Development of Low Cost, Open-Source, Machinery Access Control & Tracking System by Undergraduate Team

Owen Phillips[1], Jonathan B. Hord[2], Stefan Abare[3] , Giandre Acosta[4], Matthew B. Grooms[5], Avery White[6], Maurice Barnett[7], Garrett Ross[8], Yvon Feaster[9], and Todd Schweisinger[10]

ophilli@g.clemson.edu[1] , jhord@g.clemson.edu[2], sabare@g.clemson.edu[3], gacosta@g.clemson.edu[4], mbgroom@g.clemson.edu[5], avery5@g.clemson.edu[6], mauricb@g.clemson.edu[7], gmross@g.clemson.edu[8], yfeaste@g.clemson.edu[9], todds@clemson.edu[10] , Clemson University, Clemson, SC

CLEMSON UNDERGRADUATE RESEARCH

I. Introduction

Makerspace equipment often has inherent risks to its users. These risks can be reduced by training operators. An additional approach to reduce these risks is to install technology that restricts access to untrained users.

The Clemson [Machinery] Access Tracking System (CATS) is in development to create a more efficient way to operate a student space by automating the authentication process for a machine, so it will only power on for persons with permissions. Using CATS, facilities will be able to secure their machines by requiring students to provide credentials using their campus ID cards, and RFID card readers on machines/spaces. For double authentication a PIN number will also be required.

II. Background

The Creative Inquiry (CI) Program at Clemson University funds Undergraduate Research Projects. A CI team was formed in August 2016 from majors in Computer Science and Engineering, Mechanical Engineering, and Industrial Engineering to address this machine authentication challenge.

Most access protocols require a staff member to verify training credentials for each person wishing to use makerspace machines, but

Challenges of current access protocols can include:

- ●An Overloaded Staff Member
- ●Overly confident “I Know What I’m Doing” Users
- ●Accidental Machine Starts After Outage
- ●Effort Required to Record and Report Usage Data

Existing Solutions to Challenges Include- Makerspace Access Control System[1] - But it is not open source, which limits its application in customized student spaces.

III. Objective

Create an automated system, CATS, to provide an additional layer of safety by automatically restricting the power to machines and provide usage data for analysis by administrators.

IV. Methodology

To solve the challenges of a human dependent system (Figure 1) a new system must be designed that supplements the process with electronic back checks (Figure 2).

