POLITEHNICA UNIVERSITY
OF BUCHAREST

Doctoral School of Electronics, Telecommunications
and Information Technology

Decision No. 802 from 07-02-2022

Ph.D. THESIS SUMMARY

Eng. Vlad-Valentin Firețeanu

STRUCTURAREA APLICAȚIILOR DE ANALIZA A RISCULUI PENTRU PROIECTELE IOT

DESIGNING RISK ASSESSMENT APPLICATIONS FOR INTERNET OF THINGS PROJECTS

THESIS COMMITTEE

Prof. Dr. Ing. Ion Marghescu Politehnica University of Bucharest	President
Prof. Dr. Ing. Mihai CIUC Politehnica University of Bucharest	PhD Supervisor
Prof. Dr. Ing. Corneliu Rusu Technical University from Cluj	Member
Prof. Dr. Ing. Călin Vladeanu Politehnica University of Bucharest	Member
Prof. Dr. Ing. Dan Marius Dobrea Technical University Gh. Asachi, Iaşi	Member

BUCHAREST 2022

Content

Chapter 1

Introduction

During last years, the number of IoT projects considerably increased. So, the number of companies that are using these technologies raised from 13% in 2014 to 25% when this thesis was written [1]. Considering this raise, we deal also with an increase in research efforts for this topic, with an emphasis on optimizing the specific processes for this trend. Moreover, this increase determined a large number of challenges, such as writing feasibility and productivity reports, documents that take into consideration the possibility of various risk factors.

Apart of the constantly increasing number of companies that work with this technology, there is also important to consider the quantity of hardware equipment included in the IoT project design. The diversity of this equipment is high, ranging from simple elements such as light bulbs, led, switches to complex elements with significant data input or output (video cameras, voice recognition devices etc.) Considering the 2020 year, we have a number of 22 billion of such devices connected to the Internet. Directly proportional, we deal also with an increase number of vulnerabilities. ‚Black Hat Hacking' attacks demonstrated the fact that ignoring the software security can lead to disastrous consequences. Following a recent study, HP concluded that, in 2015, seven from ten Internet connected hardware components are vulnerable from a software security point of view [2].

Another good example, structured around a larger pool of end users, is represented by the ‚Home Automation projects. In 2015, during the annually DEFCON conference, numerous ‚white hat hacking attacks' were conducted in order to penetrate private networks through the acquiring elements that can be found in smart house devices. The exploited vulnerability was at communication protocol level, present in a Zigbee device [3].

So, when approaching IoT projects, the first step is represented by identifying a need that should be covered by the functionalities of our project. After identifying this need, the next step is structuring an implementation step by step list. For a better understanding of this plan, this thesis maps the steps from it with the implementation phases of different case studies that are, in fact, IoT projects.

1.1 Presentation of the doctoral thesis field

By definition, Internet of Things is a network of physical devices, vehicles and other entities with processing, acquiring and/or processing capability (sensors, engines, switches). These entities grant the possibility of connecting the physical world to software artifacts. An IoT equipment implies the presence of a hardware resource that we don't expect to be Internet connected. This may be considered the main difference between an IoT hardware equipment and a laptop, mobile phone, tablet that require manual intervention to update data or send large volumes of packets to a server [4].

The large number of IoT projects is split across multiple interest domains, depending of the above specified need that should be covered. Each one of these domains has its own architecture and physical components. So, the most important projects can be found in the following areas:

1) ‚Smart Cities' – projects that cover different process automation inside urban areas, with a final purpose of increasing life quality for the citizens (smart parking, monitoring air quality, selective garbage collection projects etc.)
2) ‚Smart Environment' – projects that cover certain environmental needs by implementing and automating various processes within the deployment area (avalanche prediction, avalanche prevention, landslide prediction etc.)
3) ‚Smart Watering' – improving various irrigation processes with a final purpose of small harvesting, cost efficiency, human resource management.
4) 'Smart Metering' – projects that cover and automate different measurement processes in order to reduce costs, improve security and safety of the human resources and safe hardware monitoring.
5) 'Security and Emergencies' – represented by monitoring and alerting projects which involves automatic trigger of different procedures in case of emergency.
6) 'Retail and Logistics' – projects with a main goal of improving and optimize corporate processes and flows with a final purpose of cost efficiency and work conditions improvement.
7) 'Industrial Control' – smart monitoring of the production lines, with accent on both acquiring and execution elements that are always present within the industrial environments.
8) 'Smart Agriculture' – domain which is structured around both animal monitoring and agricultural process improvement with a final purpose of human resource management and increasing the harvest.
9) 'Home Automation and Smart Houses' – monitoring and execution projects that process information within a home with a final purpose of increasing the live quality and reduce costs.
10) 'eHealth' – projects that involve the health monitoring and is usually focused on medical process improvement.

Risk analysis can be considered a procedure that optimizes the application safety and also contributes to a more improved management of hardware resources that come along within an IoT project. This analysis implies verifying and highlighting vulnerabilities and sensitive software and hardware areas. The main purpose of this analysis, besides the awareness part, is represented by adopting measures to attenuate, even completely mitigate the risks by solving the vulnerabilities [5].

Moreover, the overall project risk is determined by the technical properties of the equipment itself. Another classification of the components is based on the collected data type. So besides of their purpose, which can be either acquiring or executing, the hardware equipment can be also classified in analogical or digital as we can see in Figure 1.1. In much simpler terms, if a component has a ON/OFF state, so basically two values, it is considered digital. Analogical components are represented by the equipment which works with a range of values within an interval.

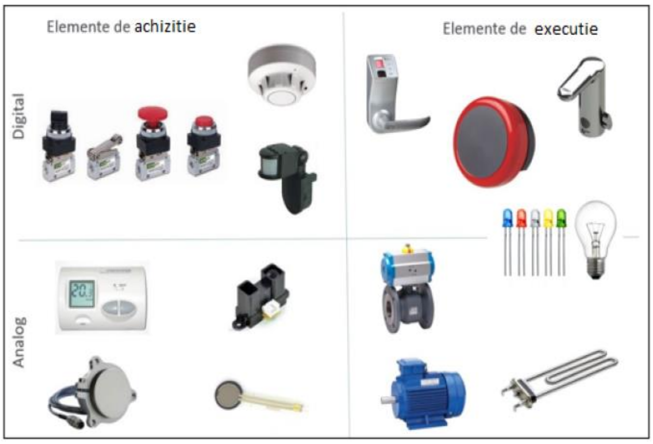


Figure 1.1 *IoT equipment types*

Besides the acquiring and execution elements, an IoT project contains also processing units, and power supply units, mandatory modules that determine the project functionality. These last two are highlighted in red, as we can see from Figure 1.2 below.

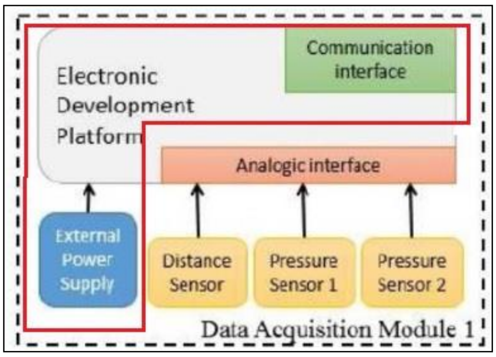


Figure 1.2 *Modules architecture within an IoT project*

Later on, we will discuss about risks that can occur in IoT project equipment that we need to acquire for us to develop the project itself (these types of risks are represented by cost, disponible, availability, scalability etc.), and also about risks that can occur when we consider using a specific type of power supply (described by the same risk factors such as costs, availability). Even more, the presence of execution elements from Figure 1.1 leads to another greater risk area which includes the risk factors on which the work accidents are based – one obvious example is represented by the presence of crushing points if we include engines in our project

1.2 Scope of the doctoral thesis

The novelty of this thesis, besides building a unique risk identification framework, is represented by the author’s intention to explore, find and quantify the potential risks, above the information security point of view. The majority of the already written papers and articles were built around the security vulnerabilities that can impact the components. Even if the majority of flaws are hidden in this area, we need to think also about risks that can occur from different areas specific for these projects. A good example for this is the presence of risk factors that can occur in the deploying environment. Even more, we also need to consider that the number of flaws and potential breaches is increasing directly proportional with number of hardware units, or the hibernation routines that should be implemented as a best practice for extending the battery lifetime. Another suggestive example can be found in the security and work safety area, which translates in the human resource safety level when the individuals are interacting with the physical part of the project. Based on the already written articles, these risk types are ignored because the main focus is on the software security vulnerabilities, sensitive data protection, broken authentication, using components with known vulnerabilities, DB injection and so on [6].

Along with the constantly increasing number of IoT projects, we also deal with a growing number of risk measurement methods. Big names, such as OWASP, created a special IoT list with top ten software vulnerabilities which is constantly updated [7]. Another giant is represented by Microsoft, company that published another list with all the required steps that should be followed in order to create a customized SDLC [1]for IoT. In greater lines, this list contains an introduction into software security, five implementation milestones split between several periods of time, but also a feedback phase. By researching these examples, we can figure out that a healthy software implementation has its roots in the project design phase [8].

There is also a must in understanding why certain risk types are neglected, and an important clue is the nature of the project itself. Note that one of the main IoT goals is the moment when the product is entering the market and it should be as early as possible. Releasing your product as soon as possible is a notable advantage because it’s easier to create a brand and solidify your reputation [9].

So, the challenges covered in this thesis are represented by the energy optimization based on the project we chose, backing the decision behind this, designing the project so it can be deployed in a safe work environment and also the information integrity which should be protected from external factors [10]. The process is based on a vector which contains major risk areas. After we quantify these areas by researching the specific risk factors, we will have a useful project overview.

After that, based on this overview we will be able to structure a solid decision, relevant for useful metrics such as implementation costs and also the overall project feasibility. Having this complex information will raise the confidence of the delivery team and we will be able to bid for a software project or accept it. Both by reading this thesis and applying the presented methods will answer to important questions, such as: ‚Which areas from my project can be improved to increase the overall project success?’ or ‚How can we quantify the possible risk for our target project, despite its low level of predictability?’ or ‚What challenges can occur after we started implementing the project?’. We can see that the answers to these questions have a common ground with the Agile principles, a SDLC method which is described by a high level of adaptability based on updated requirements through the project timeline. Even more, this SDLC method has multiple notable artifacts, such as numerous project meetings, including dedicated estimation gatherings. After all, there are a lot of similarities between the dynamic pace of IoT projects and this methodology. A whole chapter will be structured on these similarities, SDLC being also included in

[1] SDLC is the acronym for Software Development Life Cycle. Notable examples of these cycles include Agile SCRUM, Waterfall, V-model etc.

one of the presented major risk areas. By choosing the right method for our project, even from the start, will ease the whole development process.

