Risk Identification of Tailorable Context-aware Systems: a Case Study and Lessons Learned*

Mohammad Zarifi Eslami, Brahmananda Sapkota, Alireza Zarghami, Eelco Vriezekolk, Marten van Sinderen, Roel Wieringa

Department of Electrical Engineering, Mathematics and Computer Science
University of Twente - The Netherlands
{m.zarifi,b.sapkota,a.zarghami,e.vriezekolk,m.j.vansinderen,r.j.wieringa}@utwente.nl

Abstract. In this paper, we discuss possible risks posed by the application of tailorable context-aware systems in real-life practices. We use a tailorable context-aware system in the homecare domain as a case study to identify and analyse such risks. Next, we discuss which of these risks can be generalized to the use of tailorable context-aware system in other contexts than homecare. This would help the users of such systems to prevent the risks and guide the design and implementation of them.

Keywords: Risks, Tailorable context-aware systems, Homecare.

1   Introduction

A context-aware system adapts its behavior based on a model of the user's current context [2]. Such a context model is usuallyinferred from data of sensors in the environment of the user. If the adaptation is not only based on the context model, but also on user-defined preferences and requirements, we call this a Tailorable Context-aware (TC) System [19].

The use of TC systems can bring important benefits in many domains. Such benefits include easier to use, more useful and personalized services, as a consequence of proper consideration of the user's context and preferences. However, TC systems can also introduce new or increased risks for the person or organization using these systems. Such risks arise from assumptions that are made during the design, and which are typical for this type of systems, namely: the context model properly reflects reality, the tailoring is done correctly, and the provided service (e.g., in the form of advice or instructions) is used as intended.

It is therefore important to do a risk assessment of a TC system in relation to the environment in which it will be used. Such an assessment may deliver useful results for the design of the system and its introduction in the environment. So far, risk assessment of context-aware systems has mainly focused on privacy and security aspects [7], whereas other aspects such as availability and accountability have received much less attention [8, 4].

The goal of this paper is to make a first step towards introducing risk assessment concerning the availability and accountability aspects, as part of a requirements engineering approach for TC systems. As a case study, we use the design of a TC system in the homecare domain, where the system aims at supporting independent living of elderly people in their private environment.

There is an emerging trend in industrialised countries for using IT-based care services such as health monitoring and coaching and medication reminder to support independent living of elderly [1, 3, 11, 16]. The use of these services can have several benefits such as improving the quality of care, quality of life of elderly, saving time of healthcare professionals and responding to the shortage of qualified staff. The European Council recognises improvement of patient safety as one of the benefits of using eHealth systems [14]. However, IT-based care services can also introduce new types of risks.

The concept of risk has been defined differently in different domains [15, 10, 5]. However, there is a common understanding that risk is a combination of the likelihood that an incident will occur and the impact of that incident. In our work, we are not concerned with the quantification of likelihood nor of impact. Therefore, based on this common understanding, we define risk for TC systems as: the possibility of an undesirable outcome of an incident (related to the operation and/or use of the system). More specifically, we define availability risk as: the possibility of an undesirable out due to the unavailability of the system or its services; and accountability risk as: the possibility of an undesirable outcome due to the fact that no accountable actor can be found. Since risk is defined in terms of undesirable outcomes, we assume that there are stakeholders which suffer the undesirable outcomes. What constitutes a risk is therefore stakeholder-dependent. If stakeholder goals and requirements would change, we may have to repeat the risk assessment.

The rest of the paper is structured as follows. In Section 2, we describe our research methodology and define the scope of the paper. In Section 3, we briefly describe the case study with a TC system applied in homecare. In Section 4, we present the results regarding the identified risk. Finally, in Section 5, we discuss the lessons learned and conclude the paper.

2 Research Methodology

The purpose of risk assessment is to gather necessary information so that subsequent risk treatment decisions can be taken that are both effective and efficient. According to the ISO framework (ISO-31000), risk assessment consists of risk identification, analysis and evaluation [9].

