The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 2025

Volume 38, Pages 816-823

IConTES 2025: International Conference on Technology, Engineering and Science

# Retrofit Kit Design That Converts Industrial Locks into Electromechanical Smart Locks

**Selahattin Mert Aydin**
Mesan Locks INC

**Engin Gunes**
Mesan Locks INC

**Abstract**: This paper presents the design and development of a modular electromechanical retrofit kit that upgrades traditional quarter-turn mechanical cam locks into secure, digitally controlled smart locking systems. Quarter-turn locks are widely used in school lockers, server cabinets, electrical distribution panels, and industrial enclosures, but they offer limited access control, no auditability, and minimal protection against unauthorized manipulation. The proposed kit addresses these issues by introducing a compact, low-cost electromechanical module that mounts externally without altering the existing lock body. The system uses a 3.3 V DC gear motor controlled by an ATmega48P microcontroller and DRV8837 driver, providing controlled 90° rotation after successful RFID authentication. Optional LED indicators assist the user during operation. To enhance security, the device enforces a temporary self-locking (lockout) period after multiple failed access attempts, increasing security. The retrofit kit's improvement design enables adaptation to different key geometries, ensuring compatibility with a variety of lock formats. Designed for easy installation, the kit can be mounted within minutes and allows end-users to digitally upgrade their mechanical locks without replacing the mechanical body. Prototype tests confirm system stability, reliable authentication, and low power consumption. Long-term usability is supported by a standard Li-Po battery power supply, achieving an estimated 4500–5000 lock/unlock cycles per 1000 mAh battery charge. The kit is intended as a commercial solution for modernizing physical security infrastructure in industries environments, bridging legacy hardware with modern access control needs.

**Keywords**: Smart lock, Electromechanical kit, Access control, Industrial design, Digital transformation

## Introduction

With the rapid advancement of technology, electromechanical locking systems are increasingly replacing traditional mechanical locks. These systems not only increase physical security but also enable the digital tracking and management of access data, essential for modern security infrastructures. The increasing need for access control in modern institutions and public spaces has LED to a shift towards electronic solutions. Traditional keys are prone to loss or duplication and do not provide event tracking (Uppuluri & Lakshmeeswari, 2023). Contemporary requirements in educational and commercial environments require centralized credential control and auditing capabilities (Lin et al., 2021; Khan et al., 2023).

However, replacing existing mechanical systems with completely new electromechanical alternatives is often costly and results in the disposal of still-functional mechanical locks. Such practices lead to unnecessary financial investments and increased environmental waste, highlighting the need for more sustainable upgrade strategies. This study focuses on the development of a modular retrofit kit that transforms traditional mechanical locks into smart electromechanical locking systems without requiring the removal or disposal of existing hardware. The design includes a compact housing, a low-voltage gear motor, and a microcontroller-based

authentication system. Users manipulate the lock using their RFID card, which triggers the rotation of a special insert that activates the cam lock mechanism. The kit is adaptable to various key geometries, allowing users to digitize their locking systems without replacing existing mechanical components.

## Method

### Mechanical Design

The retrofit kit is designed to be compatible with standard quarter-turn cam locks commonly used in steel furniture, electrical enclosures, transportation equipment, and server cabinets. These locks typically have standard body profiles with circular, double-D, or 45° cross-sections, with diameters ranging from 16 mm to 22 mm (Figure 1).

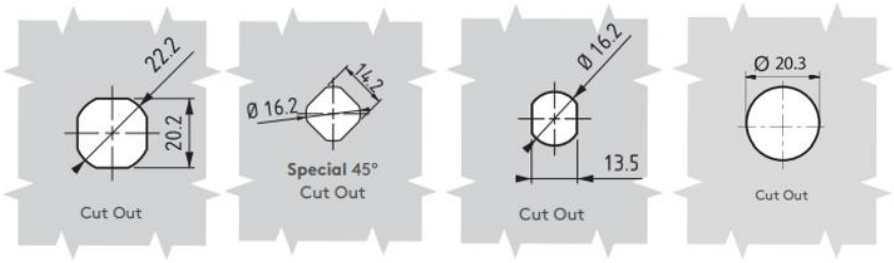


Figure 1. Standard cut-out dimensions for cam locks compatible with the retrofit kit

Manual key operation has been replaced with a motorized operating mechanism, enabling the mechanical lock to operate as a smart electromechanical system. Unlocking is triggered by RFID-based user authentication, and after verification, the rotation of the motor is achieved. The motor's rotation is transmitted to the key via a gear mechanism. Representative examples of quarter-turn cam locks supported by the retrofit mechanism are shown (Figure 2).