In conclusion, our goal is, through the documented method during the thesis, to increase the awareness level when we are thinking about developing new IoT projects. By being aware of these types of risks, it will be much easier to address them so we can optimize our delivery processes and also manage the important resources as costs and individuals. Our goal is to add value both to IoT businesses involved in delivering technical projects and skilled individuals that were delivering practical projects as a hobby. It's important that our method to provide precise indications based on the large marked of already existing projects. Another important factor that should be considered is represented by a certain domain and the specific responses for carefully crafted questions within this domain. So, as a quick example, a home automation project has a lower probability be affected by environmental hazards as a smart city project. Even if this may seem obvious, the main purpose is to have a relevant value, ideally a percentage, that should grade the actual difference between them. Besides this specific value that will be used as reference, it's also important to find a complete and intuitive data displaying application, because we will work with complex responses acquired from a large number of IoT generalists and specialists that are working within this domain. In respect to this, we chose Tableau and we presented its advantages in a dedicated chapter. So, as Agile can over the fast pace of these projects, Tableau can cover complex sets of data acquired both by our risk applications and overall IoT projects. It will be easier for us to allocate an initial budget, to bid in front of a client when we desire to buy and develop a project or simply research and develop an overview above the current link between risks and Internet of Things projects.

1.3 Content of the doctoral thesis

Starting with this section, we will begin documenting the steps that are considered useful for us to create a detailed risk overview for IoT projects. Summarizing, the main steps are represented by:

- Identifying a valid user/client need
- Identifying the required equipment that should be acquired after understanding the project architecture.
- Choosing the development environment for the project
- Setting the connections with the physical components, both local and online
- Understanding the concepts of web services and familiarizing with the libraries that can be called
- Hibernation routines and other ways of power consumption optimization

Based on these steps and after studying the already existing risk measurement frameworks, we will identify new major risk areas. There is few to none articles or books written focusing this topic of risk beyond the software security part. So, from this point of view, the thesis is structured mainly on fundamental research activities that implied creating a very interesting hypothesis and following this new knowledge journey by creating new thinking processes. Apart of the fundamental research part, it’s important that we don’t forget that we deal with a topic from the engineering field, so this paper should contain also applicative research activities with a final purpose of creating a valid and universal calculus method which will bring additional value to any IoT project developer. We will discover in the following chapters what are the research activities that pe used and how we constantly switch between the fundamental and applicative one.

So, the first actions were performed under a fundamental context. Here, based on general IoT project requirements, we identified several new areas where we need to quantify the risk. Remember that these areas are represented by environmental hazards, the power supply for the project itself, physical equipment, work safety and workers protection. As we already know, these areas have different weights depending on the IoT project domain that we choose. For a better understanding of IoT needs and solutions, we chose a detailed list of domains. By reading this paper, we will see that the results are depending on these specific domains and we deal with the military one, eHealth, home automation, smart cities etc. Also, from a fundamental point of view, to have a better coverage for the potential scenarios, we opted for a more granular approach based on risk categories and risk factors. It is my pleasure to thank the engineers behind the OWASP platform for the inspiration to organize in a granular and hierarchical way the software security risks. Even if we tackled this security topic ourselves based on the top ten IoT threats, we recommend using specialized services which can provide security consultants for this matter. So, how far ahead should we think and when the risk stops for these projects? By using the hierarchical mapping stated above, the environment major risk area contains multiple categories (weather conditions or human factor), categories that also contain the specific risk factors (high temperatures, low temperatures, wind, sabotage, data corruption, data tampering etc.) After organizing the domains and the major risk areas, we are starting to apply the applicative research methodologies.

This switch to the applicative side was represented by creating a survey sent both to specialists and generalists from the IoT areas. The helpful expertise was provided by software engineers, scientific and research papers authors or simply passionate people within this IoT that built their own technical projects with proven applicability. We have a dedicated chapter where we present the survey audience and also interesting demographic statistics represented by their job description, geographical area, overall risk awareness and their work domain. Along with these statistic reports, the most important deliverable of that chapter is represented by the risk categories weights in our risk assessment method. After studying these weights, it will be clear for us how different projects from specific areas have more risks than projects from different domains. After that, the focus is on the stakeholders and beneficiaries from our method, represented by any individual which is interested in measuring risk before starting the delivery process. This step is performed around another survey, which is not public this time and it will be sent to the engineers, project managers, product owners etc. They need a more detailed analysis and also a list with the customized best practices. We will use the weights from the first study to calculate a final grade for the IoT project and also for providing detailed clarifications. The direct beneficiary for our method, the second survey respondent, will answer to a total of 70 questions that will help us to understand the risk factors for their specific project. After we acquire all the answers, it will be easier to assign the final grade. If the respondent is aware of one risk factor, then we won’t consider it in the final assessment. If the respondent is not aware at all about one risk factor, then we will assign a default value for it. We will see during this thesis lecture, that we used interesting studies and statistics performed by Eurostat or Project Management Institute or Wellington so we can have updated data. Another relevant studies that were used to document or method were conducted by Atlassian, which is a very important player in the software delivery game. These were used to have an updated overview for the incidence rate when we are talking about SDLC risks.

From a technical point of view, this survey approach is very useful when we are trying to identify risks between executing processes [11]. After all the questions were addressed, the information will be passed to a calculus node which will have specially crafted outputs for a better report visibility. These outputs are represented by already known file types such as .xml, .txt, .csv etc. Based on these reports, a final grade along with recommendations will be presented to the stakeholders. The results will be displayed in an intuitive manner, by using Tableau. We have a dedicated chapter where we explain the advantages of this tool when we want to use it within an IoT project.

In conclusion, this thesis will contain the updated status regarding the needs and IoT domains based on constant feedback from IoT engineers that participated to our study (and they are still doing it), also new risk categories and their weights based on the most known IoT domains, the actual calculus method and mathematical formula where we use these weights, and also a unique grading system for the risk factors specific to each respondent’s needs. Even more, from a mitigating point of view we will have a chapter where we present the Agile advantages when we are delivering IoT projects. We will also see how we can use the Tableau processing functionalities to generate an intuitive interface for our risk assessment method. When talking about costs, our method is quite efficient since we used Tableau Public which is a free tool. The only infestation was performed around Facebook campaign area to reach the desired audience with relevant expertise, in diagram design application (Lucidchart) and also around professional survey crafting tools (SoGoSurvey). The las one was necessary because we wanted an ideal value of 2700[2] answers to provide accuracy for our study. The relevance ‚begins’ from 384[3] answers and it starts an ascendent trend from there. We will see in the detailed chapter for this how we chose these values. The survey is active as we speak and we received somewhere around 700 answers when the thesis was written.

[2] Target value to reach a confidence level of 99% with a margin of error of ± 2.5%.

[3] Target value to reach a confidence level of 95% with a margin of error of ± 2.5%.

Chapter 2

Major risk areas and risk factor analysis

When a delivery team accepts a project, it would be ideally if they know from an early stage the required resources and also the challenges that can occur during project implementation. We can assume that we are closer to that if we succeed in creating a general and also scalable framework for risk factor measurement. It’s imperative to conduct research efforts for a better estimation accuracy. As we will see below, this will be realized by assigning a grade/ percentage depending of each project’s purpose and the actual status of each major risk areas.

Before we present in detail how we calculate the risk that describes one of these areas (for our demo, we chose ‚Environment’), it’s important to know the major interest areas and our list is represented by:

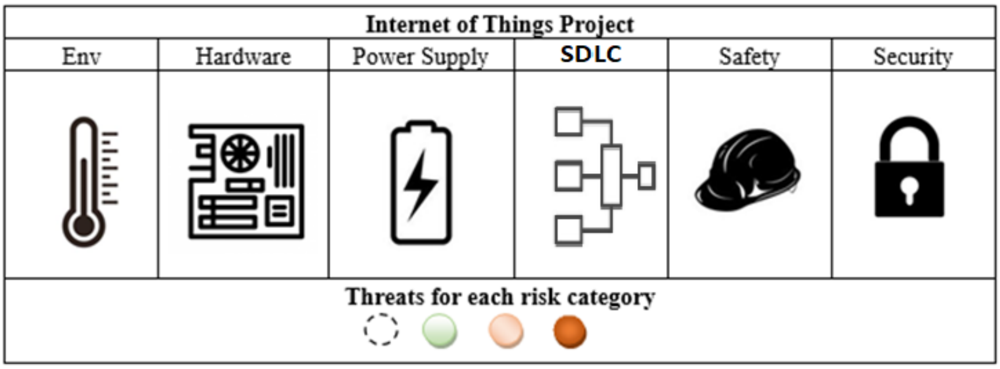


Figure 2.2 *Major risk areas for IoT projects*

As we can see above, the major risk areas are represented by:

- ‘**Env’** abbrev. **Environment**) - for deployment environment risk
- ‘**Hardware’** - for physical components hazards
- ‘**Power Supply’** – for power supply risks
- ‘**SDLC’** – used to cover the project delivery risks
- ‘**Safety’**- for risks related to work accidents
- **‘Security’** – for software security flaws and black hat attacks

As we stated in the introduction, each of these major risk areas includes multiple categories which are granularly split across different risk factors.

During this chapter, we detailed each of these specific risk factors along with their grading based on the desired project. For a better understanding of this topic and also of the hierarchical order of risk factors, we have the following figure which was specially created to document the risk analysis of the deploying environment hazards for a case study represented by a relevant project with high practical value. This project is an IoT Avalanche Prediction Project and can be seen in the following figure:

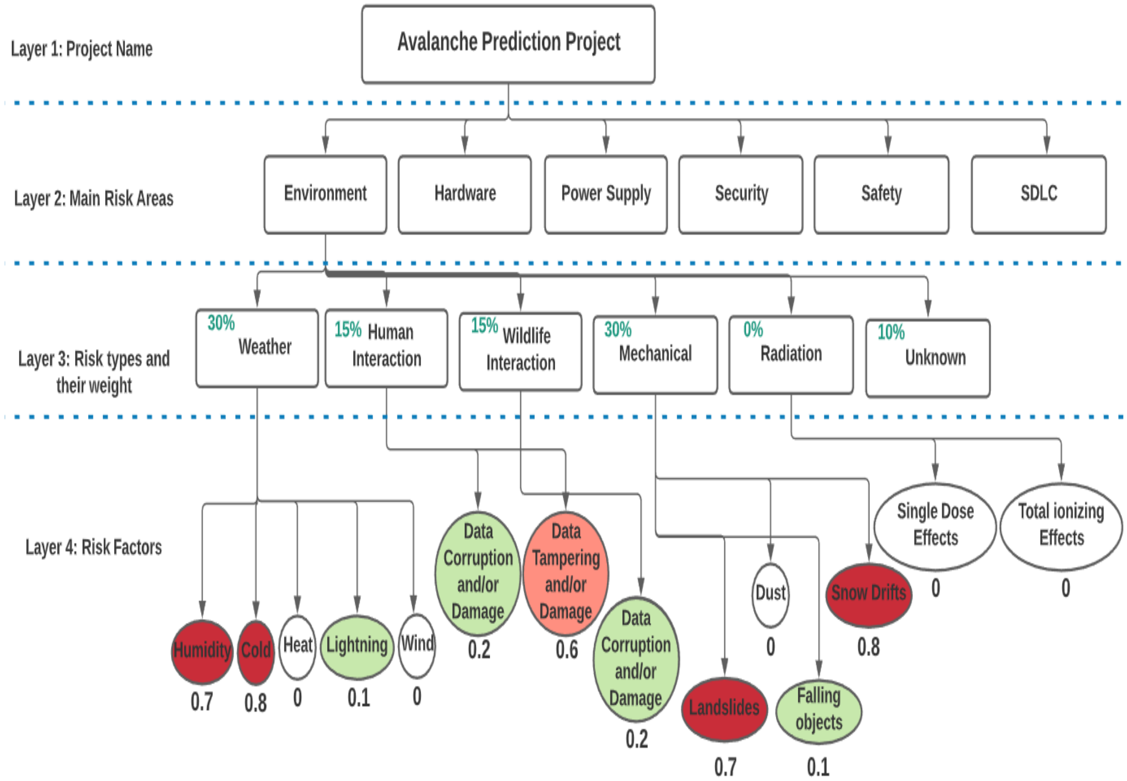
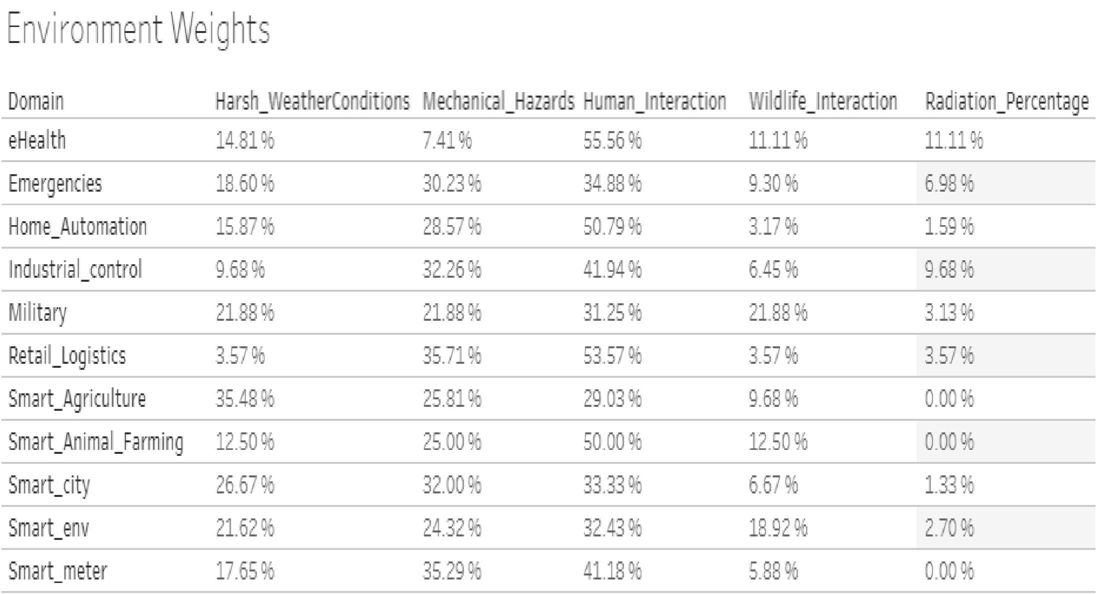


Figura 2.4 *'Environment' major risk area for IOT Avalanche Prediction Project*

By carefully inspecting the Figure 2.4, we can see that we have two types of numeric data: the first one belongs to the [0,1] interval and the second one is written in green and represented as a percentage. The first set is the individual grading of the beneficiaries of our analysis (these values are specific for each project individually), and the percentages represent the collected weights based on the IoT domain for the assessed project. These values are the result of the first survey sent to the IoT specialists. There is a journey from their response to an accurate percentage and it's detailed withing the 5th chapter of this thesis.

The deliverables are represented by the weight tables for each of the major risk areas described in the beginning of this chapter. The tables with updated values, based on the most recent answers, can be found in the special annexes section of the thesis. For a better understanding of our approach and also of our calculation method, when we presented the case studies, we used rounded values. Note that the green values are rounded percentages and the values from the official weight table are more accurate, with two decimal points precision. The rounded values were used to help the reader understanding the calculus for each project that was chosen for the case studies during this chapter.

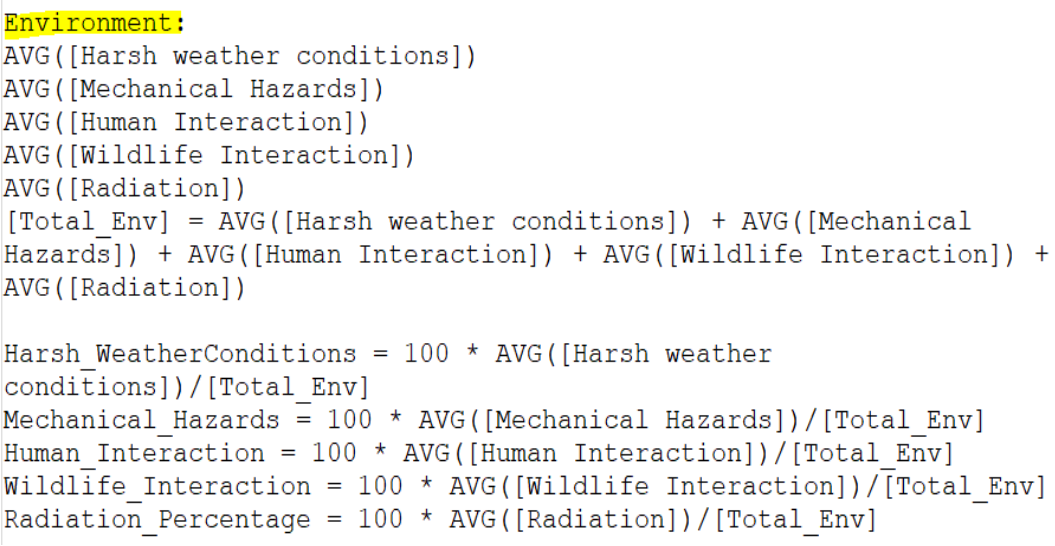
As we can see from the following figure, we chose one updated table with the real weights and also the Tableau formulas behind it:



Environment Weights

Domain	Harsh_WeatherConditions	Mechanical_Hazards	Human_Interaction	Wildlife_Interaction	Radiation_Percentage
eHealth	14.81 %	7.41 %	55.56 %	11.11 %	11.11 %
Emergencies	18.60 %	30.23 %	34.88 %	9.30 %	6.98 %
Home_Automation	15.87 %	28.57 %	50.79 %	3.17 %	1.59 %
Industrial_control	9.68 %	32.26 %	41.94 %	6.45 %	9.68 %
Military	21.88 %	21.88 %	31.25 %	21.88 %	3.13 %
Retail_Logistics	3.57 %	35.71 %	53.57 %	3.57 %	3.57 %
Smart_Agriculture	35.48 %	25.81 %	29.03 %	9.68 %	0.00 %
Smart_Animal_Farming	12.50 %	25.00 %	50.00 %	12.50 %	0.00 %
Smart_city	26.67 %	32.00 %	33.33 %	6.67 %	1.33 %
Smart_env	21.62 %	24.32 %	32.43 %	18.92 %	2.70 %
Smart_meter	17.65 %	35.29 %	41.18 %	5.88 %	0.00 %

Figure A7.2 *Updated table with major risk areas weights based on domain - 2*



```
Environment:
AVG([Harsh weather conditions])
AVG([Mechanical Hazards])
AVG([Human Interaction])
AVG([Wildlife Interaction])
AVG([Radiation])
[Total_Env] = AVG([Harsh weather conditions]) + AVG([Mechanical
Hazards]) + AVG([Human Interaction]) + AVG([Wildlife Interaction]) +
AVG([Radiation])

Harsh_WeatherConditions = 100 * AVG([Harsh weather
conditions])/[Total_Env]
Mechanical_Hazards = 100 * AVG([Mechanical Hazards])/[Total_Env]
Human_Interaction = 100 * AVG([Human Interaction])/[Total_Env]
Wildlife_Interaction = 100 * AVG([Wildlife Interaction])/[Total_Env]
Radiation_Percentage = 100 * AVG([Radiation])/[Total_Env]
```

Figure A6.2 *Tableau formulas used to calculate the weights - 2*

In conclusion, this chapter was created to document the major risk areas that we need to cover when using our risk assessment method. Independent analysis processes were applied to multiple case studies for us to understand how projects from different domains are affected by the same risk factors. All the case studies were actual IoT projects where I was involved, ranging from Quality Assurance resource to Product Owner. Even so, for a more accurate formula this is not enough and we need larger expertise and opinions, this being the reason why we started the study that involved multiple IoT specialists. The power of these weights lies in the number of responses that we receive. More responses mean more accuracy of our method.

Chapter 3

Agile methodology for IoT projects delivery

This chapter contains an objective documentation of why the Agile methodology is recommended for IoT projects delivery. For a better understanding of applying Agile fundamentals, we backed our research with a case study, represented by a home automation project (‚Smart House' type project). Even more, we compared Agile to other known methodologies, such as V-Model of Waterfall, we highlighted how we can mitigate or even solve the specific IoT challenges by choosing the right software delivery method. Naturally, after presenting the required steps when implementing our case study, we summarized all the conclusions in a well-structured list containing all of this methodology advantages.

The main advantage is represented by the quality of the implemented project. By splitting the product delivery in multiple iterative cycles, so called ‚sprints', we encourage the interaction between the QA team and the product itself. From a quality point of view, the testing team is present during all software delivery cycle, so the product is constantly verified, with even some mandatory exit criteria that should be met so we can advance with the project delivery. By following the thesis, we will observe solid connection between the Agile particularities and the risks that can be mitigated from the SDLC major area presented in Chapter 2. Due to the fact that many of the potential software defects (the so called ‚bugs') are addressed very early in the SDLC, the main risk category, represented by costs, are considerably decreased.

The next important advantage is represented by transparency over the project. This transparency is resulting from multiple mandatory meetings when we use Agile Scrum as delivery method. When we develop an IoT project, we expect a lot of changes, even more than for a normal software project [12]. These should be addressed with the client for us to decide if they impact de initial purpose. Another layer of transparency that should be addressed is present within the delivery team. Agile is also indicated for this, because this methodology implies constant productive interaction between QA and development teams [13].

Related to the actual risks, especially on their overall cost impact, by using Agile we can discover them from an early stage. The possibility of identifying them and also solving the risk factors leads us to another advantage, which is represented by the flexibility of this method. When discussing about this IoT domain, we must expect a number of updates which is larger than usual. We must adapt and overcome these deviations as part of the same delivery process. Even more, if the client needs new requirements or requires the updating of the existing ones, the development team should have the time period buffers to solve implement or update them.

