ELEC5552 Design Project 2 – Team 05

User Manual

Version 1.0

23/10/2023

Table of Contents

List of Figures and Tables

1. Introduction

This User Manual (UM) provides the information necessary for the Australian National Fabrication Facility – WA node (ANFF-WA,) and future end-users to effectively use the Data Logging and Access Control Project developed by Design Team 05. Note that it is assumed that the system has been purchased as configured by Design Team 05, and thus the required modules have been pre-configured for internal communication, and system need only be configured for external communication by the end user.

1.1 Overview

The ELEC5552 Design Project 2 produced by Team 05 is designed to remotely monitor and regulate access to equipment within a Class 1000 nanofabrication facility operated by the project client: ANFF-WA.

The system is modular in nature, consisting of two logging devices, designed to be connected to equipment, an access card reader, 240ac isolation interlock, and a network hub connected to a human machine interface (HMI.) Modules communicate wirelessly over a mesh-type Zigbee network to facilitate user access and record equipment logs on a remote web-based server.

2. Getting Started

The following figure is designed to give users a general understanding of the functionality of the system, depicting the flow of information between modules over the two networks.

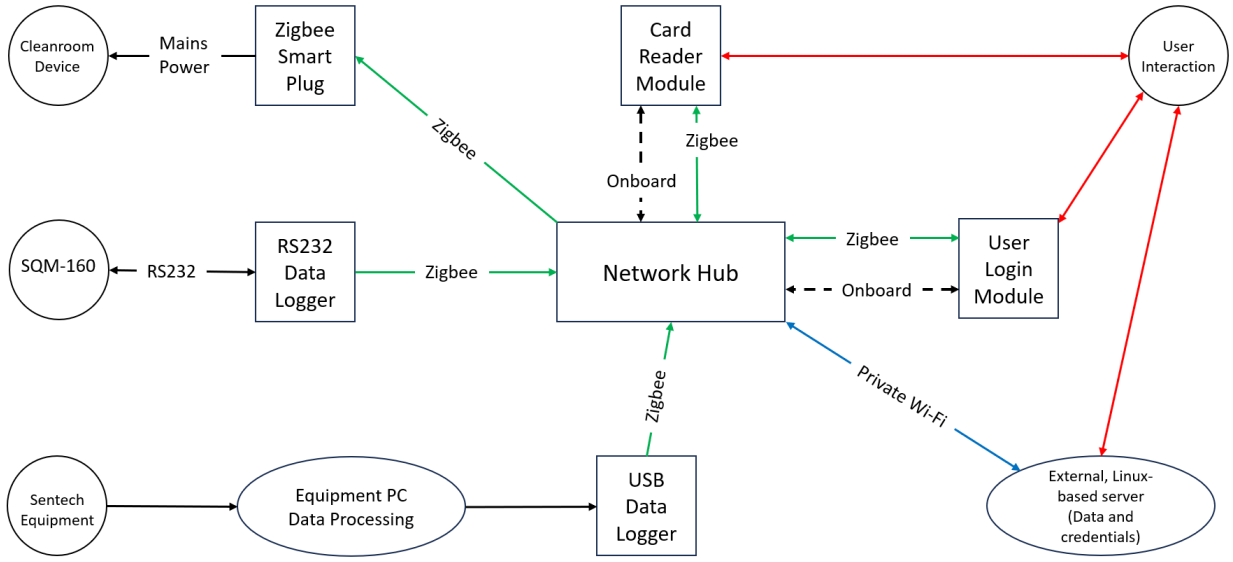

Figure 1 - System Wide Block Diagram

Section 3.1 of ELEC5552: Data Logging and Access Control Project: Final Report outlines in further detail a clear overview of design architecture.

2.1 Set-up Considerations

As the design system is largely automated, much of the work required to operate the system lies in the initial configuration, and minimal work is required once the system is operational. The following steps are required to configure the system.

1. Activate the 3.5-inch RPI display screen

Due to potential compatibility issues with the screen and the Raspberry Pi operating system used by the user, it is recommended that users select the 2021 version of the Raspberry Pi operating system when downloading the respective OS. Additionally, users should execute the following commands on the Raspberry Pi terminal:

1) Install the touch driver:

git clone https://github.com/waveshare/LCD-show.git

cd LCD-show/

2) Execute the following code to restart the device and activate the screen:

chmod +x LCD35-show

./LCD35-show

Note: The Raspberry Pi should remain connected to the network during the execution of these commands.

