Concordia University

Department of Computer Science and Software Engineering

SOEN 6481: Software Systems Requirements Specification

Instructor: Dr. Rodrigo Morales
Summer 2020
Team 18

Requirements Evaluation and Risk Analysis

Smart Home + System

Team Member	Student ID
Tushar Jain	**40094872**
Neda Kalantari	**40150261**
Qing Li	**40082701**
Mohammad Alidadi	**40077244**
Neelofer Shama	**40121559**

GitHub Repository: https://github.com/M-Alidadi/Team18

TASK 1 - Inspection Defect And Inconsistency List

1. **Project: SmartHome+**
   Inspector: Tushar Jain
   Time spent by Inspector: 3 Hours

Defect #	Location	Defect/inconsistency type	Defect/Inconsistency Description	Classification	Author	Status	Date corrected
1	VD Section 3.2	Terminology	-System Platform -Ecosystem Used in the same section	Minor	Qing Li	Closed	July 12
2	Requirements Elicitation Question 1	Noise	A stakeholder is of shorter height	Minor	End User	Closed	July 11
3	Requirements Elicitation Question 5	Infeasibility	All biometric inputs needed	Major	End User	Open	
4	VD Section 4.2	Inadequacy	Integration Issues	Minor	Neelofer Shama	Open	

2. **Project: SmartHome+**
   Inspector: Mohammad Alidadi
   Time spent by Inspector: 2.5 Hours

Defect #	Location	Defect/inconsistency type	Classification	Author	Status	Date corrected	Description
1	Vision document- Throughout the vision document	Terminology	minor	Team 18	closed	July 12	Throughout the vision document homeowner and family members are called with different names such as owner, homeowner, family, family and pets, stakeholder, user, end user.
2	Vision document 4.3 Needs and Features	Omission	major	Neda	open		There is a missing requirement that enables homeowners and family members to manually use some features such as activating security alarms.
3	Vision document 4.3 Needs and Features 5 Other Product Requirements	Weak conflict	minor	Neda Mohammad	open		There is a requirement that says priority is fingerprint followed by facial recognition or simple pin keypad whichever is more secure. But in the vision document it is mentioned differently.
4	Vision document 4.3 Needs and Features Accessibility section	Omission	major	Neda	open		In terms of accessibility there is a missing feature. As the user requires us, the system should provide accessibility for people with weak eyesight. The requirement from the user is: I am free to use any ecosystem. Smartphones, tablets, office and personal laptops, televisions, etc.

3. **Project: SmartHome+**
   Inspector: Neda Kalantari
   Time spent by Inspector: 3 Hours

Defect #	Location	Defect/inconsistency type	Description	Classification	Status	Author	Date corrected
1	Vision document 3.2User Environment	Defect: Inadequacy	The system does not adequately explain the needs related to pets and problems that should be solved about them	Major	Open	Qing	
2	Vision document 3.Stakeholder Descriptions	Defect: Inadequacy	It's not clear that Housekeepers, Nannies, and etc access to exactly what services of smart home.	Major	Open	Tushar	
3	Vision document 3.2User Environment	Inconsistency: Weak conflict	Most tasks could be completed by one person, while some users who have less knowledge about computing devices, disabilities and children may need assistance from others when using the SmartHome+ platform at the first time. only as long as that specific person is available less knowledgeable users can work with the system.	Minor	Open	Qing	

4	Questionnaire	Inconsistency: Strong conflict	Cameras should not be installed in rooms/other private areas for the privacy of users. The statement refers to the safety and security of the homeowners and their belongings. How can we keep private rooms secure without installing the Cameras	Major	Open	End-User	

4. **Project: SmartHome+**
   Inspector: Qing Li
   Time spent by Inspector: 2.25 Hours

Defect #	Location	Defect/inconsistency type	Classification	Author	Status	Date corrected	Description
1	VD 4.3 Environmental considerations - Need (2)	Noise	Minor	Neda	Closed	July 12	“Keeping the environment safe and clean” Not provide more information
2	VD 4.3 Automation-Features (5)	Unintelligibility	Minor	Neda	Open		-automatically measure the height Should be human height
3	VD 3.1 User Stakeholders-Responsibilities(2&3)	Designation clash	Major	Tushar	Closed	July 12	-temporary and limited access -temporary access Not specific the word “temporary”
4	VD 4.3 Security and Privacy-Features	Omission	Major	Nede	Open		Not include temporary guest system in the feature

5. **Project: SmartHome+**
   Inspector: Neelofer Shama
   Time spent by Inspector: 2.5 Hours

Defect #	Location	Actual Statement	Defect/inconsistency type	Reason	Classification	Author	Status	Date corrected
1	VD 2.1 Problem Statement	Homeowners, their family members, guests, and maids.	Omission	Missed pets in the affects section	Minor	Mohammad	Open	
2	VD 2.1 Problem Statement & VD 5 Other Product Requirements (Security Constraints)	-The product is equipped with a biometric and facial detection system -Authentication of the user is by facial recognition followed by a password.	Conflict-Weak	We are saying we will use biometrics in one statement and password in another	Minor	Mohammad	Open	
3	VD 3.2 User environment -people and pets involved	motion detectors would not trip when the home alarm system is activated but a pet is still inside.	Inadequacy	There might be a situation where the intruder and the pet are in the same room. How the system will deal with the presence of both intruder and known pet will be handled has not been adequately explained.	Major	End user	Open	

