Smart Addressable Control System for Optimized Electrical Distribution and Device MANAGEMENT

Dr. Lowlesh Nandkishor Yadav
Department of Computer Science and Engineering,
Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, India
Lowlesh.yadav@gmail.com

Prof Dr Midhunchakkaravarthy
Department of Computer Science and Engineering,
Lincoln University College,
Petaling Jaya Malaysia
midhun@lincoln.edu.my

Dr. Dharmesh Dhabliya
Department of Computer Science and Engineering,
VIIT Pune India
dharmeshdhabliya@gmail.com

Abstract- Modern electrical systems often rely on individual wiring for the control and monitoring of appliances, leading to excessive cabling, higher material costs, complex maintenance, and limited scalability. This project proposes the development of a centralized, intelligent control architecture using a four-core cable system—two cores for power and two for communication. Every appliance is equipped with an addressable node that includes a microcontroller for communication and device control. The central control unit communicates over the shared bus, sending uniquely formatted instructions containing specific device addresses. Upon receiving a message, only the appliance with the corresponding address will execute the command, while others will ignore it. Inspired by established protocols like KNX, this design aims to simplify the installation, maintenance, and scalability of residential and commercial electrical systems. The project will include designing a lightweight, custom communication protocol and hardware for addressable nodes and integrating them into typical home appliances. This system will enable centralized automation, real-time monitoring, and energy-efficient operation with fewer cables and reduced costs. The ultimate goal is to lay the foundation for a more intelligent and resource-efficient infrastructure in modern smart environments.

Keywords: *KNX, Addressable, RS485, Address space, firmware*

I. INTRODUCTION

In traditional electrical wiring systems, each appliance or electrical point is typically connected to the distribution board through a dedicated set of wires, often necessitating separate runs for power and control. This design, though straightforward, introduces a host of limitations as homes and buildings become increasingly intelligent and reliant on automation. More cables mean higher material and labor costs, more room for error during installation, and added complexity when modifications or expansions are needed. In large buildings or smart homes, where dozens of devices need independent control and monitoring, these issues compound rapidly. The emerging field of smart homes, Internet of Things (IoT), and building automation calls for a new approach—one where electrical wiring is not only a conduit for power but also a medium for intelligent communication. This project proposes an innovative wiring system where appliances are connected via a unified four-core cable. Two of these cores are dedicated to power delivery, while the other two enable bi-directional communication between devices and a central control unit. This significantly reduces the need for individual control lines while maintaining full control over each appliance.

The concept is analogous to how data networks function: instead of connecting each computer with its own direct line to the server, we use a shared medium and identify devices using IP addresses. Similarly, this project will implement addressable nodes for each appliance. These nodes consist of compact embedded systems that listen to communication signals, identify commands meant for them using a unique ID, and respond accordingly—either by performing a function (e.g., turning on/off, adjusting intensity, reporting status) or ignoring the message if it's not addressed to them. Inspired by standardized systems like the KNX protocol, which is widely used in building automation, the proposed system will adopt similar messaging logic while focusing on simplified and cost-effective implementation tailored for

low- to mid-range smart infrastructure. KNX supports a decentralized architecture, where every device can talk to others over a shared medium. However, its complexity and cost can be prohibitive in small-scale or residential applications. Our approach leverages the core ideas of addressable messaging and efficient communication but simplifies it into a practical, lean system.

The benefits of this system are significant. First, it slashes the need for extensive wiring, minimizing copper usage, wall conduit requirements, and installation time. Second, it greatly enhances flexibility—new devices can be added without rewiring. Third, monitoring and diagnostics become centralized and real-time, improving safety and energy efficiency. Lastly, it fosters integration with IoT platforms, voice assistants, and mobile apps for modern smart living. Such a system would be particularly valuable in new construction, where the initial installation of smart-ready wiring infrastructure can future-proof homes and buildings. It also holds promise for retrofitting, using modular plug-and-play control nodes that can be installed on existing appliances. This project aims to design, prototype, and test such a system. It will include the development of hardware nodes, communication protocols, and the central controller software. Challenges such as message collision, address management, latency, and electrical noise will be addressed through intelligent protocol design and filtering. Through this approach, we envision a smarter, more sustainable, and scalable way to distribute and manage electricity in modern environments.

