CS350 Safehome Project
USER MANUAL
Team 3

2025-12-01

20240397	Hichan Shin
20240782	Youngdo Han
20240905	Bumgyu Suh
20240951	Mohamed Elnakeeb

Korea Advanced Institute of Science and Technology

Table of Contents

I. Installing & Testing SAFEHOME

Installation

1. *Extract and navigate to the safehome root:* Download the SAFEHOME.zip and extract it, then access the root of the folder using your terminal
2. *Install Python with pyenv*: Ensure you have the required Python 3.14 version for SafeHome. Use pyenv to install and manage the correct Python version, you can don't have to specify the version since it's specified in the Safehome root(if there are problems try specifying the version after install/local, ie. install 3.14):
   `pyenv install`
   `pyenv local`
   On Windows: Consider using the Windows Subsystem for Linux (WSL) to run pyenv and the following commands. If you prefer native Windows, you can use the `pyenv-win` tool or install Python 3.14 from python.org directly.

3. Create a virtual environment: Once the correct Python version is active, create an isolated environment using `venv`:
   `python -m venv .venv`

   This will create a `.venv` directory in the project folder containing the virtual environment.

4. Activate the virtual environment: Before installing dependencies, activate the environment:

- **Linux/Mac**: `source .venv/bin/activate`

- **Windows (PowerShell)**: `.\.venv\Scripts\Activate.ps1`

- **Windows (CMD)**: `.\.venv\Scripts\activate.bat`

   After activation, your shell prompt should indicate that the environment is active (often by prefixing the prompt with the environment name).

5. Install dependencies: With the virtual environment active, install the required Python packages for SafeHome. For example, if a requirements.txt file is provided in the repository, run: `pip install -r requirements.txt`

   This will download and install all the necessary libraries. Make sure this step completes without errors. (If the project uses a different dependency file or tool, use the appropriate install command as noted in the project documentation.)

Testing

Once installation is complete, you can verify that everything is set up correctly by running the test suite or included verification script:

1. Activate the environment (if not already active): Ensure that your virtual environment from the installation steps is activated so that you are using the correct Python interpreter and dependencies.

2. Run the SafeHome test script: Use the provided cross-platform helper to execute the test suite from the project root:
   `python run_tests.py`

   To forward extra pytest arguments, add them after a `--` separator, e.g. to filter tests:
   `python run_tests.py -- -k login`

   For a quick coverage summary, add the `--coverage` flag:
   `python run_tests.py --coverage`

   To point pytest at specific test folders or files pass them with `--tests`
   `python run_tests.py --tests test api/test`

3. Check the output: The test script will run a series of checks or unit tests. Verify that all tests pass or that the script outputs the expected success messages. If the tests complete without errors, it means the installation was successful and the SafeHome system is ready to use.

4. Troubleshooting: If any tests fail or you encounter errors, double-check that you installed the correct Python version and all dependencies. It may help to re-read any project-specific notes or adjust environment variables.

The main tests are within Safehome/test, while the gui unit tests are within Safehome/gui_unit_tests these have been separated due to them requiring MANUAL RUNNING and are mainly used for documentation. These GUI tests create and destroy GUI instances, so running them one after the after without sufficient delay WILL cause errors. Proceed carefully.

II. Navigating & Using SAFEHOME

Run SAFEHOME by running **`python src/main.py`** from the SAFEHOME directory. This will first open two windows: Sensor Intruder and Control Panel. Press X on the top right of any SAFEHOME window in order to exit the program safely. We do not warrant the safety of the user from any errors arising from inappropriate shutdown of the program.

1. Sensor Intruder

The first thing that shows up is the Sensor Intruder. You can press a button to trigger the corresponding sensor, and to release it, to be detected by SAFEHOME accordingly.

