IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Password-based Circuit Breaker

Vipul Vinod More[1], Prajwal Pravin Chudiwale [2] *prof. M. H. Patil[3]*

[1,2] *UG Student*

[3]*Asst. Professor*

GF's Godavari College of Engineering, Jalgaon, Maharashtra, India, 425001

Abstract – *The Password-Based Circuit Breaker is a smart electrical protection system designed to improve safety and prevent unauthorized use of electrical power. In traditional circuit breakers, anyone can switch the power ON or OFF manually, which may lead to misuse, accidents, or electric hazards. This project introduces a password security feature that allows only authorized users to control the electrical supply.*

The system works using a microcontroller, keypad, relay, and display unit. A user must enter the correct password through the keypad to activate or deactivate the circuit breaker. If the entered password is correct, the relay allows the electrical connection and the load turns ON. If the password is incorrect, access is denied, ensuring better protection and security.

This project is useful in homes, industries, laboratories, and restricted areas where electrical equipment must be protected from unauthorized access. It also reduces the risk of electric shock and accidental operation. The system is simple, cost-effective, reliable, and easy to implement using embedded system technology.

The Password-Based Circuit Breaker demonstrates how modern security techniques can be integrated with electrical systems to improve safety, control, and efficiency.

INTRODUCTION

An automatically operated electrical switch designed to protect an electrical circuit from damage caused by overload or short circuit. Its basic function is to detect a fault condition and interrupt current flow. Unlike a fuse, which operates once and then must be replaced, a circuit breaker can be reset (either manually or automatically) to resume normal operation. When operated manually we see fatal electrical accidents to the line man are increasing during the electric line repair due to the lack of communication and coordination between the maintenance staff and the electric substation staff. In order to avoid such accidents, the breaker can be so designed such that only authorized person can operate it with a password. Here, there is also a provision of changing the password. The system is fully controlled by the 8-bit microcontroller of 16f877A family. The password is stored in an EEPROM, interfaced to the microcontroller and the password can be changed any time unlike a fixed one burnt permanently on to the microcontroller. A keypad is used to enter the password and a relay to open or close circuit breaker, which is indicated by a lamp. Any wrong attempt to open the breaker (by entering the wrong password) an alert will be actuated, indicated by another lamp. electrical accidents to the line man are increasing, while repairing the electrical lines due to the lack of communication between the electrical substation and maintenance staff. This project gives a solution to this problem to ensure line man safety. In this proposed system the control (ON/OFF) of the electrical lines lies with line man. This project is arranged in such a way that maintenance staff or line man has to enter the password to ON/OFF the electrical line. Now if there is any fault in electrical line then line man will switch off the power supply to the line by entering password and comfortably repair the electrical line, and after coming to the substation line man switch on the supply to the particular line by entering the password. The relay ON/OFF operation will be indicated

LITERATURE REVIEW

Now a days, electrical accidents of the line man are increasing while repairing the electrical lines due to lack of communication between the electrical substation and maintenance staff. This paper gives a solution to this problem to ensure line man safety. In this proposed system the control (ON/OFF) of the electrical lines lies with line man. This paper is arranged in such a way that maintenance staff or line man has to enter the password to ON/OFF the electrical line. Now if there is any fault in electrical line then line man will switch off the power supply to the line by entering the password and comfortably repair the electrical line, and after coming to the substation line man switch on the supply to the particular line by entering the password. Here, there is also a provision of changing the password. circuit breakers are actually provided as a means of protection to completely isolate the downstream network in the event of a fault. The demand for electrical energy is ever increasing. Today over 21% (theft apart!!) of the total electrical energy generated in India is lost in transmission (4-6%)[1]

[1.1] Authors: Rutvik Rohit, Deep Patel, Henil Patel, Krina Suhagia, Dr. Sweta Shah (IJERT: ISSN2278-0181)

PROJECT OBJECTIVES:

The primary objectives of a microcontroller-based, password-controlled circuit breaker can breaker be to enhance safety for maintenance personnel and prevent unauthorized access to the electrical system. This technology provides an essential layer of secure, controlled access that a traditional manual or standard circuit breaker lacks.