Another advantage, which was specified also in the introduction is the target fast entry to market, which is a must in an innovative domain such as IoT. Usually, these projects are built to cover real market needs, ranging from smart houses to smart cities, eHealth, military and so on. By activating in a such innovative environment, there is less time to analyze the competition. Moreover, there is a high chance that the first product that enters the market indirectly gains a notable reputation advantage. By having this, it's much easier for the owner to become a market leader in the future. Speaking of Agile, one notable difference between it and other SDLC methodologies is that Agile encourages early releases of the product. Currently, we deal with a high level of needs within the market, and the growing of this need is estimated to hit 26% in 2026 [14]. Another interesting statistic is represented by the fact that projects which are delivered using Agile are getting to market 37% faster than projects that are using Waterfall methodology [15].

The next advantage in our list is represented by the constant feedback present within this methodology. The client is involved starting from the first sprint in team's development efforts, his confirmation being one of the exit criteria of the spring. Moreover, by constantly interacting with him, the client is encouraged to discover and come with new functionality suggestions that weren't discussed when the project was accepted. Along with the product development, the client has enough time to research the market itself and can address all of his findings with both product owners or project managers. As a naturally consequence of this solid interaction, the professional relation between the team and the client improves, this leading also to great reputational gains and market visibility. Even more, a happy client is a loyal client, so this method encourages future interactions or contracts, recommendation etc. All of these aspects contribute to a solid portfolio for the development company and also determines high level of trust within the market. Both clients and implementation companies will benefit from this productive collaboration. Nevertheless, the key point here is flexibility, meaning that the client can choose the level of interaction with the development companies, based on his needs. As a conclusion, the communication between client and IoT companies is very important, and Agile flexibility can provide it, especially in the IoT context. Applying Agile leads both to increased efficiency of this method and risk mitigation from SDLC major risk area. The IoT domain is considered a healthy development environment which constantly encourages innovation in a fast pace. It's very important for us to keep up with this rhythm and improve the delivery methods.

Chapter 4

Tableau tool for IoT projects monitoring

Within this chapter, we explained why we recommend Tableau when thinking about mitigating risks from both data processing and display area for IoT projects. From a functionality point of view, Tableau can parse and process massive data files that can be stored both locally or on dedicated servers. For the majority of IoT projects, we need that the acquired data to be available in a real-time manner so we can consult it every time we need. We can display relevant information from different database servers across multiple technologies such as Oracle, Microsoft SQL Server, Amazon Redshift [16]. Even more, we can parse the most known file formats, such as text, JSON, Microsoft Excel, PDF.

This high diversity in the data sources area provided by the Tableau tool is mapped very well with the multiple data sets acquired by the IoT projects. High loads of data are involved when implementing monitoring and execution IoT projects [17]. In order to highlight the Tableau advantages, similar to other chapters we chose a case study, represented by an IoT project with significant volume of data that needs to be processed and passed to a real-time monitoring process. The Tableau integration with IoT projects provides the development environment healthy advantages such as:

Diversity - provided by the two available connection types represented by ‚Live’ (for projects that require constant data update, such as Smart Parking, Smart Irrigation, Smart Metering, Traffic Management, Home Automation projects) or ‚Extract’ (for projects that work with more static data that shouldn’t be updated so often, such as ‘Avalanche Prediction’, ‘Weather Stations’, ‘Air Pollution Monitoring’, ‘Garbage Monitoring’).

Applicability – Tableau Dashboards can be displayed on a high range of devices. When we create a dashboard, we can easily select the compatible devices on which our interface should be available. We are talking, of course, about the most known devices such as computers, tablets, mobile phones etc. The interface of our case study was designed to be implemented on mobile phones, so it can be used by car passenger [18]. There is no need in creating from scratch a webpage by using the provided default libraries (such as Xively for Arduino).

Scalability – every time when we need to expand the project and add new components, we can add an infinite number of stations and/or sensors without affecting the basic displaying functionalities of the application. Even if the disk space used is increasing because of the additional data, the parsing, sorting, modelling and displaying functionalities are remaining the same. For the disk space issue, we can implement some cleaning routines at certain periods.

Chapter 5

Validating risk factor weights using the survey method

During this chapter, we will explain the relationship between the respondents answers and the final weight tables. We will see how our survey has two main areas.

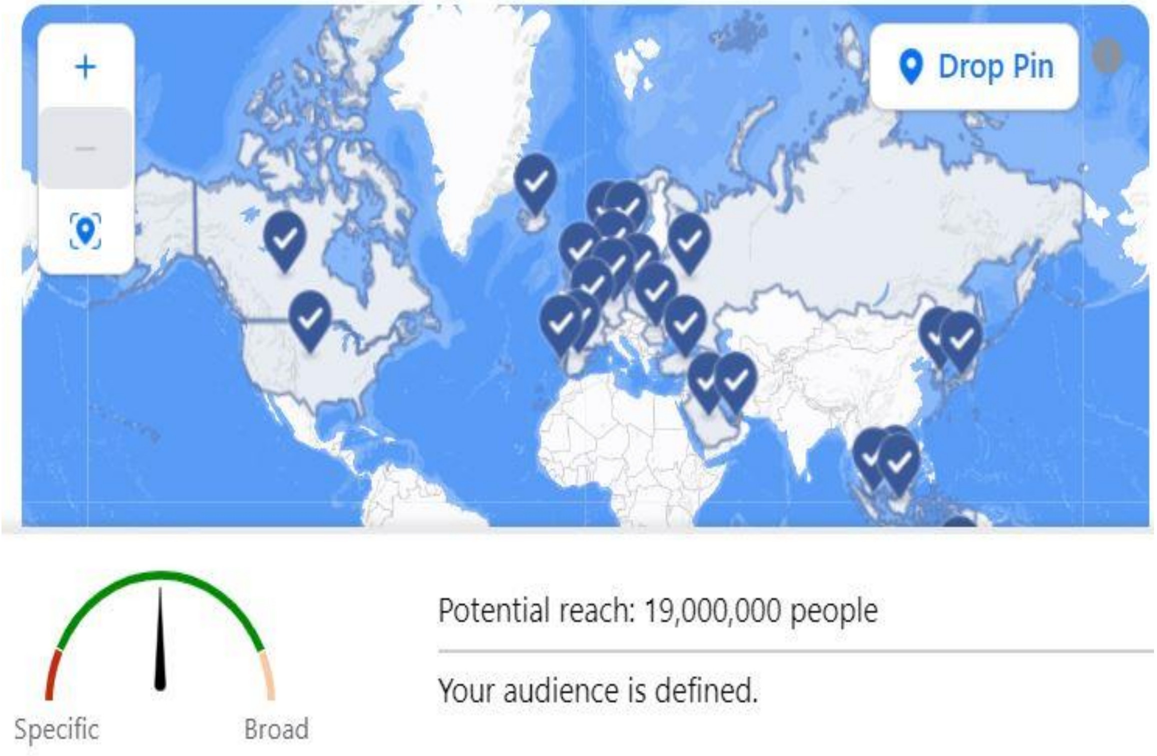
Based on the answers of both question sets, we will also argument how important is each of the chosen major risk areas and how we can organize them based on the already known parent domain, the job description within the delivery team of the respondents, how the risk is perceived by the resources working on these projects and also the overall interest and product distribution over the geographical areas.

5.1 Choosing the right audience for the survey

Before presenting the actual survey, it's imperative to understand how we chose the audience for it. The initial purpose was to approach the technical individuals which were involved in IoT projects delivery. If they delivered multiple projects, it's accepted to complete one survey for each of the resulted product. So, the first filter was represented by selecting both IoT specialists and generalists. In order to approach them, first we emailed the authors of the scientific articles used to research useful information for this thesis.

In order to approach the generalists, we started using sponsored campaigns on Facebook, also we constantly posted the survey link alongside with a QR code in IoT specialized groups. Even more, we used websites that were dedicated to survey exchange. As we can see from Figure 5.1, one of the criteria used to choose the population was represented by the geographical area. We opted for certain developed countries from an IoT point of view, such as USA, Canada, the majority of Europe countries and important Asian hubs such as India, Indonesia, Singapore, Malaysia and so on. Below that, represented in Figure 5.2 we can see the filters that we applied for an audience fine tuning process. It's important to know that the data relevance is both obtained and preserved by knowing and selecting the right audience, that's why we aimed for technically rich people, interested in trends like IoT, Robotics, Arduino and Big Data.

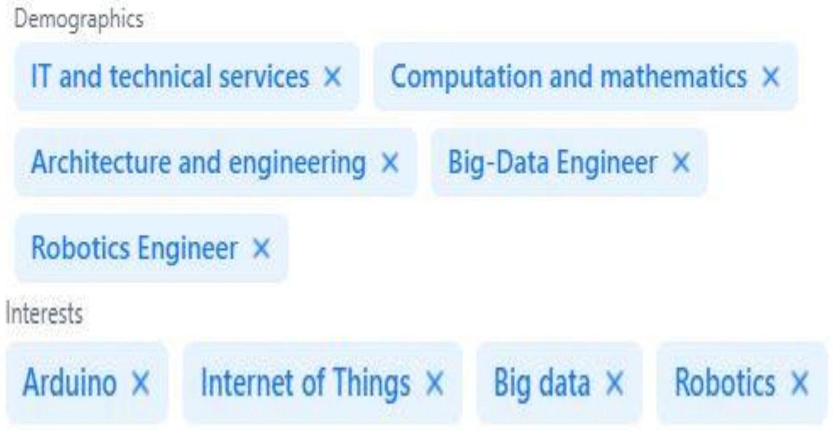
We have the tendency to assume that a bigger audience means more answers and indirectly more relevance, but we need to remember that the main goal here is that the study should include only people that interacted with this Internet of Objects domain.



Potential reach: 19,000,000 people

Your audience is defined.

Figure 5.1 *Choosing the relevant audience from a geographic point of view*



Demographics

IT and technical services ×
Computation and mathematics ×
Architecture and engineering ×
Big-Data Engineer ×
Robotics Engineer ×

Interests

Arduino ×
Internet of Things ×
Big data ×
Robotics ×

Figure 5.2 *Chosen filters for a more targeted campaign*

After applying all the above filters, we can see that the audience is satisfying. We have a total of 19 million users that can be potential resources for our study. This assumption is confirmed also by the 'Your audience is defined' which can be seen in Figure 5.1. When conducting a sponsored campaign, we are usually warned that the audience is broad and the message may not be sent to the most relevant pool of users. On the other side, the audience may be too specific. We are also warned and t might be a chance to receive less responses if the campaign is starting.

For us to create and start this campaign, we needed a Facebook dedicated technical page where we constantly posted the progress. After defining the audience, the next step was represented by the questions sets that we chose, so we can have a relevant study for our risk assessment applications. Details of the question sets can be seen in the following section.

5.2 Choosing the survey questions

Within this chapter, we can see that we have different sets of questions, each one with a purpose in mind. So, the first set was crafted to know even better our audience and the useful metrics of the projects in which they were involved.

