University of
Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialization: MSc in Risk Management/ Risk Assessment and Management	Spring/~~Autumn~~ semester, 2018 Open/~~Confidential~~
Author: Sanja Mrkšić Kovačević	(Signature of author)
Programme coordinator: Roger Flage Supervisor(s): Roger Flage	
Title of master's thesis: Smart homes from a Risk Management perspective	
Credits: 30	
Keywords: risk management risk assessment smart home/s internet of things	Number of pages: ………78………… + Supplemental material/other: …0… Stavanger, ….15/06/2018….. Date/year

Smart homes from a Risk Management perspective

Sanja Mrkšić Kovačević

Stavanger, June 2018

ABSTRACT

A smart home refers to a regular home with a difference that it contains devices and equipment mutually connected which enables additional support, control and comfort for the residents. Thus the residents are provided with the opportunity to control their own energy efficiency, to have additional safety control over their home and many other benefits. The concept is evolving, especially in the last few years with the overall technological development. Together with large benefits of the smart homes, there are certain risks that come along and they are difficult to anticipate since the concept is new and developing. Hence historical data is not enough or does not exist.

The aim of this thesis is to analyze existing risk assessment methods, that can be used for assessing cyber risks related to the smart homes, and to further analyze them from three perspectives: individual, society and government.

PREFACE

This Master thesis is written as the final part of the MSc in Risk Management with specialization in Risk Assessment and Management at Faculty of Science and Technology, University of Stavanger, Norway. The inspiration for writing the thesis with this topic came from one of the greatest scientists that our world ever had:

"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket. "

Nikola Tesla
(Interview with John B. Kennedy in 1926)
(Business Insider, 2015)

I want to thank my supervisor Roger Flage for amazing guidance, fast and precise answers to my questions in the moments when I needed it, inspiration when I had complete lack of it and overall most important excellent support. I would also like to thank my family and friends for always standing by my side.

Sanja Mrkšić Kovačević
University of Stavanger, Norway, June 2018

TABLE OF CONTENTS

(Left blank intentionally)

1. INTRODUCTION

1.1. Motivation

With the development of new technologies new risks associated are evolving as well and need to be appropriately managed. Thus, the topic of smart homes from risk management perspective can be quite challenging. Sometimes due to fast changes we cannot follow up with all the risks involved. Although smart houses are very interesting and concept that is going in the near future to grow and develop further with the goal to make everyday life easier, more convenient and efficient, it is necessary to observe all the risks involved as well.

Smart homes (SH) are developed from the wider concept of Internet of Things (IoT) which is rapidly growing and developing in the last years together with the development of the overall technology. To be aware of the impact that IoT is having in today's world it is interesting to observe data that are available. International Data Corporation (IDC, 2017) is publishing Worldwide semi-annual Internet of things spending guide which covers the following regions United States, Canada, Japan, Western Europe, Central and Eastern Europe, Asia/Pacific, Middle East and Africa and Latin America. In December 2017 (IDC, 2017) they forecasted that in 2020 the worldwide IoT spending will reach 1 trillion USD (according to current exchange rate 7,8 trillion NOK) in comparison with 674 billion USD spent in 2017. According to PricewaterhouseCoopers reports, 6 trillion USD will be spent on IoT solutions in the period from 2015 to 2020 (Forbes Technology Council, 2018). McKinsey Global Institute made an estimation that IoT could possibly have an annual economic impact of 3.9 to 11.1 trillion USD by 2025 (Manyika et al., 2015). If we take into consideration all this data we can become more aware of the impact and growth of the whole IoT nowadays and in the near future.

Smart homes are based on IoT concept and are as well independently developing extremely fast. According to Forbes Technology Council (2018) technology in these markets will reach 53.45 billion USD by 2022. Smart homes as a concept of connecting all the devices and appliances by internet are getting every day more involved in home appliances and home design in general. This expansion is influenced from one side by the overall usage of smartphones nowadays which increased in comparison with the previous years. Only in Norway there were 3.48 million smart phones users in 2015, and predictions are that there will be 4.75 million users in 2022. (Statista, 2018) Hence, in seven years observed period, increase of mobile phone users is almost 36%.

Due to expansion of smart homes and in general IoT technology, it is very interesting to see how risk management concept can adapt to those rapidly growing changes. Naturally growing technologies on this high pace are followed as well with the growth of risks accompanying them. Nowadays, used risk assessment methods have to follow this rapid development in order to provide full support for new types of risks that will appear in the future.

As Jacobsson (2016) explains prior to smart house development, risks related to a person's home were mostly related to physical threats in a sense of burglary or stealing of values or information directly from the house. With the development of smart houses those risks have expanded and it is not necessary to have physical intruders in the house for the undesirable event to occur. In case of the smart house, it is enough to access the information system related to the particular smart home. This way, the intruder does not have to enter the house physically, as a matter of fact, they can be located anywhere in the world, and depending on the smart characteristics of the house, steal valuable data and monitor residents' behavior. (Jacobsson, 2016)

When we observe SH, if we are in a position of a resident that owns or simply lives in a SH, we will assess risks related to the SH in relation to, for example, our banking information stored on our computer that can be stolen, or data related to fingerprints used for our door lock that can be misused. On the other hand if we are standing in a position of government of a country or society we will approach SH risks in a completely different way. Naturally, we will be concerned as well for the safety of a single resident of the SH but, nevertheless, we would be concerned for the whole society and effects that it can produce on a much wider level.

Thus, risk assessment related to the SH can be observed from many different perspectives. The three ones pointed out in this thesis are the individual perspective referring to a single resident of the SH, society perspective and government perspective. Each of these three perspectives is approaching risks related to SH from a different point of view and in the need of having their own mechanisms for assessing risks.

1.2. Objectives

The main objective of this thesis is to analyze existing risk assessment methods that can be used for smart home risk assessment, related to cyber risks, from three different perspectives: individual, society and government. The consequence dimensions that are going to be observed are related to monetary loss, data loss, data misuse. In order to meet this objective the following will be done:

- Presentation and literature analysis of adequate existing risk assessment methods
- Study of strengths and weaknesses of existing risk assessment methods through the three perspectives: individual, society and government
- Recommendation for improvement of existing risk assessment methods with suggestions for new method development according to the analysis

1.3. Scope and limitations

The presentation of existing risk assessment methods will be conducted according to the risk assessment methods that are found in literature. The methods chosen are going to be the ones that have, through the literature research, been analyzed as the most used related to cyber and information risks. Although the thesis is putting focus on cyber related risks, when it comes to risk assessment methods we have to take into account as well the ones oriented towards the information risks, since both can be adapted for the smart home risk assessment. More information regarding relations between information and cyber security and risks will be provided in Chapter 2.

The consequence dimensions will not be set on human losses, but on monetary loss, data loss, data misuse which are consequences that are most related to cyber risks and can influence both privacy and security of smart homes. (Elmaghraby & Losavio, 2014)

Study of strengths and weaknesses of existing risk assessment methods will be literature based and will follow with the discussion and conclusion of the characteristics from the three perspectives:

individual, society and government. The conclusions of strengths and weaknesses of the methods is primarily going to be literature based with clear references, but it will as well have conclusions based on brain storming and logical inference. The society and government perspective would be primarily limited on Norway since this thesis is done in Norway and in order to be able to provide better quality results.

1.4. List of abbreviations

The following abbreviations will be used through the text:

CIA	Confidentiality, Integrity and Availability
CRASH	Cyber Security Risk Assessment with appliance for SH
FAIR	Factor analysis of Information risk
IoT	Internet of Things
IS	Information system
ISRAM	Information security risk analysis method
NIST CSF	National Institute of Standards and Technology’s Cybersecurity Framework
NIST RMF	National Institute of Standards and Technology’s Risk Management Framework
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
RA	Risk analysis
SH	Smart homes
SoK	Strength of knowledge
WAN	Wide Area Network

2. THEORETICAL BASIS

In this chapter we will introduce the theoretical basis necessary for the comprehension of the further chapters. First in the subchapter 2.1. we would go through the explanation of risk and vulnerabilities and covering also how risk assessment is conducted and some important aspects of it. We will also, go through the explanation of cyber and information security. This will be explained in a relation to our emphasis in chapter 5, when we come to the analysis of the existing risk assessment methods, which would be on cyber related risks.

2.1. Risk and vulnerabilities

2.1.1. The concept and description of risk and vulnerabilities

Many theoreticians have been describing risk by trying to adapt definition of risk as precise as possible. As Aven (2015) explains, risk has two main dimensions that we should be aware of – consequences and uncertainties. The risk concept as he further illustrates, (C, U) where C stands for consequences and U for uncertainties shows that the activity leads to some consequences C and they are not known.

Further, general description of risk can be written as Aven pointed out (2015):

Risk description = (C’, Q’, K) or (A’, C’, Q’, K)

In the formula written above it is stated that risk description consists of a specific undesirable event (A’) which leads to some specified consequences (C’) and Q’ = (P, SoK) stands for the specific probabilities that describe uncertainties and they are assigned based on the background knowledge (K).

Vulnerability is an aspect of risk as described by Aven (2015). He defines vulnerability as a two-dimensional combinations of consequences with associated uncertainties given an initiating event. As an example, he draws an example of a patient that is already in the state of weakness and not in a fully health state, thus we can describe a probability of the undesired event occurring – patient dying is high. Therefore the person was vulnerable due to his/hers current state of health. In cases when the vulnerability is highlighted in the risk analysis, it can be described as well as vulnerability analysis. (Aven, 2015)

As Aven (2015) further explains the vulnerability concept can be observed as risk conditional on the occurrence of the event A, whereas the vulnerability description takes the form

Vulnerability description = (C', Q, K | A)

2.1.2. Risk management and risk analysis

2.1.2.1. <u>Risk management</u>

Risk management as defined by (Aven & Vinnem, 2007) is described as all measures and activities that are conducted with a goal of risk managing. Risk management is oriented on balancing the conflicts inherent in opportunities exploring from one side and avoiding losses, disasters and accidents on the other side. (Aven & Vinnem, 2007)

Risk management can be in set in three main categories as explained by Aven (2015):

- Strategic risk – the consequences in this case are related to acquisitions, mergers, laws, regulations, labor market and similar
- Financial risk – the consequences in this case are related to the influence of stock prices, foreign exchange rates, interest rates and similar
- Operational risk – the consequences are related with safety or security related events as accidental events or intentional acts

Risk management consists of different processes and risk analysis is considered to be the central part of the risk management. National Institute for Standard and Technology defines risk management as the whole process of identifying and assessing risk in order to take steps to reduce risk to an acceptable level (Jouini & Rabai, 2016)

2.1.2.2. Risk analysis

Risk analysis has as a main objective to present an informative risk picture or, in other words, to describe risk. (Aven, 2015) The term risk analysis can be put in few categories according to the simplicity or complexity of methods chosen and in which amount they are relying on quantitative or qualitative analysis in the process.

Table 1: Risk analysis methods categories. Based on (Aven, 2015)

Category	Simplified RA	Standard RA	Model-based RA
Type of analysis	Qualitative	Qualitative or quantitative	Primarily quantitative
Description	Risk picture is usually established during brainstorming sessions or group discussions	More formalized procedure than simplified RA. Presentation of results usually with risk matrices	More quantitative procedure in comparison with the other two
Example of analysis	Coarse scale (no formalized RA methods)	HAZOP, Coarse RA	Fault tree and event tree analysis

As it is shown in the Table 1, depending on the complexity of the risk analysis we have different types and examples of risk analysis used. Standard risk analysis uses both strengths of qualitative and quantitative measures. Two main types of analysis as shown are quantitative and qualitative risk analysis. Risk analysis methods that are using extremely quantitative measures are not easy to use because of the extensive appliance of complex mathematical and statistical methods, whereas qualitative risk analysis methods, where risk is being analyzed with the adjectives instead of mathematics, do not offer enough information outputs very often. (Wawrzyniak, 2006)

Risk analysis can be observed in the best way by understanding each part of risk analysis and then by observing the analysis as a whole. Usually risk analysis consists of three main elements (Aven, 2015):

- Planning phase
- Risk assessment (execution) phase
- Risk treatment (use) phase

Phases are in detail explained by Aven (2015) as follows. Planning would consider the definition of the problem by itself, gathering all the information available and selection of the analysis method. Risk assessment which can be considered as the core part of the analysis consists of the identification of the initiating events which can be different hazards, threats or opportunities, cause and consequence analysis and establishing a risk picture. After conducting the risk assessment phase it is necessary to compare all the alternatives that are available and available according to the risk picture, identify and assess measures in order to treat risk. And as a final part that, we have the management review and judgement which can be considered as one of the most important parts of the whole analysis since it shows how the data provided will be used, followed by the final decision of how to treat risk. The previously explained steps are shown in the Figure 1.

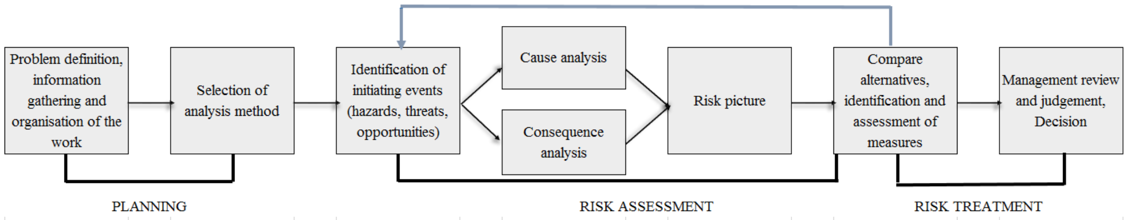

Problem definition, information gathering and organisation of the work
Selection of analysis method
Identification of initiating events (hazards, threats, opportunities)
Cause analysis
Consequence analysis
Risk picture
Compare alternatives, identification and assessment of measures
Management review and judgement, Decision
PLANNING
RISK ASSESSMENT
RISK TREATMENT

Figure 1: The steps of risk analysis process. Based on Aven (2015)

2.1.3. The Risk assessment process

Risk assessment process can be described as the execution of the risk analysis. (Aven, 2015) It is the core process of the whole risk analysis process which results in a complete risk picture of the project, business or similar which is analyzed. (Aven, 2015) As it can be seen in Figure 1 it is the part of the process where risk analysts can provide all the possible data in order to create a better base for managerial review and judgement towards getting the final decision. NIST (2016) defines risk assessment as the process of identifying, estimating and prioritizing information security risks in order to determine the extent to which events or circumstances that could adversely have an impact on an organization and the likelihood of their occurring. This whole process requires a careful analysis of threat and vulnerability information. (Jouini & Rabai, 2016) In ISO Guide 73:2009 risk assessment is described as the overall process of risk identification, risk analysis and risk evaluation. (Guide, I. S. O., 2009)

2.1.3.1. Identification of the initiating event

As Aven described (2015) the first step of risk analysis is to identify the initiating events or in other words explained, it is the critical task of risk analysis: if the potential threats are not described well we cannot know what is standing against us, thus, we cannot avoid actions or reduce the consequences if it is not clearly given what is actually the threat we are facing. Many methods are used in order to describe in more details the initiating events. Some are developed through time and since risk management is developing, the methods are developing as well. Caused by more threats appearing and some current ones disappearing or changing completely, the methods have to be improved and developed further as well. (Aven, 2015)

Aven (2015) describes few mostly used methods for the identification of the initiating events as:

- FMEA (Failure modes and effects analysis)
- HAZOP (Hazard and operability study)
- SWIFT (Structured what-if technique)

All the methods above listed are having a common characteristic which is that they are based on a structured brainstorming which takes use of checklists, guidewords or similar in relation to the problem that should be approached (Aven, 2015). As Aven (2015) further explains it is usually common to use the 80-20 rule which means that it takes 20% of the time to identify 80% of the hazards and the other way around for the rest of the 20% of the hazards that are not so often occurring and, thus, are not usual, taking 80% of the time to identify.