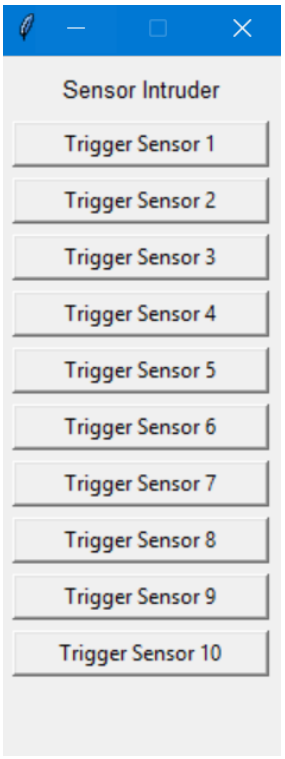

Fig 1. Sensor Intruder Default

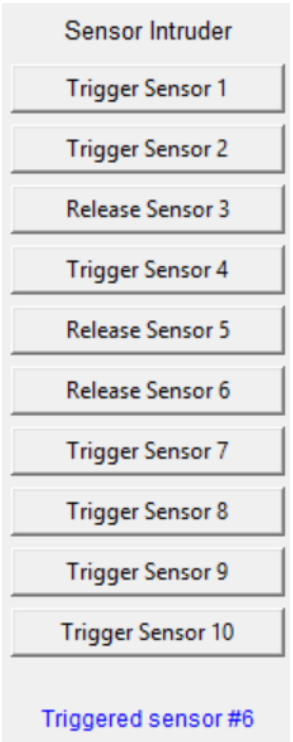

Fig 2. Pressing Trigger turns it into “Release”

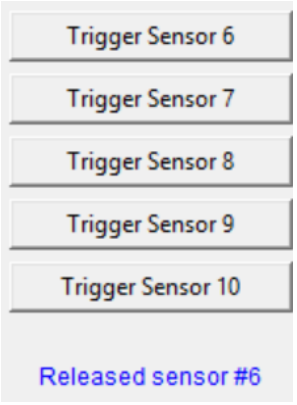

Fig 3. You can manually release a sensor.

SafeHome automatically releases sensors that have already caused SafeHome to encounter an alarm condition, but this is not reflected in the Sensor Intruder. You must manually click “Release Sensor X” and trigger the sensor again. This was designed to prevent spam.

2. The Control Panel

The second thing that shows up is the Control Panel. Press “1” to turn SAFEHOME on. The other buttons do nothing in this state.

