International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Design and Evaluation of a Password-Based Switching Authorization System for Electric Lineman Safety

B.Keerthi[1], T.Abhisharan[2], B.Ganesh Goud[3], P.Saidhiah Naidu[4].
Dept. of ECE, CMR Technical Campus, Telangana, India
Email: 237r1a0467@cmrtc.ac.in, 237r1a04c1@cmrtc.ac.in,
237r1a0468@cmrtc.ac.in, 237r1a04b3@cmrtc.ac.in

Abstract - Maintenance on de-energized distribution lines is endangered by unintended re-energization, a hazard that conventional verbal switching coordination cannot exclude. This paper presents the design of a password-based switching authorization system in which an Arduino-based controller accepts a password from a matrix keypad, validates it, and, only on a valid entry, signals a relay interface that switches a low-voltage demonstration load; an LCD and a buzzer provide status and alerts. We specify the architecture, a state model of the controller, a proposed authentication and switching algorithm, and a reproducible test protocol with acceptance criteria. A safety analysis identifies password compromise, tampering, relay and controller faults, and power loss as the dominant residual risks, and argues that automatic relay closing after maintenance is hazardous and should be replaced by deliberate authorization combined with independent confirmation that work is complete. No experimental measurements are yet available, so no performance claims are made. The system is positioned as an additional authorization measure, not a substitute for electrical isolation, lockout/tagout and verification of de-energization.

Key Words: Authorization, circuit breaker, electrical maintenance safety, embedded systems, lineman safety, password authentication, relay control.

I. INTRODUCTION

Work on overhead and distribution lines is performed after the section concerned has been disconnected from supply. The principal hazard during that interval is unintended re-energization: if switching at the substation or feeder is operated by someone who is unaware that a crew is working, the crew is exposed to live conductors. Reports on lineman-safety prototypes attribute such events to inadequate coordination between maintenance staff and substation staff [1], [4]; this paper does not add accident statistics and makes no quantitative claim about incident rates.

Conventional safety relies on administrative controls: verbal or telephonic permits, tagging and, where applicable, lockout/tagout procedures [8], [9]. Their strength is that they are well established; their weakness, with respect to switching, is that the authority to restore supply is not bound to the person doing the work by any technical mechanism. A lock bound to an individual, as in lockout/tagout, achieves this physically. A password-controlled switching device attempts a related effect electronically, by requiring a credential that the working crew holds.

Password-controlled breakers for lineman protection have been reported previously, including implementations with Arduino controllers [1], [2], [4], and extensions with GSM or internet links [2], [3], [6]. The basic concept is therefore not new. The engineering questions that remain concern how such a device should behave in the conditions that matter for safety: after a reset, after loss of power, when the credential is guessed or shared, and when the operator forgets to complete a step. The present work addresses these questions for an Arduino-based prototype.

The objectives are: (i) to define a controller architecture in which switching is conditional on validation of a password; (ii) to specify the controller's states and a proposed algorithm that make safe behaviour explicit; (iii) to define a reproducible low-voltage evaluation protocol with acceptance criteria; and (iv) to analyse residual risks and the limits of password-based control.

Contribution. The paper contributes a documented architecture and state model for a keypad-authorized switching controller; a safety analysis that identifies automatic re-closing as a hazardous feature and proposes a deliberate-authorization alternative; and an evaluation protocol with trial counts and pass criteria. It does not claim novelty for password-controlled switching, nor any measured performance. The remainder of the paper is organized as follows: Section II reviews related work, Section III states the problem and design objectives, Sections IV–VI describe the system, Section VII the evaluation method, Section VIII the status of results, Section IX the safety analysis, and Section X concludes.

II. RELATED WORK

A. Password-controlled breakers for lineman protection

Hudedmani et al. [1] describe a scheme in which a password is required to operate both the control-panel doors and the circuit breaker, with Arduino control and GSM among its keywords. Soomro et al. [2] present an Arduino-based automatic password-controlled breaker with internet communication, in which fault information is acknowledged by the lineman, who then operates the substation using a reference password. Shriwastava et al. [3] report a hardware implementation with an ATmega328P controller and a GSM module that notifies a control room of unauthorized access. A bachelor's thesis [4] implements the concept on an Arduino Uno and states the requirement that nobody should be able to restore a line without the working lineman's permission. Earlier work cited in [1] covers user-changeable passwords [5] and microcontroller-and-GSM safety systems [6]; these two were verified only as entries in [1].

