Master's thesis

Master of Engineering, Health Care Technology

2023

Mika Peltokorpi

Resilient Risk Management

– Case Study on Medical Device Risk Management

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Master’s Thesis | Abstract

Turku University of Applied Sciences

Master of Engineering, Health Care Technology

2023 | 73 pages

Mika Peltokorpi

Resilient Risk Management

- Case Study on Medical Device Risk Management

The aim of this thesis was to study Resilience Engineering methodologies, specifically four cornerstones of resilience, as a process improvement tool in area of risk management. Commissioning organization had detected that there could be a need for improvement in the detection and handling speed of realized risks. The process started with semi-structural survey inside Engineering department. While analysing the results of the survey, the risk management tool was found out to be the one that needed improvements most. The current state analysis and the failure mode effective analysis of the existing risk management tool created multiple improvement proposals to the tool. Furthermore, Resilience Delta and Kaplan-Meier were studied as candidates for visualizing risk data. Kaplan-Meier was found to be better fit for this purpose. The proposals to the risk management tool can be used for developing the risk management tool that improves resilience in risk management by adding metrics and enabling visualizing the subsets of risk data in meaningful ways. Concurrently to the tool analysis, a simple risk reporting template was created, that encourages reporting of the not realized risks and promotes organizational resilience in that manner.

Keywords:

Resilience Engineering, Risk Management, Survival Analysis, medical device, MDR

Opinnäytetyö (YAMK) | Tiivistelmä

Turun ammattikorkeakoulu

Insinööri (ylempi AMK), terveysteknologia

2013 | 73 sivua

Mika Peltokorpi

Riskienhallinta resilienssin näkökulmasta

- Tapaustutkimus lääkinnällisen laitteen riskienhallinnasta

Tämän opinnäytetyön tavoitteena oli tutkia resilienssitekiikaa, erityisesti neljää resilienssin kulmakiveä, prosessinparannustyökaluna riskienhallinnan alueella. Opinnäytetyön tilaaja oli havainnut, että havaittavassa ja toteutuneen riskin käsittelynopeudessa voisi olla parantamisen varaa. Tutkimus alkoi suunnitteluosaston sisäisesti järjestetyllä puoli-struktuurisella haastattelututkimuksella. Haastattelun tulosten analysoinnin jälkeen riskienhallintatyökalun todettiin olevan eniten parantamisen varaa. Nykytila-analyysi, sekä vika- ja vaikutusanalyysi olemassa olevasta riskienhallintatyökalusta johtivat useisiin parannusehdotuksia resilienssin näkökulmasta. Lisäksi kahta analyysityökalua - Resilience Delta ja Kaplan-Meier - tutkittiin ehdokkaina riskien käsittelyaikojen visualisoimiseksi. Kaplan-Meierin soveltuvuuden tutkimisen jälkeen kävi selväksi, että Resilience Delta ei antanut oleellista lisäarvoa riskitietojen visualisoinnissa. Työn riskienhallintatyökalua koskevia ehdotuksia voidaan käyttää kehitettäessä riskienhallintatyökalua, jonka avulla voidaan parantaa riskien hallinnan resilienssiä lisäämällä mittareita ja mahdollistamalla riskidatan osajoukkojen visualisoinnin mielekkäällä tavalla. Työkaluanalyysin lisäksi luotiin yksinkertainen riskiraportointipohja, joka kannustaa realisoitumattomien riskien raportointiin ja edistää siten omalta osaltaan organisaation resilienssiä.

Asiasanat:

resilienssitekniikka, riskienhallinta, elinaika-analyysi, lääkinnällinen laite, MDR

Content

Appendices

Figures

Tables

Equations

List of abbreviations (or) symbols

Abbreviation	Explanation of abbreviation (Source)
AIMDD	Active Implantable Medical Devices Directive
API	Application Programming Interface
AWS	Amazon Web Services
CISQ	Consortium for Information & Software Quality
CO	Commissioning Organization
CoRA	Continuous Resilience Assurance
Cox HR	Cox (Parametric) Hazard Ratio
CPSQ	Cost of Poor Software Quality
CSA	Current State Analysis
DevOps	Development - Operations
EEA	The European Economic Area
EEC	European Economic Community
EU	European Union
FMEA	Failure Mode & Effects Analysis
IBM	International Business Machines
ICT	Information and communications technology
IRM	Integrated Risk Management
ISO	International Standardization Organization
IT	Informaatiotekniikka, Information Technology

LLC	Limited Liability Company
MCEER	Multidisciplinary Center for Earthquake Engineering Research
MD	Medical Device
MDD	Medical Device Directive (Directive (EU) 93/42/EEC)
MDR	Medical Device Regulation (Regulation (EU) 207/745)
NIST	National Institute of Standards and Technology
PO	Product Owner
PM	Product Manager
RCM	Reliability Centered Maintenance
RE	Resilience Engineering
RPN	Risk Priority Number
RSA	Rivest-Shami-Adleman
SaaS	Software as a Service
SME	Small and medium-sized enterprise
STUK	Säteilyturvakeskus
SUNY	The State University of New York
SW	Software
TD	Technical Dept
TQM	Total Quality Management
QA	Quality Assurance

1 Towards resilient risk management

There are currently hundreds, if not thousands of medical devices, some of which are software products or services, that have regulatory impact on them, including the risk management processes and systems used by companies developing them. This thesis is forming an intrinsic case study (Cherry, 2022) which explores the possibility of using Resilience Engineering methods to improve the responsiveness of Risk Management for Medical Devices. Risk management is the process of identifying, assessing, and controlling individual risk events and overall risk by minimizing threats and maximizing opportunities and outcomes. Also, regulatory development in the highly regulated industries, like the medical industry, has always impacted on risk management.

As this is the first touch point to Commissioning Organization and to the author to resilience or Resilience Engineering, this thesis focuses on measuring and visualizing resilience more than policies or organizational improvements. Target process selected was Risk Management in Engineering department's development and operations, or DevOps. In the end this thesis evolved to evaluating risk management practices and tools through lens of Resilience Engineering, which revealed improvement opportunities even for a company, that has been operating successfully in highly regulated environment and that is one of first companies in Europe to achieve MDR Certification according to MDR Regulation (*Regulation (EU) 2017/745*, 2017) to their main product and second in Finland to achieve it to a software, that is also a medical device. MDR Regulation imposes regulatory requirements for medical device manufacturers to manage risks so that the residual risk is judged acceptable; see MDR Regulation Annex I, Chapter I, 4.

Resilience Engineering has been used in many scientific disciplines and each of the disciplines has its own way of interpreting what resilience is. However, one common ideal span through the disciplines and decades Resilience Engineering has been used: resilience of a system is its ability to adapt and recover from

disturbances. In Macrae's definition of sociotechnical dimension of resilience this thesis focuses on situational resilience but touches on also structural resilience. (Wiig and Fahlbruch, 2019, p. 16-17.) Collecting low hanging fruits on improving responsiveness of Commissioning Organization's Risk Management is the main goal of this thesis. Improving the responsiveness of an organization, or system, is after all the main product or all resilience improving actions.

In Risk Management perspective, when Resilience Engineering is compared to the other system analysis and improvement methods and frameworks, Resilience Engineering has the pre-emptive component in its core, of which sole purpose is to improve preparedness and to help improving the responsiveness of risk assessment and recovery from events where risks have been realized.

In scope of this document the term Medical Device means a software product, that is an independent software product for healthcare as specified in EU's MDR Regulation. During MDR Certification process Intended Use of this Medical Device has been described by Commissioning Organization as Medical Device is Active Device under Rule 11 (Software) is Class IIa (MDCG 2021-24 - Guidance on classification of medical devices, 2021, p. 23). In the current changing regulatory landscape (EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation, no date), it is beneficial to any organization, but especially for a medical device manufacturer, to anticipate future regulation related requirements and one way to achieve it is by increasing organization's resilience.

1.1 Motivation

As the scientific analysis discipline for this research Reliability Centered Maintenance (RCM) and Resilience Engineering (RE) were considered. In the medical field RCM has traditionally been used in the pharmaceutical

manufacturing industry and in medical device maintenance process optimization, whereas RE has been used mainly in clinical evaluations for similar goals. These disciplines have traditionally supported different kinds of FMEA and Time-to-Event analysis methods. There are also studies that combine RCM and RE (Cai et al., 2018).

The author of this research has used Reliability Centered Maintenance in his previous thesis (Peltokorpi, 2009), which was reason, why Resilience Engineering was selected as the scientific discipline over Reliability Engineering for this thesis. After literary research on Resilience Engineering Hollnagel's Four Cornerstones of Resilient Organization (Christopher Nemeth et al., 2019, p. 120) was selected to be the theoretical framework of this thesis. The research started with literary research, after which semi-structural interviews were conducted in Commissioning Organization's Engineering department. After the interviews CSA/FMEA analysis of the Risk Management tool used in Commissioning Organization was conducted; with focus on how the tool supports or does not support resilience when reflecting it against Four Cornerstones of Resilient Organization concept.

1.2 History of resilience engineering

Word resilience was first mentioned in the documents of British admiralty, when it was used for describing the tensile strength of oak blanks used in ship hulls. In 1973, Holling used the word 'resilience' to describe the recoverability of an ecosystem (Holling, 1973). At the end of the 1990s Holling created term engineering resilience, which they used to measure a system's capability to return to the equilibrium state (Schulze, 1996, p. 31). Since ca. 2010 resilience engineering has been used also in healthcare industry to verify organizations' safety and quality (Costella, Saurin & de Macedo Guimarães, 2009; Pretagosti et al., 2010; Fairbanks et al., 2014).

The continuous resilience concept has been used on medical (Weeks et al., 2001; DeRijk & de Kloet, 2008; Yang et al., 2014), socio-economical (Kumar and Mehany, 2022; Wei et al., 2022; Ballesteros et al., 2023) and environmental studies widely (Moberg & Folke, 1999; Rasul & Thapa, 2003; Mazzocchi et al., 2012). Even in software development there has been some academical research, namely in Continuous Resilience Assurance of Complex Software-Intensive Systems (CoRA) research program (Troubitsyna et al., 2019) 2016-2020 in Åbo Akademi funded by the Academy of Finland, but there is little (Laibinis et al., 2014) or no public information on results available on it. Amazon has implemented continuous resilience philosophy based on the four cornerstones of resilience engineering to their AWS DevOps pipeline, as can be seen from AWS Summit London 2022 agenda Well-Architected section (Boya, 2022; Grosch, 2022), but scientific research for it is not public, either. Similarly, RSA Security LLC's Archer IRM (Archer Business Resiliency, no date; Archer Operation Resilience White Paper, no date) is a very versatile risk management tool built to support resilience though it is more commonly used for legal and business risk management, than managing risks in DevOps scope. Recently, Microsoft has also started to tout the benefits of its Azure architecture in respect of resilience (Vettor & Smith, 2023, pp. 111-122). You can say that all modern cloud architectures are inherently promoting resilient practices, but the customers of the cloud service providers must adopt those themselves.

1.3 Challenges of Resilience Engineering

Multiple scientific disciplines, that have contributed to Resilience Engineering over the past have contributed to Resilience Engineering theoretical foundation have also been attributed to that very foundation's — if not fragmentation — dissension (Wiig & Fahlbruch, 2019, p. 2, pp. 121-124). Furthermore, traditional engineering disciplines have taken first steps with Resilience Engineering only in last decades. In ICT sector the idea of resilience has emerged to mainstream (outside safety engineering and cybersecurity domains) only in last five years, if

not later. Fitting models that focus on national level disaster management or improving people management in ER are not necessarily directly usable for SW development and operations (DevOps) pipeline optimization. There is little or no publicly available literature focusing on theoretical backgrounds of implemented resilience improving solutions (e.g., Azure/AWS/Archer IRM) especially about DevOps or Risk Management areas. Just as cookie recipes are not patented, the presentations of these manufacturers are telling about the benefits of said solutions and how to implement those in your products and services, but those are not revealing the details of functionalities or theories the resilience improving components are based on.

1.4 Four Cornerstones of Resilient Organization

In Exploring Resilience (Wiig & Fahlbruch, 2019) different theoretical frameworks in Resilience Engineering are described. One of those is Hollnagel's four cornerstones of resilient organization (Dekker et al., 2008, p. 54):

- knowing what to do,
- knowing what to look for,
- knowing what to expect and
- knowing what has happened.

A more refined version of this framework will be used as theoretical framework in this thesis, which is — as stated earlier (Nemeth et al., 2019, pp. 120-121). Figure 1 below is a representation of that. In future this thesis uses terms "learning", "responding", "monitoring" and "anticipating", when referring to the four cornerstones.

