IOP Conf. Series: Materials Science and Engineering **392** (2018) 062123 doi:10.1088/1757-899X/392/6/062123

# Design and Research of Passive Entry Control System for Vehicle

**Ji Gao NIU, Chen Xu LI, Xiao Li SHI, Chun Hua XU**

School of Mechanical & Electronic Engineering, Zhongyuan University of Technology, Zhengzhou, Henan 450007, China.

Email: jigaoniulucky@163.com

**Abstract.** In order to improve the security and convenience of the remote keyless entry (RKE), this paper develops a passive keyless entry (PKE) control system, which is based on the MC9S12G128 microcontroller and μC/OS-II real time operating system. The method adopts advanced radio frequency technology, which can realize the two-way authentication between the key and the vehicle without taking out the key, thus opening car door. The test results show that the proposed PKE control system has better stable performance, high security and convenient operation.

## 1. Introduction

With the development of automotive electronic technology, the anti-theft and convenient of vehicles have become a hot topic [1-2]. For a vehicle equipped with the PKE system, the door can be opened with a legitimate smart key. Because there is a bidirectional authentication relationship between the smart key and the car, and the advanced HITAG3 encryption algorithm is adopted, the security of the PKE is much higher than the RKE, and therefore the PKE is widely used in middle and high end cars [3-4].

## 2. Structure of PKE control system

The PKE control system mainly consists of MCU, body control module (BCM), smart key, microswitch, door handle antenna, internal antenna, etc. Figure 1 shows the architecture of the PKE system based on the MC9S12G128 microcontroller.

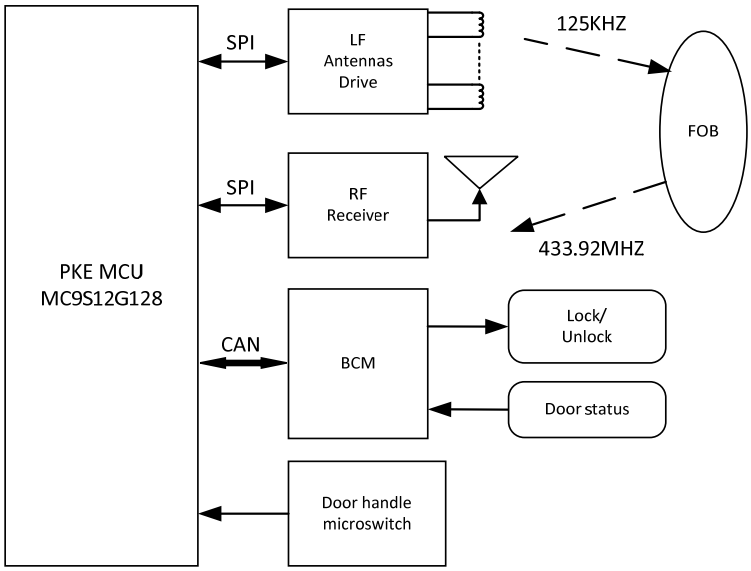


Fig.1 Structure diagram of the PKE system

## 3. PKE principle based on RFID

Figure 2 shows the PKE system authentication process. When the user presses the microswitch on the door handle, the PKE controller drives the internal antenna by the ATA5279 chip, which transmits the 125 kHz low frequency (LF) location signal to the outside. After receiving the location signal, the smart key checks whether the wake-up code is consistent with the requirement. If the wake-up code is correct, the smart key will be activated and return its position through the high frequency signal of 433.92 MHz. If the key is located outside the vehicle, the door handle antenna transmits the LF authentication signal to the outside. After the smart key is activated, the encrypted response is returned to the PKE host via a high frequency signal. If it is decrypted successfully, then the key is valid.

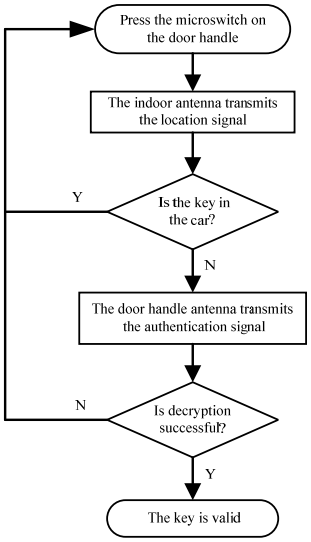


Fig.2 PKE system authentication process

### *3.1 LF transmitting module*

*3.1.1 LF coil driver chip*

The Atmel ATA5279 is an LF coil driver IC intended for passive entry system. It can drive up to six low frequency antennas (i.e., coils) to provide a wake-up and initialization channel to the key fob [5]. The maximum peak current of the chip is 1A, which can be flexibly configured up to 20 steps. In this paper, the MC9S12G128 transmits data to the ATA5279 via the SPI communication, and the ATA5279 needs to drive two door handle antennas, three internal antennas and one trunk antenna.

