ALKUBAISY, D., PIRAS, L., AL-OBEIDALLAH, M.G., COX, K. and MOURATIDIS, H. 2021. ConfIs: a tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design. In *Ali, R., Kaindl, H. and Maciaszek, L. (eds.) Proceedings of 16th Evaluation of novel approaches to software engineering international conference 2021 (ENASE 2021), 26-27 April 2021, [virtual conference].* Setúbal, Portugal: SciTePress [online], pages 80-91. Available from: https://doi.org/10.5220/0010406100800091

ConfIs: a tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design.

ALKUBAISY, D., PIRAS, L., AL-OBEIDALLAH, M.G., COX, K. and MOURATIDIS, H.

2021

ConfIs: A Tool for Privacy and Security Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design

Duaa Alkubaisy[1 2], Luca Piras [3], Mohammed Ghazi Al-Obeidallah [4],

Karl Cox[1], Haralambos Mouratidis[1]

[1] *Centre for Secure, Intelligent and Usable Systems, University of Brighton, UK*
{D.alkubaisy,, K.Cox, H.Mouratidis}@brighton.ac.uk

[2] *Imam Abdurrahman Bin Faisal University, Dammam, Saudi Arabia*
daalkubaisy@iau.edu.sa

[3] *School of Computing, Robert Gordon University, Aberdeen, UK*
l.piras@rgu.ac.uk

[4] *School of Computer Sciences and Informatics, Amman Arab University, Jordan*
m.obeidallah@aau.edu.jo

Keywords: Security Requirements, Privacy Requirements, Requirements Conflicts, General Data Protection Regulation (GDPR), Requirements Modelling, Privacy by Design.

Abstract: Privacy and security requirements, and their potential conflicts, are increasingly having more and more importance. It is becoming a necessary part to be considered, starting from the very early stages of requirements engineering, and in the entire software engineering cycle, for the design of any software system. In the last few years, this has been even more emphasized and required by the law. A relevant example is the case of the General Data Protection Regulation (GDPR), which requires organizations, and their software engineers, to enforce and guarantee privacy-by-design to make their platforms compliant with the regulation. In this context, complex activities related to privacy and security requirements elicitation, analysis, mapping and identification of potential conflicts, and the individuation of their resolution, become crucial. In the literature, there is not available a comprehensive requirement engineering oriented tool for supporting the requirements analyst. In this paper, we propose ConfIs, a tool for supporting the analyst in performing a process covering these phases in a systematic and interactive way. We present ConfIs and its process with a realistic example from DEFeND, an EU project aiming at supporting organizations in achieving GDPR compliance. In this context, we evaluated ConfIs by involving privacy/security requirements experts, which recognized our tool and method as supportive, concerning these complex activities.

1 INTRODUCTION

Conflicts arising between different requirements, such as privacy and security, are a common problem in engineering software systems [1]. Conflicts in software requirements are inevitable because of the nature of software development for realistic systems, and conflicts, therefore, are the most common cause of inconsistencies during the software development process [2]. Every case of conflict based on requirements is surrounded by complex issues, and these issues should be taken into consideration when resolving the conflicts [3]. Security and privacy requirements should be considered essential for every software system. Privacy has become a mainstream topic, and especially problematic for software development companies. Problems around misuse of presumed personal data by organizations, especially social media companies, has led to moves to 'guarantee' privacy at legislative levels, as envisioned in the EU's General Data Protection Regulation (GDPR) [4]. However, from the developer's point of view, certain issues crop up when adhering to security requirements, while others appear when adhering to privacy requirements. This can lead to conflict when trying to meet these requirements, and it is now necessary for developers to manage these conflicts in order to be compliant with GDPR. However, there is a degree of complexity within these conflicting requirements that makes resolution less immediately obvious. Recourse to the business objective is one way to determine whether a security requirement outweighs its privacy conflict in aiming to achieve compliance with GDPR. The first step in this type of conflict resolution is to be able to identify the conflict in the first place: this paper outlines an approach for doing so.

In the context of software development, a conflict is defined as a clash of interests in the development environment between privacy and security requirements [5]. Such a conflict could arise at any point in the Systems Development Life Cycle (SDLC), irrespective of whether an agile, traditional or hybrid approach is used. Regardless of the approach, it is less costly to identify incorrect requirements – and here we can add privacy and security requirements [6] – in the requirements phase than to do so later [2]. For example, pseudonymization (privacy requirement) may conflict with the need for authentication (security requirement) to avoid a data breach. While such conflicts are common, the challenge is to balance them without creating the opportunity for an easier breach of privacy or security. Conflicts arising from incompatible requirements can negatively affect information systems, even if controls are put in place [1, 2 and 3]. Consequently, it is preferable to manage conflicts that are identified early in the lifecycle, before they derail the entire project. However, a requirement conflict can still affect the development of information systems and their successful deployment, even after controls have been put in place to manage conflict or resolve it [5].

Data breaches are a key concern for businesses with large amounts of personal data, such as banks and governmental departments, as such systems are the most frequently targeted, accounting for nearly 80% of all incidents disclosed [7]. Commercial organizations are also at risk. For example, TalkTalk, a telecoms provider, was hit with a record £400K fine for a data breach in 2015 that exposed the private details of more than 150,000 customers [8].

GDPR forces organizations to implement changes that relate to the use of personal data as well as its protection. GDPR empowers citizens to take greater control of their personal data by having a say in the use of their data. Organizations are required to keep track of the use of user data, which allows the relevant authorities (such as individuals) to give consent with ease. Despite the advantages of GDPR, it can be hard to apply for several reasons, including complexities involved in measures put in place by companies to enhance security. These complexities can lead to conflicts in addition to the complexity involved in covering various aspects of data protection. Most of the existing approaches in the literature [9, 10 and 11] do not provide adequate solutions to identify and resolve conflicts between security and privacy requirements. Identifying and resolving such conflicts are essential to mitigate threats to software systems, as unresolved conflicts could make a system vulnerable to threats.

This paper is based on our previous work Alkubaisy (2017, 2019), and here we present the final framework. This paper provides a novel structured framework that fulfils the gap of the current state of the art. Above all, this paper addresses the following Research Questions (RQs):

RQ1: How to design a framework supporting the analyst to identify and resolve conflicts between privacy and security requirements?