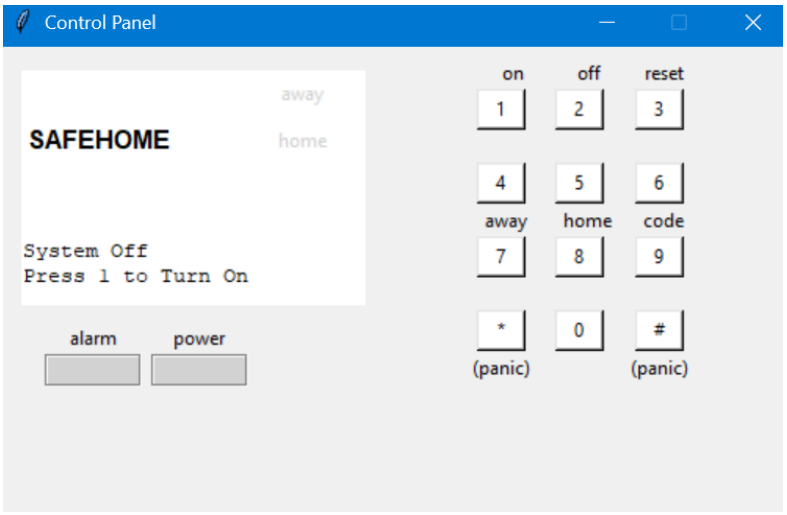

Fig 4. Control Panel Turned Off

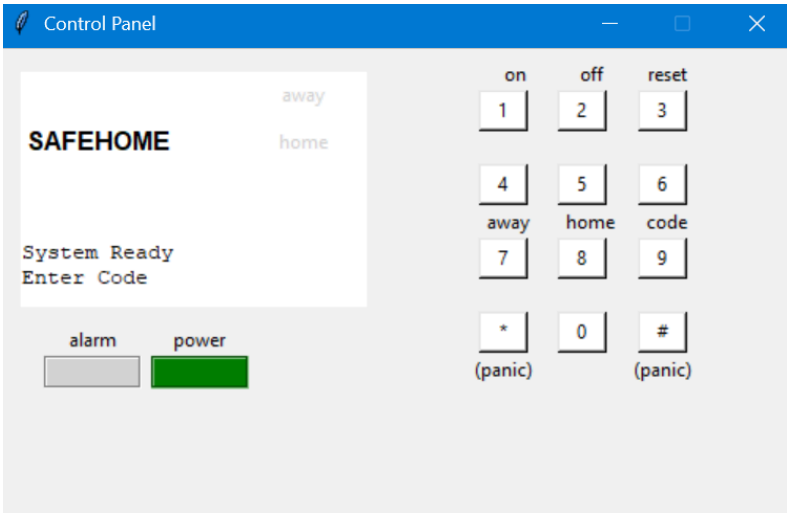

Fig 5. Control Panel Turned On

You must enter the control panel password (always 4 digits) to access the rest of the controls. The default password is “1234”.

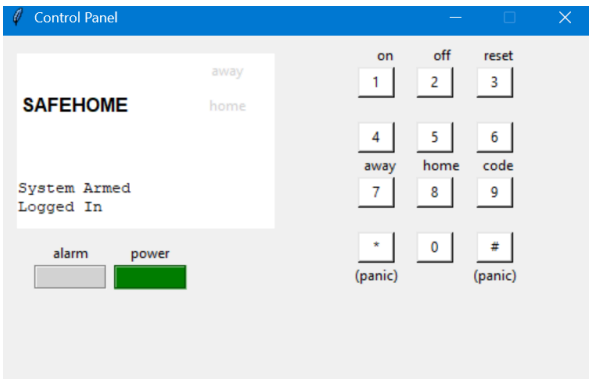

Fig 6. Control Panel Logged In

Once logged in, the “WEB UI” for SAFEHOME window will pop up.
Once logged in, you can:

- Press 2 to turn the system off
- Press 3 to reset SAFEHOME to its default configurations (WARNING: ALL configurations including security modes, security zones, system configuration, passwords, camera states & passwords will be RESET).
- Press 7 to set the security mode to “away”
- Press 8 to set the security mode to “home”
- Press 9 to change the control panel password
- Press * or # to sound the alarm

3. Web Browser UI

Turning SAFEHOME on through the control panel lets you access the WEB UI. You must login with the correct credentials to access any of its features. The username is always “admin”. The default password is “1234”. Enter in the credentials and click “LOGIN”.

Fig 7. Login Screen

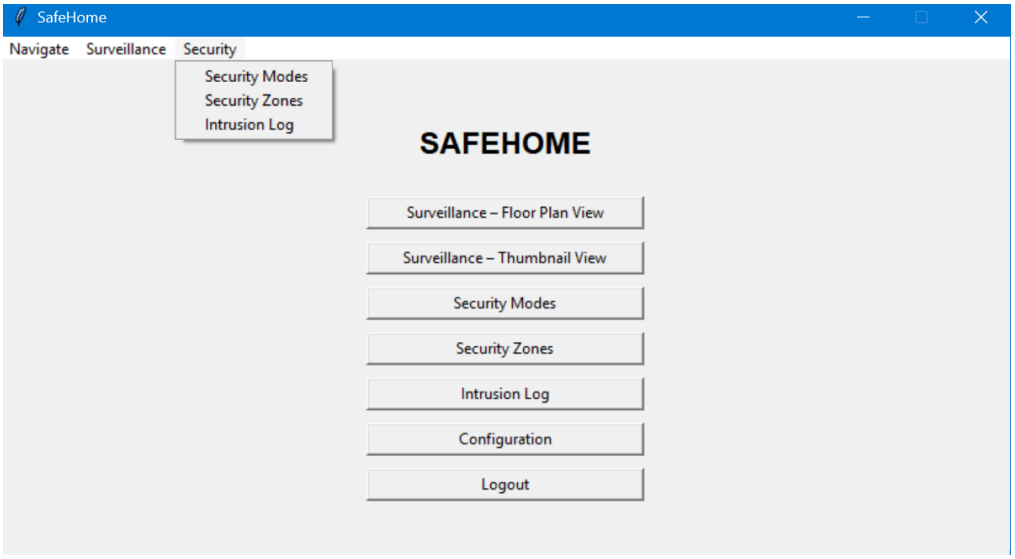

Fig 8. Main Menu

Logging in lets you access the Main Menu. The contents of the main menu is also accessible through the navigation bar at the top of SafeHome which is accessible from any page as long as you have logged in. Remember to press “Logout” to log out.

