Design and Implementation of an NFC Reader Integrated with CAN Bus for Secure Identification Systems

Aniket Dattatray Thete[1], Prof. P. A. Kale[2]

[1,2]Department of Electronics & Telecommunication Engineering, Adsul's Technical Campus, Chas, Ahmednagar, Maharashtra – 414008

Abstract

This paper presents the design and development of a secure, real-time NFC (Near Field Communication) reader system integrated with a Controller Area Network (CAN) communication interface. The system is designed for applications such as automotive access control, industrial user authentication, and secure machine operation. The hardware consists of the ST25R3920B NFC front-end, the RL78 microcontroller, and the TJA1042BT CAN transceiver. The system supports reading of NFC tags, low power operation, and robust CAN-based data exchange. Comprehensive testing validates the system's stability, RF performance, and communication integrity, demonstrating its readiness for deployment in secure, rugged environments. *Index*

INTRODUCTION

Near Field Communication (NFC) technology enables secure and intuitive wireless communication between two electronic devices at short distances, typically under 4 cm. Originating as an enhancement of Radio-Frequency Identification (RFID), NFC has found applications in contactless payments, identity verification, and smart access systems. This paper introduces a robust embedded NFC reader system that integrates a microcontroller and CAN transceiver to provide secure identification and real-time data communication in automotive and industrial contexts. The advancement of NFC technology, particularly with its integration into smartphones, smart cards, and embedded systems, has revolutionized human-machine interaction by eliminating the need for physical contact, cables, or manual input. It operates at a standard frequency of 13.56 MHz and supports several communication standards, including ISO/IEC 14443, ISO/IEC 18092, and ISO/IEC 15693. Its popularity has soared due to the growing demand for cashless transactions, digital identity verification, and IoT-based automation. Major mobile payment systems like Google Pay, Apple Pay, and Samsung Pay all rely on NFC technology to enable secure and fast transactions with a simple tap.

However, to build a practical and scalable NFC-based solution, especially for automotive or industrial use, certain challenges must be addressed. These include ensuring data security, maintaining low power consumption, minimizing electromagnetic interference, and achieving robust communication in harsh or noisy environments. Moreover, the secure and deterministic exchange of data with other system modules—such as vehicle control units, factory automation devices, or smart locks—necessitates a reliable communication backbone. This is where the CAN is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. Developed by Bosch, it has become the de facto standard in automotive and industrial applications due to its high immunity to noise, real-time capability, fault tolerance, and minimal wiring requirements. Integrating NFC technology with CAN thus provides a compelling solution for environments that demand real-time, secure, and decentralized communication.

The system is centered around the ST25R3920B, a high-performance automotive-grade NFC reader IC developed by STMicroelectronics. It is supported by the Renesas RL78 microcontroller, known for its ultra-low power operation and rich peripheral support, and the TJA1042BT CAN transceiver, which ensures reliable communication with other control modules over the CAN bus

SYSTEM OVERVIEW

The proposed NFC Reader system is a compact, embedded solution designed to provide secure and efficient access control by integrating Near Field Communication (NFC) with the Controller Area Network (CAN) protocol. It employs the ST25R3920B NFC reader IC for detecting and authenticating NFC tags or devices, a Renesas RL78 microcontroller for managing system logic and data processing, and the TJA1042BT CAN transceiver to The system supports real-time identification, battery monitoring, and diagnostic reporting over CAN, making it highly suitable for automotive, industrial, and smart automation applications. Emphasis is placed on low power consumption, electromagnetic immunity, and robustness, ensuring reliable operation even in electrically noisy and

METHODOLOGY

The development of the NFC Reader system integrated with Controller Area Network (CAN) communication was executed through a systematic and modular engineering methodology. The approach focused on achieving reliability, scalability, and compliance with automotive and industrial standards.

The process began with a detailed requirement analysis to identify the functional needs of a secure, real-time embedded identification system. Based on these requirements, critical hardware components were selected. The ST25R3920B from STMicroelectronics was chosen as the NFC front-end due to its automotive-grade robustness, ISO compliance, and low power card detection capabilities. The Renesas RL78 microcontroller was selected for its low-power operation, rich peripheral support (SPI, ADC, GPIOs), and proven reliability. For communication, the TJA1042BT CAN transceiver was selected for its high-speed capabilities and fault tolerance, essential in vehicle and industrial environments.

The hardware design phase involved creating a schematic that included all critical components along with power management circuitry. This included transient voltage suppressors, automotive-rated capacitors and resistors, ferrite beads for EMI suppression, and a TPS7B8650 LDO regulator for providing a clean 5V supply. The antenna circuit was carefully designed and tuned for optimal 13.56 MHz resonance to ensure effective NFC performance. The PCB was designed with a focus on minimizing noise, optimizing power distribution, and ensuring mechanical stability for deployment in harsh environments.