An essential step in risk identification is the identification of all stakeholders, their goals and their interactions with the system. Any interaction (either tailoring or using the system) that may lead to undesirable consequences for that or another stakeholder will be listed as a risk. Thus, we execute the following to reach the goal of the paper:

– Identifying all stakeholders that use and interact with the system;

- Describing the goals of stakeholders and their interactions with the system;
- Identifying possible undesirable outcomes (risks) of these interactions;
- Draw lessons learned for the general case of TC systems.

One important assumption restricts the scope of the paper. We assume that the TC system technically works as designed, i.e., risks due to malfunctioning of internal components of the system (the risks caused by interactive complexity [12]) are out of the scope of this paper. More specifically, we are interested only in risks arising from the interaction of stakeholders with the system.

3 Description of the Case

We performed our case study in a care-institution in the Netherlands. This institution consists of residential blocks where elderly can live and receive care services. We developed a tailorable IT-based homecare service platform to be evaluated in this care institution. To analyse the existing situation, we interviewed professional nurses who provide care services in this institution. The purposes of the interviews was to gain insight in the commonly performed tasks and the possible risks associated with these tasks.

Providing Tailorable Context-Aware Homecare (TCH) services is one of the required features of successful introduction of IT-based care services [6, 20]. Fig. 1 depicts a simple version of a TCH system. The motivation behind such system is to support a care-giver to create a user-specific *service plan* by using a *tailoring platform*, which can be executed by a *provisioning platform* and satisfy the individual needs and preference of a care-receiver. The detailed information on creating the service plan using the tailoring platform and executing these service plans by the provisioning platform are reported in our earlier works [19, 18].
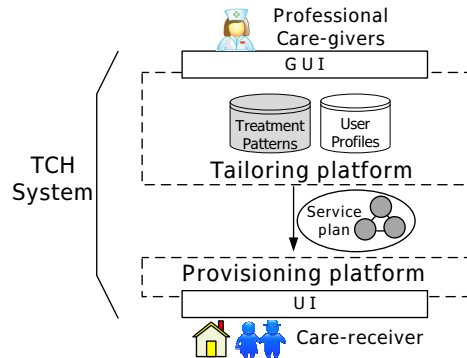

Fig. 1. A TCH system

By interviewing professional nurses we identified that high blood pressure is a common problem among elderly people. Thus we use the blood pressure example, to illustrate the functionality of TCH systems.

- Care-receivers should be reminded to attach the blood pressure measurement tool and measure the blood pressure themselves.

- If the care-receivers ignore the reminder for attaching the measurement tool, the second reminder should be sent after half an hour.
- The message, number of its repetition and the modality can be personalized based on individual requirements.
- If the measured value is high/low, the care-giver should be informed.

4   Risk Assessment

The type of the risks we are interested is caused by different stakeholders participating in the homecare domain. To analyse these risks, we begin with the identification of stakeholders in a homecare domain where care services are provided both with and without using the TCH system. Then we identify a list of possible risks in both situations, and their sources.

4.1   Identification of Stakeholders

The homecare domain is complex and involves various stakeholders with diverse interests (e.g., insurance companies, government, etc.). Excluding the stakeholders that fall outside the scope of the TCH system, we identified *care-givers*, *care-receivers* and *care centers* as three main types of stakeholders.

Anyone involved in providing care to the elderly (*care-receivers*), is considered a *care-giver*. Those who can provide care or interact with elderly include: professional nurses, informal care-givers and physicians. In this work, we consider only professional nurses as the care-givers, because: a) care-receivers spend most of their time with processional nurses while receiving care services in comparison to other care-givers, and b) Professional nurses are the main care-givers who interact with the TCH system to define service plans for care-receivers.

Care centers are institutions who pay for the care-givers and provide facilities to take care of the care-receivers. Care centers define medical protocols providing guidelines for taking care of care-receivers, which should comply with the national medical protocols defined by the government. When carrying out homecare tasks, care-givers must follow these medical protocols.