*3.1.2 LF communication protocol*

LF communication adopts Manchester code, amplitude shift keying (ASK) modulation, 125 kHz carrier frequency, and 3.9 kbps communication rate (7.8 kbps Manchester code rate). The Manchester encoding format is shown in Figure 3, in which the falling edge means "0", and the rising edge means "1", where 1 Tbit is equal to 256us. Because the ATA5279 does not have the ability to encode for Manchester, data encoding are completed using the method of programming before sending data via the SPI.

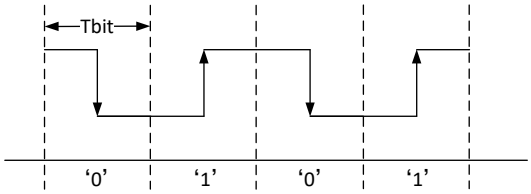


Fig.3 Manchester encoding format

The data frame structure of LF communication is shown in Figure 4. Among them, “Preamble” consists of seven "0" of the Manchester format, “Synchronization” consists of 9 Tbit specific levels, which will be identified by the smart key. “CC”, which is used to measure the magnetic field intensity, is the common carrier of 5ms. “Data” consists of the encrypted data, besides, the location signal and the authentication signal is only different in this data segment.

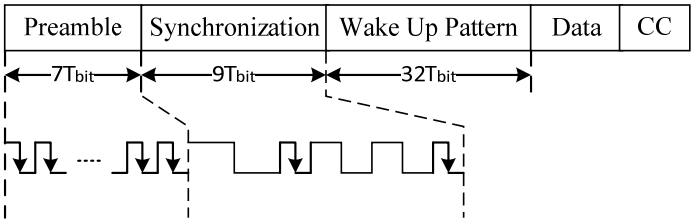


Fig. 4 The data frame structure of the LF communication

*3.2 RF receiver module*

*3.2.1 RF receiver chip*

The high frequency signal from the smart key is received by the NXP NCK2913, and the chip supports two receiving modes that are RKE and PKE. NCK2913 works in the RKE mode by default, and in order to reduce the static power consumption, the programming adopts the query pattern (i.e. working for a period of time and sleeping for a period of time). However, in order to shorten communication time in the PKE mode, NCK2913 continuously receives external signals without sleep.

*3.2.2 RKE communication protocol*

The RKE communication adopts the Manchester code, amplitude shift keying (ASK) modulation, 433.92MHz carrier frequency, 7.8kbps communication rate (15.6kbps Manchester code rate). When the button on the smart key is pressed, the high frequency transmitter inside the key sends a data

packet, which consists of several data frames.

As shown in Figure 5, the data frame consists of the preamble (Preamble), conflict code (CV), data segment (Data) and frame trail (EOF). Among them, the Preamble consists of sixteen "0" of Manchester encoding format, the CV consists of 1.5 Tbit high level and 1.5 Tbit low level. The Data is composed of frame type (FT), key serial number (ID), key value (KEY), synchronization code (SI) and encryption result (Crypto). The EOF is the end of a frame.

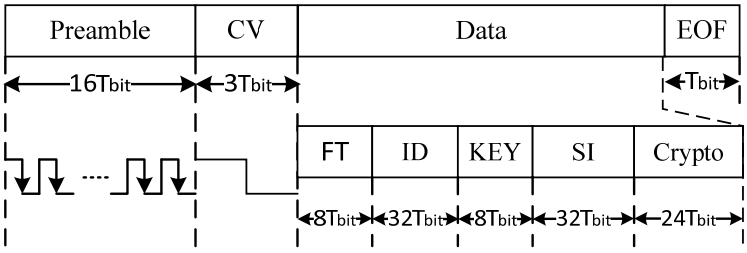


Fig.5 The data frame structure of the LF communication

*3.2.3 PKE communication protocol*

The encoding format, modulation mode, carrier frequency, communication rate and data frame structure of PKE communication are the same as those of RKE communication, but the it is different in Data segment, and Preamble also has changed from 16 to 32 Tbit.

## 4. µC/OS-II real-time operating system

µC/OS-II is an open-sourced, real-time embed operating system with the features of portability, tailor-ability, preemptive multi-task, etc. It can define as up to 64 tasks, which is sufficient for general system [6]. The main steps of porting µC/OS-II to MC9S12G128 are as follows.

(1) Modification of the OS_CPU.H file. Firstly, a series of data types are redefined based on the compiler and the MC9S12G128 processor. Secondly, the os_critical_method is defined, its function is that the system can disable the interrupt before entering the critical section, and enable the interrupt after access. Finally, the value of the os_stk_growth needs to be modified according to the growth direction of CPU stack, and the os_task_sw function needs to be redefined with software interrupt.

(2) Modification of the OS_CPU_C.C file. Six C language functions related to operating system and four assembly language functions related to processor need to be transplanted.

## 5. Software design of PKE control system

According to the design requirement, the PKE control system is divided into three tasks, namely the PKE task, the RKE task and learning task.