II. LITERATURE REVIEW

Building automation and control systems (BACS) are at the forefront of modern smart home and building technologies, with the KNX protocol emerging as one of the most widely adopted open standards for communication between devices in such systems. The literature demonstrates the protocol's robustness in integrating various devices but also highlights key challenges, particularly in security, interoperability, and adaptability for advanced applications.

Graveto et al. (2023) explored the vulnerabilities of KNX-based systems, particularly in the context of data exfiltration. Their study revealed how attackers could misuse KNX communication paths to transmit sensitive data covertly. This work underscores the need for enhanced encryption and monitoring mechanisms, especially as KNX systems are increasingly deployed in both residential and commercial infrastructures. Complementing this, Küppers et al. (2023) conducted a comprehensive security analysis of the KNX protocol, identifying design-level weaknesses and proposing strategies to mitigate the risks of unauthorized access and eavesdropping. Together, these studies establish that while KNX is effective as a control protocol, its legacy design requires modernization to support secure deployments. Addressing this security concern, Graveto, Cruz, and Simões (2023) proposed a network intrusion detection system (NIDS) tailored for BACS, capable of identifying abnormal patterns and potential threats in real-time. Their research showed the practicality of integrating cybersecurity solutions directly into KNX-based systems, which traditionally lack dynamic threat response mechanisms. In an earlier review by the same authors (2021), the general security landscape of BACS was surveyed, highlighting gaps in standardization, implementation diversity, and the lack of proactive security frameworks, which these newer works aim to fill.

On the application front, several studies demonstrate KNX's flexibility in smart environments. Vanus et al. (2023) introduced a system that merges mobile robotics with KNX infrastructure for occupancy monitoring in elderly care homes. This innovative application not only improved user safety but also showcased KNX's interoperability with external systems, a feature crucial for assistive living technologies. Similarly, López-Aguilar et al. (2023) developed a communication framework using KNX for interactive user experience (UX) testing environments. Their work emphasized real-time responsiveness and user-centric design, validating KNX's applicability beyond traditional automation contexts. Another emerging area is the integration of smart interfaces. Cariello et al. (2023) proposed a brain–computer interface

(BCI) that allows users to control home appliances using motor imagery signals. Though not limited to KNX, their work presents opportunities to integrate such interfaces with KNX for accessibility-driven smart homes. This aligns with the direction taken by Grzegorz and Vala (2024), who developed a KNX-ZigBee gateway, bridging traditional automation with IoT wireless protocols, thus enabling more flexible and mobile control systems.

Moreover, efforts to address technology fragmentation are well represented by Simeoni et al. (2021), who proposed a secure and scalable smart home gateway. Their architecture serves as a middleware between heterogeneous technologies, including KNX, ensuring both security and interoperability. This is particularly valuable in environments where legacy and modern systems coexist. Finally, Sitzia et al. (2024) introduced a broader perspective by exploring how KNX can be leveraged to facilitate energy communities and digital condominiums. Their work focused on collective energy management, enabling distributed decision-making and resource optimization using KNX-based infrastructure. This vision aligns with global sustainability goals and positions KNX as a key enabler of community-level smart grid participation.

The literature illustrates a growing maturity in KNX-based systems, transitioning from simple automation toward highly integrated, secure, and intelligent ecosystems. While KNX offers a robust foundation, emerging demands for security, interoperability, and user-centric design call for continuous innovation. The ongoing integration of AI, BCI, robotics, and cross-protocol gateways marks the beginning of a more responsive and adaptive smart infrastructure, where KNX remains a vital but evolving component.