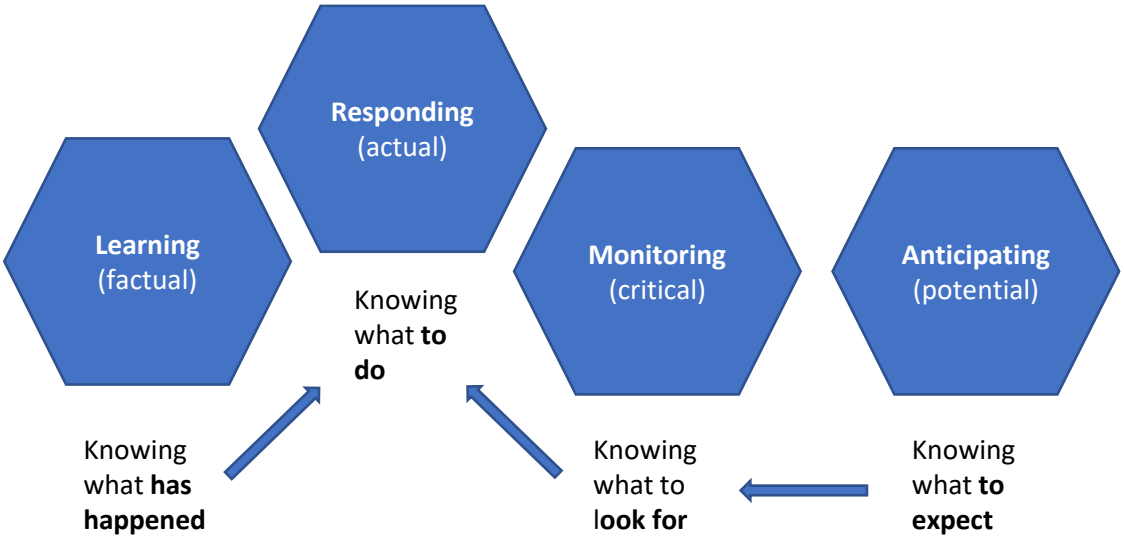

Figure 1: Four cornerstones of resilience (Nemeth et al., 2019, p. 121).

It is these four cornerstones, that are used for evaluating risk management tools, processes, and practices in use in Commissioning Organization, when this thesis was done.

1.5 Resilience Delta

A concept, which is nowadays called Resilience Delta (Nemeth et al., 2019, pp. 19-24) or Resilience Triangle was developed in Multidisciplinary Center for Earthquake Engineering Research (MCEER) at SUNY Buffalo (Bruneau et al., 2006, p. 21). It has wide array of adaptations especially in civil engineering area (Yu & Wang, 2014, pp. 3-4; Birkland, 2016, p. 2; Wang et al., 2012, pp. 113-114). A similar resilience approach has been recently used also in SW development and DevOps. Most notably Amazon's AWS team has adopted continuous resilience as one of their main quality management methods (Grosch, 2022; Boya, 2022; Hornsby, 2021).

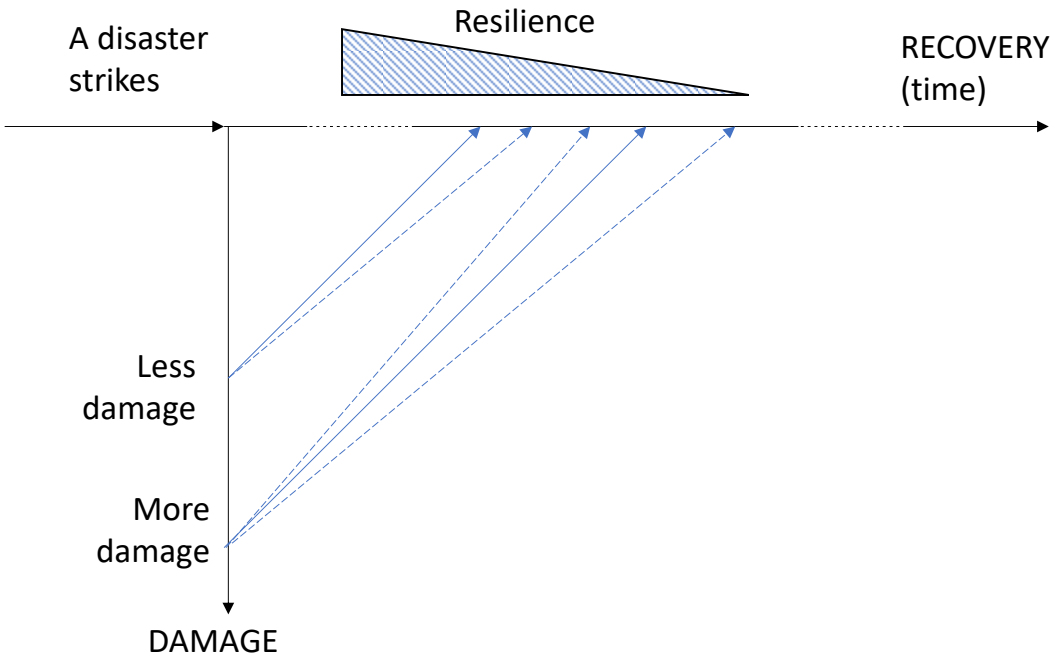

Figure 2: Resilience Delta (Birkland, 2016, p. 2).

1.6 Risk Management

Risk related FMEA worksheets usually consist of up to 16 columns of which 11 are related to FMEA Process itself (Haapanen & Helminen, 2002, pp. 18). According to Haapanen and Helminen FMEA Process columns include:

> Item and Function; Potential Failure Mode; Potential Effect(s) of Failure; Severity; Potential Cause(s) of Failure; Occurrence; Current Controls; Detection; Risk Priority Number; Recommended Action; and Responsibility and Target Completion Date. The Action Results columns include Action Taken, Severity, Occurrence, Detection, and Risk Priority Number (RPN).

Commissioning Organization follows internationally recognized risk management practices that contains these data columns and RPN estimate after risk mitigation. In 2019 during GDPR review Commissioning Organization evaluated, that company's risk process *follows* ISO 13485 (ISO, 2016) and is *based on* ISO 14971 (SFS, 2012). The main conclusion of that evaluation was

that risk control processes in Commissioning Organization cover or exceed the requirements of ISO 14971, but:

- 6.6 Risks arising from risk control process; not enough data to make conclusive assessment yet.
- 8. Risk management report; risk analysis tool converges from analysis to report during deployment planning, but deployment process had not been followed always.

This thesis includes CSA of the Risk Management process and the Risk Management tool (Chapter 4.3), which partially address development and the status of Risk Management in Commissioning Organization. However, it is recommended that Commissioning Organization reassess ISO 14971 compliance in similar manner than in 2019 to fully understand development in this area.

1.7 Requirement management and Risk Management

Most common SW development program risks are technology, requirement management and expertise (Bannerman, 2008, p. 4). As Commissioning Organization is well-established company and the main product is ongoing generational transfer to new architecture and because human resources related risks are not in the scope of this thesis, main risk area in the scope of this thesis is requirements management. The main risk from product management failure is that the detection is late in the development pipeline. If most of the bugs are found in the early phase, during the requirement specification/architecture design phase, the excreted cost of the realized risks can be minimized. Later the bug is found, the more time-consuming it is to fix, too. So sooner in the product development the bug is found, the better the SW project will keep its budget and schedule. (Krassner, 2022, p. 28.)

There are also graphs representing this causality, like one used by IBM (Dawson et al., 2010, p. 4) and an adaption of NIST's graph (Tassey, 2002, p. 97) by Deepsource.io (Sanket, 2019), see Figure 3:

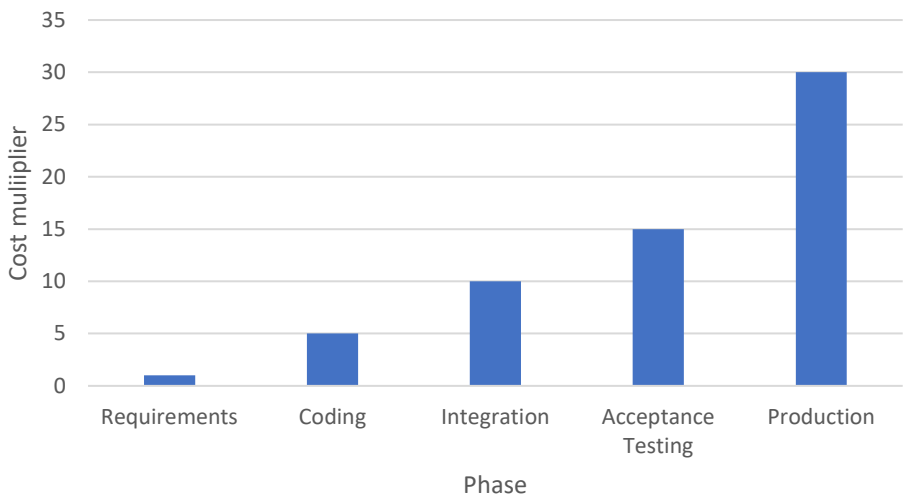

Figure 3: Relative cost to fix bugs (Sanket, 2019).

1.7.1 Requirement Flow in respect of Resilience Engineering

Generic requirement flow was described in study conducted for Ericsson (Heikkilä et. al. 2017, p. 18). A bit more extended presentation of requirement flow is described in Figure 4.

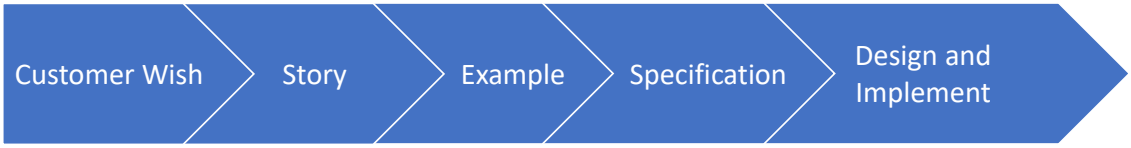

Figure 4: Requirement Flow (Continuous Delivery Ltd, 2023).

1.8 Birds eye view of situation in the ground

This research was conducted with Commissioning Organization when Commissioning Organization was acquiring certification in accordance with EU’s MDR Regulation. Commissioning organization has implemented Risk Management System and is in process of acquiring MDR Certification to the main product, that is Medical Device as described in Chapter 1, therefore Commissioning Organization wanted to find, if there is improvement needs to the current Risk Management System arising from EU’s Medical Device Regulation requirements and if the responsiveness of its Risk Management process will improve. Use of Resilience Engineering methods is on the rise in the medical industry and therefore processes and techniques used in Resilience Engineering are to be used as a process improvement method in this research.

As the target software is Medical Device under EU's MD Regulation Class IIa device, during the CSA analysis of the Risk Management System and risk process special attention on MDR Regulation's requirements in respect of data and metadata collected during Risk Management should be taken into consideration.

1.8.1 Requirement management in Commissioning Organization

Commissioning Organization has organized product development organization similar manner to the standard Scrum model (Schwaber & Beedle, 2001) and it has some similarities to some similarities to the organization of Development Organization in Ericsson though Commissioning Organization does not have Chief PO — and in the scope of this thesis it has only one product with several customer variants. (Heikkilä et. al. 2017, p. 14.) However, there could be benefits for Commissioning Organization having Chief PO, who would handle the requirements of the customer variant portfolio from bird’s-eye view —

having responsibility to approve new features for variants and review that new features are not breaking architecture.

The Commissioning Organization has also indicated that requirement management needs some improvement, as the most realized risks are that the product does not work as designed or requirements were not describing what customer need was. This was also one initial data point for this thesis.

Requirements flow in single customer variant perspective in Commissioning Organization is described in Figure 5.

Figure 5: Requirement flow in Commissioning Organization (simplified)

Every requirement flow has in common, that customer needs are formulated step by step to functional and non-functional requirements and in each step, there is opportunity to react possible issues of requirements or background data (such as user story or customer wish). As shown in Chapter 1.6, cost and schedule risk are multiplied in each step if these problems are not identified in that step. It could be feasible for Commissioning Organization to focus on testability requirements in the earlier phase of the requirement flow.

2 Research questions

Commissioning Organization has identified that most of the repeating realized risks in the main product of the company, that is also certified as a medical device, are related to requirement management and the company wants to learn why that is happening and how to minimize the repetition of such risks. After some deliberation and research, it was decided that main research question of the thesis is:

(RQ1) Can Resilience Engineering be used to improve Risk Management in Medical Device SW development?

In this thesis, this problem is studied in two phases. The first phase of the research is a semi-structural survey conducted to personnel in the Engineering department, who are involved in implementing the requirements for the device. The research questions related to the first phase are grouped into three themes: the tools currently used for the risk management, the risk management process, and the elasticity of the organization. Eventually, more questions were derived from main research question:

(RQ 1.1) What is the status of the current risk process?

1.1. a) What are the strengths of the current risk process?
1.1. b) What are the greatest deficiencies of the current risk process?

(RQ 1.2) What is the status of current risk management tools?

1.2. a) What are the benefits of the current risk management tools?
1.2. b) What should be changed on current risk management tools?