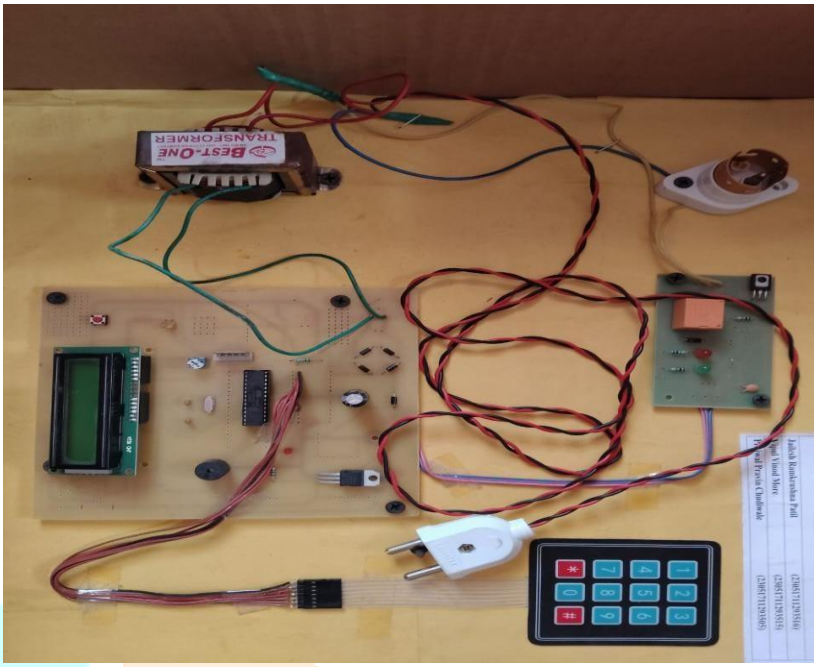
1. Ensuring Lineman and Maintenance Staff Safety: The foremost objective is to prevent fatal electrical accidents caused by miscommunication between maintenance staff and substation operators. By requiring the person on site (e.g., the lineman) to enter a specific password to control the power line, the system ensures that the circuit cannot be energized accidentally by someone at a remote location while repairs are ongoing.
2. Preventing Unauthorized Access: The system acts as a digital lock for the power supply, ensuring that only authorized personnel with the correct credentials can energize or de-energize a specific line or appliance. This prevents tampering or malicious operation of the electrical system.
3. Providing a Reliable and Secure Control Mechanism: The use of a microcontroller allows for a programmable, reliable control system that can be integrated with a secure authentication process. This replaces potentially vulnerable manual switches with a controlled electronic mechanism.
4. Improving Operational Efficiency and Accountability: The system can help manage the power supply to various sections or heavy machinery in industrial or commercial settings, ensuring only trained personnel operate specific equipment. The potential for data logging within the microcontroller also allows for an audit trail of who accessed the system and when.

PROBLEM STATEMENT

Microcontroller-based circuit breakers incorporating password authentication face several critical problems beyond standard electrical faults. The primary vulnerabilities are security-oriented: lost or stolen passwords can lead to unauthorized operation, while susceptible systems may fall victim to brute-force attacks or insecure data storage within the microcontroller's memory. Operationally, firmware bugs can cause logic errors, physical keypads are prone to damage or wear revealing passcodes, and single points of failure like power supply issues or faulty relays can entirely disable both the authentication and protective functions of the device. Identifying these issues requires checking system logs for unauthorized attempts, inspecting the physical keypad, testing power supply stability, verifying sensor accuracy against external meters, and conducting continuity checks on the high-power switching relay.

Security is a primary concern: stolen or forgotten passwords lead to unauthorized access or operational delays, while weak implementations are vulnerable to brute-force attacks or physical key wear revealing the code. System failures often stem from the microcontroller's firmware bugs causing unreliable tripping logic, or unstable power supplies leading to erratic behavior or total system failure. Component issues include the eventual mechanical failure of the high-current relay due to arcing, faulty sensors providing incorrect current/temperature data to the MCU, and physical damage to input keypads or display interfaces. Problem

identification requires a multi-faceted approach, including analyzing system logs for suspicious activity, visually inspecting physical components for wear or damage, using multimeters to verify power supply and relay continuity, and potentially debugging the firmware code itself to pinpoint logic, errors.