RQ2: How to support the analyst in the identification and resolution of conflicts between requirements in a systematic and tool-supported way in real cases**?**

RQ1 will be addressed by extending SecTro, a requirement modelling tool [18]. The proposed framework offers the analyst a process or guide to help him in identifying and resolving conflicts. The presented framework will be validated using one part of the DEFeND project [13] to ensure that this framework is GDPR compliant.

RQ2 will be addressed by reviewing the current methods to identify conflicts between requirements, and by introducing *ConfIS* framework phases to help the analyst to locate conflicts between requirements.

The rest of the paper is organized as follows. Section 2 presents the baseline from which we started and based our work. These parts are phases of the theoretical framework, DEFeND project where the framework has been applied, and answers to RQ1. Section 3 addresses RQ2 by proposing Tool-Supported Conflict Identification, Resolution and application of these within DEFeND, showing and discussing our Case Study. Section 4 evaluates the proposed ConfIS framework. Related work and conclusion are presented respectively in Sections 5 and 6.

2 BASELINE AND THEORETICAL FRAMEWORK

This section presents an overview of the key parts presented in this paper. This paper is based on our previous work Alkubaisy (2017, 2019), and here we present the final framework based on the previous work. The first part presents our proposed theoretical framework, enhanced with an explanation of each phase. We then explain more about the DEFeND project [14,16], an ongoing live project aiming to determine needs related to identifying conflicts and conflict resolution. An overview of the SecTro tool, which has been extended to fulfil the requirements of our proposed framework, is presented at the end of this section.

2.1 Theoretical Framework Phases

Our proposed framework has a sequence of phases to achieve conflict detection and resolution, presented in Figure. 1:

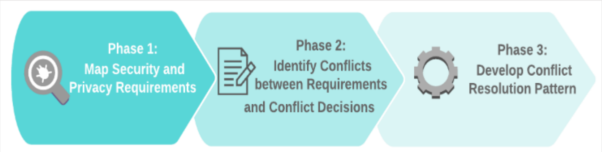

Phase 1:
Map Security and Privacy Requirements
Phase 2:
Identify Conflicts between Requirements and Conflict Decisions
Phase 3:
Develop Conflict Resolution Pattern

Figure 1: The phases of the proposed theoretical framework

As Fig. 1 illustrates, some of the steps are semi-automated, while the others are manual steps, based on the analyst's point of view.

The partners might have a special perspective on requirements. First, the conflicts between requirements are identified, based on a matrix presented by a previous study [14]. Hence, we sort the requirements that could lead to a potential conflict. After identifying the requirements that are in conflicts, the analyst must decide whether this kind of conflict would affect the system, based on the presented scenarios. Therefore, the first phase of the framework is performed manually by the software requirements analyst. Phase Two identifies the potential conflicts between requirements that were detected in the previous phase. The final phase proposes conflict resolution patterns by matching the problem to a resolution pattern for each conflict that the analyst might face. Those patterns act as a reference for the analyst to resolve conflicts between requirements. The final phase of our framework is automated by using the SecTro tool (by importing a privacy pattern library).

2.2 DEFeND Project

The DEFeND project was designed as an EU project to support organizations by defining essential tools and methods that enable organizations and authorities to monitor their actions so that they can be GDPR-compliant [13]. DEFeND stands for Data govErnance For supportiNg gDpr. DEFeND aims at improving existing frameworks and software tools, and developing and designing new integration software based on market needs. This is with the aim of delivering a unique data platform for privacy governance.

In order to achieve GDPR compliance and raise awareness of the diverse features of GDPR, DEFeND will deliver a platform which empowers organizations in various sectors to assess their compliance status. The DEFeND platform allows for designing and analysing models following a Privacy-by-Design approach. The DEFeND platform provides five main services to organizations and relevant stakeholders: Data Scope Management Service, Data Process Management Service, Data Breach Management Service, GDPR Planning Service and GDPR Reporting Service. Each of these services assists organizations in collecting, analysing and operationalizing different aspects and articles of GDPR, and providing appropriate reporting capabilities.

The DEFeND platform will be in a live laboratory pilot studies in four different areas: healthcare, finance (or banking), energy and local public administration. The DEFeND platform will be tested in an effective environment in three scenarios through two different types. The first type focuses on the GDPR compliance process for end users, while the second addresses GDPR implications for external stakeholders. Our proposed framework will identify and resolve conflicts between requirements by applying a scenario from the healthcare sector of the DEFeND project.

2.3 SecTro

SecTro tool has been used to aid in the modelling of conflicts resolution [15]. It implements the Secure Tropos Methodology which consists of an engineering approach for security and privacy requirements, starting from early-stage requirements of the IS (Information System) development process. Secure Tropos must be specified in the early phases of an IS development, as it is an organized approach for goal-oriented security and privacy requirement modelling. The Secure Tropos methodology supports a modelling language, security aware processes and automated processes. The Secure Tropos methodology enhances our framework by translating conflicts between requirements in a goal model. SecTro presents models that contain security and privacy requirements [16]. It involves modelling views which are used to facilitate system design and elicitation of security and privacy requirements.

3 TOOL-SUPPORTED CONFLICT RESOLUTION AND CASE STUDY

To solve the conflicts between requirements, we explored critical conflicts from literature review, research studies and European Projects. The needs come also from a discussion with stakeholders from different domains, such as banking, healthcare, public administration, and smart energy; all of which need to achieve GDPR compliance. In addition, we found that conducting a requirement analysis on Privacy-by-Design, found potential conflicts that could not be solved. Hence, on behalf of DEFeND – a European Project - we have interviewed those stakeholders in relation to how to create platforms to address such conflicts.

Achieving GDPR compliance is very complex. To do so, requirements analysis must be conducted, in which many conflicts arise, and stakeholders may have great difficulty in understanding how to manage and solve them. Moreover, we found that performing requirements analysis on Privacy-by-Design in real cases is essential, according to the stakeholders. We recognize that stakeholders need to achieve GDPR compliance via Privacy-by-Design, and they consider this as a problem. In addition, as mentioned above, there is a lack of recent studies which addresses this issue. Stakeholders need a tool to resolve the identified conflicts more quickly by reducing their effort and having a ready-to-use solution of any of the conflicts that could arise.