Figure 2. Common types of commercial quarter-turn cam locks supported by the retrofit kit

The mechanical components are compact and lightweight, designed to fit into an external housing that can be mounted using a single screw through a 6-8 mm hole. Installation requires only basic tools and does not permanently modify the existing lock. During operation, the motor rotates 90° to unlock the lock and automatically returns to the locked position after a short delay. Figure 3 provides a transparent view of the internal mechanism and the direction of motor rotation.

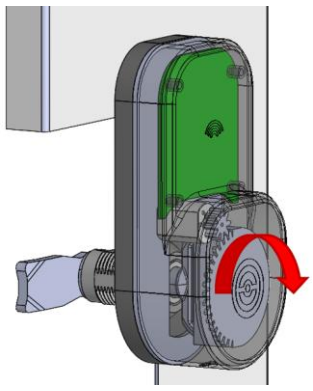

Figure 3. Transparent front view of the smart lock kit showing internal components and motor rotation direction

The proposed approach offers a low-cost, sustainable, and minimal-intervention solution for upgrading mechanical locks to smart, automated systems. This modular design contributes to both economic efficiency and environmental sustainability by providing easy maintenance, scalability, and long-term reliability (Wolniak, 2024; Xin et al., 2020; Roy et al., 2018).

## Electrical Design

The electronic architecture of the retrofit kit is built around the ATmega48P microcontroller, selected for its balance of energy efficiency, functional capacity, and compact physical footprint. This controller is tasked with managing key operations such as RFID-based authentication, motor control, and the signaling of visual and auditory feedback. To actuate the locking mechanism, a DRV8837 H-bridge motor driver enables bidirectional control of a 3.3 V brushed DC gear motor. The entire system is powered by a single-cell 3.7 V lithium-polymer (Li-Po) battery, regulated to 3.3 V via a low-dropout (LDO) converter. This arrangement ensures reliable performance while keeping current draw and thermal output within safe limits.

In practice, the motor draws approximately 130 mA during actuation, but since the motion duration is brief-generally under one second-the energy consumed per locking cycle remains low. To extend battery life, the system is engineered with a strong focus on energy conservation. When idle, the device enters a deep sleep state, drawing less than 3 mA. Power-saving is achieved not only through hardware-level design but also through firmware strategies. The microcontroller utilizes sleep and power-down modes, reactivating only in response to external interrupts-typically triggered when the RFID module detects a card.

To avoid unnecessary energy drain, the RFID reader and other peripherals are only powered when needed. This is governed by an interrupt-driven control loop that activates subsystems momentarily and then returns the system to a dormant state. Peripheral components such as timers, ADCs, and communication interfaces are likewise disabled unless actively in use. This selective activation strategy ensures that the system remains efficient even during long periods of inactivity. These measures align with established practices in the design of low-power embedded systems (Jayakumar et al., 2014). Figure 4 provides an overview of the system's electrical components and their interconnections.