4. Web Browser UI: Surveillance Floor Plan View

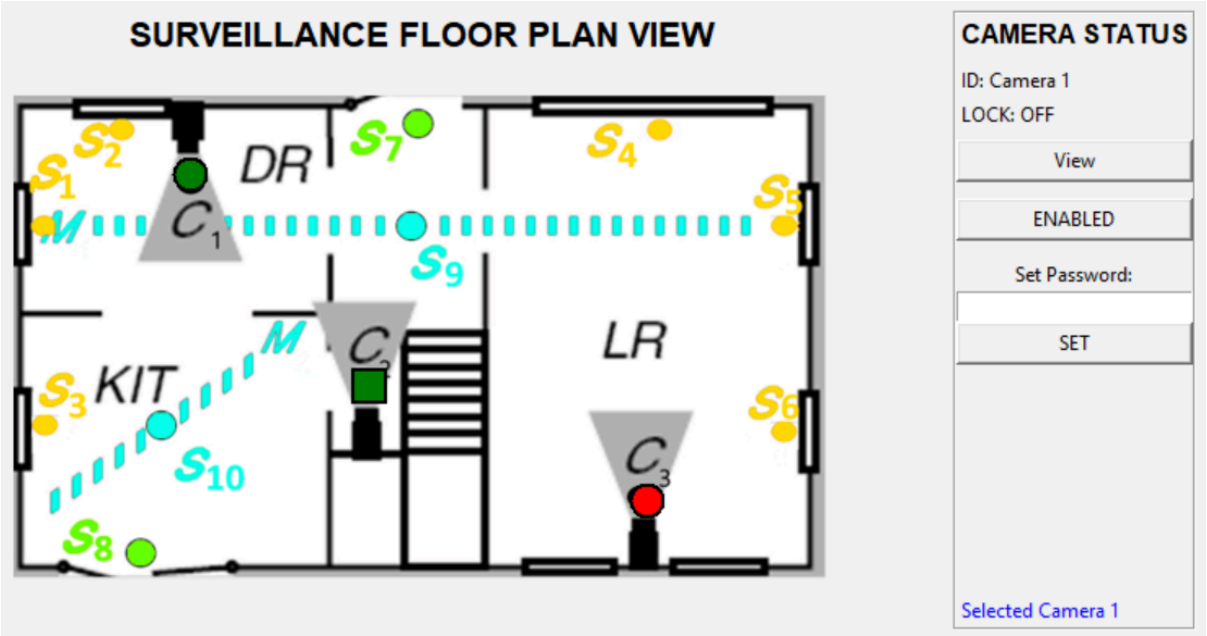

Fig 9. Surveillance Floor Plan View

Select a camera (GREEN/RED CIRCLES/SQUARES) to see and edit the camera status shown in the right. SQUARE means the camera is locked with a password (you cannot access VIEW or ENABLE/DISABLE or DELETE the password before you enter a password). CIRCLE means the camera is not locked. Remember, you can only view cameras that are ENABLED.