3.1 Motivation Scenario

As we discussed earlier, within the DEFeND project section, it comprises several services. The Centre for Secure, Intelligent and Usable Systems at the University of Brighton works on one of DEFeND's services; Data Scope Management (DSM) which supports Privacy by Design (PbD). DSM developed a case study which has been used as a storyline, to regard highly valuable PbD activities of DSM. In [17], the DSM service has been widely discussed by describing its flow phase by phase, and by using the storyline. In this paper, we will illustrate one example from the storyline and apply the ***ConfIS framework phase by phase to identify and resolve the conflicts between security and privacy requirements.*** The example being applied in the *ConfIS framework* is as follows:

One of the most critical aspects is to manage patients' medical record, have verification from a supervisor for any changes happening to it, and establish a retention period for the data.

In section 3.4 we will analyse this example and find out the related security and privacy requirements. Therefore, we will apply the ConfIS framework phase by phase to resolve conflicts.

3.2 Integrating the Theoretical Framework in SecTro

The SecTro tool has been extended with new concepts to support the analyst in identifying and resolving conflicts. The theoretical framework was completely integrated and implemented in the top of SecTro, with its analysis supporting all phases. Here, the case study shows in more details, diagrams from the tool that are integrated with the theoretical framework.

Moreover, the new concepts are added to the privacy by design view of SecTro to support the modelling of requirements conflicts. Phase two involves identifying conflicts between requirements according to the output from phase one. At This Point, the analyst needs to make conflict decisions based on each scenario and the relevant requirements. Next, in phase three, new concepts are added to identify conflicts; based on the out-come of phase two, the analyst will locate these conflicts. The next section describes the case study in further depth and applies the theoretical framework to achieve conflict resolution.

3.3 Tool Description in a Case Study

Based on the motivation example, we will illustrate the security and privacy requirements, following the phases of the ConfIS framework to resolve conflicts, using the extended supported tool. The first phase aims to map the security and privacy requirements [12]. This assumes the existence of a matrix to find out the potential conflicts between security and privacy requirements, based on our recent study [14]. The next sections show the application of our proposed framework phases in identifying and resolving conflicts, discusses the application of the motivation example in SecTro, and presents the theoretical framework to identify and resolve conflicts (3.4-3.6).

3.4 Phase 1: Mapping Security and Privacy Requirements

Based on the motivation scenario presented in section 3.1, we find that there are security and privacy requirements involved. Therefore, to determine which requirements are in conflict, we model the scenario using the organizational view of SecTro as presented in Figure 2. Each bubble represents an actor (i.e. Supervisor, Doctor, and Employee). We break the scenario into several tasks to assign a related requirement for it, and assign each task to a related requirement, to find out which task has a potential conflict. The Doctor needs to acquire patient medical results from an Employee, while sending this sort of information needs to be confidential and treated with integrity. When the Doctor runs a patient examination or updates patient medical records, this task must remain Anonymous. On the other hand, the same data needs to be validated by a Supervisor; hence, this task requires some Accountability. Any updates on patient medical records by the Doctor also needs to be Accountable based on GDPR Principles. As a result, each task has its own security and privacy requirements, which helps in identifying the conflicting requirements. For instance, anonymity as a privacy requirement conflicts with accountability as a security requirement. In Fig. 2, we model the motivation example in SecTro to pinpoint these conflicts.

3.5 Phase 2: Identify Conflicts between Requirements and Conflict Decisions

To identify conflicts, we next divide each scenario task to address the possible conflicts. Therefore, for each case, we assign the involved requirements. Based on the “Managing Patient Records” scenario presented, we will address the security and privacy requirements for each activity. For instance: The lab must perform a medical examination, then send the results to the doctor (security requirements: confidentiality and integrity). Furthermore, medical results will be sent to the doctor to update the patient’s medical record; this action must be compatible with the GDPR accountability principle. Furthermore, while the doctor is updating the patient’s medical record, this action should be anonymous. This therefore could lead to conflicts between requirements- accountability and anonymity. To process the updated results, they should be verified by a supervisor; therefore, this requirement involves accountability as a security requirement. In addition, updating the patients’ medical record involves anonymity, to keep the patients’ record private, according to Privacy-by-Design principles. On the other hand, this update must be accountable to the supervisor to keep the system secure and accurate; the supervisor must be aware of every and final updates being made and by whom. At this point ***conflicts is likely to occur between anonymity as a privacy requirement and accountability as a security requirement***. This task can require more than one requirement involved which will have potential conflicts arising between requirements, especially based on privacy and security requirements. It is therefore difficult to fulfil both requirements. Accountability is the requirement that holds entities responsible for their actions, while anonymity allows entities to use resources or services without having to reveal their identity. In Figure 3, we provide an overview of the Privacy-by-Design view of Managing Patient Records. In this view, we allocate security and privacy requirements for each soft goal.

As discussed above, we have already identified a conflict between accountability related to the supervisor and anonymity related to the doctor. In this phase, we only highlight the conflict issue.

