SMART HOMES WITH A FOCUS ON PRIVACY AND SECURITY

Safety by Design (2022-1B)

University of Twente

Group #2:

Alex Anguiano Ventura – s2676052
Chiara Vishnudatt – s2688255
Emiel Navis – s2114291
Omar Kahla – s2344572
Niek Monchen – s2187140
Varshalie Paragh – s2628198

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

1. INTRODUCTION

In 2021 the Central Bureau of Statistics listed 23.500 burglaries, which rose by 19% in the first half of 2022 [1]. Meanwhile, utility prices keep rising [2]. This means spending more for homeowners. This study provides a way for homeowners to save up money and be safer.

A smart home incorporates IoT technology and is online. Remote control is possible in a smart home, frequently using a smartphone or other mobile computing device. In a smart house, you may learn and use information about the space and the people living there to enhance their quality of life there [3].

This report will investigate smart houses with a focus on security and privacy. The aspect of security lies in the safety of the homeowner and therefore the house. Furthermore, there is looked at the smart aspect which, in this sense, includes the aspect of energy saving. A short preliminary study has been carried out, before this research, through the safety cube method. This research builds on the previous one and consists of three parts. In the first part the different stakeholders, the system's concept and risks are discussed. Followed by the second part, where the system design and residual safety risks are discussed. Finally, in the third part the operation and end life procedures are discussed. This report ends with a conclusion.

1.1. Goals

The goal of this research is ultimately to provide a secure and reliable system for smart houses. For this, different stakeholders play an important role in the process. Due to the fact that this system is a digital one, several risks lie ahead. The main areas of focus in this study are security and privacy. The security implies the security of the homeowner, the reliability of the data and the storage, user comfort, and reliable connectivity. The privacy aspect implies providing a private system. Furthermore, a sub-function or goal is affordability. However, in this research, the financial aspect is not taken into account.

1.2. Regulations

One of the biggest risks of digitizing systems is the risk of hacking. There are many technical legislations to deal with this occurrence, however, the legislation for this research is kept for essential requirements, thus the needs and safety of the main stakeholders. The scope of these regulations is covered under the ISO 12100 standards for the product safety of the system.

1.3. Challenges

Modern technological growth has both benefits and drawbacks for the creation of connected devices. The tendency would not have been possible without recent advancements. The devices' sensors and actuators are connected to the Internet, and they frequently communicate with each other using the Internet Protocol (IP). For the younger users, the current Millennials and forth, the adoption of technology is not an inhibition. Meanwhile, technology can be challenging.

2. STAKEHOLDERS AND THE SYSTEM DEFINITION

This chapter gives an overview and in-depth explanation on the stakeholders involved in this system. Furthermore, the system concept, its environment, the system (safety) objectives, the risk assessment and acceptance criteria and finally the system functions and requirements are described.

2.1. Stakeholders and their relations

In this section of the report all the stakeholders across the entire life cycle of the Smart House are presented. This section will also illustrate the relationship and importance of the stakeholders between each other, as well as the past and future possible stakeholders.

The main stakeholders related to the Smart House are:

- **End user (Client) –**

This is the client, the person who is in direct relationship with the service provider and the person who owns the home where the system will be installed.

- **Service provider (Smart house company) –**

The service provider is the main entity that owns and controls the system. They oversee designing, schedule maintenance, and provide updates to the system to deliver client's satisfaction.

- **Network provider (Internet service) –**

The network provider is the internet provider which who has a direct relationship with the owner (client) and must be considering by the service provider for the design of the system.

- **Cloud storage provider (data management service) –**

The data manager will provide cloud support to the service provider to store all the data generated by the system and the devices within the system. This will help to organize and manage the data generated by the client's smart home for later feedback.

- **Device manufacturer (Supplier of necessary hardware) –**

The device manufacturer is a simplification of all the direct and indirect suppliers of the hardware needed by the service provider team. The device manufacturer has an important and close relationship with the service provider, and it is involved from the design phase to the maintenance phase.

- **Neighbors (Community around the house) –**

The neighbors are considered not to be important stakeholders due to the low interest in the project, but they can threaten the client with complaints due to privacy concerns due to a lack of information on how the system works and because of the feeling of being watched due to the necessary hardware on the outside of the property.

- **Construction company (Architect) –**

This stakeholder is considered only in the case in which the client does not own a property to build a smart house and needs the construction company to build a home. The contractor would have to include the service provider during the design phase to ease the system installation and early adapt all the requirements needed to fulfil the client's wishes.

- **Regulators (Government) –**

Since there are permits needed, the government is considered as a main stakeholder. It will regulate the service provider (as well as the construction company and other service providers) and help maintain safe the integrity of the client.

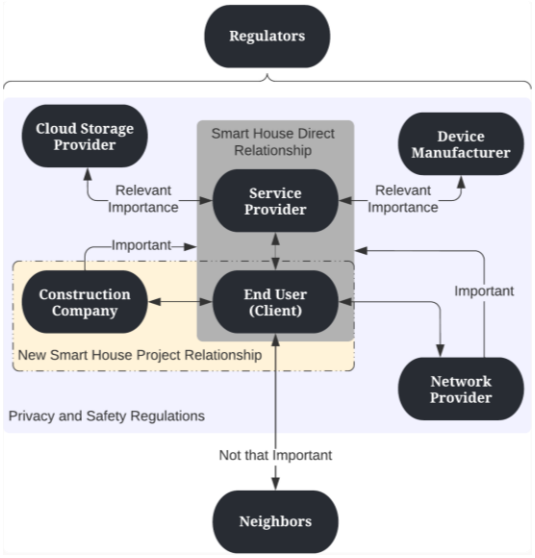


Figure 1 Smart House Stakeholders relationships

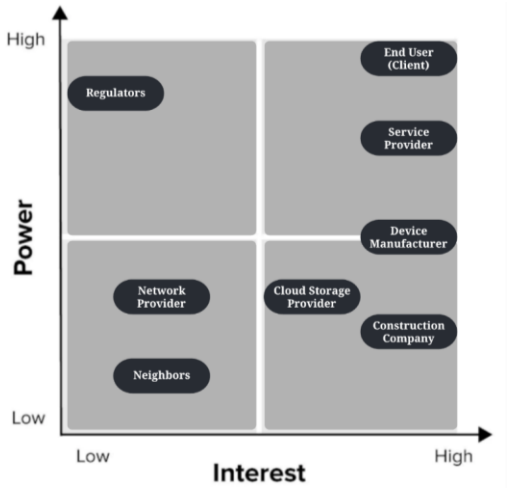


Figure 2 Power - Interest Matrix (Importance)

The future stakeholders are the ones involved in the years to come, they will be involved in one or many phases during the life cycle of the system. Some of the future stakeholders could be:

- **New service providers –**

This new service providers could not only be a competition of the smart house concept but also provide interoperability collaboration for better safety and privacy, making the market more competitive and the product more attractive to end users.