If screen orientation settings are required, users can refer to the Waveshare official guide for the 3.5-inch RPi LCD (A) at the following link: [3.5inch RPi LCD (A) Guide]

(https://www.waveshare.com/wiki/3.5inch_RPi_LCD_(A)) for further instructions)

2. Install the appropriate libraries

To successfully run the provided code, users need to download the corresponding libraries. These libraries do not come with python, and you will need to download them as an additional download Here are the libraries needed for the respective modules in the code:

1) Login interface

pip install tkinter/ pip3 install tkinter

pip install subprocess/ pip3 install subprocess

2) Card reader

pip install board/ pip3 install board

pip install busio/ pip3 install busio

pip install adafruit-circuitpython-pn532/ pip3 install adafruit-circuitpython-pn532

3) Interlock

pip install tinytuya/ pip3 install tinytuya

4) Network hub

pip install pexpect/ pip3 install pexpect

pip install watchdog/ pip3 install watchdog

pip install pyserial/ pip3 install pyserial

The libraries required by other modules already exist in previous modules, so no duplicate libraries are given.

Note: ‘pip3’ is specifically for Python 3, while ‘pip’ is usually associated with the default Python version (often Python 2).

3. Retrieve User Credentials on the Remote Web Server Host Linux Machine

To acquire user credentials, execute the 'whoami' command in a terminal window. This information is essential for authenticating SCP transfers within the network hub during the setup process.

4. Determine the IP Address of the Remote Web Server Host

Open a terminal and use the 'ipaddr' command to obtain the IP address. This is crucial for enabling automated communication between the Network Hub and the Remote Server.

5. Supply +5V Power to Logging Modules and the Network Hub

6. Establish relevant connections Between the Network Hub and the Human Machine Interface (HMI)

The Network Hub contains a mini-HDMI input for connection to a monitor, and both Bluetooth and a USB interface for connections to a keyboard and mouse.

7. Configuration of Credential Check Script

Using the Network Hub's HMI, access the Python script titled "keyboardCredentialCheck.py." Insert the IP address of the remote web server host into line 4, as illustrated in Figure 2.

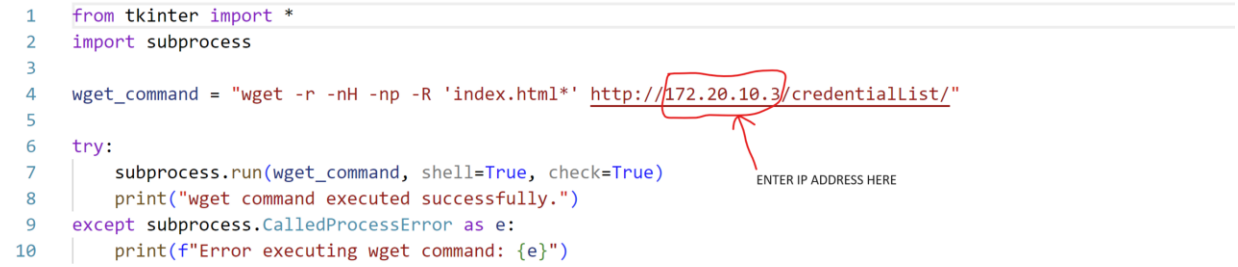

Figure 2 - Configuration of Credential Check Script

8. Configuration of Log Storage Script

Similarly, using the Network Hub's HMI, open the Python script titled "logSend.py." Enter the pertinent user and password information in the 'remote_user' and 'remote_password' prompts, found on lines 9 and 12, as depicted below in Figure 3.

```
7   # Define your local directory and remote server details
8   local_dir = "/home/pi/logData"
9   remote_user = "tomgreenland"
10  remote_host = "172.20.10.3"
11  remote_dir = "/var/www/logData"
12  remote_password = "3005"
```

Figure 3 - Configuration of Log Storage Script

9. Configure the Apache Remote Web Server on the Linux Host

Run the server configuration script titled "webServerConfig.py," which can be found in the GitHub repository. Please note that this action requires administrative privileges.