2.1.3.2. Cause analysis

Cause analysis as its name says is oriented towards discovering the causes that lead to the occurrence of the initiating events. (Aven, 2015) Methods and techniques that are used during the cause analysis as Aven (2015) further explains are mostly based on brainstorming sessions, it can also be used fault tree analyses or Bayesian networks. Normally in practice, the cause analysis will consist of few analyses that are basically “sub-risk analyses” which will give better results in the combination than by using only one approach. (Aven, 2015)

2.1.3.3. Consequence analysis

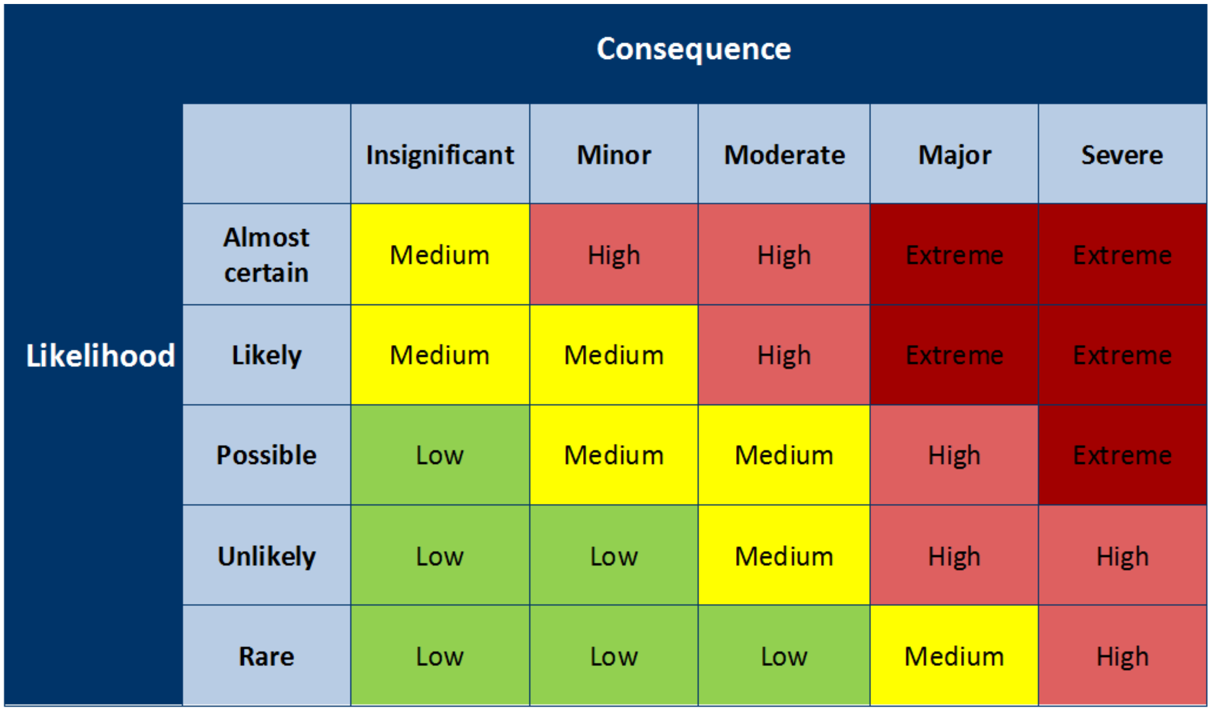
It is important to observe the other way as well, meaning, what would be the consequences that the initiating event can lead to. Basically that is done by using the consequence analysis. Aven (2015) presents the event tree analysis as the most common and most used method for analyzing the consequences. Event tree analysis is a very simple way of establishing the relations between initiating events and consequences by following the branches of the tree. The method is simple to use and to demonstrate the results. Since it is highly comprehensive even if the observer is not a risk analyst or an expert in the field. (Aven, 2015)

2.1.3.4. Establishing the risk picture

The risk picture is established based on the cause and consequence analysis. (Aven, 2015) As Aven (2015) further shows, risk picture is covering the whole risk description (A’, C’, Q’, K) where Q’ = (P, SoK) stands for the specific probabilities that describe uncertainties and are assigned based on the background knowledge (K). The risk picture should normally cover following important factors Aven (2015):

- Predictions of the quantities that are the object of observation (as number of fatalities, or number of car accidents or similar)
- Probability distributions which can be related to costs and number of fatalities
- Strength of knowledge on which the whole risk picture is based on
- Manageability factors

The risk picture can be presented in various ways. The main goal is to provide the best basis for managerial review and judgement and the decision that will follow. The rest is upon the analyst to decide which presentation method would be the best in the given case, considering the type of the problem and as well the audience that will observe the risk picture following to make the decision in the end. Aven (2015) presents few ways of setting the risk picture through graphs by presenting probabilities of the undesirable event occurring through risk matrices which can in a very simple way demonstrate the relation between probabilities and consequences and are very easy to understand. The most important task of risk analysts while presenting the risk picture is to point out the strength of the background knowledge, or simply said, on what kind of knowledge is the risk picture established. (Aven, 2015)



		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost certain	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	Extreme	Extreme
	Possible	Low	Medium	Medium	High	Extreme
	Unlikely	Low	Low	Medium	High	High
	Rare	Low	Low	Low	Medium	High

Figure 2: Example of a risk matrix. Source: (The University of Melbourne, 2018)

An example of a risk matrix is showed in the Figure2. As it can be seen, on one side of the matrix we have consequences and, on the other, the likelihood of occurrence. The rankings used in matrix are: low, medium, high and extreme. They are marked with different colors, which enables simpler interpretation.

Strength of knowledge (SoK) has crucial value of the whole risk assessment process because, if it is not clearly defined, it can be truly misleading and can lead to completely wrong decisions in the further decision making process regarding how to treat the risk. As a conclusion based on Aven (2015) if the risk picture is established on weak knowledge and that is not clearly stated in the risk picture presentation, it can lead to the decision which itself can lead to serious consequences and end up causing both material and human losses.

2.2. Information security and cyber security

In the thesis as mentioned before, emphasis will be on SH risk assessment with the emphasis on cyber risks. To be able to understand them better and differentiate between cyber and information risks this subchapter will include their definitions and further explanations.

Information security should protect the confidentiality, integrity and availability of information systems in storage, processing and transmission by application of policy, education, training, awareness and technology. (Whitman & Mattord, 2011)

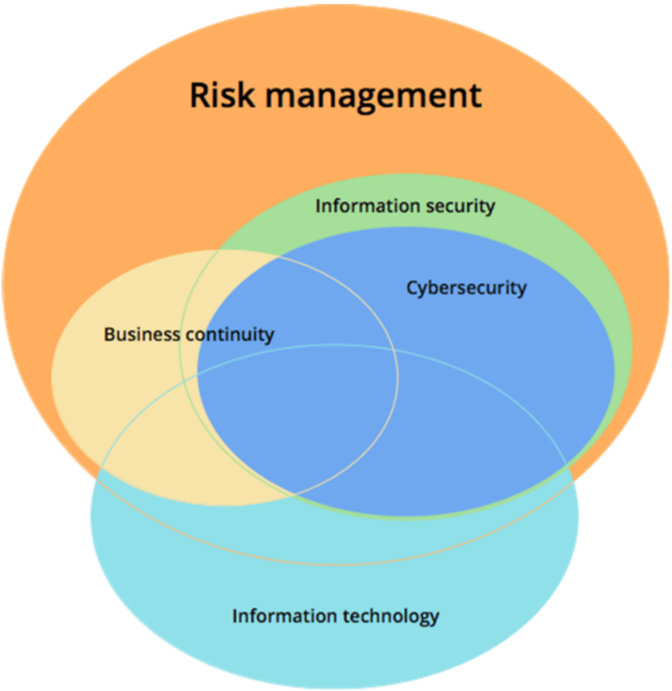


Figure 3: Information security vs. Cyber security. Source: (Kosutic, 2016)

Figure 3 shows cyber security as a part of wider information security. Although they are often mentioned together, they are not referring to the same: cyber security has an additional dimension according to Whitman & Mattord (2011). They address human factor in a sense of humans as potential as potential targets of cyber-attacks or as unknowingly cyber-attack participants. Cyber security can be defined as the practice of protecting systems, networks and programs from digital attacks which intention is usually to access, change or destroy sensitive information such as extorting money from users or similar. (CISCO, 2018)

Information security triad traditionally was designed to provide a standard when it comes to evaluation and implementation of Information Security. The three sides of the triangle represent three goals that are (Fenrich, 2008 and Whitman & Mattord, 2011):

- Confidentiality – it ensures that data can be accessed only by an authorized person. Some of methods that help implement this goal are user IDs and passwords
- Integrity – it ensures that data can be trusted in a sense that data can be changed only by an authorized person and that besides that time it will remain the same. Some of methods that cover this goal are data encryption and hashing algorithms
- Availability – it ensures that data is available when required by the authorized person. Some of the methods that are enabling that this goal is fulfilled are software update and hardware maintenance

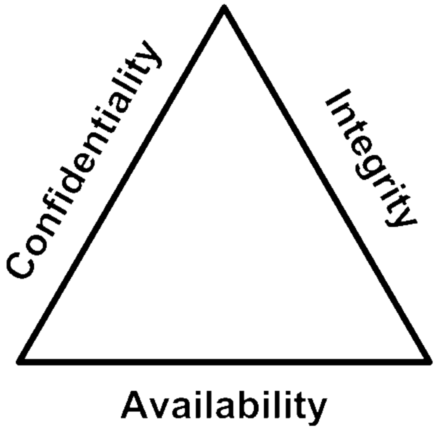


Figure 4: CIA triad. Source: (Buntz, 2013)

Although CIA triad presented in the Figure 4 describes very well what information security is all about, there are some doubts concerning if it is a correct way of describing it nowadays with the development of Big data and IoT. As explained in ISBuzz Security panel (2015), the CIA triad, due to new technologies that are developing, should be changed with the following structure on the figure 5. With IoT there are a lot of new devices from different manufacturers that are being used together so the authentication is of extreme importance. The additional goals are (ISBuzz Security panel, 2015):

- Authentication – it means that apart from the confidentiality that provides the human level of authentication it is as well necessary to fulfill the machine level of authentication. This is especially crucial for the IoT and therefor for the SH as well.
- Code validation – checking the accuracy of the code and correcting it in order to improve the quality of the code. Especially important since bad code equals high vulnerability
- Nonrepudiation – it means that the parties who have sent and received the message are the parties who were supposed to send and receive the message

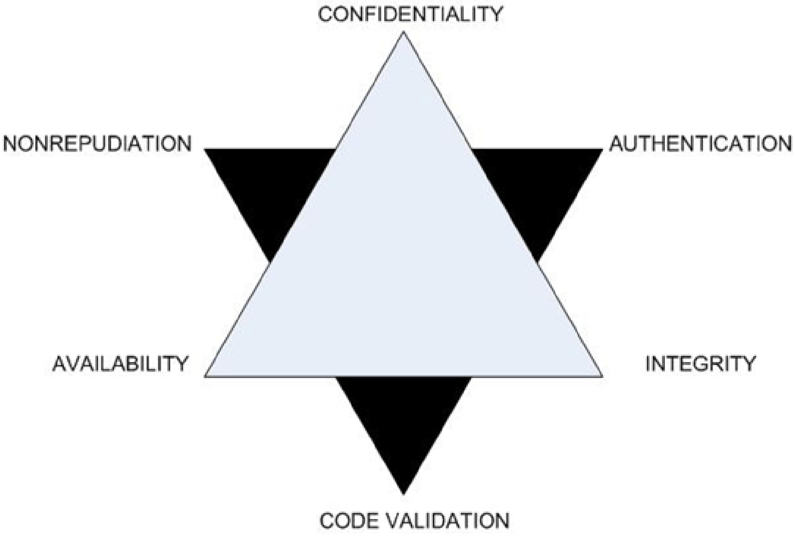


Figure 5: CIA triad improved according to the Big Data and IoT development (Source: ISBuzz Security panel, 2015)

As it can be seen in the Figure 5 the structure of information security goals has just been widened with these additional goals, and basically, it has covered more vulnerabilities than the previous one. Since we are focusing on the SH risk assessment in this thesis, this CIA triad is more useful since it gives much wider picture and it covers some important aspects of the SH related security.

Cyber security and risks related as well as information security and risks related should not be observed separately since, as explained above, cyber security can be seen as an integral part of information security. When it comes to cyber security, cyber-attacks, although they have increased in the past decades they have been known earlier as well. Cavelty (2007) describes some of the first cyber-attacks conducted in 1988 when the Morris worm brought ARPANET (the early Internet) to a standstill state. Today cyber risks and whole security related to it, although known from before, can be considered to have two important characteristics for which they should get appropriate attention: they have potential great impact and they were all once considered as improbable. (ISACA, 2013) In this thesis as explained before, emphasis will be put when analyzing risk assessment methods on cyber risks precisely for these two characteristics that make a significant difference of risks involved with smart homes and risks involved with regular homes.

3. METHODOLOGY

The information found and analyzed in this thesis is comprehensive although in some moments inconsistent and not standardized due to the actuality of the topic and not extensive historical data either on smart houses or on risk assessments and risk management approaches that are used. The aim of this thesis is to analyze all the given sources found in order to create a wider picture with the attempt to create a complete picture through the information given and to draw conclusions and future recommendations accordingly.

The theoretical basis is primarily based on the literature as a part of the curriculum for MSc in Risk Management at University of Stavanger, Norway, as well on articles, books and similar related that give a strong theoretical basis for the further analysis. The chapter 4 related to Internet of Things and Smart homes was mostly built on articles, books and similar found, related to smart homes and Internet of Things that was published after year 2010 in order to provide stronger basis for the topic. There are some articles and books that are used which are published before 2010 but they are included due to their relevance. In order to assess better the topic a visit to three private smart homes was conducted with the following discussion with the owners about the risk management regarding their homes. This way, a very good basis for the individual perspective was achieved.

Literature review was used as well to find risk assessment methods that were in use for the Chapter 5, in order to cover as many as possible risk assessment methods and provide better results further on. Inference drawn in the Chapter 5 and following in the Chapters 6 and 7 are based on the basis provided in the first part of the thesis as well as on the reasonable and logical analysis of the information provided through the analysis.

Table 2: Search engines and key words used for the literature search

Search engines:	Search - key words:
scholar.google.com	smart homes
google.com	risk management
oria.no	risk assessment
sciencedirect.com	smart homes risk management
doaj.org	smart homes risk assessment
academic.research.microsoft.com	smart homes from risk management perspective
getcited.org	smart homes risk
scienceresearch.com	smart homes cyber risk
	smart homes cyber security
	smart homes information security
	cyber security IoT
	information security IoT
	CORAS
	FAIR
	ISRAM
	Octave ALLEGRO
	Ramex
	CIRA
	NIST CSF
	CORAS risk assessment
	FAIR risk assessment
	ISRAM risk assessment
	Octave ALLEGRO risk assessment
	Ramex risk assessment
	CIRA risk assessment
	NIST CSF risk assessment
	government perspective smart homes
	Norway government regulation smart homes
	Norge smart hjem
	Norway society smart homes

In the Table 2 are shown some of the search engines and some of the key words that were used in order to find the literature for the thesis.

4. INTERNET OF THINGS AND SMART HOMES

The aim of this chapter is to describe the basics of the Internet of Things (IoT) and Smart homes (SH) in order to provide better understanding for the chapter 5. The basic principles and overview will be shown without going into details in order not to lose scope. Since SH are part of the IoT, it is necessary to start the explanation with the wider concept to understand the latter.

4.1. Internet of things (IoT)

IoT has been visualized long time ago, but nowadays it is coming to reality and it is developing very fast. The following interview with the famous scientist Nikola Tesla that was already mentioned in the Preface…

“ When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket. “

Nikola Tesla
(Interview with John B. Kennedy in 1926)
(Business insider, 2015)

... describes the wireless systems by the description of things that we are witnessing today. It is important to observe that he gave the interview almost 90 years ago when wireless technologies were pretty unimaginable and IoT concept was far away from its development.

IoT can be in a simplified manner explained as everyday objects that are connected to the internet, identified and possibly communicate with other devices that are as well connected to the internet.

