Innovating Redundancy In Over-the-air Programmable Lock Systems

Devin Britton & Ihor Marchenko

Commonwealth University of Pennsylvania // MADS Department

Abstract

The primary goal in this project was to explore innovative ways of approaching RFID locks and secure transfer protocols (STP) in adjacent areas such as Remote Keyless Entry (RKE) and other Internet of Things (IOT) systems. The first step to doing this involves reverse engineering an RFID lock system to create an environment ripe for modification and experimentation via an Arduino microcontroller and bread board setup.

After an avenue for experimentation was established, the further goals of defining a way to establish over the air (OTA) programming and experimentation with enhanced security measures were opened.

The objective of OTA programming is to allow systems to be dynamically programmed through surfaces with redundancy to internet outages, allowing the system to be independent of normal IOT device bands. For this case, the 915MHZ band using the Reyax LoRa 896 was chosen for its surface penetration and separation from cellular and WiFi. Further, bleeding edge security measures were implemented via software combining rolling-code, AES encryption, and time synchronization to explore possible avenues of providing enhanced security on a budget.

Methodology

Modern lock systems are comprised of multiple components that require to be integrated all together into a functioning system. Particularly, a breadboard and Arduino R3 were used to combine the functionalities of the MRFC522 RFID scanner, Reyax RL896 transceiver, and a 2003UNL stepper motor to simulate a physical lock, all for the lock station. The home station is what communicates and programs the lock station via a software interface connected to a URT bridge to the home station's own RL896. Since the primary operating area for this is large buildings and compounds, a field test was conducted on the grounds of an apartment complex. With one station four floors up, and the other on the ground floor on the opposite side of the building. On a software level, there are 3 registers for key uids for simplicity's sake.

Results

The combined conceptual knowledge allowed us to design a security system original in nature and was constructed using affordable solutions for each function of the system with modularity and scalability in mind. It was found that the two stations had no issue communicating over distance within a residential apartment complex. This means that there is less cost towards transceivers due to their material penetration ability. This means that there is less cost towards transceivers due to their material penetration ability. This is a result of the 915MHZ band traveling better through surfaces than a similar Bluetooth or WiFi activated system, which are on 2.4GHz. With one station four floors up, and the other on the ground floor on the opposite side of the building. This means that there is less cost towards transceivers due to their material penetration ability. This is a result of the 915MHZ band traveling better through surfaces than a similar Bluetooth or WiFi activated system, which are on 2.4GHz.

