller

Carolyn Mathas. (2012, September). The Basics of Current Sensors | DigiKey. https://www.digikey.co.za/en/articles/the-basics-of-current-sensors?srsltid=AfmBOoqdRfTuNveRzA5Xcg5nkVv2R3NCsr7mwjecffnnvZvuzQ8Rtf5F

Clinton Carter-Brown. (2003). .2 Reticulation Network Classes.

Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, IcABCD 2020 - Proceedings. https://doi.org/10.1109/icABCD49160.2020.9183851

D. -J. Ventruella, "Transformer Fuses—Mind the Gap," in IEEE Transactions on Industry Applications, vol. 56, no. 5, pp. 5670-5677, Sept.-Oct. 2020, doi: 10.1109/TIA.2020.2993523.

Dav, D. (2020). Arduino Nano Tutorial [Pinout] - DIYI0T. https://diyi0t.com/arduino-nano-tutorial/

Dejan. (2017). nRF24L01 – How It Works, Arduino Interface, Circuits, Codes. https://howtomechatronics.com/tutorials/arduino/arduino-wireless-communication-nrf24l01-tutorial/

Dejan. (2018). Arduino Wireless Network with Multiple NRF24L01 Modules. https://howtomechatronics.com/tutorials/arduino/how-to-build-an-arduino-wireless-network-with-multiple-nrf24l01-modules/

EFY Bureau. (2023). GPRS/GSM Module Made Easy: Working, AT Commands, and Uses 101 Explained. https://www.electronicsforu.com/resources/gsm-module

EG Projects. (2023). How to measure current using Arduino and ACS712 current sensor. https://www.engineersgarage.com/acs712-current-sensor-with-arduino/

Electrical4U. (2024, May 9). Voltage Sensor: What is it And How Does it Work? (Circuit Diagram Included) | Electrical4U. Electrical4U. https://www.electrical4u.com/voltage-sensor/

Electronics Clinic. N.d. an online website, available at: Nrf24l01 two way communication Archives - Electronic Clinic (electroniclinic.com)

Electronics Tutorials. (2025). RMS Voltage of a Sinusoidal AC Waveform. https://www.electronics-tutorials.ws/accircuits/rms-voltage.html

Eskom. (2015). 2015_Annual_Report: https://www.eskom.co.za/heritage/wp-content/uploads/2024/03/2015_Annual_Report.pdf

Eskom. N.d. an online website available at: Home - Distribution (eskom.co.za)

Evaldt, M. C., dos Santos, J. V. C., Figueiredo, R. M., da Silva, L. T., & Stracke, M. R. (2012). Payback analysis in identification and monitoring of commercial losses in distribution networks. 2012 9th International Conference on the European Energy Market, 1–6. https://doi.org/10.1109/EEM.2012.6254694

F. Aslam, A. Nasser, E. Ulhaq and A. Umar, "Intelligent Modeling Scheme for Detection of Line Losses in Power Distribution System," 2013 UKSim 15th International Conference on Computer Modelling and Simulation, 2013, pp. 218-223, doi: 10.1109/UKSim.2013.43.

Fulchiron, D. (1998). Cahier technique no. 192 Protection of MV/LV substation transformers. http://www.schneider-electric.com

G. Bianco et al., ""SMART STREET BOX": AN INNOVATIVE APPROACH TO REMOTE CONTROL, MONITORING & AUTOMATION FOR LV SMART GRIDS," CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution, 2021, pp. 1687-1691, doi: 10.1049/icp.2021.1747.

G. Dudek, A. Gawlak, M. Kornatka and J. Szkutnik, "The Method of Detecting Illegal Electricity Consumption Using the AMI System," 2018 15th International Conference on the European Energy Market (EEM), 2018, pp. 1-5, doi: 10.1109/EEM.2018.8470006.

Hzajkani. (2017). Help me for my NRF24L01 Problem !! :\ - Projects / Networking, Protocols, and Devices - Arduino Forum. https://forum.arduino.cc/t/help-me-for-my-nrf24l01-problem/444553

J. D. Glover, M. S. Sarma, T. J. Overbye 2012. Power System Analysis and Design, 5th addition

J. Romero Agüero, "Improving the efficiency of power distribution systems through technical and non-technical losses reduction," PES T&D 2012, 2012, pp. 1-8, doi: 10.1109/TDC.2012.6281652.

Josh Schneider, & Ian Smalley. (2024, June 4). What is a microcontroller? | IBM. https://www.ibm.com/think/topics/microcontroller

K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "Concept and Hardware Considerations for Product-Service System Achievement in Internet of Things," 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 2019, pp. 1-6, doi: 10.1109/WITS.2019.8723755.

K. Pauline N., N. Livingstone and M. James, "Embedded Power System Monitoring Of Illegal Power Connections In Kenyan Domestic Supply," 2020 IEEE PES/IAS PowerAfrica, 2020, pp. 1-5, doi: 10.1109/PowerAfrica49420.2020.9219799.

Khan, F., Nasser, A., Ulhaq, E., & Umar, A. (2013). Intelligent modeling scheme for detection of line losses in power distribution system. Proceedings - UKSim 15th International Conference on Computer Modelling and Simulation, UKSim 2013, 218–223. https://doi.org/10.1109/UKSim.2013.43

Korovkin, N. V., Minevich, T. G., & Bodrenkov, E. A. (2021). Determination of Consumer Powers by Measurements at the Supply Feeder Ends. Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, 1454–1457. https://doi.org/10.1109/ElConRus51938.2021.9396318

L. M. R. Raggi, F. C. L. Trindade, V. C. Cunha and W. Freitas, "Non-Technical Loss Identification by Using Data Analytics and Customer Smart Meters," in IEEE Transactions on Power Delivery, vol. 35, no. 6, pp. 2700-2710, Dec. 2020, doi: 10.1109/TPWRD.2020.2974132.

Last Minute Engineers. (2023). In-Depth: How nRF24L01 Wireless Module Works & Interface with Arduino. https://lastminuteengineers.com/nrf24l01-arduino-wireless-communication/

Last Minute Engineers. (2025). In-Depth: Interface One Channel Relay Module with Arduino. https://lastminuteengineers.com/one-channel-relay-module-arduino-tutorial/

Last minute Engineers. N.d. an electronics website, available at: In-Depth: How nRF24L01 Wireless Module Works & Interface with Arduino (lastminuteengineers.com)

Last Minutes Engineers. (2024). In-Depth: Send Receive SMS & Call with SIM900 GSM Shield & Arduino. https://lastminuteengineers.com/sim900-gsm-shield-arduino-tutorial/

M. Lanphier, P. K. Sen and J. P. Nelson, "An Update on Surge Protection of Medium Voltage Motors: A Comparison of the Standards and Applications," 2007 4th European Conference on Electrical and Instrumentation Applications in the Petroleum & Chemical Industry, Paris, France, 2007, pp. 1-8, doi: 10.1109/PCICEUROPE.2007.4353996.

M. M. Ahmed, "Electrical Distribution Automation System for Low Voltage (LV) System," 2006 IEEE International Power and Energy Conference, 2006, pp. 543-548, doi: 10.1109/PECON.2006.346711.

