RFID Lock Project Overview

By: Bob Glicksman, Jim Schrempp; v3, 8/30/20

NOTICE: Use of this document is subject to the terms of use described in the document "Terms_of_Use_License_and_Disclaimer" that is included in this release package. This document can be found at:

https://github.com/TeamPracticalProjects/Wireless_IO_Board/blob/master/Terms_of_Use_License_and_Disclaimer.pdf

Contents

1. INTRODUCTION.

This document provides a brief overview of the RFID Lock project. Section 2 of this document describes the project in the context of the Maker Nexus RFID Access Control system project, and the Wireless I/O Board project, both of which are published at:

https://GitHub.com/TeamPracticalProjects

Section 3 of this document describes the layout of this repository and what information is included here.

2. RFID Lock Project Overview.

2.1. What this project is about.

This project is fundamentally about the hardware and firmware for a Particle[1] Photon-based device that can control various locking mechanisms. One specific locking mechanism has been fully implemented (see: https://www.amazon.com/Tokatuker-Electronic-Cabinet-Hidden-Drawer/dp/B075QF1VPR) and is fully documented here. We have also implemented a solenoid lock activation mechanism to unlock a door. Other possible locking mechanisms have been briefly explored and some information about them has been included in the repository, albeit these other mechanisms have not been fully implemented and tested.

This project was specifically undertaken as an enhancement to the Maker Nexus RFID Access Control System (see: https://github.com/TeamPracticalProjects/MN_ACL). The concept is to have the MN_ACL RFID Stations publish a "check-in event" to the Particle cloud whenever a user taps into that Station with valid credentials. Every RFID Lock board subscribes to this event and compares the Station's deviceType (included in the event) to its internally configured "Lock Listen code". If the published deviceType matches the Lock Listen code, and if a secret key in the "check-in event" is valid, the device opens the lock. Depending upon the mechanical aspects of the lock in question, a cabinet or door may "pop open" when this happens, or else it may unlatch for some pre-specified period of time. A modified Tokatuker locking mechanism that has been fully implemented is of the type that pops a cabinet door or draw open. A solenoid controlled door unlocking mechanism has also been fully implemented and unlocks the door for a pre-specified period of time.

RFID Lock configuration can be performed via the *MN_Station_Configurator* App that is part of the MN_ACL project or via the Particle Console. Figure 1 below depicts the interactions of an

[1] Particle.io

RFID Station, RFID Lock and *MN_Station_Configurator* App, all via the Particle Cloud. Further information about system operation can be found in the document:

https://github.com/TeamPracticalProjects/MN_ACL/blob/master/Documents/RFID_ACS_Overview_Document.pdf

