Development of software for safety critical medical devices - an interview-based survey of state of practice

Lindholm, Christin; Höst, Martin

2008

Development of Software for Safety Critical Medical Devices - an Interview-Based Survey of State of Practice

Christin Lindholm
Department of Computer Science
Lund University
Box 118, 221 00 Lund
Sweden
+46 42 35 67 46
christin.lindholm@cs.lth.se

Martin Höst
Department of Computer Science
Lund University
Box 118, 221 00 Lund
Sweden
+46 46 222 90 16
martin.host@cs.lth.se

ABSTRACT

To be able to survive in the long run the medical device industry of today needs effective development processes and ways to secure quality. These development processes and quality assurance processes must follow the different laws and regulations over the world depending on what market the organisations are established on. Organisations have been developing medical devices and systems over many years but now this type of products contain more and more software. The development of software is often appended in to the existing development and quality assurance processes and these processes may not be the most efficient and correct processes when it comes to software.

This paper presents the results from an interview study with the purpose to survey how the medical device companies work today, what development processes and quality assurance techniques they use and how laws and regulations affect their way of working. Safety is very essential for the medical device organisations and all the interviewed organisations consider the software in their medical device as safety critical. Risk and risk analysis is an important part of the safety thinking and is frequently performed by the organisations. However established and systematic techniques to analyse risks of the medical devices are not so frequently used as expected.

The intension is that the results from the study could be used as a help to find more adapted processes and techniques for software development in the medical device domain. The results have also been used to derive a set of requirements on new techniques and methods in the area. The derived requirements can serve as guidance to researchers aiming at improving processes, methods and techniques in the medical device domain.

Keywords

Interview-based survey, software, safety critical medical devices, quality assurance, standards, risks analysis.

1. INTRODUCTION

Quality requirements on medical systems and devices are high. If they do not work as intended, e.g. because of errors committed in the development process, it may result in threatening of human lives. The high requirements in combination with the high complexity of this kind of systems make quality assurance procedures during development crucial.

A large and growing share of the development effort of this kind of systems is devoted to development of software. An increasing part of the functionality is implemented in software and many new features of these systems would not be possible to implement without software. This means that the requirements of the software development process are as high as for development of other parts of the systems. Important quality attributes of software include, for example, inclusion of correct functionality, reliability with respect to fault content, usability for all users, and maintainability for software engineers in continued evolution of the product [1]. A failure to comply with the high requirements on any of these quality aspects may in time result in serious failures in operation.

Development of software differs to some extent to development of other engineering domains [2]. Software is abstract and "intangible" for managers and others which means that it is hard to envision the current quality, e.g. during development and testing. Software is also easier to change than many other entities. This gives, of course, flexibility during development, but it also puts high requirements on quality assurance during development. Software is also of very high complexity and it is hard to develop fault free software in general. This means that it is an important aspect in development of medical devices where software is only one part of the product, and where there are high quality requirements.

The software that runs a medical device or affects the use of a medical device automatically belongs to the same safety classification as the medical device [3] and has to follow the same laws and regulations as the rest of the medical device. It is important to notice that it is the manufacturer's purpose and the operation of the product that decides if the product is classified as a medical device, not the designer or the user. The laws and regulations state that the medical device organisations must have quality systems and that the quality system and the quality improvement actions must be documented. The quality system must cover the whole development process including the software development process and focus on the aspects and requirements to produce and provide safe and effective devices. The typical procedure for quality assurances of software is through the application of a structured development process (e.g. as described in [4]). Due to the high requirement, e.g. on safety of medical devices, it is of interest to investigate what quality assurance

procedures, development processes that are used in development of software for medical devices. It is also of interest to investigate closer what the driving sources are for quality assurance and process improvement in the area.

The outline of the paper is as follows. In Section 2 background and related work with definition of medical device and a short description of laws and regulations in the area. In Section 3 the research questions and the research method are presented. The results are presented in Section 4, discussed in Section 5 and in Section 6 requirements on processes and methods for the medical device domain is presented. Finally, the conclusions are presented in Section 7.