(RQ 1.3) Organizational elasticity of Commissioning Organization?

1.3. a) What would be the best way to improve organizational elasticity in the company?

1.3. b) What is the greatest obstacle that could block improvement of organizational elasticity in the company?

The first two research questions (RQ 1.1 and RQ 1.1) are purely probing questions. The idea for the elasticity of organization question (RQ 1.3) came from Resilience Engineering (Wiig & Fahlbruch, 2019, pp. 45-47). The results of the first phase are also guiding the direction of the second phase of the thesis. The second phase of the research in this thesis realized as CSA and FMEA analysis of the current risk management system used in the Commissioning Organization.

The three supporting research questions were asked in the first phase of this study, a semi structured interview. Results from this study yielded some recommendations on each theme — tools currently used for risk management, the risk management process and elasticity of the organization. The answers to the first phase of the study will also highlight which theme to focus on in the second phase research.

Finally, the main research question will be answered by conducting CSA and FMEA analysis of current risk management tools, processes and/or practices reflected on the theoretical framework based on Hollnagel’s four cornerstones of resilience: responding, monitoring, learning, and anticipating (Nemeth et al., 2019, p. 121). Qualitative analysis combining FMEA and survival analysis for example of realized risks will be conducted to evaluate if survival analysis can be used to differentiate and prioritize different cohorts of realized risks in the Commissioning Organization

3 Research methods

This thesis was made using the following research methods: literature analysis, semi-structural interview, and CSA and FMEA. These methods are described in greater detail in the following chapters.

3.1 Literary research

This thesis started with literary research. At first, it was imperative to understand what resilience or Resilience Engineering means and what is its history. After initial challenges for finding enough relevant literature, two research article collections were found with good referencing: Exploring Resilience (Wiig & Fahlbruch, 2019) and Resilience Engineering Perspectives, Volume 2 (Nemeth et al., 2019). That inspired me to use Science Direct, Research Gate and other scientific paper databases similarly: references have references, and a good search query can be derived from the titles of the resources.

This most intensive part of literary research took many weeks and the total amount of research papers studied amounted to several hundreds of studies. The research papers studied were categorized in Zotero, an open-source reference management software, and in folder structure that was archived and versioned in GitHub; the folder structure can be found in Appendix 2.

3.2 Semi structured interview

Semi structured interview is a qualitative study method, where the research questions have been grouped by themes to direct interviewees attention to the limited set of topics. Naturally you should be prepared and gain enough knowledge about the topic of the interview to get good input in your research. (McIntosh & Morse, 2015.) It is also good practice to use a facilitating approach to the setup during the interview. In the first phase of the actual interview, inform

data management and disclosure practices. Then it is good to reintroduce the interviewee to the topic with a short introduction about the topic and structure of the interview (themes). It is also good to give a time estimate for the interview, if possible. Then go through the research questions one by one. However, if the interviewee hesitates, then you should give clarifying information on the research question discussed. It is also imperative to have follow-up questions always, when you think that you did not give a full answer, or you did not understand the answer fully. This approach encourages dialogue and gives a much more detailed view on interviewees' perspective about the research topic, than when you rush through the research questions. This dialogue also shows respect for the interviewees' time and opinions.

3.3 CSA and FMEA

Current state analysis (CSA) can be used to find the functional design gaps of the current solution considering resilience. The failure mode and effective analysis can be used to find out solutions and design requirements for additional or modified features, that will fill or fix these gaps.

Multiple articles about FMEA can be found easily, one such document was published by STUK in 2002 (Haapanen & Helminen, 2002). The author of this thesis has also used similar methods in his previous thesis (Peltokorpi, 2009). but without resilience at the focal point of the research. One very common technique is called Five Whys invented by Sakichi Toyoda in 1930's, but which got traction only in the 1970s, when Total quality management (TQM) was popularized in manufacturing industry. The first question will be a high lever abstraction, sometimes called user story, then more and more detailed questions give structure in form of features that implement the said user story. (5 Whys Rebranded Video, no date.) The first question could be for example: how to visualize realized risks data that shows how resilient our risk management is now? The second question could be: which visualization

method is the best in respect of visualizing resilience? The third question could be: what must be measured so that we can visualize it? And so on, until enough fine details for the requirement (or failure mode) have been reached.

4 Results

4.1 Conducting the interview

It was agreed with the Commissioning Organization that a semi structured interview will be done for a small set of employees in the Engineering department. This survey was conducted in two phases. The first three interviews were conducted in October-November 2022 and two additional interviews were conducted in January 2023, because it was perceived that answers to some of the research question did not give enough evidence to prove or disprove the original hypothesis.

Three research questions (themes) were selected to get feedback on status of processes and tools used for risk management and current resiliency (elasticity) in the organization (Byrge et al., 2019; Wiig & Fahlbruch, 2019, p. 43). The clarifying follow-up questions were asked when needed. Interviews were typically 15-20 minutes long.

After each interview, the interviews were transcribed and analysed. Transcriptions typically took 5-7 times longer than the interview. Preliminary analysis was done after three interviews, and it was noticed that more interviews were needed to get reliable results on all research questions. Two additional interviews were conducted and after analysing the results of all interviews it was concluded that some research questions that were evaluated to be inconclusive after three interviews got more evidence in a certain direction. The answers in additional interviews, however, did not justify further interviews to be conducted considering the effort and already collected evidence.

All the answers were collected into a matrix, into which answers of each interviewee were collected after subjective analysis by the author. The matrix contains condensed commentary on each of the three themes and six

supporting research questions (see Chapter 2): positive and negative implications for the tools, process, and organizational elasticity (see Appendix 1).

4.2 Results of the survey

The most notable result of the study was that the current risk management tool (RQ 1.2) is not fit for its purpose. Interviewees were volunteering this opinion already at the beginning of the interview, during process related topics and when talking about the positive sides of the tool. This issue will be the focus for CSA/FMEA analysis part of this thesis.

Other findings related to risk management tool were (RQ 1.2):

- The risk management tool covers the MDR requirements and because of this it removes the need for a significant amount of paperwork, that would need to be done during the MDR auditing phase. (1)
- The risk management tool is unergonomic, cumbersome to use, analytics part of the tool is very rudimentary (“has happened”). (4)
- Findings on risk process (RQ 1.1):
- Induction and periodic Awareness training on risk management should be arranged to the whole organization (“expect”). (3)
- Repeating risks are handled well (“do”), but new risk handling (“expect”) is not supported well. (3)

Findings on organizational elasticity (RQ 1.3):

- All interviewees perceived that there are no organization culture related issues for risk management, which would be reducing the elasticity of the organization (“expect”, “look for”), (5)
- though commitment to this from the upper management was wished for. (1)

- Inter-department communication on common risks should be increased. (“do”). (2)
- More resources for risk management in general (especially naming responsible employees with time allocation to risk management) would be needed in the development teams (“do”). (3)

4.3 CSA of Risk Management process

In general, the Risk Management process of Commissioning Organization is well described, and it fulfils regulatory requirements such as MDR. Commissioning Organization has ISO 27001:2022 (ISO, 2022) and ISO 13485:2016 (ISO, 2016) certifications and acquired MDR certification during this thesis. However, awareness and induction training to the personnel would improve awareness and response time for realized or plausible risks that Commissioning Organization will face. Currently, plausible or potential risks are not analysed in the Commissioning Organization to the level that it could be described as a highly resilient organization. Rising awareness of personnel on risk management process overall and especially when, how and why plausible and potential risks should also be managed through official channels would improve the resilience of Commissioning Organization significantly.

4.3.1 CSA of Risk Management tool

In this phase, the Risk Management tool currently in use, which was perceived to be the most problematic part of risk management in Commissioning Organization, was evaluated through the four cornerstones of resilience.

In Commissioning Organization risk management is done in Document Management System and it has separate documents or views for different purposes. As described in Chapter 4.1, interviewees highlighted that the tool is

not fit for purpose. After careful analysis, several issues were found that may contribute to this:

- There are different views - main view, product variant views and testing functionality views - and data in these views is not synchronized automatically.
- The main view has fragmented data. During preprocessing realized risks data for FMEA 10 rows were had so severely fragmented data (data in wrong columns) that it was more feasible to remove those. This is most likely due to the format change and these entries were in the old format. There were also 18 rows that collocated data on multiple customers and/or product variant.
- The naming convention for product variants as described in product naming guide was not always followed.

Due to the above findings, it is highly recommended that Commissioning Organization makes improvements to the current Risk Management tool or acquires some other tool. If the current tool from Atlassian (Atlassian, 2023b) will be used in the future, a partial automation of the risk management process in the same way as test report templates are currently managed should be considered. This would be the most cost-effective way to continue but that would require a rigid process around it. The other approach could be studying document management systems from other vendors like M-Files (M-Files, 2023). There is also full-blown Quality Management Systems from vendors like Greenlight Guru — which has English language checker focusing on Medical Devices (Greenlight Guru, 2023). This kind of tool evaluation is not in the scope of this thesis, even encouraged here.

Data entered to the risk management tool has all the fields described in traditional Risk Management literature (Bannerman, 2008; Kumar & Yadav, 2015; Sousa et al., 2015; Hou, Xu & Lian, 2022), therefore the basis for (realized) Risk Management is in strong foundation. However, the tool itself has

some deficiencies, that do not prevent data fragmentation, and which also hinder some data analytics; especially in the realm of time-to-event type analysis, like Weibull (Luko, 1999), Cox-regression (Kingsley et al., 2008) or Kaplan-Meier (Goel et al., 2010). Currently collected risk data is deliberated in Chapter 1.6.

4.3.2 Proposed visualization support for the tool

To achieve Figure 6 in the next page and other resilience improving parameters to a Risk Management tool Five Whys method was used (“Why?” is asked after every bullet:

- We cannot visualize the resilience of the risk data.
- We do not collect data points.
- We are not measuring the time of all the events that risks have.
- This is still not enough detailed.
- We do not categorize risk data according to when risk was introduced.
- We could improve categorizing, still.
- We should set value for introduced date as SW version creation according to current SW in the production.

As you find above, “Why?” was asked more than five times. The purpose of this method is to try to ask at least five times why; the exact number of asking is not the goal. You can also see that answers are getting more detailed with each step.

Improvements in resilience area are proposed be achieved by measuring Kaplan-Meier statistics on different Risk Item categories lifecycle phases as shown in Figure 6: with KM_n notation (Δt_n notation describes single Risk Item processing time between two events):

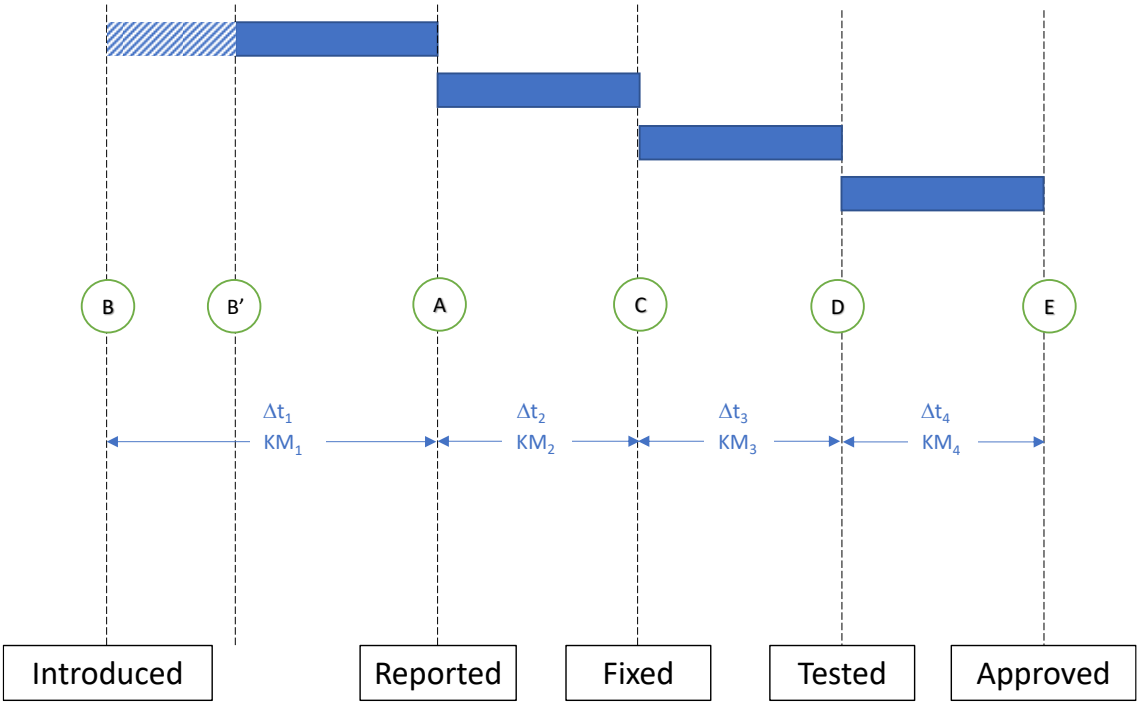

Figure 6: Risk Item Lifecycle

Calculating Kaplan-Meier statistics on mentioned phases requires recording the following event times (dates) to each of the risk items. The notation of the event in the figure above in the brackets:

- Reporting of the risk (A)
- Introduction of the risk to the system (B)
    - Initial value: the creation date of the SW when risk was reported (B')
- Implementation of the solution of the risk item (C)
- Verification of the solution (D)
- Acceptance of the solution (E)
    - When the risk is realized risk, acceptance of the solution should come from the customer.