(Fortino & Trunfio, 2014) Or in other words it can be described as devices and objects that are capable of communication and computation, which can address very basic sensor nodes, home appliances as well as the smart phones that are nowadays widely used. The network that consists of such objects is familiar under the IoT concept that is rapidly growing today. (Stojkoska & Trivodaliev, 2017)

4.1.1. History of Internet

The base of IoT is Internet. As Leiner et al. (2009) explains it started its development few decades ago, although some traces of wireless communications in a sense of ideas of concept were set longer time ago. In concrete, the true development of the concept started with the work of Defense Advanced Research Project Agency (DARPA) that started a computer research program in 1962. The key step of DARPA was in 1965 when they connected TX-2 computer in Massachusetts, USA with the other Q-32 computer in California, USA. They were using a low speed dial-up telephone line and that way they created the first small wide area computer network which brought to the conclusions that this way computers could work together very well but there should be another way how to connect them. (Leiner et al, 2009)

As Leiener et al. (2009) further explain in 1967. The ARPANET was founded and published as a computer network concept. In 1969. the first host computer was successfully connected after selecting the Network Measurement Center at the UCLA to be the first node on the ARPANET. The second node became Stanford Research Institute (SRI) and few months later the first host-to-host message was successfully sent. By the end of 1969. four computers were connected through the initial ARPANET and the networking research was and nowadays still is, based on, the incorporation of both the work on the underlying network and on the work on how to utilize the network. In 1970 the initial ARPANET host-to-host protocol was finished and presented under the name of Network Control Protocol (NCP). The problem with NCP was that it was not able to address the networks or machines connected. (Leiner et al., 2009)

As Leiner et al. (2009) further present after improving the NCP protocol the Transmission Control Protocol/Internet Protocol (TCP/IP) was introduced which presented more a communication protocol unlike the NCP that can more be described as a device driver. The initial motivation for

ARPANET and as well Internet was to make possible resource sharing. TCP was implemented first by Xerox Alto and then as well for the IBM PC which proved that different computers could be part of Internet. In the 80's it followed a widespread development of LANs, PCs and work stations which enabled the further development of Internet itself. After introducing LAN, the Domain Name System (DNS) was presented and it provided the possibility of creating an Internet address. By 1985 Internet was established as a community functioning and supported a large number of researchers and developers and slowly started its daily use. In 1995 the term Internet was completely defined as that. And the further development proceeded. (Leiner et al., 2009)

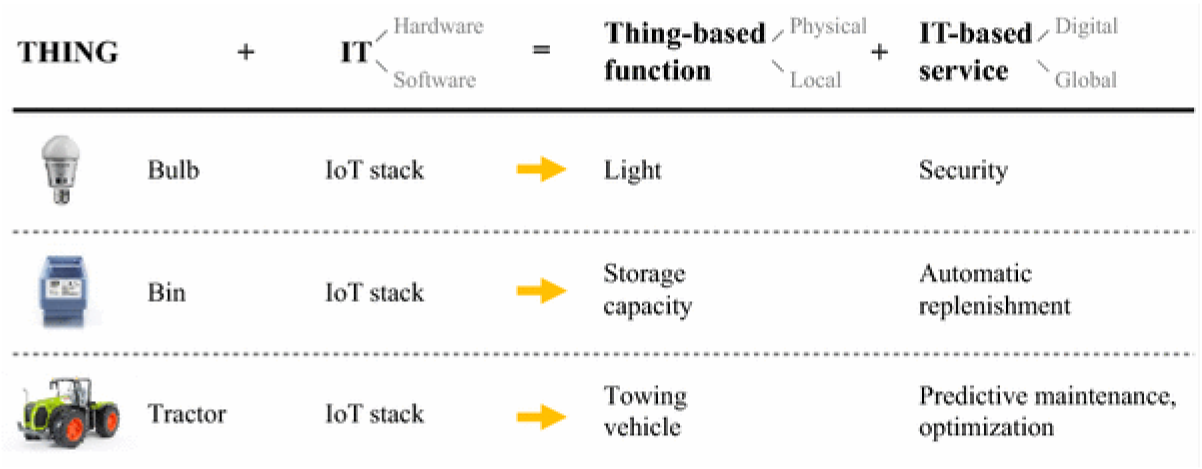
4.1.2. History and development of Internet of Things (IoT)

Internet of Things can be considered as a quite young concept though some basics can be found since the period of telegraph invention in the 1830s and as well the period at the beginning of the 20th century when the first radio voice transmission occurred. (Foote, 2016)

As Foote (2016) further explains some of the first attempts of creating Internet of Things was at Carnegie Melon University in USA where programmers would connect with the internet to the Coca-Cola vending machine that was located at the university in order to see if there was a bottle and if it was cold. After that they would come to take it.

The name of the concept was introduced in the 1999. by Kevin Ashton, the Executive Director of Auto-ID Labs at MIT when he first used the term IoT to describe the concept as it was recognized later on. In that moment IoT concept was based on networked radio-frequency identification (RFID) infrastructures. Further development of IoT naturally proceeded beyond the RFID and continued on a very fast pace. (Wortmann & Flüchter, 2015)

IoT as explained above is just starting it's development in the last decades and it is rapidly developing further. The concept allows through the combination of physical and digital components digitilazing functions and key capabilities of various objects. (Wortmann & Flüchter, 2015)



THING		+	IT Hardware Software	=	Thing-based function Physical Local	+	IT-based service Digital Global
	Bulb		IoT stack	➡	Light		Security
	Bin		IoT stack	➡	Storage capacity		Automatic replenishment
	Tractor		IoT stack	➡	Towing vehicle		Predictive maintenance, optimization

*Figure 6:*IoT product and services logic of functioning. Source: (Wortmann & Flüchter, 2015) based on (Fleisch et al., 2014)

As it can be seen from the Figure 6 the combination of the physical component addresses as the thing, e.g. the bulb, while combining it with digitalization, so by adapting hardware and adding the software component the physical component is not anymore accessible in the physical dimension but in the whole new digital dimension. This way it is enabled to access the simple lightbulb by using the Internet via an application, for example, and to switch on and switch off the lights on demand or on e.g. security basis by giving a command. Also the same can be done with heating, we can demand the heater located at our home to turn on when and from whichever place we want to by giving it a command via Internet. (Wortmann & Flüchter, 2015)

The IoT allows any object to be developed and digitalized and become the IoT object, which by using the Internet, can be accessed and maintained remotely on demand or on a planned schedule. In the Figure 6, it is given the example of the Bin that can be automatically replenished and tractor that can be optimized to usage and predictive maintainance can be done. The field of application is very wide and constrainted almost solely by costs and risks associated considering the rapid growth of technologies that are enabling on every day basis more and more things to be digitalized. (Wortmann & Flüchter, 2015)

Internet of things is developing extremely fast and the largest growth is still expected in the future, International Data Corporation (IDC, 2017) as mentioned before is publishing Worldwide semi-annual Internet of things spending guide which covers the following regions United States, Canada, Japan, Western Europe, Central and Eastern Europe, Asia/Pacific, Middle east and Africa and Latin America. In December 2017 (IDC, 2017) they forecasted that in 2020 the worldwide IoT spending will reach 1 trillion USD (according to current exchange rate 7,8 trillion NOK) in comparison with 674 billion USD spent in 2017.

4.1.3. Internet of Things fields of application

The fields of application of the IoT are various and as well as the concept by itself, they are developing very fast. Some of current and potential fields of application could be the following: (Wortmann & Flüchter, 2015)

- Smart home concept (smart electricity, smart water, smart gas, smart security systems, smart thermostats, etc.)
- Smart transport solutions (vehicle fleet tracking, mobile ticketing)
- Smart health (patients surveillance, chronic disease management)
- Smart city projects (real-time monitoring of parking space, intelligent street lightning) when we take into consideration that by the end of the current decade, over 50% of population is going to be living in cities which would happen for the first time in a human history as described in Cohen (2003) these projects are having significant potential.

4.2. Smart homes

Very often IoT is mentioned together with the smart homes (SH). The development of the IoT has a direct influence on the development of the SH.

The concrete definition of smart homes has evolved in the past few years with the development of the concept itself. There are few definitions that are often mentioned related to the concept and one of them was given by Craven (2017) where he defines a smart house as a house that contains highly advanced automatic systems that can be used for temperature control, lightning, security, multimedia and various other functions related. The key part of the definition is that it contains “highly advanced automatic systems“. (Chan et al., 2008) This part enables the house to have the smart characteristics and makes the distinction between a regular house and a smart house. A smart house is explained as any living or working environment that has been constructed so that it helps and assists people by carrying the required activities. (Chan et al., 2008). Smart homes in different approaches in the field still have the meaning of communication of different electronic devices in the house and by communicating they function as one system as described in Cooper & Keating (1996). They further explain that by granting the access for one application to information and control in another, it enables the intelligent mode of operation between different devices and subsystems. As an example they mention if the security system detects fire during the night, it will raise the fire alarm, but it can as well illuminate the exit route and unlock the doors. This way the whole system is functioning in a smart way.

There are many terms that are being used to describe SH. Here, we will consider “home”, “house”, “household” and “housing” as synonymous, as it was as well described in Chan et al. (2008). There exist terms such as “home systems”, “integrated home systems”, “smart houses”, “intelligent homes” which can as well be considered as synonymous as explained in Cooper & Keating (1996). They further explain that the difference in terms is reasoned by the primarily use of the terms which started with the different companies and consortiums in order to address the type of technology being used for the integration of the system.

4.2.1. History and development of Smart homes

There have been many attempts of creating smart homes with different motives as a background. The following attempts have been described by Chan et al. (2008):

- ACHE was created as an adaptive house which consisted of neural networks used to control the energy. The house was constructed in a way that lightning, temperature control and heating did not have to be prior set up by the residents since the home used the reinforcement learning for the functioning. Reinforcement learning means that the home itself has the ability to observe and analyze the patterns in the environment and adapt to the residents needs in that way
- GATOR TECH smart house is constructed in a way that it has a single operational platform that consists of few individual devices that are equipped with sensors

- ELITE CARE was created with a motivation to help people that suffer from Alzheimer or dementia disease. It is constructed as an assisted living facility that has one or more inhabitants that use the service. The principle on which it is based is that it detects changes in physical and cognitive condition of its residents by using the constant monitoring system
- UBIQUITOS smart home was first designed and developed in Japan. The principle is that the home contains sensors that are used to monitor human behaviors similar as ELITE CARE. In addition it has cameras and microphones that improve the coverage of monitoring by capturing the activities that sensors were unable to captivate. This concept is coming with the idea that the data collected will be used in the future smart homes development in order to improve the whole concept

The fast development of the smart homes in the last years is mainly caused by the development and spreading of internet technology. Wireless networks are the ones enabling the communication between the devices and the usage of the automations system. The smart home automation system is considered to be a key element of the future internet. (Ricquebourg et al. 2006)

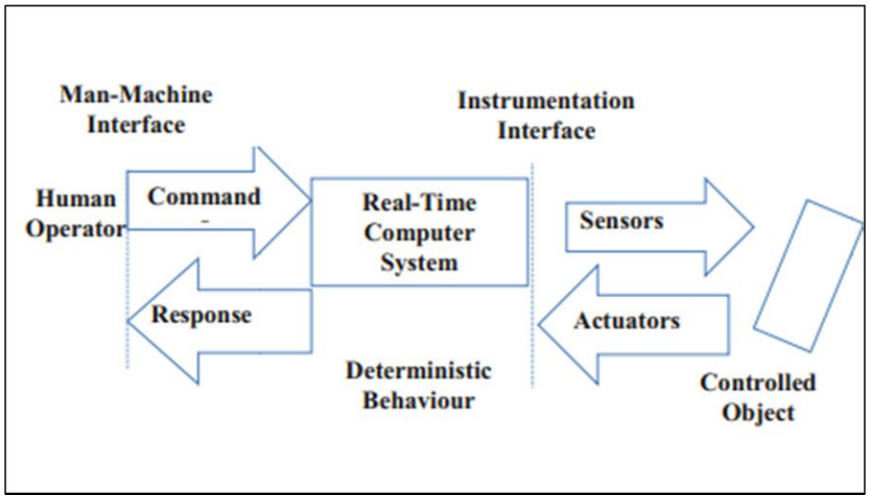


Figure 7: Connection among components of smart home management system. Source: (Suryadevara & Mukhopadhyay, 2015)

Connection between components of the smart home management system is shown in Figure 7. Smart homes unlike “traditional homes” represent the convergence of energy efficient appliances and provide real-time access to energy usage data which is facilitated by network of computers and sensors. (Oksman & Egan, 2010 as seen in Balta-Ozkan, et al., 2013). As Balta-Ozkan, et al. (2013) further explain smart homes provide increased visibility of energy and cost information, for example through interactive displays that provide residents the possibility to monitor and manage energy use actively.

The smart home integration system consists of three crucial entities as it is stated in (Suryadevara & Mukhopadhyay, 2015)

- The physical component (usually electronic equipment, e.g. smart sensors)
- The communication system for connecting the physical components (e.g. wireless network)
- The information which is processed through artificial intelligence program in order to manage and control the smart home integration system

Three main fields that the smart homes are covering are according to Icontrol (2015) as seen in Nesheim & Rosnes (2016) energy, security and health. As they further explain initially the idea of smart homes started with the concept of health support to its residents. The idea was to improve the possibility of disabled and elderly people to live an independent life through the help of the smart home. According to the trend of the increasing number of the elderly population especially in the developed countries, it is necessary to improve their quality of life and decrease the costs affecting the healthcare system as well. Some of the devices that support the health component of the smart houses are smart watches that measure the number of steps of the resident, the heart rate, pulse, than smart beds that automatically adjust to the person, calories trackers that help the nutrition improvement, smart bracelets that help the tracking of the movement of people suffering from dementia or Alzheimer disease. (Icontrol 2015 as seen in Nesheim & Rosnes 2016)

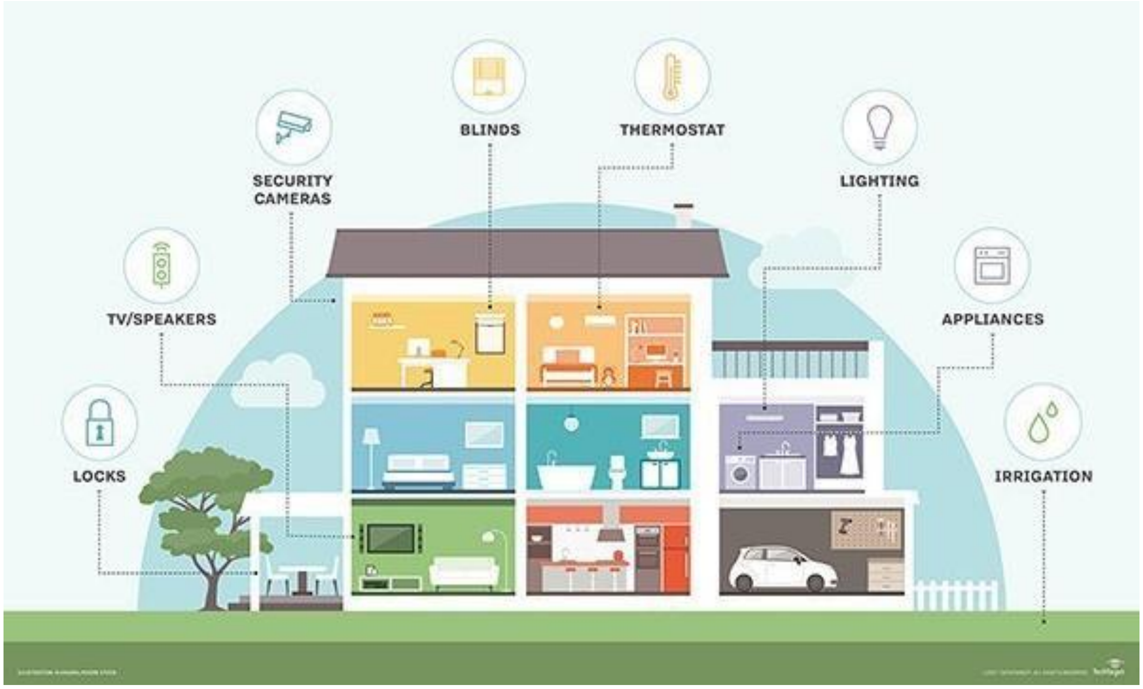


Figure 8: Smart home example. Source: TechTarget (2017)

In the Figure 8 above, it is shown the example of a smart house and some of the components that can be included. The components and the system can vary and in the future they will further develop.

4.2.2. Smart homes fields of application

As Chan (2009) explains smart homes can as well improve the quality of life and assist people with reduced physical functions and lower the social isolation as one of the important challenges they encounter. Some of the fields of application are the following:

4.2.2.1. <u>Energy efficiency</u>

Although smart home automation systems were initially designed to improve energy efficiency their scope of influence expanded rapidly. (Jacobsson et al. 2016)

Figure 9: Energy saving smart home. Source (Kaf Mobile Homes, 2018)

In the Figure 9 above it is shown how a smart home can be constructed to support energy efficiency by using solar panels and clean energy.

4.2.2.2. **Environment monitoring**

Smart home automation systems are usually equipped with a large number of surveillance cameras that monitor the whole internal and external environment, or more often complete external environment and parts of internal environment. As Jacobsson et al. (2016) explain surveillance cameras can be used to detect or to verify fires from distant locations. Usually these cameras that are supposed to detect and note if there is really a fire danger are located in critical areas close to the entrance doors or in bedrooms or kitchen.

The other usage apart from fire monitoring can be as well in the field of childcare for the parents that are for example on a lunch break to be able to monitor the house and see what their children are doing and if they are exposed to some kind of danger in case they are home alone.

