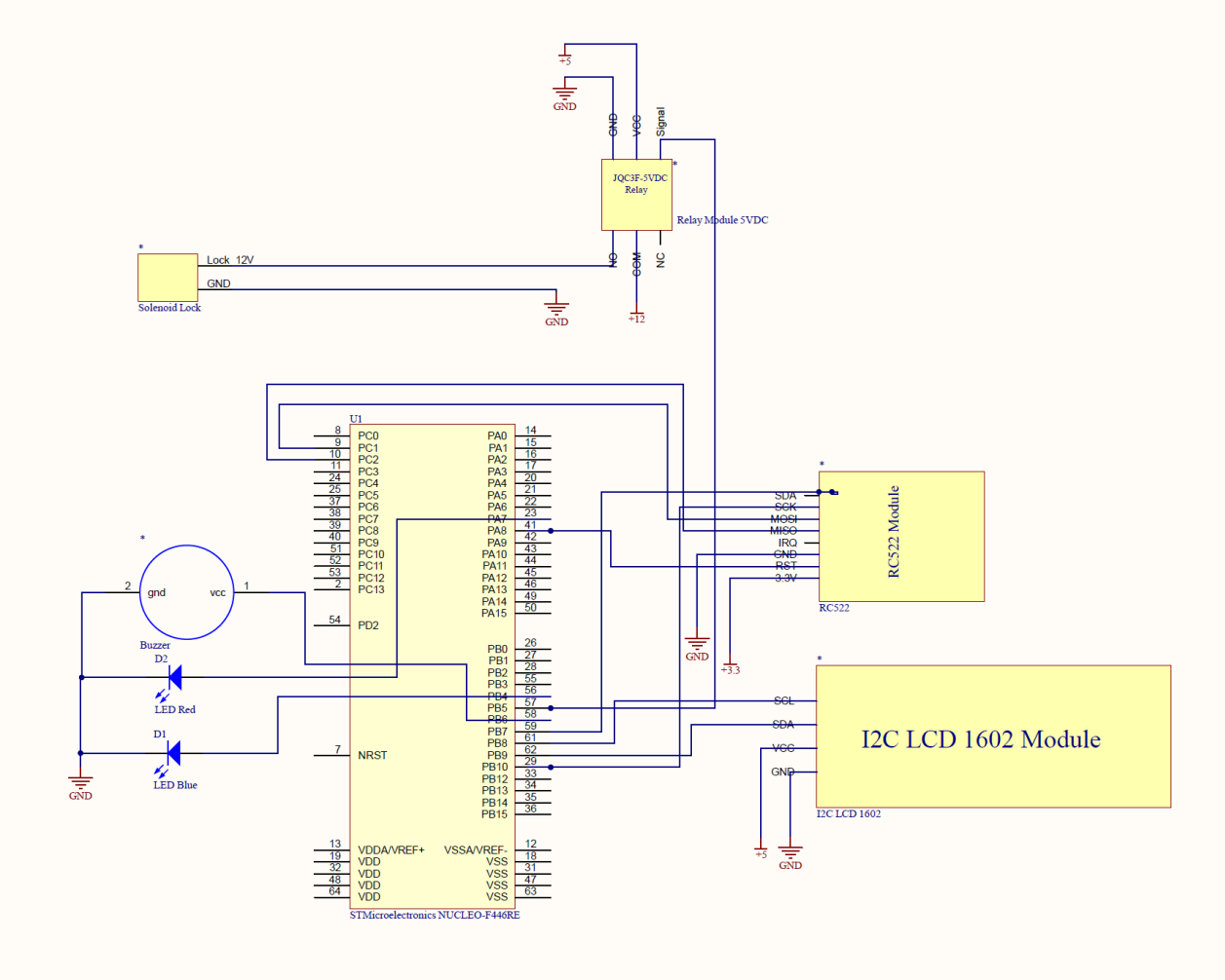
Definitions of most important functions to communicate with MIFARE 1k CARD with RC522 module.