In addition to single phase Kaplan-Meier statistics, collection of above event times enables Kaplan-Meier analysis for consecutive phases:

$$\sum_{i=n}^{m} KM_i = KM_n^m \Big\| \begin{matrix} m = \{n+1\,..\,4\} \\ n = \{1\,..\,3\} \end{matrix}$$

$$\sum_{n}^{n} KM_i = KM_n$$

Equation 1: Kaplan-Meier sum function

The above sum function shows that it is not feasible to make Kaplan-Meier analysis from two separate sections of the risk item population phases but analyzing Kaplan-Meier statistics on consecutive phases (for example time from reporting to solution/fix) may reveal issues (namely delays) on some new areas in the risk management process.

In this thesis, only KM_1 is evaluated against real world data when `B = B'`. These results can be seen in Chapter 4.4.2.

It is easy to implement Kaplan-Meier analysis between different populations in time dimension — for example, between two quarters or two halves of a year (see Figure 11), when proper metadata is collected. If risk items are categorized on in which phase of the product development the risk was introduced (“fault introduced variant” later) or in which phase the risk was detected (“defense-in-depth”) and dates for these events are also recorded, it is possible to do analysis between e.g., risk items found during development and risk items found in production and focus on the risk items that have long lead time in solving those.

In addition to Kaplan-Meier, some temporal statistical analysis methods were considered. Regarding analysis in the timescale, because the number of entries (realized risks) and the need for splitting data to cohorts (sub-populations) it

would be reasonable Kaplan-Meier analysis to be selected instead of Cox and Weibull, which typically require at much more data points than Kaplan-Meier before converging to fit with real world data. Kaplan-Meier is also widely used in the medical field, so it would be easy to communicate with it to customers, if that kind of need were realized. This thesis also explored usability of (modified) Resilience Delta for time domain analyses.

4.3.3 Analysis of Resilience Delta

From Figure 2 it can be deducted, that better the organizational resilience is, the faster the recovery time from an adverse event is. Therefore, the steeper the angle of the arrow in the figure, the more resilient the organization was in the handling of the event.

As mentioned in Chapter 1.6 of most cost impacting Risk Management area is Requirement Management and in it the most important way to minimize cost and schedule related risks is to detect requirement related issues and errors as early as possible. Requirement flow is one way to evaluate this risk. Therefore, in this thesis Modified Resilience Delta is proposed, where the severity of the requirement management related risk is quantified to following levels:

- Customer Wish
- User Story
- Functional Requirement
- Development
- Integration
- Testing
- Production

are derived from widely used Reason’s Swiss cheese-model (Perneger, 2005; Drogoul, 2006; Carthey, 2013; Larouzée & Guarnieri, 2015; da Silva & Krishnamurthy, 2016) sometimes called as defense-in-depth in Resilience

Engineering (Nemeth et al., 2019, p. 117). These steps are also used as an ordered list for Defense-in-depth values during the FMEA when modified Resilience Delta analysis is processed. As Commissioning Organization has not been focusing its effort on *anticipating* or *learning* from realized risks, all the realized risks had been found in Production phase (on *Defense-in-depth*).

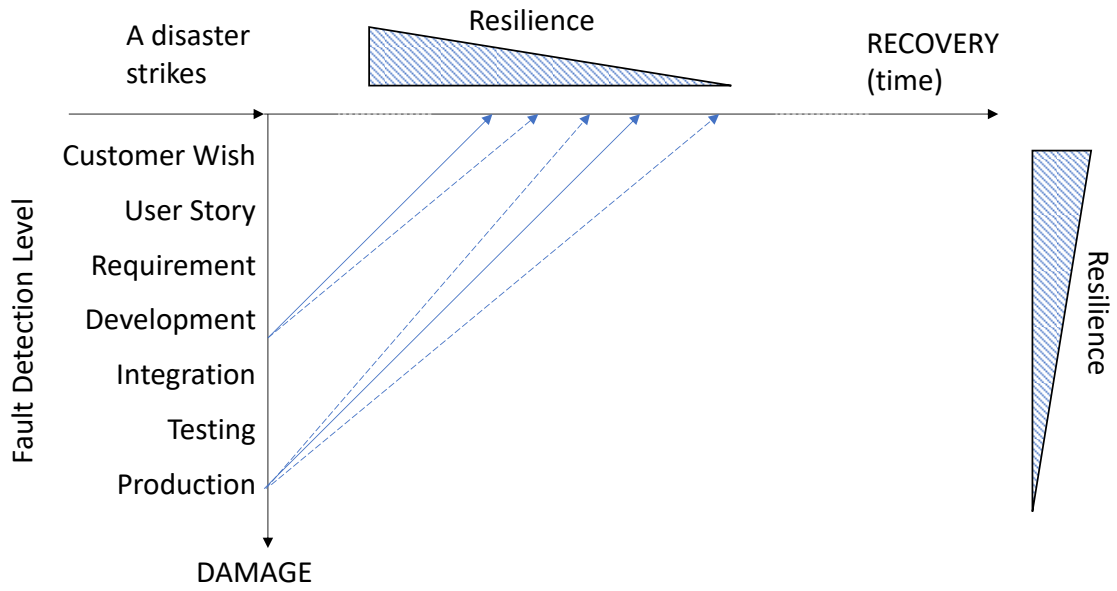

Figure 7: Modified Resilience Delta

When comparing Figure 7: Modified Resilience Delta above to Figure 2, it shows that resilience is not only the matter of fast recovery time from a fault event, but also about finding solutions to detect possible mistakes during earlier steps in the requirement flow.

It would be highly beneficial for Commissioning Organization to study in which phase of the product development process the fault was introduced (*Fault detection level*). *Fault level* uses the same categorization labels as *Defense-in-depth*. *Fault detection level* study is out of the scope of this thesis.

However, after analyzing possibilities of Kaplan-Maier statistics, it came apparent that even if resilience delta is a usable tool for understanding the

impact of the risks and visualizing resilience in graphical manner, it gives little of additional value in this respect, Kaplan-Meier or even a box plot are to be used in temporal analysis. For example, in Kaplan-Meier you can see box plot statistics in the horizontal axis, and that is valid also to the Resilience-Delta graphs. However, it might be feasible to be used in spark line visualization, where 45º is describing average performance, a steeper angle is describing faster (more resiliently achieved) solution for the risk item and a gentler slope would describe a risk item, where solution took longer than average. Irrespective of this deficiency, Resilience Delta concept helped to reaffirm that for Risk Management in SW development it is most damaging to find faults late in the product development (requirement flow). Moreover, the need analyzing the risk items also by their *Fault detection level* and *Defense-in-depth* categories became apparent only after studying Resilience Delta concept.

4.3.4 Proposed changes to the tool

In this chapter there are recommendations about the needed changes to the Risk Management System to improve performance considering resilience. Already collected data and metadata related to resilience analysis in risk management the tool is:

- Reporting date
- The reported SW version of the product variant
- Risk category ID
- Customer name
- Product variant name

In addition to these fields, data points related to requirement flow steps should be collected:

- Fault introduced version
- Fault introduced date

- Fault fixed version
- Fault fixed date
- Customer accepted date

For more detailed analysis, also already following earlier discussed metadata should be collected:

- Defense-in-depth
- Fault detection level
- Plugin version

Data fragmentation was a significant issue during the analysis of risk data. Therefore, all categorizing field values should be managed in separate part of the tool and only one value should be possible to insert as value in one risk item; one way to achieve this is to use drop-down element where to select category value(s). That means, that each risk item should be an independent representation of one combination of these fields' values. This is valid for all data or metadata; including current Customer name and Product variant name metadata fields, that were causing the most extra effort needed during the data analysis and the biggest source of data fragmentation.

It should also be considered if in future risk items would be handled in a tool that uses a relational database as data storage. In that case SW versions could be collected in one table/relational subsystem, which could also be an external source through an API or a database interface; at least partly. The following data should be able to be collected and shown in the tool using this data:

- Product variant name
- Customer name
- SW version
- QA approval date
- Production deployment date
- Product generation

4.3.5 Requirement specifications of some of the proposed changes

In this chapter, some proposed changes are described in greater detail to help the implementation of such features in the future Risk Management System in Commissioning Organization.

Meta data field - Status

Purpose: Risk items' progression tracking.

New/Existing: New

Type: Select list

Possible values: "Not Started", "Started", "Completed", "Reopened".

State diagram:

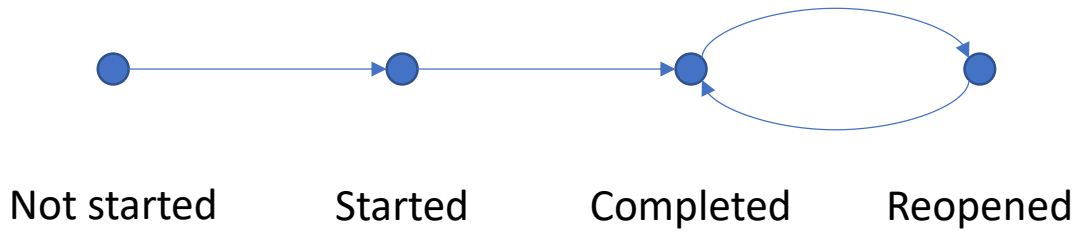

Figure 8: State Diagram, Status field

Temporal filed - Reported date

Purpose: To record the date of detection of risk items. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets. (A) in Figure 6.

New/Existing: Existing

Type: date; dd.mm.yyyy

Example value: "01.02.2022"

Source: Manual input

Meta data filed - Reported version

Purpose: To record SW version of detection of the risk items. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets.

New/Existing: New

Type: Calculated/selected value of exact SW version string

Example value: "1.2.10"

Source: Selected from a variant version table, where the *reported date*, *register type* and *customer name* fields are matched to the latest existing version of the register variant in the date, when the risk item was reported.

Meta data filed - Introduced version

Purpose: To record SW version of introducing of the risk items. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets.

New/Existing: New

Type: Select list of SW version strings in format of "x.y.z", where `{x,y,z}` are integer numbers `>=0`.

Example value: "1.2.10"

Source: Value is selected from a subset of *version* column values from the SW version table, where the current risk item's *register type* and *customer name* are used as a filter.

Default value: Reported version.

Temporal field - Introduced date

Purpose: To record the date of detection of risk item. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets. (B') or (B) in Figure 6.

New/Existing: New

Type: date; dd.mm.yyyy

Example value: "01.02.2022"

Value: Currently, QA approval date of the customer variant version of Introduced version.

Default value: Calculated (selected) value of the reported customer variant version's QA testing passed date — or other reliable product variant creation date; in case of the Commissioning Organization QA testing passed date was the only commensurable date that could be used for this purpose.

Temporal field - Fixed date

Purpose: To record the date of solution implementation of a risk item. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets. (C) in Figure 6.

New/Existing: New

Type: date; dd.mm.yyyy

Example value: "01.02.2022"

Source: Calculated value of the reported customer variant version's Production testing passed date — or other reliable product variant creation date.

Meta data field - Fixed version

Purpose: To record the register variant version, in which a solution for the risk item was created.

New/Existing: New

Type: SW version strings in format of "x.y.z", where `{x,y,z}` are integer numbers `>=0`.

Example value: "1.2.11"

Source: Manual input

Temporal field - Tested date

Purpose: To record date of verification of solution implementation of the risk items. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets. (D) in Figure 6.

New/Existing: New

Type: date; dd.mm.yyyy

Example value: "01.02.2022"

Source: Manual input

Temporal field - Accepted date

Purpose: To record the date of approval of a solution implementation of the risk itema. Used also in combination of other similar fields to calculate and generate Kaplan-Meier statistic of risk sets. (E) in Figure 6.

New/Existing: New

Type: date; dd.mm.yyyy

Example value: "01.02.2022"

Source: Manual input

4.4 FMEA of the realized risks

In this thesis FMEA of the realized risks is focusing on assessing (modified) Resilience Delta and Kaplan-Meier analyses in respect of visualizing differences on different subsets of realized risks and changes of those differences over time. The usability of these methods in the specific case under study is also evaluated.

