# 2. System Requirements and Use Case Models

Given a House Alarm System problem statement, we’ve identified a set of functional and non-functional requirements. Using these requirements, we’ve generated various scenarios to isolate a minimal list of system use cases. The following section of the report details our identified system requirements and the resulting set of use cases.

## 2.1 System Requirements

The following system requirements were identified through analysis of the problem statement.

### 2.1.1 Functional Requirements

* The system must allow the user to enable and disable the House Alarm System.
* The system must allow the user to arm and disarm the House Alarm System.
* The system must sound alarm upon detection of intrusion.
* The system must place a phone call upon failure of break-in invalidation.
* The system must provide an interface to facilitate multi digit password entry.
* The system must prompt for password to perform Disable, Arm and Disarm actions.
* The system must allow the user to invalidate a break.
* The system must perform self tests on sensors and alarms.

### 2.1.2 Non-functional Requirements

* The system shall be verbose.
* The system’s configuration shall be stored in persistent memory.
  + The system shall be configurable for variable number of sensors and alarms.
  + The system’s emergency contact number shall be configurable.
* The system shall contain an internal alarm.
* The system’s events shall be recorded to a log.
* The system shall be compatible with various types of sensors.

The following requirements have been assumed during system implementation:

### 2.1.3 Assumed non-functional Requirements

* The system password is 4 numeric characters, 0-9.
* The system break-in invalidation timeout is 5 seconds.
* The system will sound the alarm indefinitely, until disarmed.
* The system may not be disabled until it is disarmed.
* The system will respond to the failure of a self test as it would to detection of intrusion.

## 2.1 Use Case Model

We’ve identified the following set of use cases to satisfy the requirements defined in section 2.1 System Requirements: Arm System, Disarm System, Enable System, Disable System, Run Self Test, Enter Password, Notify Break-In, Invalidate Break-In and Handle Break-In.

### 2.2.1 Use Case Diagram

The House Alarm System has 6 system actors: The Keypad, Phone Line, Timer, Alarm and Sensor, and the Display, which outputs messages to the user. Figure 1 is a Use Case Diagram which representations the relationships between the 6 actors and our system use cases.