Below, we have the first set of questions which is split in:

- Which was the domain of your latest IoT Project?
  Answer Options: each one the already addressed domains (eHealth, Smart City, Military, Demotic and Home automation, Retail/Logistics etc.)
- Which was your role within the IoT project team?
  Answer Options: each possible job descriptions within a delivery team for IoT projects (Developer, QA, Project Manager, Product Owner, Scrum Master) and individual projects
- Which was the name or main functionality of your latest IoT project?
  For this question we don't have any answer options, but instead we have a text box where a string is mandatory. We will use the information from this field to have a better overview of both possible IoT applications and functional diversity that describes these types of projects.
- Do you think that risk assessment procedures add value to IoT projects?
  This question is optional and has three predefined answer options represented by Yes, No, Don't Know. This question was asked for us to see if the IoT specialists of generalists considered this aspect when they delivered or estimated a IoT project.
- What do you know about risk assessment for IoT projects?
  This is not a mandatory field and has no answer options. We are provided with a text box that has no restrictions so we can see what is the current level of awareness within our respondents.
- What SDLC was used when you delivered your latest IoT project?
  Answer options: Agile, Waterfall, V-Model, Big-Bang, Other SDLC
- Was your project designed to comply with work safety procedures?
  Answer options: Yes, No, Don't know/Not my job – this question was asked so we can see what is the current level of work safety procedures awareness within our respondents.
- What country do you live in?
  This question is not mandatory but it helps us understand the geographical distribution of the respondents.
- Please provide your email address if you want to receive both the results and conclusions of this study Also, this question is not mandatory because we don't want to store respondent personal information. The specialist which provides his email address will receive a detailed analysis of his project after the results of this thesis are published.

This was the first set of questions and we will use it to generate the demographic reports for a better understanding of the IoT context over the world.

One of these reports is the one from Figure 5.3 where we have a relative uniform distribution based on their implementation domain. Also, we can see from Figure 5.4 the job description distribution of all the human resources that participated to our IoT Risk Assessment Study.

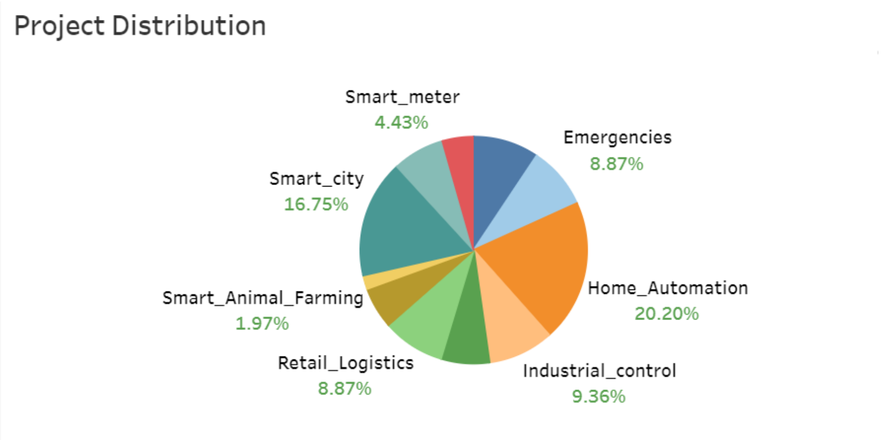


Figure 5.3 Visual representation for project distribution based on the implementation domain

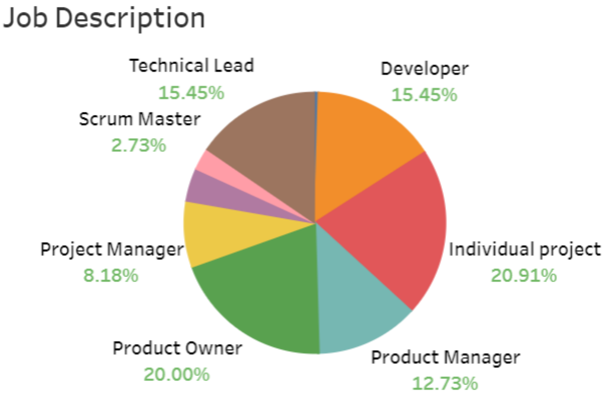


Figure 5.4 Demographic report relevant for respondent job description within his IoT project

The second question set has the main purpose of populating weight tables for each major risk area. All of these values are getting more accurate directly proportional to the number of people that responded to our survey. Speaking of this number, the weights are considered ideal if we achieve a requirement of 2700 respondents. Moreover this 2700 value is related to other significant metrics that describe our study. Between the most relevant, we remind of the target confidence level of 99% with a margin of error equal to 2.5%.

Back to the question set, with answers that determine the exactly percentual results, we have the following list:

- Which was the domain of your latest IoT project?
  Answer options: each one of the already addressed domains described in previous chapters (eHealth, Smart City, Retail/Logistics, Military etc.).
  We can observe that this is a common question with the first data set. Besides of its demographic importance, this is the main criteria used to calculate the weights. The user is interested in the risks specific for a certain domain, and it's easy to understand why a project from the smart agriculture area has more environmental risks that a home automation project.
- After possible deployment of your project, it can be affected by:
  Answer options: harsh weather conditions, mechanical hazards, human interaction, wildlife interaction, radiation.
  This question was asked so we can cover the ‚Environment' risk area.

- Which of the following vulnerabilities were addressed during project development?
  Answer options: DB Injection, Broken Authentication, using components with known vulnerabilities.
  This question was asked so we can cover the ‚Security' risk area.
- What hardware equipment did you use when building your latest IoT project?
  Answer options: acquiring elements (analog sensors, digital sensors), execution elements, additional physical equipment.
  This question was asked so we can cover the ‚Hardware' risk area.
- What challenges did you faced during the project delivery?
  Answer options: estimating costs, more people were needed, not enough visibility and transparency over the project, faulty planning, the client changed his mind too often, not enough testing for deliverables.
  This question was asked so we can cover the ‚SDLC' risk area.
- Power Supply Management – Did you used:
  Answer options: Batteries, Wall sockets, code routines to increase battery lifetime, solar panels with accumulators, USB for power supply, removed unnecessary power consumers.
  This question was asked so we can cover the ‚Power Supply' risk area.
- The physical equipment deployed after finalizing my latest IoT project:
  Answer questions: generate loud noise, toxic fumes, electrocution etc.
  This question was asked so we can cover the ‚Safety' risk area.

After addressing these questions, the answers will be processed by our calculus method and they will generate weights based on the implementation domain. This will lead to a very complex and customized risk management process that can be easily targeted on the customer needs.

5.3 From survey question to weight variable

An interesting exercise is to transform the survey answers in the needed weight variables. When talking about these variables, we are thinking of the percentages used to populate the wight tables for each major risk area. Let's see, for example, the major risk area represented by ‚Environment' with the specific weights in Figure 5.5 below:

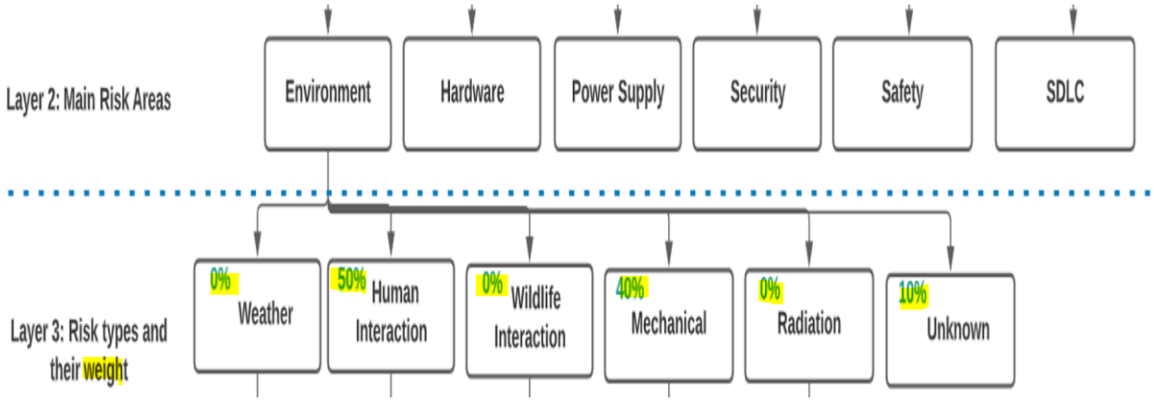
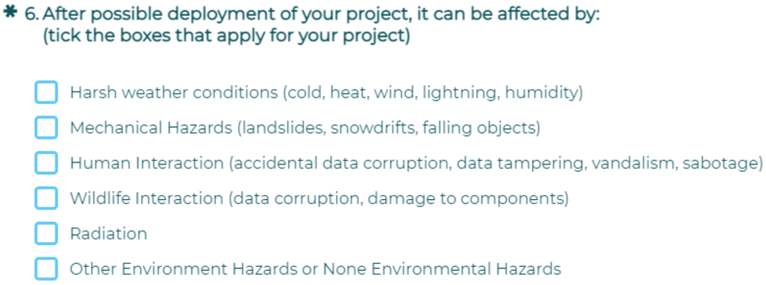


Figure 5.5 *Examples of rounded values for the category's weights*

The first step after calculating the weights is achieving a large number of survey answers. Continuing on the same ‚Environment’ topic as main risk area, let’s see the question from the second set, represented by: ‚*After possible deployment of your project, it can be affected by:*’, with the already known answers of mechanical hazards, harsh weather conditions, radiation, wildlife interaction, human interaction. Below, in Figure 5.6 we have survey area dedicated for this question:

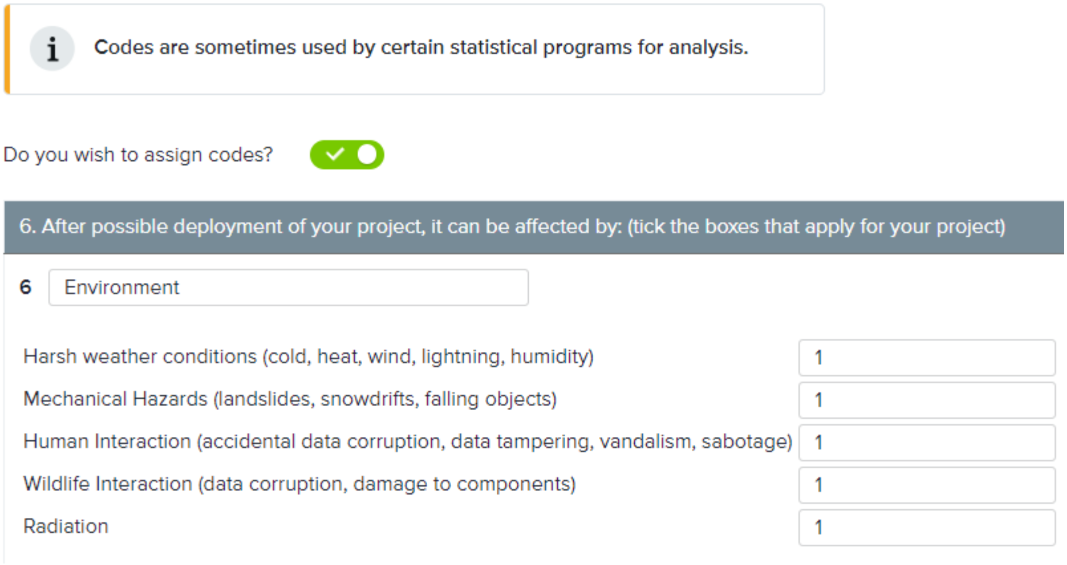


✱ 6. After possible deployment of your project, it can be affected by:
(tick the boxes that apply for your project)

□ Harsh weather conditions (cold, heat, wind, lightning, humidity)
□ Mechanical Hazards (landslides, snowdrifts, falling objects)
□ Human Interaction (accidental data corruption, data tampering, vandalism, sabotage)
□ Wildlife Interaction (data corruption, damage to components)
□ Radiation
□ Other Environment Hazards or None Environmental Hazards

Figure 5.6 *Question asked to the relevant audience in order to calculate weights from specific major risk area, represented by ‚Environment’*

In the above figure, we can see that each answer option is explained, encouraging the person that fills in our survey to think about all the possible scenarios which can occur after the project goes live. This aspect contributes to an increased awareness about the risk assessment process, which is very important when delivering software. For both creation and survey distribution, we used a paid service, represented by the SoGoSurvey tool. We chose this service because it had different advantages, such as the diversified functionality options and also the possibility to assign specific values to the answers. Why do we need to assign these values? The answer is that, using aliases and Boolean types for data, it will be easier to generate relevant statistics and map the values to percentages. Moreover, we can use these values to structure a more solid data source for Tableau. After presenting the questions and getting answers, the next step is the data export. We can see in the 5.7 figure below all the data that was considered relevant for answer representation:



i Codes are sometimes used by certain statistical programs for analysis.