4.4.1 Data-analysis limitations

In this thesis evaluation, if current RPN values — default or diluted — are valid, is not made. No evaluation of whether RPN dilution actions are effective is done either. Data analysis in this thesis focuses only to determine if Kaplan-Meier analysis can be used as Time-to-Event analysis for detecting differences in Risk Management performance on different cohorts defined by defense-in-depth levels described in Chapter 4.4. No other Time-to-Event analyses are made in the scope of this thesis. Reasoning for selecting Kaplan-Meier for Time-to-Event analysis is discussed in Chapter 4.4.2.

The selection of the risk events for this case study was limited to one year of samples. The tool had some risk data collocated to one row. For example, in the same row several register variants or customers were given as a value — or the value for customer(s) and/or register variant(s) was stated simply as “all”. Then, if the customers or register variant value was “all”, the row was simply discarded. In the case. When multiple register variants or customers were mentioned, separate entry rows were created to each register variant and customer combination. As the current tool had not been yet equipped to collect data in the time domain, the data analysis in the time domain was done only for time difference between:

1. The current SW version of the register variant — customer combination on the moment report was reported (*Fault introduced date*).

2. The moment when the realized risk was reported (*Fault reporting date*).

The same analyses that were used for this analysis can be used to visualize the differences of different subsets of data in the time domain between other events. It should be noted that if in later during FMEA analysis of a realized risk it will be found that the fault was introduced in the previous SW version, not in the latest SW version, the fault introduction date should be updated; this corresponds (B') to (B) transition in Figure 6. This kind of deep dive is out of the scope of this thesis as it was deemed too laborious in context of the thesis. The other time domain analyses were decided to be out of the scope of this thesis. It is, however, highly recommended, that Commissioning Organization completes the time domain analyses in the foreseeable future.

4.4.2 Kaplan-Meier analyses of the realized risks, detection time

Detection time is the time between reporting the realized risk and time when the fault was introduced to the system. For initial assumption current SW version can be used for the fault introduction point and time of building the SW version as fault introduction time. In this chapter detailed analysis of subsets of realized risk data will be conducted. This aggregation was made to all realized risk items and the data was divided according to three product platform generations that were identified to have realized risks in 2002. Distributions for three generations is shown in Figure 9.

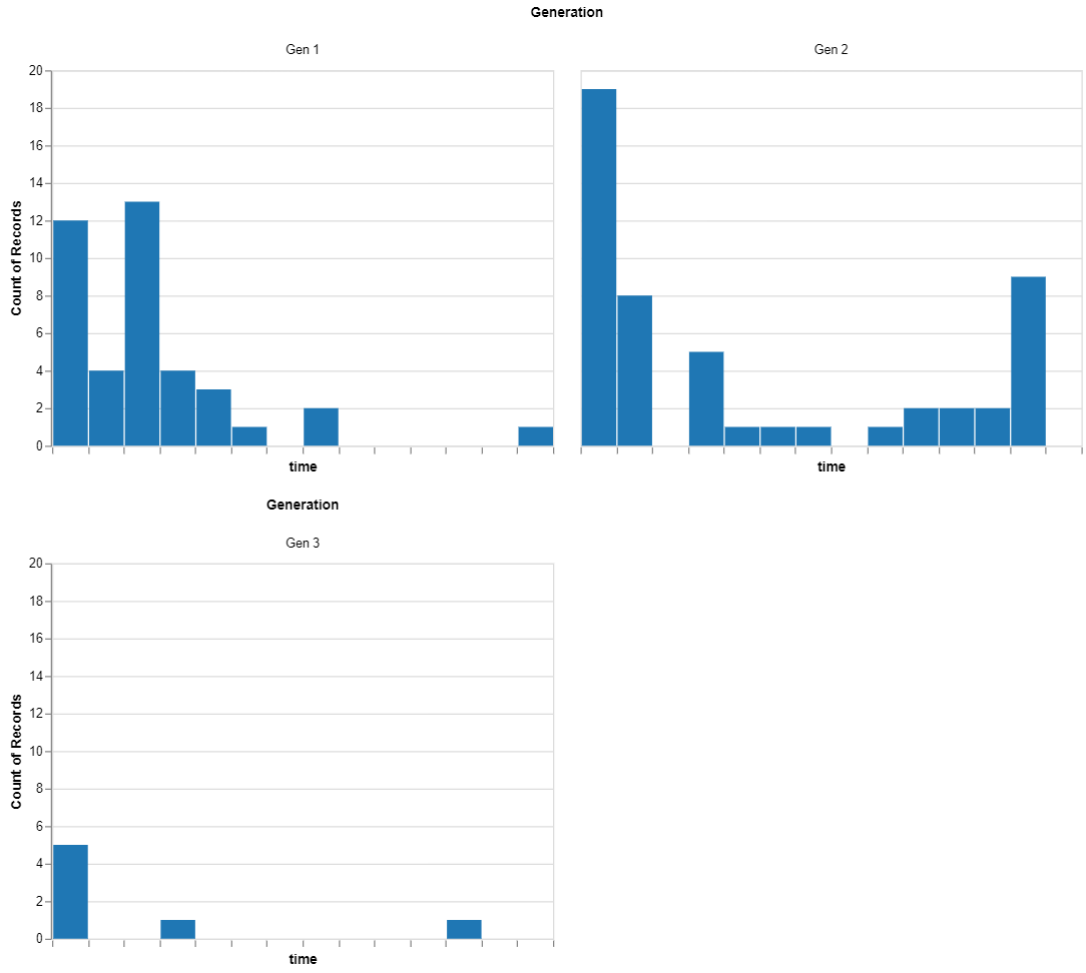

Figure 9: Distribution of detection times between generations.

The same data in Kaplan-Meier graph is shown in Figure 10. It was very quickly identified that Kaplan-Meier is better for visualizing this kind of data. In Figure 10 halfway to first time axis tick (less than 0,5 time units) was analyzed to be normal, hard to improve area of risk management as same product is offered to several customers and the delay in this area is generally related to delay between deployments to separate customers or customers decision to delay an upgrade. The long delay risk items, seen in the right half of the Figure 10, are related also mostly to customer related approval processes; these risk items were usually the ones, that were fixed in lead product, but other customers had not made upgrade decisions before end of fiscal year. Therefore, the rest of the risk items, where the delay is longer than the half time units and less than three

time units have best potential for process improvement. However, the detailed analysis for improvement potential was not in scope of this thesis.

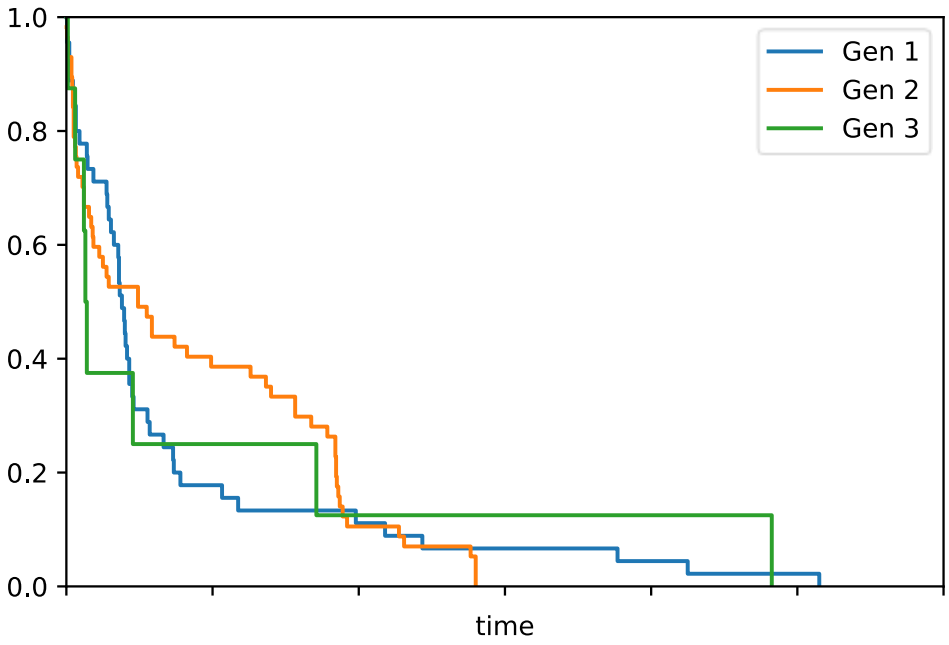

Figure 10: Kaplan-Meier results between the generations

Kaplan-Meier analysis can also be done between different time periods. Performance difference between H1 and H2 of 2022 can be seen in Figure 11. As we know already, that critical are where performance can be improved is in area t = 1.5 – 3.0 time units, you can say that handling of realized risks has been degraded in H2 of 2022. So, it would be advisable to analyze the realized risks in H2 and have handling time on t = 0.5 - 3, what are root causes for this degradation. That analysis is not in the scope of this thesis.

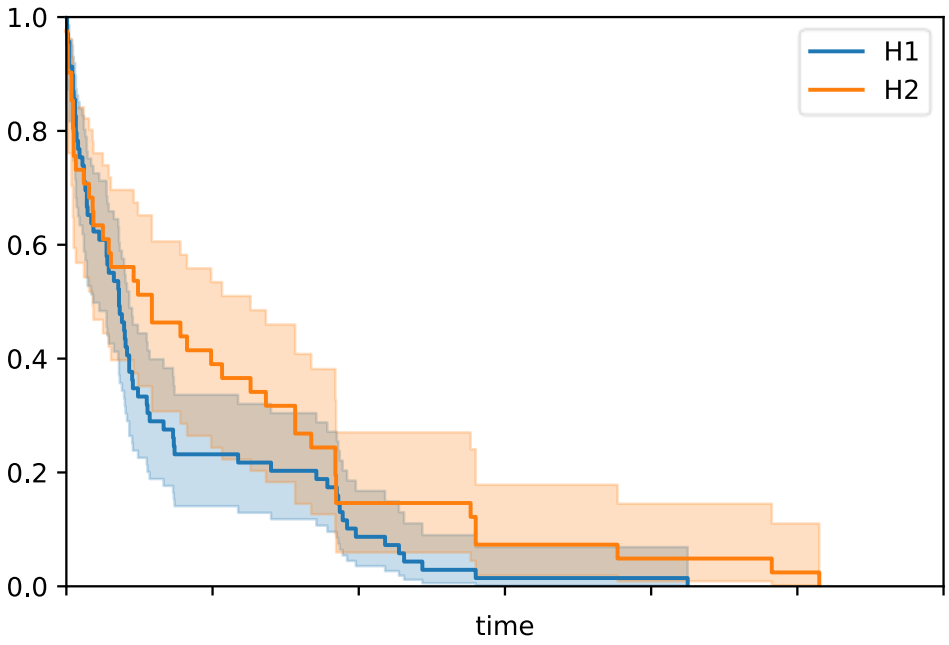

Figure 11: Kaplan-Meier, detection time difference 2022 H1 vs. 2022 H2

This analysis can also be implemented on a customer basis. In Figure 12 difference between Customer 16 and the rest of realized risk population is shown. If confidence intervals were not presented in the figure, assessment for Customer 16 risks would be, that those have been processed in slightly better manner than the rest of the customers' risks (refer to t = 0.5 – 3 time units zone). However, this must be ruled out as the difference is not statistically significant.

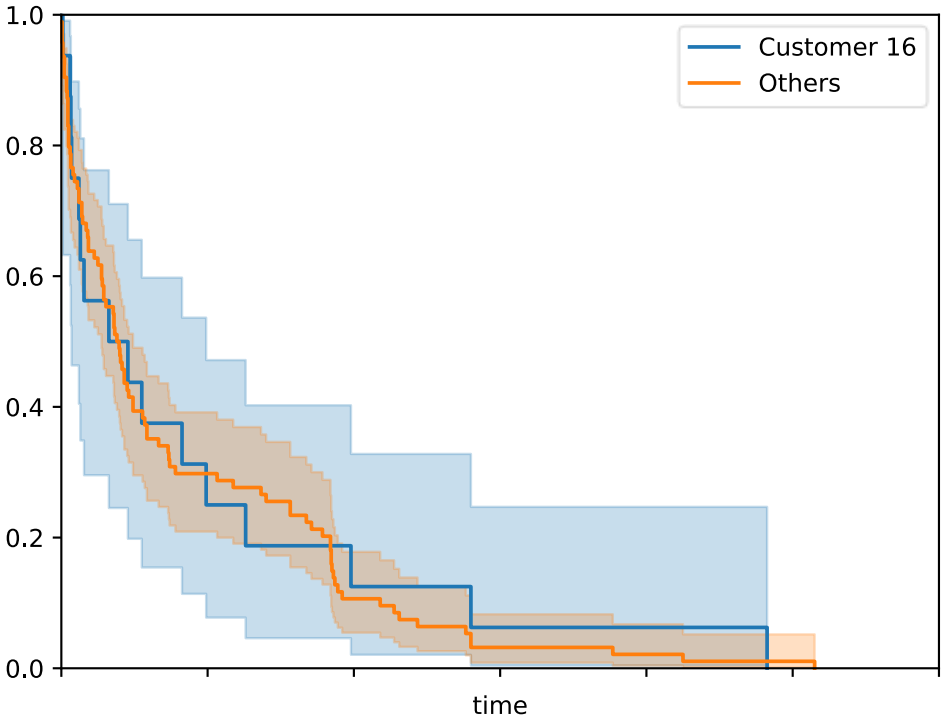

Figure 12: Kaplan-Meier, detection time Customer 16 vs. other customers

4.4.3 Rapid risk assessment template

During this thesis, an idea for a method of a rapid reporting of the possible risks in any possible area even remotely involving the Commissioning Organization's main product was arisen. This is related to ISO 13485 Quality Management process in Commissioning Organization and illustrates how the company could be more initiative taking to react to potential risks that could evolve to delays in product development or quality deviation in the product itself ("anticipate"). The format for reporting such findings is simple. It is recommended that each of these findings be managed via the Commissioning Organization's existing Quality process. For the clarity and uniformity of risk reporting following (or similar) fields should be introduced to the description part of the created quality related issue/task as shown in Table 1.