As shown in Fig. 2, after introduction of the TCH system, four new types of stakeholders appear in the homecare domain. These new types of stakeholders are *IT specialists*, *third-party service providers*, *infrastructure providers* and *hackers*.

An *IT specialist* is a person who can install, test, operate and maintain the TCH system. IT specialists are responsible for defining the treatment patterns based on existing medical protocols and care-givers recommendations and refining them based on operational experiences and test results. *Third-party service providers* own and manage services (such as blood pressure measurement, location determination and medication dispensing services) which can be used and composed by the TCH system to provide desired services to the care-receivers. These providers are located outside the care center and their services are accessible to other services through the Internet. *Infrastructure providers* are responsible for providing the necessary infra services to realise the TCH system such as the Internet and power supply. *Hackers* are individuals or organizations who break into the TCH system and its network and violate its function.
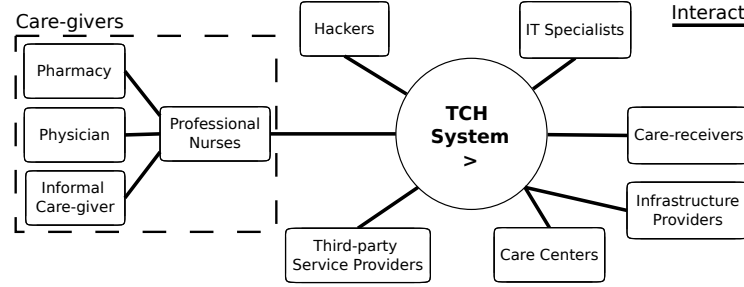
Fig. 2. A context diagram of a care center which is equipped with TCH system

4.2 List of Possible Risks

One of the benefits of a TCH system, compared to the current way of providing services, is the mitigation of existing risks that stakeholders, mainly care-receivers and care-givers, are already dealing with. We identify these existing risks and discuss whether the proposed TCH system can indeed mitigate them. We also identify new risks that might be introduced due to use of a TCH system.

Existing Risks We interviewed care-givers to identify the common tasks generally performed in the homecare domain. Based on the result of these interviews, we identified the risks in the current situation and determined whether these can possibly be decreased using a TCH system.

- **Forgetting to Treat Patients:** The care-givers usually follow a routine schedule in providing care services based on the medical protocols and doctors advice, for example measuring blood pressure every morning right after the care-receiver wakes up. However, it is likely that a care-giver forgets to measure blood pressure for a specific care-receiver or measures it late which might result in unreliable readings. A TCH system can be used to remind a care-receiver to attach the measurement tool whenever it is required.
- **Observation Error**: The care-givers give reports about the situation of the care-receivers to the doctors, family members, pharmacy, etc., based on which the authorised stakeholders take appropriate actions. For example, a doctor can prescribe new medication based on the current situation of the care-receivers, then the pharmacy can provide it, and the care-giver can give the medicine to the care-receivers. However, while measuring the care-receivers vital signs such as blood pressure, the care-givers can make mistakes in reading/writing of values, which can affect the diagnosis made by the doctor. A TCH system can automatically create a correct report based on the measured data which is accessible by a doctor.
- **Action Error**: The care-givers can make a mistake in providing care services to the care-receivers. For example, a care-giver can provide a wrong medicine to a care-receiver. A TCH system can be used to provide medication through a digital dispenser filled with medicine by a pharmacy based on doctor's prescription. We should take to account that there is still the possibility of the pharmacy making a mistake when filling the medicine dispenser.
- **Overlooking the Medical Protocols**: Nurses should follow the medical protocols in providing care services, and are examined yearly to prove that

they still recall them. However, a care-giver may overlook these protocols and make a wrong decision. A TCH system ensures the conformance of medical protocols, because those protocols are embodied in the treatment patterns.