4	VD 3.1 Stakeholders-non essential members	Receives temporary and limited access to home features like one time access key, internal system status , maintenance status etc.	Opacity	Need to elaborate on one time access key-validity? ,time duration, how will it be shared. And internal system status- what details will be given? Who decides / reviews the details in case of any modifications ?	Minor	End User	Open	
5	VD 5 Other Product Requirements-Security constraints	Users can only monitor the system and manually place a medical alert 911 emergency request for an ambulance	Omission	System needs to provide feature of handling medical emergencies	Major	Mohammad	Open	
6	VD 4.3 Needs and Features	homeowner would get a notification for alteration in any of sensors	Omission	Should mention about notifications to users of the system, specially in case of users with disabilities.	Major	Neda	Open	

INSPECTION SUMMARY REPORT

Project: SmartHome+

General:

Total Number of open defects: **13**
Total Number of open conflicts: **4**
Total Number of close defects: **5**
Total Number of close conflicts: **0**

Summarize number of defects by defect type and conflict type

Defect type	Number of open defects	Number of close defects
Noise	0	2
Infeasibility	1	0
Inadequacy	4	0
Omission	6	0
Unintelligibility	1	0
Opacity	1	0
Terminology Clash	0	2
Designation Clash	0	1

Conflict type	Number of open conflicts	Number of close conflicts
Weak Conflict	3	0
Strong Conflict	1	0

Total Person-Hours expended in inspection: **13.2 Hours**

TASK 2 - Documenting Conflicts

Statements

	Statements
S1	RD asks for All of the biometric security systems. Priority is fingerprint followed by facial recognition or simple pin keypad whichever is more secure.
S2	Our system only provides these three with Planned release 1: Fingerprint , Planned release 2: Facial recognition, Planned release 3: Pin keypad(Vision Document).
S3	RD-Cameras should not be installed in rooms/other private areas for privacy of users.
S4	In VD it states that In terms of security, the home is equipped with cameras, door/window sensors, smart locks, motorized blinds.
S5	V Doc-Most tasks could be completed by one person, while some users who have less knowledge about computing devices, disabilities and children may need assistance from others when using the SmartHome+ platform at the first.
S6	RD-Every person should be able to work with the system.
S7	The Vision document says the product is equipped with a biometric and facial detection system.
S8	The Vision documents say authentication of the user is by facial recognition followed by a password.

Interaction Matrix

	S1	S2	S3	S4	S5	S6	S7	S8	**TOTAL**
S1	0	1	0	0	0	0	1000	1000	2001
S2	1	0	0	0	0	0	1000	1000	2001
S3	0	0	0	1	0	0		0	1
S4	0	0	1	0	0	0	0	0	1
S5	0	0	0	0	0	1	0	0	1
S6	0	0	0	0	1	0	0	0	1
S7	1000	1000	0	0	0	0	0	1	2001
S8	1000	1000	0	0	0	0	1	0	2001
TOTAL	2001	2001	1	1	1	1	2001	2001	**8008**

Non -Conflicting Overlaps - 8 || Conflicts - 8

TASK 3 - Conflict Resolution Document

Conflicts

1. **S1-S2**

   S1: RD asks for All of the biometric security systems. Priority is fingerprint followed by facial recognition or simple pin keypad whichever is more secure.

   S2: Our system only provides these three with Planned release 1: Fingerprint , Planned release 2: Facial recognition, Planned release 3: Pin keypad(VD).

   - **Option1:**
     A solution to the conflict between statements 1 and 2 by proposing the operator (Weakening the Conflict) by changing the S2 with our system will initially provide these 3 methods with the provision to add more later based on need.
   - **Option2:**
     Weaken the conflicting statement: I would change the S2 statement to: SmartHome+ provides all biometric security systems 1: Fingerprint, Planned release 2: Facial recognition, Planned release 3: Pin keypad and voice recognition.

2. **S3-S4**

   S3: RD-Cameras should not be installed in rooms/other private areas for the privacy of users.

   S4: VD-In terms of security, the home is equipped with cameras.

   - **Option1:**
     This particular conflict can be resolved using the technique of (identifying the source of conflict and specializing it). So in this particular scenario, the source of conflict is camera installed. So, we can change the S4 to that the home will be equipped with cameras in all rooms except those with privacy concerns. In those areas we can install specialized detectors which will only detect motion once the alarm system will be activated.
   - **Option2:**
     Avoid boundary condition:
     In Vision Document: In terms of security, private areas will be equipped with motion detector sensors and other parts will be equipped with cameras.
   - **Option3:**
     Weaken conflicting statement:
     In Vision Document: In terms of security, The private rooms will not be equipped with cameras unless the owners ask for installing cameras in the private rooms.

- **Option4:**
  Specialize conflict source or target: I would change the S4 to this: -In terms of security, security cameras are installed outside and inside the house except for rooms and private areas, door/window sensors, smart locks, motorized blinds.

3. **S5-S6**

   S5: VD-Most tasks could be completed by one person, while some users who have less knowledge about computing devices, disabilities and children may need assistance from others when using the SmartHome+ platform at the first.

   S6: RD-Every person should be able to work with the system.