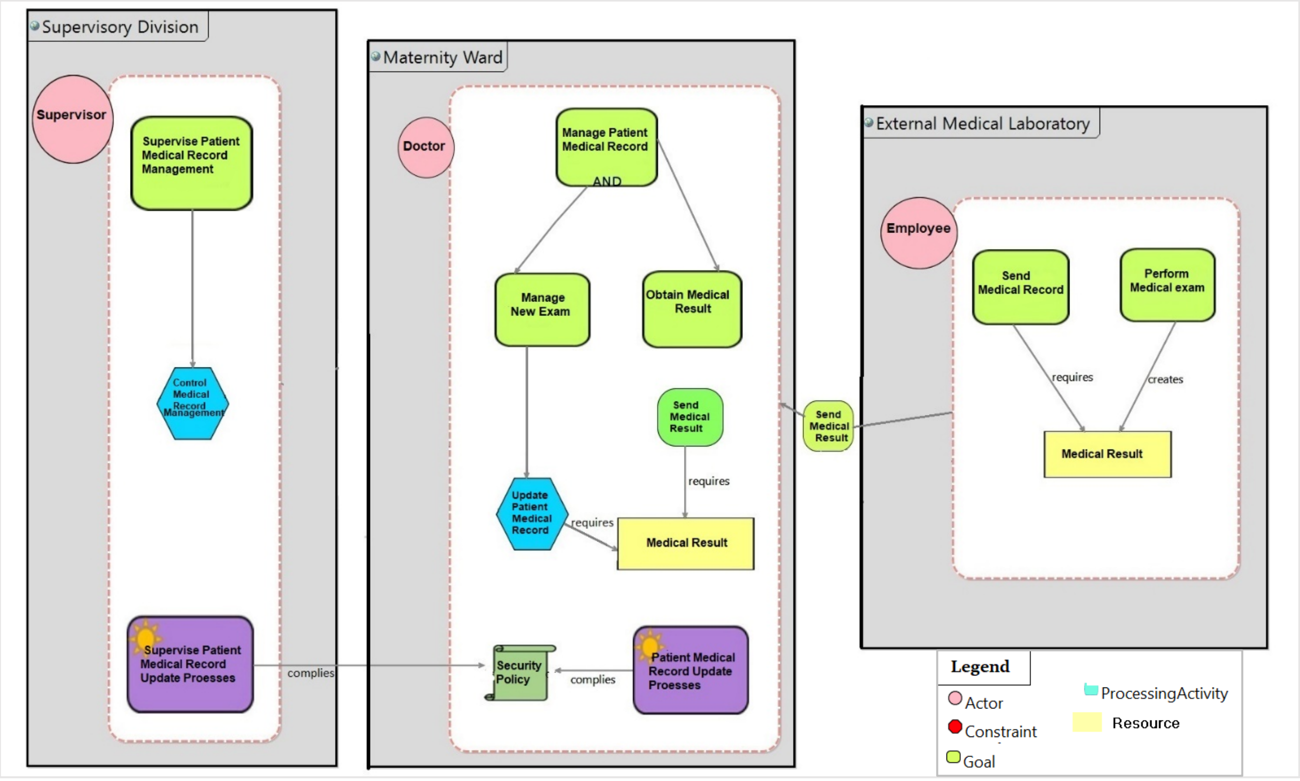


Figure 2: Organization View of Managing Patient Records

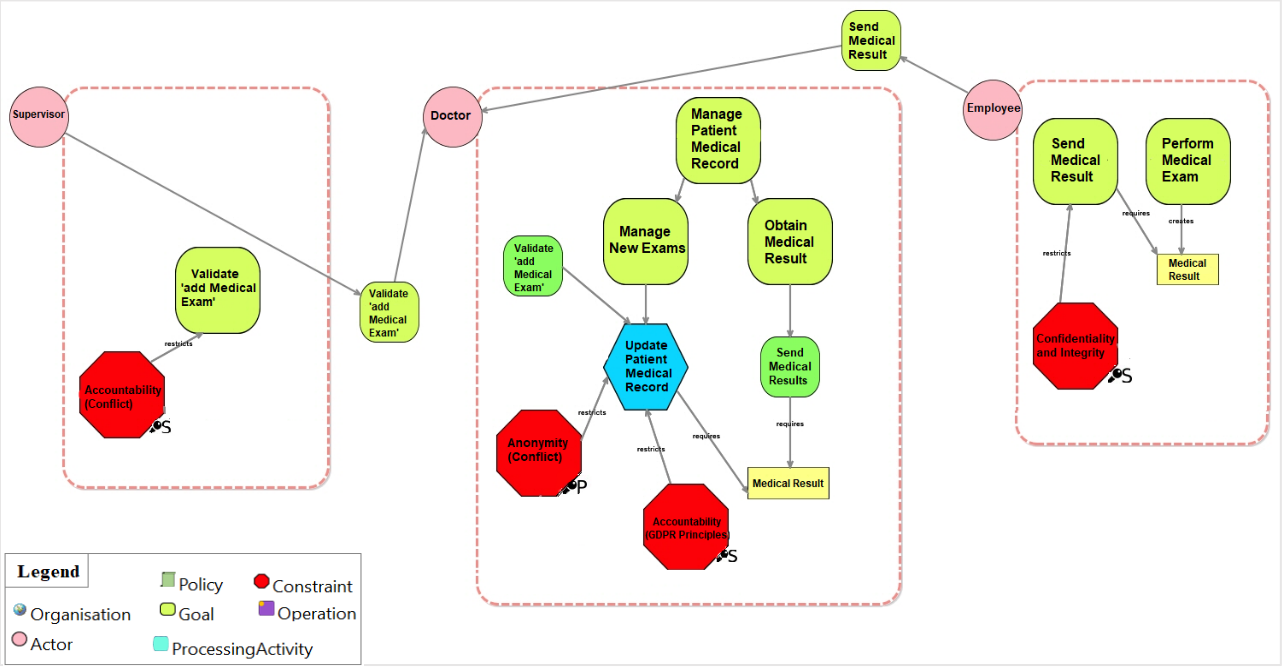


Figure 3: Privacy by Design View of Managing Patient Records

3.6 Phase 3: Conflict Resolution Patterns

In this phase, for each type of conflicts, we model a pattern to link two conflicting requirements, and a suitable supporting tool.
To resolve a conflict via supported tools, we identified a relevant tool that could satisfy both types of privacy and security requirements. By applying this scenario in SecTro, we must add the tool to the Privacy Pattern Library. In this case, we identify two supporting tools, but determine that the IDEMIX tool is more appropriate [19]. Figure4 shows how we add the supporting tool into the framework. Consequently, Figure.5 shows the Privacy-by-Design view after adding the new concepts to identify conflict between requirements and imports a suitable mechanism to satisfy the requirements.

4 DISCUSSION

There is a need to fulfil the anonymity requirement for the *Update Patient Medical Record* process, making sure that nobody knows which doctor has made the change on a record. This is fulfilled by the mechanism, which IDEMIX fulfils our solution requirement. In addition, the accountability constraint is related to the validate aspect of the *Add Medical Exam* process, i.e., a supervisor needs to validate the change. However, for this, the supervisor needs to know which doctor made the change; thus, there is a conflict between accountability and anonymity, because the supervisor cannot know, due to the anonymity requirement, who the doctor is, so accountability cannot be fulfilled. We solve this by introducing the IDEMIX mechanism, which will be used by the supervisor, so that accountability can be fulfilled.