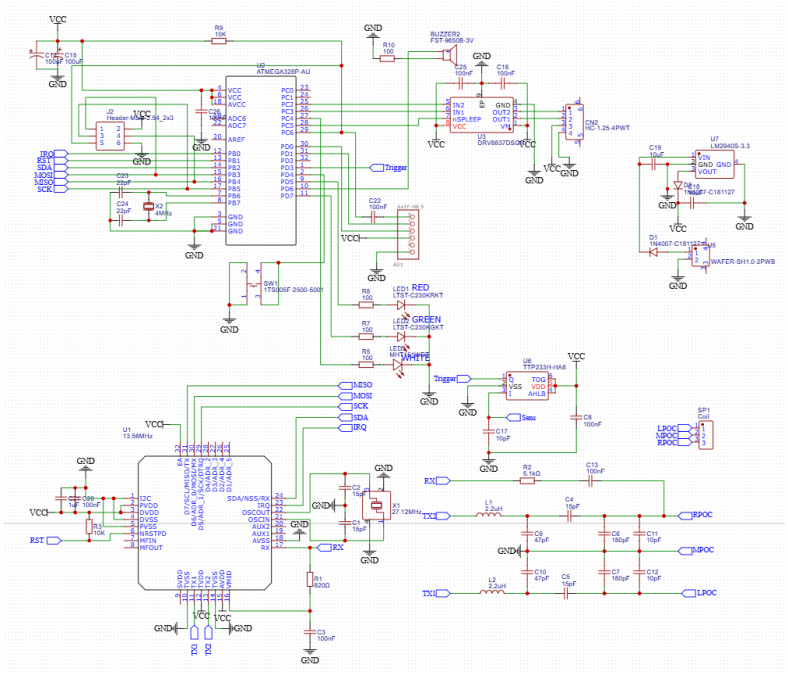


Figure 4. Electrical circuit diagram of control and motor systems

The main circuit includes the microcontroller, motor driver, voltage regulator, a 13.56 MHz ISO/IEC 14443-compliant RFID reader, and a user feedback interface consisting of dual-color LEDs and a piezoelectric buzzer. The visual and acoustic signals assist users during lock operation. For instance, a brief green flash and a beep confirm successful authentication, while a red light and a distinct tone indicate access denial or an error.

From a hardware reliability standpoint, flyback protection and careful PCB layout were prioritized to safeguard sensitive components. High-current traces are kept short, and analog and digital sections are isolated to reduce electromagnetic interference. Figure 5 illustrates the compact 3D PCB layout, where all major components, including the MCU and driver circuitry, are housed behind the motor inside the enclosure.

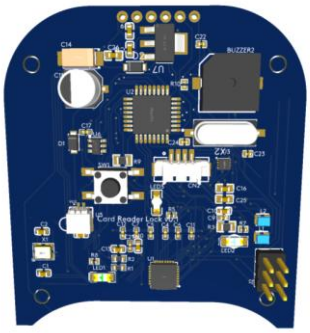

Figure 5. 3D View of PCB with Atmega48P and DRV8837 motor driver

The firmware embedded in the ATmega48P manages the complete authentication process and motor actuation sequence. When a valid RFID card is presented, the controller matches the card ID with pre-stored credentials in flash or EEPROM memory. If authorized, the motor is activated to rotate approximately 90°, unlocking the mechanism. This motion is either time-limited or halted through a current-sensing routine that detects when the cam mechanism reaches its endpoint. After unlocking, the system can re-lock automatically after a preset delay or wait for another user-triggered action, depending on firmware configuration. In the event of invalid credentials, access is denied, the red LED is illuminated, and an error tone is emitted. Failed attempts are tracked internally, and after three consecutive failures, the firmware initiates a temporary lockout—disabling input for 30 seconds and providing a warning signal. This security feature mitigates brute-force attempts and mirrors functionality found in commercial smart locking systems.

The feasibility of such a design has been supported by similar implementations in the literature, where cost-effective 8-bit microcontrollers have proven reliable in access control applications (Roy et al., 2018; San Hlaing, & San Lwin 2019; Hoque & Davidson, 2019). In prototype testing, the current system achieved between 350 and 400 full actuation cycles on a 1000 mAh battery, demonstrating suitability for long-term standalone use. To maintain usability in cases of battery depletion, the system includes a USB-C port, designed to support both emergency external powering and battery charging. If the internal battery is drained, users can connect a 5 V power source-such as a standard USB-C power bank-to restore functionality. Simultaneously, this connection begins charging the onboard battery.

As depicted in Figure 6, the USB-C port is accessible from the side of the housing and does not disrupt the overall compact form of the device. Once powered and authenticated, the lock is actuated normally and returns to the locked position either automatically or on user command. This dual-purpose input ensures system continuity, especially in field environments where battery replacement may not be immediately possible.