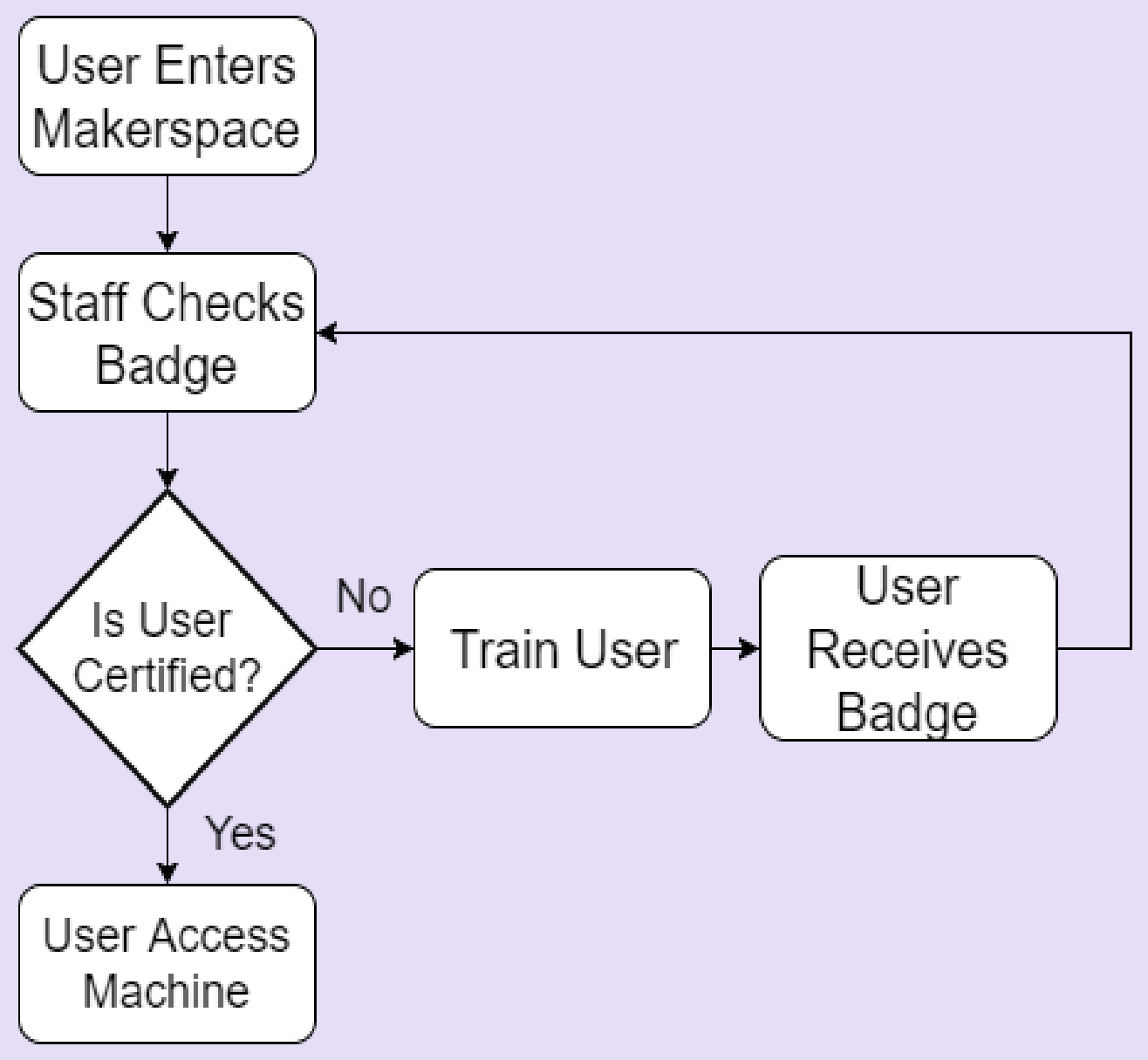

Figure 1: Human Dependent Credential Checks

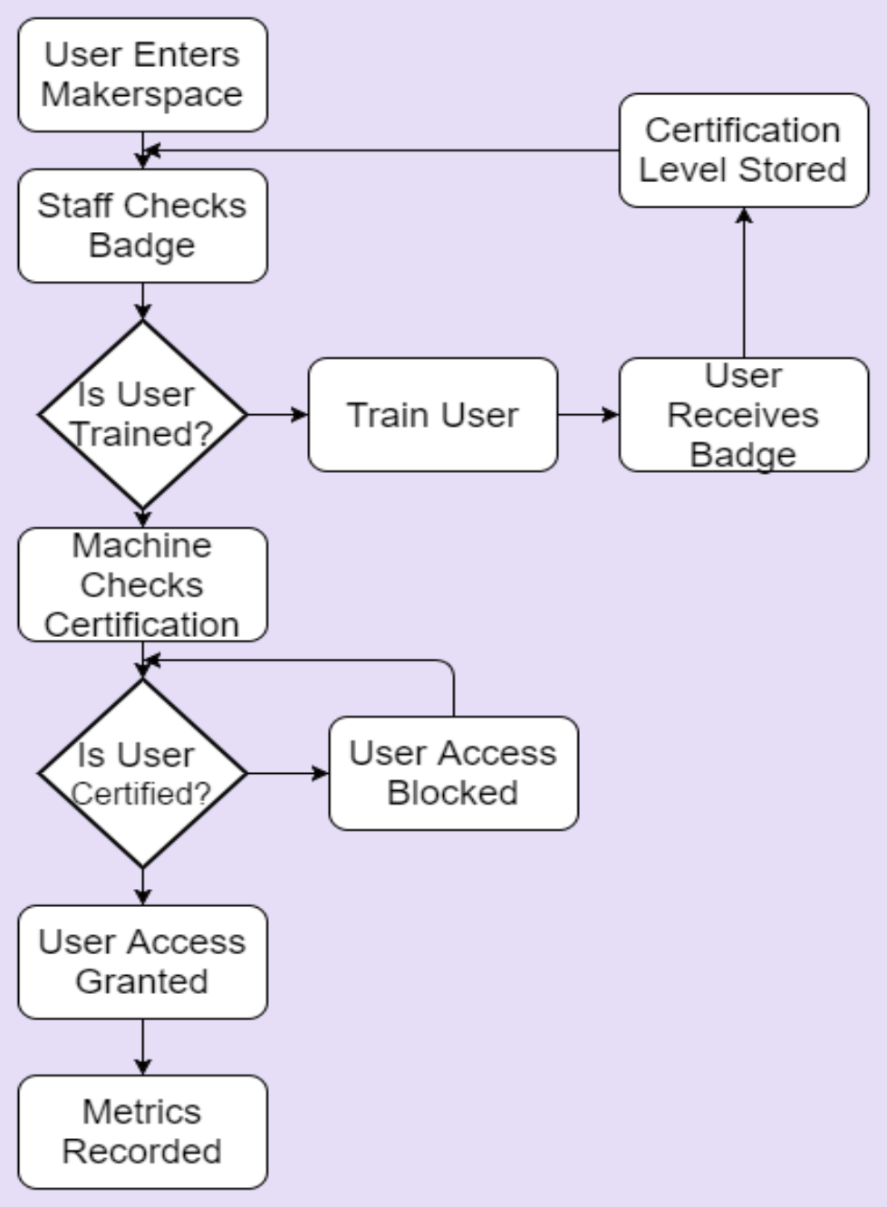

Figure 2: Electronic Control of Access

V. Results

The detailed logic for the CATS system can be seen in Figure 3. In contrast to Figure 1 this process will solve all the challenges from the previous access protocols and provide technical solutions to the proposed system in Figure 2.