- **New maintenance companies –**

This could be an external stakeholder, now separating the main service provider with his previous role of maintainer. Due to competition and interoperability, in the near future many companies will provide maintenance with a better price.

Regarding the topic of the past stakeholders, they would have been the past providers, as an example, the internet provider will deliver a firewall protection for the personal devices of the client while they are connected to the network. Another provider could have been a webcam security provider (smaller-scale system), which would have provided data protection for the client.

2.2. System concept and its environment

The system is a smart system that provides security and privacy for homeowners. Therefore, the environment of study for this system consists of the smart system, its sub-systems and the different stakeholders as defined in chapter 2.1 (such as the end user, the device manufacturer, and the data communication system).

Within the system concept, the subsystem consists of three main areas, namely the operation infrastructure, the operation management, and the operation strategy. These areas each provide the hardware, the human interfaces, and other components (the non-physical or conceptual components). Furthermore, future phases for this system are taken into consideration, such as maintenance and regulations.

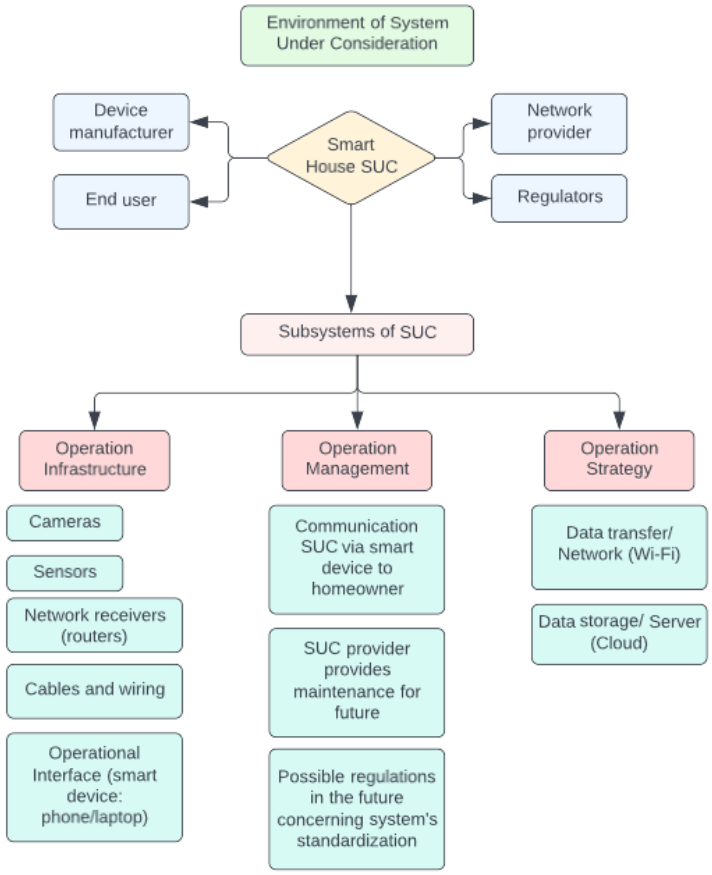


Figure 3 System Concept and Environment

As seen in Figure 3 System Concept and Environment the operation management area refers to future phase in the life cycle of the system, namely maintenance. It is important, with technological innovations, to stay one step ahead, therefore providing security and privacy within this system against hacking. The maintenance in this area thus entails hardware maintenance as well as software (updates). A graphical or visual explanation of the system is given in Figure 4 Visual representation of the system.

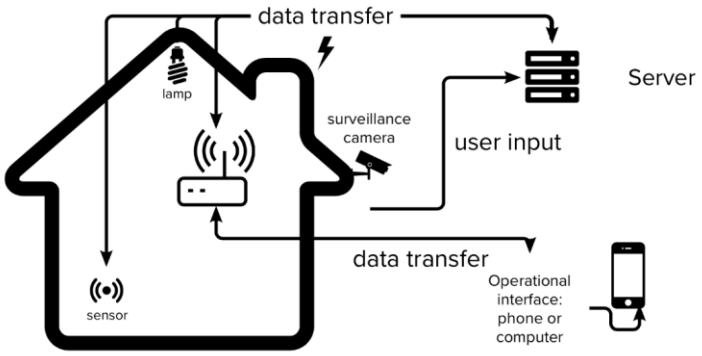


Figure 4 Visual representation of the system

This system under consideration is not one to be updated and that has existed throughout decades. However, forms of this system have existed, such as camera security, and window and door sensor security. These have always been connected to a smart device and a security company but haven't been smart. Therefore, these can be considered as past comparable systems. A possible future system can be an advanced version of this system that solely works on biometrics and has a higher energy-saving system in combination with solar energy. This futuristic system can be considered of higher financial issue.

2.3. System (safety) objectives

For the system under consideration to function optimally, certain objectives are stated. These are primarily safety objectives. As stated in the first chapter, the goal is to provide a secure and reliable system for smart houses that focuses on security and privacy. For these to be implemented, one first has to define safety. According to the Oxford dictionary safe defines as "*protected from or not exposed to danger or risk; not likely to be harmed or lost*", therefore this system incorporates risks. These risks are regulated by the EU legislation.

The Treaties that initially founded the European Economic Community (EEC) and later updated and changed its constitution make up the EU's primary legislation. Secondary legislation is developed under the power of the Treaties, which conclude regulations, directives, decisions, and recommendations and opinions [4].

These regulations and legislations are bounded to the goals. The goals are stated in a broad sense. To define these, a problem tree and an objective tree are created. The problem tree states the challenges to deal with when creating the SUC, whereas the objective tree deals with handling these challenges and therefore states the safety goals.