As well there is an important usage regarding water leaks that can be noticed on time or confirm if there were any water leakages during the time of family vacation, for example, when no residents are at home. It is as well possible to use the surveillance cameras together with some sensors or other devices in order to create a complete picture of risk. (Jacobsson et al. 2016)

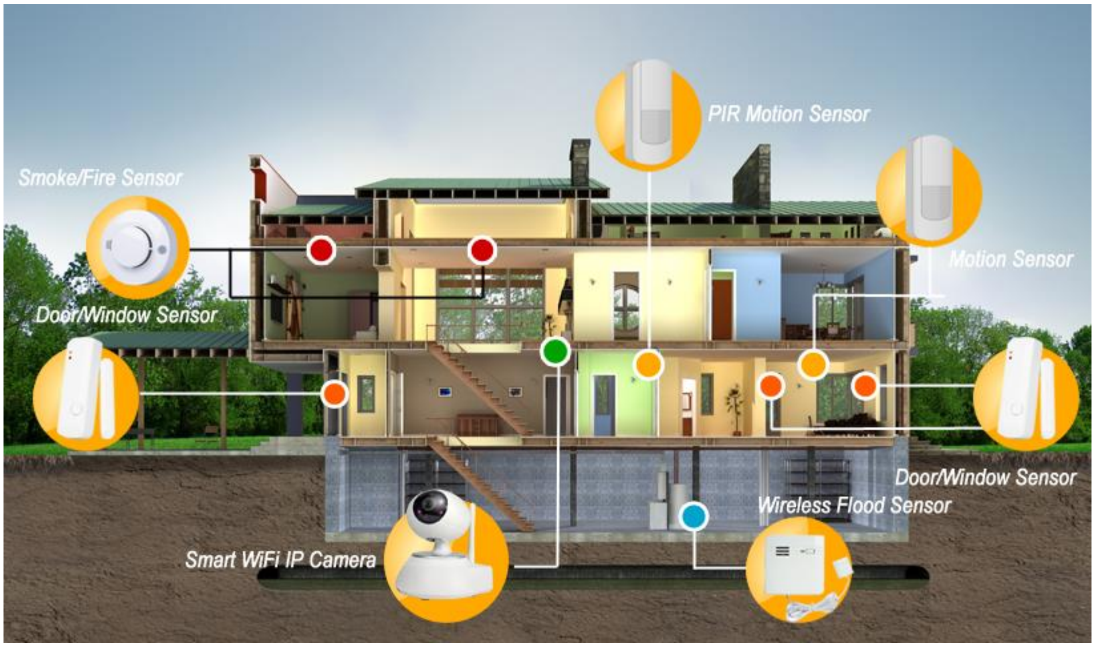


Figure 10:Smart home monitoring system. Source: (Unifore, 2015)

In the Figure 10 the example shows some of the smart home monitoring possibilities by using Wi-Fi IP cameras, motion sensors and similar.

4.2.2.3. Special needs supporting

When it comes to special need supporting, one of the important fields of appliance might be for independent living communities for children and adults that are in need for special care. For example there are a lot of communities for children experiencing some development difficulties when they reach certain age and can live partly independent together in one home with surveillance. In this case SH is extremely helpful because it can provide them with additional comfort and independence without putting their security into danger. As described in Chan et al. (2008) smart homes or modern sensor-embedded houses not only can they help people with reduced physical functions, but also assist with the social isolation that they face and provide them with assistance without changing their everyday routine, and, this way providing them with larger comfort and well-being.

4.2.2.4. Elderly population supporting

When it comes to elderly communities or elderly people living independently in their apartments, SH can be very helpful. In the context it should be considered that the population in many countries is aging rapidly and assistance should be provided. In USA, currently, approximately 15% of population is older than 65 (cca. 46 million people), but according to the estimates by 2030 it will reach 21% and further by 2060 24% (cca. 98 million people) which is a significant increase (Colby & Ortman, 2017). According to the estimation done by Cohen (2003), global population, by 2060 when it comes to people aged 60 and older, is going to come to the rate of 21,4%. As he explains the 20th century according to the data available, it would be probably the last century in which younger population has outnumbered the older population.

As explained in Chan et al. (2008), technology can help in avoiding the institutionalizing older people costs. In the 80s that was achieved with the appearance of different portable devices, such as small transmitters that could be carried around the wrist or neck and help elderly people send an emergency signal and today this is achieved by smart homes. The concept of home-based eHealth has been introduced by Demiris (2004) and further explained in Chan et al. (2008) which connects the terms of electronic home healthcare and the smart home. As Demiris (2004) explains this way home-based disease management and monitoring is enabled. One of the challenges, as he states, is in providing the privacy and confidentiality of the medical and private data.

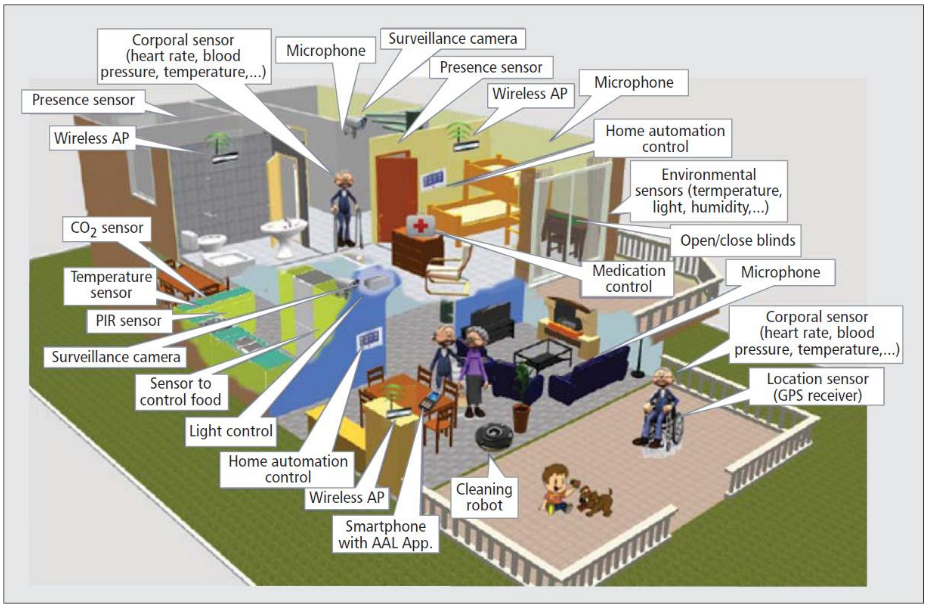


*Figure 11***:** *Elderly population supporting Smart home example. Source: AAL (2016)*

As it can be seen on the Figure 11 it is shown an example of a smart home when applied for the elderly population support. This type of smart home can be further developed by adding more sensors and cameras. This way, elderly people get adequate support and yet independent life quality.

5. SMART HOMES FROM RISK MANAGEMENT PERSPECTIVE

When it comes to Smart homes, it is very important to manage the risks related to them very carefully and with full attention. This is due to the fact that SH are creating large amount of extremely sensitive information about the home residents and their habits that can be misused if they are not used for the purpose that they were collected for. Jacobsson et al. (2016) notice that it is very significant to assess all possible risks while designing and constructing the SH and as well emphasizes the need of setting standards regarding the scope of the autonomous decision-making by all the SH vendors. This should be done in order to provide better risk management and to lower the vulnerabilities of the SH.

5.1. Necessity of analysis of the existing risk assessment methods

As it was explained by Karabacak & Sogukpinar (2005) regarding information security risk assessment, researchers had experienced problems and difficulties when attempting to apply traditional risk assessment methods in information security field which can be a conclusion when it comes to these types of methods for all the other fields in general as well. When it comes to qualitative oriented methods usually the difficulties are in inconsistency of the results due to strong correlation with the ideas of the analyst so the results often have a subjective character. From the other side, quantitative methods are not practical for complex systems such as information systems due to their complicated structure and inability of modelling highly complex risk scenarios (Karabacak & Sogukpinar, 2005). Enabling and enforcing security when it comes to IoT environments is one of the highest barriers for further development of the smart homes. It is as well important to note that SH are developing extremely fast but as in ways that are very difficult to predict. The system is completely not static but rather completely dynamic with all the time changes. (Jacobsson, et al. 2016)

As a starting point of analysis and improvement suggestions of risk assessment methods suitable for SH, it is important to analyze the existing methods related to information and cyber security in order to avoid some weaknesses of the existing methods and to try to use and improve good characteristics of them.

The reason for analysis of the existing methods and suggestions for improvement instead of using a “greenfield“approach is in the benefits that it has. This way, by analyzing different existing methods that are in the use, it is possible to observe all the strengths and weaknesses and as it was visible from the analysis some are repeating in various methods. Hence this way by conducting the approach of analysis of different methods it is as well the prevention of the same mistakes or the same weaknesses that existing methods already have. Since the improvements are being suggested based on the literature review and not in a cooperation with a company on a concrete example where it would be far simpler to test it and see all the implications it has, this approach is the most beneficial.

5.1.1. Analysis of the existing risk assessment methods

There exist several methods that are widely used in information or cyber related risk assessment and therefore are useful for SH risk assessment to some extent as well. Primarily, they are combining qualitative and quantitative analysis in order to get the best results since technology based risks are developing extremely fast following the development of technology itself. Other approaches normally include more quantitative oriented tools. Some of them are supported with a software package as it was mentioned in Karabacak & Sogukpinar (2005). On the other side, risk analysis methods that are executed completely without the assistance of software are referred as paper-based methods (Gordon, 1992 as seen in Karabacak & Sogukpinar, 2005). Some of the risk assessment methods used combine the risk assessment matrix and questionnaires, where in the risk matrix risks are defined as low, medium or high, whereas in questionnaires, risk scale is used for ranking. (Munteanu, 2006)

There are many risk assessment methods and methods used and many of them are focusing on adapting to fast changes in the field. Agrawal (2017) discusses CIRA, CORAS, ISRAM and IS methods as most relevant for the IS risk assessment. Karabacak & Sogukpinar (2005) as well suggest ISRAM as a method for information security risk assessments. In Bako (2016) we can see the whole explanation of OCTAVE Allegro approach which is used as risk assessment tool for a smart home example. FAIR Institute developed FAIR risk assessment framework. Shukla &

Kumar (2012) compare and discuss OCTAVE, CORAS, ISRAM and CORA. Below are listed these and some other methods found in literature that are related to information security or cyber security risks which are emphasized in the thesis related to the SH. There exist more methods that are in use, but after literature analysis based on scientific articles, books available and internet search, the following methods were mentioned as the most used ones or most significant ones. Some methods that will be presented were further developed through the years and adapted to the high pace technology development but most of the methods presented were developed completely in the past few years.

It will be presented how the methods are functioning and then the strengths and weaknesses of the methods would be drawn.

5.1.1.1. OCTAVE Allegro

OCTAVE is short for Operationally Critical Threat, Asset and Vulnerability Evaluation methodology. The development of the method started with OCTAVE, continued with OCTAVE-S version and current version is OCTAVE Allegro methodology. It is focused on positioning risk assessment in an adequate organizational context, but it provides an alternative approach to the information assets and the resilience related to them. It as well primarily focuses on information assets with emphasize on how they are stored, transferred, processed and how they are exposed to threats, vulnerabilities and disruptions as a result.(Caralli et al., 2007). The OCTAVE framework was first published by the Software Engineering Institute (SEI) and Carnegie Mellon University in 1999. (Alberts et al.1999 as seen in Caralli et al., 2007).

The OCTAVE Allegro method as explained in Caralli et al. (2007) consists of a method implementation guide (procedures, guidance, worksheets, information catalogs) and training. It is conducted in a series of workshops that is managed by an interdisciplinary analysis team including members from various organizational parts of the organization. (Alberts & Dorofee, 2002 as seen in Caralli, et al. 2007).

The OCTAVE Allegro method is initially designed for organizations that (Caralli et al., 2007):

- Are having more than 300 people but it is adapted in the Allegro version as well for individuals who want to run a risk assessment without organizational environment.
- Have a multi-layered hierarchy
- Are administrating their own IT infrastructure
- Are in condition of running vulnerability evaluation tools
- Are in condition of result interpretation of vulnerability evaluations
- Organizations can adapt the method to their specific environments by tailoring it

The approach as described in Figure 12 below consists of eight steps divided in four phases as explained in (Caralli et al., 2007). During the first phase, the risk measurement criteria that is consistent with organizational drivers is designed and developed. In the second phase profiling of critical information assets is conducted. Following with the phase three where threats to the information asset are identified from the aspect of the asset storage location, transfer or process. And in the fourth and the final phase risks related to information assets are identified and analyzed and the selection of mitigation approach is being done.

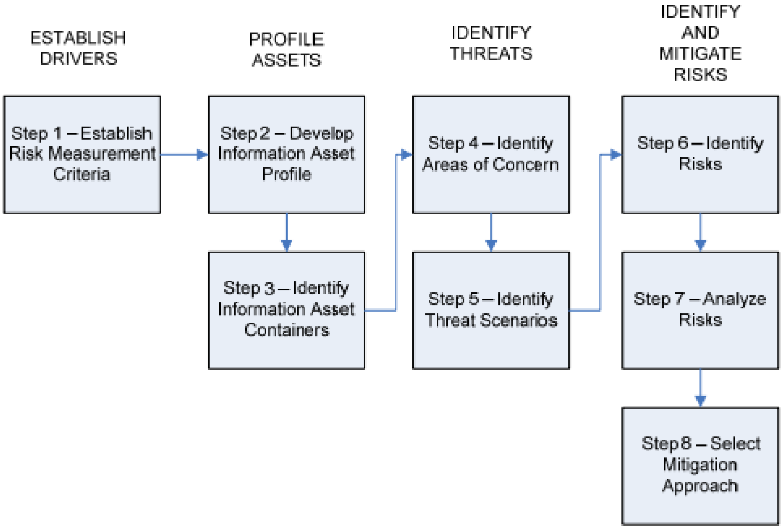

ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Figure 12: OCTAVE Allegro steps. Source (Caralli et al., 2007)

OCTAVE Allegro method has its strengths and weaknesses. Some of them summarized are the following:

STRENGHTS

- It is free for use (Bako, 2016)
- The fact that various organizational units are working together it gives wider risk picture
- Its complexity provides different perspectives through filling the worksheets (Bako, 2016)

WEAKNESSES

- Complexity. Due to many worksheets, it has a large amounts of documentation in case of assessing more complex risks (Bako, 2016)
- Since it is solely qualitative method it can have some amount of inconsistency and subjectivity of the analysts

5.1.1.2. FAIR

FAIR is acronym that stands for Factor Analysis of Information Risk. FAIR is considered to be the only international standard quantitative method made for cyber and operational risks. (FAIR Institute, 2016) FAIR was established in 2005 by Risk Management Insight LLC. The FAIR Framework is shown graphically on the Figure 13.

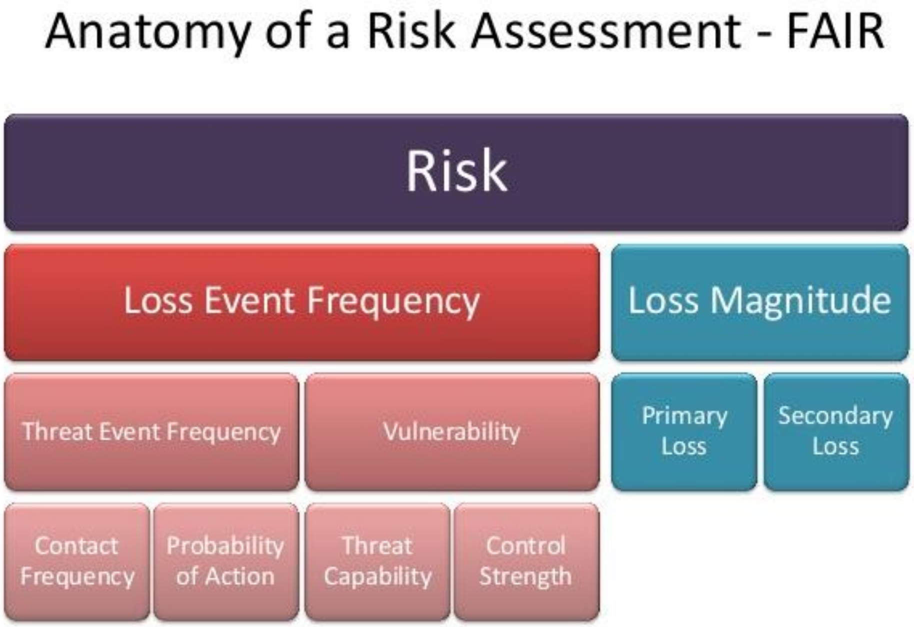


Figure 13: FAIR Framework (FAIR Institute, 2016)

Following strengths and weaknesses can be considered in a case of FAIR:

STRENGTHS

- Easy to understand since it is underlined with the logic of thinking (FAIR Institute, 2016)
- Relatively defendable results (FAIR Institute, 2016)

WEAKNESSES

- Complex to use
- Difficult to apply in absence of metric data
- Inconsistent and not precisely defined terminology (RSA Conference, 2014)
- Checking results is complex

5.1.1.3. NIST CSF

NIST RMF stands for National Institute of Standards and Technology's Risk Management Framework. Further on NIST developed the NIST CSF which stands for Cybersecurity Framework and thus it is far more interesting for this thesis than the general NIST RMF (NIST, 2016)

NIST CSF was first published in 2014 which means that it is quite up to date and as it has been explained by The National Institute of Standards and Technology (NIST, 2016), today, it has been used in many large companies in order to assess cyber security risks. It focuses on five functions of the cyber security management which are to identify, protect, detect, respond and recover and each of the categories has further subcategories that are paired with an appropriate list of standards. The intent is that companies create their profiles based on their business requirements, risk tolerance and available resources and classify themselves in the Tier (Tier 1 – Partial to Tier 4 which stands for adaptive). (NIST, 2016)
NIST CSF framework is graphically shown on the Figure 14.