B. Embedded keypad access control

Keypad-and-microcontroller access control is a mature pattern outside the power domain. A representative Arduino-

based system supports keypad, Bluetooth and GSM entry of a four-digit password for a door lock [7]. Such systems establish the keypad-comparison mechanism but are not designed around the consequences of a wrong or forced switching state, which is the distinguishing concern here.

C. Isolation, lockout/tagout and functional safety

The OSHA lockout/tagout standard, 29 CFR 1910.147 [8], sets minimum requirements for controlling hazardous energy during servicing, including isolation of equipment and application of locks or tags; OSHA's guidance directs power generation, transmission and distribution work to 29 CFR 1910.269 [9]. The standard also establishes that the person who applies a device is the person who removes it, with limited exceptions [8]; this ownership principle is the physical analogue of what a password attempts to provide, but a password, unlike a personal lock, can be shared, observed or guessed. IEC 61508 [10] provides the general framework for functional safety of electrical, electronic and programmable electronic systems; its overview documents note that precautions against unauthorized interference are outside its scope. No safety integrity level is claimed for the system described here.

D. Comparison and research gap

Table -I: Comparison of related methods (verified sources only)

Ref.	Control mechanism	Reported strength	Limitation / relevance
[1]	Password for breaker and panel door; Arduino; GSM keyword	Lineman-controlled ON/OFF; access control to panel	Reset and power-loss behaviour not evident from abstract; adds door control beyond this design
[2]	Arduino, internet link, reference password after fault acknowledgement	Remote operation; fault handling	Network dependence and security not assessed here; evidence not examined
[3]	ATmega328P with GSM module; control-room notification	Control-room alert on unauthorized access	Hardware report; restoration workflow not evident
[4]	Arduino Uno password breaker (B.Sc. thesis)	Same platform and goal	Not journal peer reviewed
[7]	Arduino keypad door lock with Bluetooth/GSM	Mature keypad pattern	Not designed for hazardous switching consequences
[8]–[10]	Lockout/tagout, power-line work rules, functional safety	Established isolation and safety frameworks	Define what a password device must not replace

Within the sources whose abstracts could be examined, password control, GSM alerting and Arduino implementation are well covered. What is less evident is (i) an explicit specification of controller behaviour on reset and power loss, (ii) a defined restoration workflow that does not rely on the controller alone, and (iii) a reproducible test protocol with acceptance criteria. This paper targets these three aspects. The assessment rests on abstracts and should be re-checked against full texts before any novelty statement is made.

III. RESEARCH PROBLEM AND DESIGN OBJECTIVES

Problem. A circuit that has been opened for maintenance must not be closable by anyone other than those responsible for the work, and no single failure, mistaken entry or loss of power should close it. Manual coordination does not provide a technical barrier, and a password device that is poorly specified can introduce new failure modes.

The design objectives are:

1. O1: Switching is permitted only after validation of a password.
2. O2: An incorrect entry produces no switching action and a distinct alert.
3. O3: Reset or power interruption must not energize the load.
4. O4: Closing the circuit requires a deliberate, authorized action; no automatic closing.
5. O5: The controller state is visible to the operator on the LCD and by the buzzer.
6. O6: The design is simple, repairable and testable on a low-voltage load.

Wireless communication is a possible extension and is not part of the confirmed design. Objectives O3 and O4 are design requirements; whether the present prototype meets them is not established and is the subject of the evaluation in Section VII.

IV. PROPOSED SYSTEM ARCHITECTURE

Fig. 1 shows the functional architecture. The keypad supplies key codes to an Arduino microcontroller, whose firmware performs two functions: password validation, in which the entry is compared with a stored value, and switching control, which drives the status outputs and the relay interface. The LCD presents prompts and status, the buzzer provides audible alerts, and the relay interface switches a low-voltage demonstration load. A power supply feeds the controller.