Mamtaz Alam. (2022). Send GSM SIM800/900 GPRS Data to Thingspeak with Arduino. https://how2electronics.com/send-gsm-sim800-900-gprs-data-thingspeak-arduino/

Medrado R, Silva L, Soto Marambio J, da Rocha Cavalcanti K, de Lima Santos Ede Carvalho Santos M, Moreira F, Rego D, “Illegal connection location on distribution lines using traveling waves method," 2016 51st International Universities Power Engineering Conference (UPEC), 2016, pp. 1-6, doi: 10.1109/UPEC.2016.8114050.

Mike Grusin. (2025). Serial Peripheral Interface (SPI) - SparkFun Learn. https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi/all

Mithun Subbaroybhat. (2023, June 17). Everything You Need to Know About Microcontrollers | RS. https://uk.rs-online.com/web/content/discovery/ideas-and-advice/microcontrollers-guide

Mohammadreza Akbari. (2020). Interfacing ZMPT101B Voltage Sensor with Arduino [full guide]. https://electropeak.com/learn/interfacing-zmpt101b-voltage-sensor-with-arduino/?srsltid=AfmBOorbMDLfekrTCDDQpGeqkF81UP6mNQFZ6F_l0dvaV7RXKliFLEoH

Mohammadreza Akbari. (2020). Interfacing ZMPT101B Voltage Sensor with Arduino [full guide]. https://electropeak.com/learn/interfacing-zmpt101b-voltage-sensor-with-arduino/?srsltid=AfmBOorWlPnUJavLUEaimKj85MSfWLQ5WGiPUoSbvRE42abHynX79akj

MPS. (2025). Current Sensors: Types, Key Parameters, Performance Comparison, and Common Applications | Article | MPS. MPS. https://www.monolithicpower.com/en/learning/resources/current-sensors-types-key-parameters-performance-comparison-and-common-applications

N. Penner, A. L. Bettiol, J. A. Cortina, L. F. d. N. Passos, A. Carniato and R. P. Martin, "Equipment for monitoring and combating of non-technical losses in distribution networks: Design and preliminary results," 2014 49th International Universities Power Engineering Conference (UPEC), 2014, pp. 1-4, doi: 10.1109/UPEC.2014.6934592.

Ndlovu, S., Mudali, P., & Oki, O. A. (2020, August 1). Evaluating the energy efficiency of s of tware defined networking controllers for different topologies. 2020 International

Neagu, B. C., Grigoras, G., & Scarlatache, F. (2018). Influence of Outliers on Transformer Power Losses Estimation Using a Statistical Based Data Mining Approach. 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 1–4. https://doi.org/10.1109/ECAI.2018.8679002

NK Technologies. (2025). Current Sensing Theory | NK Technologies. https://www.nktechnologies.com/engineering-resources/current-sensing-theory/

OMRON. (2025). What is an Electrical Relay? | OMRON Device & Module Solutions - Americas. https://components.omron.com/us-en/products/basic-knowledge/relays/basics
Pavic, A., Stojkov, M., & Trupinic, K. (2004). Illegal Connection Location on Main Power Cable.

Pealy, S., & Matin, M. A. (2021). Tackling Energy Theft in Smart Grid-A Comprehensive Review and Framework. Proceedings - 2021 International Conference on Control, Automation, Power and Signal Processing, CAPS 2021. https://doi.org/10.1109/CAPS52117.2021.9730689

Peňa and Legaspi. (2020). UART: A Hardware Communication Protocol Understanding Universal Asynchronous Receiver/Transmitter | Analog Devices. https://www.analog.com/en/resources/analog-dialogue/articles/uart-a-hardware-communication-protocol.html

Q. Louw and P. Bokoro, "An Alternative technique for the detection and mitigation of electricity theft in South Africa," in SAIEE Africa Research Journal, vol. 110, no. 4, pp. 209-216, December 2019, doi: 10.23919/SAIEE.2019.8864147

R. Alves, P. Casanova, E. Quirogas, O. Ravelo and W. Gimenez, "Reduction of Non-Technical Losses by Modernization and Updating of Measurement Systems," 2006 IEEE/PES Transmission & Distribution Conference and Exposition: Latin America, 2006, pp. 1-5, doi: 10.1109/TDCLA.2006.311590.

Ran Li, Xiaobo Zhang, Qi Zhao and Guowei Liu, "Economic optimization of self-healing control of power grid based on multi-agent system," 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016, pp. 1334-1337, doi: 10.1109/IMCEC.2016.7867429.

Raspberry Pi. (2025). Pico-series Microcontrollers - Raspberry Pi Documentation. https://www.raspberrypi.com/documentation/microcontrollers/pico-series.html
Rockwell Automation. (2025). What Is A Voltage Sensor? | Glossary | Fiix. https://fiixsoftware.com/glossary/what-is-a-voltage-sensor/

RS Components. (2023). A Complete Guide to Contactors. https://uk.rs-online.com/web/content/discovery/ideas-and-advice/contactors-guide

Shahinzadeh, H., Moradi, J., Gharehpetian, G. B., Nafisi, H., & Abedi, M. (2019). IoT Architecture for smart grids. International Conference on Protection and Automation of Power System, IPAPS 2019, 22–30. https://doi.org/10.1109/IPAPS.2019.8641944

Shahzada Fahad. (2021). NRF24L01 Multiple Transmitters and Single Receiver for Sensor Monitoring using Arduino. https://www.electroniclinic.com/nrf24l01-multiple-transmitters-and-single-receiver-for-sensor-monitoring-using-arduino/

Sharma, K., Malik, A., & Isha. (2021). An Efficient IoT Based Electricity Theft Detecting Framework for Electricity Consumption. Proceedings - 2021 International Conference on Computing Sciences, ICCS 2021, 244–248. https://doi.org/10.1109/ICCS54944.2021.00055

T. W. Mennell, "Protection of LV networks," IEE Colloquium on Protection of Industrial Networks (Digest No: 1997/097), London, UK, 1997, pp. 1/1-1/8, doi: 10.1049/ic:19970551.

Tarantula. (2025). Driving a Relay With an Arduino : 9 Steps - Instructables. https://www.instructables.com/Driving-a-Relay-With-an-Arduino/

The electricity Forum. n.d. an online website, available at: Power System Training - The Electricity Forum (EFTI)

ThingSpeak. (2025). Sign In - ThingSpeak IoT. https://thingspeak.mathworks.com/login?skipSSOCheck=true

Trupinic, K., Stojkov, M., & Poleto, D. (2005). Reduction of non-technical losses based on time domain reflectometer (TDR) principles and function. 18th International Conference and Exhibition on Electricity Distribution (CIRED 2005), v5-85-v5-85. https://doi.org/10.1049/cp:20051367

Usman ali Butt. (2024). Non-invasive current sensor with Arduino. https://www.engineersgarage.com/non-invasive-current-sensor-with-arduino/
W. Hauer and M. Bartonek, "A novel low voltage grid protection component for future smart grids," 2016 51st International Universities Power Engineering Conference (UPEC), 2016, pp. 1-6, doi: 10.1109/UPEC.2016.8114141.