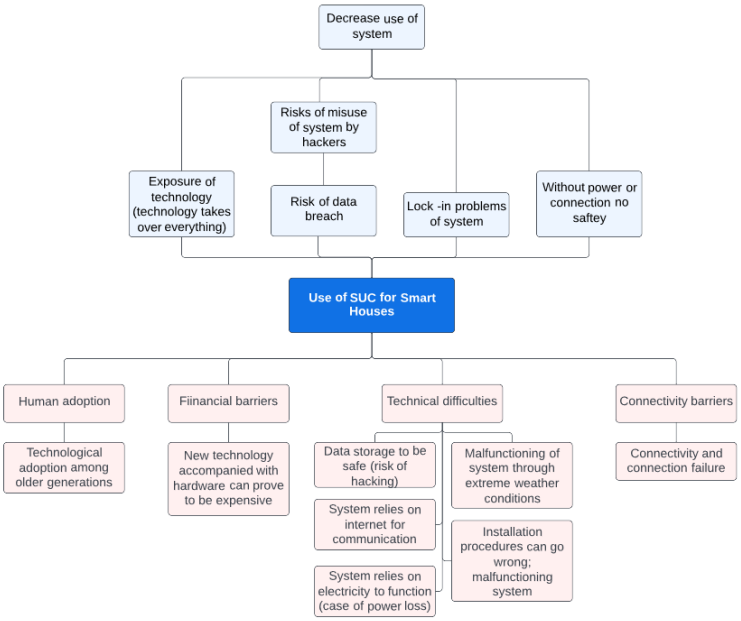


Figure 5 Problem tree

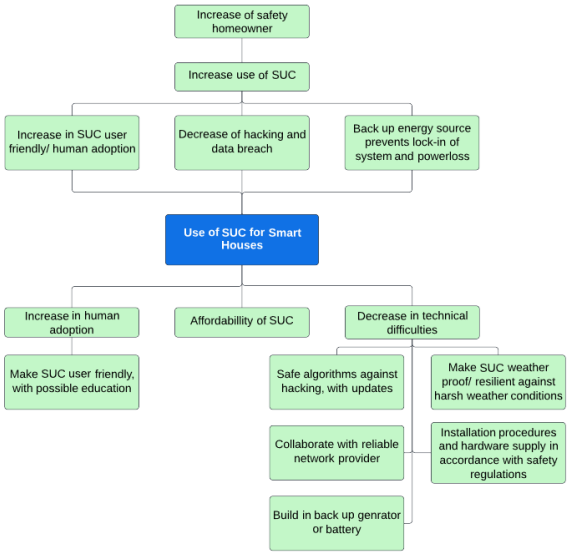


Figure 6 Objective tree

Having looked at the safety goals for the system under consideration through first a problem tree and then an objective tree, the legislation for these have become clear. The legislation (directives and standards) is bound to these goals.

Several different legal acts are used to accomplish the objectives outlined in the EU treaties. Others are not, while some are binding. Some only apply to a select few EU nations, while others are applicable to everyone. **Regulations** take effect on a specific date in each Member State and are legally obligatory throughout the Union. Although **directives** specify the outcomes that must be attained, each Member State is allowed to choose how to incorporate directives into its own national laws. **Decisions** are special EU regulations that are addressed to one or more Member States, corporations, or private individuals. They have legal effect for the people they are intended for [5].

The figure below provides a chart in which is stated what legislation applies to the system for smart houses providing security and privacy.

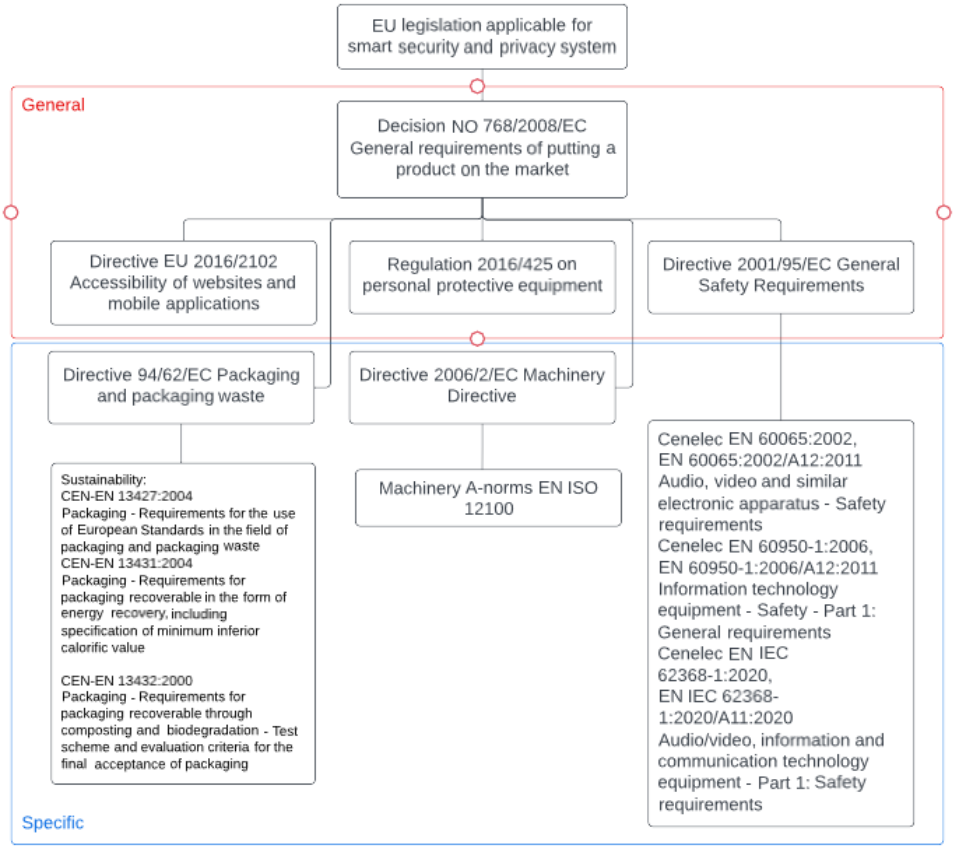


Figure 7 Legislation Chart

2.4. Risk assessment and acceptance criteria

For the smart house, the following risk were detected within the entire life cycle of the project:

1) **Users insufficient use of smart system due to lack of instructions before use phase:** This risk talks about the previous knowledge of the user of the digital system or lack of training before using the system.
2) **Loss of power:** Due to a cut in the public powerline.
3) **Loss of internet connection:** Due to a 3rd party provider or weather conditions.
4) **Connectivity problems within the system and the hardware:** Service provider bug issues with the software.
5) **Compromise of client's privacy:** Due to poor safety performance of the service provider.
6) **Hacking:** Low safety firewall of the service provider system.
7) **House adaptability/incompatible with the system:** This risk talks about the incompatibility of the property to use the service provider's system.
8) **Risk of fire due to bad installation/connection:** Poor installation or unacceptable maintenance.
9) **Restrictive ability to use the house without connectivity:** Due to bugs in the software or limitations of the system.
10) **Third-Party Flaws (service providers mistakes):** Any issues that could produce discomfort in the user experience excluding the main service provider services.
11) **A not user-friendly system for the clients:** Due to poor system design by the service provider.
12) **A "lock in" risk:** This risk talks about a situation where the client gets stuck in a room due to a system error or breakdown, and the client is unable to perform a basic function of the house.
13) **Extreme weather conditions can influence the hardware of the system:** Weather conditions might inflict damage to the performance of the system.
14) **Risk of theft of outside hardware:** Someone stealing a piece of hardware compromising the system performance.