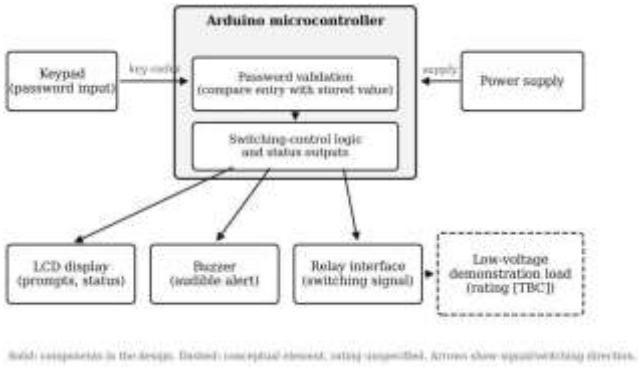


Fig -1: Functional architecture of the password-based switching authorization system. Dashed block: conceptual element with unspecified rating.

Confirmed and proposed elements are distinguished as follows. The controller, keypad, LCD, buzzer, relay module and a load circuit appear in the prototype's block diagram and are treated as confirmed components. The password-storage method, the handling of a forgotten password, the buzzer's trigger conditions and the relay's state at power-up are not specified and are marked [TBC]. Wi-Fi or GSM links, encrypted storage, cloud logging and mobile applications are not part of the design and are discussed only as future work.

V. HARDWARE DESIGN AND OPERATING METHODOLOGY

Table II lists the components and their roles, and Fig. 2 illustrates the component types. A 4×4 matrix keypad provides sixteen keys (digits, letters and two symbols), which sets the size of the password space (Section IX). The relay module

isolates the controller's logic-level output from the switched circuit; its coil drive, contact ratings and the type of load are not specified [TBC].

Table -II: Hardware components and functional roles

Component	Functional role	Specification status
Arduino microcontroller	Reads keys, validates password, controls outputs	Board model, clock, pin map [TBC]
4×4 matrix keypad	Password and command entry	Model and wiring [TBC]
LCD display	Prompts and status messages	Size and interface [TBC]
Buzzer	Audible alert	Type, driver, alert patterns [TBC]
Relay module	Switching interface to the load	Coil voltage, contact ratings [TBC]
Load circuit	Low-voltage demonstration load	Type and rating [TBC]
Power supply	Supplies the controller	Voltage, current, backup [TBC]

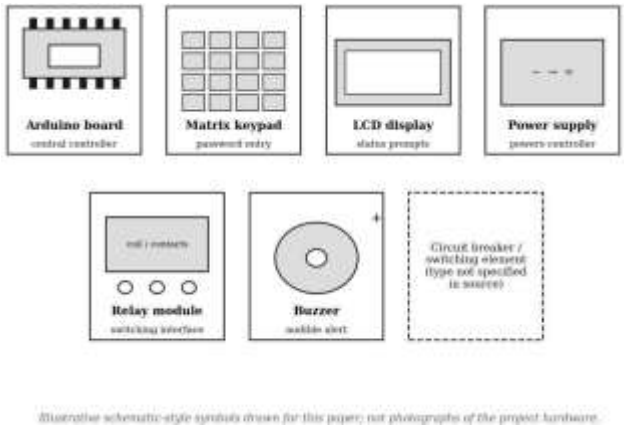


Fig -2: Component types used in the design (illustrative symbols, not photographs of the prototype).

Fig. 3 gives a conceptual schematic. Only the functional connections between blocks are shown; pin assignments, voltage levels and relay ratings are not available and are deliberately omitted. The figure must not be used to derive wiring, and mains-level switching is outside the scope of this work.

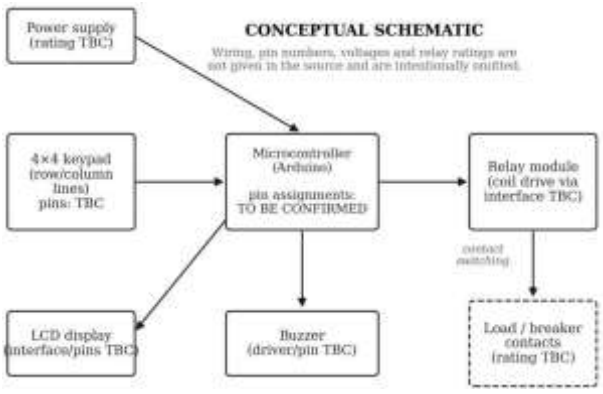


Fig -3: Conceptual circuit schematic showing functional connections. Pin numbers, ratings and wiring are unspecified [TBC].