W. Xie, "Application of Relay in Low Voltage Apparatus of Electrical Engineering Automation," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 343-347, doi: 10.1109/ICCES51350.2021.9488964.

Weckx, S., Gonzalez, C., Tant, J., De Rybel, T., & Driesen, J. (2012). Parameter identification of unknown radial grids for theft detection. 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), 1–6. https://doi.org/10.1109/ISGTEurope.2012.6465644

Williams, D. O., Li, Z. S., & Ghanavati, A. (2023). Mitigating Electrical Losses Through a Programmable Smart Energy Advanced Metering Infrastructure System. 2023 IEEE International Conference on Prognostics and Health Management, ICPHM 2023, 153–157. https://doi.org/10.1109/ICPHM57936.2023.10194102

Y. Qianjun, W. Guichu, Y. Fenqun and X. Hongyan, "Design and applications of intelligent low voltage distribution system based on ZigBee," 2011 International Conference on Electronics, Communications and Control (ICECC), 2011, pp. 791-794, doi: 10.1109/ICECC.2011.6066383.

Yang, F., Wu, Y., Rong, M., Sun, H., Murphy, A. B., Ren, Z., & Niu, C. (2013). Low-voltage circuit breaker arcs - Simulation and measurements. In Journal of Physics D: Applied Physics (Vol. 46, Issue 27). https://doi.org/10.1088/0022-3727/46/27/273001

Yuan-Liang Lo, Shih-Che Huang and Chan-Nan Lu, "Non-technical loss detection using smart distribution network measurement data," IEEE PES Innovative Smart Grid Technologies, 2012, pp. 1-5, doi: 10.1109/ISGT-Asia.2012.6303316.

Zulu, C. L., & Dzobo, O. (2021). Design of electric meter with double connected data capture system for energy theft monitoring. IEEE AFRICON Conference, 2021-September. https://doi.org/10.1109/AFRICON51333.2021.9570859

APPENDICES

A. APPENDIX A: NRF24L01 RADIO MODULE

Appendix A4.1: NRF24L01 Radio module operation

Wireless communication among two or more microcontrollers expands the range of potential applications to include home automation, robotic control, and remote monitoring of sensor data. When comparing two-way RF solutions, the Nordic Semiconductor nRF24L01+ transceiver is frequently highlighted for offering a favourable balance between cost and reliability. Reports indicate that the nRF24L01+ is among the most economical data-connection options available, with online prices cited as starting below forty rand.

Radio Frequency

The nRF24L01+ transceiver transmits data using Gaussian Frequency Shift Keying (GFSK) modulation and is designed to operate within the 2.4 GHz global Industrial, Scientific, and Medical (ISM) frequency band. Its data transfer rate is configurable to 250 kbps, 1 Mbps, or 2 Mbps, allowing versatility for a range of applications. The 2.4 GHz spectrum is globally allocated as an ISM band for unlicensed, low-power devices. ISM frequencies are utilized by a variety of technologies, including Bluetooth, cordless telephones, Near Field Communication (NFC) devices, and Wi-Fi networks.

Power

The module operates over a supply voltage range of 1.9 to 3.9 V. Notably; no logic level translator is required because the logic ports are 5-V tolerant even when powered within this range. Output power can be configured to 0 dBm, -6 dBm, -12 dBm, or -18 dBm. Transmission at 0 dBm draws 12 mA, which is less than the current typically required by a single LED. In standby mode, the device consumes 26 µA, and in power-down mode, 900 nA. Collectively, these low-power characteristics position the module as a preferred wireless solution for low-power applications.

SPI Interface

The nRF24L01+ transceiver communicates with a host microcontroller via a four-pin Serial Peripheral Interface (SPI). Through this SPI interface, the device can be configured to operate with specific RF characteristics, including 125 selectable frequency channels, output power levels of 0 dBm, −6 dBm, −12 dBm, or −18 dBm, and RF data rates of 250 kbps, 1 Mbps, or 2 Mbps. In SPI terminology, the microcontroller acts as the master that initiates and controls data transfers, while the nRF24L01+ functions as the slave that responds to the master’s commands.

The SPI bus is inherently a multi-slave protocol; each slave device is selected via a dedicated chip-select line, enabling a single master to manage multiple slaves. Consequently, the

practical number of slaves is determined by the available chip-select resources on the host microcontroller. As noted by Last Minute Engineers (2023), a typical configuration can support up to two SPI slaves (e.g., two nRF24L01+ modules), though in practice the number of slaves can exceed two provided sufficient chip-select lines are available.

nRF24L01+ module and nRF24L01+ PA/LNA module

Numerous modules utilize the nRF24L01+ transceiver, among which two have emerged as particularly prevalent. The first module is comparatively compact due to its integrated on-board antenna; however, the reduced size is associated with a diminished transmission range. In open, line-of-sight conditions, this module can achieve a communication range of approximately 100 meters, whereas indoor environments impose a shorter range, primarily due to wall attenuation.

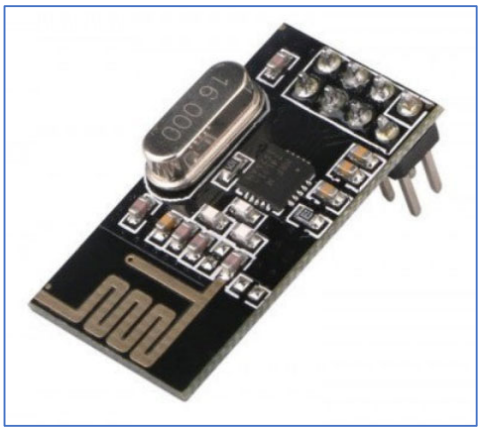

Figure A.1: nRF24L01+ Wireless Module (Dejan, 2017)

Compared with the first module, the second version exhibits several notable differences, including the incorporation of a rubber-duck antenna and an SMA connector. It includes a range-extender integrated circuit, the RFX2401C, which integrates transmit–receive switching, a low-noise amplifier (LNA), and a power amplifier (PA). Consequently, the module can achieve a transmission range of up to 1,000 meters, substantially greater than that of the first module.

Figure A.2: nRF24L01+ PA LNA Wireless Transceiver Module with External antenna (Dejan, 2018)

Although the two modules differ only modestly, they remain interchangeable within a project at any stage. If a project is developed using one module, it can be disconnected and replaced with the other without requiring any modifications to the overall system.

PA and LNA

Within the RF front end, the Power Amplifier (PA) serves to amplify the signal transmitted by the nRF24L01+ transceiver. By contrast, an exceedingly weak signal received from the antenna—often below microvolts or approximately −100 dBm—is amplified by a Low-Noise Amplifier (LNA) to a more usable level, typically ranging from 0.5 to 1 V. The PA and LNA in the transmit path are connected to the antenna through a duplexer, a passive RF device that provides isolation between the transmit and receive paths and prevents the comparatively strong PA output from saturating or overwhelming the LNA input. This arrangement ensures that transmission does not degrade reception, thereby preserving receiver sensitivity and overall link performance.