III. PROPOSED WORK

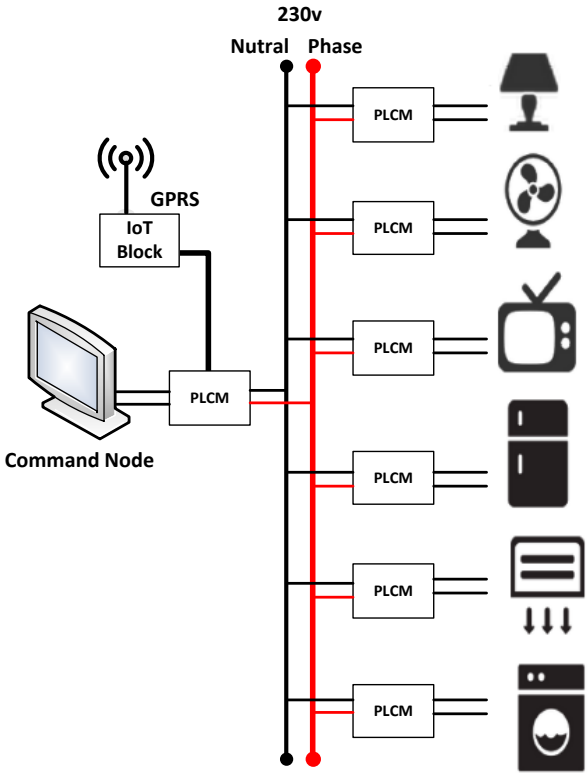

Figure 1.0: Proposed block diagram

The proposed work aims to design and implement a centralized, addressable control system for managing electrical appliances using a shared communication and power infrastructure. The key

objective is to replace the traditional multi-cable layout with a simplified four-core cable system—two cores for AC power and two for digital communication—enabling both power distribution and data transmission over the same physical wiring. This unified cabling approach is intended to reduce installation complexity, minimize material usage, and enhance scalability and control flexibility in residential and commercial electrical systems. At the core of the system are addressable control nodes, which will be installed at each appliance point. These nodes will consist of microcontrollers (e.g., ATmega328, STM32, or ESP32), RS-485 transceivers, AC to DC power supplies, and appropriate actuator drivers such as relays, TRIACs, or PWM circuits. Each node will be assigned a unique address, allowing it to recognize and respond to commands sent by a central control unit (CCU). The CCU will act as the master in a master-slave RS-485 bus topology, communicating with all devices and managing control logic, sensor feedback, and automation routines.

The system will support both ON/OFF control and variable control (for dimmable devices or fan speed regulators). Additionally, it will be equipped to collect data from integrated sensors (e.g., temperature, humidity, or light sensors) to enable environment-responsive automation. For example, if a temperature sensor detects a rise above a predefined threshold, the system could automatically turn on a connected cooling device. A custom communication protocol will be developed to ensure reliable message delivery, including features such as addressing, command encoding, data payloads, and checksums for error detection. The CCU will also provide a user interface through a mobile app, web portal, or smart assistant integration, enabling users to control and monitor their appliances remotely.

The proposed work also involves designing firmware for both the CCU and addressable nodes, developing automation logic, and testing the system in a lab environment. The final goal is to demonstrate a fully functional prototype capable of managing multiple appliances and sensors, with reduced wiring, centralized intelligence, and enhanced energy efficiency.

This proposed system has the potential to transform conventional electrical installations into intelligent, adaptable, and user-friendly environments aligned with the future of smart homes and buildings.

IV. METHODOLOGY

The implementation of a smart addressable control system over a shared power and communication line requires a multidisciplinary approach, combining elements of electrical engineering, embedded systems design, and communication protocols. The methodology of this project is structured into several interrelated components: network architecture design, addressable node design, communication protocol development, central control unit implementation, firmware and software development, system integration, and testing. Each of these stages involves detailed technical considerations to ensure system reliability, scalability, and performance.

- *Network Architecture Design*

The foundation of this system lies in the design of a simplified but robust physical network. The system uses a four-core cable structure where two cores (Live and Neutral) carry AC power, and the remaining two are dedicated to digital communication. To support reliable data transmission across multiple nodes over potentially long distances, a differential communication method such as RS-485 is used. RS-485 is particularly suited for this application due to its noise immunity and capability to support multiple devices on the same bus. The RS-485 bus can be implemented using SN75176 or MAX485 transceivers at each node, enabling full-duplex or half-duplex communication as needed. Proper line termination using 120-ohm resistors at both ends of the communication bus is essential to reduce reflections and maintain signal integrity.