In the software development phase, a modular firmware architecture was implemented using the Renesas e^2 studio IDE. This included SPI drivers for communicating with the NFC IC, CAN drivers for transmitting UID and status messages, and ADC modules for battery voltage monitoring. Power-saving modes, error handling mechanisms, and interrupt-based NFC tag detection were incorporated for efficient operation.

During the integration phase, communication between the NFC IC and the MCU was validated through SPI transactions, and CAN communication was tested using a CAN analyzer. System-level testing was conducted with simulated and real NFC tags. Diagnostic features such as low battery warnings and CAN error reporting were also verified

RESULT & DISCUSSION

The NFC Reader system, designed with integrated Controller Area Network (CAN) communication, underwent comprehensive testing and validation to assess its functional performance, robustness, and suitability for deployment in automotive and industrial environments. The system was evaluated in both isolated and integrated conditions, covering each functional block—NFC tag detection, microcontroller operation, CAN message handling, power regulation, and software execution. This section details the outcomes of these tests and discusses their implications in the context of secure, real-time embedded applications.

A. NFC Reader Performance

The NFC module, built around the ST25R3920B NFC reader IC, was tested with ISO14443-A compliant NFC cards and smartphones. The system consistently detected passive tags within a range of 2.5 to 4 cm, even in noisy environments with electromagnetic interference. The reader demonstrated fast card detection, typically under 100 milliseconds, and extracted the UID (Unique Identifier) of tags reliably.

The Low Power Card Detection (LPCD) feature was particularly effective. It enabled periodic scanning while maintaining low power consumption, making the system highly efficient for always-on use cases such as door access control or keyless vehicle entry. The system could detect standard 1k S50 tags as well as mobile-based NFC credentials, showing broad compatibility with commercial NFC devices.

Antenna tuning was validated using RF analysis tools. The antenna showed a resonance peak at 13.56 MHz with a measured quality factor (Q-factor) between 18 and 23, within optimal NFC operating parameters. This confirmed the antenna design's efficiency and its ability to maintain signal integrity across different environmental conditions.

B. CAN Communication Results

CAN communication, facilitated by the TJA1042BT CAN transceiver, was tested across multiple nodes in a simulated automotive network using a CAN analyzer and oscilloscope. NFC tag data was transmitted over the CAN bus at a standard bit rate of 500 kbps. The latency from tag detection to CAN message transmission was measured consistently under 2 milliseconds, fulfilling the requirements for real-time applications.

The system demonstrated low average bus load, typically under 10%, indicating efficient use of bandwidth even during frequent NFC interactions. Error handling mechanisms such as re-transmissions and CAN error frames were properly triggered during simulated faults, confirming compliance with ISO 11898-2 standard specifications.

The system successfully communicated with other Electronic Control Units (ECUs) in the simulated network, allowing data such as tag UID, authentication success/failure status, and diagnostic flags (e.g., low battery) to be transmitted and received without data loss or corruption.

C. Microcontroller Operation and Firmware Response

The Renesas RL78 microcontroller (R5F10PBELNA) managed NFC tag detection, battery voltage monitoring via ADC, and CAN communication effectively. SPI communication between the MCU and

NFC IC was validated using logic analyzers, showing clean clock and data signals with minimal jitter. The firmware was modular and interrupt-driven, ensuring rapid response to tag detections and CAN requests.

Firmware testing showed that: The main loop executed all tasks within 100 ms per cycle under typical operation. Interrupt latency was consistently low (within 10 µs), which is suitable for time-critical tasks. The system's sleep mode enabled power savings during idle periods, making it ideal for vehicle standby applications. The firmware included robust exception handling routines. During simulation of communication faults or hardware errors (e.g., tag misread, CAN disconnect), the MCU successfully logged faults and reported status over the CAN bus.

D. Power Supply and Stability

The power regulation circuit, centered around the TPS7B8650 LDO regulator, delivered a stable 5V output from a 12V automotive supply input. The regulator demonstrated high line and load regulation under varying input conditions ranging from 10V to 14.4V. Ripple voltage was kept below 30 mVpp even during full system operation, which is essential to ensure the proper functioning of sensitive analog and digital components.

The circuit also included transient protection features using TVS diodes and ferrite beads, which successfully suppressed voltage spikes during simulated load dumps and ESD events. Thermal testing showed no significant overheating under normal load, and thermal shutdown protection was never triggered during long-term operation, proving the regulator's robustness.

Battery monitoring through an analog voltage divider and internal 10-bit ADC allowed the MCU to detect low battery conditions accurately. A threshold was set at 10.8V; once the battery voltage fell below this, the system triggered a low battery warning message over CAN, which was confirmed during testing.