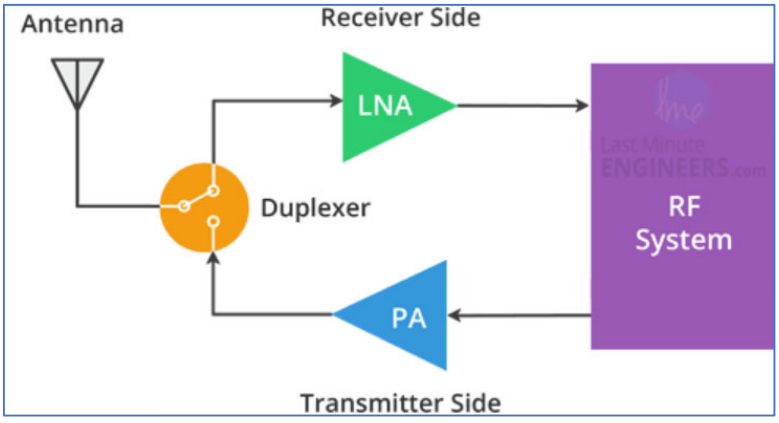

Figure A.3: nRF24L01+ PA/LNA Block Diagram (Last Minute Engineers, 2023)

RF Channel Frequency

In the context of the nRF24L01+ transceiver, the term “channel” denotes the specific frequency used for data transmission and reception. For two or more devices to communicate, they must be configured to operate on the same channel. The permissible frequencies for these channels lie within the 2.4 GHz ISM band, specifically between 2.400 and 2.525 GHz (2400 to 2525 MHz). Each channel possesses a bandwidth of less than 1 MHz. Consequently, there are approximately 125 channels available when spaced at 1 MHz intervals. This arrangement implies that a network of up to 125 independently functioning modems could be established in a single locality by utilizing the 125 distinct channels supported by the nRF24L01+.

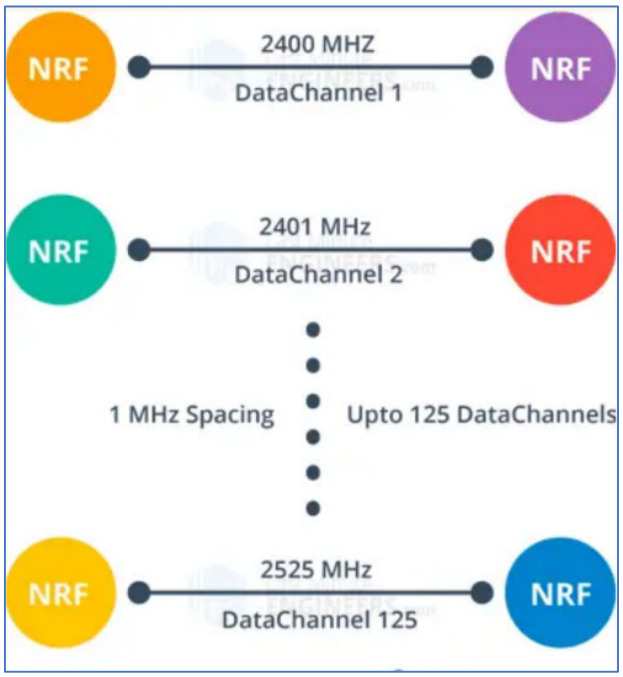

Figure A.4: **nRF24L01+ Wireless Transceiver 2.4GHz 125 RF Channels 1MHz spacing**

(Last Minute Engineers, 2023)

An RF system employing two channels requires careful management of inter-channel separation to avoid interference. Specifically, when each channel uses less than 1 MHz of bandwidth at 250 kbps and 1 Mbps air data speeds, a nominal 1 MHz gap exists between channels. However, achieving a 2 Mbps air data rate necessitates a total bandwidth of 2 MHz, which exceeds the resolution of the RF channel frequency setting. Consequently, to prevent channel overlap and minimize crosstalk in 2 Mbps mode, a 2 MHz guard band must be maintained between the two channels. The selected RF channel frequency is determined by the relationship.

$$Freq_{(Selected)} = 2400 + CH_{(Selected)}$$

For instance, selecting channel 108 yields an RF channel frequency of 2508 MHz (2400 + 108).

nRF24L01+ Multiceiver Network

The nRF24L01+ transceiver supports a feature commonly referred to as a multiceiver, which enables multiple transmission streams to be managed through a single receiver. In a multiceiver configuration, each RF channel is conceptually divided into six parallel data channels, or data pipes; equivalently, a single physical RF channel comprises six logical channels, including the primary data stream. Each data pipe is assigned a unique address, known as its data pipe address, and a data pipe can receive only one packet at a time. The network of multiceivers is illustrated in Last Minute Engineers (2023).

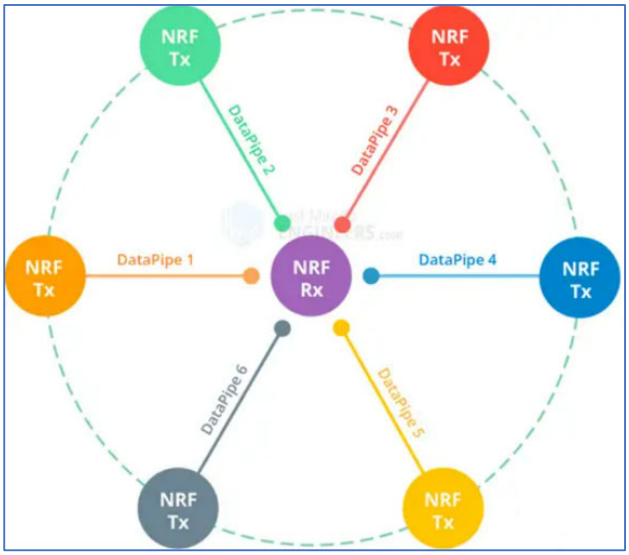

Figure A.5: nRF24L01+ Multiceiver Network – Multiple Transmitters Single Receiver
(Last Minute Engineers, 2023)

This scenario envisions the primary receiver functioning as a central hub, simultaneously aggregating data from six discrete transmitter nodes to illustrate the operational principles of a multiceiver network. The hub is endowed with bidirectional capability, capable of both transmitting and listening at any given moment, thereby enabling real-time data collection, coordination, and assessment of network performance. As noted by Last Minute Engineers (2023), such simultaneous transmit-receive operations are a defining feature of hub-based architectures and underpin the study of communication dynamics within multiceiver systems.