2. BACKGROUND AND RELATED WORK

The term "medical device" is defined according to law in many countries. For example in the Swedish law (1993:584) [5] about medical devices the term is defined with the following definition: "Medical device" means any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, investigation, replacement or modification of the anatomy or of a physiological process*
- *control of conception*

Medical devices for the European market are regulated by Council Directive 93/42/EEC concerning medical devices (MDD) [3]. In the US the regulatory body of the Food and Drug Administration (FDA) [6] must approve medical devices. A medical device has to go through one or two evaluation processes, premarket notification (510(k)) or premarket approval (PMA) [7]. Every Member state in the EU must adopt and publish laws, regulations and administrative provisions to implement the Directive [3]. There are some variations in national requirements, most of these concerns the need to notify the Competent Authorities when medical devices are placed on the market in their countries. There are different laws, legislations and a duplication of registration procedures for a medical device placed on the US market and the European market even if it is the same medical device.

According to the MDD [3], medical devices in EU are divided into four classes Class I, IIa, IIb and III based on the level of control necessary to assure safety and effectiveness. Class III is reserved for the most critical devices. The classification in the U.S. differs and they have three different classes, named FDA Class I, FDA Class II and FDA Class III. The software that runs a medical device or affects the use of a device for example surveillance the medical device automatically belongs to the same class as the device. The classification are build up on the risks the human body can be exposed to due to the design, the use or the mode of manufacture of the medical device. It is assigned to the manufacturers, based on the regulations to establish in which class the medical device belongs and after that establish which procedure to apply to ensure that all the demands in the regulations are met. The manufacturer carries out the classification of the devices, possibly in cooperation with a Notified Body (third part assessment).

Medical healthcare is one of the traditional areas considered as safety critical according to Knight [8] and he defines safety criticality as "Safety-critical systems are those systems whose failure could result in loss of life, significant property damage or damage to the environment". Embedded systems have increasingly become predominant in a rage of safety critical applications for example in medicine, nuclear power plants, aviation and aerospace industries [9]. According to Hewett and Seker [9] other safety critical industries as well as medical device industries mandate certification for the code and its development process to assure quality of the system. The certification process is a highly labour activity and the cost for developing a safety critical software system is reported by Nilsen [10] to be 20 to 30 times the cost of developing typical management information software.

Risk management is according to Doernemann [11] highly accepted in safety critical industries as for example aerospace and healthcare but more and more branches see the value or establishing risk management processes. In a recent article Rakitin [12] states that it is the medical device companies that must show that their software is safe and efficient. He means that for the companies to meet these responsibilities it is required of the companies to have expertise in effective risk management practices, to be familiar with software safety and to be able to adopt risk management mind set. Prakash et al [13] have examined requirements engineering process practices in three multinational pharmaceutical and healthcare companies and found large differences in the processes used between the companies in the development and that none of the projects followed the recommended best practice.

How FDA´s laws and regulations can affect the development of software for medical devices are for example discussed by Branningan [14] where the effects of the "Safe medical device act of 1990" (replaced by Federal Food, Drug and Cosmetic Act in 1995) on non-embedded software is discussed. To the best of our knowledge the effects of European or Swedish laws and regulations on the development of software for medical devices has not prior been systematically analysed so in 2006 a survey was done by the authors of this article together with the Fraunhofer Institute for Experimental Software Engineering in Germany and the Fraunhofer Center in Maryland, USA [15]. The main objective of the survey was to characterise the state of the practice of software development in the context of medical devices. The survey was carried out through a web-designed questionnaire and the study presented in this paper is based on interviews with special focus in special areas such as quality, standards and risk analysis.

3. INTERVIEW RESEARCH METHODS

This section describes the interview study, the objectives for the study, the interview planning, the operation as well as the analysis and validity threats.