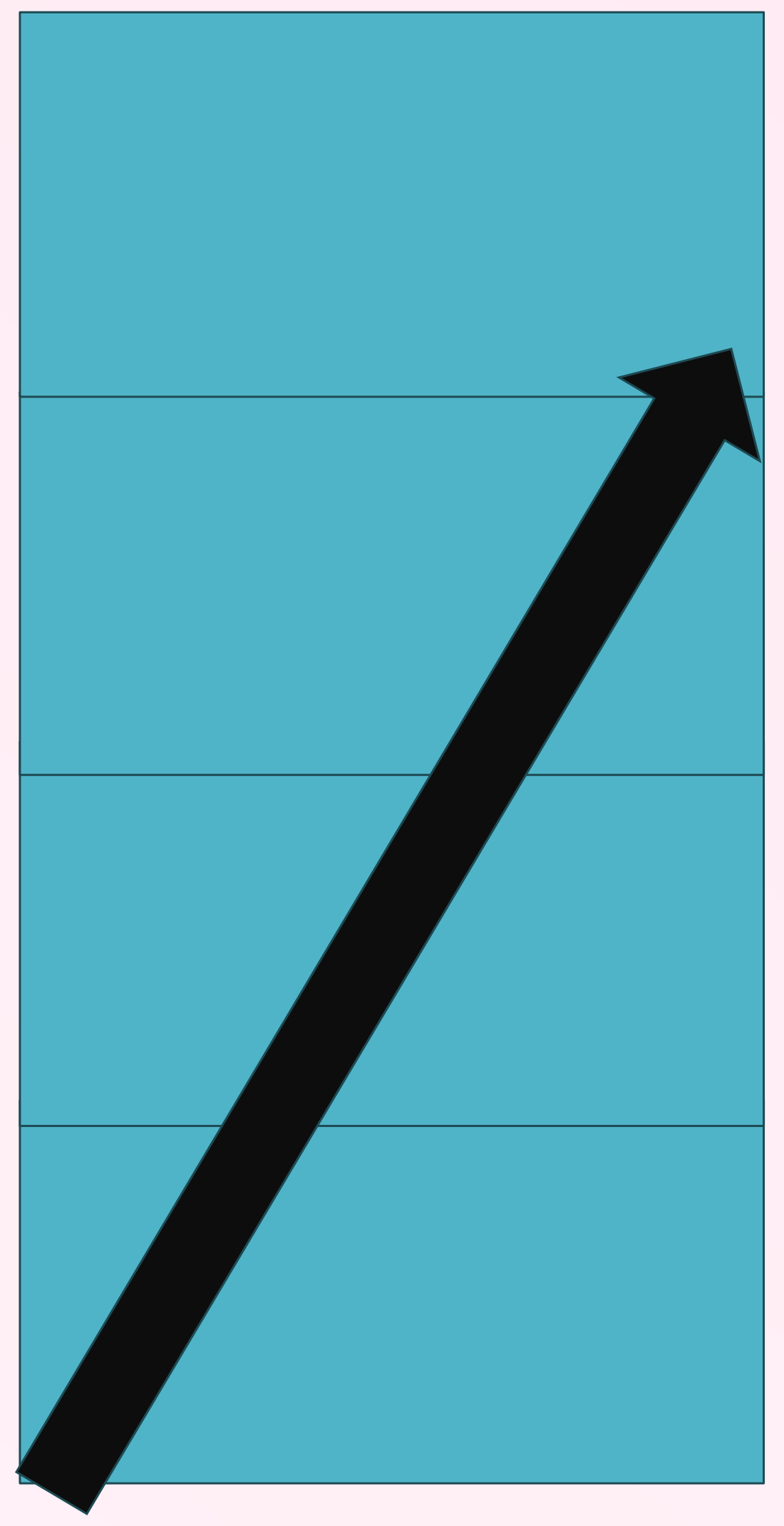
Key Features:

~Encrypted Communication
~Add/Remove Keys
~Monitor Entrance Activity
~Internet Outage Redundancy
~High Surface Penetration

Conclusion

With our time and research coming to an end at the Commonwealth of University, Bloomsburg Campus. We hope we have given new insight into the world of radio waves and the amazing infrastructure behind the security of digital signal communication. Most RFID systems are static, and the lock can only be interfaced with physically or via hardwire, RFID being a technology meant for the purpose of verification. The addition of a wireless transceiver to the physical lock enables it to become an IoT device using protocols separate from Wi-Fi and Bluetooth and not interrupting scanner function. Since our research led to a functioning prototype, it opens new avenues to explore in the context of secure transfer protocols of information via radio waves since the nature of usage for this specific system is directly related to security.