On the following matrix all the previous listed risks are allocated regarding their probability and severity levels.

Commented [OK1]: What do you mean here?

Commented [AVA(SMC2R1]: A bad internet connection (by a 3rd party provider), energy loss (3rd party provider)

Commented [AVA(SMC3]: A "lock in" risk, that you get locked in a room without possibilities to exit or enter

Commented [OK4]: What do you mean here?

Commented [AVA(SMC5]: A "lock in" risk, that you get locked in a room without possibilities to exit or enter

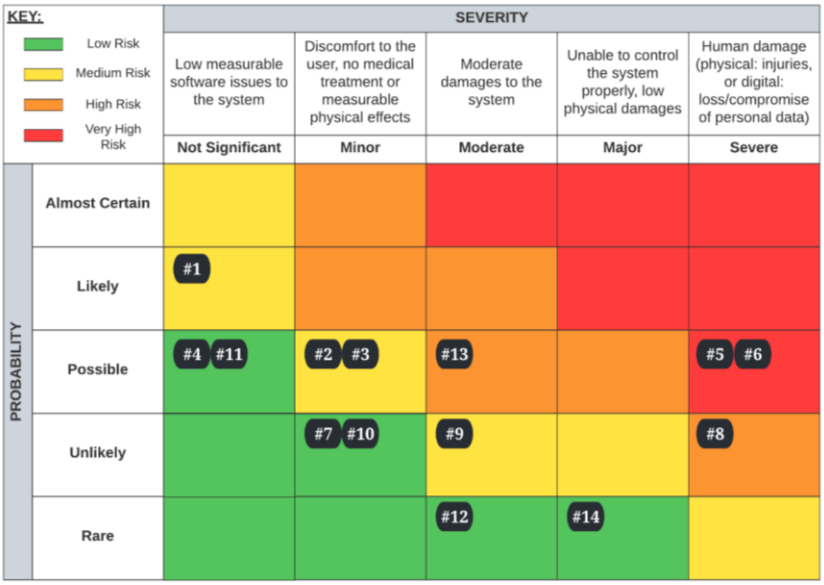


Figure 8 Hazard-event risk matrix

2.5. System functions and requirements

The primary **critical functions** of the system are listed below:

- **Connection with the server:** A stable connection within the internet provider, the user system, and the service provider database.
- **Storage data:** A database where all the user's data is collected, organized, and stored for later system updates.
- **Data security / Data sharing:** A safeguard system that prevents data leakage but provides secure data transferring between the client and the service provider.
- **Stable connection to the remote-control device:** Limited connectivity issues within the user's devices and the main system.
- **Identity check:** System identity check to connect with the main system.

For the previous main functions to be achieved, a list of **requirements** is presented:

- **Physical power switch:** To prevent a "lock in" risk and to prevent the system to shut down if hacked.
- **Users training:** To better use the system and connect to it. Take full advantage of the system.
- **System updates:** To provide safer and faster data sharing.
- **Data room (House room/space for data storage and maintenance, control panel):** To store and control the main system.
- **Internet connection:** Connectivity to the service provider's network.
- **House compatibility:** That the property is capable to be upgraded and perform as the client desires.

3. SYSTEM ARCHITECTURE AND DESIGN

3.1. System architecture

Primarily, the system architecture of the entire system is defined. The primary safety functions are defined are mentioned in section 2.5.

Whenever a subsystem fails the control system will check whether this can be solved by itself. If that's not the case, e.g., when the system reaches a critical/escalating state like overheating or breaking down, the other subsystems that are designed for de-escalating the concerning situation are failing/ unable to control the situation. In this instance, humans get allocated to perform safety tasks. As the user often does not have in depth knowledge of the system, the user should be notified to send a report to the customer service which will assess the problem and take action if needed. This can be a third-party product failing or a bug in the software. The type of problem will determine which action follows.

In the past, not many incidents have been reported. Several incidents are listed below:

- Spreading of faeces of pet by robot vacuum cleaner. [6]
- Streaming of inappropriate content to children via voice interaction [7]

The reason why the number of reports on incidents is relatively small is unknown, however it might be related to the number of hacks going unnoticed. It is known that smart homes and devices could be exposed to up to 12,000 hacking attempts per week [8].

3.2. System design

One subsystem is elaborated in this part to reduce the risks by focusing on the interactions and safety control system. The system which is focused on is a vacuum cleaner, often used in a smart home by automatically cleaning and mopping the floor. In the vacuum cleaner multiple sensors are present, for example a LIDAR sensor, gyroscope, motion sensor and camera. As the vacuum cleaner is often connected to the central smart home controller, it can be controlled remotely. However, this creates opportunities for hackers, as a smart home is often connected to the internet to be controlled from outside the house. Via an unencrypted connection, man in the middle attack, or a weak password a hacker can take control of the system. These systems can be used in a botnet for a DDoS attack without anyone noticing [9]. Besides, a hacker can spy on the smart home with the cameras installed. To improve this safety a proposal for the accessing of the control system is to implement an extra authentication step, like a fingerprint or Two Factor Authentication (2FA) and a secure password requirement. The security of the password could be ensured by requiring the password to cope with the constraints that are ruled in EU organizations [10]. Besides a safe connection the main system controller should be the only device connected to the internet.

Internal interactions

The vacuum cleaner can interact with other devices and with the humans in the house. The interactions between devices should be constructed with the use of an encrypted connection. The interactions between the devices of the smart home and the human are more related to physical contact. Humans can be hurt by the system if it is not properly designed. Therefore, each system needs to have a sensor to prevent this, which is not able to be influenced from the outside.

