Team 9 testing, by team 8

This is the bug report of all bugs found by team 8 when testing the implementation of team 9.

Error 1:

Input Sequence:

-Login to the control panel as admin
-Open the front door
-Activate away more
-Close the front door
→ Alarm activates.

Erroneous behaviour:

Based on Team 9's SRS: use case 2A, scenario 5: "If arming, the system may prompt the user to confirm that all monitored doors/windows are closed. " and exception 5a: "5a. User attempts to arm but a monitored sensor is open: The system displays a warning message ("Door/window open") and may prevent arming until the condition is resolved or manually bypassed. "
Based on old team 3's SRS: use case 2A exception 2-a, we get the same idea.

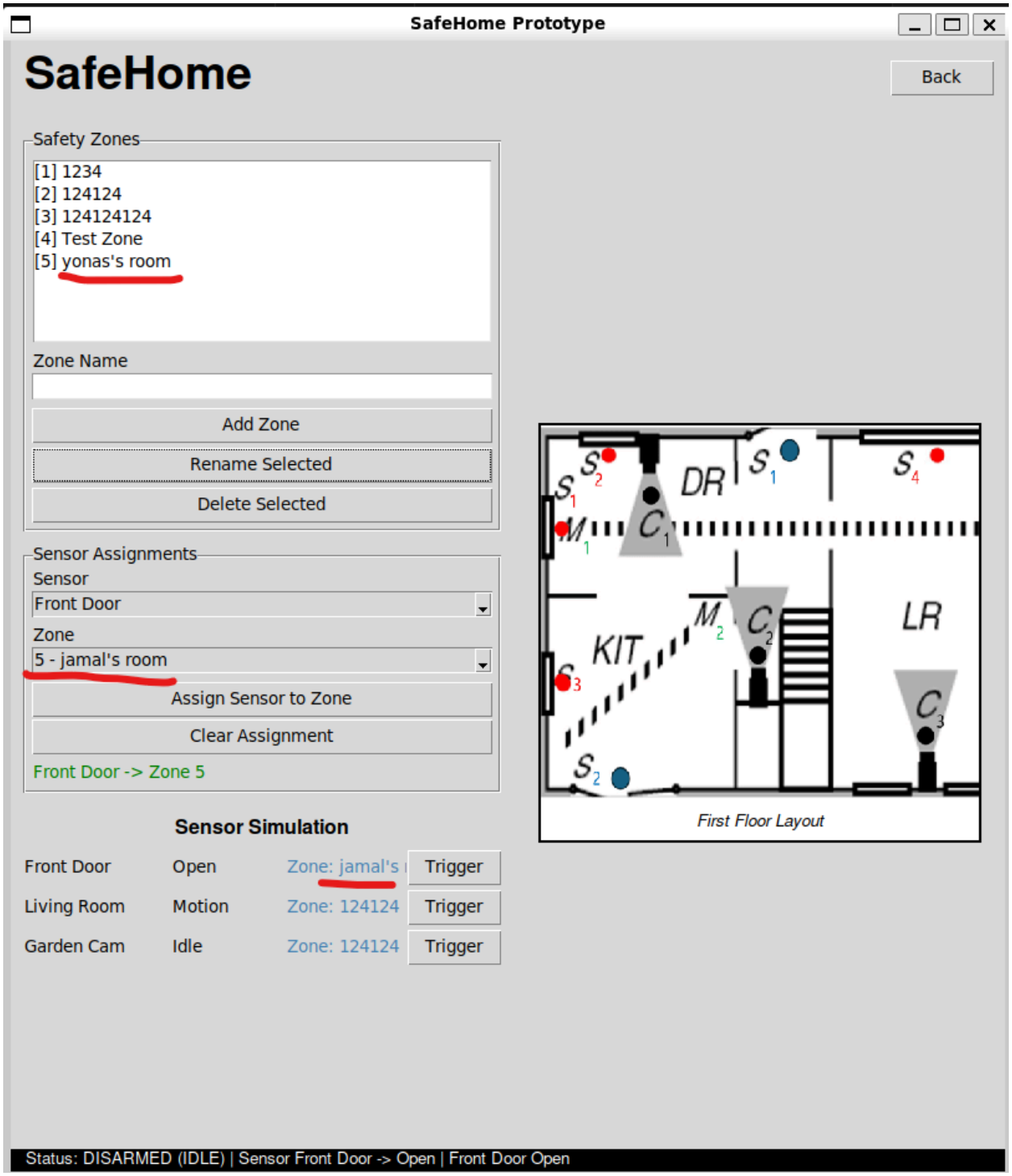
→ We are expected to not be allowed to arm the system if a Door/Window is open, at least not without manual bypassing. Yet in the implementation the alarm activates without any error warning nor manual bypass needed

