Task 1 – **Consolidated Inspection Defect and Inconsistency List**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Defect # | Location | Defect/inconsistency type | Classification | Author | Status | Date corrected |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |

* To be filled by each of team members separately
* Add as many columns as necessary
* Classification values: Major/Minor
* Status values: Open/Closed
* Defect type values: **Categories:** Opacity, Remorse, Noise, Poor modifiability, forward reference, Overspecification, Poor structuring, Unfeasibility, Unintelligibility
* Type of inconsistency : terminology, designation, structure clash; strong, weak conflict

**INSPECTION SUMMARY REPORT (one per team)**

Project: Smart Home+

General:

Total Number of open defects\_\_\_\_\_\_\_\_\_\_\_

Total Number of open conflicts\_\_\_\_\_\_\_\_\_\_\_

Total Number of close defects\_\_\_\_\_\_\_\_\_\_\_

Total Number of close conflicts\_\_\_\_\_\_\_\_\_\_\_

Summarize number of defects by defect type and conflict type

|  |  |  |
| --- | --- | --- |
| Defect type | Number of open defects | Number of close defects |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Conflict type | Number of open conflicts | Number of close conflicts |
|  |  |  |

Total Person-Hours expended in inspection\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 2 – Documenting conflicts**

Build an interaction matrix (Kotonya & Sommerville, 1997) based on the information generated in task 1

**Task 3 –  Conflict resolution**

Apply operators to transform the conflicting statements (or objects involved in such statements) derived  from task 2.  If necessary, introduce new requirements

**Task 4 –  Conflict evaluation**

Evaluate the conflict counter measures proposed in Task 3, and select the most cost effective ones.

Use Weighted matrices.

**5 Risk Management:**

**1. Identified Risk:** Unauthorized access to any of the installed devices using default password used for connectivity. (NFR: Security)

**Risk Type**: Product Related Risk

**Risk Likelihood** - Low. The attacker needs to possess sufficient technical skill/knowledge to exploit this security loophole.

**Qualitative assessment:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Consequences** | **Likely** | **Possible** | **Unlikely** |
| Loss of security | Catastrophic | Catastrophic | Severe |
| Loss of privacy | Sever | Severe | High |
| Gain access to other devices in network | High | High | Low |
| Use the devices as bots for security attacks | Low | Low | Low |

Rationale:

1. Loss of privacy and security defeats the whole vision of the product and it can result in catastrophic outcomes like break in, burglary, violence etc.
2. Gain access to other devices in the network - A hacker can gain access to other devices in the network and use it inappropriately. Though it’s not catastrophic it will have a high impact on user experience of the system.
3. Use the devices as bots for security attacks - Users may not have any impact on user experience or the impact can be low like high bandwidth usage. In some cases, users may not even be aware of the impact.

**Counter Measure 1:** Controller resets the default password of the smart device with a uniquely generated password as soon as the device is successfully paired with the controller.

**Tactic used: Avoid risk**

**Counter Measure 2:** Display warnings to the user via the mobile app, local monitor or the voice-based assistants that the smart device has the default password and the user needs to reset it. User is given the option to fix it or snooze the warning.

**Tactic used: Reduce risk likelihood**

**2. Identified Risk:** Loss of camera footages or usage pattern data when storage is full (applies to both local and cloud storage) NFR: Performance

**Risk Type**: Product Related Risk

**Risk Likelihood** - Moderate. 1. Users will not be able to view the latest surveillance footage. 2. Improper functioning of the devices in self-evolving mode as it depends on the usage pattern data.

**Qualitative assessment:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Consequences** | **Likely** | **Possible** | **Unlikely** |
| Loss of footages | Severe | High | High |
| Loss of surveillance | Severe | Severe | High |
| Improper function of devices based on outdated usage data | Severe | High | Moderate |
| Low performance of controller in case of retries to store/upload data | Low | Low | Low |

Rationale:

1. Loss of surveillance and footage are deemed severe since the customer will lose the sense of safety and security of the home.
2. If the device evolves on outdated usage data, the actual output can severely affect the user experience.
3. In some cases, multiple retries by the controller to store/update data can affect performance.

**Counter Measure 1:** Clear the storage when it reaches a specified threshold in the order of earliest data first until the available storage comes below the threshold.

