Test Plan documentation

Contents

[Objective: 1](#_Toc190732965)

[Scope 2](#_Toc190732966)

[Test Approach 2](#_Toc190732967)

[Test Environment 3](#_Toc190732968)

[Test Deliverables 3](#_Toc190732969)

[Schedule 4](#_Toc190732970)

[Risks 4](#_Toc190732971)

# Objective:

The primary objective of the system test plan is to ensure that the **Home Security Embedded System** (based on the VISTA-20P control panel) meets all functional, performance, and reliability requirements as specified by the manufacturer. This includes:

* Verifying all system features (e.g., IP alarm reporting, zone management, partitions, event logging, etc.).
* Ensuring the system operates correctly under normal and edge-case scenarios.
* Validating the system's usability and security.

# Scope

The scope of testing includes:

* **Functional Testing**: Verify all features work as intended.
* **Performance Testing**: Test system responsiveness under various conditions (e.g., high load, low network bandwidth).
* **Security Testing**: Ensure data integrity and secure communication (e.g., IP alarm reporting, user authentication).
* **Usability Testing**: Evaluate the user interface and ease of use (e.g., keypad navigation, event log readability).
* **Compatibility Testing**: Ensure the system works with various hardware and software configurations (e.g., different keypads, sensors, and communicators).

# Test Approach

The testing will be conducted in the following phases:

1. **Functional Testing**:
   * Verify all system features (e.g., IP alarm reporting, zone doubling, partition functionality).
   * Test boundary conditions (e.g., maximum zones, partitions, and users).
2. **Performance Testing**:
   * Test system responsiveness under high load (e.g., multiple alarms triggered simultaneously).
   * Evaluate the system's behavior under low network bandwidth.
3. **Security Testing**:
   * Verify secure communication for IP alarm reporting.
   * Test user authentication and access control.
4. **Usability Testing**:
   * Evaluate the user interface (e.g., keypad navigation, event log readability).
   * Test user scheduling and macro button functionality.
5. **Compatibility Testing**:
   * Test the system with different hardware configurations (e.g., keypads, sensors, communicators).
   * Verify compatibility with various firmware versions.

# Test Environment

The test environment will include:

* **Hardware**:
  + VISTA-20P control panel.
  + Keypads (graphic touchscreen and standard).
  + Sensors (hardwired and wireless).
  + Output devices (lights, alarms, relays).
  + IP communicators (iGSMV4G, 7845i-ENT, GSMV4G, GSMX4G).
* **Software**:
  + Firmware for the VISTA-20P control panel.
  + Configuration tools for setting up zones, partitions, and user codes.
* **Network**:
  + Internet and Intranet connectivity for IP alarm reporting and uploading/downloading.

# Test Deliverables

The following deliverables will be produced during the testing process:

* **Test Cases**: Detailed test cases for all system features.
* **Test Results**: Results of test execution (pass/fail).
* **Defect Reports**: Logs of any defects found during testing.
* **Test Summary Report**: A summary of testing activities, results, and recommendations.

# Schedule

The testing will be conducted over four weeks:

* **Week 1**: Test planning and environment setup.
* **Week 2-3**: Test execution (functional, performance, security, usability, and compatibility testing).
* **Week 4**: Defect retesting and final reporting.

# Risks

Potential risks include:

* **Network Connectivity Issues**: IP alarm reporting may fail due to network problems.
* **Hardware Failures**: Sensors or keypads may malfunction during testing.
* **Incomplete Configurations**: Incorrect system configurations may lead to false test results.