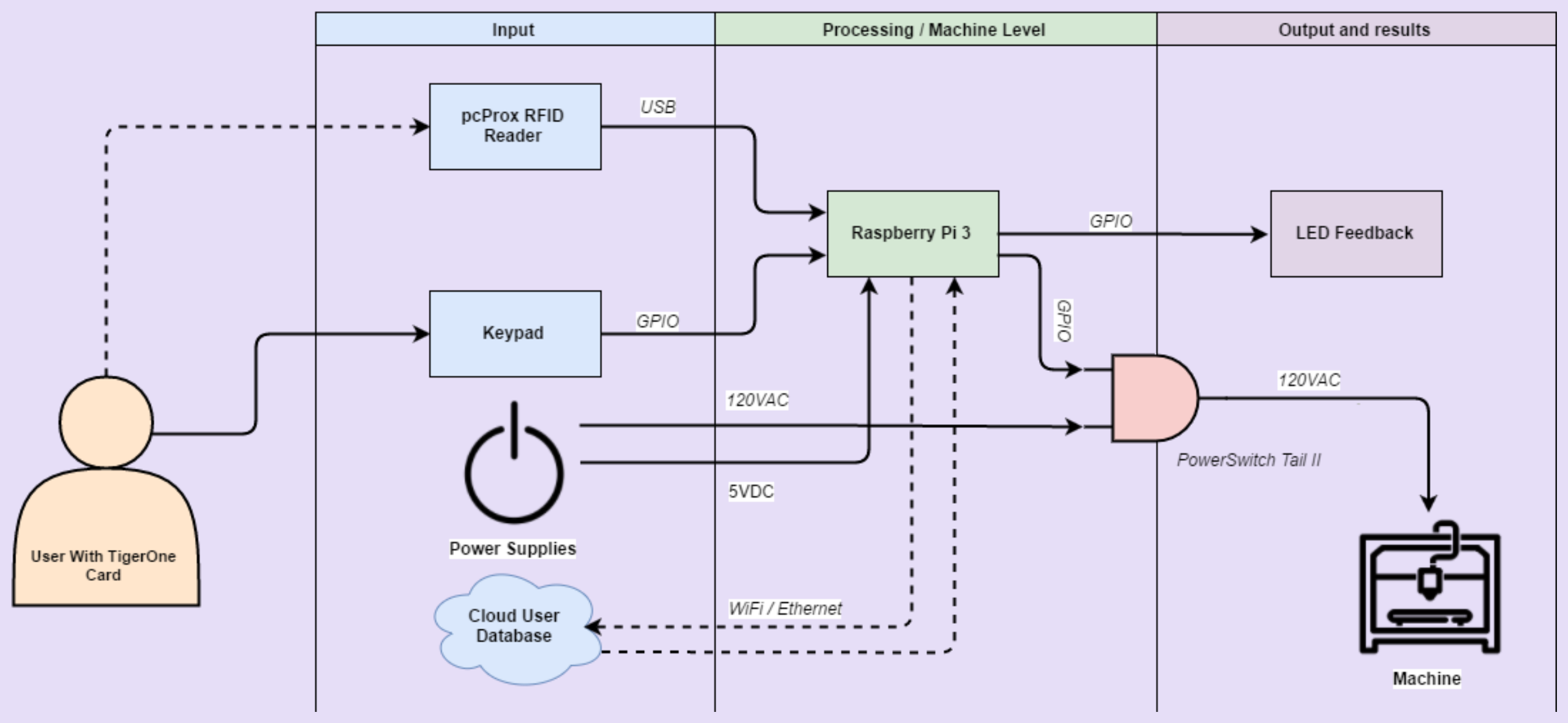

Figure 3: CATS Context Level Schematic

This prototype (Figure 4) provided a proof of concept. It uses both RFID User ID and PIN authentications. This prototype was redesigned into a Pi shield to organize input and output connections.