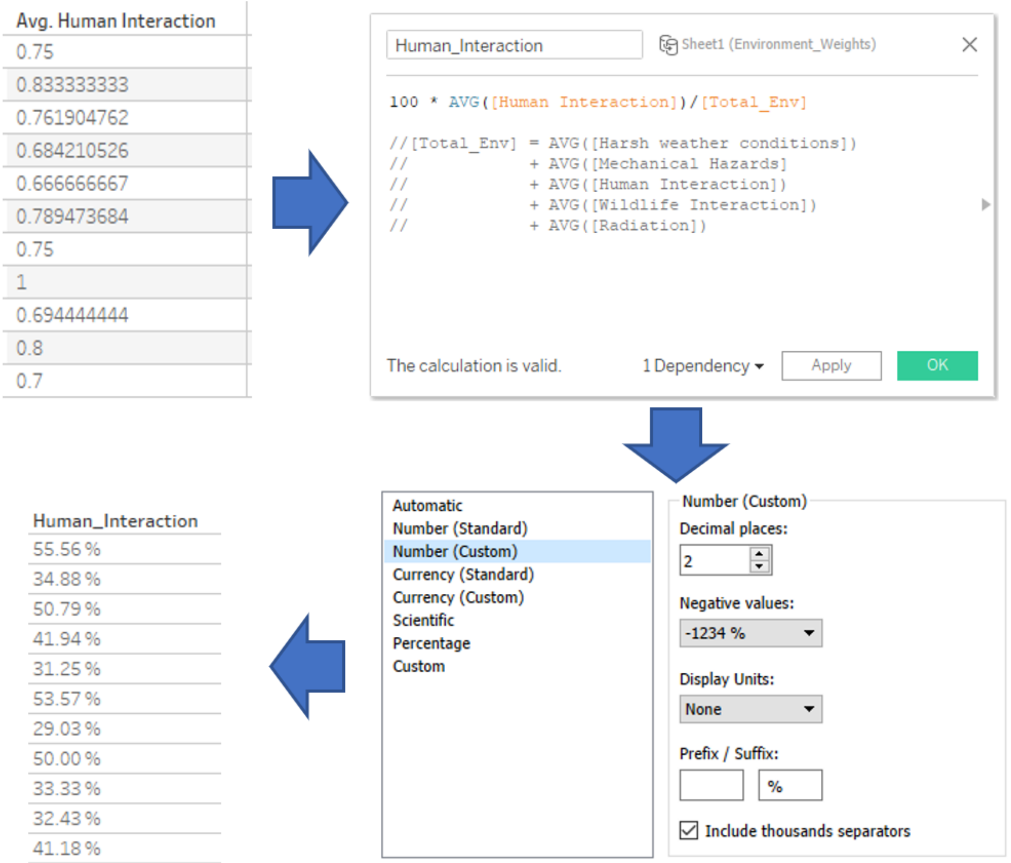
Do you wish to assign codes? ✓

6. After possible deployment of your project, it can be affected by: (tick the boxes that apply for your project)

6	Environment
Harsh weather conditions (cold, heat, wind, lightning, humidity)	1
Mechanical Hazards (landslides, snowdrifts, falling objects)	1
Human Interaction (accidental data corruption, data tampering, vandalism, sabotage)	1
Wildlife Interaction (data corruption, damage to components)	1
Radiation	1

Figure 5.7 *Assigning Boolean types value so we can generate relevant statistics*

We assigned the value 1 every time when a specific answer option was chosen, meaning that in our exported excel file we will have a list with all the answers mapped with this value. If a respondent chose both the first and last answer option, each of the corresponding columns will be grated with 1. For all of the other options we will have three NULL values which translate to 0 in the final formula. In order to realize a relevant statistic based on the IoT domain, we will also export the answer to the first question that is common in each of the sets. We chose the 0 and 1 values, because when we are applying the arithmetic mean on each column, it will be much easier to convert the resulting value in a percentage. Each major risk area is split in different categories and we calculate the total of the category values. If we keep in mind that we also have an ‚unknown' parameter of 10%, the total should be 1 (100%). After we have the total categories sum, we will calculate the percentage of each category from the total sum. All the applied functions are part of the aggregating process crafter to generate easy to read values that can be used also in our calculation method. The data processing based on the assigned values can be seen in Figure 5.9:



Avg. Human Interaction
0.75
0.833333333
0.761904762
0.684210526
0.666666667
0.789473684
0.75
1
0.694444444
0.8
0.7

Human_Interaction

Sheet1 (Environment_Weights)

```
100 * AVG([Human Interaction])/[Total_Env]

//[Total_Env] = AVG([Harsh weather conditions])
//            + AVG([Mechanical Hazards]
//            + AVG([Human Interaction])
//            + AVG([Wildlife Interaction])
//            + AVG([Radiation])
```

The calculation is valid.

Number (Custom)

Decimal places: 2

Negative values: -1234 %

Display Units: None

Prefix / Suffix: %

☑ Include thousands separators

Human_Interaction
55.56 %
34.88 %
50.79 %
41.94 %
31.25 %
53.57 %
29.03 %
50.00 %
33.33 %
32.43 %
41.18 %

Figure 5.9 *Data processing necessary for getting an easy-to-read percentage*

For our risk assessment application, we chose Tableau because, besides the complex monitoring functions, we can define useful actions to navigate between dashboards and reports. Each of the weight value can be opened with just one click and lies in a separate webpage which is constantly updated as soon as we process different batch of survey answers. The values within tables have informative purpose and also applicative when we use the wights to calculate the final risk for a target project. We can see the main page of the interface in the following figure:

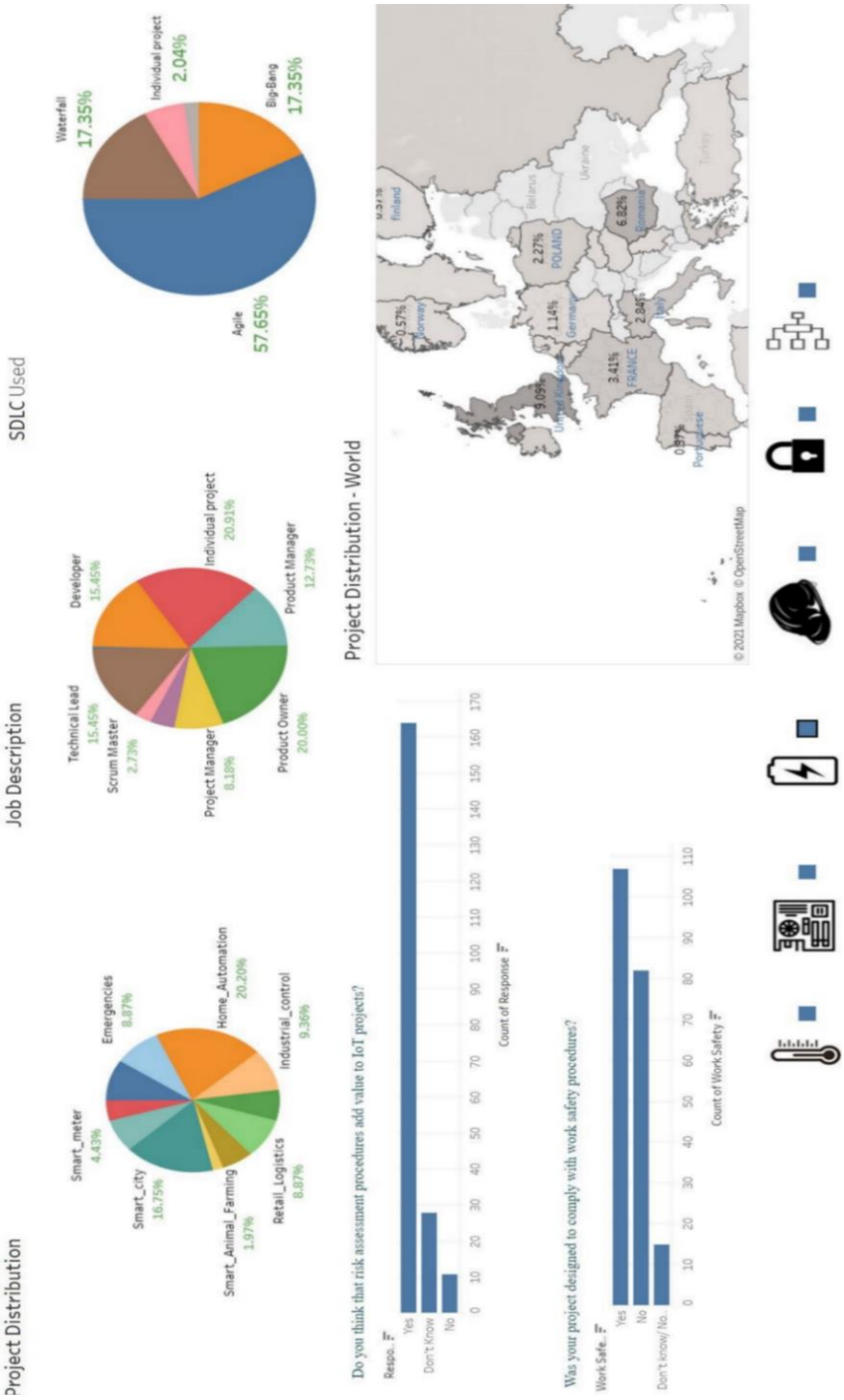


Figure A5.1 *Tableau interface for the risk assessment application*

Chapter 6

Conclusions

First of all, the total risk of the IoT project should be as close to the zero as possible. Moreover, we also need a small buffer that should cover the unexpected risks that weren't covered where the analysis was performed. There is no software application or project that have zero risks. Secondly, the total percentage coverage should be as close as possible to the full value of 100% which is also an ideal one. There is no existing application that hasn't any vulnerabilities or uncovered areas [19].