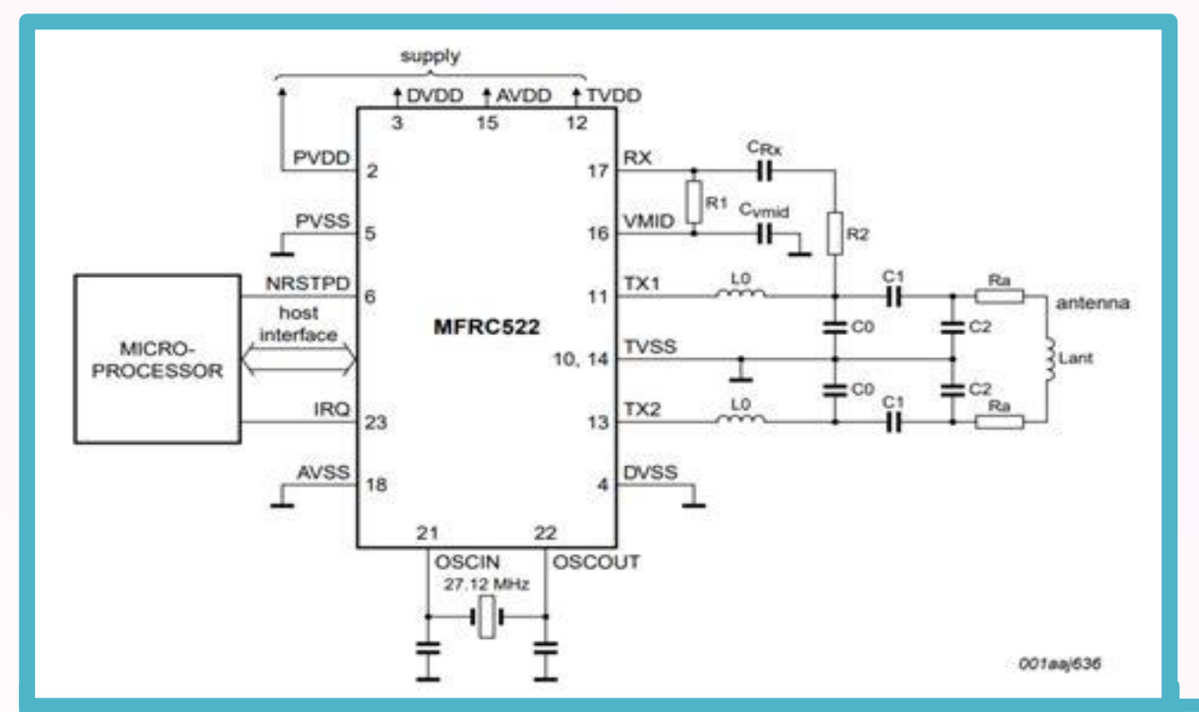
3 floor penetration



Acknowledgements

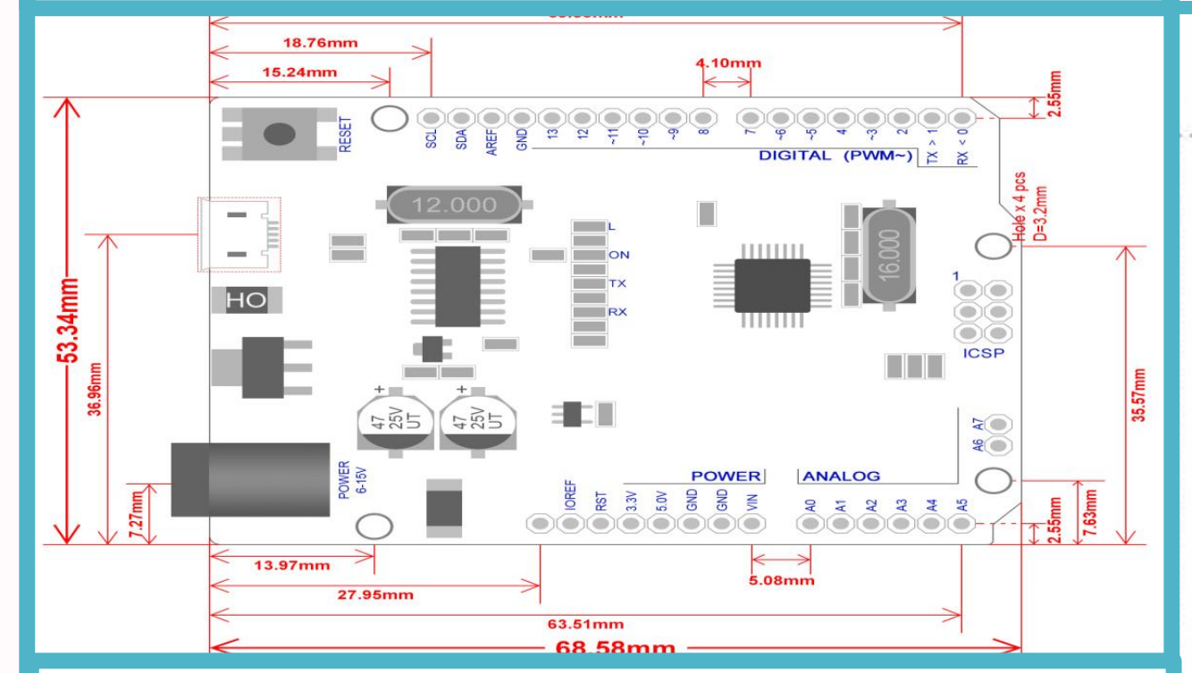
Dr. Diane Barret PhD
Dr. Phillip Polstra PhD
Brett Logan