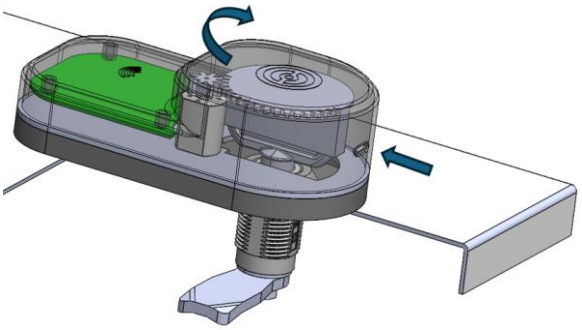

Figure 6. Internal layout and dual-function USB-C input for external powering and battery charging

When external power is supplied and authentication is successful, the motor performs the unlock and subsequently re-locks after a set timeout or user prompt. This dual-function feature enhances operational reliability in field deployments and reduces service interruptions.

**Assembly and Integration**

A primary objective of the retrofit kit is easy installation without altering the existing lock mechanism. If needed, a small hole is drilled into the cabinet or locker door. The device is then aligned so that its motor-driven insert fits into the back of the cam lock and is secured with a single screw passing through the housing and fastened from the inside. This screw also maintains alignment. Figure 7 shows the assembled kit mounted externally on a metal locker, demonstrating its mechanical integration.

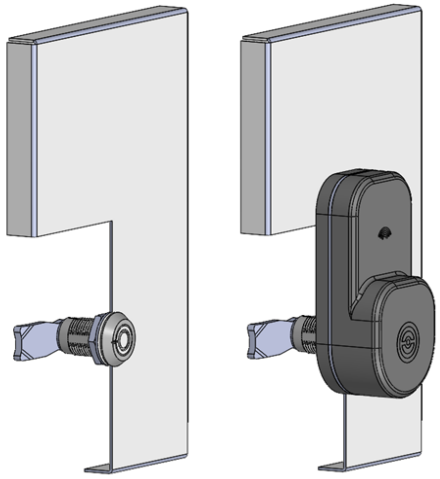

Figure 7. Installed smart lock kit on a metal locker

The housing is compact and low-profile, slightly larger than the lock, ensuring it fits even on densely packed panels. Internal contours help align it with the existing lock nut, while molded markings guide installation. The key insert is connected before securing the housing, and minor misalignments are tolerated, allowing reliable motor operation. Both mechanical and electrical systems are modular for easy upgrades and maintenance. The circuit board can be detached for servicing, and external components like the RFID reader or keypad connect via slim cables routed discreetly through the same or adjacent hole. The PCB also includes space for future BLE or Wi-Fi modules to enable wireless functionality. This approach preserves the mechanical override: the user can revert to key operation by removing the housing, or-if the design permits-use the key without removal, thanks to the motor's pass-through coupling.

Overall, the kit is designed for scalable deployment. Installation requires minimal tools and time, making it practical for retrofitting many units in settings like schools or data centers. The only permanent change is a small screw hole—ensuring that legacy infrastructure remains largely intact while gaining smart capabilities.

**Prototype Testing**

A fully functional prototype of the smart lock retrofit kit was developed and tested for mechanical, electrical, and authentication performance under realistic conditions. Over 500 lock-unlock cycles were performed using a metal locker, with tests including door misalignment to evaluate torque reliability. The system consistently completed 90° actuation without motor stalls or mechanical degradation.

*Authentication and Security*

Tests included RFID card and keypad PIN inputs across multiple users. Valid credentials unlocked the system in under two seconds; invalid ones triggered visual (LED) and acoustic (buzzer) feedback. After three failed attempts, the system entered a 30-second lockout, effectively preventing brute-force access.

*Power Consumption*

Power draw during standby remained below 3 mA, while peak motor activity reached ~130 mA for ~1 second per actuation. A 1000 mAh Li-Po battery supported approximately 350–400 cycles. Low-battery warnings via blinking red LED activated reliably before voltage dropped below safe thresholds.