VI. AUTHENTICATION AND SWITCHING-CONTROL ALGORITHM

The controller is modelled as the five-state machine of Fig. 5 with an initial state, S0. After initialization the controller waits for a password (S1), validates the entry (S2), and either performs the authorized operation (S3) or rejects the request with an alert (S4). Both outcomes return the controller to a safe idle state (S5) and then to the waiting state. A reset or loss of power returns the controller to S0. Table III states the expected response in each state.

Table -III: Functional states and expected switching responses

State	Condition	Expected switching response
S0 Initialization	Power-up or reset	Load not energized; relay state at start-up to be confirmed [TBC]
S1 Wait for entry	Prompt displayed	No change in relay state
S2 Validate entry	Entry complete	No change until validation result is known
S3 Authorized operation	Valid password and valid request	Relay driven to the requested state; status shown on LCD
S4 Rejected request	Invalid password	No switching; buzzer and LCD indicate rejection
S5 Safe idle	After S3 or S4	Relay state retained; return to S1

The proposed algorithm (Algorithm 1) is a design specification. The firmware of the prototype was not available, so the algorithm is not a description of existing code. Request selection (open or close) and password storage are not specified in the source and are left as design choices [TBC]. A distinguishing feature is that closing the circuit requires both a valid password and an explicit operator confirmation that maintenance is complete, entered as a separate step; the controller never closes the circuit on its own.

```
Algorithm 1 (proposed): password-authorized switching
on reset or power-up: relay <- OPEN (load de-energized);
  show prompt
loop:
  entry <- read_keypad_entry()
  if entry == stored_password then
    request <- read_request()   // OPEN or CLOSE [TBC]
    if request == OPEN then relay <- OPEN
    else if request == CLOSE and
    operator_confirms_work_complete()
      then relay <- CLOSE   // only on explicit input
    show status on LCD
  else
    buzzer <- ALERT; show 'incorrect'; relay unchanged
    failures <- failures + 1   // attempt limit/lockout
    [TBC]
  return to safe idle; continue loop
```

Fig. 4 shows the corresponding flowchart and Fig. 5 the state model. Neither implies a verified hardware interlock: all safety behaviour here depends on the controller and relay functioning correctly.

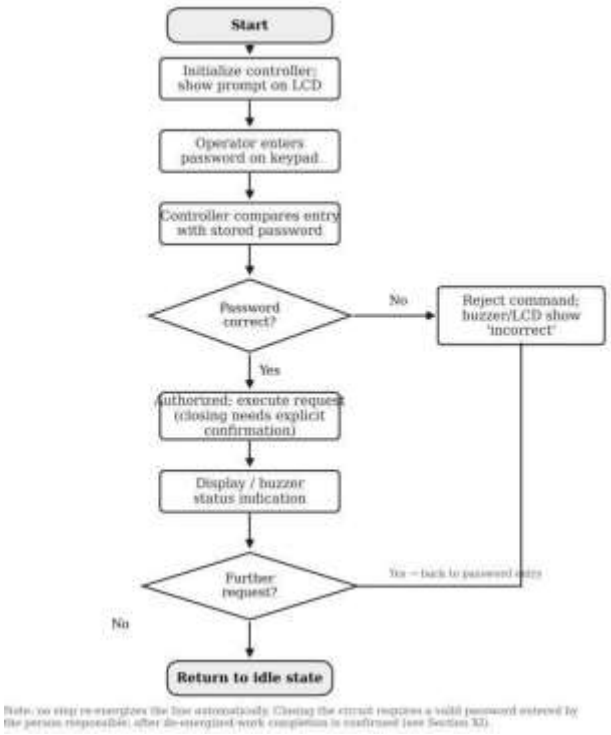


Fig -4: Password authentication and switching flowchart (proposed). The flowchart contains no automatic re-energization step.