3.1 Objective

The objective of the research presented in this paper is to try to investigate how the medical device companies works today, what development processes and quality assurance techniques they use

and how laws and regulations affect their way of working. More specifically, the objectives are as follows:

- To examine what type of products the organisations develop and for what market. This question is meant to provide background knowledge that is important when the answers to the other questions are interpreted.
- To understand the role of software in medical device and to investigate to what extent the organisations regards and treats it as safety critical.
- To investigate what standards and techniques that is used by organisations that develop safety critical medical devices and how laws and regulations affect the work.
- To investigate how the organisations guarantee the quality of the software in the medical devices.
- To investigate how requirements are handled and the use of risk analyses.
- To derive requirements that can serve as guidance to researchers aiming to improve processes, methods and techniques in the medical device area

The objectives are investigated in an interview study containing interviews with eight development sites in Sweden. The last objective arises during the analysis of the interview answers when the need of requirements on techniques, methods and processes was identified based on the answers.

3.2 Method

The research in this interview study can be described as flexible according to Robson [16]. Flexible design allows the high-level research questions to be specified in advance but it also allows the study to develop. With a flexible design, a common way of collecting data is to carry out interviews. According to Lethbridge [17] interviews are inquisitive first-degree (direct involvement of software engineers) techniques that allow the researcher to obtain a general understanding of the software engineering process. Since the overall objectives for this study is to get a good general understanding of the role of software and software engineering processes in the medical device industry are interviews suitable form for the study. They are flexible and allow the researcher to clarify questions. Another advantage is that people are familiar with answering questions and often the participants enjoy the opportunity to answerer questions about their work.

The interview questions are open-end questions written to cover the objectives of this study and the interviews are based on an open dialogue between the researcher and the respondent. Each interview took between half an hour and forty-five minutes depending o the extent of the answers from the respondent.

There are twelve main questions areas the interview questions try to cover and these question areas are:

1. **The organisations.** Information about the organisations' background and products.
2. **Software**. Information about the use of software, safety criticality, development process, platforms etc
3. **Quality and standards**. Information about quality systems, quality assurance, use of standards, reviews, test etc.
4. **Law and regulations** Information about the laws and regulations the companies has to adjust to, classification and CE-mark.
5. **Requirements and risk analysis**. Information about the requirement process and risk analysis.
6. **Challenges** pointed out by the persons interviewed.
7. **Problems** described by the interviewed persons
8. **Verification** how it is done for the whole product and the verification of the safety critical parts.
9. **Statements**, interesting statements connected to some of the questions from the interviewed persons.
10. **Validation**, how the validation process looks like for the different companies.
11. **Traceability**, how requirements are traced during the development process.
12. **Observation**, cause and effect expressed during the interviews.

These question areas are the same areas as the twelve main categories used in the analysis phase.

The interview question document has been updated over time. The first version of questions was put to the three first interviewed organisations and then some questions was removed and added according to Table 1. Removed and added question on subject relate to what subject the question covered.

Table 1. History of interview questions

Question document	Nr of org.	Removed question on subject	Added question on subject
1:st version	3		
2:nd version	1	Product year?	Dev. process Risk analysis Clinical test
3:rd version	4		ISO 13485 standard

After the interviews, the material was transcribed and pieces of text were labelled with predefined factors. The text pieces were sorted after predefined factor and codes (keywords) were derived from the text according to each factor. A factor can consist of several codes for example factor Standard consist of the codes that are names of the different used standards ISO 9001, ISO 13485 etc. The material was then analysed by two researchers described in chapter 3.4

When the analysis of the interview answers was conducted a need for requirements on techniques, methods and processes was identified. The requirements were identified in three different areas: a) process, b) quality system and c) validation, methods, techniques. The requirements were identified in the interview answers, then specified and the cause for the different requirements was explained. After the specification of the requirements was conducted, the requirements were checked against the interview answers in order to assure that all requirements are grounded in the collected data. The requirements are presented in section 6.

3.3 Interview subjects and context

This interview study contains interviews with eight development sites in Sweden. The organisations were chosen in order to obtain valid sample and geographical vicinity. One of the organisations' devices does not contain software but is used for comparison, to investigate similarities or differences. Many safety critical

medical devices on the Swedish market are not developed in Sweden, just manufactured and this limits the suitable selection of organisations for the interview study.