Enhanced ShockBurst Protocol

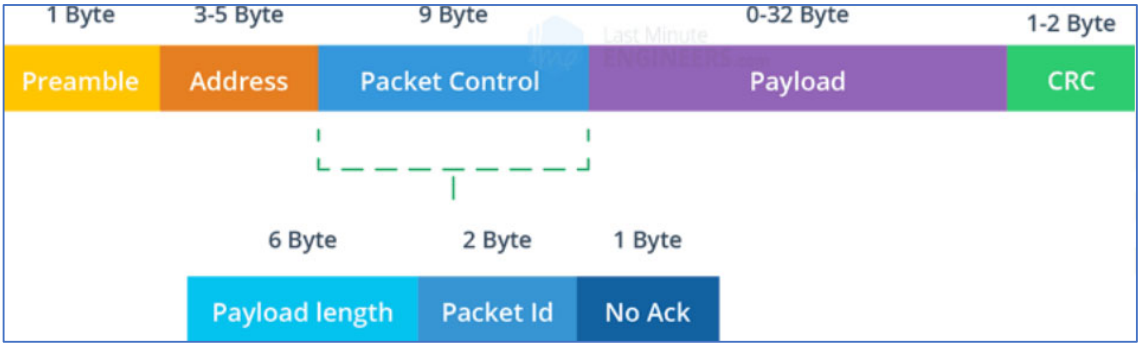

Figure A.6: nRF24L01+ Enhanced ShockBurst Packet Structure

(Last Minute Engineers, 2023)

The Enhanced ShockBurst (ESB) packet structure, used by the nRF24L01+ transceiver, comprises five distinct fields. While the original ShockBurst format included the Preamble, Address, Payload, and CRC, the Enhanced version introduces an additional Packet Control Field (PCF) that expands its capabilities for more sophisticated communications. This augmentation yields several advantages for data transmission.

Several features contribute to the effectiveness of this design. First, the inclusion of a payload-length specifier enables handling payloads ranging from 1 to 32 bytes, accommodating variable data sizes. Second, each transmitted packet is assigned a unique packet ID, allowing the receiver to determine whether a message is fresh or a retransmission. Finally, every communication frame includes an acknowledgment field, enabling the recipient to send acknowledgments as part of a reliability mechanism.

nRF24L01+ Automatic Packet Handling

The following are three scenarios that illustrate the interactions between two nRF24L01+ modules:

Transaction with an acknowledgment: An acknowledged transaction is exemplified by a straightforward data-transfer scenario in which a sender (transmitter) initiates communication by delivering a data packet to a receiver. The transmitter then waits for an acknowledgment (ACK) for approximately 130 microseconds after the packet is sent. Upon successful reception of the packet, the receiver responds with an ACK to the sender. The exchange is considered complete when the sender receives this acknowledgment. This sequence represents a fundamental Stop-and-Wait Automatic Repeat reQuest (ARQ) protocol, illustrating reliable data transfer through immediate acknowledgment.

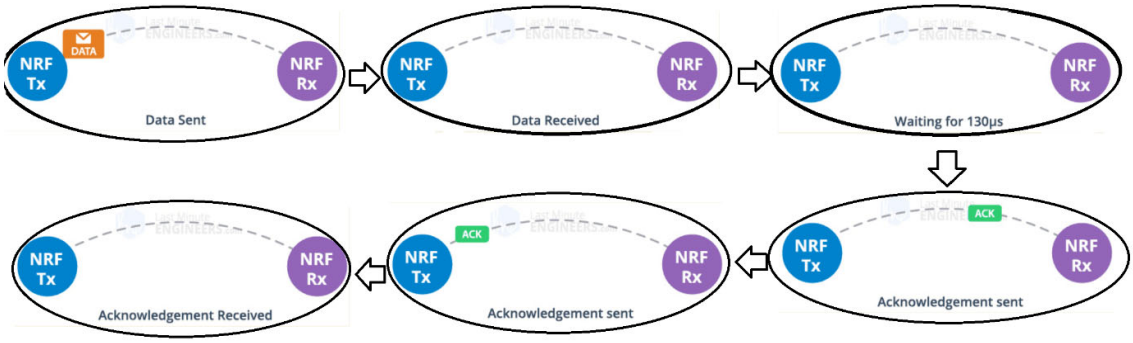

Figure A.7: nRF24L01+ Transceiver Working Packet Transmission

(Last Minute Engineers, 2023)

Transaction with a lost data packet: Packet loss introduces a problematic condition in data communication, necessitating retransmission to recover the lost information. After a packet is transmitted, the sender awaits an acknowledgment (ACK) from the receiver. If the ACK is not received within the auto-retransmit-delay (ARD) period, the packet is retransmitted. The transaction is considered complete when the recipient acknowledges the retransmitted packet.

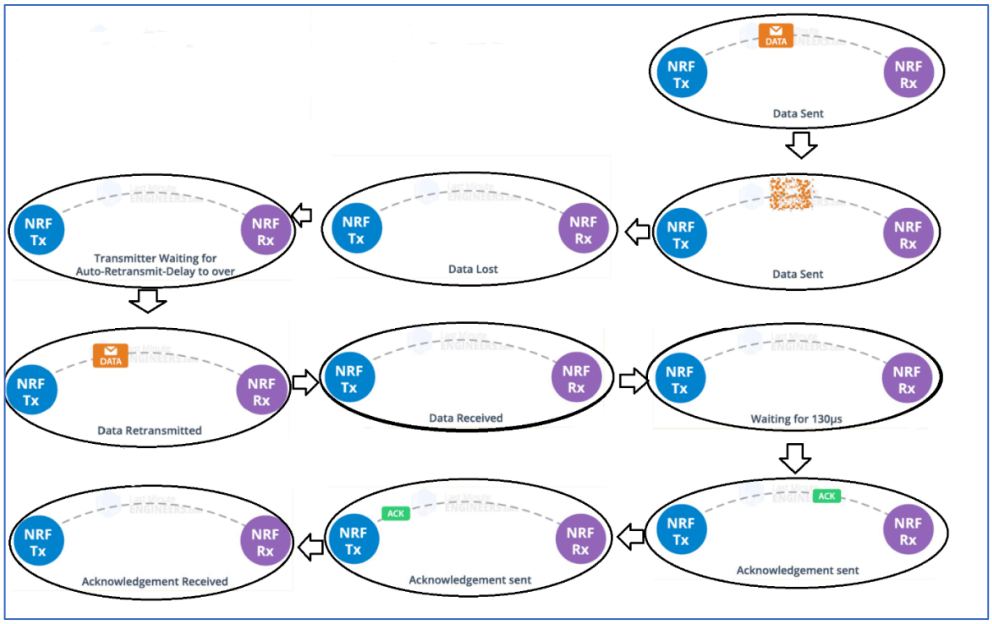

Figure A.8: nRF24L01+ Transceiver Working Packet Transmission Data Lost

(Last Minute Engineers, 2023)

Transaction with a lost acknowledgment: An additional adverse scenario arises when the loss of an acknowledgement (ACK) necessitates retransmission. Although the receiver has successfully received the packet on the initial transmission, the transmitter interprets the absence of an ACK as an indication that the packet is lost. Consequently, after the Auto-Retransmit-Delay timeout expires, the transmitter retransmits the packet. The receiver, upon

receiving a duplicate with the same identifier, discards the duplicate and issues an ACK again. The transaction is concluded when the sender receives the.