   - **Option1:**
     To resolve the conflict in S5 & S6, we can use (Avoid boundary conditions) to rephrase the S5 to All users will be equipped to use and benefit from the system without assistance from others after they have been given a one time training based on their specific needs by appointed professionals.
   - **Option2:**
     Specialize conflict source or target
     Eliminating this conflict by specializing the word “assistance”.
     “Each task is able to be completed by one person, the users who have less knowledge about computing devices and illiteracy could get temporary help from their family members when they read the user manual for the first time.”
   - **Option3:**
     Avoid boundary condition: I would change the S5 to this: The SmartHome+ is designed to be accessible to everyone using the system in the house. The system is specially designed so that people with weak eyesight and short height are able to interact with the system effortlessly. The user interface of the system is designed in a way that anyone can use the system even with the lowest understanding IT domain. The user interface also provides features based on age and level of permission after automatically recognizing them by the facial recognition system. Based on the person recognized by the system the user interface changes accordingly. The company will present a tutorial on-site for the initialization of the system and using the system.

4. **S7-S8**

   S7: The Vision document says the product is equipped with a fingerprint and facial detection system.

   S8: The Vision document says authentication of the user is by facial recognition followed by a password.

   - **Option1:**
     Avoid boundary condition: The Product is equipped with a fingerprint and facial detection along with a pin keypad for two layer security.
   - **Option2:**
     Restore conflicting statements
     Authentication of users is mainly achieved by fingerprint and facial detection, pin keypad is invoked to use for authentication only if the biometric authentication is failed.

TASK 4 - Conflict Evaluation Document

Conflicts

1. **S1-S2**

S1: RD asks for All of the biometric security systems. Priority is fingerprint followed by facial recognition or simple pin keypad whichever is more secure.

S2: Our system only provides these three with Planned release 1: Fingerprint , Planned release 2: Facial recognition, Planned release 3: Pin keypad(VD).

- **Option1:**
  A solution to the conflict between statements 1 and 2 by proposing the operator (Weakening the Conflict) by changing the S2 with our system will initially provide these 3 methods with the provision to add more later based on need.
- **Option2:**
  Weaken the conflicting statement: I would change the S2 statement to: SmartHome+ provides all biometric security systems 1: Fingerprint, Planned release 2: Facial recognition, Planned release 3: Pin keypad and voice recognition.

Evaluation criteria NFR	Significance weighting	Option 1	Option 2
Software Interoperability	**0.1**	0.6	0.3
Maintainability	**0.3**	0.7	0.4
Cost	**0.2**	0.7	0.3
Security	**0.4**	0.4	0.7
Total	**1.0**	**0.57**	**0.49**

2. **S3-S4**

S3: RD-Cameras should not be installed in rooms/other private areas for the privacy of users.

S4: VD-In terms of security, the home is equipped with cameras.

- **Option1:**
  This particular conflict can be resolved using the technique of (identifying the source of conflict and specializing it). So in this particular scenario, the source of conflict is the camera installed. So, we can change the S4 to that the home will be equipped with cameras in all rooms except those with privacy concerns. In those areas, we can install specialized detectors which will only detect motion once the alarm system will be activated.
- **Option2:**
  Avoid boundary condition:
  In Vision Document: In terms of security, private areas will be equipped with motion detector sensors and other parts will be equipped with cameras.
- **Option3:**
  Weaken conflicting statement:
  In Vision Document: In terms of security, The private rooms will not be equipped with cameras unless the owners ask for installing cameras in the private rooms.
- **Option4:**
  Specialize conflict source or target: In terms of security, security cameras are installed outside and inside the house except for rooms and private areas, door/window sensors, smart locks, motorized blinds.

Evaluation criteria NFR	Significance weighting	Option1	Option2	Option3	Option4
Security	**0.4**	0.7	0.6	0.5	0.8
Privacy	**0.4**	0.7	0.6	0.7	0.6
Installation	**0.2**	0.5	0.5	0.7	0.6
Total	**1.0**	**0.66**	**0.62**	**0.62**	**0.68**

3. **S5-S6**

S5: VD-Most tasks could be completed by one person, while some users who have less knowledge about computing devices, disabilities and children may need assistance from others when using the SmartHome+ platform at the first.

S6: RD-Every person should be able to work with the system.

- **Option1:**
  To resolve the conflict in S5 & S6, we can use (Avoid boundary conditions) to rephrase the S5 to All users will be equipped to use and benefit from the system without assistance from others after they have been given a one-time training based on their specific needs by appointed professionals.
- **Option2:**
  Specialize conflict source or target
  Eliminating this conflict by specializing the word “assistance”.
  “Each task is able to be completed by one person, the users who have less knowledge about computing devices and illiteracy could get temporary help from their family members when they read the user manual for the first time.”
- **Option3:**
  The user interface of the system is designed in a way that anyone can use the system even with the lowest understanding IT domain. The user interface also provides features based on age and level of permission after automatically recognizing them by the facial recognition system. Based on the person recognized by the system the user interface changes accordingly. The company will present a tutorial on-site for the initialization of the system and using the system.

Evaluation criteria NFR	Significance weighting	Option 1	Option 2	Option3
User Interaction	**0.5**	0.6	0.4	0.9
Development Cost	**0.2**	0.6	0.6	0.3
Performance Cost	**0.3**	0.5	0.5	0.4
Total	**1.0**	**0.57**	**0.47**	**0.63**

4. **S7-S8**

   S7: The Vision document says the product is equipped with a fingerprint and facial detection system.

   S8: The Vision document says authentication of the user is by facial recognition followed by a password.

   - **Option1:**
     Avoid boundary condition: The Product is equipped with a fingerprint and facial detection along with a pin keypad for two-layer security.
   - **Option2:**
     Restore conflicting statements
     Authentication of users is mainly achieved by fingerprint and facial detection, pin keypad is invoked to use for authentication only if the biometric authentication is failed.