Error 2:

Input Sequence:

-Login to the control panel as admin
-Create new safety zone with name A
-Assign sensor to zone A
-Change the name of zone A to B
→ The name does not change in the sensor's assignment

Resulting bug:



Erroneous behaviour:

Based on Team 9's SRS: Use Case 3C "Update Safety Zone", scenario 5 states: "The System validates the input and applies the updated configuration. The System displays a confirmation message ('Zone information updated successfully')." This update includes zone Name, which must be propagated wherever the system displays zone-related information.
Furthermore, the Team 9 User Manual specifies under Zone Management that users can "View all sensors and their current zone assignments", meaning the UI must reflect the updated name immediately.

Based on the original Team 3 SRS: the Configure Safety Zone requirement also states that safety zone updates are "saved for system and for sensors," implying consistent propagation to all components that reference the zone.

→ We therefore expect that renaming a safety zone updates its name everywhere, including the sensor–zone assignment list. Yet in the implementation, after renaming zone A to B, the sensor assignment panel continues to display the old name A, meaning the updated configuration is not applied system-wide, violating both SRS and User Manual expectations.

.

Error 3:

Input Sequence:

-Login to the website
-Go to "surveillance"
-Click "Pick a Camera"
-Click "Camera 1"
-Click "Disable"
-Click "Back"
-Click "Pick a Camera"
→There is no way to enable Camera 1 again

Erroneous behaviour:

Based on Team 9's SRS: the Surveillance System Management requirement specifies that users must be able to "Enable/disable individual cameras and view their status in real time." This implies both actions must be available (enable and disable), and that camera status should be manageable through the same UI flow.

Additionally, the Camera Control interface described in the User Manual shows that the user can "Pick a Camera" and then manage its operational state (enable/disable). The manual does not

present disabling as a permanent or irreversible action; therefore, a way to re-enable a camera must be accessible through the same navigation path.

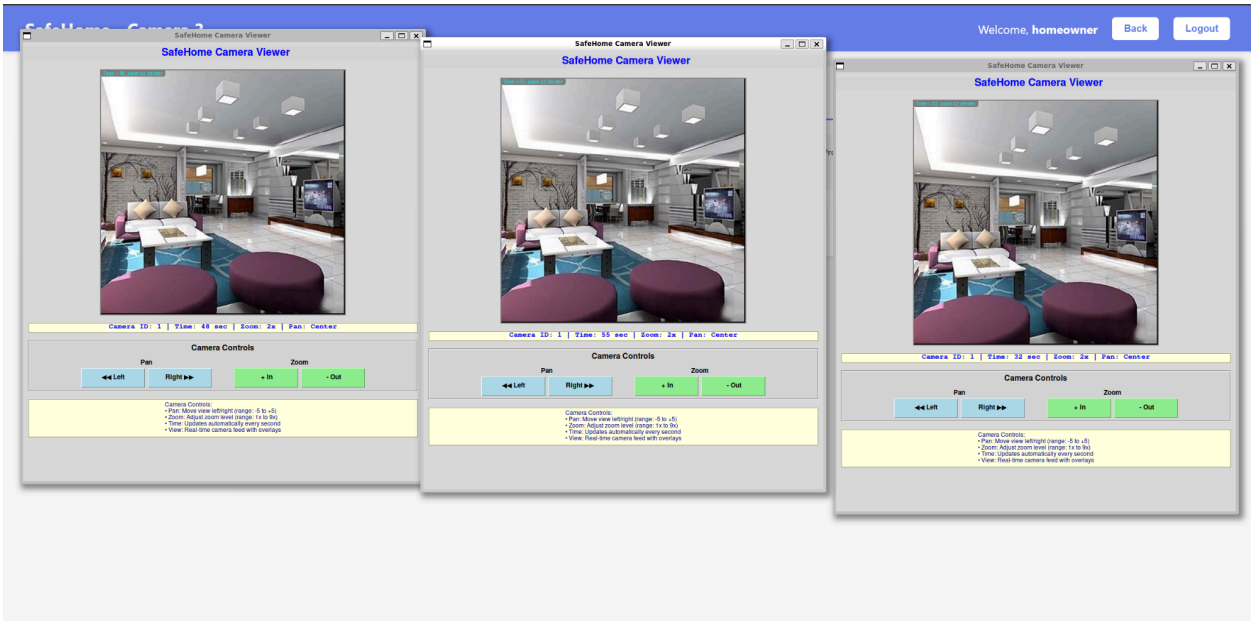
→ There is no option to enable Camera 1 again, meaning the system provides a one-way action (disable) that contradicts the SRS requirement for bidirectional camera control and violates the User Manual's implied functionality.