The preparation of the interview questions was made by the researcher (the first authors of this article) with the intention to cover the objectives of the study. According to Robson [16] there are different types and styles of interviews and a commonly made distinction is based on the degree of structure or standardisation of the interview. The three types are fully structured interview, semi-structured interview and unstructured interview. In this case the semi-structured interview form was chosen, considered a suitable form since it is an early study and a respondent interview study. It is important to be able to update the interview questions according to the interviews and to get flexibility. A semi-structured interview has predetermined questions but the order of the questions can be modified based on what is most appropriate during the interview. It is also possible to add more questions, omit inappropriate questions, change question wording and give explanations.

All interviews were face-to-face interviews carried out in Swedish by the same interviewer. One person was interviewed from each organisation and it was one person interviewed at the time. All the interviews were recorded and then transferred to computer. The technique provides a permanent record and allows the interviewer to fully concentrate on the interview. The interviews were held at the respective organisation and the persons that were interviewed worked as quality assurance manager, clinical affairs manager, strategy manager, development or technical manager. The interview questions were updated twice (see Table 1) but there were no significant changes made to the original questions. However, a couple of new questions were added about development processes, risk analysis and clinical test, and one question about the product was removed.

3.4 Interview analysis

Data reduction is a part of the analysis and denotes a systematic way of selecting information for the continued analysis and also simplifies and abstract raw data. The next step is to find summarising word or symbols for a segment of words and in some way code the material without the sense getting lost. The interviews were then fully transcribed to text format before the analysis was done. The researchers specified thirty-four predefined factors before data was collected from the interviews. The predefined factors were derived from the interview questions and were for example development process, class and standard. The data collected from the interviews was then reduced to remove irrelevant information and the text was labelled with the predefined factors. One of the interviews was labelled with the predefined factors individually by the two authors of this article and then the result was compared to see that the labelling not diverted too much which it did not do. The predefined factors were organised in twelve main categories to systemise the factors so a category contain several factors. These twelve main categories are as mentioned the same as the twelve question areas presented in section 3.3.

The factors and codes were then put together in a matrix. The matrix was constructed with the predefined factors in the column (in Table 2. Dev. Process, Class and Standard) and one row containing codes (in Table 2. for example V-model, III, ISO 9001) for each interviewed subject.

Table 2. Example of matrix data

Org.	Dev. Process	Class	Standard
1	V-model	III	ISO 9001
2	Own model similar V-model	IIb	ISO 13485

The constructing of matrix was done the first time after the first four interviews and the second time was after all eight interviews were made. The second round of factor was similar to the first round but was extended with some more factors to make sure that no meaningful material was overlooked.
The matrix was then analysed and discussed by the two researchers, and the results for each factor in the matrix were written down. The codes and parts of the interviews were reviewed again before conclusions were drawn.

3.5 Validity

Validity can according to Yin [18] be classified in construct validity, internal validity, external validity and reliability. Construct validity is affected by how correct the colleted operational measures represent the concepts studied by the researcher. There is a risk that the interviewer and the interviewee interpret terms or concepts different. To reduce this risk, the interviewer explained concepts as for example “quality plan” and “inspections” during the interview. Another risk in this study is that the interviews were only preformed by one researcher but this risk was reduced since all the interviews were recoded.
Internal validity is affected by factors that are outside the control of the researcher but affects the measures. A threat to this study could be to establish incorrect causal relationships when we analyse relations between different interview responses. However, in this study no conclusions about causal relationships are drawn, only relationships between factors were analysed.

External validity concerns the problem of how general findings are with respect to the subject population and beyond the immediate study. The result from this study is based on interviews with a limited numbers of subjects from a limited number of organisations, so it should be regarded upon as an exploratory study and further studies are needed in this area.

The validity is also affected by the reliability, how well described procedures are followed and documented so that the study can be repeated in the same way again. The goal is also to minimize the errors and biases in a study. In this study we have tried to minimize threats by recording the interviews and then fully transcribe them. The procedures and all changes to the study over time have been closely documented in a special document so that the study procedure can be reflected on and repeated in the same way again. In order to reduce researcher bias, one of the interviews was categorised and classified by two researchers individually in parallel, and the results were compared to verify that the results did not differ too much. The analysis of the results was also made the two researchers. A threat in this study can be participant’s bias, if the interviewees have deliberately answered incorrectly, for example to given a more positive picture of their way of working or their organisation.