Safety control system

The control system of the vacuum cleaner consists of several parts. The lidar sensor, combined with the hit sensors form the input to the microcontroller (MCU). The temperature of the MCU is monitored by a thermistor [11]. The thermistor is of severe importance regarding the safety of the vacuum cleaner. Thermistors could also be applied to the motors and brushes. If the motor is overheating, the cleaner is forced to pause and run system diagnostics. The type of thermistor that is chosen, must suit the required temperature range and accuracy that is desired.

3.3. Residual risks

The goal of this section is to provide an overview of the risks. The risks are ranked to unacceptable (eliminated) risks, risks that are tolerable (controllable risks) and broadly acceptable risks that should only be communicated to the user.

Unacceptable	**Tolerable or ALARP**	**Broadly acceptable**
Death/ injury to pets, users or others	Failure of passive component	System UI not responding
Compromising of system by external factors	Overheating of any hardware	Not optimal performance of task
Data leakage	Disturbance to environment	Measurement errors
Failure of vital security components	Noise	
Damage to environment	Internal spreading of chemicals by smart devices	

3.4. Safety during production and installing

For the system the only relevant phases are instalment and production. The production only faces severe risks during software development. The main risks associated with the development of the software is that access to the code gets compromised. When this happens vulnerabilities can easily be found by malicious parties, or a backdoor can be installed.

As the system depends on subsystems, which are often bought from a third party, the risks associated with the production of these are not relevant for the SUC.

During installation there are risks present. For example, when the system is not properly installed this can lead to malfunction and result in the residual risks described in the previous section. Also, people with malicious intents can sabotage the system to gain access.

Finally, the CE marking needs to be applied. Generally, the products that are used in the smart home ecosystem are obliged to follow the low voltage guidelines for consumer products [12].

During the transportation of the system, the user does not experience any interaction with the products. Therefore, the risks to the user are negligible during transport. However, during the instalment of the hardware, the user is exposed to privacy risks for the installer.

4. OPERATION AND PERFORMANCE

In chapter four the hazard scenarios are identified and analysed. First, the hazards are analysed on three dimensions, namely: Technical, Functional, and Operational view. The functional perspective involves identifying potential functional hazards and deepening the causes and consequences of these hazards. In addition, technical and operational analyses are performed by identifying hazards, causes, and consequences. The most critical hazards have been analysed using fault tree analysis (FTA). Thereafter, the risk assessment matrix is used for risk analysis for organizations to determine and prioritize potential risks in a product/system. Then the human factors and culture are discussed when using the system. The dangers are considered here. ultimately looking at the possible future of the system design, to make it as sustainable as possible in terms of environmental friendliness, and economic and social aspects.

4.1. Hazards Scenarios identification

The Safety Cube Methods expands the risk awareness of the product by assessing risk in three different dimensions during its whole lifecycle. These dimensions include looking at the product in the past which helps from learning from previous experiences, the present to identify the hazards of current technology used, and the future scenario to assess the capabilities of the product and potential hazards. Looking at these scenarios enables one to ensure better adaptation of the product by predicting future changes in the system, interaction of the product with the surrounding environment, potential risks, etc. The past scenario includes using past technologies such as having a fence to prevent thefts or using stronger doors/windows locks to improve the property's security. By Looking at prior analysis, requirements, and maintenance data, one is able to identify hazardous scenarios in the past. The present scenario includes using the current basic technologies such as having one fire alarm for preventing the occurrence of a fire, or CCTV cameras. Whereas the future scenarios show the expected future performance of the product, future trends, potential hazards, and the transition needed to adapt to the smart system.

Furthermore, the three dimensions that were prescribed are previewed from three different hazard perspectives which are Technical, functional, and operating view (see Table 1-3). The functional perspective includes identifying possible functional hazards and looking more in-depth for the causes and consequences of these hazards. Moreover, technical and operational analyses are performed by identifying hazards, causes, and consequences as well. Moreover, the analysis is conducted on three main levels of the product starting with the interaction of the system with the environment, the whole system, and then the components of the system.

Table 1 Technical hazard analysis

Technical View	Past	Present	Future
Product environment	A fire could start at the house, and users are not alarmed about it. The house has higher chances of being theft with no security cameras nor alarms.	Users have cameras to monitor their houses, but not all are connected with their phones (Remotely). Thus, A hazard might occur without notifying the user.	A complete disconnection of the product with the shareholders including the user, which could endanger the security of the house.

			Financial barriers due to high cost of the system.
Product	Users invests in getting more/better locks for higher security or by installing higher fences to prevent accessibility to the property from thefts.	There is only one alarm in every home, so if an alarm happens in a different roam the alarm will only go on if the fire smoke reaches the sensor (fire could get stronger until it reaches the sensor).	Power failure or Internet failure will shut down the whole system. The smart system needs periodic system updates. Risk of hacking
Components	The locks could be damaged (Corrosion) with time and become easy to break. Fences could have a week point, where it becomes easier to breach.	Currently, most alarms are dependent on batteries and thus alarms could run out of power when battery life ends.	Power failure and Internet failure stop connection within the system.

Table 2 Functional hazard analysis

Functional View	Past	Present	Future
Product environment	The used system is not efficient enough to provide security like doors and windows, since they are in most cases breakable. In addition, the user is not alarmed (whether the users are inside or outside the property) in case of the occurrence of a fire or break in.	Current alarms used in houses are mostly dependent on batteries to function which require the user for periodic check-ups to assess the batteries functionality and for changing them.	Safety design models/ software for environmental conditions when a fire or explosion occurs, and the devices shut down so that the models can warn before this happens. Low speed internet might influence the functionality of the system.
Product	When the system is misuse, it can occur that the door will be broken or not working, broken window, damaged fence, etc.	The system can partially secure the property and components are not connected with each other.	A complete interconnected smart home is System for assuring the security of the property against any probable hazards.
Components	Users are limited to available resources to secure their properties.	Users might turn off the alarm assuming that the fire is already	The defect of one component in the system could influence

		turned off, but then goes on again. An earlier defect in a battery's life would endanger users in case potential hazards.	the whole performance of the system.