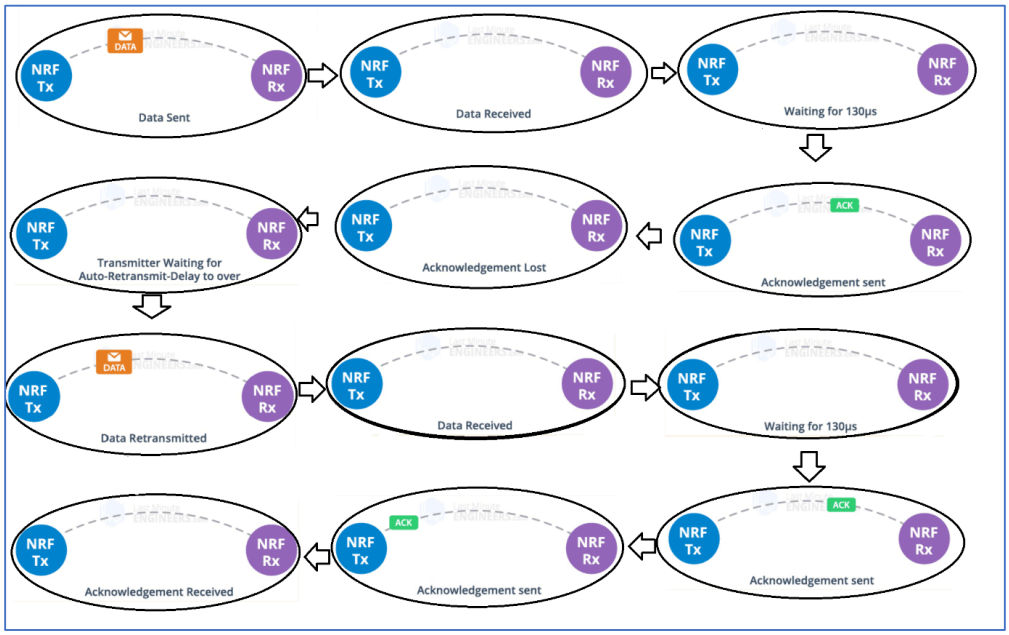

Figure A.9: nRF24L01+ Transceiver Working Packet Transmission Acknowledgement Lost (Last Minute Engineers, 2023)

The nRF24L01+ transceiver autonomously handles all packet processing, eliminating the need for microcontroller intervention during operation.

Multiple NRF24L01 modules communication

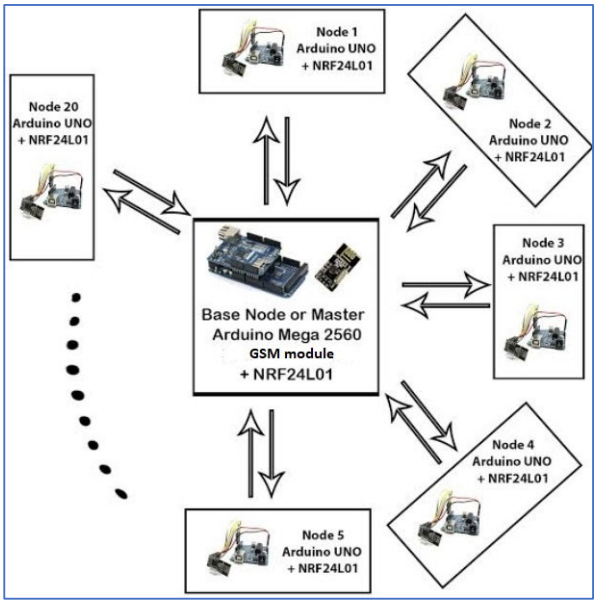

Figure A.10: NRF24L01 can listen up to 6 other modules at the same time (Hzajkani, 2017)

A single NRF24L01 module can simultaneously listen to up to six additional NRF24L01 modules. The RF24Network library leverages this capability to implement a tree-structured network in which a base node is followed by subsequent nodes, which may be either the base node's children or nodes in other branches. Each node can connect to up to five children, and because the tree can extend to a depth of five levels, the network can, in total, comprise up to 3,125 nodes. Every node must be assigned a 15-bit address that encodes its exact position within the tree.

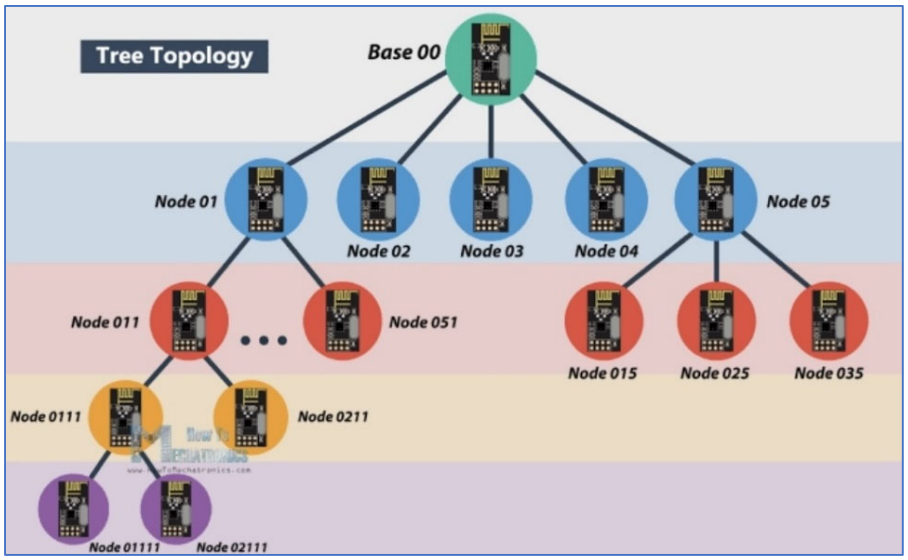

Figure A.11: **Tree Topology Wireless Network** (Dejan, 2018)

Node addresses can be defined using octal notation. The master (base) address is 00; its immediate children are designated from 01 to 05. The children of the node 01 are designated from 011 to 051, and this hierarchical pattern continues for subsequent generations.

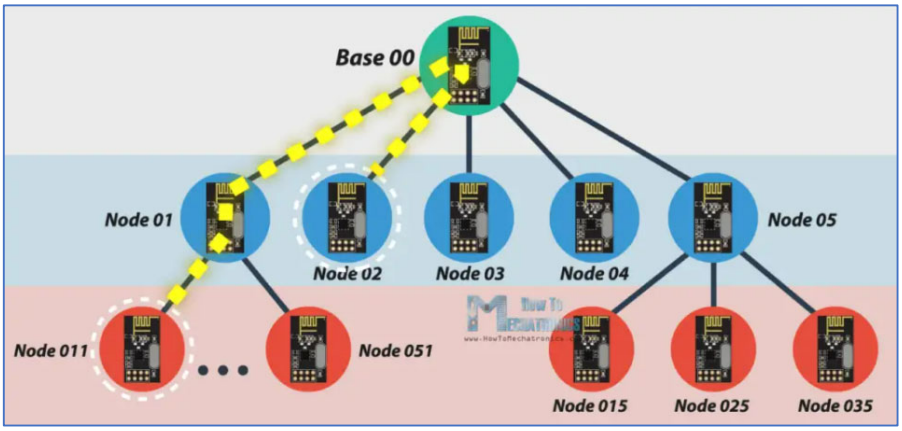

Figure A.12: **Communication between two notes through the base node** (Dejan, 2018)

Within this network, any node can initiate communication with any other node. For example, when Node 011 transmits data to Node 02, the communication path traverses Node 01 and the base node 00. Consequently, the successful delivery of such communications depends on the continuous availability of these intermediary nodes—Node 01 and the base node 00.