– **Conflict in Medication/Treatment**: Care-receivers typically use multiple medications which are prescribed by different specialists. A doctor may prescribe a medicine without considering other prescribed medications that can have negative effects at other diseases/medicines. It is also common that for a specific disease, a doctors prescribes a new medicine, which has better effect, but without stopping the previously prescribed medicines. It is also possible to have conflict in treatment. For example, a care-receiver can use advise or treatment from different professionals, such as a family doctor, hospital doctor and physiotherapist, which may in itself be correct, but not optimal if used in combination. This risk can be easily detected by a TCH system, if there are predefined rules for conflicting medicines/treatments.

Risks of Using the TCH System One of the key motivations for replacing manual activities with automatic IT-based systems is *human error reduction*. However, many practical experiences shows that in reality, automation may produce new sources and types of errors [17]. This is also true when a TCH system is used in providing personalized IT-based homecare services. We identify the following risks for each stakeholder that interacts with the TCH system.

– **Care-givers:**

Wrong Configuration: Setting the wrong values for the configuration parameters, e.g., setting higher/lower values for the threshold of blood pressure.

Conflicting Service Plans: Creating conflicting service plans. An elderly usually suffer from a combination of diseases and hence, a care-giver may ignore the suggestion from the system and potentially create conflicting service plans for the same care-receiver. For example, in a service plan a care-receiver is asked to take his blood pressure at 8:00 AM while in another service plan he is asked to take a walk at the same time.

Missing Service Plan: Forgetting to create a service plan for a care-receiver.

Too Little Information: The face-to-face communication will be decreased, so care-giver's knowledge about care-receivers' situation will be limited.

– **Care-receivers:**

Cheating with the System: Lying to the system whenever a confirmation is needed, for example, a care-receiver may lie about taking the medicine.

Increased Loneliness: Feeling lonely is a common issue among elderly people. This could get worse by using a TCH system.

– **IT Specialists:**

Inappropriate Treatment Patterns: Translating the medical protocols to treatment patterns incorrectly or providing incomplete patterns. The possibility of occurring this risk is very low, because this a one-time activity (with minor changes per year) and the incompleteness or incorrectness of the patterns can be detected easily during a testing phase.

– **Third-party Service Providers:**

Service Failures: Services provided by the third-party service providers may not function or function improperly. These services such as the blood pressure measurement service are outside the control of TCH system.

– **Infrastructure Providers:**

Data/Power Network Failures: The data/power network may go down.

– **Hackers:**

Malicious Action: The care-receiver data or configured service plans may be altered/stolen. In fact, we do not consider hackers as new source of risk, since thieves can do the similar damage in the existing situation.

5   Discussion and Conclusions

Context-awareness is becoming an important aspect of any information system. We all can imagine what new features such a system can have: selection of fitting services and adapting system behavior and providing services tailored to users' needs and preferences. However, such a context-aware system can raise new risks because of unpredictable behavior. To the best of our knowledge, there is a limited amount of research and information regarding what new risks and challenges such a system can pose to its users. In this paper, we assume that the context-aware system can perceive and process context information accurately and in-time. In other words, we are only interested in undesired outcomes arising from the interaction of the user/services with a context-aware system.

In order to discuss the risks of TC systems, we need to clarify our understanding of context and context-awareness. In the literature, there are a number of definitions for context, however it is still difficult to say what information is context information and what is not. In this paper, we do not provide a new definition of context-awareness, but analyse context-aware systems and identify their potential risks. We consider context as any information that can be used to adapt the response of a system and add value to provided services for target users. A context-aware system mainly performs context-triggered actions in the form of 'If-then' rules to specify how the system should be adapted [13]. We discuss further the facts that can be generalised to any TC system.

5.1   What Can Go Wrong in TC Systems?

Since we are interested only in risks arising from the interaction with the tailorable context-aware system, to be able to generalize the identified risks, first we should identify the main type of stakeholders who interact with the system. We also discuss why they are the source of risks. Generalizing from our case study, four types of stakeholders interact with the tailorable context-aware systems:

Developer (IT specialists in the case study): Designs and implements the system. Because of lack of domain knowledge, the developer can be the source of risks. However, since a developer's action is not a frequent one, the impact of such a risk is relatively low. Once the risk is identified, it can be fixed and the probability of occurring the same risk again remains low.