Table 3 Operational hazard analysis

Operational View	Past	Present	Future
Product environment	The users do not notice the occurrence of a fire/theft at the house. The available products to secure properties in the market had limited capabilities for preventing hazards.	for the safe operation of electrical appliances the system under normal and extreme conditions (high temperature) is one several important devices to be installed. Like alarms and cameras.	Monitoring could be done with user interface for the temperature in the house and energy use. In a critical situation a notification will then be sent and in an emergency, the emergency service will be contacted automatically.
Product	Simple to operate by all ages/background knowledge differences	Easy to operate by all ages/background knowledge differences	Smart homes use sensors to monitor residents conduct, and respond to this information in one autonomous mode. This includes Door entry system as well. Operating the system requires prior knowledge for the correct use of the system. Risk of data breach
Components	No Motorized control systems such as Window and Curtain controls Components are not connected to each other, thus a failure in one of the components	The system can be controlled in case of power loss or fire occurrence by alarms and warnings Components are not connected to each other, thus a failure in	Components of the system are all connected to each other; thus, one failure could influence all.

	does not affect the other components	one of the components does not affect the other components	

Due to the high differences in the future and past technologies, it is decided to neglect the past scenario and focus more on the present and future. The most critical hazards that are found from this analysis are:

1. Lose Connectivity (Loss of power & Loss of internet connection)
2. Compromise of client's privacy
3. Risk of Theft
4. Risk of Fire

To get a better understanding of these hazards, each will be analysed using fault trees analysis (FTA). The FTA is a graphical tool that is used to understand the causes of failures (hazards) in a system [13]. The FTA is implemented on the 4 main hazards (See Appendix A).

4.2. Risk assessment matrix

The risk assessment matrix is used for risk analysis for organizations to determine and prioritize potential risks in a product/system [14]. Thus, this allows one to be familiar with failures that could occur from the implementation of the current design. Then, the design can be improved to mitigate such risks. The matrix requires determining the severity of such risk and the probability of its occurrence. Table 4 shows the assessment of the 4 main hazards of the smart system. Here, one realizes that the risk of theft and fire have the highest priority for further design development.

Table 4 Risk assessment matrix

	Catastrophic	Critical	Minor	Negligible
Frequent (A)				
Probable (B)				
Occasional (C)				
Remote (D)	4	3		
Improbable (E)		1, 2		
Eliminated (F)				

4.3. Human factors and culture

Smart home automation is a system in which all the appliances in the home are automated and smarter than they are now. It connects electronics to human life and improves man's ability to control his surroundings. Smart security systems, on the other hand, make our lives safer and more secure.

Users discovered that Smart Housing design elements improved their self-assessed feelings of safety [15]. They appreciate the positive effects of the house's lighting, camera, sensors which can contribute to their sense of comfort and safety. The positive components of the house have changed the user's perspective on how houses can be designed as a measure of success in terms of safety. However, some components can be poorly designed, such as the garage door's reliance on electronic

operation/ installation and power loss during extreme weather, which could frustrate the users or injuries can occur during these occasions. Some of the house's features should be modified to improve safety and to reduce injuries. While it is important to recognize that users had to adjust before they could trust certain design features, the design has had a positive impact on their sense of satisfaction and ease within the house over time.

The security of a smart home is improved by adding features that reduce break-ins. Effective design of the built environment reduces crime and increases people's sense of security.one of the crime-fighting principle that can be implemented is target hardening which includes alarms, security screens, door-viewers, an intercom, security locks, security louvers, exterior sensor lights, and smoked glass sidelights.

The report [15] states that residents cited the heavy-duty safety screens and smoked-glass side windows as features that contributed most to safety. Residents felt safe knowing that there were multiple barriers to entry before an intruder could break into the home. Adding the security left one of the residents with the impression of being exposed and vulnerable to public scrutiny from the street. While they appreciated the smoked glass, taller windows, and security screening, the visibility of the interior from the outside was an issue that was resolved when the garden was constructed.

In addition to its use in home security systems, artificial intelligence is used to control smart devices. Artificial intelligence is extremely powerful. It simulates human knowledge and learning abilities on a technological level. Recent advancements in smart home automation systems have resulted in advancements in artificial intelligence in terms of cloud communication, learning human behavioural patterns, and automating smart home devices based on user preferences [16].

The human factor has a significant impact on security risk. There are some mistakes when using security devices and installing the smart system:

Weak password protection: If passwords are not used correctly, they can be easily cracked, guessed, or otherwise obtained by malicious perpetrators, giving them full access to the system. Administrators can mitigate risk by implementing aggressive password policies (e.g., enforce password history, maximum password age, minimum password length, and password must meet complex requirements).

Smart devices must collect a large amount of data for smart homes to function. **Careless data handling by the company** can result in leaking of information. Large amounts of information or manipulated sensitive data sometimes leave that data open to the public. This omission may be due to a simple error, or it may be due to the employee not understanding the importance of such information.

Users generally have **little knowledge of phishing** and social engineering practices, which can allow malicious to inadvertently gain access to the data (by hacking).

Little knowledge of installing the system, while people should always hire an electrician if they're not sure how to do it themselves, the fact that smart devices are often marketed as "easy to install" and "plug and play" encourages people to try and install them themselves. to install. This is also a clear risk. This kind of behaviour can result in injuries and even death.

As smart devices are increasingly used to power smart homes and lives. The more people rely on connectivity, the more difficult their lives will become. As a result, it is important to make the design as secure as possible. Misuse of the system can also result in accidents. The accidents could be

reported via UI (human interactions with the system), which can result in evaluation by the system designers.

4.4. Safety-risk monitoring

A smart home is essentially a huge, networked computer system. the devices such as cameras and lamps are connected to each other via the internet (Wi-Fi) and can be hacked like anything else digital. Someone else then has control over the connected devices and takes over the house. It can go very wrong. One option to control the system is to use devices from experience manufacturers that take security seriously. Also use security measures such as a strong password and a secure network.

Another big privacy-related concern many people and experts have is what companies do with all the data they spend hours collecting at home. For smart homes to work, smart devices need to collect a lot of data. Through a camera or smart device, people can know when you leave home and when you come back. therefore, one should always read the privacy policy of any smart product or service before making use of it.

There is also a chance that the cloud service will go offline. This may affect cloud-connected smart home devices. Then people can't turn on their smart lights and they're in the dark. Others can't control their alarm system, garage door, and smart TVs. people then depend on smart devices, and it can become more problematic as more and more people use them. In this case, it should be ensured that essential devices such as Wi-Fi smart thermostats and lamps are purchased with a local option. This means that the devices can continue to work even without an Internet connection.