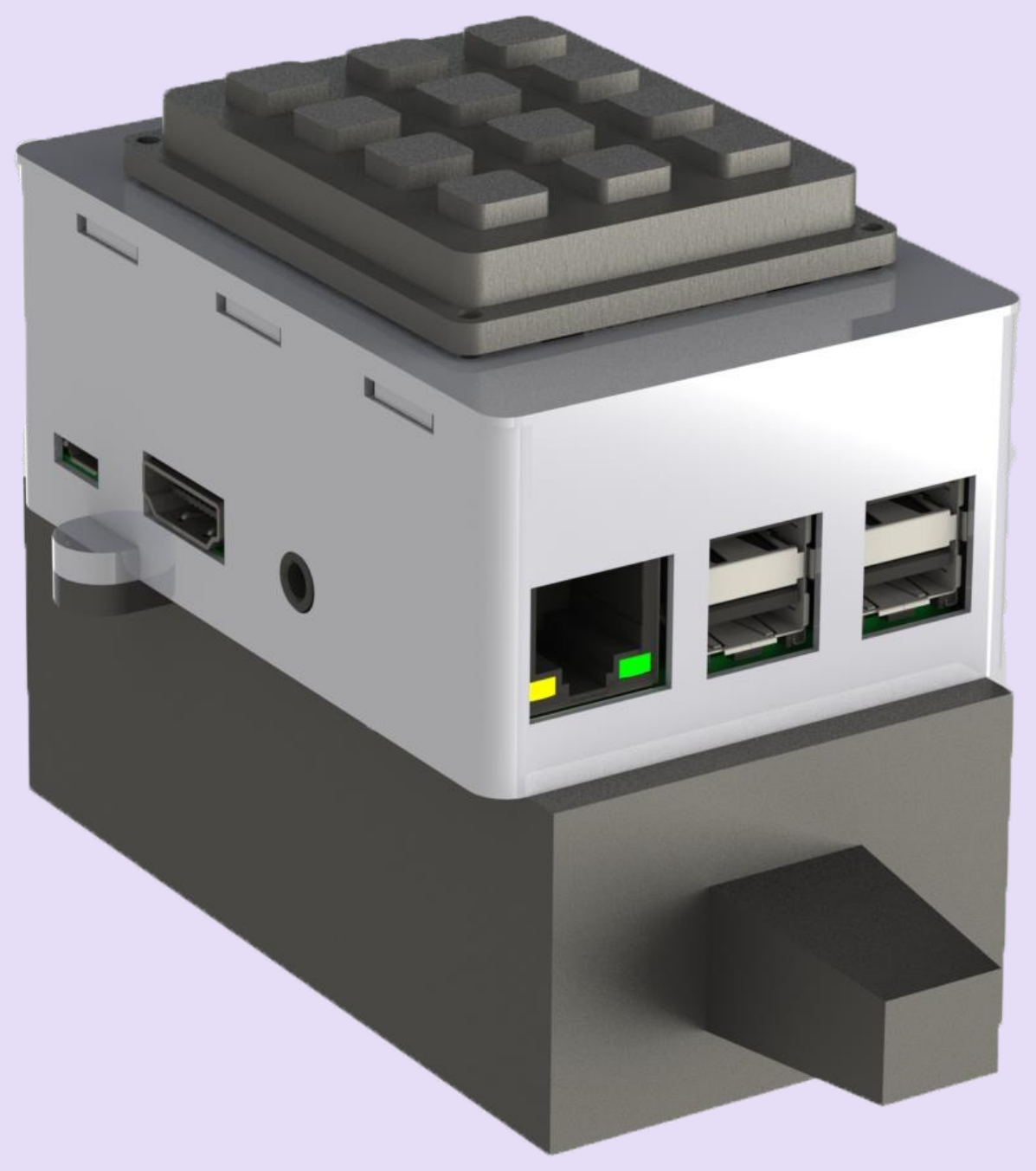

Figure 4: CATS Hardware Prototype

V. Results

The CATS Pi shield (Figure 5) organizes inputs (keypad) and outputs (Status LED, Power to Machine).