**Tactic used: Avoid risk**

**Counter Measure 2:** Display warning to the user that storage is full, and they need to clear it or it will result in loss of data.

**Tactic used: Reduce risk likelihood**

**Counter Measure 3:** Before applying modifications to the device based on the usage pattern in self-evolving mode check if the data used include the latest hour data.

**Tactic used: Reduce risk consequence likelihood**

**APPENDIX:**

Project: **Smart Home+** Inspector: **Apoorv Semwal**

Time spent by Inspector :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Defect # | Location | Defect/inconsistency type | Classification | Author | Status | Date corrected |
| 1 | Product Perspective – Usage of term IOT without providing any prior explanation /reference to it. | Forward Reference | Minor |  | Open |  |
| 2 | Needs and Features – Security Measures - Home Alarms – Stating just a device name is not enough to define it as a feature and its purpose. | Unintelligibility | Major |  | Open |  |
| 3 | Needs and Features – User Mode of Operation – In Multi User Mode User 1 sends cmd to lower room temperature using AC while User2 sends cmd to open the windows on a sunny day. | Strong Conflict | Major |  | Open |  |
| 4 | Needs and Features – Emergency Detection System detects a fire emergency and User Sends command to close windows and doors. | Strong Conflict | Major |  | Open |  |
| 5 | Security Measures - System should automatically locks all point of entries when an intrusion happens and user trying to unlock a point of entry at the same time. | Strong Conflict | Major |  | Open |  |
| 6 | Energy Management - System detects it is raining and did not start daily evening garden water sprinklers but Users try to send commands to open Garden Water Sprinklers. | Strong Conflict | Minor |  | Open |  |

Time spent by Inspector :60 minutes Inspector: **Divya Bhagavathiappan Shiva**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Defect # | Location | Defect/inconsistency type | Classification | Author | Status | Date corrected |
| 1 | Assumptions:  Controller and the smart devices both provide support for connectivity using Wi-Fi/Bluetooth | Poor Structuring  Assumption does not differentiate local and remote connectivity | Minor | Divya | Open |  |
| 2 | Security Measures:  Home Alarm and Intrusion detection | Overlapping - Home Alarm is triggered when intrusion is detected | Minor |  | Open |  |
| 3 | Emergency Detection | Incomplete - Does not provide insight on how to notify emergencies | Major |  | open |  |
| 4 | Automation of the Lightning of the room and Automated window blinds | Strong Conflict - Lighting in a room can be affected by natural light | Minor |  | open |  |
| 5 | Emergency notification | Omission - Emergency notifications should also be displayed in local monitors and through voice based assistants | Major |  | open |  |
| 6 | Storage | Overlapping - Local and cloud storage | Minor |  | open |  |
| 7 | Routine Activities | Overlapping - Kitchen and medicine inventory management | Minor |  | open |  |
| 8 | Emergency Notification & Safety measures | Weak Conflict - Automated calls should not happen if the customer takes responsibility for the emergency notification event. | Minor |  | open |  |

**Automation of the Lightning of the room and Automated window blinds**

Conflict Resolution

1. Close the window blinds before adjusting the lightning of the system in self evolving mode. (Tactic used - Restore conflicting statements)
2. When the user tries to control light send and if the blinds are open popup a notification regarding the state of the blinds and expected action. (Tactic used - Weaken conflicting statements)

Conflict Evaluation:

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation criteria NFR** | **Significance weighting** | **Close Blinds** | **Send notifications** |
| Reliable outcome | 0.7 |  |  |
| Usability | 0.3 |  |  |
| **Total** | **1.0** |  |  |

**Emergency Notification & Safety measures**

Conflict Resolution

1. In case of emergency, trigger alarms and send notifications to customers, if the alarm was not cancelled within a specific time by the user dispatch 911 (Tactic used - Weaken conflicting statements.)

2. The controller will operate in two states armed (full protections) and disarmed (minimal protection). Automated calls to 911 will occur only during armed state (Tactic used - Avoid boundary condition)

Conflict Evaluation:

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation criteria NFR** | **Significance weighting** | **Armed State** | **Time given to cancel alarms** |
| Reliability | 0.5 |  |  |
| Usability | 0.3 |  |  |
| Minimal inconvenience | 0.2 |  |  |
| **Total** | **1.0** |  |  |