Evaluation criteria NFR	Significance weighting	Option1	Option2
Installation	**0.3**	0.6	0.6
Integrity	**0.4**	0.4	0.4
Convenience	**0.3**	0.5	0.8
Total	**1.0**	**0.49**	**0.58**

TASK 5 - Risk Management Document

A. We identify the risks using brainstorming activity and we list down all the risks that most affect the system and their impact on it.

#	Risk Identified	Impact Category	Impact	Priority
1	Some smart devices may store sensitive information about the users like banking information which could be compromised.	Privacy	In most cases end users provide all banking and vendor information, giving the device unlimited access. If someone hacks the system homeowner will probably face expensive consequences.	High
2	Malfunction in sensors.	Reliability	A malfunction could turn on the oven and cause a house fire while the users are away from home. Also, sensors like smoke detectors, carbon dioxide detectors etc. can also lead to catastrophic incidents. The system will change the temperature based on incorrect readings of faulty sensors.	High
3	The devices we integrate, increase the risk of intrusion from unwanted parties.	Security	It could serve as an entry point to access the SmartHome network. Hackers take control of devices such as cameras, smart locks.	High
4	Tricking the Facial biometric system by photos of homeowners.	Security /privacy	It could give unlimited access to the home and smarthome system to the intruders.	High
5	Risk of leaking biometric information that is stored on cloud servers.	Security and privacy	The risk of leaking information such as fingerprint, facial and other sensitive data.	High
6	Internet and Power Failure	Robustness /availability	Since the whole system is built on the infrastructure of the internet, disconnection would lead to the whole system stop working.	High
7	False fire alarm is invoked in case of no fire but smoke from various day to day activities, which also affects other systems like the ventilation.	Accuracy /Reliability	It would force the users to call emergency services while vacating the house and cause a lot of trouble frequently.	Medium
8	Biometric identification failure when people wear masks, gloves, sunglasses etc.	Accuracy	The users won't be able to access some key features of the home like access to the house.	High
9	There are risks associated with the system's performance.	Performanc e	The system would not perform well if it faces unexpected conditions. This could happen because of outside elements like power outage or network down etc.	Medium

10	New and experimental services and devices used in the system integration.	Reliability	The System would incorporate the use of many new and experimental technologies. These may or maynot have been tested well enough and might be prone to attacks and privacy intrusion.	Medium

B. Now we use Qualitative Assessment to assess these risks in terms of consequences and their likelihoods.

 # RISK ASSESSMENT

A. Risk Likelihood Rationale

Likelihood	Rationale
Likely	Having a high probability of occurring or being true.
Possible	Being something that may or may not occur.
Unlikely	Having an extremely low probability of occurring or being true.

B. Consequence Severity Rationale

Severity	Rationale
Catastrophic	Consequence that has the potential to greatly impact project cost, project schedule or performance.
High	Consequence that has the potential to highly impact project cost, project schedule or performance.
Moderate	Consequence that has the potential to slightly impact project cost, project schedule or performance.
Low	COnsequence that has relatively little impact on cost, schedule or performance.

Risk number 1: Some smart devices may store sensitive information about the users like banking information which could be compromised.

Consequences	Likely	Possible	Unlikely
Fraud by using homeowner credit card	Catastrophic	Catastrophic	High
Stealing bank account information	Catastrophic	High	High
Company reputation will be damaged	High	High	Low
Loss of money	High	Moderate	Low

Risk number 2: Malfunction in sensors.

Consequences	Likely	Possible	Unlikely
Water and air quality control malfunction	High	High	Moderate
Air Conditioning system malfunction	High	Moderate	Low
Possibility of theft if window or door sensor do not work properly	Moderate	Moderate	Low

Risk number 3: The devices we integrate, increase the risk of intrusion from unwanted parties.

Consequences	Likely	Possible	Unlikely
Serious injuries	Catastrophic	High	Moderate
Criminals are able to see the house	High	High	Moderate
Property damage	High	Moderate	Moderate
Stealing valuable items	High	Moderate	low

Risk number 4: Tricking the Facial biometric system by photos of homeowners.

Consequences	Likely	Possible	Unlikely
Serious injuries	Catastrophic	High	Moderate
Home intrusion	High	High	Moderate
Financial loss	High	High	Moderate
Property damage	High	Moderate	Low

Risk number 5: Risk of leaking biometric information that is stored on cloud servers.(Neelofer)

Consequences	Likely	Possible	Unlikely
Loss of confidentiality	Catastrophic	High	Moderate
customer dissatisfaction	High	High	Moderate
Data Breach Lawsuit	High	High	Low
Unauthorised access to users to devices, bank accounts	High	Moderate	Low

Risk number 6: Internet and Power Failure

Consequences	Likely	Possible	Unlikely
User loses the ability to control the house feature when he/she is away	Catastrophic	High	High
Loss of system functionality	Catastrophic	High	High
Possibility of theft	High	High	High
Loss of data	Migh	Moderate	Moderate

Risk number 7: False fire alarm is invoked in case of no fire but smoke from various day to day activities, which also affects other systems like the ventilation.

