Smart Keys/Key box

Team 72 — Jacob Connor, Mehul Kaushik, Yingtong Hu

ECE 445 Project Proposal — Spring 2021

TA: Yichi Zhang

1. Introduction

• Objective

Car dealers deal with a lot of car keys during working hours, and have a central location where they keep keys to the cars on the lot. Unfortunately, employees sometimes misplace the car keys, forget to return them after using them for test drives, or the car keys could even be stolen. Replacing car keys takes time and money, and also poses a security concern.

To combat all of these issues we are proposing a smarter set of keys and a corresponding key box to house all of these and some of the system's features. The keys would be able to be located by making sounds when looking for them. The key box system would be able to activate, deactivate the keys and give a direction to the key which the user is looking for.

• Background

Car keys now have only a tag on each of them, dealers can know which employee took it and which car it belongs to, but not exactly where it is. When it comes to the case that an employee lost the key, dealers can’t do anything with a tag. The same can be said for if the key was stolen. Sure, the dealer could change the keyhole, but it may be stolen with the old key before the keyhole is changed, not to mention the time and money associated with changing out the locks on the vehicle. With our smart keys and key box, dealers will be able to find the key when it’s within some distance away from the key box, and be able to deactivate the key when it’s too far away from the key box, which will help reduce the probability of a stolen key leading to a lost vehicle.

• High-level requirements

1. Keys that are within certain distance can be tracked easily by sound and direction hints

2. Keys that are out of the distance range after a specified amount of time and are unaccounted for will be deactivated automatically (for example, if the salesman forgets where the keys are and loses them, there’s a chance they were stolen and should be deactivated, but if the car was purchased by a customer, obviously the key would still be gone but should not be deactivated)
3. Keys are small, so all the implementations on the keys should be small enough for keys to carry.
4. The ability to handle a large quantity of keys

2. Design

- **Block Diagram**

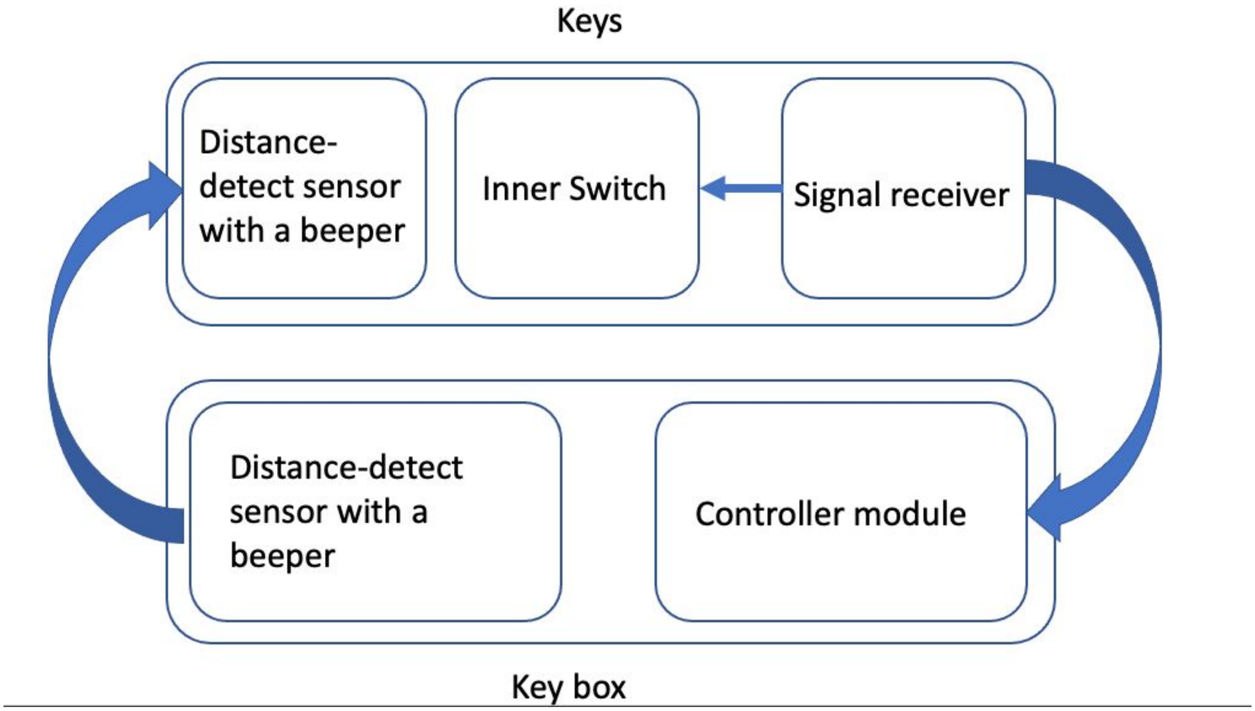
Keys
Distance-detect sensor with a beeper
Inner Switch
Signal receiver
Distance-detect sensor with a beeper
Controller module
Key box

Figure 1. Block diagram

- **Functional Overview**

1. Beeper

The key box will have beepers with distance sensors, each sensor is responsible for a specific key. Every key will have a beeper with a distance sensor that reacts to the sensor on the key box. When the user is looking for a specific key, the user will press the button that activates the sensor responsible for the specific key, then the beeper on the key and the key box will both make sounds. When the user is moving towards the key, the sound will be larger, indicating that the user is approaching the specific key.