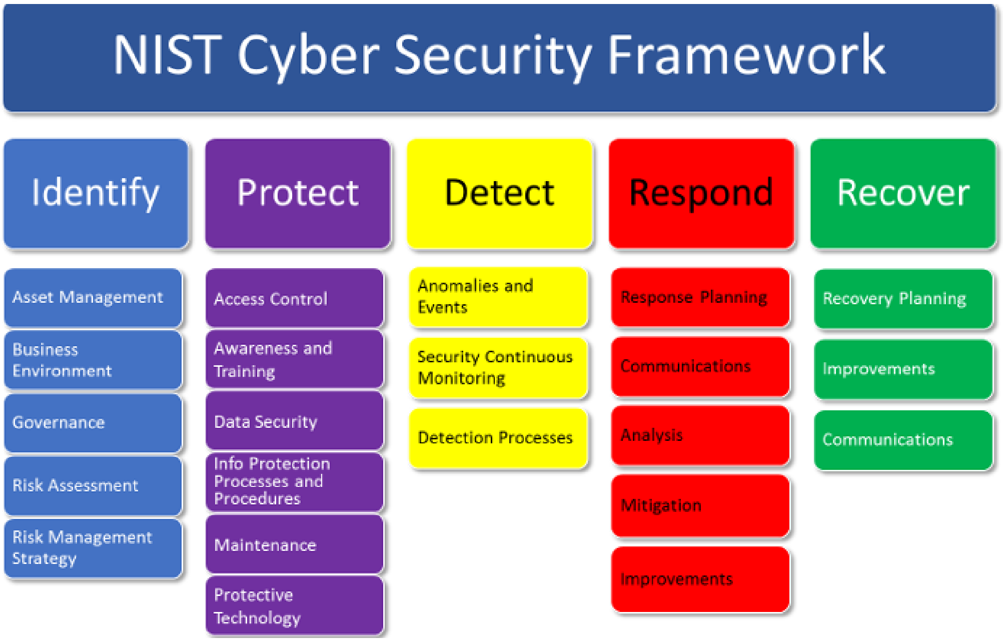


Figure 14: NIST CSF. Source: (Northstar Technology group, 2016)

Following strengths and weaknesses shall be taken into account when considering NIST CSF as the method for risk assessment:

STRENGHTS

- It uses systematic methodology and a common language for cybersecurity risks treatment (NIST, 2016)
- It is easily adapted to any organizational needs and specificities (NIST, 2016)
- It enables scalability
- It can be used in organizations of any size (NIST, 2016)
- It is concise and efficient

WEAKNESSES

- Unclear which metrics should be used for measurement because it is required from the users to define their own metric system

5.1.1.4. RaMEX

It is a qualitative tool used for risk assessment and it does not take into account any mathematical or statistical instruments. (Karabacak & Sogukpinar, 2005). The procedure of the tool goes in following seven steps (Kailay & Jaratt, 1995):

- Identification of assets (physical environment, hardware, communications, software, information, personnel and procedures)
- Identification of threats (natural disaster, local accident, global accident, unintentional employee action, intentional employee action, intentional non-employee action)
- Identification of vulnerabilities (inadequate back-up procedures, insecure input/output procedures, lack of management support related to security, inadequate software/hardware maintenance, insecure communications software, ineffective physical access control)
- Identification of existing security countermeasures (avoid the risk, reduce the threat, reduce the vulnerability, reduce the impact, detection, recovery)
- Business impact assessment (loss of personnel, loss of equipment, complete business failure and similar)
- Assessment of security countermeasures (they take into account vulnerability, strength and impact severity levels)
- Report generation

The information about the system and the environment is gathered in a form of an automated menu-driven questionnaire (Kailay & Jaratt, 1995).

STRENGHTS

- Simple to use automated menu-driven questionnaire

WEAKNESSES

- Not updated and adapted to the current needs of information or cyber risk assessment

5.1.1.5. ISRAM

As Karabacak & Sogukpinar (2005) explain normally two independent and separate survey processes are being conducted for the two risk parameters given in the formula below. The preparation and execution of the survey and analysis of its results are done in the well-defined steps that are mathematically represented in the formula below. The value, the unit of “risk“ is given as the result in the values, usually from 1 to 25. The surveys used for the ISRAM method are composed of questions and answer choices that are in a relation with the IS problem. As explained in Shukla & Kumar (2012) ISRAM complies to following standards: NIST SP 800-30, ISO/IEC 17799 and ISO/IEC 13335.

ISRAM as explained in Karabacak & Sogukpinar (2005) is based on the following formula:

$$\begin{aligned} Risk\ &= Probability\ of\ occurance\ of\ security\ breach \\ &\quad \times Consequence\ of\ occurance\ of\ security\ breach \end{aligned}$$

The risk method deducted from the formula above comes in the following formula (Karabacak & Sogukpinar, 2005):

$$\text{Risk} = \left(\frac{\sum_{m} \left[T_1 \left(\sum_{i} w_i p_i \right) \right]}{m} \right) \left(\frac{\sum_{n} \left[T_2 \left(\sum_{j} w_j p_j \right) \right]}{n} \right)$$

The formula consists of i – the number of questions for the survey of probability of occurrence, j – the number of questions for the survey of consequences of occurrence, m – number of participants in the survey of probability of occurrence, n – number of participants in the survey of consequences of occurrence, wi, wj – weight of the question i, j; pi, pj – numerical value of the selected answer choice for question i, j; T1 – risk table for the survey of probability of occurrence, T2 – risk table for the survey of consequences of occurrence, Risk – single numeric value

ISRAM consists of the following steps:

- Awareness of the problem
- Listing and weighing the factors

- Converting factors into questions, designating answer choices and assigning numerical values to answer choices
- Preparation of risk tables
- Conduction of the survey
- Application of the formula given and obtaining a single risk value
- Assessment of the results

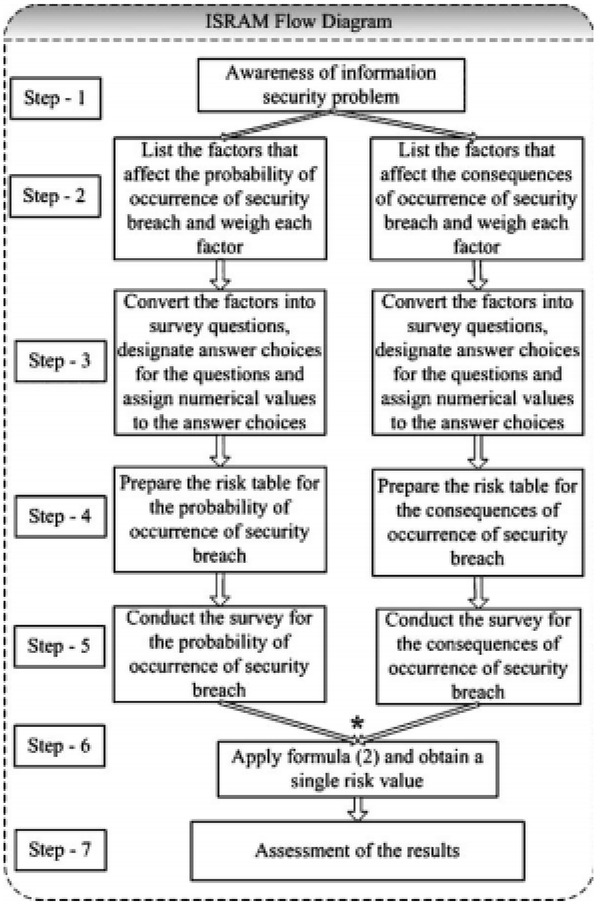

ISRAM Flow Diagram
Step - 1
Awareness of information security problem
Step - 2
List the factors that affect the probability of occurrence of security breach and weigh each factor
List the factors that affect the consequences of occurrence of security breach and weigh each factor
Step - 3
Convert the factors into survey questions, designate answer choices for the questions and assign numerical values to the answer choices
Convert the factors into survey questions, designate answer choices for the questions and assign numerical values to the answer choices
Step - 4
Prepare the risk table for the probability of occurrence of security breach
Prepare the risk table for the consequences of occurrence of security breach
Step - 5
Conduct the survey for the probability of occurrence of security breach
Conduct the survey for the consequences of occurrence of security breach
Step - 6
*
Apply formula (2) and obtain a single risk value
Step - 7
Assessment of the results

Figure 15: Basic flow of the ISRAM. Source: (Karabacak & Sogukpinar, 2005)

All the steps of the ISRAM method are shown on the Figure 15**.**

STRENGHTS:

- Unlike many quantitative methods ISRAM does not use any complicated mathematical or statistical instruments (Agrawal, 2017)

- If conducted with careful operation it provides objective results (Karabacak & Sogukpinar, 2005)
- It does not have rigid frames (number of questions and similar can be adapted to the situation)
- No need for expert participation, enough to have standard skills (Agrawal, 2017)
- It is not costly (Agrawal, 2017)
- Complies to various standards (Shukla & Kumar, 2012)

WEAKNESSES:

- Time consuming with filling both questionairres
- Completely subjective classification (Agrawal, 2017)
- Complex to use (Shukla & Kumar, 2012)
- Risk = Expected consequences (Flage, 2018)

5.1.1.6. CORAS

As described in Agrawal (2017) CORAS addresses Information security risks by using a qualitative approach. It was first developed under the Information Society Technologies program (IST). As Agrawal (2017) further explains the methodology is based on UML language that uses diagrams to describe relationships among users and environment. The method suggests eight steps in total. CORAS complies to following standards: ISO 31000, ISO/IEC 17799, AS/NZS 4360. (Shukla & Kumar, 2012)

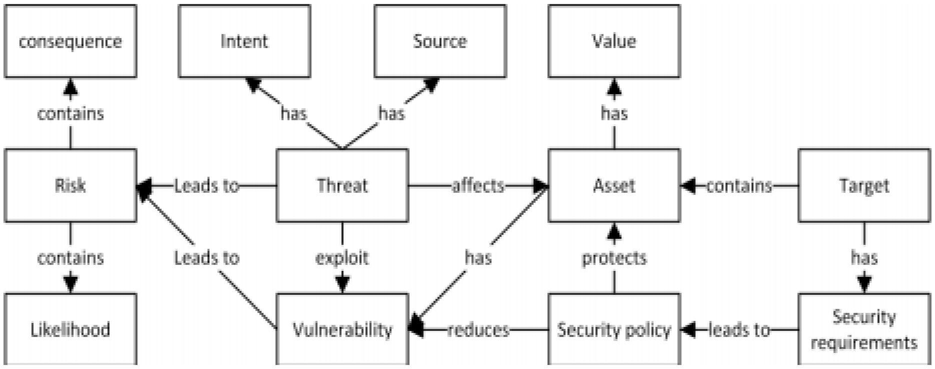


Figure 16: CORAS basic ontology. Source (Agrawal, 2017)

On the Figure 16 it can be seen the basic ontology of the CORAS method. The Target consists of Assets that have some Value and Security requirements which lead to Security policy which helps in reducing Vulnerabilities and protecting Assets. Assets can consist of one or more Vulnerabilities, whereas Threat has specific Source and Intent. Threat and Vulnerability together may rise Risk level that has a certain Likelihood and Frequency. (Agrawal, 2017)

As detailed explained in Agrawal (2017) the method in first four steps enables common understanding of the target analysis by determining the scope and focus of the analysis and giving the overall description of the target. The latter four steps are focused on the more detailed analysis by identifying concrete risks and risk levels and identifying and assessing potential treatments for the risks described as unacceptable.

STRENGHTS:

- Integrates a number of risk analysis techniques as Hazop, FMEA, FTA, etc. by underlying data structure (Vraalsen et al., 2004)
- It gives the analyst freedom in selecting analysis methods and modelling techniques depending on the target and security issues that are analyzed (Vraalsen et al., 2004)
- Complies with various international standards (Shukla & Kumar, 2012)

WEAKNESSES:

- It is complex and demands expert participation thus expensive (Agrawal, 2017)
- It is time consuming since it is necessary to identify assets, vulnerability, threat scenario, risk (Agrawal, 2017)
- Difficult to assess scalability (Vraalsen et al.. 2004)

5.1.1.7. CIRA

CIRA stands for Incentives Risk Analysis. As explained in Agrawal (2017) it was developed in 2014 in Norway on Gjøvik University College by Rajbhandari and Snekkenes.

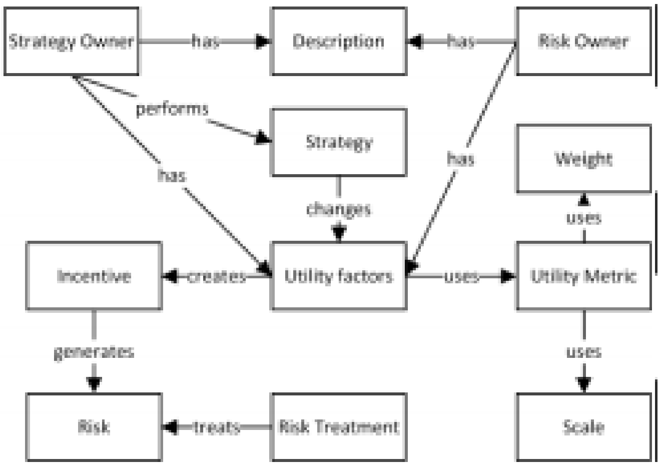


Figure 17: CIRA basic ontology. Source (Agrawal, 2017)

As it can be seen from the Figure 17 and as explained in Agrawal (2017), the Risk owner and Strategy owner are defined with the Description. Strategy owner further performs some Strategy that modifies Utility factors of both Risk and Strategy owners. Utility factor uses Utility Metric which as its part has Weight and Scale in order to compute its value. The change in Utility factors generates Risk in the system which can be treated with use of Risk treatment methods.

STRENGHTS:

- Insight and understanding of what motivates actors to contribute in the process and circumstances that can lead to adverse actions is obtained which improves decision making (Wangen, 2015)

WEAKNESSES:

- It is complex and demands expert participation thus expensive (Agrawal, 2017)
- Extremely time consuming (Agrawal, 2017)
- It is not compliant with any regulation or IT standard (Agrawal, 2017)

Apart from the more formal and shaped methods that were presented above, there exist various discussions and method recommendations that are not completely developed but can be found in literature as well. Denning & Levy (2013) as seen in Jacobsson et al. (2016), provides the suggestion of method that relies on three components. They are the feasibility of conducting an attack, the attractiveness of a system as a compromised platform and the damage caused by the attack execution. The damage caused by the attack execution in this case provides the measure to weigh the overall risk whereas the first two components when combined together provide the indication of likelihood of the initiating event occurring. As Jacobsson et al.(2016) explains, this framework provides a skeleton of risk characterization. The limitation is that people that are not having risk related prerequisite knowledge will encounter difficulties when acquiring the method. Djemame et al. (2011) has done research on the risk assessment frameworks and they established a framework and a software toolkit for cloud service ecosystems and the digital home was presented as an example. The framework offered comprises risk into four categories: legal, technical, policy and general. It is interesting as concluded by Jacobsson et al. (2016) that this approach excludes the normally important user perspective which has to be central to any smart home risk analysis.

In the following Table 3, an overview of all previously analyzed risk assessment methods will be offered. The table structure would provide a simpler overview of the characteristics of the offered methods in one place.

Table 3: Overview of analyzed risk assessment methods suggested for SH risk assessment. Based on: (Bako, 2016), (Agrawal, 2017), (FAIR Institute, 2016), (NIST, 2018), (Caralli et al., 2017), (Karabacak & Sogukpinar, 2005), (RSA Conference, 2018), (Wangen, 2015)

Suggested method	Methodology	Level	Time	Strengths	Weaknesses
OCTAVE Allegro	Qualitative	Standard	Medium time-consuming	It is free for use	Complexity - many worksheets
				Wider picture - various organizational units are working together	Inconsistency and subjectivity to some extent
				Different persp. – w.sh.	
FAIR	Quantitative	Specialist	Medium time-consuming	Underline with logic of thinking - easy to understand	Complexity
				Defendable results	Non-applicable without metric data
					Inconsistent terminology

Suggested method	Methodology	Level	Time	Strengths	Weaknesses
NIST CSF	Qualitative	Standard	Medium time-consuming	Systematic methodology and a common language use	Users define their own metric system - unclear
				Easily adapted to any size and specificities of organization	
				Enables scalability	
				Concise and efficient	
RaMEX	Qualitative	Standard	Medium time-consuming	Simple to use - automated menu driven questionnaire	Not updated
ISRAM	Quantitative	Standard	Medium time-consuming	No complex mathematical and statistical instruments	Time consuming due to two questionnaires
				If conducted carefully it provides objective results	Subjective classification
				No rigid frames	Relatively complex to use
				Not costly	Risk = Expected consequences?
				Complies with various standards	
CORAS	Qualitative	Specialist	Extremely Time-consuming	Integrates a number of risk analysis techniques	Complex, expert participation
				It gives freedom to analyst in selecting analysis methods and modelling techniques	Expensive
				Complies with various standards	Time consuming
					Difficult to assess scalability
CIRA	Qualitative	Specialist	Extremely Time-consuming	Insight and understanding of motivation of actors and circumstances	Complex, expert participation
					Expensive
					Time consuming
					It does not comply with any standards

Further analysis of the strength and weaknesses will be conducted in the following Subchapter from three different perspectives with the discussion and conclusion following.