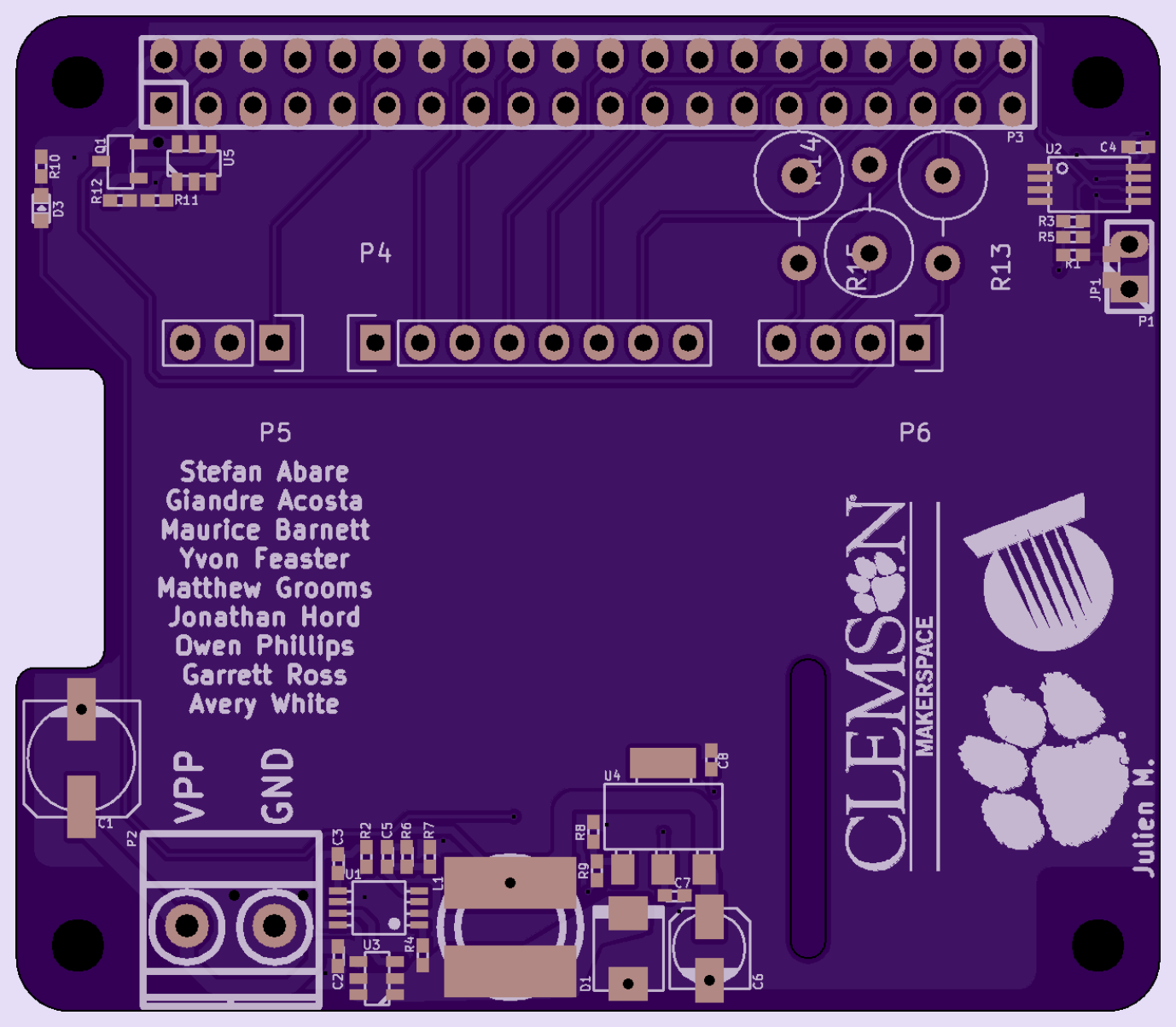

Figure 5: PCB Design of CATS Prototype

The CATS Pi shield connects to a Raspberry Pi 3 (Figure 6). The Pi 3 redirects inputs given through the RFID reader and keypad to a MySQL Database.