Field	**Purpose/possible values**
Realized risk	None, undefined or brief description of realized risk
Category	Learning, Responding, Monitoring, Anticipating
Background	Description how the issue was found / reasoning for raising the issue
Analysis	Detailed analysis of the incidence
Recommendation(s)	Recommended actions (if any)

Table 1: Rapid Risk Assesment Template

As not all potential risks are of technical nature, this template is void of technical fields such as SW version number on purpose. The following subchapters show a subset of the actual findings. These findings are already reported on Quality Management tool so those can be managed according to the Quality Management process. These findings show the effectiveness of even one person in the organization just thinking resiliently for extented time. It is recommended that Commissioning Organization should elevate awareness and support the development of resilient organization culture and resilient thinking

within the company. See the examples of found improvement items and areas using this template in the following pages.

Enhancing Technical Account role for Customer Support

Field	Description/value
Realized risk	Undefined
Category	Anticipating
Background	Enhancing Technical Account role for Support in Commissioning organization. Commissioning organization has technical roles in their Customer Support Functionality, but full potential for Tier 1 to Tier 2 analysis capability of it has not been taken fully in operation.
Analysis	Customer Support tickets may have sensitive information, for example identifying information about patients. Therefore, access to the customer support tickets is (and should be) highly restricted for Engineering roles in the Commissioning Organization. Customer tickets sent to Engineering seldom have technical data and metadata or first level of FMEA included in. Example of minimum recommended information to collect already in Customer Support functionality can be found in the Feasibility Study of Reliability Centered Maintenance Process (Peltokorpi, 2009, 12). If such data would be collected already in Customer Support functionality, that would both increase situational awareness of Customer Support functionality and remove the workload from Engineering as this analysis work would be transferred from Engineering to Customer Support.

Recommendation	During the transmission of a customer report to RND there should be technical analysis of possibly existing similar issues. Also, the wording used by the customer should be translated to the way Engineering is talking about the product.

Table 2: Enhancing Technical Account role for Customer Support

API Integration of Customer Service Software and Issue Ticketing Software

Field	**Description/value**
Realized risk	Undefined
Category	Anticipating
Background	Currently, Commissioning Organization's Customer Support functionality has SaaS solution to tracking and handling customer tickets and Engineering functionality has SaaS solution to tracking development related issues. There is an API-integration available for integrating these two SaaS solutions, but Commissioning Organization has not taken it in use.

Analysis	Automating information flow between Customer Support and Engineering functionality could improve speed and the quality of the customer originated issues through the activation of API-integration between Customer Ticket Tracking system and Issue Tracking System. The possibility of searching to combine technical bug reports with single or multiple customer tickets would improve response time to the customer tickets. This would also improve situational awareness of Customer Support functionality.
Recommendation 1	Commissioning Organization should conduct economic feasibility study for the impacts of possible deployment of API-integration between Customer Ticket Tracking System and Issue Tracking SaaS solutions.

Table 3: API Integration of Customer Service Software and Issue Ticketing Software

End-of-Life status for all product generations

Field	**Description/value**
Realized risk	None
Category	Anticipating

Background	Commissioning Organization has different product generations, which can be split to roughly to two categories: old product generations, that fall under the MDD regulation and new (and future) generation(s) that fall under the MDR regulation. There is a good description about the active development phase of the products in different generations, but there is no end of active support definition in the process for the different product generations. For example, first generation products are not updated any more — or in the active support phase. Products in the first generation are therefore in the end-of-life support phase, but there are no information available when this has become effective.
Analysis	Automating information flow between Customer Support and Engineering functionality could improve speed and the quality of the customer originated issues through the activation of API-integration between Customer Ticket Tracking system and Issue Tracking System. Possibility to search and combine technical bug reports with single or multiple customer tickets would improve response time to the customer tickets and improve situational awareness of Customer Support functionality.

Recommendation	It would be beneficial to all staff in Engineering functionality to have easy access to the latest status of the development cycle of each product generation. For example, if there are plans to upgrade certain products to the next or latest generation. This would elevate the level of understanding for prioritizing of different product version updates and upgrades.

Table 4: End-of-Life status for all product generations

Regulation, analysis of the MDR Certification process adequacy

Field	**Description/value**
Realized risk	None
Category	Responding
Background	Commissioning Organization has acquired MDR certification for the latest product generation of its main product.
Analysis	Commissioning Organization (CO) commissioned a thesis on MD Regulation's possible impact (Lehtonen, 2019), what impacts upgrading from the MDD directive scope to the MDR regulation scope will have to product development. Now, after acquiring the MDR Certification, it would be feasible to analyze if the previous analysis is valid or if there are some improvements to be made.

Recommendation	When a future generation is taken onto the product roadmap, it should be analyzed at the very beginning of the development project, what impact it will have to the MDR auditing process. For example, if a current MDR Certificate covers the new product generation or if an adjacent MDR Certification Process for new product generation should be planned for it. Commissioning Organization has done this analysis prior to this thesis, already.

Table 5: Regulation, analysis of the MDR Certification process adequacy

Incidence report: Specification change after development started

Field	**Description/value**
Realized risk	New version of product variant had to be done
Category	Responding
Background	In Commissioning Organization there is no SOP how the communication between Product Manager (PM) and Product Owner (PO)/development team happens when development sprint for a certain product variant is started. Functional Specification was changed after development team had already tested related change tasks to the realized risk causing change in Functional Specification.

Analysis	Development team started development and testing, and PM was not aware of that development team developed and tested multiple related tasks to the realized risk causing the bug but was not aware of relevant change to the realized risk causing a functional specification mismatch. There was no task created by PM for Functional Specification change causing realized risk, so development team was not aware of it.
Recommendation 1	Development team (namely PO) informs PM, when customer variant version is started to be tested
Recommendation 2	Product Managers (PM) should create a change when making any changes to Functional Specification. PM informs development team about all changes to the product variant's Functional Specification in detail after the customer variant version development has started — regardless of the fact it should or should not be implemented in the currently ongoing development sprint or in the future development sprint.

Table 6: Incidence report: Specification change after development started

Incidence report: Key vault destruction in lab environment

Field	**Purpose/possible values**
Realized risk	None
Category	Learning

Background	In early December test automation for nightly batch processing data migration verification was done. In January when test engineer was developing (obfuscated) real world data test message test to this data pipeline in lab environment it failed due "`KeyVaultEncryptionKeyNotFound`" error.
Analysis	It was noticed that lab environment was deemed to be a test sandbox environment only, where everything is set to prevent the erasing of the keys without prior notice for development team. The key vault for the lab environment was also soft deleted. The key vault for the lab environment was restored. When it was restored from the garbage collection, the functionality of test harness was restored after the test engineer logged out and logged back in to Azure development environment (`az logout`, `az login`). There was no realized risk due soft deletion of vault key in lab environment and because retest for the system was run one week prior to the production deployment. Net effect was less than 1/2 man-hours overall.
Recommendation 1	Development (lab)/QA/Production key vault management process and documentation subprocess should be defined.

Recommendation 2	All pipeline storages (Dev/QA/Production) should have good documentation, where usage and the owners of different pipelines. This will ensure that relevant bodies can be contacted prior to the erasure of any data related to pipeline recipes or other pipeline configurations, authentication methods etc. are released.
Recommendation 3	The hard deletion of the storage environment content or the key vault should have separate, more stringent subprocess with an additional escalation route compared with the soft delete. This subprocess should allow hard delete only after soft delete for the erased data or other related files have been effective for minimum time. This time could be for example 30 days.
Recommendation 4	Each storage container should have its own key vault. This is to ensure that accidental or intentional erasure (soft or hard delete of) the key vault for one storage environment does not have adverse effect on the other storage environments.

Table 7: Incidence report: Key vault destruction in lab environment

Other findings

Other findings were:

- Practical Quality Process and Risk Management Induction training are not held for new personnel.
- Product Development Process and Product Maintenance Process are not translated into English and there are no Induction trainings for new personnel on these matters.

It is highly recommended to conduct induction training for all the processes mentioned above for new personnel; a periodic awareness training of these topics for all personnel should also be considered. As Commissioning Organization’s official language is now English, all process documents should be translated into English.

5 Conclusions

The main purpose of this thesis was to evaluate, if Resilience Engineering could be used in Risk Management to improve responsiveness to realized risks. In this thesis Four Cornerstones of Resilience Framework was used for this analysis. First three research questions:

- “What is status of the current risk process?”
- “What is status of the current risk management tools?”
- “Organizational elasticity of Commissioning Organization?”

were asked in a semi-structural survey to know where the main effort in this thesis should be focused. Results of the survey are described in Chapter 4.1. Two first research questions are purely probing questions to find status in the Commissioning Organization. This kind of survey would be beneficial to other entities to make, because it will generate good discussion and give new insights to improvement areas in case of tools and processes (“Learning”) The third question comes directly from Resilience Engineering. Chapter 6 shows how Risk Management process could adapt Resilience Engineering in a way that organization will improve its elasticity in this area (“Anticipate”).

The fourth research question was found to hold the most significant importance. Therefore, solving fourth research question: “Could Resilience Engineering be used as a risk management method for software, that is also a medical device?” focused on tool improvement; not forgetting other aspects of Resilience Engineering. The most typical risk in SW development is related to requirements management and this is the case also in Commissioning Organization. Chapter 4.3.4 proposes improvements to risk analysis tool which will help to understand overall risk status better (“Monitoring”) and react those faster (“Respond”).

5.1 Recommendations

In this chapter, the main recommendations for Commissioning organization are described. Any small and medium-sized enterprise (SME), which is developing medical devices, is planning to acquire MDR Certification and want to improve their Risk Management on the medical device planned to be certified or under certification can benefit from these recommendations, too. All these recommendations have resiliency improving factors, too. In addition to the SMEs, also national regional (such as recently formed wellbeing service counties in Finland) or local governments can use these recommendations to craft questions related to resilience in their calls for tenders.

The risk management tool should be further developed from the current state, that is not only conformant to generic risk FMEA process (Haapanen & Helminen, 2002), but it would also create tool assisted resilience — especially in monitoring and anticipating areas — within the company. The suggested modifications are discussed in 4.3.4.

Development team members should have at least indirect access to underlying information, why a feature was created (customer wish, user story) and to Support ticket of realized risks; refer to Chapters 1.6, 1.5 and 4.4.3.

Every realized risk should be assigned a solution task in Risk Management Tool, now it is not the case. The fix task can be normal bug report or an ISO 13485 related process development task. This will improve speed and accuracy of post analysis phase of realized risks especially in are of Time-to-Event analyses; refer to Chapter 4.4.

As a periodical check Commissioning Organization should reassess ISO 14971 compliance in similar manner as in 2019 and possibly acquire ISO 14971 Certification.

Commissioning Organization should elevate awareness and support the development of resilient organization culture and resilient thinking within the company.

An API integration between Customer Ticket Tracking System and Issue Tracking System would improve the quality and the speed of risk processing.

The Product Development Process should be described in greater detail to avoid communication breaks related to Requirement Management.

As Commissioning Organization has switched official language to English, all process documentation should be translated into English. Mandatory induction training and periodic awareness training on all processes should be organized in the company.

Role or Chief Product Owner, whose responsibility is to evaluate that the new features proposed to customer variants are not breaking the architecture of the main product, should be created. This is especially important now, when Commissioning Organization is about to be transforming its main product line from current generation architecture to a newer one; refer to Chapter 1.8.1.

6 Discussion

Combining new techniques (like Resilience Engineering in this thesis) and old techniques (TQM's 5 Whys and FMEA) can give new insights to an organization on its processes and therefore reduce improvement cycle times. Combined with a quantitative research method, like semi-structural interview used in this thesis encourages members of the organization to discuss processes and tools in totally new perspective, which encourages discussion and promotes openness in the organization; these behaviours are traits of a resilient organization.