Consequences	Likely	Possible	Unlikely
Unnecessary cost on extinguishment	High	High	Low
Loss of ventilation system functionality	High	High	Low
Catch cold	High	Moderate	Low

Risk number 8: Biometric identification failure when people wear masks, gloves, sunglasses etc

Consequences	Likely	Possible	Unlikely
Users may need to share confidential passwords with secondary users like housekeepers, maintenance guys etc.	High	High	Moderate
It would make the system very unreliable.	High	High	Moderate
Users might not like the smart lock system.	High	Moderate	Low
Users may need to use a pin keypad instead of more secure biometric options.	Moderate	Moderate	Low

Risk number 9: There are risks associated with the system's performance.

Consequences	Likely	Possible	Unlikely
Time critical operations like notifying users about intruders may be delayed	**Catastrophic**	**High**	**High**
Loss of Reliability	**High**	**High**	**Medium**
Lag in system performance.	**Medium**	**Low**	**Low**

Risk number 10: New and experimental services and devices used in the system integration.

Consequences	Likely	Possible	Unlikely
Loss of confidentiality	**Catastrophic**	**High**	**Low**
Loss of system functionality	**Catastrophic**	**Moderate**	**Low**
Loss of customer satisfaction	**High**	**Moderate**	**Low**

C. Now we apply Risk Reduction Tactics to address these risks defined above and evaluate measures if there are more than one option for risk reduction.

Risk #	Risk	Risk Reduction Tactics	Choice Justification
1	**To access sensitive information of the users and any transaction request by user through SmartHome+ system should require user biometric and password**	1. **Reduce risk likelihood:** system requires user to change their passwords in two periods. 2. **Avoid risk consequences:** all the sensitive information which is stored should be encrypted.	**Choice : Tactic 2** Encrypting data seems to be more logical since properly encrypted data is very difficult to decrypt by hackers. In Addition, asking users to change password frequently is not easy to achieve.
2	**Malfunction in sensors.**	1. **Avoid risk** All the sensors should be checked every year by an expert 2. **Reduce risk likelihood:** There should be two sets sensors in each section, so if one fail the other one continue to work	**Choice : Tactic 1** First option is more cost effective since overall cost for this tactic is far less and is paid over year however in option 2 not only is it not possible for all sensors to have a pair-backup sensor but also it is way more expensive than the first option.

3	**The devices we integrate, increase the risk of intrusion from unwanted parties.**	1. **Avoid risk:** A network firewall should be installed to prevent hackers to take control of the devices 2. **Reduce risk likelihood:** system requires user to change their passwords in two periods. 3. **Reduce risk likelihood:** Activate two-factor authentication	**Choice : Tactic 1** Although the cost of the first option seems to be a bit high it is far more effective than other options. Firewalls protect the whole network however other options just solve a part of the risk.
4	**Tricking the Facial biometric system by photos of homeowner**	**Avoid risk** The Facial biometric system should be designed in a way that accepts only live faces.. It means the homeowner must blink or smile to be allowed to login to the system.	**Choice : Tactic 1** We tried to solve the risk of facial authentication by accepting only the alive faces. So no one except the main user can access the smartHome system.
5	**Risk of leaking biometric information that is stored on cloud servers**	1. **Avoid risk;** Access to biometric data storage will be restricted. 2. **Mitigate risk consequences**:the system will encrypt all the data before uploading to the cloud.	**Choice : Tactic 2** Data leakages can happen even after restricting and strengthening access rules. However if the data is encrypted it cannot be used in any form and thus reducing the consequences.
6	**Internet and Power Failure**	1. **Avoid risk consequences** Security features should have a backup battery and be able to work without the internet. 2. **Avoid risk consequences** In case of power outage all windows and doors should be locked using backup battery 3. **Avoid risk consequences** There should generator to generate electricity and back up satellite internet	**Choice : Tactic 1** Although option 3 seems more robust and very great but option one is more cost-effective and would reduce the risk consequence noticeably.
7	**False fire alarm is invoked in**	1. **Avoid risk consequences:** Sending a fire notification to the user's smartphone before	**Choice : Tactic 1** Using cameras to detect fire will involve a lot of development

	case of no fire but smoke from various day to day activities, which also affects other systems like the ventilation.	taking actions on extinguishment. If there is not a fire, the user could choose to clear the fire alarm and take no action. 2. **Avoid risk:** Use surveillance cameras to differentiate smoke from day to day activities and actual fire.	cost. Hence notifying the user and letting him/her stop the alarm is a more suitable and cost effective solution.
8	**Biometric identification failure when people wear masks, gloves, sunglasses etc.**	1. **Reduce Risk Likelihood** Introduce the requirement that the system will prompt the user to remove masks, hats, gloves and glasses before using any biometric system which will help reduce the risk likelihood. 2. **Avoid Risk** We should include the new requirement that the system will adjust the detection algorithm so that the biometric system detects the user input with masks, glasses or gloves.	**Choice : Tactic 1** For this risk we would choose this tactic because it will be very cost effective as it won't need much modifications to the system.
9	**There are risks associated with the system's performance.**	1. **Avoid risk:** Regular maintenance checkups for devices and the system as whole should be conducted.All the required software/hardware updations should be carried out. 2. **Mitigate risk Consequence**: Keep backup features for time critical operations that are reliable and can be handled both manually by users and automatically by system.	**Choice : Tactic 2** The devices might fail even after regular servicing.Having backup features like alternate power supply incase of power outage or switching to cellular data in case disconnectivity in WiFi will ensure the tasks continue to happen and there is no hindrance to system performance.
10	**New and experimental services and devices used in the system integration.**	1. **Avoid risk consequence** For each feature that is related to the new technology user must be able to use them manually. 2. **Avoid risk** Device firmware should be updated regularly.	**Choice : Tactic 2** Option two is more cost-effective and more reliable this way devices are always working properly and as expected.