5.2. Risk Management Perspectives

The importance of different perspectives in which smart homes and as well risk assessment of smart homes should be observed can be seen at Balta-Ozkan, et al. (2013) where it is explained that the development of smart homes should be observed through the following frameworks:

- Policy (incentives which enable the technology uptake)
- Regulatory (consumer data access, frequency of access, enabling emergence of new actors and services)
- Commercial and market and investment conditions (funds for the installation of communications and grid infrastructures)

We can set different perspectives from many points of view, but in this thesis, we will observe three perspectives and those are individual, society and governmental. In the following subchapters we will further explain these perspectives and analyze the offered risk assessment methods from those three perspectives and suggest some improvements and recommendations on which methods could be used from which perspective.

5.2.1. Individual perspective

Individual perspective is oriented towards a standard resident of a smart home and influences what potential risks can have on the quality of their life. For the individual perspective it is very important to consider the resident in a way of limitations, since residents do not have to obtain any deep knowledge regarding risk management which automatically excludes any complicated risk assessment methods for individual use. The method that a single resident can use to conduct a risk assessment of its own SH should be simple, yet wide enough to cover all the necessary risks that can affect their privacy or in any sense affect their being.

Wilson et al. (2017) had made a questionnaire based research between the potential and current users of smart home technologies in order to get as a result the risks that individuals are the most concerned about. The perspective of a single resident, by assumptions, lies on the following risks that are the field of their concern given in the Figure 18.

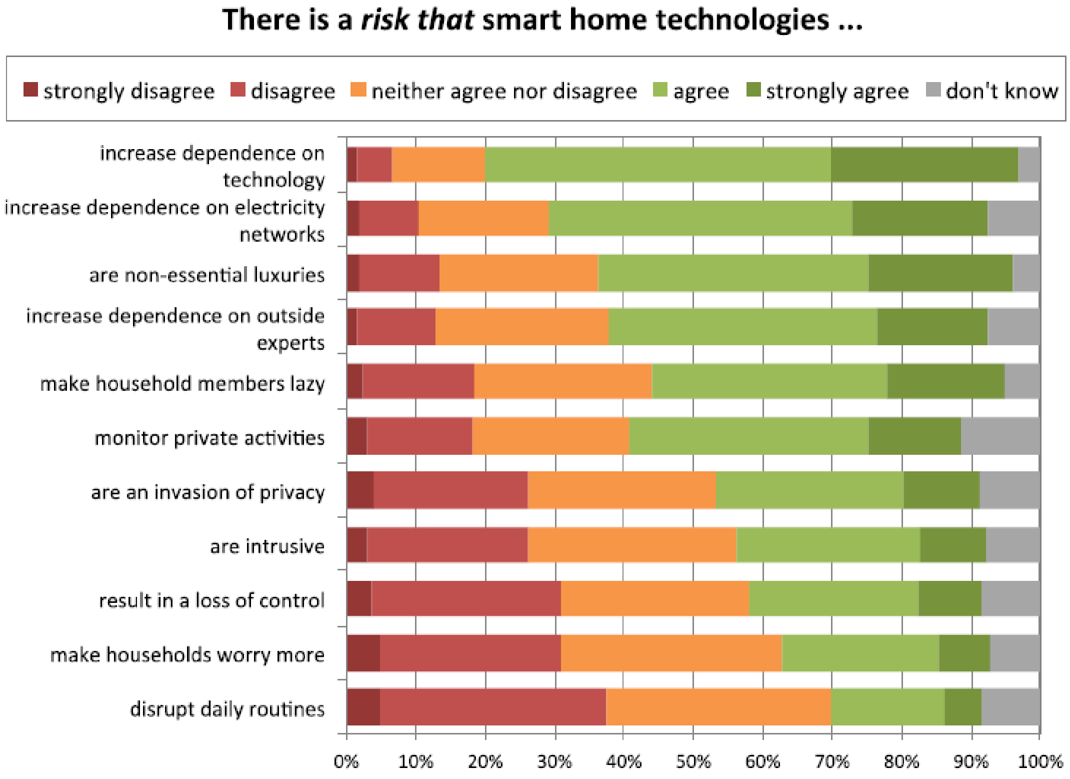


Figure 18: The main risks to the smart home technologies according to individual people answers on the survey conducted. Source: (Wilson et al., 2017)

As it can be seen in the Figure 18 by Wilson et al. (2017), the risks that mostly were worrying individuals, when it comes to smart home technologies, were the increase of dependence on technology, the increase of dependence on electricity networks, that they are non-essential luxuries, the increase dependence on outside experts, making household members lazy, etc. As we can see in the first five risks marked, there are mostly the risks based on general settings, apart from the awareness of dependence on outside experts, whereas most concrete risks, as monitoring private activities, invasion of privacy, intrusivity, loss of control are marked as not so relevant and they can be found in the lower part of the graph. These results show that individuals are probably more concerned about the positive effects of the smart home technologies than about the negative sides that can affect their privacy, security and finances.

In Table 4 are shown some of the most important vulnerabilities and threats associated with the cyber related risks from the perspective of an individual resident of a smart home. We can conclude that the consequence categories that were presented before as our main focus in objectives: monetary loss, data loss and data misuse are present in all of the vulnerabilities stated in the table.

Table 4: Vulnerabilities related to SH with focus on cyber risks from the individual perspective. Based on: (Juvigny, 2016)

Vulnerabilities	Threat/Consequence categories	Level of importance	Historical data or example
Security flaw on a smart device	Privacy invasion/possible monetary loss, data loss and data misuse	HIGH / information collected by sensors, cameras and other devices	2014 - a hacker succeeded in overtaking baby monitor/
Wi-Fi security lack	Privacy invasion/ possible monetary loss, data loss and data misuse	LOW / possible overtaking of whole network, but reasonably low due to precautious measures since Wi-Fi protection is usually on high level (known threats)	by accessing the information transferred between equipment hackers would gain access to whole network
Lack of consumer awareness	Smart device hijacking/ possible monetary loss, data loss and data misuse	HIGH / extremely high possibility of identity usurpation	2015 - Imperva the security company revealed that 900 of their control cameras had been converted into a botnet
Default bad conception of the smart device	Smart device stops working/ possible monetary loss, data loss and data misuse	HIGH / in case of bad design or problems in the design phase	2015 - NEST company lost control over its devices for several hours

5.2.1.1. <u>Analysis of the offered methods from the individual perspective</u>

In the Table 5 it is shown the comparison of the presented risk assessment methods, like earlier in the Chapter 5, now from the individual perspective. Methods highlighted in orange are excluded as non-applicable from the individual perspective as it can be seen in the table and text following:

Table 5: Comparison of risk assessment methods for SH from Individual perspective. Based on Table 3

Suggested method	Methodology	Level	Time	INDIVIDUAL PERSPECTIVE
OCTAVE Allegro	Qualitative	Standard	Medium time-consuming	**It is free for use, complexity is avoided since it is individual user thus it cannot be too many worksheets, but therefore different perspectives cannot be achieved**
FAIR	Quantitative	Specialist	Medium time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**
NIST CSF	Qualitative	Standard	Medium time-consuming	**Common language, concise, enables scalability, can be confusing due to creation of their own metric scale since it is an individual user without prerequisite knowledge**
RaMEX	Qualitative	Standard	Medium time-consuming	**Simple, but not updated**
ISRAM	Quantitative	Standard	Medium time-consuming	**No complex mathematical and statistical instruments, no rigid frames thus adaptable to the SH specificities, two questionnaires are not so feasible when it is an individual resident, complex and time consuming, risk=expected consequences**
CORAS	Qualitative	Specialist	Extremely Time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**
CIRA	Qualitative	Specialist	Extremely Time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**

As it can be seen FAIR, CORAS and CIRA are marked orange and their strengths and weaknesses from this perspective were not taken into account, since in the analysis of the risk assessment methods they were already marked as demanding specialist level, which means that individual resident would not be able to use them without assistance of an expert. The other methods are presented and we can discuss their appliance from the perspective of individual resident of the smart home.

OCTAVE Allegro method is a qualitative method which is free to use and enables application of different perspectives through different worksheets. This characteristic is good when we have an organization where different departments would fill different worksheets in order to influence the objectivity of the method. In the case of the SH resident that is not the case. We could say that each family member could fill out different sheets but even then the objectivity would not be achieved since sometimes there will be no more family members or there will be children or similar. NIST CSF from the other hand provides systematic methodology with common language that can be quite beneficial for an average resident that does not have any specific knowledge regarding risk terminology. RaMEX is marked as simple to use and ISRAM with no complicated mathematical and statistical instruments and no rigid frames. Although all the offered risk assessment methods have strengths, as mentioned, some are more influential when it comes to the SH resident and some are less, but they as well have weaknesses. OCTAVE Allegro is complex, NIST CSF has unclear metrics, RaMEX is outdated and ISRAM is time consuming and we still have a question of putting equality between two questionnaires regarding risks and consequences.

As a conclusion, when existing risk assessment methods are offered, OCTAVE Allegro would be the best choice despite its weaknesses. ISRAM is time consuming thus we cannot expect from a smart home resident to devote so much time to manage risks especially when we take into account e.g. that a Deloitte study showed that 90% of their consumers accept legal terms and conditions without reading them first on the Internet (Business Insider, 2017). Thus we cannot expect that the individual resident devotes much time to the risk assessment either and to provide quality of the data. RaMEX is outdated, so, it is not beneficial to use. NIST CSF since it has unclear metrics to set the risk assessment can be problematic due to a high chance that risk assessment in the start would not be set correctly thus the results obtained would not be relevant. Hence, OCTAVE

Allegro seems to be the best choice although it is a qualitative method, but precisely for that it is comprehensive to use and the complexity due to many worksheets can be overcome much easier than weaknesses of the other methods, especially when we have in mind that it will be used by a resident and not an organization.

5.2.2. Society perspective

Society perspective is oriented towards a society in which smart homes exist and influence that potential risks can have on the whole society. For the society perspective, it is very important to consider the limitations in a way that society does not have necessarily have experts regarding risk management which automatically excludes any complicated risk assessment methods. The same was case for the individual use. The society perspective is extremely correlated with the government perspective and it depends on its regulations. Although it is expected that society will not rely on large investments in risk assessments as e.g. government. The method that society can use to conduct a SH risk assessment should be simple, yet wide enough to cover all the necessary risks that can affect it in any sense.

When it comes to society perspective it is important to take into account the current state of SH on this level.

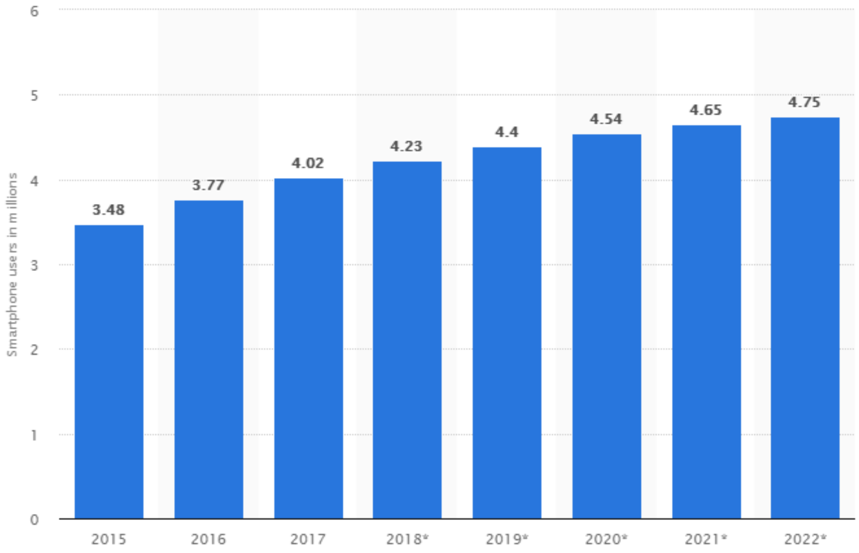
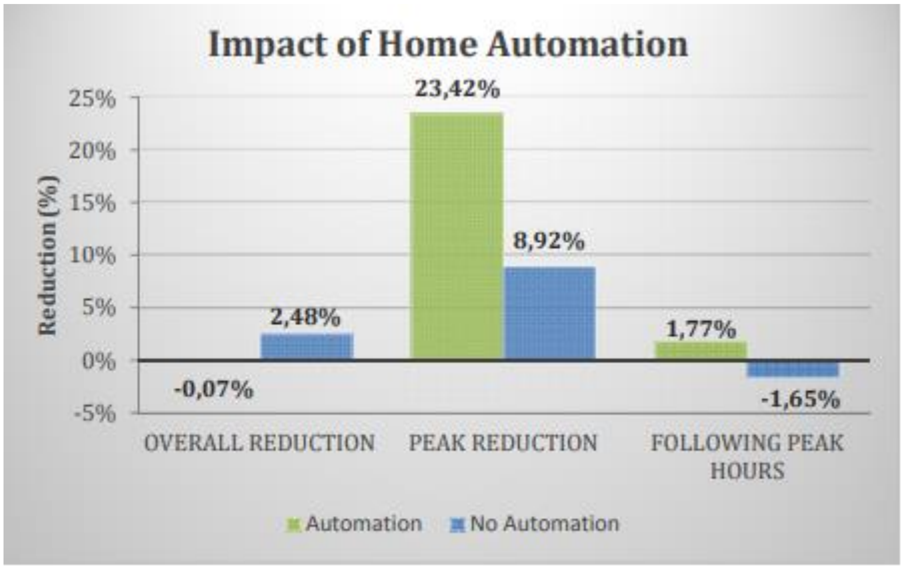
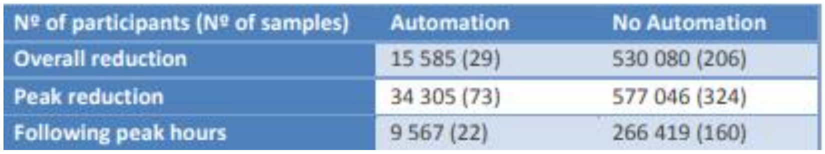


Figure 19: Number of smart phone users in Norway. Source: (Statista, 2018)

SH development can be observed in relation to the growth of usage of smart phones since smart phones are one of the instruments that are supporting SH. As it can be seen from the Figure 19, number of smart phones in Norway increased from 3.48 to 4.75 million users from 2015 to 2022. The increase of almost 27% in only seven year period. According to Statista (2018) current household penetration of SH in Norway is 31.6% in 2018 and it is expected to reach 52.5% by 2022 and this projection is made disregarding households that only have smart TVs or smart gardening devices.





Nº of participants (Nº of samples)	Automation	No Automation
Overall reduction	15 585 (29)	530 080 (206)
Peak reduction	34 305 (73)	577 046 (324)
Following peak hours	9 567 (22)	266 419 (160)

Figure 20: Impact of home automation on electricity consumption. Source: (VaasaETT, 2017)

In the Figure 20 it is shown the effect of SH on electricity consumption in Norway which is one of the examples of effect of SH to the entire society. Figure 20 shows that, in the case of peak reduction, home automation has a significant effect of almost 24% which can be explained by the fact that automation enables fast reactions and controllable levels of reduction among other. (VaasaETT, 2017) This way it is shown that home automation has effect on the society as well as on individual user. When the SH function as they are supposed to, benefits, for the entire society exist, but in cases when SH is experiencing e.g. cyber attack, risks related can affect all the society in some way.

The perspective of society is different than the individual person as the user. As it can be seen in the literature the impacts of new technologies can be often difficult to predict and expected benefits in some cases cannot be realized since sometimes insights regarding important interactions among technology and society are neglected. (Geels & Smit, 2000 as seen in Balta-Ozkan, et al., 2013)

The society perspective is very important especially considering the growth of the smart homes in Norway. We also have to take into account that consequence categories that society is worried about, would not be personal data loss of a single resident of a smart home, since it will not have any effect on society in total. Whereas data misuse and monetary loss are a field of concern for the society.