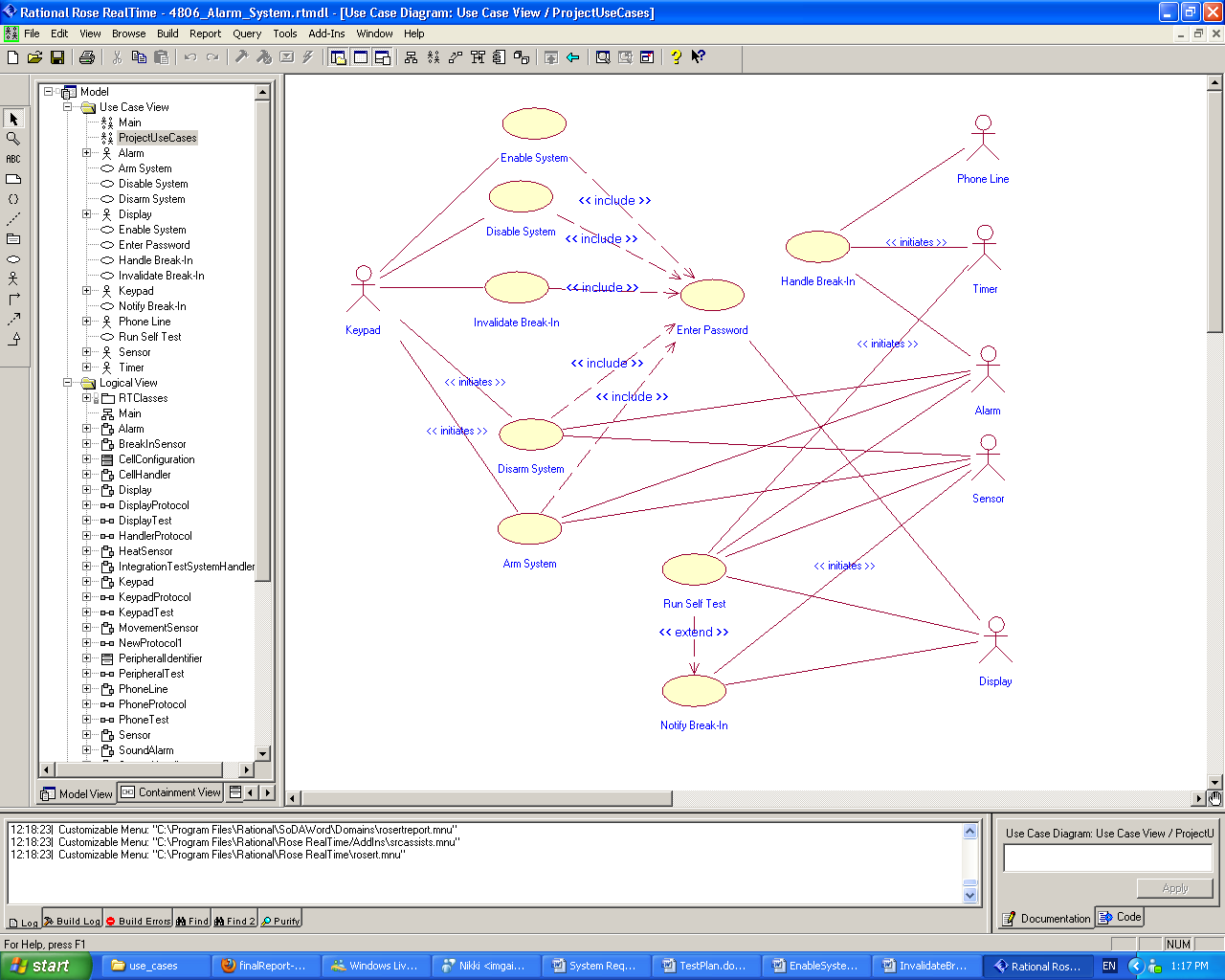


Figure : Home Alarm System Use Case Diagram

## 2.3 Use Case Descriptions

The following section is a collection of summaries of each identified use case. A formal Use Case description for each use case is available in Appendix A.

### 2.3.1 Arm System

The user uses the keypad interface to send the arm signal to the system. Password verification is needed for this function. The system must be enabled and must be disarmed.

The following is the expected flow of events:

1. The arm system button on the keypad is pressed.
2. The system requests a password from the user.
3. The system validates that the password is correct.
4. The system sends an arming signal to all connected sensors.
5. The system sends an arming signal to all connected alarms.

Given these steps, the system should be armed. In the event that the entered password is invalid,

1. System handler sends ‘invalid password’ message to Display.

As a result of incorrect password entry, the user is notified of invalid password and the system is not armed.

### 2.3.1 Disarm System

The user uses the keypad interface to send the disarm signal to the system. Password verification is needed for this function. The system must be enabled and armed.

The following is the expected flow of events:

1. The disarm system button on the keypad is pressed.
2. The system requests a password from the user.
3. The system validates that the password is correct.
4. The system sends disarming signal to all connected cells.
5. The system sends a disarming signal to all connected alarms.

Given these steps, the system should be disarmed. In the event that the entered password is invalid,

1. System handler sends ‘invalid password’ message to Display.

As a result of incorrect password entry, the user is notified of invalid password and the system remains armed.

### 2.3.1 Enable System

The user uses the keypad interface to send the enable signal to the system. Password verification is needed for this function. The system must be disabled.

The following is the expected flow of events:

1. Keypad sends ‘enable alarm system’ signal to the system.
2. The system requests a password from the user.
3. The system validates the entered password is correct.
4. The system is set to ‘alarm system enabled’ state.
5. The system sends an ‘alarm system enabled’ message to Display.

Given these steps, the system should be enabled. In the event that the entered password is invalid,

1. System handler sends ‘invalid password’ message to Display.

As a result of incorrect password entry, the user is notified of invalid password and the system remains disabled.

### 2.3.1 Disable System

The user uses the keypad interface to send the disable signal to the system. Password verification is needed for this function. The system must be enabled and disarmed.

The following is the expected flow of events:

1. Keypad sends ‘disable alarm system’ signal to the system.
2. The system requests a password from the user.
3. The system validates the entered password is correct.
4. The system is set to ‘alarm system disabled state.
5. The system sends an ‘alarm system disabled message to Display.