NFC Scanner - MRFC552 @ 3.3v

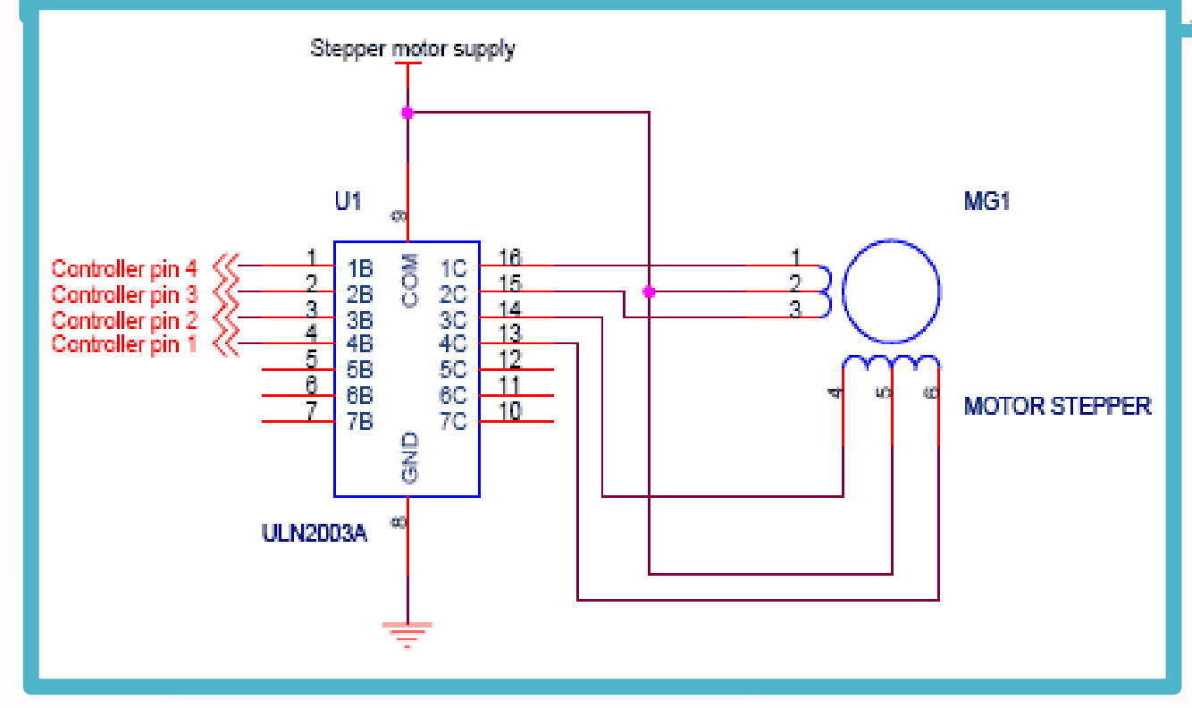


Arduino UNO R3

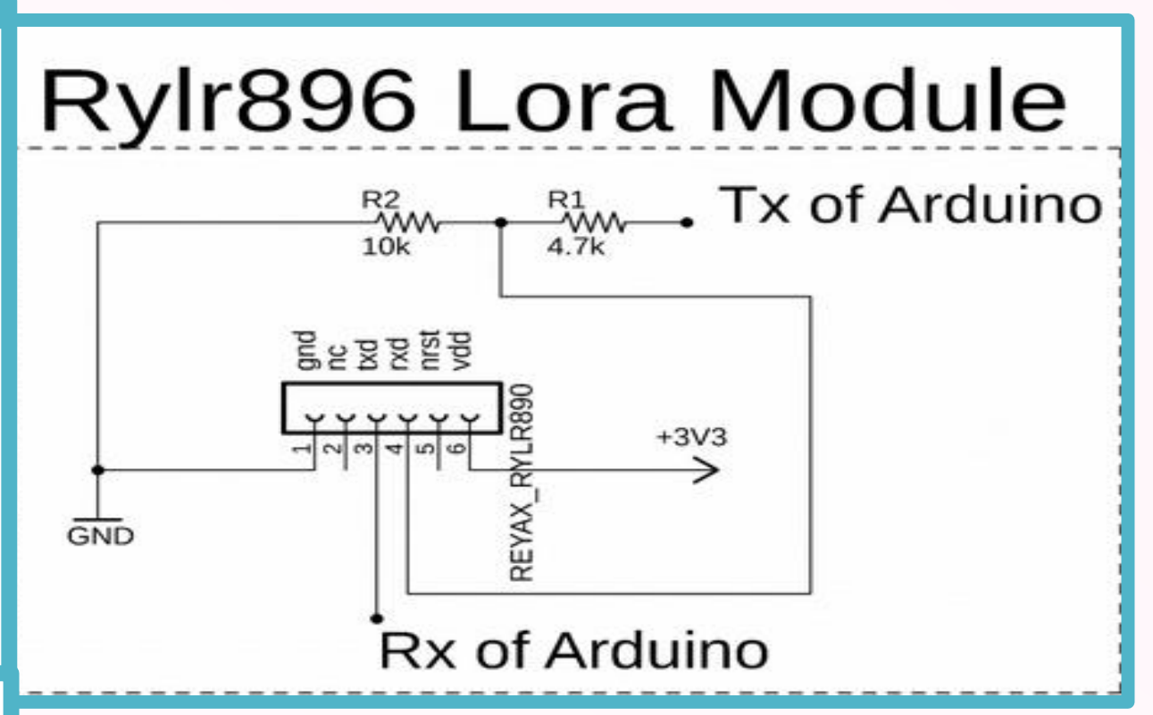
~AT-Mega 328 3.3v
Microcontroller



UNL2003A stepper motor
~5v-12v
~INT1-INT2-INT3-INT4-VDD-GND