5.2.2.1. Analysis of the offered methods from the society perspective

In the Table 6 it is shown the comparison of the presented risk assessment methods like earlier in the Chapter 5, now from the society perspective. Methods highlighted in orange are excluded as non-applicable from the society perspective as it can be seen in the table and text following:

Table 6: Comparison of risk assessment method for SH from Society perspective. Based on Table 3

Suggested method	Methodology	Level	Time	**SOCIETY PERSPECTIVE**
OCTAVE Allegro	Qualitative	Standard	Medium time-consuming	**It is free for use, different perspectives can be achieved, complexity due too many worksheets**
FAIR	Quantitative	Specialist	Medium time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**

Suggested method	Methodology	Level	Time	**SOCIETY PERSPECTIVE**
NIST CSF	Qualitative	Standard	Medium time-consuming	**Common language, concise, enables scalability, feasible to create a good quality metric scale since on a society level there should be enough skills for achieving it**
RaMEX	Qualitative	Standard	Medium time-consuming	**Simple, but not updated**
ISRAM	Quantitative	Standard	Medium time-consuming	**No complex mathematical and statistical instruments, no rigid frames thus adaptable to the SH specificities, two questionnaires are feasible when it comes to society, complex and time consuming, risk=expected consequences thus can be misleading**
CORAS	Qualitative	Specialist	Extremely Time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**
CIRA	Qualitative	Specialist	Extremely Time-consuming	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**

As it can be seen, FAIR, CORAS and CIRA are still marked orange and their strengths and weaknesses from this perspective were not taken into account since in the analysis of the risk assessment methods they were already marked at specialist level, which means that even on society level we cannot expect large investments without any specific regulations from the government level. The other methods are presented and we can discuss their appliance from the society.

OCTAVE Allegro method is a qualitative method which is free to use and enables usage of different perspectives through different worksheets. This characteristic is good when we have an organization where different departments would fill different worksheets in order to influence the objectivity of the method. In the case of society, this is the case since we can observe the influence of SH cyber related risks on the different parts of the society. NIST CSF from the other hand provides systematic methodology with common language that can be quite beneficial for the society since there is no need for any specific knowledge regarding risk terminology and thus the costs are lower in the start. RaMEX is marked as simple to use and ISRAM with no complicated mathematical and statistical instruments and no rigid frames. Although all the offered risk assessment methods have strengths, as mentioned, some are more influential when it comes to the SH resident, some less, but they as well have weaknesses. OCTAVE Allegro is complex, NIST CSF has unclear metrics, RaMEX is outdated and ISRAM is time consuming and we still have a question of putting equality between two questionnaires regarding risks and consequences.

As a conclusion, when existing risk assessment methods are offered, OCTAVE Allegro, although marked as the most beneficial for the individual resident when it comes to society level, would be too complex due to a large number of worksheets where its complexity would be problematic. ISRAM is time consuming but from society level we can expect to devote much more time than a single resident to manage risks, but we cannot exclude the risk=consequences principle in ISRAM which can be misleading. RaMEX is outdated so it is not beneficial to use. NIST CSF, since it has unclear metrics to set the risk assessment, can be problematic for a single resident to use it, but for the society, it should be expected to be able to set the metrics precisely and in a correct way. Hence NIST CSF is the best choice although it is a qualitative method, but precisely for that, it is comprehensive to use and its systematic methodology, scalability and efficiency then can give very good results.

5.2.3. Government perspective

Government perspective is very important especially regarding the legislative that is affecting the field of SH and IoT in general and the ways of assessing risks in the current state. Ødegaard (2017) explains that, in Norway, many cities are starting to invest and experiment with the smart city technology. Interest is wide, and as well big cities as Oslo, and smaller as Bodø are conducting several smart city projects and strategies. Although the projects started, they can still be considered as fragmented, relatively small scale and oriented towards specific sectors as he further explains.

ENOVA SF is government funding scheme in Norway and it is owned by the Ministry of climate and environment. It provides incentives for buying of the smart homes and it works so that when you buy a smart home you can get reimbursement up to 20% with the goal to make Norwegian households more energy efficient. (ENOVA, 2018)

According to the Statistics in Norway exist 2.3 million households. (VaasaETT, 2017). According to this number of households and the fact that Norway is going for example to set smart meters in all the households for the electricity measurements by 1st January 2019 (VaasaETT, 2017) and all the other incentives in which it motivates the smart home automation, it is necessary to also acquire the strategy of how to assess and treat the risks related or how to face the threats that come along with the automation.

As it can be seen previously, government perspective is very important likewise the society perspective, especially considering the growth of smart homes in Norway. Norwegian government as it can be seen from the above has included itself in the development of smart homes and smart cities. As well as with society perspective, we have to take into account that consequence categories that government is worried about would not be personal data loss of a single resident of a smart home since it will not have any wider effects. Whereas data misuse and monetary loss are a field of concern for the society since in that case both society and government have to intervene with its mechanisms.

5.2.3.1. **Analysis of the offered methods from the government perspective**

In the Table 7 it is shown the comparison of the presented risk assessment methods like earlier in the Chapter 5, now from the government needs. Methods highlighted in orange are excluded as non-applicable from the government perspective as it can be seen in the table and text following:

Table 7: Comparison of risk assessment method for SH from Government perspective. Based on Table 3

Suggested method	Methodology	Level	Time	**GOVERNMENT PERSPECTIVE**
OCTAVE Allegro	Qualitative	Standard	Medium time-consuming	**Non-applicable due to low quality of the results on this level. We can expect large investments and expert participation. Risks that should be analyzed are on a more complex level**
FAIR	Quantitative	Specialist	Medium time-consuming	**does not have consistent terminology which can be overcome on this level due to expert participation, but still has complexity in result checking**
NIST CSF	Qualitative	Standard	Medium time-consuming	**Non-applicable due to low quality of the results on this level. We can expect large investments and expert participation. Risks that should be analyzed are on a more complex level**
RaMEX	Qualitative	Standard	Medium time-consuming	
ISRAM	Quantitative	Standard	Medium time-consuming	
CORAS	Qualitative	Specialist	Extremely Time-consuming	**integrates number of RA techniques, difficult scalability, complies with various standards**
CIRA	Qualitative	Specialist	Extremely Time-consuming	**It does not comply with any standards**

As it can be seen this time OCTAVE Allegro, NIST CSF, RaMEX and ISRAM were marked as orange in Table 7, and from this perspective were not taken into account, since in the analysis of the risk assessment methods they were marked as a standard level and as well their characteristics and complexity, in taking into account all the necessary threats is not adapted for this perspective.

This time we can expect large investments in the risk assessment process and serious risk assessment approach by providing the best experts. The methods presented as suitable are FAIR, CORAS and CIRA.

FAIR is a quantitative method, easy to understand, with defendable results but which needs metric data, it does not have consistent terminology and has a significant complexity in the checking of results. CORAS integrates a number of RA techniques and gives freedom in the selecting of the RA method and complies with various standards. On the other hand, it demands expert participation and it is time consuming with difficult scalability. CIRA also demands expert participation, it is time consuming but it does not comply with any standards although it supports improved decision making through actors motivation insights.

Even though all three methods would be beneficial, the one recommended would be CORAS. Although it has similar characteristics as CIRA, it complies with standards whereas FAIR needs metric data and has inconsistent terminology. We cannot expect to have all the metric data available due to specificity or risks analyzed. It is expected that on the governmental level it is necessary to have standard compliance of the method used. Therefore CORAS is very suitable from the government perspective.

6. DISCUSSION AND FUTURE RESEARCH

6.1. Discussion

As we explained in Chapter 2, risk assessment is the core process of the whole risk analysis, which results in a complete risk picture of the project, business or similar which is analyzed. (Aven, 2015) In Chapter 5 we have presented different risk assessment methods that might be suitable according to the literature for smart home risk assessment related to cyber risks. All the presented methods showed their weaknesses apart from their strengths. As we said in Chapter 2, risk analysis methods that are using extremely quantitative measures are not easy to use because of the extensive appliance of complex mathematical and statistical methods, whereas qualitative risk analysis methods, where risk is being analyzed with the adjectives instead of mathematics, do not offer enough information outputs very often. (Wawrzyniak, 2006). This was shown in the Chapter 5 as completely correct. From the individual perspective it was complicated to use extensive mathematical and statistical methods, but still when we were observing government perspective, there the qualitative methods were far too subjective and without enough precise outputs. Society perspective although more oriented towards quantitative methods, still did not provide enough investment inputs in order to support the expensiveness of the complex quantitative methods.

In the Chapter 4, we stated that the smart home automation system is considered to be a key element of the future internet. (Ricquebourg et al. 2006) According to Manyika et al. (2015) linking the physical and digital worlds could, by 2025, generate up to an 11, 1 trillion dollars a year in economic value observed. This shows the strength and pace of the development of the technology, and by it, of the smart homes as well. As it can be seen on the Figure 21 the global smart home market growth through the years is on a very high pace. The Figure offers further explanation by the application category, nevertheless the complete expected growth is extremely high.

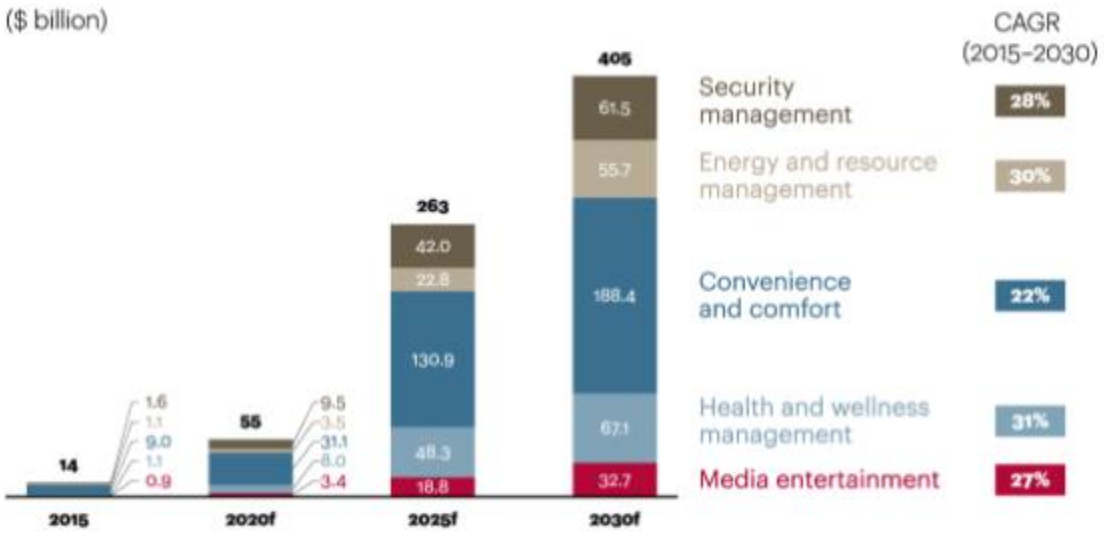


Figure 21: Global smart home market growth by application category. (AtKearney, 2017)

Although we limited our analysis for the society and government perspective to Norway, in order to provide specific data for the country, we can see that the growth of smart homes is large on the global level. We tried by limitations to give more relevance to the perspectives, in order to be able to draw more objective conclusions. It would be possible to expand the analysis on the world level as well and according to the worldwide smart home growth to draw possibly the same or similar conclusions.

We did set the consequence dimensions on monetary loss, data loss and data misuse and we were observing the whole analysis through that frame. It would be also interesting to include another consequence dimensions as human loss or similar and to expand the analysis.

As it was stated in the limitations and methodology as well, literature offered is limited since smart homes are relatively new concept and as well risk assessment methods that could be suitable are not completely adapted and updated. For example RaMEX which has potential but it is outdated and thus cannot follow the fast development of the cyber risks. In the following period we expect that more research will be done in this field.

6.2. Recommendations

The following are some recommendations related to the risk assessment methods suitable to be used for SH risk assessment. They came inspired by the analysis in the Chapter 5:

- Primarily for the individual perspective it could be interesting to develop an Android/iStore application for SH risk assessment that could be downloaded and used on a smartphone. The application could be in a simple and graphically rich form in order to provide the comprehensive interface and flow. Residents could then download the application, and by answering all the questions offered, they could obtain a complete risk picture and could be advised on how to act towards the risks that are present in the application. This way risk assessment method could be adapted completely to the needs of the individual resident and we would avoid the complexity of use of different offered methods.
- For the individual users risk assessment, it would be interesting to apply some new simple graphical approaches in order to present the results of risk assessment. On the Figure 22 a polar matrix shows probabilities and consequences. A polar matrix is based on the risk matrix, it is just an attempt to refresh the appearance of the classical risk matrix. The left one is showing a smaller group of risks (it would always show four risks at the time or six due to the limitation of the figure) and the right one is showing larger group of risks consisting of smaller risks. Consequences are shown in different fields grouped around the risk, their probabilities are shown with the different colors. As it can be seen, different colors are having different values and therefore they are having different positions in the graph, this way, the significance of the probabilities assigned is visible. In a sense the field will not just be green it will show the value that determined the green color as well. On the right figure it is shown as well the prevailing color of smaller risks grouped into a larger category. This way it is visible which smaller risks the group consists of and what their probabilities of occurrence are.

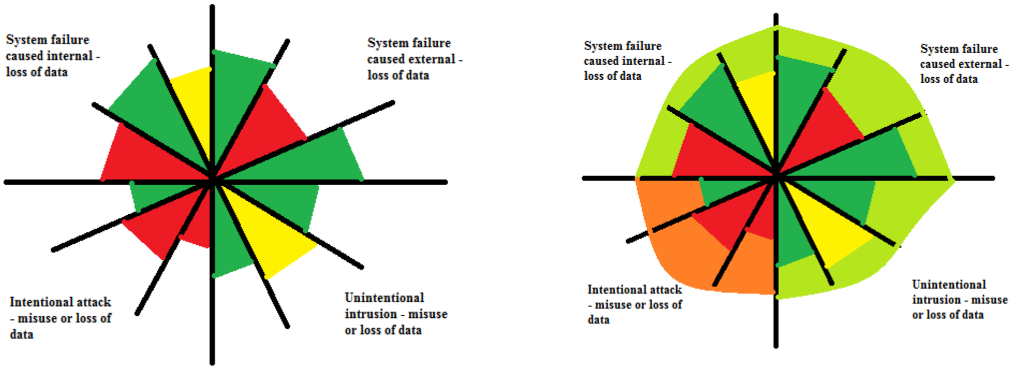


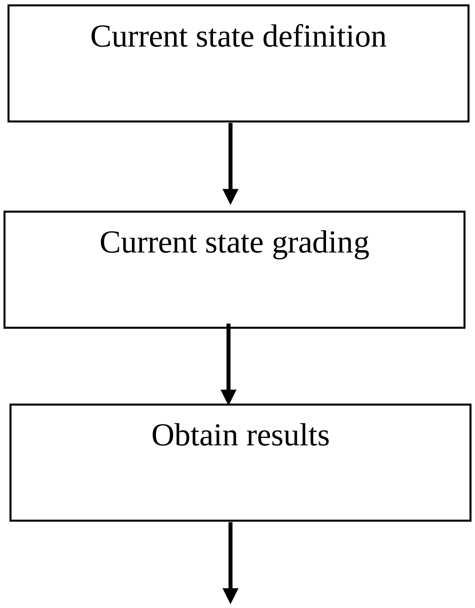
Figure 22: Polar matrix showing probabilities and consequences

- When it comes to government level it would be good to improve standardization in the area of SH in order to reduce risks that can be reduced in the design phase. As described by The Scientific Committee of the Norwegian Smart Grid Centre (2015), standardization is not a technical research issue by itself, nevertheless, it can be regarded as a consensus arena which is opened for all stakeholders meeting to develop standards which would cover a market need. For example in Chapter 5, while observing the government perspective we decided not to use CIRA due to the lack of compliance with standards.
- Especially for society and government perspective it would be good to combine benefits of both qualitative and quantitative methods in order to provide a better risk picture. Although we have to be aware that complete objectivity is difficult to reach, for both qualitative and quantitative approach, when it comes to risk assessment, the moral hazard of the risk analyst has less or more influence on the final results due to the subjectivity of the human nature. (Munteanu, 2006). It is important to notice that although quantitative methods offer scalable results nowadays with the development of new technologies they are not anymore able to model complex scenarios that are occurring in complex environments of today, whereas qualitative methods are more suitable with necessity of paying attention to their nature of yielding inconsistent results. (Karabacak & Sogukpinar, 2005)
- Since as previously mentioned, when it comes to cyber risks, there exist a significant lack of historical data. Therefore it would be beneficial especially for the society and government perspective to enable the gathering of the data on one web application or through Android application in order to have a significant sample to get some average

results and then to be able to set a fair objective ranking scale that would provide more objectivity. This as well can be achieved through a standardized risk assessment models that could provide some of the data without revealing sensitive data.

6.3. Future research

According to all the methods previously presented and analyzed and taking into account the structure and needs of SH we suggest as future research, the development of a new method with a possible name CRASH – Cyber Security Risk Assessment with appliance for SH (Idea for the name Flage, 2018). The proposed method would consist of five steps. It would take into account all the specific needs related to SH as well the strengths and weaknesses of previously presented methods. CRASH would be designed and developed with the idea to help efficient risk assessment which can be done in a simple way by any random user or by risk analysis expert. CRASH would be semi-qualitative, semi-quantitative method which would combine both benefits of qualitative and quantitative methods. The necessity of including partly qualitative characteristics into the method are from the characteristics of cyber risks that cannot completely be described by metric data.