 # Risk Reduction Tactics using RRL

Risk #	Risk	Risk Reduction Tactics	RRL Justification
1	**To access sensitive information of the users and any transaction request by user through SmartHome+ system should require user biometric and password**	1. **Reduce risk likelihood:** system requires user to change their passwords in two periods. 2. **Avoid risk consequences:** all the sensitive information which is stored should be encrypted.	Risk probability= 25%, Impact= $50000 Option1: Reduced risk to 5%, Cost $10000 RRL2=(0.25*50000-0.05*50000)/10000=1 Option2: Reduced risk to 15%, Cost $400 RRL1=(0.25*50000-0.15*50000)/400= 12.5 RRL1 < RRL2. **Option2 is prefered.**
2	**Malfunction in sensors.**	1. **Avoid risk** All the sensors should be checked every year by an expert 2. **Reduce risk likelihood:** There should be two sets sensors in each section, so if one fail the other one continue to work	Risk probability= 20%, Impact= $52000 Option1: Reduced risk to 5%, Cost $20000 RRL1=(0.20*52000-0.05*52000)/20000=0.39 Option2: Reduced risk to 15%, Cost $10000 RRL2=(0.20*52000-0.15*52000)/10000=0.26 RRL1 > RRL2. **Option1 is prefered.**
3	**The devices we integrate, increase the risk of intrusion from unwanted parties.**	1. **Avoid risk:** A network firewall should be installed to prevent hackers to take control of the devices 2. **Reduce risk likelihood:** system requires user to change their passwords in two periods 3. **Reduce risk likelihood:** Activate two-factor authentication	Risk probability= 10%, Impact= $77000 Option1: Reduced risk to 2%, Cost $12000 RRL1=(0.10*77000-0.02*77000)/12000=0.51 Option2: Reduced risk to 8%, Cost $5500 RRL2=(0.10*77000-0.08*77000)/5500=0.28 Option3: Reduced risk to 5%, Cost $12000 RRL3=(0.10*77000-0.05*77000)/12000=0.32 RRL1 > RRL3 > RRL2. **Option1 is prefered**.

4	**Tricking the Facial biometric system by photos of homeowner**	**Avoid risk** The Facial biometric system should be designed in a way that accepts only live faces.. It means the homeowner must blink or smile to be allowed to login to the system.	Risk probability= 10%, Impact= $17000 Option1: Reduced risk to 6%, Cost $2000 RRL1=(0.1*17000-0.06*17000)/2000=0.34 **Option 1 is prefered.**
5	**Risk of leaking biometric information that is stored on cloud servers**	1. **Avoid risk;** Access to biometric data storage will be restricted. 2. **Mitigate risk consequences**:the system will encrypt all the data before uploading to the cloud.	Risk probability= 15%, Impact= $63000 Option1: Reduced risk to 8%, Cost $700 RRL1=(0.15*63000-0.08*63000)/700=6.3 Option2: Reduced risk to 1%, Cost $400 RRL2=(0.15*63000-0.01*63000)/400=22.05 RRL1 < RRL2. **Option2 is prefered.**
6	**Internet and Power Failure**	1. **Avoid risk consequences** Security features should have a backup battery and be able to work without the internet. 2. **Avoid risk consequences** In case of power outage all windows and doors should be locked using backup battery 3. **Avoid risk consequences** There should generator to generate electricity and back up satellite internet	Risk probability= 15%, Impact= $39000 Option1: Reduced risk to 6%, Cost $900 RRL1=(0.15*39000-0.06*39000)/900=3.9 Option2: Reduced risk to 5%, Cost $10000 RRL2=(0.15*39000-0.05*39000)/10000=0.39 Option3: Reduced risk to 2%, Cost $4000 RRL3=(0.15*39000-0.02*39000)/4000=1.27 RRL1 > RRL3 > RRL2. **Option1 is prefered.**
7	**False fire alarm is invoked in case of no fire but smoke from various day to day activities, which also affects other systems like the ventilation.**	1. **Avoid risk consequences:** Sending a fire notification to the user's smartphone before taking actions on extinguishment. If there is not a fire, the user could choose to clear the fire alarm and take no action. 2. **Avoid risk:**	Risk probability= 26%,Impact= $27000 Option1: Reduced risk to 8%, Cost $2000 RRL1=(0.26*27000-0.08*27000)/2000=2.43 Option2: Reduced risk to 5%, Cost $10000 RRL2=(0.26*27000-0.05*27