4. RESULTS

4.1 The background of the organisations

Eight organisations took part in this interview study. Four of the organisations are multinational companies with a branch of the organisations in Sweden and the rest of the organisations are located only in Sweden. The organisations vary in size from a couple of hundred to a couple of thousand employees. The medical devices are mainly embedded, real time systems containing software. The devices supplied are various surgical equipment, equipment for microwave thermotherapy, analytic instruments, cardiac and respiratory equipment, sterilisation equipment and modifications of patient management systems. For all the medical device systems, they are indented for continuous use for not more than 30 days per occasion and so according to MDD [3] definitions they are short-term medical devices. The medical devices are mainly used by experienced personal that frequently use the medical devices but have no deeper technical knowledge. The users are mainly physicians but in most case (six out of eight) other personnel in the health care sector, e.g. nurses are also users of the medical devices. The organisations' main customers are hospitals and some private medical clinics all over the world. In most cases the devices are procured by departments with procurement responsibilities, which means that the customer are often not the same as the users of the medical devices.

The development processes used by the organisations differ. The answers given of the organisations are presented in Table 3 where "Org." represents the eight different organisations and "A. Dev. Process whole product" is the development the organisation states that they use for the development process for the whole product and "B. Dev. Process software is the development process" stated for the development of the software.

Table 3. Development processes

Org.	A. Dev. Process whole product	B. Dev. Process software
1	V-model	CAPA process
2	V-model	V-model
3	Design and control	Design and control
4	Own model - similar to V-model	QSR quality system
5	V-model (modified)	No software
6	GAMP4	GAMP4
7	*No answer*	*No answer*
8	*No answer*	*No answer*

The V-model mentioned as a modified V-model is a variant of the basic V-model with product specifications and standards for type tests and environment tests influenced by the Swedish defence industry. One of the respondents states the use of an own model but describes it very similar to the V-model. It can be noticed that three of the organisations have the same development process for both the software development process and the development process for the whole medical device.

Two of the respondents chose to not state their choice of development process at all and one of the organisations' devices does not contain software but is used in this study for comparison, to investigate similarities or differences, however in respect to development process, standards and quality assurance. No differences were how ever found according to organisations with medical devices containing software.

4.2 Software

All the organisations consider the software in their medical device a safety critical and this corresponds well to the classifications of the medical devices according to MDD [3]. The software that belongs to a medical device is classified in the same class as the medical device and based on the level of control necessary to assure safety and effectiveness a device is assigned to a regulatory class where devices in Class IIa has a high risk potential and Class IIb has an even higher risk potential (Class III are the class for the most critical devices). The software in this study is classified in Class IIa or Class IIb. Since the software belongs to the medical device it is also included in the CE labelling. All the organisations medical devices are labelled with the CE-mark, otherwise the organisations are not able to manufacture the medical devices on the EU market. The software in the study is used in different types of systems for example control systems, automation systems, safety systems and information systems and the software is used for example for control, regulation, registration, navigation and protection. When it comes to developing the software three of the organisations develop their own software, one of the companies only uses software from suppliers and three of the companies both develop their own software and use software from suppliers.

It was difficult to get information from the interviewees about the programming languages and platforms used by the organisation. Either the interviewees did not possess the information or they did not want to share this type of information. However three organisations uses C++ but the same organisations also uses other programming languages for example C, C#, PCL. Three interviewees stated that their organisation uses PC platforms and there were no answer to this question by the rest. But some interesting remarks were made by the interviewees according to platforms and programming languages. One of the interviewees stated, "I think it will take a while before our customers accept PC based code" and another one of them means that C++ is on its way out and is replaced with C# and .NET platforms instead.