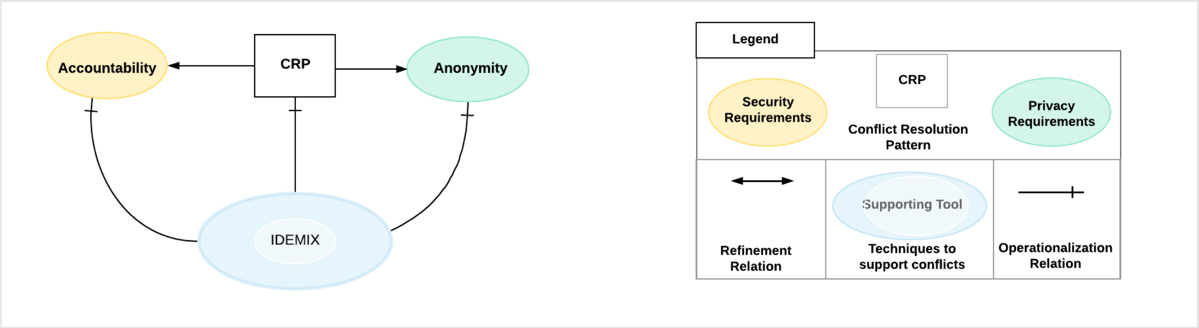


Figure 4: Conflict Resolution

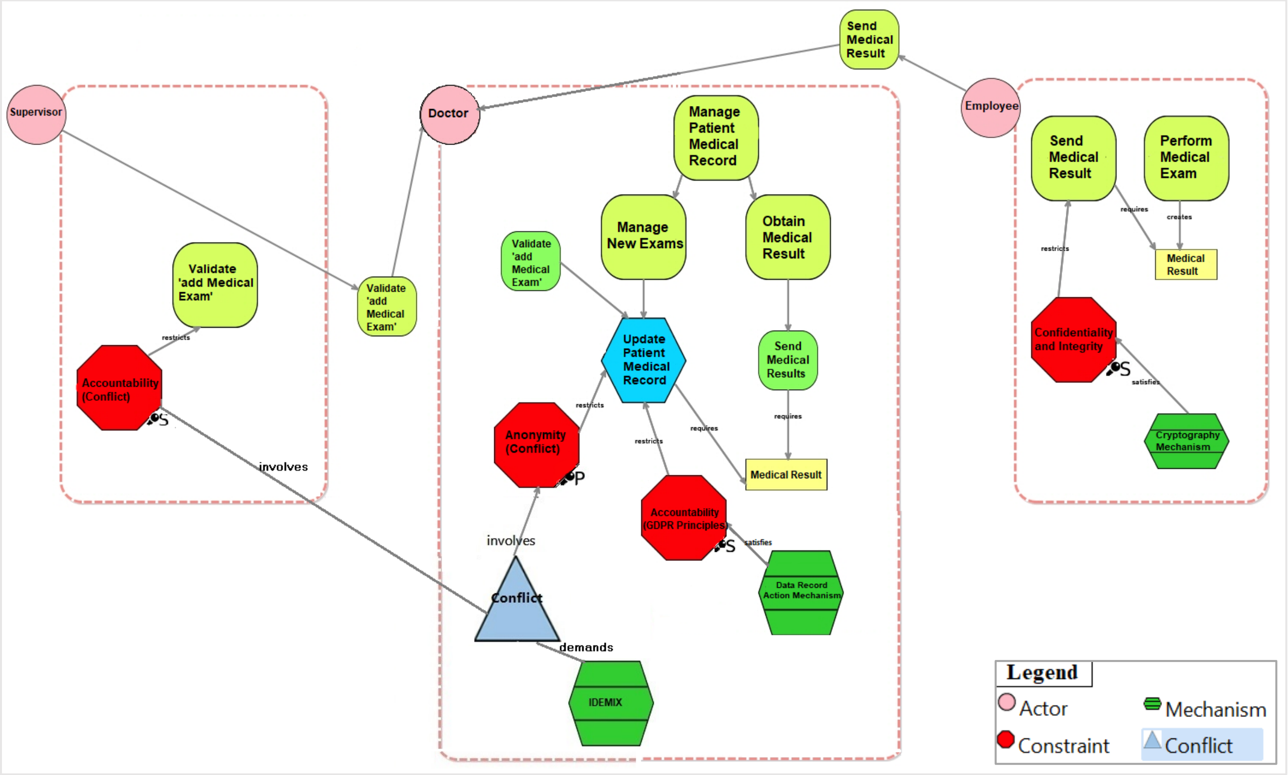


Figure 5: Integrating conflict resolution in Privacy-by-Design view of Managing Patient Records

IDEMIX is a solution for minimizing the release of personal information and can be based on one of many proposed techniques for anonymizing the transport medium used between users and service providers. IDEMIX is an optimizing cryptographic compiler that achieves an unprecedented level of assurance, without sacrificing the practicality for a comprehensive class of cryptographic protocols. This protocol satisfies the conditions for anonymous, authenticated, and accountable transactions between users and service providers. On the lab side, the employee should fulfil confidentiality and integrity while sending medical results; we fulfil this with the cryptographic mechanism. In addition, the last point is related to fulfilling GDPR principles, and an example is accountability, where it is necessary to record which doctor did the change. We fulfil this by the Record Data Action mechanism.

5 EVALUATION

In this section, we describe the preliminary evaluation we carried out within the DEFeND project, for the tool and method described in this paper. Here we report the evaluation strategy and results. The framework is Human Oriented, which supports the investigation to conduct this kind of analysis based on the importance of usable systems and promotes the process of human centered design as a way to achieve them [20]. Human Oriented is useful to design the evaluation in a human centered way, to obtain feedback from experts of security and privacy engineering. We have fifteen participants, who are researchers of privacy and security engineering. They work within different universities from various countries including the United Kingdom, Italy, Greece, Germany, Saudi Arabia, and China; this gives scope for a variety of perspectives (achieving heterogeneity).