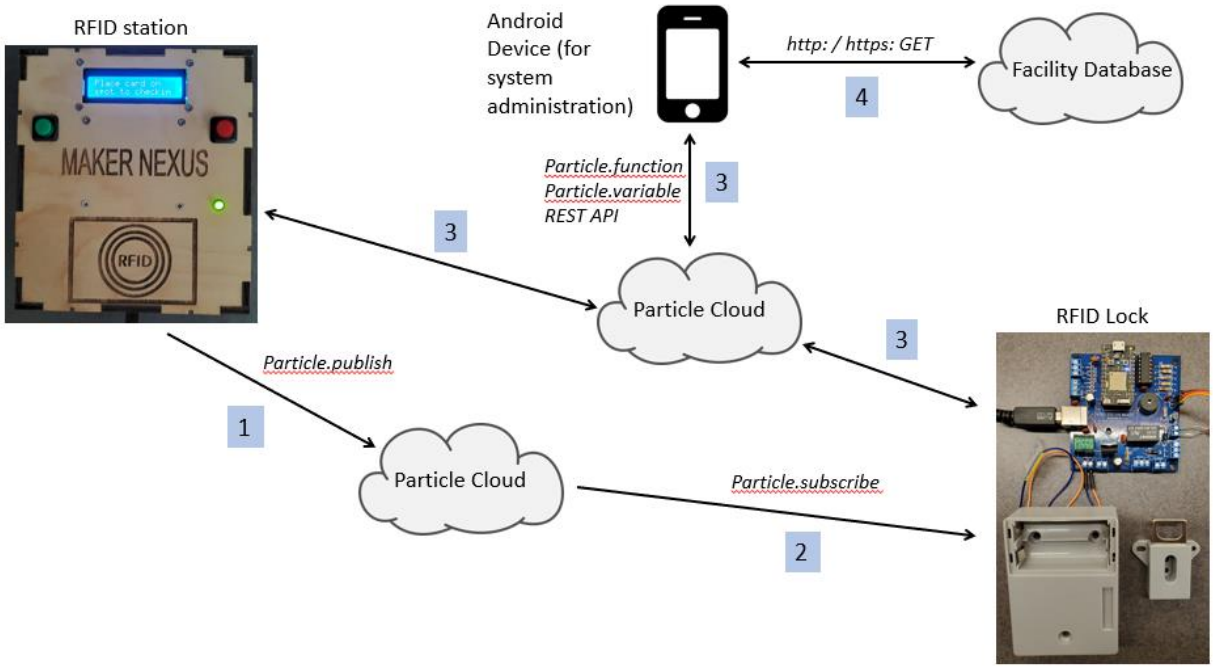

Figure 1. RFID Lock Architecture in Context of MN_ACS.

Referring to figure 1, the dataflows are:

(1). RFID Stations publish check-in events to the Particle cloud whenever a user taps in with a valid RFID card and the user is authorized to that Station's function. The check-in event contains the RFID Station's type and a facility secret key in a JSON encoded data set.

(2). RFID Locks subscribe to check-in events via the Particle cloud. When a check-in event's deviceType data matches the Lock Listen code configured for the RFID Lock, and the check-in event's secret key is valid, the RFID Lock unlocks the electromechanical lock to which it is wired.

(3). The *MN_Station_Configurator* App, running on an Android phone or tablet, allows a system administrator to configure deviceTypes into the RFID Stations, and both deviceTypes and Lock Listen Codes into RFID_Locks. The App does this by calling Particle cloud functions on these devices and the App obtains station configuration information by reading Particle cloud variables from these devices. The App (source code and install file) can be found at:

https://github.com/TeamPracticalProjects/MN_ACL/tree/master/Software/Android_Apps

The RFID Lock is made from a Photon based electronic printed circuit board and associated electromechanical locking hardware. The details of the printed circuit board are available in the following repository:

https://github.com/TeamPracticalProjects/Wireless_IO_Board

Although this project was driven by specific requirements of the Maker Nexus RFID Access Control project, the hardware, software and firmware may be useful in other contexts.

2.2. Story.

The MN_ACL project (https://github.com/TeamPracticalProjects/MN_ACL) creates an infrastructure for secure, RFID-based access control to a Makerspace and it's various internal equipment locations. That project integrates Particle Argon-based RFID stations with a commercial cloud CRM system and an internal tracking database. The MN_ACL project ensures that people who access the facility are paid up members in good standing and that members who access certain locations containing sophisticated industrial equipment have basic operating and safety instruction credentials. The project controls access via red/green illuminated buttons and an audible beeper.

Certain locations within the Makerspace contain expensive materials, parts and accessories. We decided to create a Particle Photon-based add-on that could subscribe to publications sent by the Argons in the RFID stations and unlock cabinets containing these expensive accessories. We therefore needed to find an inexpensive but effective electrically controlled locking mechanism and create a Photon-based printed circuit board (and associated Particle firmware) to unlock the cabinet when a member taps into one of the relevant RFID stations with credentials that allow them access to these accessories.

COVID-19 related health and safety regulations require that the front door be locked to the outside and access to the facility be controlled. There is a 24 volt (DC) solenoid in the door mechanism that is wired back into the facility equipment room. We determined that mounting an RFID station at the front entrance and using the same publish/subscribe mechanism as for cabinet locks, we could remotely and securely activate the front door solenoid lock to admit members when they tap their badge to the front door RFID station.

We decided to generalize this mechanism as much as possible in order to accommodate other access control requirements as they arise in the future.

We decided that we needed a separate WiFi enabled circuit board for this purpose because:

- The relationship between RFID stations and cabinets/locks is many to many.

- Hardwiring a lock control signal from an RFID station to certain cabinets or locks is both inconvenient and easily hacked.

- A general-purpose, secure, WiFi enabled locking mechanism is a worthwhile and useful project in and of itself, independent of the MN_ACL project and it's RFID stations.

We selected the Particle Photon for this project because it provides a low cost and secure means of WiFi control and communication and because of Particle's simple and elegant cloud communication capabilities.

2.3. Locking Mechanisms.

We investigated a number of solutions for electrically controlled locking mechanisms and we ultimately decided to hack an off-the-shelf mechanism from Tokatuker; see:

https://www.amazon.com/Tokatuker-Electronic-Cabinet-Hidden-Drawer/dp/B075QF1VPR

The Tokatuker cabinet lock is a complete RFID solution in itself, but it does not have the required security or database integrations required for this project. We therefore removed the electronics and provided our own Photon-based hardware to control the lock. We also removed the batteries and we power the Tokatuker mechanism from our hardware so that the cabinets would not be stuck locked if a battery runs down.