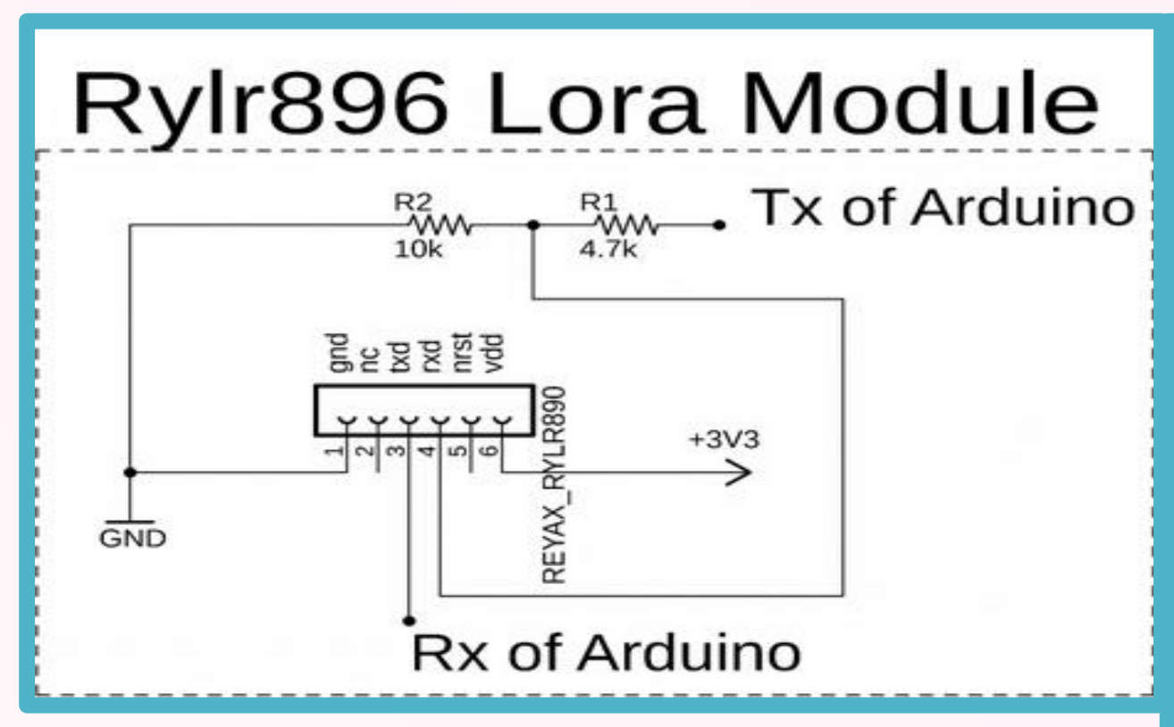


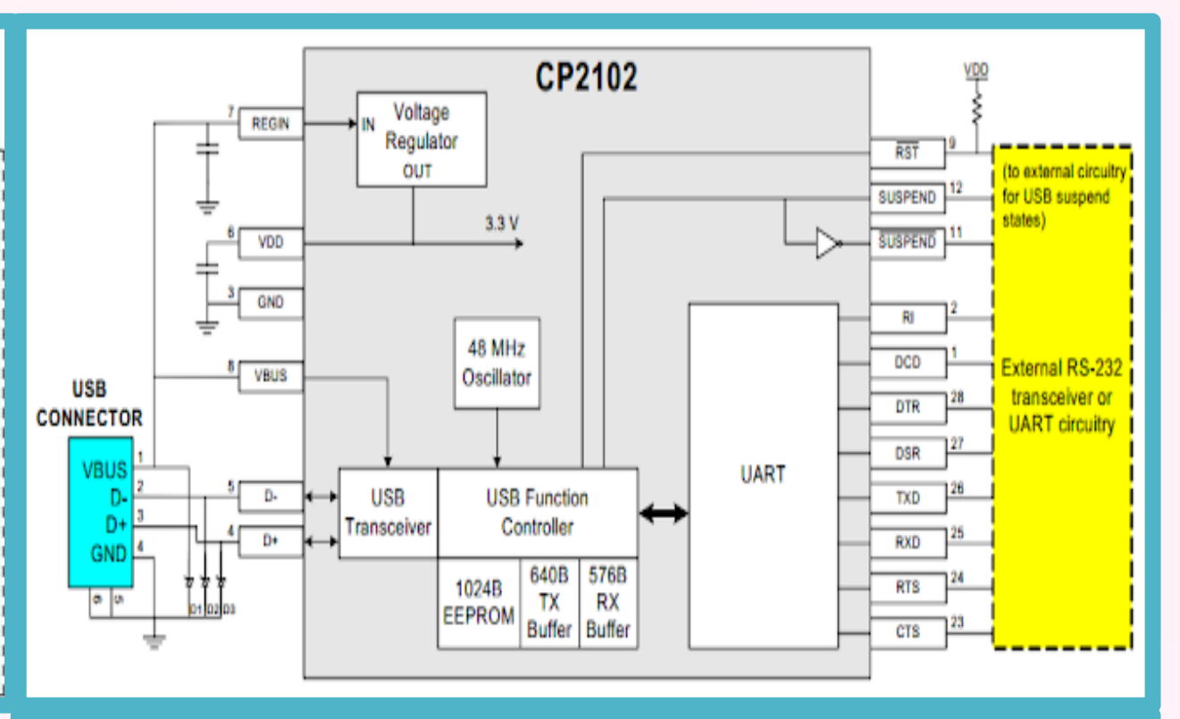
UNL2003 Motor



Transiever-Lora896
3.3v
~<5km range
~AES-128 Encryption
~PWR-GND-RST-TX-RX

LoRa 896 -> UART Bridge -> Pi 4


Rylr896 Lora Module
R2
10k
R1
4.7k
Tx of Arduino
gnd
nc
txd
rxd
nrst
vdd
REYAX_RYLR890
+3V3
GND
Rx of Arduino


CP2102
Voltage Regulator
USB CONNECTOR
48 MHz Oscillator
USB Transceiver
USB Function Controller
UART
1024B EEPROM
576B TX Buffer
576B RX Buffer
External RS-232 transceiver or UART circuitry