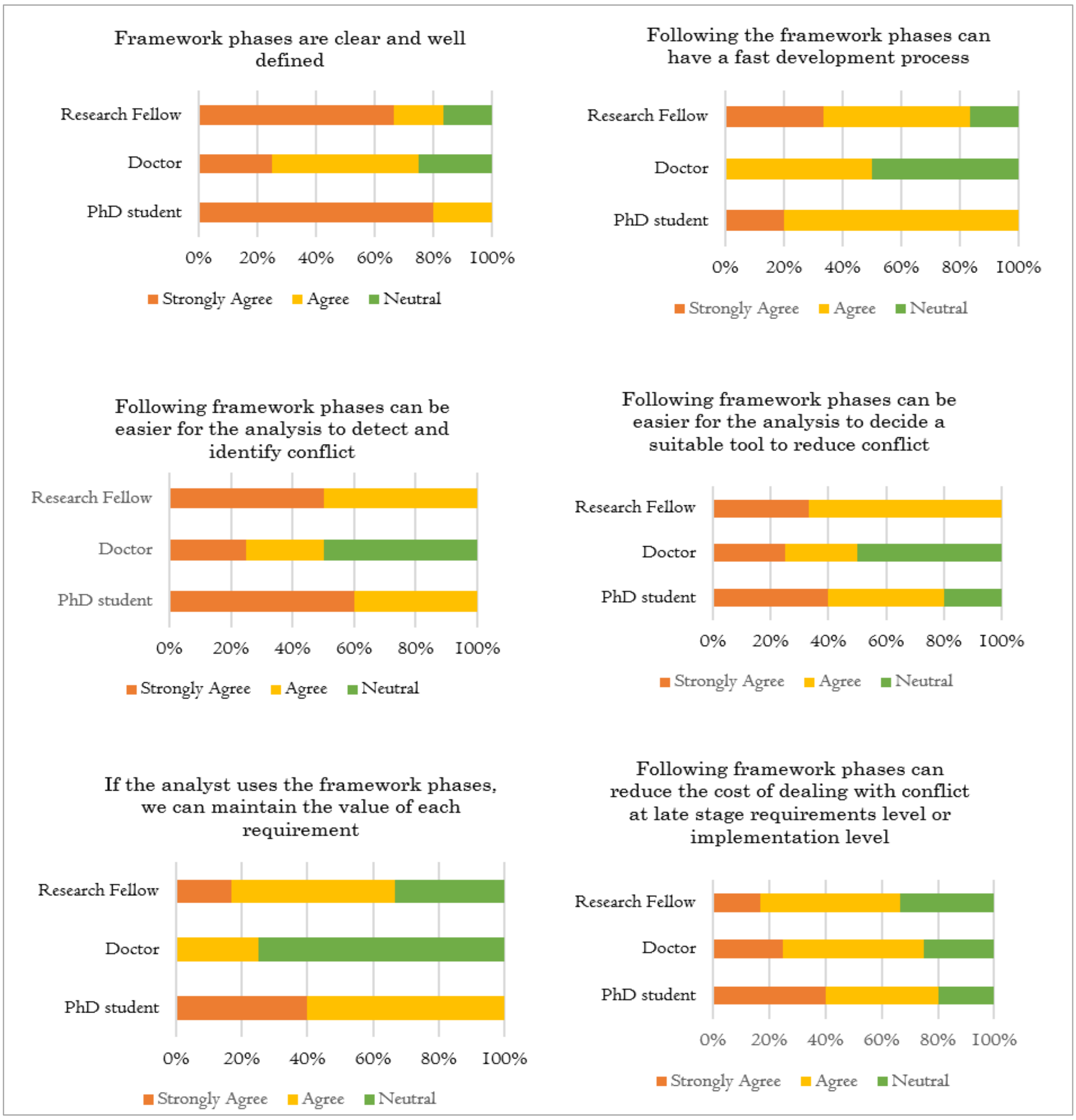
Evaluation Strategy. To have a comprehensive evaluation, we use qualitative and quantitative analyses. For the qualitative aspect, we design a focus group session, having participants who are both experts and researchers. Before we began the evaluation, we constructed a pilot focus group evaluation with three participant groups, namely- PhD student, Doctor and Research Fellow. This revealed to us the possibilities of improving the focus group evaluation according to the participants' feedback. Moving forward, we could perform the full-scale focus group evaluation. The rational of the problem, is to allow the participants to interact with a task in order to find out how the researcher can identify conflicts between requirements. Therefore, we describe the ConfIS framework with an example provided (as discussed in this paper) and provide the participants a useful handout containing a description of the focus group sessions, and what the input and outputs for each phase of the framework are. In addition, each part has full content. After the participants have grasped the full idea and learned how to use the framework, we asked them to apply ConfIS to the same task that we started the presentation with it. This comparison method gave us some insight into using the framework and without using it. By the end of the session, participants are required to complete a survey, evaluating the framework in general- phase by phase.

This evaluation strategy covered the qualitative evaluation. By having the focus group and during discussions in this session, we observe how the participants understand the framework. Additionally, answering the survey thereafter gave a quantitative evaluation of the framework.

Evaluation Results. The survey consisted of fifteen participants, of which 100% are respondents. Encouraging responses of its design, revealed it showed huge efforts, with a well and confident presentation, interesting field and helpful work, utilizing real cases within EU projects. Its clarity in understanding the research objective, deemed a supportive method which could be used in an iterative way, and for each phase there is good support for the analyst. Additionally, it brought revelations of much more alternatives that could arise for the designer. The tables are a valuable form of presentation, but models could be a better way to visualize potential analysis of elements and solutions, speeding up the process. The evaluation was in general a positive experience, and the evaluator clearly presented the framework and its main objectives. Furthermore, suggested areas for improvement included, considering additional features/phases such as prioritization and the conflicts involved with this. The material and tools used to resolve conflicts could be more informative especially for those without much knowledge of the field, which could mean including more examples. Furthermore, specifying the basis of any choice of solution; when the participant identifies conflicts, and then chooses a possible solution, specifying how to choose one if there is more than one option is not supported. Moreover, creating a more structured evaluation that guides the subjects in their evaluation should be noted. Participants were a bit unsure of the utility (or the ordering) of the conflict identification phase. The identification of the enforcement technologies that "resolve" the identified conflicts, eliminated the conflict and some participants did not see the reason identifying them, if there were no more conflicts to search.