*Fail-Safe and Data Retention:*

Tests confirmed that the system safely halted motor operation during jams. Credential memory was retained through power loss. Physical tampering (e.g., prying) was unsuccessful, and the mechanical override via original key remained functional. Overall, the prototype validated the system's durability, low power consumption, secure authentication, and ease of integration, confirming its suitability for real-world use (Khan et al., 2023; Uppuluri & Lakshmeeswari, 2023).

## Results and Discussion

The developed retrofit kit exhibited robust and consistent performance across more than 500 actuation cycles, maintaining mechanical and electrical reliability even under conditions involving mild misalignment or uneven door tension. Throughout testing, no detachment, stalling, or synchronization errors were recorded, affirming the structural integrity and operational stability of the system.

Authentication using RFID cards was rapid and accurate, with successful access consistently completed in under two seconds. The absence of keypad input simplified user interaction and eliminated potential failure points, contributing to both reliability and intuitive operation. Credential matching remained accurate across multiple RFID tags, validating the firmware's authentication handling and memory management.

Power efficiency was another key strength. The combination of low quiescent current, optimized actuation routines, and interrupt-driven sleep mode allowed the system to achieve approximately 350–400 locking cycles per 1000 mAh battery charge. This level of performance supports extended maintenance intervals and is well aligned with the low-power design objectives. The inclusion of algorithmic power management—such as disabling non-critical peripherals and periodic RFID polling-further minimized standby energy use.

Security features functioned as intended: after three consecutive failed authentication attempts, the system entered a temporary lockout state, effectively deterring unauthorized access and brute-force attempts. The visual and auditory feedback provided clear cues to the user at each stage of operation, and the mechanical override capability was preserved for emergencies, ensuring that physical key access remained viable in case of battery failure or electronic malfunction.

Installation proved to be straightforward and repeatable. On average, mounting the kit-including alignment and securement-took less than a minute using only basic tools. The modular and non-invasive design allowed integration without modifying the existing lock or enclosure, preserving the original aesthetics and mechanical function. Cost analysis indicated that the retrofit solution could be implemented at 40–60% less than full smart lock replacements, offering considerable savings in both materials and labor.

While the current prototype does not include wireless connectivity, the PCB layout reserves space for optional BLE or Wi-Fi modules, enabling future remote access or cloud-based monitoring. Additional areas for refinement include user interface enhancements, improved tamper detection (e.g., housing removal alerts), and better battery replacement ergonomics.

In summary, the prototype effectively delivered on its goals of energy efficiency, secure access control, ease of installation, and compatibility with legacy lock infrastructure. Its modular architecture and minimal power requirements position it as a scalable and sustainable solution for digitally upgrading mechanical locks in institutional and industrial settings.

## Conclusion

This study demonstrated a practical and cost-effective approach for upgrading mechanical quarter-turn locks with smart access control functionality. The proposed retrofit kit integrates seamlessly with existing lock hardware, offering digital authentication via RFID cards entry, visual and indicator feedback, lockout protection,

and modular mechanical compatibility. By retaining the original lock mechanism, the system enhances security and manageability without sacrificing the reliability or emergency override capability of traditional keys.

Prototype development and testing confirmed the system's robustness, low power consumption, and user-friendly installation. The device can be deployed in environments such as schools, offices, and industrial facilities with minimal modification and training requirements. Compared to full smart lock replacements, the retrofit solution presents a substantial advantage in cost, time, and sustainability by modernizing access infrastructure while preserving existing assets.

While the current design addresses essential access control needs, future enhancements could expand its capabilities. Wireless modules, for instance, could enable remote monitoring and integration into building automation systems. The modular architecture also allows adaptation to a broader range of lock types. In summary, the retrofit kit represents a scalable, maintainable, and efficient solution for bridging legacy hardware with modern security demands.

## Recommendations

Based on the prototype evaluation and current limitations, the following recommendations are proposed to guide future developments and large-scale implementations:

*Wireless Connectivity:* Incorporate Bluetooth Low Energy (BLE) or Wi-Fi modules to enable remote unlocking, centralized credential management, and real-time access notifications via smartphones or enterprise software.

*Expanded Adapter Library:* Develop a broader range of interchangeable key inserts and mounting adapters to support additional lock types, including deadbolts, padlocks, or other specialty formats.