B. APPENDIX B: CODE RUNNING ON THE IoT DEVICES

Appendix B4.2: Code running on the customer side pole box IoT device

Presented below is a representative sample of the software code executed on the customer-side pole-top box IoT device. Given that the code is largely identical across all five IoT devices, only the source code for a single device is reproduced in this appendix.

```
// Include necessary libraries
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>

// Define pins for sensors and relay module
#define CURRENT_SENSOR A0
#define VOLTAGE_SENSOR A1
#define RELAY_PIN 2

// Define variables for ADC values and RMS values
int currentADC[1000];
int voltageADC[1000];
float instantaneousCurrent[1000];
float instantaneousVoltage[1000];
float currentRMS;
float voltageRMS;

// Define variables for allowable ranges
int maxCurrent = 20; // for 20A customer
int maxVoltage = 230; // +/- 5% variation

// Create instance of nRF24L01 radio module
RF24 radio(9, 10); // CE, CSN pins

// Create array for transmitting data
float data[2]; // [current, voltage]

void setup() {
        // Initialize serial communication
        Serial.begin(9600);

        // Initialize nRF24L01 radio module
        radio.begin();
        radio.setPALevel(RF24_PA_MIN); // set power level to minimum
        radio.openWritingPipe(0xF0F0F0F0E1LL); // set address for transmitting data
        radio.stopListening(); // stop listening for incoming data

        // Set relay pin as output
        pinMode(RELAY_PIN, OUTPUT);
}

```

```
43  void loop() {
44      //Take 1000 ADC sample values at an interval of 0.1ms using acs712 sensor
45      float sumCurrentInstSqures = 0;
46      int count =0;
47      for (int i = 0; i < 1000; i++) {
48          currentADC[count] = analogRead(CURRENT_SENSOR); // read ADC value
49          //Convert ADC values to AC instantaneous current values
50          instantaneousCurrent[count] = (7.071 / 511.5) * currentADC[count] - 7.071;
51          sumCurrentInstSqures += pow(instantaneousCurrent[count], 2);
52          count++;
53          delayMicroseconds(100); // delay 0.1ms
54      }
55
56      //Calculate RMS value from instantaneous values
57      currentRMS = sqrt(sumCurrentInstSqures/1000);
59
60      //Take 1000 ADC sample values at an interval of 0.1ms using zmpt101b sensor
61      float sumVoltageInstSqures = 0;
62      count = 0;
63      for (int i = 0; i < 1000; i++) {
64          voltageADC[count] = analogRead(VOLTAGE_SENSOR); // read ADC value
65          //Convert ADC values to AC instantaneous voltage values
66          instantaneousVoltage[count] = (353.55 / 511.5) * voltageADC[count] - 353.55;
67          sumVoltageInstSqures += pow(instantaneousVoltage[count], 2);
68          count++;
69          delayMicroseconds(100); // delay 0.1ms
70      }
71
72      //Calculate RMS value from instantaneous values
73      voltageRMS = sqrt(sumVoltageInstSqures / 1000);
74
75      //Check RMS current value against allowable range
76      if (currentRMS > maxCurrent) {
77          // Abnormal condition detected, trigger isolation of customer power
78          digitalWrite(RELAY_PIN, HIGH);
79      }
80
81      // Check RMS voltage value against allowable range
82      if (voltageRMS > maxVoltage || voltageRMS < (maxVoltage - (maxVoltage * 0.05))) {
83          // Abnormal condition detected, trigger isolation of customer power
84          digitalWrite(RELAY_PIN, HIGH);
85      }
86
87      // Transmit data to another node using nRF24L01 radio module
88      data[0] = currentRMS;
89      data[1] = voltageRMS;
90      radio.write(&data, sizeof(data)); // transmit data
91
92  }
```