The majority's share, well over 70% of research fellows agree with the general framework. They approve that the relevant phases are clear, well defined, sequentially in order, can have a fast development process, is easier for identifying conflict, reducing it and its relevant costs, and maintaining the value of each requirement. The same can be said for doctors, with the exception of 50% indicating a neutral response to the framework phases having a fast development process, being easier for detecting/identifying and reducing conflict, and for maintaining the value of each requirement. Additionally, more than 80% of PhD students agree with the design of the general framework, and its phases Figure 6.

Figure 6: General Framework Per Respondent Group



A summary analysis of the evaluation survey reveals most respondents were research fellows (40%), followed by PhD students (33%) and doctors (27%). They all found the research design questions to be appropriate, useful, well presented (87%) and the research field quite interesting (93%) in gaining their feedback. On the other hand, just 54% agreed that the results were clearly presented; this leaves room for improvement Additionally, the general framework was also well received by the majority, proving to be sequentially in order (87%), clear and well defined (80%), easier for analysis (80%) and for making feasible decisions such as reducing cost, conflict, and faster development processing (73%) (Figure 7). Among the three phases, to Phase 1 (74-80%) agreed that Mapping between security and privacy to identify conflict was clear. Phase 2 was well received with the majority (80-86%) agreeing that the researcher adequately addressed conflicts between requirements and decisions.

Additionally, feedback on Phase 3 showed varying responses (67-87%), yet the participants still agreeing that there was an ease to understanding conflict resolutions patterns and its supporting tools. (Table 1).

Phase 1: Mapping Security and Privacy Requirements	74-80% (strongly/agree)
Phase 2: Identify Conflicts between Requirements and Conflict Decisions	80-86% (strongly/agree)
Phase 3: Conflict Resolution Patterns	67-87% (strongly/agree)

Table 1: Phases

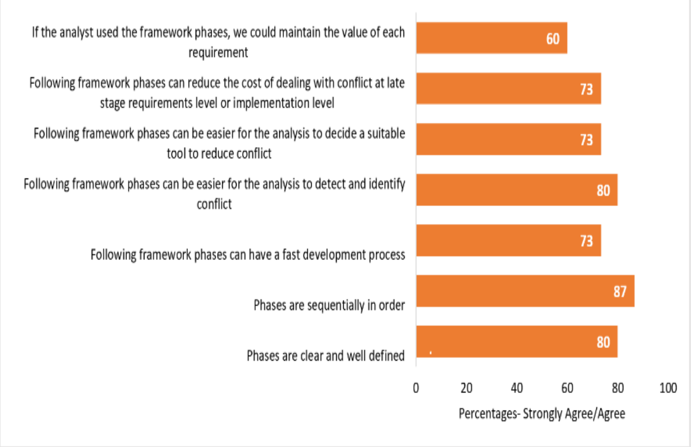


Figure 7. General Framework

6 RELATED WORK

Studies have been conducted regarding conflicts in requirement engineering approaches. Aldekhail et al [9] provide a comparative review on the conflict analysis approach, which was conducted with 20 studies from 2001 to 2014. Moreover, approaches in the literature are focused only on considering the following important aspects separately: identification, analysis, and resolution of conflicts. In fact, most of them focus only on identifying conflicts between requirements, especially NFR (non-functional requirements), without considering an overall, systematic approach for identifying, analysing and, above all, resolving them. This paper aims exactly to fulfil such gap, by supporting the analyst in all three phases, in a tool-supported, semi-automatic, interactive way, with the systematic approach we propose.

A recent study conducted by Ramadan et al [21, 22] examine- detecting conflicts between data-minimization and security requirements. They investigate how conflicts between security and privacy requirements gather into the systems, in business process models.

Salnitri et al. [23] in their work, propose a novel method named SePTA (Security, Privacy and Trust Approach). This method supports a unified specification of security, privacy and trust requirements, under one framework. It, more so, enables software designers and security experts to enforce such requirements, and is designed for sociotechnical systems. They focus on how security, privacy and trust requirements can be specified in the early requirement phase, using a goal-based modelling language, and how such requirements can be correctly enforced in the late requirement phase, using goal-based modelling languages and a modelling language for business processes. Horkoff et al [24] examined the top-cited 246 papers over the past 20 years, as per Scopus. They make several observations about the Goal-oriented requirements engineering (GORE) field, where goals are used as a useful conceptualization to elicit, model, and analyse requirements, capturing alternatives and conflicts. Despite extensive efforts in this field, the requirements engineering (RE) community lacked a recent, general systematic literature review of the area.

An expressive goal-based modelling language for requirements that supports the representation of nice-to-have requirements, preferences, optimization requirements, constraints and more, have been proposed by Nguyen et al. [25]. They exploited automated reasoning solvers in order to develop a tool that supports sound and complete reasoning, with respect to goal models, and scales well to goal models with thousands of elements. Their proposal advances the state-of-the-art on goal modelling and reasoning. Additionally, for future work they propose an empirical validation of the CGM-Tool with modelers and domain experts, currently working in this direction with PhD students and post-docs. While their work is in the preliminary stages, our framework has already been applied to a real case study named DEFeND, which has been validated, and is now in the evaluation process.

Bhavsar et al [26] presented a survey paper comparing recent studies of conflict between requirements in the early stage of development. In their survey, they summarize case studies related to different domains of software engineering, with respect to requirement gathering techniques, and how conflicts could be resolved, that arise at the RE phase, using the Agile software development method. This model includes a continuous iteration of development and testing phases, so that it could deliver the product in the early stage, which makes Agile software development used widely by companies. While this is so, it also increases the complexity of the system. The authors have also cited the work of Alkubaisy et al., [15] who investigates conflicts between security and privacy requirements.

Maxwell et al., [27] also conducts a cross- reference approach for identifying conflicting software requirements. Their work revealed that rules and laws are easier to handle, and the reputation of the company depends on the rules and regulation which are followed. On the other hand, this can lead to an increase in costs, because system laws have overloads.

Furthermore, Schon et al., [28] investigates agile software development, and discovers that rapid changing in requirements can be easy to handle, whilst on the other hand, there are more complexities because a hybrid development model is used.