- *Addressable Node Design*

Each appliance in the system is paired with a dedicated addressable node, acting as a local controller and communication endpoint. These nodes are designed around low-power microcontrollers such as the Atmel ATmega328, ESP32, or STM32F103C8T6, chosen based on cost, availability, and required

functionality. The node includes an RS-485 transceiver for communication and an isolated AC-DC power supply module to derive a low-voltage DC supply (typically 3.3V or 5V) from the mains for the microcontroller. For safety and electromagnetic compatibility, opto-isolators (like PC817 or 6N137) are used between the communication transceiver and the microcontroller.

Each node maintains a unique address stored in non-volatile memory (e.g., EEPROM or flash). During communication, the node continuously listens on the bus and parses incoming messages. If the embedded address in the message matches the node's ID, the command is executed; otherwise, it is ignored. The node also includes circuitry to control the appliance, such as solid-state relays (e.g., SSR-25DA), TRIAC drivers for dimmable loads, or MOSFET drivers for DC appliances. Feedback from the device (e.g., ON/OFF status, power consumption using current sensors like ACS712 or INA219) is optionally sent back to the master controller.

- *Communication Protocol Design*

To ensure reliable and deterministic operation, a custom communication protocol is developed. This protocol is designed to be lightweight yet robust, suitable for the constrained environment of a shared bus. Each communication frame includes the following structure:

a) Start Byte (0xAA): Indicates the beginning of a frame.

b) Device Address (1 byte): Specifies the destination node.

c) Command Byte (1 byte): Represents the instruction (e.g., TURN_ON, TURN_OFF, QUERY_STATUS).

d) Payload (0–4 bytes): Optional data, such as dimming level or temperature setpoint.

e) Checksum (1 byte): For error detection, calculated as a simple XOR or CRC-8 checksum.

f) End Byte (0x55): Marks the end of the message.

The use of start and end bytes prevents desynchronization, and the checksum ensures data integrity. The communication follows a master-slave model, with the central controller polling each node or broadcasting commands. To avoid collisions, time-slot-based communication or carrier-sense mechanisms may be implemented. For future scalability, an extended addressing format (e.g., 16-bit address space) can be adopted.

- *Central Control Unit*

The central controller orchestrates communication and user interaction. It can be built using a powerful microcontroller platform such as STM32, or a single-board computer like the Raspberry Pi, which supports more advanced control logic and user interface capabilities. This controller includes an RS-485 interface to the communication bus and connects to the internet or local network via Wi-Fi or Ethernet. It maintains a device registry, polling each node periodically for status and logging activity. It also hosts a web-based GUI or mobile API for end-user interaction. The software stack on the central controller is modular and includes a communication handler, command parser, scheduler, device manager, and UI interface.

- *Firmware and Software Development*

Firmware for each node is written in C or C++, optimized for responsiveness and low power. It includes interrupt-based UART handling for efficient message parsing, watchdog timers for reliability, and a command handler for executing device-specific actions. Address assignment during installation can be handled via a temporary configuration mode or dynamically via the controller. On the controller side, the software is developed using Python or C++, with support for MQTT or REST APIs for integration with third-party systems like smart home hubs or voice assistants.

- *System Integration and Power Design*

An important consideration is the electrical isolation between high-voltage AC and low-voltage DC control circuitry. Isolation transformers, opto-couplers, and careful PCB layout practices (creepage and clearance distances) are implemented to ensure user safety and regulatory compliance. Surge protection devices and EMI filters are also integrated at the board level to increase robustness.

- *Testing and Validation*

Extensive testing is conducted in a controlled lab environment. Test cases include command latency, error injection, bus load analysis, electromagnetic interference resistance, and response time under heavy load. Oscilloscopes and logic analyzers are used to monitor signal quality. The system is validated for:

a) Correct message decoding under noise
b) Timely response to control signals
c) Stability under multiple simultaneous commands
d) Electrical safety and thermal performance

By following this detailed methodology, the proposed system can be effectively developed, prototyped, and validated to ensure it meets its goals of simplified wiring, enhanced control, and intelligent home or building management.