Configurator (Care-givers in the case study): Has enough domain knowledge and configures the system parameters and creates new services to satisfy individual needs. Because of lack of IT knowledge, the configurator can be the source of risks. Since he uses the system frequently, the possibility of same risks occurring repetitively is high.

End-user (Care-receivers in the case study): Is a target user and benefits from the output of the system. Because of the lack of knowledge or interest about the system, the end-user can be the source of risks. Even though an end-user has higher rate of interaction with the system, since he usually performs the same type of actions (such as confirmation of receiving a message/service), possibility of same risks occurring repetitively is relatively low.

Third-party Service Provider (Third-party providers in the case study): Provides third-party services (services outside of the control of the system). Because of the lack of amenability, the third-party service provider can be a source of risks. Since his services have a higher rate of interaction with the system, the possibility of same risks occurring repetitively is relatively high.

Based on the fact that the *configurator* and *third-party service provider* are the main sources of risks, we limit the types of risks which are caused by them. Looking at the list of risks we identified for the homecare domain, in the following we generalize risks which can occur in any tailorable context-aware systems.

Wrong Configuration Values: This type of risks occurs due to the tailorability of the system. It is important to consider what can be tailored and what not. This risk happens when a user puts a configuration value which is not in the context model. For example, suppose that the location of a care-receiver is modeled as only *inside home* and *outside home*. A care-giver may insert a value *at park* as the location value. This type of risks can easily be prevented by limiting the possible configuration values, e.g., by checking the value against the model, decreasing the likelihood of this type of risk.

Conflict in a Task with Multiple Context Information: This type of risks occurs due to bad reasoning of the system regarding a task with multiple context information. The system should decide what to do based on context information, however there will be a conflict if there are two different actions for different context information. For example, a reminder should be sent to a care-receiver mobile phone when he is outside home and based on another reasoning he should not receive any reminder message on his phone when he is with somebody. So if he is outside home and is accompanied by somebody, there will be a conflict on sending the reminder message. Since this conflict occurs in one task (for example sending a reminder), a context-aware system can be designed in a way to detect such a conflicts and inform user in advance. This type of risks can be prevented by prioritizing the rules.

Conflict of Different Tasks: This type of risks occur because of performing different tasks which are in conflict. For example, one task is to attach a blood pressure measurement tool and the other task is to take a walk outside. Since this risk occurs in different tasks, it is difficult to detect and prevent it.

Third-parties Service Failure: Service Oriented Architecture (SOA) is becoming popular for designing IT-based systems. A SOA-based context-aware system may utilize services offered by different providers. There are usually Service Level Agreements (SLAs) among the partners to assure the availability of the services. However, in some domains like homecare, which is a safety critical domain, relying on the SLAs may not fully compensate the risks that occur.

The accountability aspects are mainly concerned with identifying the source of the risks and ultimately making that source responsible. Unlike in existing definitions, we treated the accountability as a means of identifying the source of risks (identifying where and how it can be fixed). This treatment is realistic because in the homecare domain, regardless of who is making a mistake, the care center is accountable for any risks that arise to its customers.

The risks due to wrong *configuration values* may lead to unavailability of desired services because the wrong configuration values may cause the system to behave differently. This kind of risk can also be classified as the accountability aspects, because the source of the risk can be traced back.

The risks due to *conflict of different tasks* and the *conflict in a task with multiple context information* may lead to providing undesired services, which can be considered as unavailability of the desired services. It might be difficult to exactly identify the source of risk and hence the accountability, because risk occurs when a newly created task conflicts with the existing one which might have been configured by a different configurator.

The risk due to *third-parties service failure* will lead to unavailability of desired services. The source of the risk can be identified only in terms of service providers, and accountability aspect should be considered in SLAs.

5.2   What More is Needed?

We have performed a first assessment of risks of TC systems in general, and of homecare systems in particular. This has led to a classification of *availability* and *accountability* risks. This is new regarding the current risk assessment literature of context-aware systems, which is mainly about security and privacy risks.