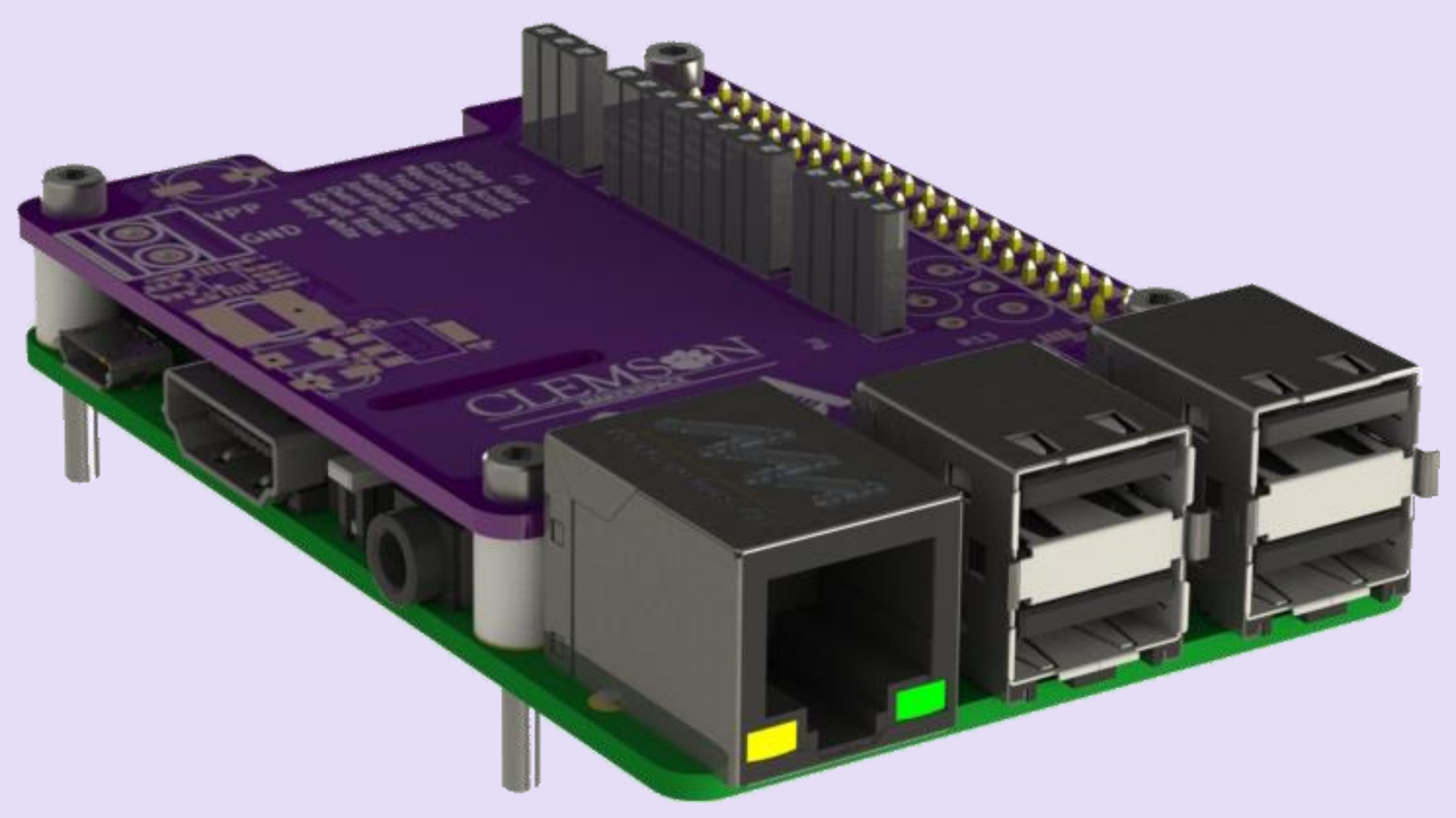

Figure 6: CATS Pi shield with Raspberry Pi 3

VI. Conclusions

Access Protocols for Makerspaces have inherent challenges which threaten safety. The team has developed an open source technology, the CATS system, that has the ability to automate the authentication process for machines.

VII. References

[1] George Carlson, Kolja Windeler, “An Introduction to the MACS - Makerspace Access Control System,”   MakerBarn. 2015. youtube.com/watch?v=CI3xxsBM9SE
[2] Crumpacker, Chris. "Using 3x4 Matrix Keypad with the Raspberry Pi." Crump Projects:. N.p., 13 May   2013. Web. 16 Sept. 2016.
[3]"How Can I Read Input from the Hosts Keyboard When Connected via SSH?" Linux. N.p., 1 Nov. 2013.   Web. 28 Sept. 2016.
[4] PyMySQL Methane. "PyMySQL/PyMySQL." GitHub. N.p., Nov. 2013. Web. 20 Oct. 2016.
[5] Tutorialspoint.com. "Python 3 MySQL Database Access." Www.tutorialspoint.com. TutorialsPoint, n.d.   Web. 20 Oct. 2016.

github - github.com/clemsonMakerspace/CATS
blog - ci.clemson.edu/blogs/cats/

This work was supported in part by the Clemson University Creative Inquiry Program

The presentation of this work was supported in part by - ISAM