5. Web Browser UI: Single Camera View

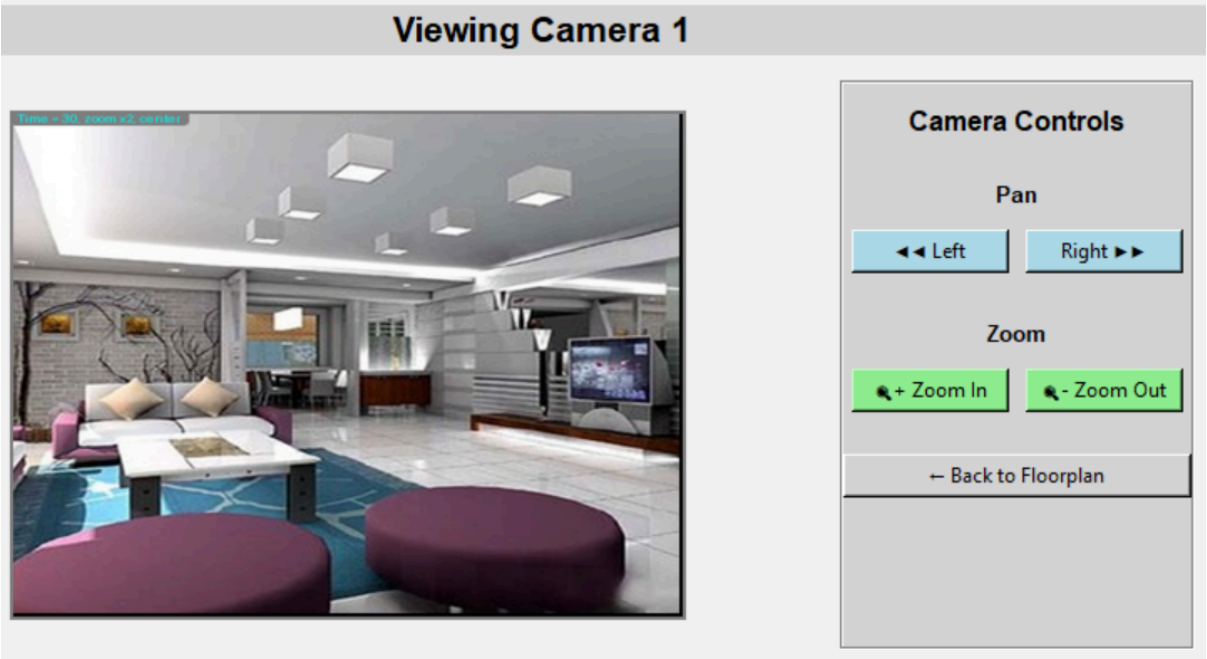

Fig 10. Single Camera View

6. Web Browser UI: Surveillance Thumbnail View

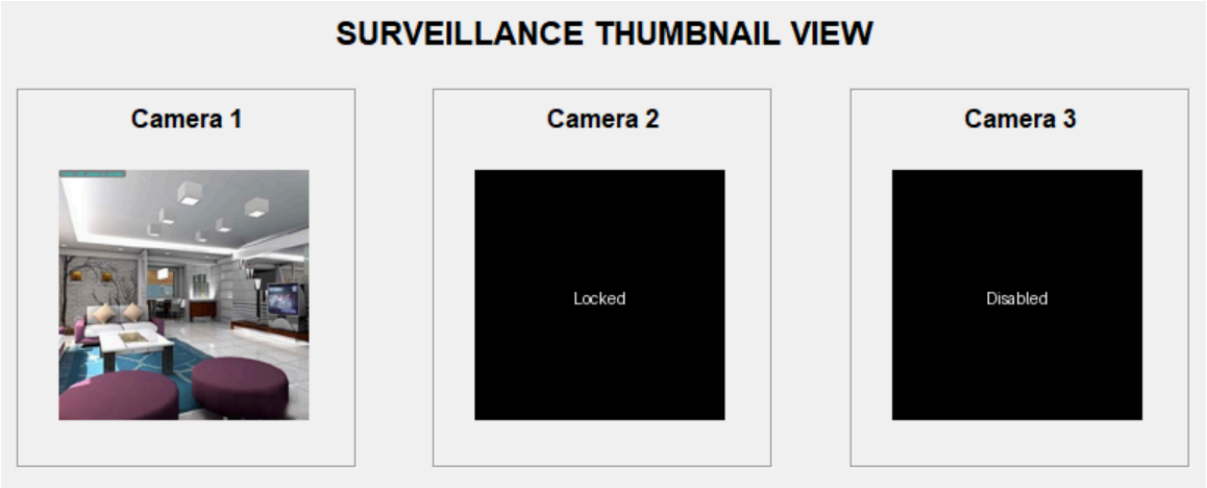

Fig 11. Surveillance Thumbnail View

This shows all the camera views at once. Locked and Disabled cameras are not viewable.