*5.1 PKE task*

Figure 6 shows the flow chart of the PKE task. When the user presses the microswitch on the door handle, the PKE applet switches the RF receive chip NCK2913 from the RKE mode to the PKE mode. Then the smart key and the controller conduct the two-way authentication. After the authentication is successful，according to the current status of the door, the controller sends the corresponding lock or unlock command and the smart key ID to the BCM through the CAN communication. BCM performs the corresponding action after receiving the instruction.

*5.2 RKE task*

Figure 7 shows the flow chart of the RKE task. When the user presses the button on the smart key, the high frequency transmitter inside the key will send the high frequency signal to the outside. After receiving the signal, the NCK2913 chip sends it to the PKE host for decryption via SPI communication. If the decryption is successful and the key ID is consistent with the ID stored in the host, the BCM will perform the corresponding unlock or lock action.

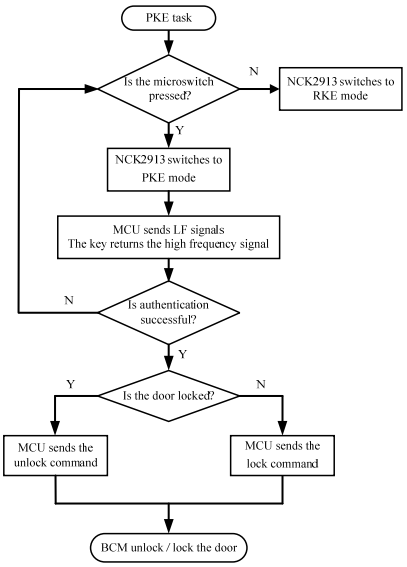


Fig.6 Flow chart of the PKE task

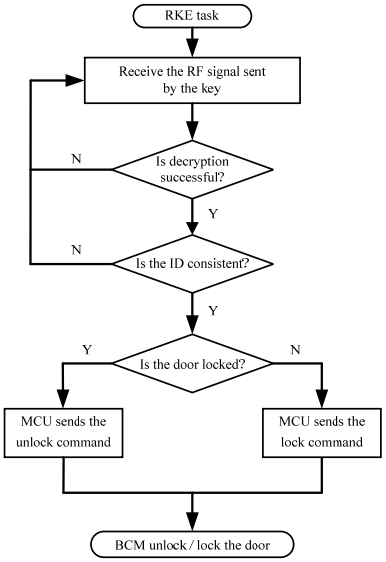


Fig.7 Flow chart of the RKE task

*5.3 Learning task*

Figure 8 shows the flow chart of the learning task. When the prescribed action is triggered, the PKE control system enters the learning mode. In this mode, the door handle antenna sends the LF learning signal to the outside world. After the smart key receives this signal, it returns the smart key ID to the PKE host. If the PKE host receives the ID within a specified time, the key ID is updated and written to the EEPROM.

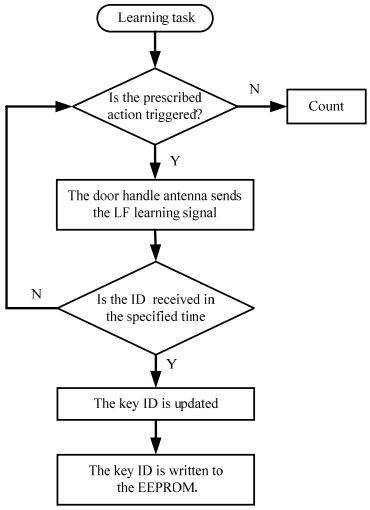


Fig.8 Flow chart of the RKE task

## 6. Conclusion

RFID has greatly promoted the change of the vehicle entry system from RKE to PKE, which makes it more convenient for users to enter the vehicle, and greatly enhances the anti-theft of vehicles. This paper studies the data frame structure of high-low frequency communication and its two-way authentication. In addition, the μC/OS-II real-time operating system and its porting method are briefly

introduced. The test results show that the designed system runs well and can accurately realize PKE functions, RKE functions, and support the learning mode.

**References**

[1] Yu S D, Feng J Z, Zheng S L, et al. Studying of a start control function mode based on PEPS system [J]. Modern Manufacturing Engineering, 2013, (1): 42-45.
[2] Li B, Qin G H, Zhao R, et al. Passive keyless entry system based on CAN bus and Internet [J]. Computer Engineering and Design, 2016, 37(4): 897-901.
[3] Mason S. Vehicle remote keyless entry systems and engine immobilisers: Do not believe the insurer that this technology is perfect [J]. Computer Law & Security Review the International Journal of Technology & Practice, 2012, 28(2): 195-200.
[4] Hu W, Zhang J X. Low power vehicle entry system based on RFID technology [J]. Journal of Mechanical & Electrical Engineering, 2015, 32(5): 733-738.
[5] Qiu Z G, Ma B, Ma D G. The application design of PKE system based on LF coil driver ATA5279 [J]. Global Electronics China, 2011, (1): 57-59.
[6] Zhang F, Guo L L, Xu Z. Miners Positioning System Wireless Collector Based on μC/OS-II [J]. Instrument Technique and Sensor, 2014, (1): 34-36.