As presented in Table 3 the organisations follow different development processes for their software, and the processes stated are the V-model, Design Control, CAPA process (Corrective Action and Prevented Action), QSR quality system and GAMP4. The V-model is a traditional development process and one of the interviewees motivated the use of the process with "because it is easy to repeat and to describe". GAMP4 is a guide for validation of automated systems and medical devices. It focuses on for example risk assessment, design reviews and traceability. CAPA is a process for existing products problems, customer complains etc and also a process for detecting potential problems. The process also includes risk assessment of the problems. Both FDA and ISO require an active CAPA process as an essential element of a quality system. Quality system regulation (QSR) is an American law for medical devices and corresponds to the

international quality standard ISO 13485, but they differ on a detailed level. Design Control is a major subsystem to QSR and its purpose is to assure that devices meet user needs, intended use and specified requirements. It focuses for example on design review, design verification and design validation. The similarities between the processes are that they are all managed processes with focus on risk assessment, validation and design reviews.

4.3 Quality and standards

All the interviewed organisations have quality systems, a system of regulations and methods for how the work with quality assurance and quality management is carried out in an organisation. The laws and regulations state that the medical device organisations must document their quality systems and also document all the quality improvements made over time. The quality system must cover the whole development process and focus on the aspects and requirements to produce and provide safe and effective devices. To be able to CE-mark a device it is also required of the organisations to have some form of quality management system.

The organisations follow different standards and an organisation can often follow several different standards. The majority of the organisations in the study have stated that they follow more than one standard and this explains total number of organisations in Figure 1.

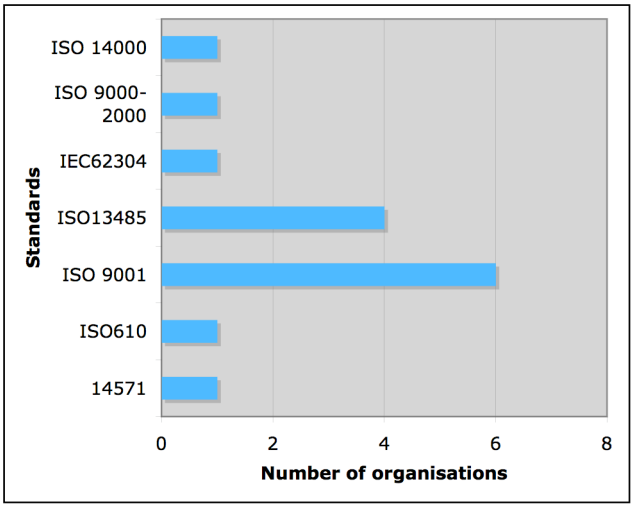

Figure 1. Standards in use

As shown in Figure 1 the dominant standards used are ISO 9001 and ISO 13485. ISO 9001 is a quality system standard applicable to many kinds of industries where as ISO 13485 is a standard specific to medical device quality systems, which is especially developed to harmonise with constitutional requirements and is also a supplement to the ISO 9001 standard. Some of the additional requirements in ISO 13485 compared to ISO 9001 relate to design controls, process controls, traceability and regulatory actions, which are more critical for the medical device industry. All the organisations work with quality in some way, for example with quality plans, manuals and quality systems. According to standards, the organisations have to work with quality improvement and focusing on the customers, which means that management shall guarantee that the customers' requirements are established and fulfilled. One of the organisations with medical devices on the US market is working according to Quality system regulation and this process covers design, production, servicing and corrective/preventive (CAPA) activities.

That the organisations according to the standards must focus on the customer is something the organisations are well aware about. They work, for example, with user feedback, measuring change orders, forms for quality remarks and complaints, post market meetings, and incident handling. Looking at different quality assurance techniques, the organisations have, for example, different kinds of internal inspections. Most common are reviews of requirements specifications, design reviews and code reviews. Similarities found are that the same person who has written the documents or the code does not make the reviews. The reviews are usually carried out without tool support. One of the interviewees states that reviews are "a cultural matter and are experienced as trespassing on the personal work". According to ISO 13485 and ISO 9001 the organisation must review the product requirements before they make a commitment to provide the product to the customer. American law states that design reviews must be conducted and in the FDA guidelines for software code reviews are recommended.

The organisations' quality systems and quality improvements documentation are inspected at external inspections conducted by a Notified Body (third part). All the organisations develop devices that are classified in Class IIa or IIb, so a Notified Body must assess them. Three of the organisations also have external inspections carried out by experts from FDA.