In a more practical, closer to reality way, the individuals which are project managers or technical leads for the delivery teams should be aware of these values before starting the implementation process. Discovering risks as soon as possible in SDLC leads a cost efficiency but also a better management of the human resources that are working on the project. This approach can bring major improvements to estimation practices, especially when using Agile as software delivery method [13]. We explained in chapter 3 why this method is preferred when we are developing an IoT project. Besides the cost efficiency by early risk discovery, this assessment process can add value also the negotiation portfolio when bidding for a specific project. A lot of the benefits are influencing also the customer, which is the direct and most important stakeholder, that receives the product from the development team. A complete risk analysis process leads to a transparent relationship and a productive collaboration by highlighting several KPIs that can be achieved easier when addressing targeted issues from the development process.

By applying each step of our ‚framework' when building a project, it helps us understand what we need to buy and early implement for minimizing initial risk, therefore to proactively contribute to our project success. In other words, if we see a high value for a major risk area, we ca think of specific mitigation actions that can be performed, not for a higher grade, but for minimizing the potential flaws within that area. One of the first benefits of these analysis is represented by the achieved awareness when talking about hazards that have roots above the information security area. The next step is represented by the precision that we use in order to address the issue. After that, by using this method, we contribute to a large database that can be queried anytime so we can obtain very useful business statistics. These statistics can be demographics of technical ones that can be used as checkpoints when analyzing similar Internet of Things projects. One example of such a statistic is that only 26.78% of the human resources involved in IoT Smart City project delivery didn't have a problem with estimating costs. Moreover, a great percentage of the people that didn't have a precise job within IoT area weren't aware of the security flaws that can affect their project. Even more, they had difficulties choosing the right SDLC for their project. It takes some software delivery knowledge to state that you are using a special SDLC method called Big-Bang for your individual project.

When accepting and bidding for a technical IoT project, it's useful, maybe imperative to inform the customer that we already know about the potential risks within that area and we also have specific solutions for carefully managing the assigned budget that we want to invest in project development.

6.1 Obtained results

From an obtained results point of view, we can say that we achieved the majority of the objectives defined when we started the research activities, both fundamental and applicative. For a better traceability, we will present the specific results, based on the chapter number where they were elaborated. After the introduction chapter where we presented the desired research directions, the next chapter was dedicated to defining the chosen major risk areas and also to applying our risk factor grading method to a specific IoT project.

So, the main contributions that were highlighted during the research activities can pe presented as below.

Starting with chapter 2 from the thesis, we defined the major risk areas that impact the IoT projects and we dissected them in categories and specific granular risk factors. Each zone has its own dedicated section with a paired case study for us to better understand how the beneficiaries can apply our method by choosing their specific risk factors. Also, within the same chapter, we documented the equations used to build the calculus method. These are revolving around the major risk areas weights depending on the implementation domain and also by the arithmetic mean of the risk factors within a category. So, besides information security area, we identified important major risk areas, such as power supply, deploying environment, work safety, hardware area and software delivery methods area. Each of these have a specific weight table based on the occurrence frequency within a certain domain. We created these tables after conducting a study involving both IoT specialists and generalists. Based on this study, we saw what area has a more relevancy in specific domain – keep in mind that our list includes a number of twelve relevant IoT domains (eHealth, military, demotic home automation, smart cities, smart agriculture, smart farming, retail/logistics, smart metering, security and emergencies, industrial control, smart environment). Also, in the same chapter, we highlighted how we can assign a grade to a risk factor. This process is realized with the help of other survey sent to direct beneficiary of our method (company, project manager, technical lead, architect, individual developer etc.). By sending this survey, the customer grades the risk factors for his domain based on its own needs, objectives and specific constraints. When the client has a difficult time and can't provide a relevant value, we can use default values that are provided by other updated studies conducted by Eurostat and Project Management Academy. As a small and relevant example, if we are thinking about the 'managing the conflicts within a team' which is included in the 'Human Resources' category which is also included in 'SDLC' major risk area, it's pretty difficult to estimate the risk before knowing, even work a small period of time with the delivery team. Therefore, it is safe to have a risk factor default value of 0.09 for our methods (as we stated in this section, we saw that 9% of projects failed due to conflicts within the development team). Based on the specialized literature, we are the first that propose a calculus method for quantify and analyze the risk from multiple IoT areas regarding IoT projects. So, based on relevant data resulted from the conducted study, we, at least, increased the risk awareness between the people that participated. Our risk assessment method will be more precise directly proportional with the number of the survey received answers.

The thesis third chapter proposes a risk mitigation solution by adopting a delivery method which has a lot in common with IoT trend and its evolution within the rapid technology development within this context. This delivery method is represented by Agile, and within this chapter we presented the advantages and how approaching them can lead to a drastically risk decreasing process, especially in the SDLC major risk area. This analysis was performed by using another case study with steps mapped directly on the Agile methodology principles and milestones. Because of its flexibility and also the possibility of addressing the risk factors from the previous chapter, we recommend using this methodology both developing and delivery of IoT projects.

Similar to this, the fourth chapter has another risk mitigation recommendation represented by the using of a data processing and project monitoring toll which is, of course, Tableau. Within these pages, we highlighted the fact that many of the IoT projects requirements can be covered. For achieving this, we chose a case study which was based on real market need, which is represented by a smart parking project. The implementation of the processing and monitoring solution was realized with zero costs, because we used the free version of this application. We recommend using it for monitoring and displaying, because addresses a large part of the risk factors presented in the second chapter., especially in the physical components area. Tableau can provide a very useful solution when working with large volumes of data, also providing the possibility to sustain major parts of the processing logic in real time, moving it from the processing boards integrated with the acquiring and execution elements.

During fifth chapter, last one before the conclusion part, we had a main goal of validating the weights, by using the survey method and also processing the responses using Tableau. We started by defining the required audience for us to provide IoT study relevance. At first, we expected a lot of responses, so a great challenge was represented by both choosing and managing the large volumes of received data. As long as the chapter was written, we presented the useful formulas needed for defining each category weight, so we can use them in our final calculus method. Even more, we highlighted the proposed technical solution needed to transform the answers for our survey into final grade value. As we already know, we used Tableau even for our risk applications because it had all the required functionalities so we can provide an easy and intuitive interface, where the user can see all the updated values and metrics. Additionally, based on this information which is updated each time we process several response batches from the targeted customers, we created variables used to calculate the final grade based on the risk value for the project itself. These will be applied on the specific responses received from our client. Even if this final grade is a useful and interesting reference, we will also provide for our customer detailed analysis for the areas that contributed to this final grade.

The advantages of using such a method which is not present in the already articles and scientific communications when the thesis was written, will ease the decisional processes needed if an individual or company are interesting in choosing, developing and delivery of Internet of Things projects. This last chapter comes with relevant information which demonstrates that the risk approach discussion can be held in different areas, but the security information and software vulnerabilities. Even more, within this chapter, all the provided data and solutions represent an important step on our quantification journey when talking about risks that seem inapproachable or unexpected.

6.2 Original contributions

We will dedicate this section to document the original contributions that were detailed during the thesis. So, we will start, from a business point of view, with the needs and constraints that are specific to the IoT area, the most important part that motived us to write this thesis. Based on this, we have the following original contributions:

1) Recognizing and documenting the need of a calculus method so we can quantify the risk present in other domains, besides the information security part. The need and the actual status were presented within the first scientific report which is documented in the following section at [25]. For a better understanding of this topic, I choose examples from my professional experience, being easier to highlight uncovered risk areas. One of these examples is represented by the avalanche prediction module which is impacted by a great number of risk factors, especially in the deploying environment area. The case study was published and detailed in the scientific article that can be found in the following section at [20]. Going through the written thesis, we can find these aspects in the introduction and also in chapter 2.

2) Presenting specific risk factors from new major risk areas that can affect Internet of Things project and the actual structuring process for a classifying and representation method. These aspects were documented in both scientific article and report from [21,27]. These are generously detailed in chapter 2.

3) Elaboration a calculus method so we can represent the weight of the risk factors based on the most recent domains where we implement IoT projects. These was presented in the scientific report from [26]. For a specific risk quantifying method structured around another case study, we published the formula that we conceived in the scientific article from [24]. Going through the thesis, the method based on the major risk categories is presented within the second and fifth chapter.

4) Developing unique survey logics oriented to both specialists and generalists from the IoT domain area for us to have a relevant risk factor weight based on the domain chosen where they implemented the IoT project. Even more, we have a detailed version of one of the surveys which is targeted to potential customers, meaning beneficiaries that can profit from our calculus method. They can realize this risk processing action with a final purpose of adding value to their business. The survey questions, benefits, logic are detailed, along with the target KPIs within the scientific report from [28]. During the thesis, the surveys, the audience and the answer processing methods are presented within chapter 5.

5) SLDC risk mitigation methods by choosing the right delivery method based on the actual project requirements. Describing these and also the specific risk

factors can be found in the published scientific article from [23]. Going through the thesis, detailed information can be found in our third chapter.

6) SDLC and 'Hardware' risk mitigation methods by choosing the right application for both processing and displaying of data. These can be found within the published scientific article that can be see also in the following section under [22]. Through the thesis, the methods and also the advantages of this tool can be seen in chapter 4.

7) Building the main functionalities so we can have an intuitive interface that should cover the main purpose and requirements of our calculus method, from getting survey answers to graphical representation of risk weights. These functionalities were documented withing the research report from [29], and the actual technologies and technical solution are detailed in the published scientific article from [22]. Both the interface and acquired data processing method from the IoT specialists can be found in the figth chapter.

6.3 List of original publications

The structuring of the calculus method in the presented context, both processing and grading risk factors, and also the obtained results within this thesis were published to specialized conferences and dedicated magazines which are relevant in the engineering domain. Apart of the scientific research reports presented in each semester of preparing to this Ph. D, the publishing list contains five scientific articles where I contributed as main author.

Before presenting the list, I want to thank one more time to the specialists that contributed with their time and expertise to grade and analyze these articles. So, we have the following list of original papers, classified based on their purpose, and chronologically ordered.