CONCLUSION

A password-based circuit breaker using a microcontroller effectively enhances lineman safety by preventing unauthorized activation and allowing for controlled, remote operation, as concluded in projects. These systems are generally successful in creating a safe prototype that requires a specific password to operate the circuit breaker, providing a secure and inexpensive method for electrical maintenance. While prototypes have been successfully developed, the overall effectiveness hinges on strong password security and proper implementation. Key conclusions from project reviews Enhanced safety: The primary conclusion is that these systems significantly improve the safety of electrical maintenance workers by preventing accidental power restoration during repairs. The system ensures that only authorized personnel can turn the line back on after maintenance is complete. Remote control and convenience: Projects have demonstrated that the system can be interfaced with components like a GSM modem to allow for remote operation via SMS, enabling control from a distance and making maintenance more efficient. Security features: The system incorporates security measures such as a password protection mechanism and a lockout feature for multiple incorrect attempts, which can also trigger an alert to a control room, notes this paper from Research Gate

.Successful implementation: Multiple projects have successfully built and demonstrated a functional prototype, confirming that the concept is feasible and the results are satisfactory .Cost-effectiveness: The use of microcontrollers and readily available components makes the system an inexpensive and practical solution.

Future Scope

1. Enhanced security measures

   Multi-factor authentication: Combine passwords with other methods like fingerprint scanners or RFID tags to prevent unauthorized access.

   Biometric identification: Replace passwords entirely with fingerprint or iris scanners for a more secure and direct authentication method.

   Dynamic passwords: Use system-generated, time-sensitive passwords to eliminate the risk of compromised static passwords.

2. Improved functionality and safety

   Remote control via SMS: Enables the circuit breaker to be controlled by sending text messages, useful for remote substations.

   Fault detection and notification: Incorporate sensors to detect faults and automatically send an SMS or app notification to linemen, improving response time and safety.

   Digital lockout/tagout: Integrate with digital procedures to create a clear chain of custody and prevent accidental re-energizing of lines.

   SCADA integration: Connect with SCADA systems to get direct feedback on fault locations, allowing linemen to pinpoint issues faster.

3. Integration with advanced technologies

   Internet of Things (IoT): Connects breakers to the internet for remote monitoring and control, enabling emergency shutdowns and power restoration from a central location.

   Artificial Intelligence (AI): Enables the system to learn from data, automatically detect faults, and take corrective actions, making it more efficient.

   Mobile Apps: Allow for remote operation and control through a smartphone interface, providing a more user-friendly experience.

Reference

- IEEE Std 1036-2010 — IEEE Guide for Application of Shunt Power Capacitors.
- IEC 60831-1/2 — Shunt Power Capacitors – General and Performance Requirements.
- T. B. Smith, Electricity theft: a comparative analysis, Elsevier Journal Energy Policy, vol. 32, no. 18, pp. 2067-2076, Dec. 2004.
- A. J. Dick, Theft of electricity-how UK electricity companies detect and deter, in proceedings of European Convention on Security and Detection, pp. 90-95, May 1995.
- C.J. Bandim, J.E.R. Alves Jr., A.V. Pinto Jr., F.C. Souza, M.R.B. Loureiro, C.A. Magalhaes, and F. Galvez-Durand, Identification of energy theft and tampered meters using a central observer meter: a mathematical approach, in proceedings of IEEE PES Transmission and Distribution Conference and Exposition, vol. 1, pp. 163-168, Sept. 2003.
- S.S.S.R. Depuru, L. Wang, and V. Devabhaktuni, A conceptual design using harmonics to reduce pilfering of electricity, in proceedings of IEEE Power and Energy Society General Meeting, pp. 1-7, Jul. 2010.