Given these steps, the system should be disabled. In the event that the entered password is invalid,

1. System handler sends ‘invalid password’ message to Display.

As a result of incorrect password entry, the user is notified of invalid password and the system remains enabled.

### 2.3.1 Run Self Test

A periodic timer triggers a complete self-test of the system. The system sends test signals to all connected alarms and sensors, and triggers a break-in alert if any alarm or sensor fails to respond with a heartbeat signal.

The following is the expected flow of events:

1. The timer sends a signal to the system to initiate the self-test procedure.
2. Until all connected sensors have been tested...
   1. The system sends a self-test signal to a connected sensor.
   2. The system signals the timer to start a new timeout of predefined length.
   3. The sensor performs a self-test routine.
   4. The sensor sends a heartbeat signal to the system to indicate test success.
   5. The system validates that a heartbeat signal is received from the sensor before the timeout expires.
3. Until all connected alarms have been tested...
   1. The system sends a self-test signal to a connected alarm.
   2. The system signals the timer to start a new timeout of predefined length.
   3. The alarm performs a self-test routine.
   4. The alarm sends a heartbeat signal to the system to indicate test success.
   5. The system VALIDATES THAT a heartbeat signal is received from the alarm before the timeout expires.

Given these steps, a heartbeat signal has been received from all connected alarms and sensors and all connected alarms and sensors have performed a self-test routine.

In the event that a test does not receive an alarm or sensor heartbeat within the timeout period,

1. The system logs the current time and identifying information of the sensor that failed to self-test.
2. If the system is armed then activate the break-in process, otherwise display the failure on the display.

As a result of test failure, at least one alarm is identified as faulty or has lost connection to the system.

### 2.3.1 Enter Password

The Display prompts the user to enter password on the Keypad. An action requiring a password must have first been received by the system.

The following is the expected flow of events:

1. The system sends an ‘enter password’ message to Display.
2. The User enters a 4 digit numeric password into Keypad.
3. Keypad sends password message to system.
4. The system sends a signal to clear the Display.

As a result, the password has been entered.

### 2.3.1 Notify Break-In

A break-in signal (or a failed self-test) from a connected sensor causes the system to trigger a break-in notification. The system logs the event, and starts a timeout during which a password can be entered to dismiss the break-in alert. The system must be enabled and armed.

The following is the expected flow of events:

1. A sensor sends a break-in signal to the system (or fails to respond to a self-test signal before the self-test timeout expires)
2. The systems logs the current time and identifying information of the sensor the break-in signal (or test failure) originated from.
3. The system sends a signal to the display to output an indication that a break-in alert has been triggered.
4. The system sends a signal to the display to output the identifying information of the sensor that triggered the alarm.
5. The system sends a signal to the timer to initiate a timeout of predefined length.

As a result, a break-in alert timeout is triggered by the system. In addition, a message is displayed on the system display indicating that a break-in alert has been triggered.

### 2.3.1 Invalidate Break-In

The system waits for a pre-determined interval, during which the owner can enter the password to invalidate the alarm process started by the “break-in” signal. If password received the break-in will be nullified. The system must be enabled and a break-in time must be pending.

The following is the expected flow of events:

1. A sensor sends a break-in signal to the system (or fails to respond to a self-test signal before the self-test timeout expires)
2. The user is prompted for a password.
3. The system validates that password is correct.
4. The system cancels the pending break-in timeout.

Given these steps, the break-in is invalidated and the break-in timeout is no longer pending.

In the event the entered password is invalid, the break-in process resumes.

### 2.3.1 Handle Break-In

The system triggers its own internal sound alarm, broadcasts trigger signals to all cells, causing all alarms in the entire house to be triggered, places a phone call to a pre-defined phone number and finally writes the event to the log. The system must be armed and enabled with a break-in in progress.

The following is the expected flow of events:

1. The timer sends a signal to the system to initiate the handle break-in procedure.
2. The system triggers internal sound alarm.
3. Until all connected alarms are triggered,
   1. The system sends a trigger system to a cell handler.
   2. The cell handler triggers its connected alarms.
4. The system places a phone call through the phone line.
5. The system logs the break in with all the relevant information.

Given these steps, the internal sound alarm and all connected alarms have been triggered, and a phone call has been placed.

In the event that a phone call fails, a phone line failure event is logged.