It is highly recommended that Commissioning Organization completes the FMEA analyses in the time domain on realized risks, that were out of the scope of this thesis. That should give a better insight on which phase of the handling of realized risks Commissioning Organization should focus its efforts. Also, categorization on Fault level for realized risks should be done during that analysis.

As various events led to the fact that thorough time-to-event analysis was not conducted during this thesis, it may be beneficial to the Commissioning Organization to collect the historical data of realized risks, albeit it will be time-consuming effort as required data is distributed to several, partly decommissioned tools. Another approach to this is to implement changes proposed in this thesis to the risk management tool and start recording required parameters for realized (and possibly also for non-realized) risks.

Following up Regulatory changes in the EU and the local level should be continued. For companies that develop software that is critical infrastructure, like medical devices, it would be good practice to make an impact analysis of recent EU-level regulatory changes in cybersecurity domain. In Finland scope, the relevant authorities would be at least ENISA and Valvira. For example, impacts of EU's Cybersecurity Act (Regulation (EU) 2019/881, 2019) and

proposed AI Act (ARTIFICIAL INTELLIGENCE ACT, 2021) are discussed in ENISA’s web pages and events.

Aalen regression, Lexis graph and Cox HR analyses have interesting possibilities of visualizing risk data and/or defense-in-depth related risk data when sample size increases. Therefore, those pose a great opportunity to improve tool assisted resiliency by enhancing the visualization capabilities of the tool. Because of the improvement of the visualization capabilities the issues will be detected faster, which typically also improves the organizational resiliency.

Incorporating AI enforced analysis tools for Risk Management is also a great further study subject. Studying the suitability of Microsoft’s and Amazon’s anomaly detection and DevOps tools for Medical Device Risk Management is a very suitable new thesis topic. Goode examples for a starting point of such research can be found in CISQ 2022 report (Krasner, 2022, pp. 41-47).

References

5 Whys Rebranded Video (no date). Available at: https://content.jwplatform.com/previews/WbIPHn6a-5WSyalpf (Accessed: 14 May 2023).

Archer Business Resiliency (no date) *Archer*. Available at: https://www.archerirm.com/business-resiliency (Accessed: 14 April 2023).

Archer Operation Resilience White Paper (no date). Available at: https://go.archerirm.co/${OGShareURL} (Accessed: 14 April 2023).

Atlassian (2023) *Confluence | Your Remote-Friendly Team Workspace | Atlassian*. Available at: https://www.atlassian.com/software/confluence (Accessed: 18 February 2023).

Atlassian (2023) *Jira | Issue & Project Tracking Software | Atlassian*. Available at: https://www.atlassian.com/software/jira (Accessed: 18 February 2023).

Ballesteros, L.M.S. *et al.* (2023) 'Evaluating the interaction effects of housing vulnerability and socioeconomic vulnerability on self-perceptions of psychological resilience in Puerto Rico', *International Journal of Disaster Risk Reduction*, 84, p. 103476. Available at: https://doi.org/10.1016/j.ijdrr.2022.103476.

Bannerman, P.L. (2008) 'Risk and risk management in software projects: A reassessment', *Journal of Systems and Software*, 81(12), pp. 2118–2133. Available at: https://doi.org/10.1016/j.jss.2008.03.059.

Birkland, T. (2016) 'Conceptualizing Resilience', *Politics and Governance*, 4, p. 117. Available at: https://doi.org/10.17645/pag.v4i4.823.

Boya, V. (2022) 'Towards Continuous Resilience'. Available at: https://d1.awsstatic.com/aws-summit-london-session-slides/Towards%20Continuous%20Resilience.pdf (Accessed: 19 February 2023).

Byrge, C. *et al.* (2019) 'Development of New Business Models: Introducing the Cultural Elasticity Model', *Journal of Business Models*, 7(4), pp. 13–19. Available at: https://doi.org/10.5278/ojs.jbm.v7i4.2942.

Cai, B. *et al.* (2018) 'Availability-based engineering resilience metric and its corresponding evaluation methodology', *Reliability Engineering & System Safety*, 172, pp. 216–224. Available at: https://doi.org/10.1016/j.ress.2017.12.021.

Carthey, J. (2013) ‘Understanding Safety in Healthcare: The System Evolution, Erosion and Enhancement Model’, *Journal of public health research*, 2, p. e25. Available at: https://doi.org/10.4081/jphr.2013.e25.

Cherry, K. (2022) *What Is a Case Study in Psychology?*, *Verywell Mind*. Available at: https://www.verywellmind.com/how-to-write-a-psychology-case-study-2795722 (Accessed: 10 April 2023).

Christopher Nemeth, Erik Hollnagel, and Sidney Dekker (2019) *Resilience Engineering Perspectives, Volume 2: Preparation and Restoration*. CRC Press. Available at: https://www.routledge.com/Resilience-Engineering-Perspectives-Volume-2-Preparation-and-Restoration/Hollnagel-Nemeth/p/book/9780367385408 (Accessed: 5 February 2023).

Continuous Delivery Ltd (2023) *‘The Most Powerful Software Development Process Is The Easiest’*. Available at: https://www.youtube.com/watch?v=nCuDrWxlh4Y (Accessed: 22 February 2023).

Costella, M.F., Saurin, T.A. and de Macedo Guimarães, L.B. (2009) ‘A method for assessing health and safety management systems from the resilience engineering perspective’, *Safety Science*, 47(8), pp. 1056–1067. Available at: https://doi.org/10.1016/j.ssci.2008.11.006.

da Silva, B.A. and Krishnamurthy, M. (2016) ‘The alarming reality of medication error: a patient case and review of Pennsylvania and National data’, *Journal of Community Hospital Internal Medicine Perspectives*, 6(4), p. 31758. Available at: https://doi.org/10.3402/jchimp.v6.31758.

Dawson, M. *et al.* (2010) ‘Integrating Software Assurance into the Software Development Life Cycle (SDLC)’, *Journal of Information Systems Technology and Planning*, 3, pp. 49–53. Available at: https://www.researchgate.net/publication/255965523_Integrating_Software_Assurance_into_the_Software_Development_Life_Cycle_SDLC.

DeRijk, R.H. and de Kloet, E.R. (2008) ‘Corticosteroid receptor polymorphisms: Determinants of vulnerability and resilience’, *European Journal of Pharmacology*, 583(2), pp. 303–311. Available at: https://doi.org/10.1016/j.ejphar.2007.11.072.

Drogoul, F. (2006) *Revisiting the ‘Swiss Cheese’ model of accidents*. Available at: https://www.eurocontrol.int/publication/revisiting-swiss-cheese-model-accidents (Accessed: 23 February 2023).

EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation (no date). Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/ (Accessed: 18 May 2023).

Fairbanks, R.J. *et al.* (2014) 'Resilience and Resilience Engineering in Health Care', *The Joint Commission Journal on Quality and Patient Safety*, 40(8), pp. 376–383. Available at: https://doi.org/10.1016/S1553-7250(14)40049-7.

Goel, M., Khanna, P. and Kishore, J. (2010) 'Understanding survival analysis: Kaplan-Meier estimate', *International journal of Ayurveda research*, 1, pp. 274–8. Available at: https://doi.org/10.4103/0974-7788.76794.

Greenlight Guru (2023) *Greenlight Guru: #1 QMS for Medical Devices | EDC for Medical Devices*. Available at: https://www.greenlight.guru (Accessed: 18 February 2023).

Grosch, G. (2022) 'Resilient and well architected apps with chaos engineering'. Available at: https://d1.awsstatic.com/aws-summit-london-session-slides/Resilient%20and%20well-architected%20apps%20with%20chaos%20engineering.pdf (Accessed: 19 February 2023).

Haapanen, P. and Helminen, A. (2002) 'Failure mode and effects analysis of software-based automation systems', p. 37. Available at: https://www.julkari.fi/handle/10024/124480 (Accessed: 5 February 2023).

Holling, C.S. (1973) 'Resilience and Stability of Ecological Systems', *Annual Review of Ecology and Systematics*, 4, pp. 1–23. Available at: http://www.jstor.org/stable/2096802 (Accessed: 5 February 2023).

Hornsby, A. (2021) 'Towards continuous resilience', *The Cloud Architect*, 2 April. Available at: https://medium.com/the-cloud-architect/towards-continuous-resilience-3c7fbc5d232b (Accessed: 19 February 2023).

Hou, G., Xu, K. and Lian, J. (2022) 'A review on recent risk assessment methodologies of offshore wind turbine foundations', *Ocean Engineering*, 264, p. 112469. Available at: https://doi.org/10.1016/j.oceaneng.2022.112469.

ISO (2016) *ISO 13485:2016*, *ISO*. Available at: https://www.iso.org/standard/59752.html (Accessed: 5 February 2023).

ISO (2022) *ISO/IEC 27001:2022*, *ISO*. Available at: https://www.iso.org/standard/82875.html (Accessed: 5 February 2023)

Kingsley, D. *et al.* (2008) 'Cox Proportional Hazards Regression Analysis as a Modeling Technique for Informing Program Improvement: Predicting Recidivism in a Boys Town Five-Year Follow-up Study', *The Journal of Behavior Analysis of Offender and Victim Treatment and Prevention*, 1, pp. 82–97. Available at: https://doi.org/10.1037/h0100436.

Krassner, H. (2022) *Cost of Poor Software Quality in the U.S.: A 2022 Report*. Available at: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/cpsq-report-nov-22-1.pdf (Accessed: 22 February 2023).

Kumar, C. and Yadav, D.K. (2015) 'A Probabilistic Software Risk Assessment and Estimation Model for Software Projects', *Procedia Computer Science*, 54, pp. 353–361. Available at: https://doi.org/10.1016/j.procs.2015.06.041.

Kumar, S. and Mehany, M.S.H.M. (2022) 'A standardized framework for quantitative assessment of cities' socioeconomic resilience and its improvement measures', *Socio-Economic Planning Sciences*, 79, p. 101141. Available at: https://doi.org/10.1016/j.seps.2021.101141.

Laibinis, L., Vistbakka, I. and Troubitsyna, E. (2014) 'Modelling Resilient Systems-of-Systems in Event-B', in, pp. 157–166. Available at: https://doi.org/10.1007/978-3-319-10557-4_19.

Larouzée, J. and Guarnieri, F. (2015) 'From theory to practice: itinerary of Reasons' Swiss Cheese Model', in. *ESREL 2015*, CRC Press, p. 817. Available at: https://doi.org/10.1201/b19094-110.

Luko, S. (1999) 'A Review of the Weibull Distribution and Selected Engineering Applications'. Available at: https://doi.org/10.4271/1999-01-2859.

Mazzocchi, M.G. *et al.* (2012) 'Stability and resilience in coastal copepod assemblages: The case of the Mediterranean long-term ecological research at Station MC (LTER-MC)', *Progress in Oceanography*, 97–100, pp. 135–151. Available at: https://doi.org/10.1016/j.pocean.2011.11.003.

McIntosh, M.J. and Morse, J.M. (2015) 'Situating and Constructing Diversity in Semi-Structured Interviews', *Global Qualitative Nursing Research*, 2. Available at: https://doi.org/10.1177/2333393615597674. (Accessed: 16 May 2023).

MDCG 2021-24 - Guidance on classification of medical devices (2021). Available at: https://health.ec.europa.eu/latest-updates/mdcg-2021-24-guidance-classification-medical-devices-2021-10-04_en (Accessed: 5 February 2023).

Moberg, F. and Folke, C. (1999) 'Ecological goods and services of coral reef ecosystems', *Ecological Economics*, 29(2), pp. 215–233. Available at: https://doi.org/10.1016/S0921-8009(99)00009-9.

Peltokorpi, M. (2009) *Feasibility study of reliability centered maintenance process : applying RCM II approach to customer feedback in SW development environment*. fi=AMK-opinnäytetyö|sv=YH-examensarbete|en=Bachelor's thesis|. Tampere Polytechnic University. Available at: http://www.theseus.fi/handle/10024/8654 (Accessed: 5 February 2023).

Perneger, T.V. (2005) 'The Swiss cheese model of safety incidents: are there holes in the metaphor?', *BMC Health Services Research*, 5, p. 71. Available at: https://doi.org/10.1186/1472-6963-5-71.

Pretagostini, R. *et al.* (2010) 'Risk Management Systems for Health Care and Safety Development on Transplantation: A Review and a Proposal', *Transplantation Proceedings*, 42(4), pp. 1014–1016. Available at: https://doi.org/10.1016/j.transproceed.2010.03.100.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (2021). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (Accessed: 10 June 2023).

Rasul, G. and Thapa, G.B. (2003) 'Sustainability Analysis of Ecological and Conventional Agricultural Systems in Bangladesh', *World Development*, 31(10), pp. 1721–1741. Available at: https://doi.org/10.1016/S0305-750X(03)00137-2.