Appendix B4.3: Code running on the Transformer pole box IoT device

Presented below is a representative sample of the software code executed on the transformer side pole-top box IoT device.

```
// Include necessary libraries
#include <SPI.h>
#include <nRF24L01.h>
#include <RF24.h>
#include <SoftwareSerial.h>

// Define pins for sensors and modules
#define VOLTAGE_SENSOR_1 A0
#define VOLTAGE_SENSOR_2 A1
#define CURRENT_SENSOR_1 A2
#define CURRENT_SENSOR_2 A3
#define CURRENT_SENSOR_NEUTRAL A4
#define RELAY_MODULE_1 2
#define RELAY_MODULE_2 3
#define NRF_CE_PIN 7
#define NRF_CSN_PIN 8
#define SIM900_TX_PIN 9
#define SIM900_RX_PIN 10

// Define variables for sensor readings
float voltage1, voltage2, current1, current2, currentNeutral;
int currentADC[1000];
int voltageADC[1000];
float instantaneousCurrent[1000];
float instantaneousVoltage[1000];
int maxCurrent = 120; // maximum current per phase
int maxVoltage = 252; // 240+ 5% variation
int minVoltage = 228, // 240- 5% variation

// Define variables for nRF24L01 communication
RF24 radio(NRF_CE_PIN, NRF_CSN_PIN);
const uint64_t pipe = 0xE8E8F0F0E1LL; // Address for communication with other nodes
float receivedVoltage[5]; // Array to store received voltage values
float receivedCurrent[5]; // Array to store received current values

// Define variables for ThingSpeak communication
SoftwareSerial sim900(SIM900_TX_PIN, SIM900_RX_PIN);
String apiKey = "U6N49OFETK3DQCSM"; // ThingSpeak API key
String server = "api.thingspeak.com";
String postStr = " "; // String to store data to be sent to ThingSpeak

// Setup function
void setup() {
        // Initialize serial communication
        Serial.begin(9600);

        // Initialize nRF24L01 radio module
        radio.begin( );
        radio.openReadingPipe(1, pipe);
        radio.startListening( );

        // Initialize SIM900 GPRS/GSM Shield
        sim900.begin(19200);
        delay(2000);
        sim900.print("AT+CMGF=1\r"); // Set SMS mode to text
        delay(100);
```

```
57              sim900.print("AT+CNMI=2,2,0,0,0\r"); // Set SMS notification to text
58              delay(100);
59      }
60
61      // Main loop
62      void loop() {
63              //Take 1000 ADC sample values at an interval of 0.1ms using zmpt101b sensor
64              float sumVoltageInstSqures = 0;
65              int count = 0;
66              for (int i = 0; i < 1000; i++) {
67                      voltageADC[count] = analogRead(VOLTAGE_SENSOR_1); // read ADC value
68                      //Convert ADC values to AC instantaneous voltage values
69                      instantaneousVoltage[count] = (353.55 / 511.5) * voltageADC[count] - 353.55;
70                      sumVoltageInstSqures += pow(instantaneousVoltage[count], 2);
71                      count++;
72                      delayMicroseconds(100); // delay 0.1ms
73              }
74              //Calculate RMS value from instantaneous values
75              voltage1 = sqrt(sumVoltageInstSqures / 1000);
76
77      //Take 1000 ADC sample values at an interval of 0.1ms using zmpt101b sensor
78      sumVoltageInstSqures = 0;
79      count = 0;
80      for (int i = 0; i < 1000; i++) {
81              voltageADC[count] = analogRead(VOLTAGE_SENSOR_2); // read ADC value
82              //Convert ADC values to AC instantaneous voltage values
83              instantaneousVoltage[count] = (353.55 / 511.5) * voltageADC[count] - 353.55;
84              sumVoltageInstSqures += pow(instantaneousVoltage[count], 2);
85              count++;
86              delayMicroseconds(100); // delay 0.1ms
87      }
88      //Calculate RMS value from instantaneous values
89      voltage2 = sqrt(sumVoltageInstSqures / 1000);
90
91      //Take 1000 ADC sample values at an interval of 0.1ms using acs712 sensor
92      float sumCurrentInstSqures = 0;
93      count =0;
94      for (int i = 0; i < 1000; i++) {
95              currentADC[count] = analogRead(CURRENT_SENSOR_1); // read ADC value
96              //Convert ADC values to AC instantaneous current values
97              instantaneousCurrent[count] = (7.071 / 511.5) * currentADC[count] - 7.071;
98              sumCurrentInstSqures += pow(instantaneousCurrent[count], 2);
99              count++;
100             delayMicroseconds(100); // delay 0.1ms
101     }
102     //Calculate RMS value from instantaneous values
103     current1 = sqrt(sumCurrentInstSqures/1000);
104
105     //Take 1000 ADC sample values at an interval of 0.1ms using acs712 sensor
106     sumCurrentInstSqures = 0;
107     count =0;
108     for (int i = 0; i < 1000; i++) {
109             currentADC[count] = analogRead(CURRENT_SENSOR_2); // read ADC value
111             //Convert ADC values to AC instantaneous current values
112             instantaneousCurrent[count] = (7.071 / 511.5) * currentADC[count] - 7.071;
113             sumCurrentInstSqures += pow(instantaneousCurrent[count], 2);
114             count++;
115             delayMicroseconds(100); // delay 0.1ms
116     }
117     //Calculate RMS value from instantaneous values
118     current2 = sqrt(sumCurrentInstSqures/1000);
119
120     //Take 1000 ADC sample values at an interval of 0.1ms using acs712 sensor
```

```
121     sumCurrentInstSqures = 0;
122     count =0;
123     for (int i = 0; i < 1000; i++) {
124             currentADC[count] = analogRead(CURRENT_SENSOR_NEUTRAL);
125             //Convert ADC values to AC instantaneous current values
126             instantaneousCurrent[count] = (7.071 / 511.5) * currentADC[count] - 7.071;
127             sumCurrentInstSqures += pow(instantaneousCurrent[count], 2);
128             count++;
129             delayMicroseconds(100); // delay 0.1ms
130     }
131     //Calculate RMS value from instantaneous values
132     currentNeutral = sqrt(sumCurrentInstSqures/1000);
133
134     //Check RMS values against allowable range
135     if (voltage1 > maxVoltage || voltage1 < minVoltage || current1 > maxCurrent) {
136             // Abnormal condition detected, trigger isolation for phase 1
137             digitalWrite(RELAY_MODULE_1, LOW);
138     }
139     if (voltage2 > maxVoltage || voltage2 < minVoltage || current1 > maxCurrent) {
140             // Abnormal condition detected, trigger isolation for phase 2
141             digitalWrite(RELAY_MODULE_2, LOW);
142     }
143
144     //Check for broken conductor fault in the network
145     bool noSupply = (current1 == current2 == currentNeutral == 0);
146     bool unbalancedSystem = (current1 + currentNeutral == current2 || current2 + currentNeutra
147     == current1);
148     bool balancedSystem = (current1 == current2 || currentNeutral == 0);
149     if (noSupply == false && unbalancedSystem == false && balancedSystem == false) {
150             //broken conductor detected, trigger isolation of for both phases
151             digitalWrite(RELAY_MODULE_1, LOW);
152             digitalWrite(RELAY_MODULE_2, LOW);
153     }
154
155     // Check for incoming data from other nodes
156     if (radio.available()) {
157             radio.read(&receivedVoltage, sizeof(receivedVoltage)); // Read received voltage values
158             radio.read(&receivedCurrent, sizeof(receivedCurrent)); // Read received current values
159     }
160
161     //Check RMS values against allowable range
162     float totalCurrentPhase1 = receivedCurrent[0] + receivedCurrent[1] + receivedCurrent[2];
163     float totalCurrentPhase2 = receivedCurrent[3] + receivedCurrent[4];
164     bool illegalConnectionPhase1 = (totalCurrentPhase1 > (current1 + 0.03*current1));
165     bool illegalConnectionPhase2 = (totalCurrentPhase2 > (current2 + 0.03*current2));
166
167     if (noSupply == false && unbalancedSystem == false && balancedSystem == false) {
168             //illegal connection detected, trigger isolation of customer power
169             digitalWrite(RELAY_MODULE_1, LOW);
170             digitalWrite(RELAY_MODULE_2, LOW);
171     }
172
173     // Send data to ThingSpeak
174     postStr = "field1=" + String(voltage1) + "&field2=" + String(voltage2) + "&field3=" +
175     String(current1) + "&field4=" + String(current2) + "&field5=" + String(currentNeutral);
176
177     sim900.print("AT+HTTPINIT\r"); // Initialize HTTP service
178     delay(100);
179     sim900.print("AT+HTTPPARA=\"CID\",1\r"); // Set HTTP connection ID
180     delay(100); // Wait for response
181     sim900.print("AT+HTTPPARA=\"CID\",1\r"); // Set HTTP connection ID
182     delay(100); // Wait for response
183     sim900.print("AT+HTTPPARA=\"URL\",\"http://" + server + ".com/update\"\r");
```

```
184     delay(100); // Wait for response
185     sim900.print("AT+HTTPPARA=\"CONTENT\",\"application/x-www-form-urlencoded\"\r");
186     delay(100); // Wait for response
187     sim900.print("AT+HTTPDATA=" + String(postStr.length()) + ",10000\r");
188     delay(100); // Wait for response
189     sim900.print(postStr); // Send data
190     delay(100); // Wait for response
191     sim900.print("AT+HTTPACTION=1\r"); // Execute HTTP POST request
192     delay(100); // Wait for response
193     sim900.print("AT+HTTPTERM\r"); // Terminate HTTP service
194     delay(100); // Wait for response
195     Serial.println("Data sent to ThingSpeak!"); // Print message to serial monitor
196     }
```