*Field Deployment Testing:* Conduct long-term trials in real-world, multi-user environments (e.g., schools or shared workspaces) to assess durability, usability, and environmental resilience under diverse usage conditions.

*Management Dashboard:* Design a software interface or API for device configuration, access log retrieval, and health monitoring (e.g., battery level, tamper alerts). This would enhance system oversight in institutional deployments.

*Enhanced Security Features:* Explore options such as biometric authentication (e.g., fingerprint or facial recognition), two-factor verification (RFID + PIN), and improved RFID encryption to address higher security requirements.

Implementing these enhancements would strengthen the retrofit kit's value proposition and broaden its applicability. All improvements should maintain the core principles of modularity, simplicity, and cost-efficiency to support scalable deployment.

## Scientific Ethics Declaration

* The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

## Conflict of Interest

* The authors declare that they have no conflicts of interest

## Funding

* This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology, Engineering and Science ( www.icontes.net ) held in Antalya/Türkiye on November 12-15, 2025.

## References

Alzhrani, A. A., Balfaqih, M., Alsenani, F., Alharthi, M., Alshehri, A., & Balfagih, Z. (2024). Design and implementation of an IoT-integrated smart locker system utilizing facial recognition technology. *Engineering, Technology & Applied Science Research, 14*(4), 16000-16010.

Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. *International Journal of Networked and Distributed Computing, 7*(2), 85-92.

Jayakumar, H., Raha, A., & Raghunathan, V. (2014). Hypnos: An ultra-low power sleep mode with SRAM data retention for embedded microcontrollers. In *Proceedings of the 2014 International Conference on Hardware/Software Codesign and System Synthesis* (pp. 1-10).

Khan, S., Thapa, C., Durrani, S., & Camtepe, S. (2023). Access-based lightweight physical-layer authentication for the Internet of Things devices. *IEEE Internet of Things Journal, 11*(7), 11312-11326.

Krishna, G., Singh, R., Gehlot, A., Shaik, V. A., Twala, B., & Priyadarshi, N. (2024). IoT-based real-time analysis of battery management system with long range communication and FLoRa. *Results in Engineering, 23*, 102770.

Lin, C., Khazaei, H., Walenstein, A., & Malton, A. (2021). Autonomic security management for IoT smart spaces. *ACM Transactions on Internet of Things, 2*(4), 1-20.

McCluskey, P. (2002, May). Design for reliability of micro-electro-mechanical systems (MEMS). In *52nd Electronic Components and Technology Conference 2002* (pp. 760-762). IEEE.

Roy, S., Uddin, M. N., Haque, M. Z., & Kabir, M. J. (2018). Design and implementation of the smart door lock system with face recognition method using the Linux platform Raspberry Pi. *IJCSN-International Journal of Computer Science and Network, 7*(6), 382–388.

San Hlaing, N. N., & San Lwin, S. (2019). Electronic door lock using RFID and password based on Arduino. *International Journal of Trend in Scientific Research and Development, 3*(2), 799-802.

Uppuluri, S., & Lakshmeeswari, G. (2023). Secure user authentication and key agreement scheme for IoT device access control based smart home communications. *Wireless Networks, 29*(3), 1333-1354.

Wolniak, R. (2024). *The usage of smart locks in smart home.* Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska.

Xin, Z., Liu, L., & Hancke, G. (2020). AACS: Attribute-based access control mechanism for smart locks. *Symmetry, 12*(6), 1050.

## Author(s) Information

**Selahattin Mert Aydin**
Mesan Locks INC, Mimar Sinan Mah Ulubey Caddesi Fabrikalar Sitesi, No: 7 34570 Silivri, İstanbul, Türkiye

**Engin Gunes**
Mesan Locks INC, Mimar Sinan Mah Ulubey Caddesi Fabrikalar Sitesi, No: 7 34570 Silivri, İstanbul, Türkiye
Contact e-mail: engingunes@essentra.com

**To cite this article:**

Aydin, S. M., & Gunes, E. (2025). Refrofit kit design that converts industrial locks into electromechanical smart locks. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 38,* 816-823.