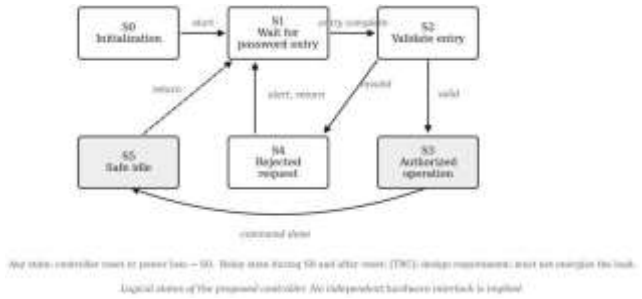


Fig -5: Switching-control state diagram (proposed). No independent hardware interlock is implied.

VII. EXPERIMENTAL SETUP AND EVALUATION METHOD

No experiments have been reported. This section defines a protocol that should be completed before the paper is submitted. All testing uses a low-voltage demonstration load with no mains connection. The test board arrangement is visualized in Fig. 6 and the test circuit in Fig. 7.

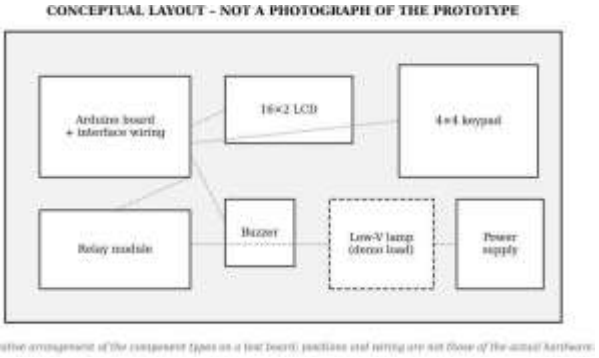


Fig -6: Conceptual visualization of the test-board arrangement. Not a photograph of the prototype.

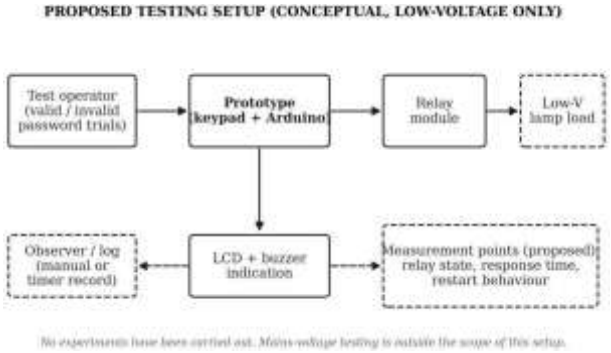


Fig -7: Proposed low-voltage evaluation setup (conceptual). No experiments have been performed.

Table IV lists the tests, measurement methods and acceptance criteria. Trial counts are chosen so that a zero-failure result gives a stated confidence bound: if no failure occurs in n independent trials, the 95% upper confidence bound on the per-trial failure probability is approximately 3/n (the "rule of three"); n = 100 therefore bounds it near 3%. Response time is measured from the final key press to the relay state change, using a logic analyser or oscilloscope on the keypad scan line and relay drive output [TBC], and reported as mean, standard deviation and maximum. Any failure must be reported with its conditions.

Table -IV: Experimental test cases, measurements and acceptance criteria (proposed)

Test	Method and number of trials	Acceptance criterion
Valid password	Enter the valid password, 100 trials; record relay state	Accepted in every trial
Invalid password	100 distinct incorrect entries, including near-misses and single-key errors	No relay action; alert in every trial
Unauthorized attempts	Arbitrary keys and repeated failures (at least 20 consecutive)	No switching; documented behaviour after repeated failures
Relay response time	30 valid operations; timestamp key press and relay output	Mean, SD and maximum reported; no missed operation
Buzzer and LCD	Trigger every defined state and alert	Correct message or tone for each
Controller reset	20 resets with relay open and 20 with relay closed	Load not energized after reset (objective O3)
Power interruption and recovery	20 supply interruptions in each relay state, varied duration	Defined state on recovery; never an unintended closure
Safe-state behaviour	Keypad disconnection, stuck key, noise on inputs	System remains in S1 or S5 with no switching

VIII. RESULTS AND DISCUSSION

Experimental measurements are not yet available, and no result table is presented. Presenting estimated times or success rates would imply validation that has not occurred. The discussion below is therefore analytical and bounded to what the design implies.