		Use surveillance cameras to differentiate smoke from day to day activities and actual fire.	000)/10000=0.51 RRL1 > RRL2. **Option 1 is prefered.**
8	**Biometric identification failure when people wear masks, gloves, sunglasses etc.**	1. **Reduce Risk Likelihood** Introduce the requirement that the system will prompt the user to remove masks, hats, gloves and glasses before using any biometric system which will help reduce the risk likelihood. 2. **Avoid Risk** We should include the new requirement that the system will adjust the detection algorithm so that the biometric system detects the user input with masks, glasses or gloves.	Risk probability= 40%, Impact= $10000 Option1: Reduced risk to 15%, Cost $600 RRL1=(0.4*10000-0.15*10000)/600=4.17 Option2: Reduced risk to 9%, Cost $7400 RRL2=(0.4*10000-0.09*10000)/7400=0.41 RRL1 > RRL2. **Option1 is prefered.**
9	**There are risks associated with the system's performance.**	1. **Avoid risk:** Regular maintenance checkups for devices and the system as whole should be conducted.All the required software/hardware updations should be carried out. 2. **Mitigate risk Consequence**: Keep backup features for time critical operations that are reliable and can be handled both manually by users and automatically by system.	Risk probability= 22%, Impact= $15000 Option1: Reduced risk to 11%, Cost $7000 RRL1=(0.22*15000-0.11*15000)/7000=0.23 Option2: Reduced risk to 7%, Cost $2000 RRL2=(0.22*15000-0.07*15000)/2000=1.125 RRL1 < RRL2. O**ption2 is prefered.**
10	**New and experimental services and devices used in the system integration.**	1. **Avoid risk consequence** For each feature that is related to the new technology user must be able to use them manually. 2. **Avoid risk** Device firmware should be updated regularly.	Risk probability= 26%, Impact= $170000 Option1: Reduced risk to 13%, Cost $200 RRL1=(0.26*17000-0.13*17000)/200=11.05 Option2: Reduced risk to 8%, Cost $14000 RRL2=(0.26*17000-0.08*17000)/14000=0.22 RRL1 > RRL2. **Option1 is prefered.**

 # Summary of RRL

Risk #	RRL1	RRL2	RRL3	Prefered option
1	1	12.5	NA	2
2	0.39	0.26	NA	1
3	0.51	0.28	0.32	1
4	0.34	NA	NA	1
5	6.3	22.05	NA	2
6	3.9	0.39	1.27	1
7	2.43	NA	NA	1
8	4.17	0.41	NA	1
9	0.23	1.125	NA	2
10	0.22	11.05	NA	2

D. Lastly we document in the requirement document risk management process to provide rationale for countermeasure requirements and to support requirements evolution.

Risk Scenario	Risk Impact	Risk Likelihood	New Requirement Introduced	New Feature Added	Risk Impact After New Feature	Risk Likelihood after New Feature	Rationale for New Requirement
To access sensitive information of the users and any transaction request by user through SmartHome+ system should require user biometric and password	High	High	all the sensitive information which is stored should be encrypted.	Sensitive data encryption	Low	Low	Encrypting data seems to be more logical since properly encrypted data is very difficult to decrypt by hackers. In Addition, asking user to change password frequently is not easy to achieve
Malfunction in sensors.	High	Medium	All the sensors should be checked every year by an expert	Regular updates for devices firmware	Low	Medium	First option is more cost effective since overall cost for this tactic is far more less and is paid over year however in option 2 not only is it not possible for all sensors to have a pair-backup sensor but also it is way more expensive than the first option
The devices we integrate, increase the risk of intrusion from unwanted parties.	High	Medium	A network firewall should be installed to prevent hackers to take control of the devices	Firewall protected network	Low	Low	Although the cost of the first option seems to be a bit high it is far more effective than other options. Firewalls protect the whole network however other options just solve a part of the risk

Tricking the Facial biometric system by photos of homeowner	High	Medium	Introduce the requirement that the biometric system only accepts live faces (while blinking or smiling)	System will now ask the user to blink or smile in order to access to the smart Home system	Low	Low	
Risk of leaking biometric information that is stored on cloud servers.	High	High	The system should encrypt all the data before uploading to the cloud	Data encryption	Low	Low	Data leakages can happen even after restricting and strengthening access rules. However if the data is encrypted it cannot be used in any form and thus reducing the consequences.
Internet and Power Failure	Medium	High	Security features should have a backup battery and be able to work without the internet.	Backup battery equipped security features	Low	Mediu m	Although option 3 seems more robust and very great but option one is more cost-effective and would reduce the risk consequence noticeably
False fire alarm is invoked in case of no fire but smoke from various day to day activities, which also affects other systems like the ventilation.	Medium	High	Sending a fire notification to the user's smartphone before taking actions on extinguishment. If there is not a fire, the user could choose to clear the fire alarm and take no action.	Smart notifier	Low	Mediu m	Using cameras to detect fire will involve a lot of development cost. Hence notifying the user and letting him/her stop the alarm is a more suitable and cost effective solution
Biometric identification failure when people wear masks, gloves, sunglasses etc.	Medium	High	Introduce the requirement that the system will prompt the user to remove masks, hats, gloves and glasses before using any biometric system which will help reduce the risk likelihood.	System will now prompt the user to remove any kind of mask, gloves or glasses before using the biometric system.	Low	Mediu m	This new requirement was introduced to: Reduce risk of biometric failure where users might not be able to access the system. This requirement will be cost effective and less time consuming. It will ensure user interaction with the system is well informed and detailed.

There are risks associated with the system's performance.	High	High	Keep backup features for time critical operations that are reliable and can be handled both manually by users and automatically by system.	Automatic and manual feature	Low	Mediu m	Having backup features like alternate power supply incase of power outage or switching to cellular data in case disconnectivity in WiFi will ensure the tasks continue to happen and there is no hindrance to system performance.
New and experimental services and devices used in the system integration.	High	Medium	Device firmware should be updated regularly.	Firmware updates	Low	Low	Option two is more cost-effective and more reliable this way devices are always working properly and as expected

D.1. Task A-C Iterated for New Requirements gathered in Part C.