7. Web Browser UI: Phone Number Verification

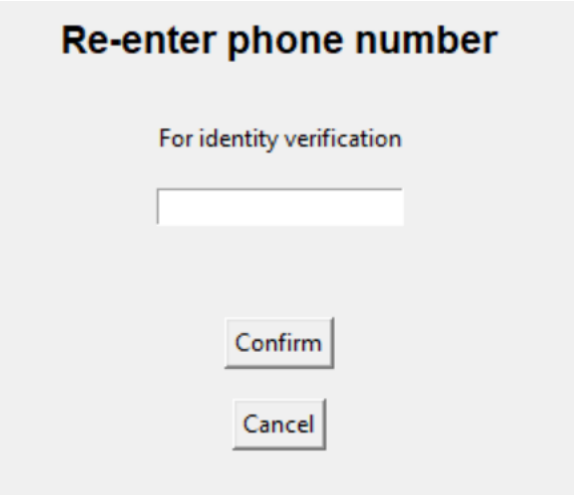

Fig 12. Phone Number Verification

In order to access the following pages: Security Modes, Security Zones, Intrusion Logs, and Configuration, you must enter your preset home phone number to verify your identity. The default phone number is **01012345678**.

8. Web Browser UI: Security Modes

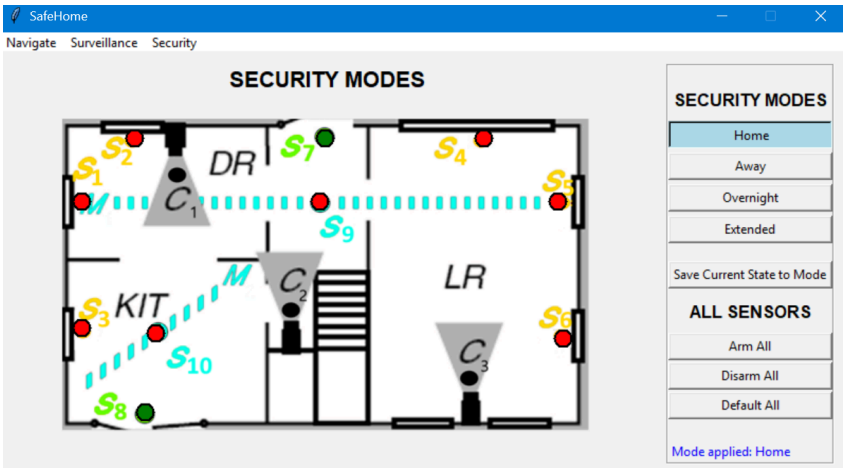

Fig 13. Security Modes

Select a security mode to turn into that mode. You can arm/disarm sensors by clicking on them in the floor plan (RED OR GREEN CIRCLES, RED means DISARMED, GREEN means ARMED). The current map of armed and disarmed sensors can be saved to the current security mode by pressing "Save Current State to Mode."

For convenience, you may use the "Arm All" and "Disarm All" to arm/disarm all sensors, ignoring both security modes and security zones. There is also a "Default All" option to make the sensors follow security modes/zones first. The details on which setting the sensors will follow is in: [Sensor Armed/Disarmed order]