First, correct acceptance and rejection of passwords is a deterministic comparison; any failure would indicate a firmware or input-handling defect, such as keypad bounce, and the 100-trial protocol is intended to expose such defects rather than to estimate a rate. Second, relay response time will be dominated by the relay's mechanical operating time and the output driver rather than by the comparison, but this should be confirmed by measurement. Third, the most informative tests are those for reset and power interruption (objective O3): the property that matters is the absence of an unintended closure, which a single observed occurrence would be sufficient to refute.

A completed Table V of observed results should be added once the tests in Table IV are carried out, and any objective not met should be stated in the conclusion.

IX. LIMITATIONS AND SAFETY ANALYSIS

Authorization is not isolation. A password restricts who can operate the breaker. It does not prove that the line is de-energized, grounded or safe to touch. Independent isolation, lockout/tagout, testing for absence of voltage and local grounding remain essential [8], [9], and this device is an additional administrative-style control only. Fig. 8 summarizes the residual risks in comparison with conventional switching.

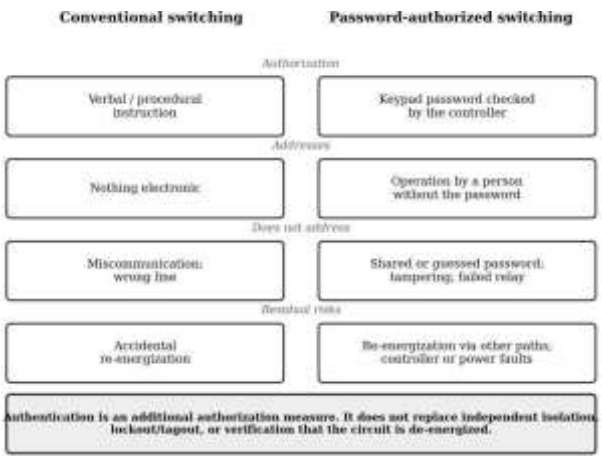


Fig -8: Safety-oriented comparison of conventional switching and password-authorized switching.

Automatic re-closing is hazardous. The prototype description includes a relay action that closes the circuit automatically if the lineman forgets to do so. This paper does not adopt that feature. Automatic closing replaces a deliberate decision by a timer or default; if the crew is still on the line, for example delayed, working at a second location or unable to respond, closing energizes conductors they are working on, which is exactly the hazard the system is meant to prevent. A forgotten step is better handled by escalating reminders (buzzer, LCD), leaving the circuit open, and requiring a valid password plus an explicit confirmation, ideally independently verified, that all personnel are clear and work is complete (Algorithm 1, lines 7–8).

Password compromise. Passwords can be shared, observed, guessed or forgotten. For a keypad of 16 keys and a password of k key presses, the search space is 16^k when all keys are allowed. Without an attempt limit, an exhaustive search needs on average half of that number of attempts:

E[attempts] = 16^k / 2 (e.g. k = 4: 65 536 / 2 = 32 768; k = 6: about 8.4 million)

These are computed values for the stated assumptions, not measurements. In practice, observed or shared passwords are a more likely route than exhaustive search; attempt limiting and per-user credentials are mitigations that are not yet part of the design. A related operational issue is ownership: if only the person who set the password can reclose the breaker, recovery when that person is unavailable needs a defined procedure.

Physical tampering and bypass. Exposed wiring, a removable controller or a parallel manual switch can bypass the system. The enclosure and the physical route of the switched circuit are therefore part of the safety case.

Relay and controller faults. Welded contacts can leave a line energized when the controller commands opening; a stuck or failed coil can prevent switching. Firmware faults, brown-outs and watchdog resets may produce undefined outputs unless the relay driver defaults to open. Feedback from an independent contact or voltage sensor would allow the state to be verified, but is not part of the present design.