 # RISK IDENTIFICATION for new Requirements

#	New Requirement	Risk Identified	Impact Category	Impact	Priority
1	All the sensors should be checked every year by an expert.	User do not have the sensors checked for any reason	Reliability	System malfunction. Many of the system features might be affected since they are using a sensor	Medium
2	A network firewall should be installed to prevent hackers to take control of the devices	Hackers might bypass the firewall	Security	Hackers can access to the SmartHome System and information of the user might be leaked	High
3	Introduce the requirement that the biometric system only accepts live faces (while blinking or smiling)	End users cannot stop hackers and cameras of capturing their photos and videos and storing them .	Security/ Privacy	Hackers can access to the SmartHome System	High
4	Sending a fire notification to the user's smartphone before taking actions on extinguishment. If there is not a fire, the user could choose to clear the fire alarm and take no action.	There is a possibility that the user is unable to respond to fire notification in case of an actual fire.	Safety	There may be loss of property or loss of life depending on the severity of fire.	High

5	Introduce the requirement that the system will prompt the user to remove masks, hats, gloves and glasses before using any biometric system which will help reduce the risk likelihood.	The biometric system may not recognise in case there is any kind of bandages on the face or fingers or the user may still wear masks or gloves.	Identity	The user will not be allowed to perform operations that need biometric authentication.	High
6	Device firmware should be updated regularly.	Newer devices firmware may come with newer features that are not compatible with the system.	Accuracy	The system may face integration issues where the devices work well individually but not when combined together	High

 # RISK ASSESSMENT for new Requirements

A. Risk Likelihood Rationale

Likelihood	Rationale
Likely	Having a high probability of occurring or being true.
Possible	Being something that may or may not occur.
Unlikely	Having an extremely low probability of occurring or being true.

B. Consequence Severity Rationale

Severity	Rationale
Catastrophic	Consequence that has the potential to greatly impact project cost, project schedule or performance.
High	Consequence that has the potential to highly impact project cost, project schedule or performance.
Moderate	Consequence that has the potential to slightly impact project cost, project schedule or performance.
Low	COnsequence that has relatively little impact on cost, schedule or performance.

Risk number 1: User do not have the sensors checked for any reason

Consequences	Likely	Possible	Unlikely
Loss of functionality of sensors	**High**	**High**	**High**
Loss of information accuracy detected by sensors	**High**	**High**	**Low**
Loss of customer satisfaction	**Medium**	**Medium**	**Low**

Risk number 2: Hackers might bypass the firewall

Consequences	Likely	Possible	Unlikely
Criminals may have access to the whole system.	Catastrophic	High	Moderate
Stealing valuable information about the users	High	High	Moderate
Devices stop functioning as intended	High	Moderate	Low

Risk number 3: End users cannot stop hackers and cameras from capturing their photos and videos and storing them.

Consequences	Likely	Possible	Unlikely
Home intrusion	High	Moderate	Low
Property damage	High	Low	Low

Risk number 4: There is a possibility that the user is unable to respond to fire notification in case of an actual fire.

Consequences	Likely	Possible	Unlikely
Loss of lives	Catastrophic	High	Moderate
Property damage	High	High	Moderate
Serious Injuries	High	High	Low
Financial loss	High	Moderate	Low

Risk number 5: The biometric system may not recognise in case there is any kind of bandages on the face or fingers or the user may still wear masks or gloves.

Consequences	Likely	Possible	Unlikely
User is not authorized to perform tasks	High	High	Medium
User may be forced to use pin identification	Medium	Low	Low

Risk number 6: Newer devices may come with newer features that are not compatible with the system

Consequences	Likely	Possible	Unlikely
The newer devices may have integration issues with the system.	**High**	**Medium**	**Medium**
Loss of reliability	**High**	**Medium**	**Low**
Lag in system performance	**Medium**	**Medium**	**Low**

 # Risk Reduction Tactics for new Risks associated with new Requirements

Risk #	Risk	Risk Reduction Tactics	Choice Justification
1	User do not have the sensors checked for any reason	**Reduce risk likelihood:** System will send reminders to the homeowner that he/she needs to have the sensors checked otherwise there is no guarantee that security and safety features will be working properly.	This tactic is very cost-effective since it has almost no cost
2	Hackers might bypass the firewall	**Avoid risk consequence:** The password of home internet should be encrypted to prevent hackers even if they bypass the firewall.	An effective and cost-saving measure to resolve the risk.
3	End users cannot stop hackers and cameras of capturing their photos and videos and storing them .	**Avoid Risk** The system must ask the user to do a combination of different gestures in order to access the system. For example smiling and raising his/her eyebrows at the same tim**e**.	An effective tactic to keep the biometric system safe and secure .
4	There is a possibility that the user is unable to respond to fire notification in case of an actual fire.	**Avoid Risk** Cameras should be able to detect fire using live image recognition to identify actual fire.	In case of fire the fire alarm should be activated. If there is no fire then send notification to the user and then invoke fire alarm based on user response.
5	The biometric system may not recognise in case there is any kind of bandages on the face or fingers or the user may still wear masks or gloves.	**Avoid risk:** The system should invoke a fingerprint recognition system for identification when facial recognition is failed three times.	This tactic is effective and financially friendly, because it does not introduce any new features.

6	Newer devices firmware may come with newer features that are not compatible with the system.	**Avoid risk:** all the devices should have rollback update feature that undo changes if they are not compatible with system	This tactic is basically free of charge since it simply goes back to the previous firmware.