9. Web Browser UI: Security Zones

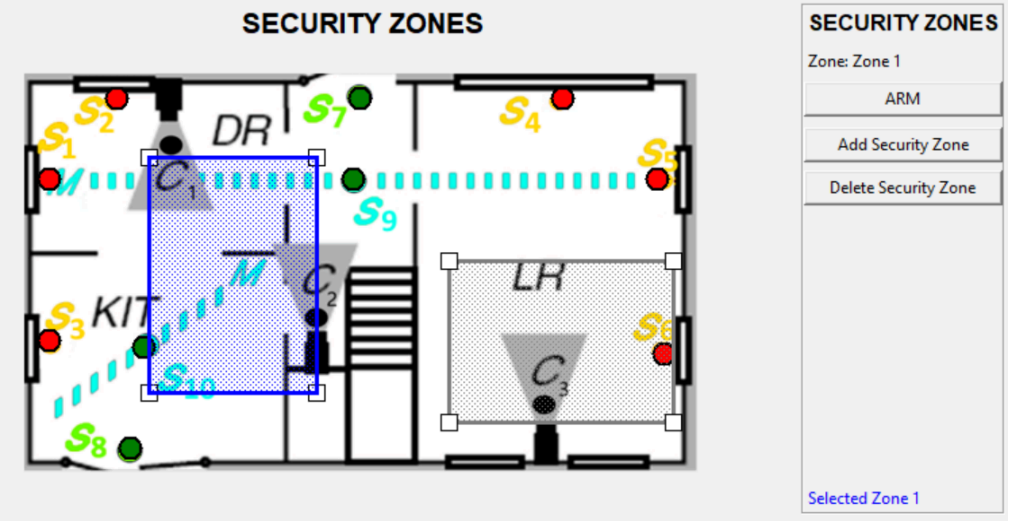

Fig 14. Security Zones

Security zones can be added, deleted, armed/disarmed. Clicking and dragging the boxes moves the security zones accordingly, and you can resize the zones by using the corners. To include a sensor, the security zone must cover its corresponding red dot. For motion sensors, if a safety zone overlaps with any part of the sensor's detection area, the sensor is considered part of that zone. A sensor shared by multiple zones will remain active unless all zones it belongs to are deactivated.

10. Web Browser UI: Intrusion Logs

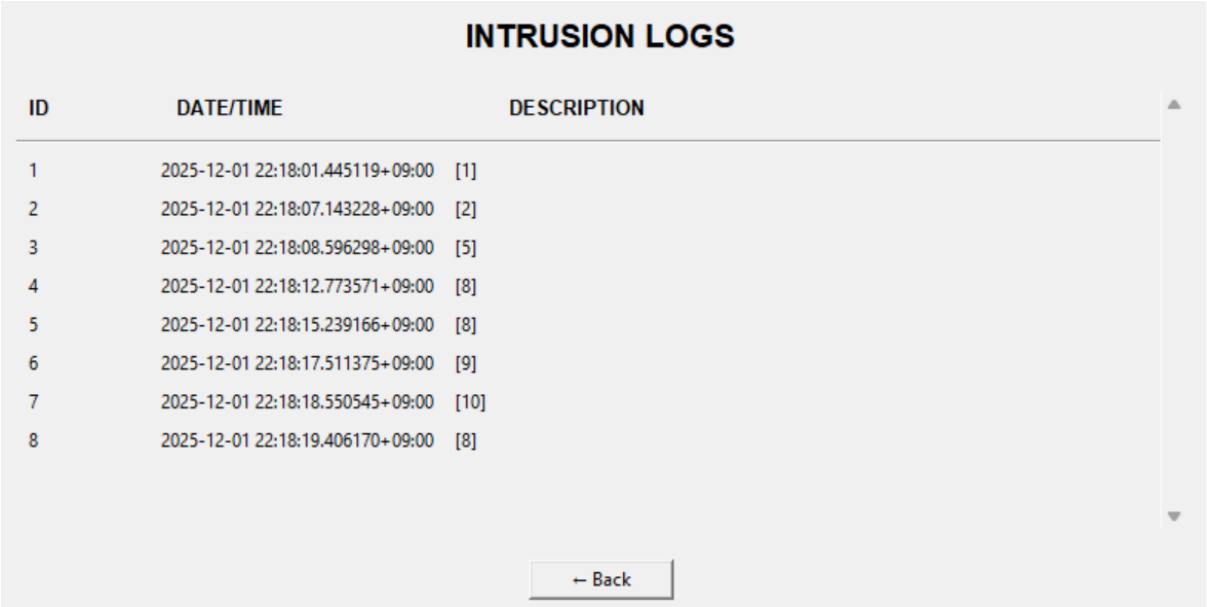

Fig 15. Example Intrusion Logs

Every time an armed sensor is triggered, it is written in the Intrusion Logs. The date/time of the intrusion is shown, and the description shows which sensor was triggered, by ID.