V. SYSTEM WORKFLOW

The proposed smart addressable control system redefines the way electrical appliances are managed in homes and buildings by introducing a shared infrastructure for power and communication. At the heart of this system lies a four-core cable infrastructure, composed of two wires for delivering standard AC power (Live and Neutral) and two wires for digital communication (typically Data+ and Data− using differential signaling). This combination allows for both powering appliances and communicating with them over the same wiring framework, reducing the amount of physical cabling and enabling centralized control. Each appliance—whether it's a light, fan, air conditioner, or heater—is connected to an addressable control node. These nodes are embedded microcontroller-based modules installed close to or within the appliance housing. Each node is given a unique digital address stored in its internal EEPROM. This ID is used by the central controller to send specific commands over the communication bus. Internally, each node consists of a microcontroller (e.g., ATmega328, ESP32, STM32), an RS-485 communication interface using drivers like MAX485, a power regulation module (converting AC to 5V/3.3V DC), and an actuator interface such as a relay, TRIAC, or PWM driver circuit.

When a user wants to control an appliance—such as turning on a lamp or adjusting a fan speed—they do so through a central interface. This could be a touch panel, mobile app, voice assistant, or a web portal hosted on the central controller. The user interface (UI) is connected to the central control unit (CCU), which serves as the master in the master-slave communication protocol implemented over the RS-485 bus. The UI sends the user's instruction (e.g., "Turn on Living Room Light") to the CCU. The controller maps this instruction to a unique device address and constructs a communication packet using a predefined protocol. This protocol consists of a start byte, target device ID, command type, optional data payload, a checksum for error detection, and an end byte. For example, a packet to turn on a light may look like: 0xAA (Start) | 0x01 (Device ID) | 0x10 (Turn ON Command) | 0x00 (Payload) | 0xB7 (Checksum) | 0x55 (End). This message is sent over the communication line. All devices on the network receive it, but only the node with the matching ID will process it.

For ON/OFF appliances like lights, sockets, or pumps, the node interprets the command and energizes a relay connected in series with the appliance's AC power line. When the relay is closed, the appliance receives power and turns ON; when the relay is open, it turns OFF. Solid-state relays or electromechanical relays can be used depending on load type and switching speed requirements. The microcontroller ensures safe switching, potentially incorporating zero-cross detection to reduce arcing and inrush current

surges. For dimmable appliances, such as ceiling fans or LED lights, the control node includes a TRIAC-based phase control circuit (for AC) or a PWM-based driver (for DC). The user sends a command like “Set Bedroom Fan Speed to 3”, which is encoded with both the target address and a data payload (e.g., speed level or duty cycle value). The microcontroller uses a zero-cross detection circuit to synchronize with the AC waveform and trigger the TRIAC gate at specific phase angles to achieve the desired power delivery. This phase-cutting technique effectively controls fan speed or light brightness in a smooth and energy-efficient manner.

Beyond control, the system also supports sensor monitoring, which is vital for automation and energy management. Sensor nodes, either standalone or integrated into appliance nodes, measure environmental parameters such as temperature, humidity, or ambient light. Common sensors include the DHT22 (temperature and humidity), DS18B20 (precision temperature), and LDRs (light level). These sensors are read periodically by the microcontroller, and the values are sent back to the CCU either on request (polling) or on threshold breach (event-based). For instance, a temperature sensor node in the living room measures 28°C. The central controller, based on a pre-set automation rule, compares this value against a threshold (e.g., 26°C). If the value exceeds the threshold, it automatically sends a command to turn on the AC node, effectively implementing autonomous environmental control. This intelligent feedback loop allows the system to not just respond to manual input but to operate based on sensor conditions, thereby improving comfort and energy efficiency.

From the user’s perspective, monitoring is seamless. The central controller aggregates sensor data and displays it through the UI. Users can check the current temperature in each room, energy usage trends, and device statuses from their smartphone or computer. If the system is integrated with a home assistant platform like Home Assistant or Alexa, voice commands such as “Turn off kitchen light” or “What’s the temperature in the bedroom?” are interpreted by the smart assistant and translated into protocol messages sent to the appropriate device. Internally, all these operations are managed by a scheduler and event handler within the central controller. This software component maintains a registry of all known devices and their states, checks for incoming messages (like feedback from nodes), and executes automation scripts. These scripts can include time-based rules (e.g., turn off garden lights at 6:00 AM), sensor-based triggers (e.g., turn on exhaust fan if humidity > 70%), or user-defined scenes (e.g., “Movie Mode” dims lights and turns on the TV).