4.5. Retirement

A smart house should be designed to be as sustainable as possible so that it can be used by all people to the greatest extent possible and without the need for modification or specialized design. Universal design is the most effective contributor to sustainable housing [17]. It extends the use of the home through design and products that are durable, adaptable, and suitable for people's changing lifestyles over time, making homes built with cheaper alternatives that last longer. This means that, in theory, a family can live in a sustainable home for life. The features built-in from the start ease the need to move if or when lifestyles and physical abilities change. Importantly, the exterior of a universally designed home looks like a traditional home. It is the universal design principles and products that make the difference. The house should be designed for everyone and every ability, it should be easy to use and easy to see the information. The design should also minimize error and hazards and low physical activity will minimize injury.

5. CONCLUSIONS

The SUC is a smart system that provides homeowners security and privacy. This system is built up from different sub-systems. This subsystem consists of three main areas, the operation infrastructure, the operation management, and the operation strategy. This system is to be regulated under EU legislation.

If subsystems of the smart home are unable to de-escalate a critical event, the task is shifted to humans. The major vulnerability in the system can be accounted for by the software. Therefore, nearly all the safety risk is due to hackers, possibly exposing the smart home to more than 10,000 hacking attempts per week.

A man in the middle attack or a weak password hack are most common. Two factor authentication and a password according to EU guidelines will severely decrease the safety risk. The subsystems of the smart home consist of hardware that each follow a different set of regulations for a CE mark.

The risks of the entire smart home are ranked to their severity. Unacceptable (eliminated) risks, risks that are tolerable (controllable risks) and broadly acceptable risks are the main classifications.

Risks during production arise when the software development yields leakage. During installation privacy risks are of main concern.

The 4 main potential hazards that are found from analysing past, present, and future hazard scenarios which are Lose Connectivity, Compromise of client's privacy, Risk of Theft, Risk of Fire. These hazards are analysed by using the fault tree analysis and then it was put in a risk assessment matrix, and it was found that risk of having a theft or fire is the most critical. Thus, the system requires further development to mitigate these risks by implementing the following recommendations:

1. Provide alternative power supply for essential components of the system in case of any power cut then the system can still function the essentials (fire alarm/sensors can be powered by batteries).
2. Enable a feature of operating the system without internet (data storage/monitoring/alarms can still function without internet)

Implementing such recommendation have high influence not only on the two critical hazards, but other hazards too. Thus, this would be great to mitigate the risks of hazards.

6. REFERENCES

[1] CBS, "Federatie Veilig Nederland," 2022. [Online]. Available: https://federatieveilignederland.nl/nl/handige-informatie/feiten-en-cijfers/feiten-en-cijfers-beveiliging.

[2] Energievergelijk, "Energievergelijk," 2022. [Online]. Available: https://www.energievergelijk.nl/english/price-cap-energy.

[3] IOTAP, "Malmö University," 14 June 2016. [Online]. Available: https://medium.com/@iotap/on-privacy-and-security-in-smart-homes-543f62aa9917.

[4] GlasgowUniversity, "European Union Legal Information: How to find and use EU legal sources: EU legislation," 2022. [Online]. Available: https://guides.lib.strath.ac.uk/eu_legal_information/legislation. [Accessed 3 December 2022].

[5] USDA, "United States Mission to the European Union," Foreign Agricultural Service, 2022. [Online]. Available: https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/. [Accessed 4 December 2022].

[6] "Roomba creator responds to reports of 'poopocalypse': 'We see this a lot'," The Guardian, 2016. [Online]. Available: https://www.theguardian.com/technology/2016/aug/15/roomba-robot-vacuum-poopocalypse-facebook-post. [Accessed 4 December 2022].

[7] "Child Safety in the Smart Home: Parents' Perceptions, Needs,," *ACM Hum.-Comput. Interact,* vol. 5, no. CSCW2, p. 471:12, 2021.

[8] "How a smart home could be at risk from hackers," 2021. [Online]. Available: https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU. [Accessed 4 December 2022].

[9] "What is a DDos botnet," 2022. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/. [Accessed 4 December 2022].

[10] E. U. Institute, "Strong Password Policy," 2022. [Online]. Available: https://www.eui.eu/ServicesAndAdmin/ComputingService/PolicyDocuments/StrongPasswordPolicy. [Accessed 2 December 2022].

[11] V. S. a. M. D. a. N. B. B. a. B. B. J. a. A. M. Z. Turkani, "A carbon nanotube based NTC thermistor using additive print manufacturing processes," *Sensors and Actuators A: Physical,* vol. 279, pp. 1-9, 2018.

[12] "CE Marking Manufacturers," [Online]. Available: https://single-market-economy.ec.europa.eu/single-market/ce-marking/manufacturers_en. [Accessed 4 December 2022].

[13] T. Hessing, "Fault Tree Analysis," Six Sigma Study Guide, 2020. [Online]. Available: https://sixsigmastudyguide.com/fault-tree-analysis/.

[14] I. Markovic, "How to use the risk assessment matrix to organize your project better," TMS, 8 November 2019. [Online]. Available: https://tms-outsource.com/blog/posts/risk-assessment-matrix/.

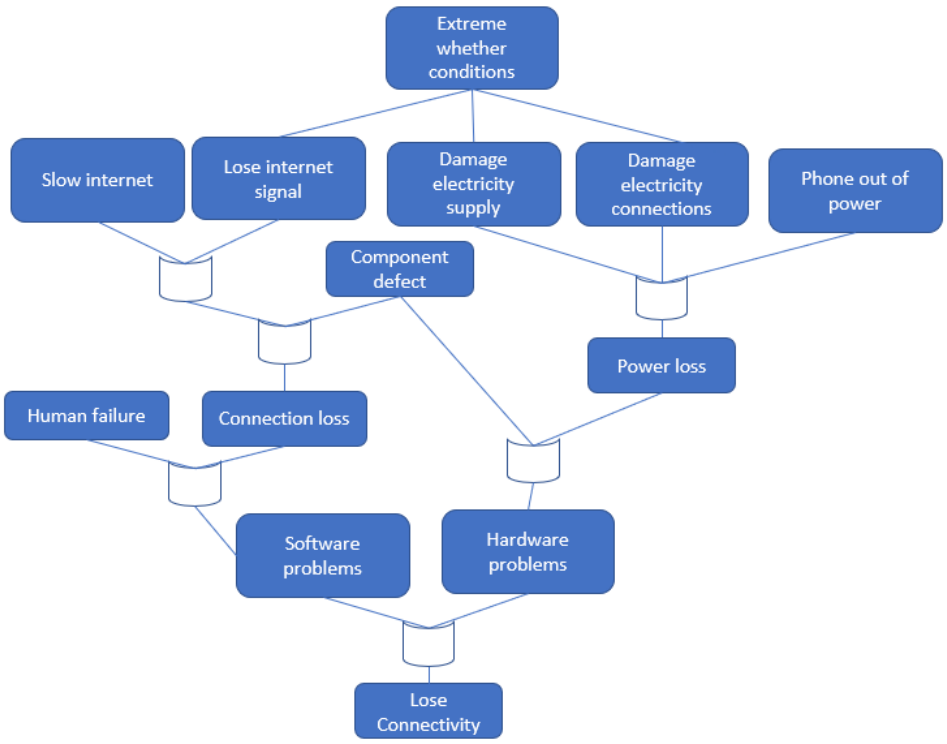
[15] L. Buys, K. Barnett, E. Miller and C. Bailey, "Smart housing and social sustainability: Learning from the residents of Queensland's Research House," *Australian Journal of Emerging Technologies and Society,* 2005.