Error 4:

Input Sequence:

-Login to the website
-Go to "surveillance"
-Click "Pick a Camera"
-Click "Camera 1"
-Click "View"
-Click "Back"
-Click "Pick a Camera"
-Click "Camera 2"
-Click "View"
-Click "Back"
-Click "Pick a Camera"
-Click "Camera 3"
-Click "View"
-Click "Back"
→All 3 "View's" show the same camera feed (the living room)

Resulting bug:



Erroneous behaviour:

Based on Team 9's SRS, Use Cases, 5b "Display Specific camera view" it's established that the system must be able to display the view for a specific camera selected by the user, not a generic or shared view.

In addition, the SRS Surveillance use cases distinguish between "View thumbnail Overview" and "Display Specific camera view", which implies that when the user chooses a particular camera (Camera 1, Camera 2, Camera 3), the system must show that camera's own feed rather than a common default feed.

Based on Team 9's User Manual, in the User Guide → Surveillance Management section, the "How to View Camera" description explains that the user navigates to the Surveillance page, selects a camera, and then the camera feed displays in the main area. This workflow assumes that the feed corresponds to the camera that was selected (for example, Camera 1 vs Camera 2 vs Camera 3).

→ We expect that selecting Camera 1, Camera 2, and Camera 3 and pressing View will display three distinct feeds corresponding to each camera. However, in the implementation, all three View actions (for Camera 1, Camera 2, and Camera 3) display the same feed (the living room).

Error 5:

Input Sequence:

-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
-Click “Set password” and add password X
-Click “Back”
-Click “All Cameras”
→ We can still see the thumbnail of Camera 1 without inputting the password.

Erroneous behaviour:

Based on the original SafeHome SRS, in the Surveillance section under use case View thumbnail Shots (Surveillance use case 3.e), step 4 specifies that the system displays thumbnail snapshots from all cameras except the cameras that have a password. This means that once a password is set on a camera, its thumbnail must not appear in the general thumbnail overview without first satisfying the password requirement.

The corresponding SafeHome SDS swimlane diagram for Surveillance use case View thumbnail Shots also distinguishes between cameras without passwords and cameras that have a password, indicating that password-protected cameras should not appear in the thumbnail grid unless the password condition has been handled.

→ We expect that once Camera 1 is assigned a password, the system should not display its thumbnail in the All Cameras overview unless the password has been entered. However, in the implementation, after setting password X on Camera 1 and returning to the All Cameras screen, the thumbnail of Camera 1 remains fully visible without requiring the password.

Error 6:

Input Sequence:

-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
-Click “Set password” and add password X
-Click “Delete password”
-Click “Set password” and add password Y

→ System says “Old password required“

Erroneous behaviour:

Based on the original SafeHome SRS, the Surveillance use case for managing camera passwords (Surveillance use case 3.c in the old SRS) specifies that the system requests the old password only when a password is already set on the selected camera. If the camera does not currently have a password, the user may set a new password without providing any previous password. This establishes a state-based rule:

-If a password exists → old password is required.
-If no password exists → old password is not required.

In the SafeHome SDS, the corresponding swimlane for camera password management also shows that the system verifies an existing password only when the camera already contains one, indicating that the old password check applies strictly when a stored password must be validated.