7 CONCLUSION

In this paper, we outline the need to identify conflicts between requirements and to have a suitable tool to resolve such conflicts. The ConfIS framework has been presented for identifying conflicts between security and privacy requirements. ConfIS allows the analyst to deal with the potential conflicts that may be discovered later and has been applied to a case study from the DEFeND project. Lastly, we demonstrate the phases of ConfIS step-by-step, to investigate how it helps the analyst to identify and resolve conflicts via a supporting tool.

ACKNOWLEDGMENTS

The DEFeND project received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 787068.

REFERENCES

1. Kim, Minseong, et al. "Managing requirements conflicts in software product lines: A goal and scenario based approach." Data & Knowledge Engineering 61.3 (2007): 417-432.
2. Egyed, Alexander, and Boehm, Barry. "A comparison study in software requirements negotiation." Proceedings, INCOSE’98. 1998.
3. Van Lamsweerde, et al. "Managing conflicts in goal-driven requirements engineering." IEEE Transactions on Software Engineering 24.11 (1998): 908-926.
4. Albrecht, Jan Philipp. "How the GDPR will change the world." Eur. Data Prot. L. Rev. 2 (2016): 287
5. Schär, B. "Requirements Engineering Process HERMES 5 and SCRUM." University of Applied Sciences and Arts (2015).
6. Liu, L., Yu, E., and Mylopoulos, J. (2003). "Security and privacy requirements analysis within a social setting." In: Proceedings, 11th IEEE International Requirements Engineering Conference 2003. [Online]. 2003, Washington, DC: IEEE, pp. 151–161. Available from: http://www.cs.toronto.edu/pub/eric/RE03.pdf. [Accessed: 11 March 2016].
7. Botha, Johnny, Grobler, Marthie, and Eloff, Mariki. "Global data breaches responsible for the disclosure of personal information: 2015 & 2016." European

Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2017.

8. Farrell, S. "Nearly 157,000 had data breached in TalkTalk cyber-attack." 2015. Available at: https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack [Accessed: 15 May 2017].
9. Aldekhail, Maysoon, Chikh, Azzedine, and Ziani, Djamal. "Software requirements conflict identification: Review and recommendations." International Journal of Advanced Computer Science & Applications 1.7 (2016): 326-335.
10. Mairiza, Dewi, and Zowghi, Didar. "Constructing a catalogue of conflicts among non-functional requirements." International Conference on Evaluation of Novel Approaches to Software Engineering. Springer Berlin Heidelberg, 2010.
11. Mairiza, Dewi, et al. "Conflict characterization and analysis of non-functional requirements: An experimental approach." Intelligent Software Methodologies, Tools and Techniques (SoMeT), 2013 IEEE 12th International Conference on. IEEE, 2013.
12. Alkubaisy, Duaa. "A framework managing conflicts between security and privacy requirements." *2017 11th international conference on research challenges in information science (RCIS)*. IEEE, 2017
13. Mouratidis, H.: Secure Software Systems Engineering: The Secure Tropos Approach. JSW (2011)
14. Piras, Luca, et al. "DEFeND Architecture: A Privacy by Design platform for GDPR compliance." International Conference on Trust and Privacy in Digital Business. Springer, Cham, 2019.
15. Alkubaisy, Duaa, Cox, Karl, and Mouratidis, Haralambos. "Towards detecting and mitigating conflicts for privacy and security requirements." 2019 13th International Conference on Research Challenges in Information Science (RCIS). IEEE, 2019.
16. Piras, L., Al-Obeidallah, M.G., Pavlidis, M., Mouratidis, H., Tsohou, A., Magkos, E., Praitano, A., Iodice, A., Crespo, B.G.N.: DEFeND DSM: A Data Scope Management Service for Model-Based Privacy by Design GDPR Compliance. In: 17th International Conference on Trust, Privacy and Security in Digital Business (TrustBus) (2020)
17. Mouratidis, H. & Giorgini, P. (2007). "Secure Tropos: A security-oriented extension of the Tropos methodology." International Journal of Software Engineering and Knowledge Engineering. [Online]. 17 (02). pp. 285–309. Available from: http://www.worldscientific.com/doi/abs/10.1142/S0218194007003240. [Accessed: 10 February 2016].
18. Pavlidis, Michalis, and Islam, Shareeful. "SecTro: A CASE tool for modelling security in requirements engineering using Secure Tropos." CAiSE Forum. 2011.
19. Camenisch, J., and Lysyanskaya, A. "Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation." In EUROCRYPT 2001, vol. 2045 of LNCS, pp. 93-118. Springer Verlag, 2001.
20. Maguire, M.: Methods to Support Human-Centred Design. International Journal of Human-Computer Studies (2001)
21. Ramadan, Qusai, et al. "Detecting conflicts between data-minimization and security requirements in business process models." European Conference on Modelling Foundations and Applications. Springer, Cham, 2018.
22. Ramadan, Qusai & Strüber, Daniel & Salnitri, Mattia & Jürjens, Jan & Riediger, Volker & Staab, Steffen. (2020). A semi-automated BPMN-based framework for detecting conflicts between security, data-Mmnimization and fairness requirements. Software and Systems Modeling. 10.1007/s10270-020-00781-x.
23. Salnitri, Mattia, Angelopoulos, Konstantinos, Pavlids Michalis, Diamantopoulou Vasiliki, Mouratidis, Haralambos, Giorgini, Paolo. (2020). "Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach." *Software and Systems Modeling* 19.2 (2020): 467-491.
24. Horkoff, Jennifer, et al. "Goal-oriented requirements engineering: an extended systematic mapping study." Requirements Engineering 24.2 (2019): 133-160.
25. Nguyen, Chi Mai, et al. "Multi-objective reasoning with constrained goal models." Requirements Engineering 23.2 (2018): 189-225.
26. Bhavsar, Raj, et al. "Resolving Conflicts in Requirement Engineering Through Agile Software Development: A Comparative Case Study." International Conference on Innovative Computing and Communications. Springer, Singapore, 2019.
27. Maxwell JC et al (August 2011) A legal cross-references taxonomy for identifying conflicting 160 software requirements. In: 2011 IEEE 19th international requirements engineering conference, 161 pp 197–206.
28. Schon Eva-Maria (2017) Agile requirements engineering: a systematic literature review. Comput 158 Stand Interfaces 49:79–91.