10. Execute the Following Scripts via Terminal in the HMI

Run the 'cardreader1.py,' 'interlock.py,' 'keyboardCredentialCheck.py,' 'logSend.py,' and 'reception.py' scripts via the Human Machine Interface on the network hub.

11. With these steps completed, the system is now fully configured and ready for the end-user's application.

2.2 User Access Considerations

Instructions: Describe the different users and/or user groups and the restrictions placed on system accessibility or use for each.

The system is designed to facilitate access control to the machines within the ANFF-WA cleanroom facility, and thus requires a system administrator to manage user access. The system administrator requires administrative access to the Linux webserver host and the network hub HMI.

In the directory titled “credentialList” on the web server host, the system administrator should add two text files titled “Account” and “UID” respectively. In the “Account” text file the administrator should add the usernames and passwords for individuals who require access to the cleanroom equipment and wish to log in via the HMI keyboard. The file should have the following structure:

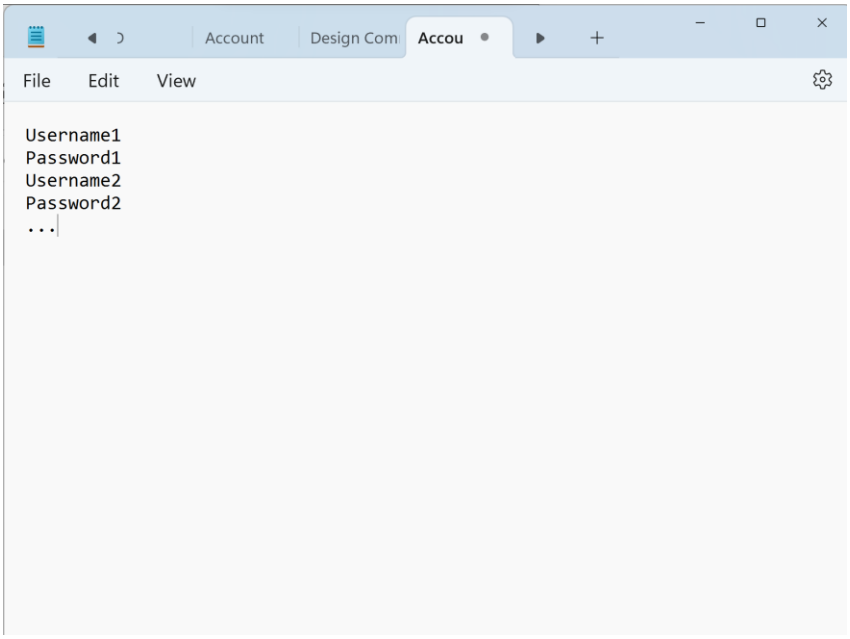

Figure 4 - Account Text File Structure

The UID text file is designed for facilitating access via UWA campus card. Each UWA campus hard has a unique UID code (e.g. 99fc335d.) Those who require access should have their UID appended to this text file. Note that the UID is printed on the “cardreader1.py” script terminal upon scanning, and thus can be obtained for any unknown cards via the Network Hub HMI.

2.3 Accessing the System

To access the system, users should ensure that their credentials are presented within the correct text file in the “credentialList” directory of the web server, as discussed in the previous section. The user should then proceed to either tag their card or enter their username and password via the HMI to allow power to the cleanroom equipment.

2.4 Exiting the System

Users are responsible for logging out of the system and isolating the equipment when their work is complete. This is done by either retagging their UWA campus card on the card reader or clicking the “Return to Login” button on the Network Hub HMI as shown.

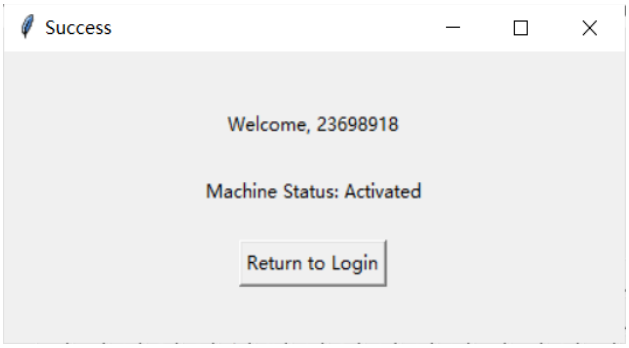

Figure 5 - Exiting the System via HMI

For the card reader, the user needs to bring the card close to the reader once again. The reader will recognize the card, providing information to the network hub. The network hub will then send a signal to the interlock to shut off the power. In essence, the initial card activation of the interlock refers to powering up the system, while the second card swipe will turn off the power supply.