In terms of robustness, the RS-485 communication bus is designed to support up to 32 nodes over distances up to 1.2 km. For larger installations, signal repeaters or a CAN-based extension can be used. Message integrity is protected by checksums, and each node features a watchdog timer to recover from potential lockups. In summary, this system provides users with centralized, flexible, and intelligent control of all electrical appliances and sensors in their home or building. Through a shared wiring infrastructure and an addressable control scheme, users can interact with their environment with minimal wiring, efficient automation, and real-time feedback, all while maintaining scalability and ease of installation.

VI. CONCLUSION

The proposed smart addressable control system represents a significant advancement in the field of residential and commercial electrical distribution. By combining a streamlined four-core wiring architecture with embedded addressable control nodes and a centralized command unit, this system offers an intelligent, efficient, and scalable alternative to conventional point-to-point wiring. The approach eliminates the need for running multiple individual control cables, thereby reducing installation complexity, material costs, and maintenance overhead.

Through the implementation of a robust communication protocol over a shared bus (such as RS-485), the system allows precise, real-time control and monitoring of appliances, whether simple ON/OFF loads or more complex dimmable devices. The inclusion of environmental sensors and automation logic further enhances its utility, enabling proactive energy management and comfort control based on actual

environmental conditions. The central controller serves as the brain of the system, seamlessly interfacing with user inputs through mobile apps, web dashboards, or voice assistants while ensuring that the correct command is delivered to the right device.

Technically, the modular design, fault tolerance, and addressable nature of each node ensure that the system remains expandable and reliable across a wide range of use cases. Ultimately, this project not only paves the way for smarter and more sustainable living environments but also lays the groundwork for future integration with IoT, AI-based automation, and advanced energy analytics.

References

Graveto, V., Cruz, T., & Simões, P. (2023). Using KNX-Based Building Automation and Control Systems for Data Exfiltration. *IEEE Internet of Things Journal*, 10, 13727-13741. https://doi.org/10.1109/JIOT.2023.3262873.

Vanus, J., Hercík, R., & Bilik, P. (2023). Using Interoperability between Mobile Robot and KNX Technology for Occupancy Monitoring in Smart Home Care. *Sensors (Basel, Switzerland)*, 23. https://doi.org/10.3390/s23218953.

López-Aguilar, A., Bustamante-Bello, M., Navarro-Tuch, S., & Molina, A. (2023). Development of a Framework for the Communication System Based on KNX for an Interactive Space for UX Evaluation. *Sensors (Basel, Switzerland)*, 23. https://doi.org/10.3390/s23239570.

Simeoni, E., Gaeta, E., García-Betances, R., Raggett, D., Gil, A., Carvajal-Flores, D., Fico, G., Cabrera-Umpiérrez, M., & Arredondo, M. (2021). A Secure and Scalable Smart Home Gateway to Bridge Technology Fragmentation. *Sensors (Basel, Switzerland)*, 21. https://doi.org/10.3390/s21113587.

Küppers, M., Schuba, M., Neugebauer, G., Hoener, T., & Hack, S. (2023). Security Analysis of the KNX Smart Building Protocol. *Proceedings of the 18th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3600160.3605167.

Graveto, V., Cruz, T., & Simões, P. (2023). A Network Intrusion Detection System for Building Automation and Control Systems. *IEEE Access*, 11, 7968-7983. https://doi.org/10.1109/ACCESS.2023.3238874.

Graveto, V., Cruz, T., & Simões, P. (2021). Security of Building Automation and Control Systems: Survey and Future Research Directions. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102527.

Grzegorz, D., & Vala, D. (2024). KNX-ZigBee Gateway. *IFAC-PapersOnLine*. https://doi.org/10.1016/j.ifacol.2024.07.376.

Cariello, S., Sanalitro, D., Micali, A., Buscarino, A., & Bucolo, M. (2023). Brain–Computer-Interface-Based Smart-Home Interface by Leveraging Motor Imagery Signals. *Inventions*. https://doi.org/10.3390/inventions8040091.

Sitzia, G., Roscia, M., Valerii, M., & Ghiani, E. (2024). Integrating Energy Communities and Digital Condominiums with KNX Technology. *2024 AEIT International Annual Conference (AEIT)*, 1-6. https://doi.org/10.23919/AEIT63317.2024.10736760.