E. System Integration and Validation

The complete system was tested in an integrated environment simulating real-world usage. This included scenarios such as: Continuous tag presentation for access control. Multiple CAN nodes sending and receiving data. Sudden power loss and recovery. ESD discharge simulation at external interfaces. In all cases, the system responded reliably. The MCU resumed normal operation after power cycles, and the NFC reader re-initialized correctly. System stability was confirmed through a 72-hour stress test with repeated tag scans and continuous CAN messaging, during which no malfunctions were observed.

F. Practical Implications

The results of this testing validate that the developed NFC Reader system is not only functionally complete but also robust, scalable, and ready for real-world deployment. The combination of fast NFC tag detection, low latency CAN messaging, and real-time diagnostics makes it suitable for: Automotive access control (e.g., keyless entry, driver authentication).Industrial machine access with usage logging. Smart infrastructure where decentralized user verification is needed. Compared to traditional key-based or manual access systems, the NFC-CAN approach provides enhanced security, contactless convenience, and data traceability.

G. Limitations

Despite the successful implementation, the system has a few limitations. The NFC range is constrained to a few centimeters, which, while enhancing security, limits flexibility in certain use cases. Also, the current system does not support mobile-based app configuration or cloud data logging, which are desirable in future iterations.

Security Solutions for Communication Channels Securing 5G communication channels is crucial for preventing threats and leveraging advantages like SDN. IPsec is a common protocol for 4G-LTE and can be adapted for 5G using IPsec tunneling. While existing LTE security relies on authentication, integrity, and encryption, these methods suffer from high resource consumption overhead, and coordination issues, making them unsuitable for critical 5G infrastructure. Higher levels of 5G security are achieved through new mechanisms like physical layer security, Radiofrequency (RF) fingerprinting, asymmetric security schemes, and dynamically changing security parameters.

CONCLUSION

The development of the NFC Reader system integrated with Controller Area Network (CAN) communication presents a comprehensive and scalable solution for secure, real-time identification in automotive, industrial, and smart access control applications. The project aimed at designing a low-power, robust, and modular embedded system capable of reading NFC tags and securely transmitting the information to other control units using the CAN protocol. Through detailed design, implementation, and testing phases, the project successfully met its objectives and demonstrated practical viability in real-world use cases. The integration of the ST25R3920B NFC reader IC, Renesas RL78 microcontroller, and TJA1042BT CAN transceiver ensures that the system supports industry-standard communication protocols and performs reliably even in electrically noisy environments.

The NFC reader provided accurate and fast tag detection within the standard range, while the CAN interface facilitated low-latency communication with connected ECUs. This combination of technologies makes the system ideal for vehicle authentication, keyless entry, factory access systems, and tool or machine authorization. From a hardware perspective, the use of automotive-grade components and careful PCB design including transient voltage suppression, low dropout regulation, and EMI filtering contributed to the system’s electrical stability and durability. The firmware, built using modular architecture and interrupt-driven programming, ensured real-time responsiveness, efficient task management, and easy scalability for future feature additions.

The testing phase validated the functionality of each subsystem under varying voltage, environmental, and operational conditions. The system demonstrated strong performance in power management, NFC tag handling, data transmission over CAN, and self-diagnostic capabilities such as battery monitoring and error reporting. Overall, the project not only delivers a functional embedded NFC Reader system but also lays the groundwork for future enhancements. Potential improvements include the integration of biometric-enabled NFC tags, Bluetooth or Wi-Fi communication for mobile interaction, secure elements for cryptographic authentication, and cloud-based data logging for real-time analytics. These advancements would position the system for adoption in a broader range of applications aligned with the ongoing evolution of smart infrastructure and Industry 4.0.In conclusion, the designed NFC Reader system achieves its intended goals of providing a secure, contactless, and intelligent identification platform.

RESEARCH PAPERS:

List all the material used from various sources for making this project proposal

1. Madlmayr et al., "NFC devices: Security and privacy," IEEE ARES, 2008.
2. STMicroelectronics, "ST25R3920B Datasheet", 2023.

3. Bosch, "CAN Specification 2.0", Stuttgart, 1991.
4. Korkalainen et al., "Secure driver authentication via NFC", IEEE VTC, 2017.
5. Wang & Liu, "Low-power MCU-based NFC systems", IJESA, 2021.
6. Texas Instruments, "Protection Design for Automotive Electronics", SNVA995, 2022.
7. Sharma & Verma, "NFC-Based Security for Smart Vehicles", IEEE ICCCIS, 2021.
8. STMicroelectronics, "Antenna Tuning for ST25R", App Note, 2023.
9. Mohan & Rajan, "Embedded CAN for Automotive", IJAREEIE, 2020.
10. Horowitz & Hill, The Art of Electronics, Cambridge University Press, 2015.