2. Controller module

This module controls the activation and deactivation of keys. When the user wants to deactivate a key, a button will be pressed and send out a signal to the signal receiver on the specific key. It will alert the user of active/inactive keys through a simple interface and allow them to track the keys when a key needs immediate attention or when it is stolen/lost.

3. Signal receiver (Communication module)

This device receives the signal sent by the control module indicating activation or deactivation of the specific key. We plan to use RF circuits to transmit and receive data without the need of line of sight and considerably higher range for broadcasting of signal compared to other technologies within the scale of the key casing. Sizing of the casing will have to be adjusted based on the needed range of the RF module.

4. Inner Switch

The switch will turn off or turn on the key according to the signal received by the signal receiver. This will be the interface between the receiver and the key deactivation module which might be necessary since the deactivation actuators may not operate on the same voltage as the receiver module.

5. Key Deactivation (part of inner switch)

For cars with physical keys, we could use actuators that extend a metal piece into place that prevents the key from entering the car's key hole. This would mean the key activation module may sit on the key as a jacket-like casing. For keys with no physical keys, the solution would be slightly different. Keys will have an inner switch on each of them that can only be turned up and off by the control module. (or like disabling the key fob's ability to unlock the vehicle so that they couldn't reach the push button start.)

● Risk analysis

The signal receiver is the most crucial part of our project. It will have to be powered sufficiently so its status can be monitored by control box on regular intervals but at the same time the power source for this module needs to be sized in a manner that it can fit in the minimalistic casing of the key but still power the communication system. Without this, the actuators in the key deactivation process will not do their function.

Wireless communication between the keybox and the key is our main challenge and it extends to the beeper module as well. Communication breakdowns will have to be handled properly and charging of both devices (communication and beeper module) needs to be managed by choosing the appropriate power supply for our respective devices.

If our communication devices work well, the second part of our project is the conversion of the communication data to their appropriate actions by the actuators and the buzzers for the beeper module and the tracking of key status in general. Data that is communicated between the key and key box needs to be monitored regularly so system failure that results in the key surveillance getting suspended cannot be afforded will require proper power management along with signal processing to make sure all functions are being carried out based on input data to key box and key.

The last most important feature that is crucial to completion of our project is the security aspect of course. We want to make sure that the actuators perform their role in deactivating the key and that the key box appropriately alerts the user of any tampering with key/ key discharged/ key lost or stolen and not mix up the different conditions in which the key may be in.

3. Ethics and Safety

Since our project relies heavily on RF communication with (possibly) multiple keys. Our project runs the risk of "emitting by products of radio emission" [1]. This would have to control our radio emission in the radio frequencies so as to minimize disruption to other services working close to our device's operating range. A possibility is to remain below 9kHz which is highly unlikely for our project given the fact that we want considerable range when tracking our keys but we will actively search for alternatives that could work on lower transmission frequencies if possible. We will try our best to remain within the FCC regulations for RF devices as possible[2]. We haven't decided upon our power source at this stage but most likely, we will be working with rechargeable batteries like Li ion or button cell batteries. Whichever the case, we will do our best to adhere to all safety precautions related to Li ion batteries which may involve double checking our power supply voltages and current, and work within the safe operating points of our chosen battery so as to avoid harm to our consumer through shock from uncontrolled voltage/current [2].

Consumer safety may also extend to moving parts in our project: for example, the actuator that deactivates physical keys by lodging a piece of metal in the key that prevents it from fitting in the keyhole. One way to prevent harm to user of key in case the actuator is triggered, is to carefully control torque such that it has sufficient strength to block the key from usage but at the same time, it is slow enough and comes with a warning through sound so as to alert user of the deactivation process. The slower motor will be less of a mechanical hazard since it gives the user time to move out of its way though in future design, we will continue to work on this challenge keeping user safety and security in mind.

Citation

[1]"Equipment Authorization – RF Device." *Federal Communications Commission*, 20 Mar. 2018, www.fcc.gov/oet/ea/rfdevice.

[2]Reczek, Karen, and Lisa M Benson. "A Guide to United States Electrical and Electronic Equipment Compliance Requirements." 2017, doi:10.6028/nist.ir.8118r1.