11. Web Browser UI: Configuration

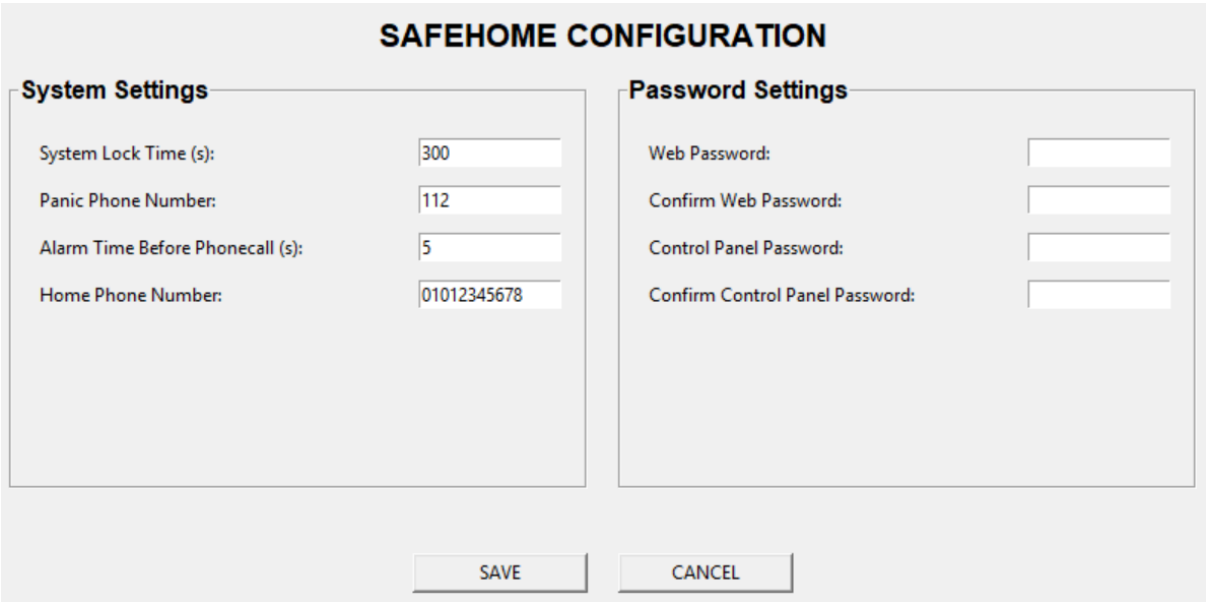

Fig 16. Default SAFEHOME Configuration

You can change system settings here. The current settings are shown when the page is opened. If the password settings are left blank, they are not changed. Remember to click SAVE to save the settings, CANCEL will ignore the inputs. All the inputs can only be numbers (0123456789), and each field has a maximum length.

III. Other SAFEHOME Details

1. Detecting Intrusion

SAFEHOME can detect intrusions through ARMED sensors when it is ON. The control panel will show the latest information on which sensor was triggered, show an ALARM light, send an ALARM sound (OS-dependent as it is actually printing a '\a' character) and wait a user-determined amount of time before calling emergency phone number configured by the user. The alarm light goes off when the call happens.

2. Delays

There are set delays in SAFEHOME. The most important delays are the camera and sensor update times. There are slight delays between each update.

3. Sensor Armed/Disarmed order

a. If each sensor is armed or disarmed, it applies under the highest conditions
b. If security zone is enabled, the sensors in the zone are armed. (But if each sensors are disarmed, it remains disarmed.)
c. If security mode is not none, sensors are armed/disarmed by data in the mode. (But if security zone is enabled, sensors belonging to that zone remain armed even if they are disarmed in security mode. And if each sensor is armed/disarmed, it follows that condition.)