Published articles

[20] *Vlad-Valentin Firețeanu, Andreea Tudor-Şerban, Ioan Ştefan Sacala, Mihnea Alexandru Moisescu,* Avalanche Prediction Based on Snow Level Monitoring using Wireless Sensor Networks, Applied Mechanics and Materials, (ICMERA), vol 656, pp 369-377, October 2014

[21] *Vlad-Valentin Firețeanu,* Risk Assessment parameters for Internet of Things projects, 15th International Conference on Engineering of Modern Electric Systems (EMES) IEEE, pp 41-44, June 2019

[22] *Vlad-Valentin Firețeanu,* Integrating Tableau with Internet of Things Acquiring Projects, 12th International Conference on Electronics, computers and Artificial Inteliggence (ECAI) IEEE, June 2020

[23] *Vlad-Valentin Firețeanu,* Agile Methodology Advantages when delivering Internet of Things projects, 12th International Conference on Electronics, computers and Artificial Intelligence (ECAI) IEEE, June 2020

[24] Vlad-Valentin Firețeanu, Mihai Ciuc Ph. D. *Designing Risk Assessment Applications for Internet of Things projects*, ‘Polyethnic University of Bucharest’ Bulletin, vol. Electrical Engineering and Computer Science, June 2021

[25] *Vlad-Valentin Firețeanu,* Quantifying Work Safety Risk Factors for Internet of Things Projects, International Conference on Electrical, Computer and Energy Technologies, ICECET2021, December 2021

Scientific Research Reports:

[26] Vlad-Valentin Firețeanu, *Scientific Report: Needs and Constraints in IoT project context*, June 2016

[27] Vlad-Valentin Firețeanu, *Scientific Report: Risk Calculation Methods for IoT projects,* December 2016

[28] Vlad-Valentin Firețeanu, *Scientific Report: Risk Factors for Internet of Things Projects*, June 2017

[29] Vlad-Valentin Firețeanu, *Scientific Report: Analyzing, grading and processing of risk factors for Internet of Things projects,* December 2017

[30] Vlad-Valentin Firețeanu, *Scientific Report: Main functionalities of the risk assessment application for Internet of Things projects,* June 2018

6.4 Perspectives for further development

Efficiency of this framework is determined by the needed research efforts for both updating and maintaining it. Based on the actual status of IoT projects, their performance and also on the constant updates that occur in such fast pace environment, the risk weights must be updated accordingly. Even if most of the already existing frameworks are built around the idea of software security, during this thesis was demonstrated that we also need to cover and improve another major risk areas.

One of the most relevant perspective for further development is represented by the constant market research so we can add new major risk areas or update the already existing ones. In the same manner, we can also add new IoT domains to our method parameters, being helped by the scalability of the application. Even more, in parallel with these market research activities, it’s mandatory to approach even more IoT specialists and generalists. We can say that, as long as our method is widely used and the survey is circulated withing the IoT community to reach more people, we can provide much more accurate feedback to our beneficiaries, closer to the actual point in time when the survey is completed. Another advantage of approaching specialists is represented by the interesting statistics that we can generate when using large volumes of data. Given this, when we need to parse and interpret more and more data, we can choose different algorithmic flows in the response tree of our study. We can observe several trends, and based on them audit and best-practices can be provided before starting a technical project. As a suggestive example for this is that a notable part from smart house projects were realized in an individual project context, so the owner is not part of a dedicated development team that follows any software delivery methodology. Based on this, after carefully querying the responses, these projects were more prone to risks related to overall cost estimation and resources in general. Also, these projects had a very low level of coverage when talking about the software vulnerabilities (the owners weren't aware of any attacks ranging from DB injection to broken authentication). The purpose of our method is generating very detailed metrics on which we can generate a customized set of best practices based on the project.

Therefore, another valid perspective for our calculus method is represented by the updating of the user interface, oriented to the benefits part. Depending on the intelligent flows within the decisional tree, we can add numerous functionalities and new actions. With an interactive approach where additional diagrams are structured, we want to filter the weights only for the domains that we are interested in by using just one simple mouse click or hover on its pictogram. So, based on actionable field, just the paired wight table will be generated. This will include all of the major risk areas and also the required percentages. We want a smart fragmentation of data – the current state of application displays the whole data. Also, from a much easier to follow decisional tree, we thought about implementing a color gradient functionality in the future, more like a traffic system. By doing so, after selecting a color range from green to red, both us and the beneficiaries will have a better overview of risk that should be addressed from a certain category. This improvement will notably contribute also to the risk awareness level. Starting from the same example, an amateur developer which wants to 'take a dive' into the IoT domain will know from the start what is the nature for some of the risk that can occur during developing the project and even after the installation was deployed in a certain environment and it's considered functional. Therefore, we increase the possibility of the developer realizing from an early stage the implied risks and he will concentrate on crafting a more detailed analysis before approaching the technical challenge. He will think of aspects that weren't considered before the risk analysis, such as acquiring additional resources, paying for components that are not considered and marked as vulnerable etc. Switching to this domain will be healthier, being aware of many more aspects that are present in the market and require documentation so he can achieve success.

At a higher level, regarding the delivery within a larger company, a project manager will have a relevant additional resource before starting to manage the development team or before accepting a project from a certain interest area. To give a quick example, when the PM is confronted with the risks present in one specific domain and their weights, he can choose to invest much more resources in non-functional testing for military projects, proactively contributing early to the project success. Also, as we specified during the thesis, when bidding for a new project, using our risk assessment method can be presented as an advantage in client discussions. By using a risk assessment application, all of the delivery team benefits will indirectly affect in a positive way the customer.

In conclusion, as long as this domain faces a constant evolution, we should expect more and more delivery and functionality standards. Our vision is that our framework to be or encourage the first steps that are performed in this standardization journey. As time passes and by implicating the relevant individuals, we will be able to understand how the already existing software best practices are applied also to IoT projects, what new challenges come with this new domain and what can we do as people, from enthusiastic technicians to highly skilled engineers to contribute to a healthier, balanced and safe development.

Bibliography

[1] Mohammad Ammad-Udidin, Imran Baig, El-Hadi M.Aggoune, Muhammad Ayaz, *Wireless Sensor's Civil Applications, Prototypes, and Future Integration Possibilities: A Review*, IEEE Sensors Journal, vol.18, 2017, pp 4-30

[2] H.P. Enterprise, *Internet of Things research study*, Hewlett Packard Enterprise Release, 2015

[3] Y. Qing, L. Jun, *Take unauthorized control of Zigbee devices*, online published on 2015, available online at https://media.defcon.org/defcon23/defcon23presentations/ accessed on 9 September 2018

[4] S. Ranger, *What is IoT? Everything you need to know about the Internet of Things right now*, Zdnet, 2020

[5] Bruce Potter, *Microsoft SDL Threat Modelling Tool*, Network Security, vol. 2009, number 1, January 2009, pp 15-18

[6] David Levitsky, *Assessing Security Risk in IoT Devices*, 2018, available online at https://digitalcommons.calpoly.edu/theses/1954, accessed on 15 November 2020

[7] Colin Tankard, *The security issues of the Internet of Things*, Computer Fraud and Security, vol 2015, pp 11-14

[8] Hanny F. Atlam, Ezz El-Din Hemdan, Ahmed Alenezi, *Security Development Lifecycle, Internet of Things Forensics: A review*, Internet of Things, vol 11, 2020, pp 1-41

[9] Arne Bröring; Stefan Schmid; Corina-Kim Schindhelm; Abdelmajid Khelil; Sebastian Käbisch; Denis Kramer, *Enabling IoT Ecosystems through Platform Interoperability*, IEEE Software, Volume: 34, Issue: 1, Jan.-Feb. 2017, pp 54 – 61

[10] Montbel Thibaud, Huihui Chi, Wei Zhou, Selwyn Piramuthu, *Internet of Things (IoT) in high- risk Environment, Health and Safety (EHS) industries*, vol 108, 2018, pp 79-95

[11] G.G. Gable, *Integrating case study and survey research methods: an example in information systems*, European Journal of Information Systems, Volume 3, December 2017, pp 112-126

[12] Jim Chase, *The Evolution of the Internet of Things*, White Paper, Texas instruments USA 2013

[13] Kent Beck,Mike Beedle,Arie van Bennekum,Alistair Cockburn,Ward Cunningham,Martin Fowler,James Grenning,Jim Highsmith,Andrew Hunt,Ron Jeffries,Jon Kern,Brian Marick,Robert C. Martin,Steve Mellor,Ken Schwaber,Jeff Sutherland,Dave Thomas, *Manifesto for Agile Software Development*, February 2021

[14] Mordor Intelligence Report, *Internet of things Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021-2026)*, available online at https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry accessed on 21 June 2021

[15] Mike McCormick, *Waterfall vs. Agile Methodology*, MPCS.Inc Publishing House, 2012

[16] Data Flair Trainings, *Types of Tableau Data Sources with Connection Establishment Process*, Technical Training, Data Flair available online at https://data-flair.training/blogs/tableau-data-sources/ accessed on 16 August 2020

[17] Sugimiyanto Suma Rashid Mehmood Aiiad Albeshri, *Automatic Event Detection in Smart Cities Using Big Data Analytics*, International Conference on Smart Cities, Infrastructure, Technologies and Applications SCITA 2017: Smart Societies, Infrastructure, Technologies and Applications ,2017, pp 111-122

[18] Tableau Community, *Create Dashboard Layouts for Different Device Types*, official information from Tableau available at https://help.tableau.com/current/pro/desktop/en-us/dashboards_dsd_create.htm, accessed on 12 February 2020

[19] Dorothy Graham, *Foundation of Software Testing*, Cengage Publishing House, USA, 2006

[20] Vlad-Valentin Firețeanu, Andreea Tudor-Șerban, Ioan Ștefan Sacala, Mihnea Alexandru Moisescu, *Avalanche Prediction Based on Snow Level Monitoring using Wireless Sensor Networks*, Applied Mechanics and Materials, (ICMERA), vol 656, pp 369-377, October 2014

[21] Vlad-Valentin Firețeanu, *Risk Assessment parameters for Internet of Things projects*, 15th International Conference on Engineering of Modern Electric Systems (EMES) IEEE, pp 41-44, June 2019

[22] Vlad-Valentin Firețeanu, *Integrating Tableau with Internet of Things Acquiring Projects*, 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) IEEE, June 2020

[23] Vlad-Valentin Firețeanu, *Agile Methodology Advantages when delivering Internet of Things projects*, 12th International Conference on Electronics, computers and Artificial Intelligence (ECAI) IEEE, June 2020

[24] Vlad-Valentin Firețeanu, Mihai Ciuc Ph. D. *Designing Risk Assessment Applications for Internet of Things projects*, 'Polyethnic University of Bucharest' Bulletin, vol. Electrical Engineering and Computer Science, June 2021

[25] Vlad-Valentin Firețeanu, Quantifying Work Safety Risk Factors for Internet of Things Projects, International Conference on Electrical, Computer and Energy Technologies, ICECET2021, December 2021

[26] Vlad-Valentin Firețeanu, *Scientific Report: Needs and Constraints in IoT project context,* June 2016

[27] Vlad-Valentin Firețeanu, *Scientific Report: Risk Calculation Methods for IoT projects*, December 2016

[28] Vlad-Valentin Firețeanu, *Scientific Report: Risk Factors for Internet of Things Projects*, June 2017

[29] Vlad-Valentin Firețeanu, *Scientific Report: Analyzing, grading and processing of risk factors for Internet of Things projects*, December 2017

[30] Vlad-Valentin Firețeanu, *Scientific Report: Main functionalities of the risk assessment application for Internet of Things projects*, June 2018