There are some limitations to this study. We have done only one case study and even in this study, we may not have found all available risks. We have interviewed the care-givers about the tasks they perform, and then identified the list of possible risks while they perform their tasks. However, there is a possibility that the interviewees have forgotten important tasks and accordingly important risks. Based on their explanation, we have listed possible risks and there is a possibility that those risks are not real risks. In other cases, other risks may exist too, that are not present in our investigated case. Despite these limitations, we can still claim that we have found a list of *possible* risks. We intend to do more case studies in the near future to identify the importance of the risks as well as the completeness and correctness of the list of identified risks.

Another aspect of future work is to further confirm and elaborate the risks that we found for homecare systems. In addition, we would like to extend this assessment towards requirements engineering, by incorporating the risk assessment as a first step in a requirements engineering process for homecare systems.

References

1. Amigo: Ambient intelligence for the networked home environment project (2008), available at: http://www.hitechprojects.com/euprojects/amigo
2. Baldauf, M., Dustdar, S., Rosenberg, F.: A Survey on Context-aware Systems. IJAHUC 2(4), 263–277 (2007)
3. Batet, M., et al.: Knowledge-driven Delivery of Home Care Services. JIIS pp. 1–36 (2010)
4. Bellotti, V., Edwards, K.: Intelligibility and Accountability: Human Considerations in Context Aware Systems. HCI 16, 193–212 (2001)
5. Duffus, J., Brown, S., Fernicola, N.: Glossary for Chemists of Terms Used in Toxicology. Intl. Union of Pure and Applied Chemistry 65, 2003–2122 (1993)
6. European Commission: Ageing well in the information society - an i2010 initiative - action plan on info. and comm. tech. and ageing. Tech. rep., EU (Jun 2007)
7. Hong, J., Suh, E., Kim, S.J.: Context-aware Systems: A Literature Review and Classification. Expert Syst. Appl. 36(4), 8509–8522 (2009)
8. Hussein, M., Han, J., Colman, A.: Context-Aware Adaptive Software Systems: A System-Context Relationships Oriented Survey. Tech. rep. (2010)
9. ISO: Risk management – principles and guidelines. Intl. Std. 31000 (2009)
10. ISO/IEC: IT – Security Techniques – Guidelines for the Management of IT Security – Part 1: Concepts and Models for IT Security. Intl. Std. 13335-1 (2004)
11. Korhonen, I., Parkka, J., Van Gils, M.: Health Monitoring in the Home of the Future. Engineering in Medicine and Biology Magazine, IEEE 22(3), 66 – 73 (2003)
12. Leveson, N.G.: Engineering a Safer World: Systems Thinking Applied to Safety, p. 4. To be published by MIT Press in Fall (2011)
13. Schilit, B., Adams, N., Want, R.: Context-aware Computing Applications. In: Workshop on Mobile Computing Systems and Applications. pp. 85 –90 (1994)
14. The Council of The European Union: Council Conclusions on a Safe and Efficient Healthcare through eHealth. In: Official Journal of EU (December 2009)
15. United Nations International Strategy for Disaster Reduction UN-ISDR: Terminology on disaster risk reduction. Geneva (May 2009)
16. White, C., et al.: Improving Healthcare Quality through Distributed Diagnosis and Home Healthcare. In: Transdisciplinary Conference on D2H2. pp. 168 –172 (2006)
17. Wiener, E.L.: Cockpit Automation. In: Human factors in aviation, Academic Press series in cognition and perception. pp. 433–461 (1988)
18. Zarghami, A., et al.: Dynamic Homecare Service Provisioning Architecture. In: IEEE Conf. on SOCA. pp. 213–220 (2011)
19. Zarifi Eslami, M., et al.: Flexible Homecare Application Personalization and Integration Using Pattern-based Service Tailoring. In: CIT. pp. 467 – 474 (2011)
20. Zarifi Eslami, M., van Sinderen, M.: Flexible Home Care Automation. In: IEEE 3rd Intl. Conf. on PervasiveHealth (2009)