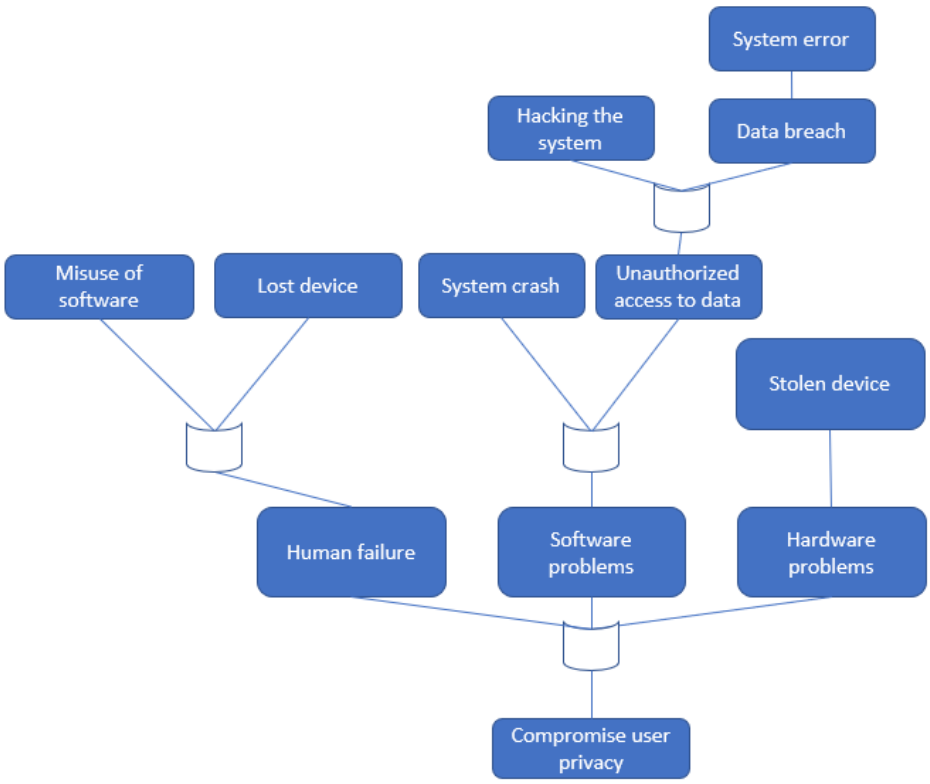
[16] "Human Factors: How We Designed an Adaptive Culture for Our AI Company," 2018.

[17] "The Centre for Excellence in Universal Design," 2020.

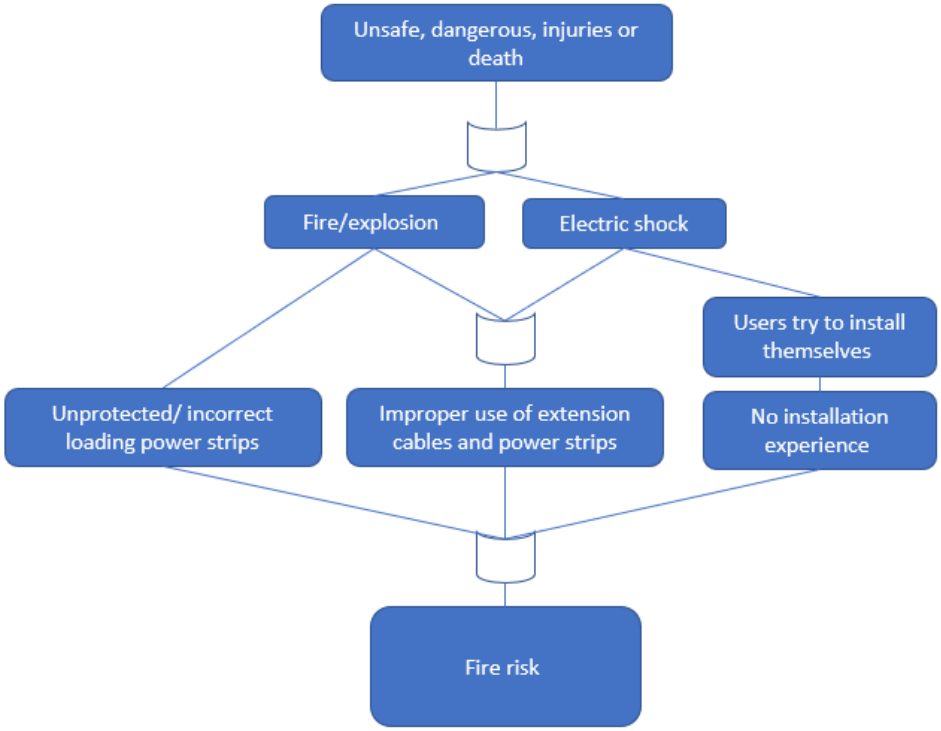
7. APPENDIX

Appendix A: Fault trees




System error
Hacking the system
Data breach
Misuse of software
Lost device
System crash
Unauthorized access to data
Stolen device
Human failure
Software problems
Hardware problems
Compromise user privacy


Unsafe environment and misuse of data
Taking control of the devices like cameras
Lose of data / leak of information
No use smart lights, home alarm systems, garage door and smart TVs
Unable to use devices
Smart connected devices not working
Phone being hacked
Company Offline cloud service
Break-in by shutting down the system
Risk of theft


Unsafe, dangerous, injuries or death
Fire/explosion
Electric shock
Users try to install themselves
Unprotected/ incorrect loading power strips
Improper use of extension cables and power strips
No installation experience
Fire risk