Power loss and unintended re-energization. The behaviour at start-up and after power restoration must be to leave the load de-energized (objective O3). Re-energization through paths outside the controller cannot be prevented by it.

Human factors. Password entry delay under stress, forgotten passwords and the temptation to share a credential for convenience all weaken the control. Procedural training and clear status indication mitigate but do not eliminate these risks.

X. CONCLUSION AND FUTURE WORK

This paper specified the architecture, controller states, a proposed algorithm and an evaluation protocol for an Arduino-based password-authorized switching system for lineman safety, and analysed its residual risks. The basic concept is established in earlier work; the contribution lies in the explicit state model and safe-behaviour requirements, the rejection of automatic re-closing in favour of deliberate authorization with confirmation, and a reproducible low-voltage test plan. Because no measurements are available, no claim of effectiveness is made, and the system does not guarantee lineman safety. It should be used only as an additional measure alongside isolation, lockout/tagout and verification of de-energization.

Future work, none of which is implemented, includes completing the evaluation of Section VII; adding attempt limiting and per-user or one-time credentials; logging of attempts and operations; independent state feedback from the load side; a hardware interlock that does not depend on the microcontroller; a defined fail-safe relay default and backup supply; and, if remote features are added, a security analysis of the communication path.

REFERENCES

[1] M. G. Hudedmani, N. Ummannanavar, M. D. Mudaliar, C. Sooji, and M. Bogar, "Password based distribution panel and circuit breaker operation for the safety of lineman during maintenance work," Adv. J. Grad. Res., vol. 1, no. 1, pp. 35–39, Feb. 2017. [Online]. Available: https://journals.aijr.org/index.php/ajgr/article/view/160

[2] S. A. Soomro et al., "Design of IoT based protection system for distribution breakers using Arduino," QUEST Res. J., Dec. 2021, doi: 10.52584/QRJ.1902.05. [Online]. Available: https://publications.quest.edu.pk/ojs/index.php/qrj/article/view/194 (volume and pages [TBC])

[3] R. G. Shriwastava, P. C. Tapre, R. M. Rewatkar, and S. M. Choudhary, "Hardware implementation of safety smart password based GSM module controlling circuit breaker," Int. J. Appl. Power Eng., accepted Jan. 2025. [Online]. Available: https://ijape.iaescore.com/index.php/IJAPE/article/download/21538/13325 (volume, pages and DOI [TBC])

[4] A. N. S. Mohamed, A. A. A. Ahmed, M. K. I. Mohamed, and M. M. E. Jala Aldeen, "Password based circuit breaker using Arduino Uno," B.Sc. thesis, Coll. Eng., Sudan Univ. Sci. Technol., Khartoum, Sudan, 2020. [Online]. Available: http://repository.sustech.edu/handle/123456789/26413

[5] J. Veena, G. Srivani, Afreen, M. Sunil Kumar, J. Santhosh, and K. B. V. S. R. Subrahmanyam, "Electric lineman protection using user changeable password based circuit breaker," Int. J. Curr. Eng. Sci. Res., vol. 2, no. 5, pp. 44–49, 2015. (Verified only as cited in [1].)

[6] P. N. Mahadik, P. A. Yadav, S. B. Gotpagar, and H. P. Pawar, "Electric line man safety using micro controller with GSM module," Int. J. Sci. Res. Dev., vol. 4, no. 1, pp. 205–207, 2016. (Verified only as cited in [1].)

[7] "Keypad/Bluetooth/GSM based digital door lock security system," in Proc. Int. Conf. Commun. Signal Process. (ICCASP 2016), Atlantis Press, Dec. 2016, pp. 726–734, doi: 10.2991/iccasp-16.2017.102. (Author list [TBC] from the DOI record.)

[8] Occupational Safety and Health Administration, "The control of hazardous energy (lockout/tagout)," 29 CFR 1910.147. [Online]. Available: https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.147

[9] Occupational Safety and Health Administration, "Control of hazardous energy (lockout/tagout)," overview page (refers to 29 CFR 1910.269 for power generation, transmission and distribution). [Online]. Available: https://osha.gov/SLTC/controlhazardousenergy/index.html

[10] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 1: General Requirements, IEC 61508-1:2010, Apr. 2010.