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) (2017) *OJ L*. Available at: http://data.europa.eu/eli/reg/2017/745/oj/eng (Accessed: 5 February 2023).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (2019) *OJ L*. Available at: http://data.europa.eu/eli/reg/2019/881/oj/eng (Accessed: 10 June 2023).

Sanket, S. (2019) 'The exponential cost of fixing bugs', *DeepSource*, 29 January. Available at: https://deepsource.io/blog/exponential-cost-of-fixing-bugs (Accessed: 22 February 2023).

Schwaber, K. and Beedle, M. (2001) *Agile Software Development with Scrum*. 1st edn. USA: Prentice Hall PTR. Available at: https://www.amazon.com/Agile-Software-Development-Scrum/dp/0130676349.

SFS (2012) *SFS-EN ISO 14971:2012:en*. Available at: https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID6/1/195431.html.stx (Accessed: 18 February 2023).

Sousa, S., Nunes, E. and Lopes, I. (2015) 'Measuring and Managing Operational Risk in Industrial Processes', *FME Transactions*, 43, pp. 295–302. Available at: https://doi.org/10.5937/fmet1504295S.

Tassey, G. (2002) *The Economic Impacts of Inadequate Infrastructure for Software Testing*, p. 309. Available at: https://www.nist.gov/system/files/documents/director/planning/report02-3.pdf (Accessed: 22 February 2023).

Troubitsyna, Elena, Vistbakka, Inna, and Majd, Amin (2019) *Continuous Resilience Assurance of Complex Software-Intensive Systems*, *Åbo Akademi*. Available at: https://research.abo.fi/en/projects/continuous-resilience-assurance-of-complex-software-intensive-sys (Accessed: 23 January 2023).

Vettor, R. and Smith, S. (2023) *Architecting Cloud Native .NET Applications for Azure*. Available at: https://dotnet.microsoft.com/en-us/download/e-book/cloud-native-azure/pdf (Accessed: 10 May 2023).

Weeks, W.B. *et al.* (2001) 'The Organizational Costs of Preventable Medical Errors', *The Joint Commission Journal on Quality Improvement*, 27(10), pp. 533–539. Available at: https://doi.org/10.1016/S1070-3241(01)27047-3.

Wei, D. *et al.* (2022) 'Socioeconomic impacts of resilience to seaport and highway transportation network disruption', *Transportation Research Part D: Transport and Environment*, 106, p. 103236. Available at: https://doi.org/10.1016/j.trd.2022.103236.

Wiig, S. and Fahlbruch, B. (eds) (2019) *Exploring Resilience: A Scientific Journey from Practice to Theory*. Cham: Springer International Publishing (SpringerBriefs in Applied Sciences and Technology). Available at: https://doi.org/10.1007/978-3-030-03189-3.

Yang, Z. *et al.* (2014) 'Factors influencing resilience in patients with burns during rehabilitation period', *International Journal of Nursing Sciences*, 1(1), pp. 97–101. Available at: https://doi.org/10.1016/j.ijnss.2014.02.018.

Yu, K. and Wang, Y. (2014) 'A Resilience Engineering Framework: Adapting to Extreme Events', in. Available at: https://doi.org/10.1061/9780784413609.096.

Interviews analysis template

	I1	I2	I3	I4	I5
Process+	it exists repeating errors are handled well	Risk based tests are yielded from realized risks and thus followed on.	Covers well needs of (MDR) certification and thus reduces need of documentation during audits. Testing functionality goes trough realized risks weekly.	We are collecting realized risks from Support.	It is detailed and works for product development well.
Process-	not yet realized risks, how to approach?	More thorough training for all employees would be good.	Not fully utilized, as it should. Risks found during development are not documented promptly; only repeating risks are handled properly. Feels like everyone in company are not involved as much as should.	Scope is limited to perspective according to sertificates (MDR). It is not covering personnel risk or business risks and thus does not support our doing. Some steps require too much searching how to do and you may give up on reprioting risk at hand.	I m not convinced, that it is covering all the aspects, it should. In evaluation phase some smaller new risks may be not recorded, If technical basis is lacking at that moment and them may miss (forgotten) also L2L phase.
Tools +	realized risks visible to everybody	I do not know how to use	Replaces multiple tools.	Categories. Fullfills foman requirements arising from sertifications such as MDR.	Maybe this is good enough. At least all risks are collected to same place.
Tools -	cumbersome to use too many manual steps main view is very long and discourages browsing trough	I do not know how to use	Quite hard to use. And that might be the reason, why it is unterutilized. Main table is gigantic.	Hard to use. Discurages to enter risks that are not fitting to the template. Which new risks quite often may be. When you have to find out how to use it, you may lose opportunity to record that new risk, if you have to do something in between and you forget that risk.	Unpractical to use, because it is so large. Issue Tracking System could be more involved? Cybersecurity related risks could be have more role?
What would be way to improve elasticity?	Lessons from realized risks should be required phase, in my mind this has not happened.	Earlier handling of possible risks may help. Bettter handling of the risks. Assignment of responible person/team for a realized risk is sometimes off, improving this could help.	Realized risks in production should be documentd in grater detail. Now especially small deviations are fixed immediatelty, but not documeted in detail.	Risk process should be low sill process. Effectiveness of communication between involving team differs depending on who are involved. Awareness of risk process and toos could be improved in CO.	Naming technical duty officers in weekly basis. So that you would know whom to ask how to handle a potential risk.
What would prevent improving eleasticity?	It is always hard to change current work processes, when this kind of change has to go trough upper management and plan training.	Internal communication between different teams (horizontally and vertically) could be better. How we would act on dirsuptive situation?	Not enough time to improve processes. There should be dedicated person or team to handle this kind of improvement, perhaps?	Different pars of organization have different priorities. If you do not have dedicated time for developing your processes, it will not happen.	Duty officer compensation (money) could be an issue, perhaps?

Zotero Folder structure

- Thesis (28)
  - Bills and Standards (6)
  - Books (6)
  - Requirement management (6)
  - Resilience engineering (3)
    - Building tech (1)
    - Defence-in-depth (5)
    - Environmental (3)
    - Medical (3)
    - Medical safety (3)
    - Resilience delta (8)
    - Socioeconomical (4)
    - Web pages (8)
  - Risk management (4)
  - Statistics (3)

Total: 91

Visualization mock-up Jupyter code

```
#!/usr/bin/env python
# coding: utf-8
#!pip install altair
#!pip install pandas
#!pip install matplotlib
#!pip install lifelines
#!pip install altair_saver
#!pip install vl-convert-python
#!pip install selenium==4.2.0 --force-reinstall
#!python -m pip show selenium

get_ipython().system('python -c "import os, sys;
print(os.path.dirname(sys.executable))"')
get_ipython().run_line_magic('config', "InlineBackend.figure_formats =
['svg']")
import matplotlib.pyplot as plt
get_ipython().run_line_magic('matplotlib', 'inline')

import json
import numpy as np
import altair as alt
import pandas as pd
from lifelines import KaplanMeierFitter

f = open('conf.json')
tconf = json.load(f)

df1_cols = ['Nro', 'Register', 'Customer', 'PVM', 'ID','Reported
version',
       'Inroduced version', 'Introduced date']
df1 = pd.read_excel("RISKIT.xlsx", sheet_name=0)
df1 = df1.loc[:, df1.columns.isin(df1_cols)]
df1['Join'] = df1['Register'] +' '+ df1['Customer'] + df1['Inroduced
version']
df1.head()

df2 = pd.read_excel("RISKIT.xlsx", sheet_name=1)
df2['Version join'] = df2['Version']
df2['Join'] = df2['Register'] +' '+ df2['Customer'] + df2['Version
join']
df2.head()

df3 = pd.merge(df1, df2, on=['Join'] )
df4 = df3
df4.info()

df4['Version'].equals(df4['Reported version'])
df4.loc[~(df4['Version'] == df4['Reported version'])]
df4_cols = ['Nro', 'Register_x', 'Customer_x', 'PVM', 'ID', 'Reported
version',
       'Inroduced version', 'Introduced date', 'QA',
'PROD','Generation',
```

```
       'Customers']
df4 = df4.loc[:, df4.columns.isin(df4_cols)]
df5 = df4.rename(columns={"Register_x": "Register", "Customer_x":
"Customer", "PVM": "Reported date"}, errors="raise")
df5["Days"] = df5["Reported date"] - df5["Introduced date"]
df5['Days'] = df5['Days'].dt.days
df5.head()

df5.describe()

# Data fragmentation related pruning
df6 = df5[['Customers','Generation','Days']]
df5 = df5[df5['Generation'].notnull()]
df5 = df5[df5['Generation'].notnull()]
df5 = df5[df5.Register != 'Register 19']
df5 = df5[df5.Nro != 64]
df5[df5.isnull().any(axis=1)]
chart =alt.Chart(df6).mark_bar().encode(
    alt.X("Days", bin=alt.Bin(extent=[0, tconf["TMAX2"]],
step=tconf["TSTEP2"]), axis=alt.Axis(labels=False, domain=False),
title="time"),
    y='count()',
    color=alt.value("#1f77b4"),
    column='Generation'
)
chart

chart.save('Gen_chart_1.svg', engine="altair_saver")
df6.describe(include='all')

kmf = KaplanMeierFitter()
days = pd.DataFrame(df5[['Days', 'Reported date', 'Customers',
'Generation']])
days[days.isnull().any(axis=1)]
days['Observed']= 1
T = days['Days'].to_list()
E = days['Observed'].to_list()
kmf.fit(T, event_observed=E)
ax = kmf.plot_survival_function(xlabel='time')
ax.axes.xaxis.set_ticklabels([])
ax.set_ylim([0.0,1.0])
ax.set_xlim([0.0, tconf["TMAX1"]])
days.head()

h1_df = days[days['Reported date'] <  '2022-07-01']
h2_df = days[days['Reported date'] >=  '2022-07-01']
kmf_h1 = KaplanMeierFitter()
kmf_h2 = KaplanMeierFitter()
kmf_h1.fit(h1_df['Days'], h1_df['Observed'], label='H1')
kmf_h2.fit(h2_df['Days'], h2_df['Observed'], label='H2')
ax = kmf_h1.plot()
ax.set_ylim([0.0,1.0])
ax.set_xlim([0.0, tconf["TMAX1"]])
ax.axes.xaxis.set_ticklabels([])

ax = kmf_h2.plot(ax=ax, xlabel='time')
ax.get_figure().savefig("H1 vs H2.svg", format="svg")
```

```
chart2 = alt.Chart(days).mark_rect().encode(
    x='Generation:O',
    y =alt.Y('Customers', bin=alt.Bin(step=4)),
    color=alt.Color('Days:Q', legend=None)
).properties(
    width=200,
    height=150)

chart2

chart2.save("Generations Customers heatmap.svg",
engine="altair_saver")

days.describe(include='all', datetime_is_numeric=True)
gen1_df = days[days['Generation'] ==  'Gen 1']
gen2_df = days[days['Generation'] ==  'Gen 2']
gen3_df = days[days['Generation'] ==  'Gen 3']
kmf_gen1 = KaplanMeierFitter()
kmf_gen2 = KaplanMeierFitter()
kmf_gen3 = KaplanMeierFitter()
kmf_gen1.fit(gen1_df['Days'], gen1_df['Observed'], label='Gen 1')
kmf_gen2.fit(gen2_df['Days'], gen2_df['Observed'], label='Gen 2')
kmf_gen3.fit(gen3_df['Days'], gen3_df['Observed'], label='Gen 3')
ax = kmf_gen1.plot(ci_show=False)
ax.set_ylim([0.0,1.0])
ax.set_xlim([0.0, tconf["TMAX1"]])
ax.axes.xaxis.set_ticklabels([])
ax = kmf_gen2.plot(ax=ax,ci_show=False)
ax = kmf_gen3.plot(ax=ax, xlabel='time',ci_show=False)
ax.get_figure().savefig("Generations KM.svg", format="svg")

regs_df = pd.read_excel("RISKIT.xlsx", sheet_name=2)
regs_df.describe(include='all')
g1regs_df = regs_df[regs_df['Generation'] >=  'Gen 1']
g2regs_df = regs_df[regs_df['Generation'] >=  'Gen 2']
g3regs_df = regs_df[regs_df['Generation'] >=  'Gen 3']
g1regs_df = g1regs_df.astype({"Customers":"int"})
g2regs_df = g2regs_df.astype({"Customers":"int"})
g3regs_df = g3regs_df.astype({"Customers":"int"})

print(str("Customers: "+str(g1regs_df["Customers"].sum())+" |
Registers: "+str(g1regs_df["Customers"].count())))
print(str("Customers: "+str(g2regs_df["Customers"].sum())+" |
Registers: "+str(g2regs_df["Customers"].count())))
print(str("Customers: "+str(g3regs_df["Customers"].sum())+" |
Registers: "+str(g3regs_df["Customers"].count())))
```