We chose the Tokatuker solution because the locking mechanism itself is very innovative and uses only a small, low power DC motor to control a mechanically robust locking system. We found that pulsing this motor for 30 milliseconds in one direction unlocks the lock and pulsing it for 30 milliseconds in the opposite direction re-locks the lock. Unlocking the lock springs the cabinet door open and the door can thereafter be closed and will lock anytime after the small motor returns to the locked position. The device can therefore unlock, opening the cabinet door, and then immediately re-lock and the door can be closed and will automatically lock at any time thereafter.

The facility front door has a locking pushbar that includes a solenoid for remote unlocking. This solenoid was already wired back to the facility's equipment room. We experimentally determined that activating the solenoid for 2 seconds after a successful RFID card tap-in by a member in good standing is more than sufficient to provide entry to the facility.

This project contains complete instructions for building an RFID Lock using the Tokatuker product. This project also contains instructions and firmware for activating a door-unlocking solenoid. We also investigated various other locking mechanisms based upon servos, solenoids, etc. We have included some information about these other approaches in this repository but we cannot supply complete mechanics and Particle firmware to use them, as we did not carry these other locking solutions through to a complete project solution.

2.4. Electronics.

We developed a printed circuit board that houses a Photon and integrates the Photon with components that allowed us to test out various locking solutions. This printed circuit board seemed so generally useful to us that we have made it a project unto itself. See:

https://github.com/TeamPracticalProjects/Wireless_IO_Board

This project uses the Wireless_IO_Board hardware and we have added the Particle firmware necessary to subscribe to publications from MN_ACL RFID stations. The documentation included with this project provides ample references to these other projects where necessary.

2.5. Mechanics.

The modifications to the Tokatuker lock are documented in this repository. Likewise, instructions are provided for mounting the hardware in a small test cabinet that is demonstrative but also useful in its own right.

2.6. Firmware.

This project includes Particle firmware (source code) for the Photon that integrates the RFID Lock into the complete MN_ACL access control solution. Two sets of firmware are documented:

- firmware to respond to valid check-in events and unlock the modified Tokatuker motor lock.
- firmware to respond to valid check-in event and activate a door unlock solenoid.

3. Repository Contents.

3.1. Repository (Top Level).

The top level of this repository contains the following documents:

- "**Terms_Of_Use_License_And_Disclaimer.pdf**": this document contains the license and copyright information about the information in this repository and limitations on its

use. You must read and agree to all of the statements in this document before you are permitted to use any of the information in this repository for any reason whatsoever.

- "**RFID_Lock_Project_Overview.pdf**": This is the document that you are reading. It contains an overview of the project and a guide to what is in this repository.

- "**Readme.md**": This is a markdown document that contains the overview material found on the home page of this repository.

- "**.gitattributes**": This is a GitHub-generated file with repository information. It contains information for GitHub, but nothing specific to this project. You do not need to open this file to use the material in this repository.

3.2. Documents.

This folder contains the project documentation:

- "**RFID_Lock_Build_Instructions.pdf**": This document provides step-by-step instructions to build an RFID lock, including assembling the Wireless I/O Board, modifying the Tokatuker lock, installing the firmware on the Particle Photon, and assembling the hardware into a candidate cabinet.

- "**Solenoid_Lock_Build_Instructions.pdf**": This document provides step-by-step instructions to build a device to activate a solenoid lock, including assembling the Wireless I/O Board, installing the firmware on the Particle Photon, and assembling the hardware into an enclosure.

- "**Tokatuker_Cabinet_Digital_Lock_Testing.pdf**": This is a report of our investigations, experiments and findings about the Tokatuker lock and how it might be operated from a Particle Photon.

3.3. Hardware/Other Mechanisms.

This folder contains information about other electro-mechanical lock mechanisms that we surveyed. As of this date, we have not tested any of these other mechanisms. However, we feel that some of these other locks may be appropriate for situations where the Tokatuker lock is unsuitable; e.g. where it is undesirable to have the lock mechanism pop open the cabinet door or draw.

3.4. Software/Particle_SW/LockFirmware.

This folder, and its included subfolders, contains the firmware for the Particle Photon. Download this folder to your computer. You can then point the Particle Workbench IDE to this subfolder in order to:

- View the Particle source code.
- Compile the source code (locally or via the cloud).
- Flash the code to your Photon device.