After deleting the password from Camera 1, the camera returns to a state where no password exists. Therefore, setting a new password should proceed without any requirement for an old password.

→ However, in the implementation, after removing the password from Camera 1 and attempting to set a new password Y, the system still reports that the old password is required.

Error 6.5:

Input Sequence:

-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
-Click “Set password” and add password X
-Click “Delete password”
→ System says the Camera is password protected (explaining error 6 and any related issue)

Erroneous behaviour:

Based on the original SafeHome SRS, the Surveillance password-management behaviour (Surveillance use case for setting and deleting a camera password in the original SRS) specifies that deleting a camera password returns the camera to an unprotected state. After deletion,

there is no existing password associated with that camera, meaning the system must treat it as a camera with no password. The SRS further describes that password protection applies only when a password is currently set.

In the SafeHome SDS surveillance swimlanes for camera password handling, the logic similarly shows that the system checks for an existing stored password only when a password is actually present. Once the password is deleted, the camera transitions back to the state where password validation should not be triggered.

After removing the password from Camera 1, the camera should no longer be considered password-protected, and the user should be able to assign a new password without encountering errors relating to a previous password state.

→ Yet it is still written in the “Camera Information” that the camera is password protected (Password Protected→Yes)

Error 7:

Input Sequence:

-Login to the control panel as admin
-Click on “Turn Off System” and confirm
-Login to the website
-Click “Arm Away”
-Click “Arm Stay”
→ The website says the system is armed (both for away and stay) yet the system is supposed to be off

Erroneous behaviour:

Based on the original SafeHome SRS, the System Power Management behaviour (System use cases for turning the system on and off in the original SRS) specifies that when the administrator turns the system off from the control panel, the entire security subsystem becomes inactive. In this state, arming functions such as Away or Stay are not available, because the system is not operational. The SRS describes arming and disarming only as actions performed on an active and powered system.

In the SafeHome SDS, the system state model also distinguishes between the powered state and the armed states. The state diagrams indicate that arming transitions (Away, Stay, Disarmed) occur only when the system is in its operational state. When the system is turned off,

the SDS depicts no transition path that allows the system to enter an armed mode from that state.

After turning off the system from the control panel, the system should therefore remain in the off state, and commands issued from the website interface—such as Arm Away or Arm Stay—should not be accepted or should result in an error indicating that the system is offline.

→ However, in the implementation, after turning off the system at the control panel, logging into the website and selecting Arm Away or Arm Stay displays the system as armed, even though the system is supposed to be off.

Error 8:

Input Sequence:

-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
-Click “Set password” and add password X
-Login to the control panel as admin
-Click on “Turn Off System” and confirm
-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
→ It does not ask for a password, ie. the reset of the system also reset the camera password

Erroneous behaviour:

Based on the original SafeHome SRS, in the Surveillance section the use cases Set camera password and Delete camera password define camera passwords as part of the camera’s stored configuration: when a camera has a password, the system must ask for that password before showing the camera state or view, and only an explicit delete operation removes it.

In the same SRS, the common-function use case Turn the system off specifies that, when turning off, the system stops recording camera and saves data before powering down, which implies that configuration data such as camera passwords persist across power cycles and are not reset simply by turning the system off and on.

Team 9’s SDS further refines this by introducing the Live Surveillance feature Protect Sensitive Camera Feed with a Password, which treats password protection as a stable security mechanism for camera feeds rather than a temporary state that disappears on restart.

→ After setting password X on Camera 1 and turning the system off and back on, Camera 1 should still be password protected, and selecting it through “Pick a Camera” should trigger a password prompt. However, in the implementation, after the system restart, selecting Camera 1 no longer asks for a password and the camera behaves as if no password exists.

Error 8.5:

Input Sequence:

-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
-Click “Set password” and add password X
-Login to the control panel as admin
-Click on “Configure”
-Click “System Control”
-Click “Reset Systems” and confirm
-Login to the website
-Go to “surveillance”
-Click “Pick a Camera”
-Click “Camera 1”
→ It does not ask for a password, i.e. the reset of the system also reset the camera password

Erroneous behaviour:

Same exact issue as Error 8, we just get it through Resetting instead of turning Off and On.