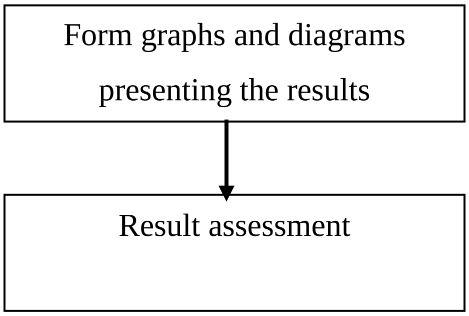


Figure 23: Steps of potential CRASH method

On the Figure 23 are shown the steps of the possible method that are the sum of all the methods presented previously. The model would have common language as NIST CSF in order for all users to be able to understand and conduct the risk assessment. Though it would have a simple but consistent terminology in order to avoid weaknesses of for example FAIR. It would enable scalability and clear and precise instructions for creating the metric scale in order to provide more comparable results. It would be supported with a software package which would provide the simplicity for the analyst regarding the mathematical and statistical instruments used.

The goal would be to provide simplicity in use with effective and precise results.

7. CONCLUSION

The main objective of this thesis was to analyze existing risk assessment methods that can be used for SH risk assessment, related to cyber risks, from three different perspectives: individual, society and government. In order to achieve that, the analysis of the existing risk assessment methods that are suitable for SH risk assessment use has been conducted with emphasis on cyber related risks and consequence dimensions: monetary loss, data loss and data misuse. The existing risk assessment methods were then observed from all three perspectives and recommendation for improvement with suggestions for new method development according to the analysis has been provided. From the whole analysis we can draw the following conclusions:

Currently the greatest challenge when it comes to SH cyber related risks, is the fast development of smart homes and lack of standardization since there exist many devices that come with different terms and conditions of use. Thus, levels of protection can still not be on a high level. This is a significant challenge since the system becomes more vulnerable and it is possible to enter the whole system by accessing the weakest device in the system.

Risk assessment methods analyzed are all having weaknesses and strengths. As a conclusion it can be drawn out that with the technology development it is necessary to improve existing risk assessment methods in order to follow the rapid growth and development of the risks. In the table 8 conclusions have been drawn on all the analyzed methods from all three perspectives. Methods highlighted in green are the ones suggested for the chosen perspective, whereas methods highlighted in orange are non-applicable for the selected perspective, as it can be seen in the table and text following:

Table 8: Conclusion based on analyzed methods from different perspectives

Suggested method	INDIVIDUAL PERSPECTIVE	SOCIETY PERSPECTIVE	GOVERNMENT PERSPECTIVE
OCTAVE Allegro	**It is free for use, complexity is avoided since it is individual user thus it cannot be too many worksheets, but therefore different perspectives cannot be achieved**	**It is free for use, different perspectives can be achieved, complexity due too many worksheets**	**Non-applicable due to low quality of the results on this level. We can expect large investments and expert participation. Risks that should be analyzed are on a more complex level**
FAIR	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**	**does not have consistent terminology which can be overcome on this level due to expert participation, but still has complexity in result checking**
NIST CSF	**Common language, concise, enables scalability, can be confusing due to creation of their own metric scale since it is an individual user without prerequisite knowledge**	**Common language, concise, enables scalability, feasible to create a good quality metric scale since on a society level there should be enough skills for achieving it**	**Non-applicable due to low quality of the results on this level. We can expect large investments and expert participation. Risks that should be analyzed are on a more complex level**
RaMEX	**Simple, but not updated**	**Simple, but not updated**	
ISRAM	**No complex mathematical and statistical instruments, no rigid frames thus adaptable to the SH specificities, two questionnaires are not so feasible when it is an individual resident, complex and time consuming, risk=expected consequences**	**No complex mathematical and statistical instruments, no rigid frames thus adaptable to the SH specificities, two questionnaires are feasible when it comes to society, complex and time consuming, risk=expected consequences thus can be misleading**	

Suggested method	**INDIVIDUAL PERSPECTIVE**	**SOCIETY PERSPECTIVE**	**GOVERNMENT PERSPECTIVE**
CORAS	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**	**integrates number of RA techniques, difficult scalability, complies with various standards**
CIRA	**Non-applicable due to specialist level thus expert participation is necessary and too complex for an individual user without prerequisite knowledge**	**Non-applicable due to specialist level thus expert participation is necessary and too time consuming hence expensive**	**It does not comply with any standards**

Different concerns are associated with different perspectives, thus the same existing methods are not the best option for all the three perspectives. The individual resident is concerned about their data and their money whereas society and government are concerned about e.g. vulnerabilities that they can face if number of smart houses on the market increase. Also, individual resident does not necessarily have expert knowledge and like society cannot invest large extent of money to risk assessment, whereas government has experts and larger budget for the risk assessment.

New technology brings new risks but IoT and thus the SH as well due to its pervasiveness has the potential to increase risk significantly. (ISACA, 2015) Hence it is extremely important to treat risks in the best way possible. Thus, the best way is to develop a new method that would cover the strengths of the current methods and remove the weaknesses. This way the model would not be developed from scratch, since there exist models that can be applicable already (most used ones are presented in the thesis) and thus they can be combined and that way an improved model could be developed.

REFERENCES

AAL (2016) – *Objectives of the AAL Programme*. Retrieved May 25, 2018, from AAL - Active and Assisted Living Program : http://www.aal-europe.eu/about/objectives/

AGRAWAL, V. (2017). *A Comparative Study on Information Security Risk Analysis Methods*. *JCP*, *12*(1), 57-67.

ALBERTS, C. J., BEHRENS, S. G., PETHIA, R. D., & WILSON, W. R. (1999). Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0.

ALBERTS, C. J., & DOROFEE, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

ATKEARNEY (2017). *The Battle for the Smart home*. Retrieved April 24, 2018, from ATKearney, http://www.atkearney.no/paper/-/asset_publisher/dVxv4Hz2h8bS/content/the-battle-for-the-smart-home-open-to-all/10192?inheritRedirect=false&redirect=http%3A%2F%2Fwww.atkearney.no%2Fpaper%3Fp_p_id%3D101_INSTANCE_dVxv4Hz2h8bS%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1

AVEN, T. (2015). *Risk analysis*. John Wiley & Sons

AVEN, T., & VINNEM, J. E. (2007). Risk management: *With applications from the offshore petroleum industry*. Springer Science & Business Media.

BAKO, A. (2016). *Internet of Things based Smart Homes: Security Risk Assessment and Recommendations (master thesis)*. Retrieved April 1, 2018, from DiVA Portal, http://www.diva-portal.org/smash/get/diva2:1032194/FULLTEXT02.pdf

BALTA-OZKAN, N., DAVIDSON, R., BICKET, M., & WHITMARSH, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, *63*, 363-374.

BUNTZ, B.. (2013). *A CIA – Inspired Approach to Medical Device Cybersecurity*. Retrieved April 8, 2018 from MDDI Online: *https://www.mddionline.com/cia-inspired-approach-medical-device-cybersecurity*

BUSINESS INSIDER. (2015), *The inventor that inspired Elon Musk and Larry Page predicted smartphones nearly 100 years ago.* Retrieved February 3, 2018, from Business Insider, : http://www.businessinsider.com/tesla-predicted-smartphones-in-1926-2015-7?r=UK&IR=T&IR=T

BUSINESS INSIDER. (2017), *No one reads terms and agreements.* Retrieved Mai 2, 2018, from Business Insider, : *http://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T&IR=T*

CARALLI, R. A., STEVENS, J. F., YOUNG, L. R., & WILSON, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process* (No. CMU/SEI-2007-TR-012). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

CAVELTY, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

CHAN, M., ESTÈVE, D., ESCRIBA, C., & CAMPO, E. (2008). A review of smart homes—Present state and future challenges. *Computer methods and programs in biomedicine*, *91*(1), 55-81

CHAN, M., CAMPO, E., ESTÈVE, D., & FOURNIOLS, J. Y. (2009). Smart homes—current features and future perspectives. Maturitas, 64(2), 90-97

CISCO (2018). *What is cybersecurity?*. Retrieved Mar 25, from CISCO, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

COHEN, J. E. (2003). Human population: the next half century. *science*, *302*(5648), 1172-1175.

COLBY, S. L., & ORTMAN, J. M. (2017). Projections of the size and composition of the US population: 2014 to 2060: Population estimates and projections.

COOPER, M., & KEATING, D. (1996). Implications of the emerging home systems technologies for rehabilitation. *Medical engineering & physics*, *18*(3), 176-180.

CRAVEN, J. (2017). *What Is a Smart House? What is domotics?*. Retrieved March 28, 2018 from Thought.co, https://www.thoughtco.com/what-is-a-smart-house-domotics-177572

DEMIRIS, G. (2004). Electronic home healthcare: concepts and challenges. *International Journal of Electronic Healthcare*, *1*(1), 4-16.

DENNING, T., KOHNO, T., & LEVY, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94-103.

DJEMAME, K., ARMSTRONG, D., KIRAN, M., & JIANG, M. (2011). A risk assessment framework and software toolkit for cloud service ecosystems. *Cloud Computing*, 119-126.

ENOVA (2018). Retrieved May 23, 2018 from Enova SF, www.enova.no

FAIR INSTITUTE (2016). Retrieved April 25, 2018 from FAIR Institute, https://www.fairinstitute.org/what-is-fair

FENRICH, K. (2008). Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, *112*(2), 44-49.

FLAGE R., guidance meeting, June 2018

FLEISCH, E., WEINBERGER, M., & WORTMANN, F. (2014). Business models and the internet of things, *Bosch IoT Lab Whitepaper*.

FOOTE, K.D. (2016). *A Brief History of the Internet of Things.* Retrieved March 5, 2018 from Dataversity, http://www.dataversity.net/brief-history-internet-things/

FORBES TECHNOLOGY COUNCIL (2018), *14 Predictions for the Future of Smart Home Technology*, *Forbes*. Retrieved March, 14 from Forbes, https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/forbestechcouncil/2018/01/12/14-predictions-for-the-future-of-smart-home-technology/

FORTINO, G., & TRUNFIO, P. (Eds.). (2014). *Internet of things based on smart objects: Technology, middleware and applications*. Springer Science & Business Media

GEELS, F. W., & SMIT, W. A. (2000). Failed technology futures: pitfalls and lessons from a historical survey. *Futures*, *32*(9-10), 867-885.

GUIDE, I. S. O. (2009). 73: 2009. *Risk management—Vocabulary*, *551*.

ICONTROL. (2015). *State of the Smart Home Report*. Retrieved from http://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf

IDC. (2017), *IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018*. Retrieved February 27, 2018 from IDC – International Data Corporation https://www.idc.com/getdoc.jsp?containerId=prUS43295217

ISACA (2013). *A simple definition of Cybersecurity*. Retrieved June 1, 2018 from ISACA, https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

ISACA (2015). *Internet of Things: Risk and Value considerations*. Retrieved April 15, 2018 from Aalborg Universitet,Forsknings portal, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

ISBUZZ EXPERT PANEL. *CIA Triad and New Emerging Technologies: Big Data and IoT*. Retrieved April 10, 2018 from Information Security Buzz, https://www.informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/

JACOBSSON, A., BOLDT, M., & CARLSSON, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719-733

JOUINI, M., & RABAI, L. B. A. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science*, *83*, 1084-1089.

JUVIGNY J. (2016). *Smart home security: Overview of ENISA's report*. Retrieved March 15, 2018 from Digital Security: https://www.digital.security/en/blog/smart-home-security-overview-enisas-report

KAF MOBILE HOMES (2018), *Smart home energy saving.* Retrieved May 24, 2018, from Kaf Mobile homes, http://kafgw.com/stunning-smart-home-energy-saving-16-photos/

KAILAY, M. P., & JARRATT, P. (1995). RAMeX: a prototype expert system for computer security risk analysis and management. *Computers & Security*, *14*(5), 449-463.

KARABACAK, B., & SOGUKPINAR, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159.

KOSUTIC, D. (2016), *Where does information security fit into a company?* Retrieved April 8, 2018, from Advisera Expert Solutions ltd. , https://advisera.com/27001academy/blog/2016/10/24/where-does-information-security-fit-into-a-company/

LEINER, B. M., CERF, V. G., CLARK, D. D., KAHN, R. E., KLEINROCK, L., LYNCH, D. C., ... & WOLFF, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

MANYIKA, J., CHUI, M., BISSON, P., WOETZEL, J., DOBBS, R., BUGHIN, J., & AHARON, D. (2015). Unlocking the Potential of the Internet of Things. *McKinsey Global Institute*

MUNTEANU, A. (2006), *Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma*. Managing Information in the Digital Economy: Issues & Solutions - Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, pp. 227-232

NESHEIM M. B., ROSNES K.S., *A smarter home, the smarter choice? (Master thesis)*. Retrieved April 15, 2018, from BYBSIS Brage http://hdl.handle.net/11250/2401571

NIST (2016), *NIST Cybersecurity Framework (CSF). Retrieved February 16, 2018 from* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE, NIST Headquarters, www.nist.gov

NORTHSTAR TECHNOLOGY GROUP (2016). NIST Security Framework. Retrieved March 25, 2018 from Northstar Technology group, http://www.northstartechnologygroup.com/nist-security-framework

OKSMAN, V., & EGAN, J. (2010). Applications of ITUT G. 9960, ITU-T G. 9961 transceivers for Smart Grid applications: Advanced metering infrastructure, energy management in the home and electric vehicles. *ITU-T Technical Paper*.

RICQUEBOURG, V., MENGA, D., DURAND, D., MARHIC, B., DELAHOCHE, L., & LOGE, C. (2006, December). The smart home concept: our immediate future. In *E-Learning in Industrial Electronics, 2006 1ST IEEE International Conference on* (pp. 23-28). IEEE.

RSA CONFERENCE (2014). *Measuring and Managing Information Risk: A FAIR Approach. Retrieved April 25, 2018 from RSA Conference, https://www.rsaconference.com/blogs/measuring-and-managing-information-risk-a-fair-approach*

SHUKLA, N., & KUMAR, S. (2012). A comparative study on information security risk analysis practices. *IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies ICNICT (3)*, 28-33.

STATISTA (2018), *Number of smartphone users in Norway from 2015 to 2022*. Retrieved May 20, 2018 from Statista – the statistics portal, https://www.statista.com/statistics/494647/smartphone-users-in-norway/

STOJKOSKA, B. L. R., & TRIVODALIEV, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454-1464.

SURYADEVARA, N. K., & MUKHOPADHYAY, S. C. (2015). *Smart homes: design, implementation and issues* (Vol. 14). Springer.

TECHTARGET (2017). *Smart home or building*. Retrieved May 20, 2018 from IoT Agenda: https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

THE UNIVERSITY OF MELBOURNE (2018). *Incident reporting risk matrix*. Retrieved May 20, 2018 from The University of Melbourne, https://safety.unimelb.edu.au/incident-reporting/incident-reporting-risk-matrix

The Scientific Committee of the Norwegian Smart Grid Centre (2015). *Norwegian Smart Grid Research Strategy*. Retrieved June 1, 2018 from The Norwegian Smart Grid Centre, https://smartgrids.no/wp-content/uploads/sites/4/2015/08/Norwegian-Smart_Grid__Research_Strategy_DRAFT_June10_WT_ks_hii.pdf

UNIFORE (2015), *Home alarm system with camera for interactive monitoring*. Retrieved April 25, 2018 from Unifore: https://www.hkvstar.com/technology-news/home-alarm-system-with-camera-for-interactive-monitoring.html

VAASA ETT (2017). Assessing the Potential of Home Automation in Norway, Norwegian water resources and energy directorate. Retrieved from Norges vassdrags- og energidirektorat, http://publikasjoner.nve.no/rapport/2017/rapport2017_34.pdf

VRAALSEN, F., DEN BRABER, F., HOGGANVIK, I., ASS, M., LUND, S., & STØLEN, K. (2004). The CORAS tool-supported methodology for UML-based security analysis. *SINTEF Norway*

WANGEN, G. (2015). Conflicting incentives risk analysis: A case study of the normative peer review process. *Administrative Sciences*, *5*(3), 125-147.

WAWRZYNIAK, D. (2006). Information security risk assessment model for risk management. In *International Conference on Trust*, *Privacy and Security in Digital Business* (pp. 21-30). Springer, Berlin, Heidelberg

WHITMAN, M. E., & MATTORD, H. J. (2011). *Principles of information security*. Cengage Learning

WILSON, C., HARGREAVES, T., & HAUXWELL-BALDWIN, R. (2017). Benefits and risks of smart home technologies. *Energy Policy*, *103*, 72-83

WORTMANN, F., & FLÜCHTER, K. (2015). Internet of things. *Business & Information Systems Engineering*, *57(3)*, 221-224.

ØDEGAARD A.R.S. (2017). *Smart, Social & Sustainable? (Master thesis)*. Retrieved May 10, 2018 from BYBSIS Brage, http://hdl.handle.net/11250/2479823