Short description of this PDF document

In this PDF document I am showing you how I wired the STM32F446RE Nucleo board with all of the components that you can see are used in Picture 1. Furthermore, I will try my best to explain how the RC522 module communicates with the MIFARE card by the below highlighted in my opinion the most important functions. If you want to go and understand how the RC522 module really communicates and should with the MIFARE 1k cards then **I highly recommend** checking out the **IEC 14443-3a document** with the **datasheet of the MFRC522 module**. This document in detail explains how to communicate with MIFARE 1k card, it also includes detailed explanations of all the communication protocols. Here I will describe this in a crude way. Included can be found all the documentation that I used to make this project possible and to make it work for my specific needed functionality.

P.S. Bare with me regarding the comments in the project that are scattered around in my language and in English. Translate as you go. Most of the comments are connected to the MFRC522 datasheet.



Picture 1 - Wiring and used modules

MFRC522_INIT

This function starts with a MFRC522_RESET function the resets the software it is described in the MFRC522 datasheet.

The MFRC522 module has an ability for a timer to be used. This timer is configured in a way where after the transmission of any data across the antenna the timer starts to count down. Timer will hit zero from the start in 25ms. The timer is used in the function MFRC522_TO_PICC for control flow of the program. The reason of the timer is because during transmission of data from the RC522 module to the MIFARE 1k card there are errors and interrupts that can occur in the RC522 module, these are checked right after the transmission starts until it ends for the duration of the timeout(lines 75 to 79 of RFID.c).

The communication is configured with a modulation of 100% ASK at a default setting bitrate of 106kBits/s (otherwise known as fc/128).

Antenna is turned on.

MFRC522_TO_PICC

Firstly, with the writing to register commands we call the command PCD_IDLE which stops all active commands beforehand. Then all the interrupt requests are cleared and after that the FIFO buffer of the RC522 module is intialized, flushed. In the for() loop data is written to the FIFO buffer and after that the TRANSCEIVE command which is started by setting the StartSend bit in the Bit framing register.

Furthermore, the waiting of the command execution is executed that is explained in the MFRC522_INIT above.

Lastly there is more error checking inside the error register and also if a combination of interrupt requests have been set inside the irq com register. Data is after this being read from the FIFO buffer while also reading the amount of bytes inside the FIFO level register these bytes are important for the later case of checking if there are any valid bits of the last received byte. More of this is explained in the MFRC522 datasheet.

MFRC522_REQA_WUPA

This command is a combination of the MFRC522_TO_PICC command with a different buffer. The buffer it cointains is the REQA or it can be also set to a WUPA command if needed. These MIFARE 1k specific commands are in detail explained inside the ISO IEC 14443-3 document.

MFRC522_ANTICOLLISION

The anticollision is the command with which we acquire the UID of the MIFARE 1k card it is in detailed explained in the ISO IEC 14443-3 document. Anti collision is in essence a protocol or in other words software logic that can differentiate between multiple MIFARE 1k cards and choose one to communicate with. This is acquired with the Anticollsion cascade levels each cascade levels has its own HEX value and also with the other requirements such as the NVB(number of valid bits). In this case the 1st anticollsion cascade level is used.

MFRC522_GET_UID

This function is a combination of the two above mentioned functions and by combining them we acquire the UID. This has been realized according to the ISO IEC 14443-3 document and the detailed specification of PCD to PICC communication protocols.

MFRC522_HALT

This function puts the MIFARE card into a state of HALT. When a MIFARE 1k card is in this state, only way to wake it up is by sending the WUPA command. Bascially the MIFARE 1k card is in some sort of sleep mode if it is still in the range of the antenna of the RC522 module. If it isn't then it will just go into the power off state.

There is a certain format of data that needs to be sent to the PICC for the MIFARE 1k card to go to a HALT state. This is where CRC calculation goes into play.

MFRC522_CRC_CALCULATION

As described in previous function you can figure out what these write commands do. After this data is written to the FIFO buffer to be later used for CRC calculation after it is started. Waiting for the CRC calculation is initiated. Lastly, acquired data from registers is saved into the dataOut buffer which later is used in the MFRC522_HALT function.