3. Using the System

Once configured, the system operation is automated and does not require any user interaction beyond logging in/out and administrative management of access lists as described in previous sections.

When logged in, the user should proceed to use cleanroom equipment as normal, and observe the processed logs appear on the web server.

4. Troubleshooting & Support

4.1 Error Messages

Upon system configuration and initial running of scripts, the user should monitor the terminals on the Network Hub HMI for any errors. The following examples, reasons and solutions are commonly found.

SCP Error Messages

1.) No Such File or Directory:

Meaning: This error indicates that either the source or destination file or directory does not exist.

Fix: Double-check the file paths for typos, and ensure the files or directories exist at the specified locations.

WGET Error Messages

1.) Connection Timed Out:

Meaning: Wget couldn't establish a connection to the specified URL within the given timeout period.

Fix: Check the URL for correctness and ensure the network hub is on the same external network as the remote web server.

2.) 403 Forbidden:

Meaning: The server refuses to fulfill the request, often due to insufficient permissions.

Fix: Check the user configured in the network hub has the necessary permissions to access the resource.

Access Errors:

1.) New User is not given provided access.

Meaning: The credential lists the network hub currently has downloaded do not have the latest user additions.

Fix: Rerun the keyboardCredentialCheck script on the network hub HMI.

Logging Errors:

1.) Logs are being received, but not sent to the remote web server.

Meaning: The SCP command isn’t being received by the remote web server.

Fix: Ensure the Linux web server host is not asleep or shutdown.

4.2 3.5inch screen not working

When the screen cannot be displayed, it may be caused by the following reasons

1.) Using the wrong version of raspberry pi system.

Meaning: the newest version of raspberry pi system doesn't fit the display soft.

Fix: use the version before 2021.

2.) Using the wrong version of display software

Meaning: the screen only fit certain display software.

Fix: this screen only fit the waveshare version. Make sure you use the right one.

4.3 interlock missing

If you find that the login interface and card reader cannot control the wireless switch, it may be caused by the following reasons:

Interlock information error:

1.) using the wrong Device_id and local_key

Meaning: the raspberry sending the command to a wrong wireless address.

Fix: download the tinytuya source for python in your computer, then use command "-m tinytuya scan" to find the current Device_id and local_key of the smar plug. Then open switchtest3.py file in raspberry pi to change the Device_id and local_key.

2.) Using the wrong version of tinytuya.outletdevice

Meaning: the smart plug can not be controlled when using wrong version of tinytuya.

Fix: this smart plug use the 3.4 version of tinytuya. Open the switchtest3.py in raspberry pi to check the version of tinytuya.

4.4 Support

Table 1 - Support Points of Contact

Contact	Organization	Phone	Student #	Role	Responsibility
Thomas Greenland *Gal Naveh* *Timothy Ludovico* *Miles Lockwood* *Chengyun Ji* *According to Lei.*	*UWA*	*-*	*22478465* *22733389* *22711175* *22731994* *23741675* *23698918*	*Design Team*	*Hub and Server* *USB Module and LAN* *RS232 Module and LAN* *Hub* *Interlock* *Card Reader and HMI User Access*

Appendix A: Record of Changes

Table 2 - Record of Changes

Version Number	Date	Author/Owner	Description of Change
<1.0>	*<23/10/2023>*	*Team 05*	*<Document Creation>*

Appendix B: Referenced Documents

Table 4 - Referenced Documents

Document Name	Document Location and/or URL	Issuance Date
UWA ELEC5552 Data Logging and Access Control Project Team 5: Final Report	*Contact Team 05*	*<23/10//2023>*
Relevant System Python Scripts	*https://github.com/NavehGal/ELEC5552-Team-5-Data-logging-and-access-control-ANFF-*	*<23/10//2023>*