The organisations state that they do verification, for example verification of requirements, verification against standards, pilot study, or evaluation of performance. One organisation also describes that they start with code review, then conduct unit testing, followed by integration testing, and last system testing. According to standards and regulations, verification shall be conducted in a way that the organisation secure that the requirements are fulfilled and so the documentation of the verification is preserved.

When it comes to validation it is also regulated in standards and by FDA´s Quality system regulation and guidelines. The validation shall secure that devices fulfil the requirements for intended use. As a part of the validation of the development results shall the organisation do clinical evaluation and/or evaluation of performance. Also the documentation of the validation must be preserved and validation must be done before delivery or use of the device. Four organisations state that they have validation, the rest of the organisations ought to have validations according to regulations but they chose to not comment on the questions about validation given during the interview. One of the organisations has usability studies, a special usability group and a special validation group. They also attempt to use human factors and to get early feedback from the end users.

4.4 Requirement engineering and risk analysis

Requirement engineering is an important area for the organisations and the sources where the requirements are collected from are standards, laws, users, vendors and sales departments. A problem mentioned by an interviewee is that "we engineers do not always understand what the sales-department means and they do not always understand what we mean". It is stated in standards and regulations that the organisations must establish requirements from customers, including requirements

concerning delivery. The organisations must also establish that the constitutional requirements for the device are covered in the requirement specification.

The organisations using the V-model state the requirement engineering is carried out as part of the model, starting out with a requirements specification with user and marketing requirements. This specification is then broken down in one or several technical requirements specifications. A few of the organisations treat safety critical requirements different than non-safety critical requirements ad this means that safety critical requirements are traced more thoroughly though the development process, from requirement to design to code to verification and validation and backwards.

Top priority for all organisations is the safety of the medical devices. All the organisations state that they make risk analysis on a regular basis and this is exactly according to the regulations which state that such a process must be executed and the results must be documented. The organisations do the risk analysis in different areas such as development, production, problems, users and risk analysis if changes are made. One of the organisations follows for example ISO 14971. This standard describes that continual control of the final residual risks shall be done. The risk is evaluated, the risk level is updated and corrective measures are taken to reduce the remaining risk. Risk management reviews are also done where all available data about the risks are collected to control the risk level. Risk analysis can be performed by using different techniques such as for example HazOp [19], Failure Modes and Effects Analysis (FMEA) [20] and Fault Tree Analysis (FTA) [21]. These risk analysis techniques are suitable for identifying risk during development of medical devices and are recommended by different standards. HazOp and FTA are more suitable for systems and software whereas FMEA is more suitable for components. Two of the organisations state that they use FMEA and one that they use FTA. The other organisations do risk analysis, but they have not specified any special risk analysis technique. One of the organisations, however, mentioned that it has worked with so called “emergency plans”, ready to use if a risk should appear.

5. DISCUSSION

For many of the organisations it is seen as a problem that the laws and regulations are different in different parts of the world. It had for example been an advantage for all organisations of medical devices if the laws and regulations were the same over the whole world and no duplication of registration procedures and many external inspections of different third part were needed. The Global Harmonization Task Force[1] (GHTF) is a voluntary group of representatives from national medical device regulatory authorities and the regulated industry working towards harmonisation in medical device regulations.

Laws, regulations and standards affect the organisations’ way of working and the processes used are at a large extent managed. The development of software is often appended in to the existing development and quality assurance processes and these processes may not be the most efficient and right processes when it comes to software. Maybe the organisations should benefit more from tailor made development processes for the medical device domain with focus on correct functionality, reliability, safety, risk assessment usability and other important areas for the domain.

The dominant standards used in the interviewed organisations are the ISO 9001 and ISO 13485. According to the survey focusing on software engineering techniques used in medical device industry [15] ISO 13485 is also stated as one the most frequent used (53%) standard. A probable reason for this is that the standard is specific for medical device quality systems and it is also especially produced to harmonise with constitutional requirements. Maybe more organisations should be guided and helped to change to ISO 13485 and this standard should be well incorporated in tailor made development processes.

Quality assurance is one of the major areas that are dealt with in laws and standards and in the context of quality assurance it was found that inspections are frequently performed but it is was not cleared during the interview how they were done (checklists, reading techniques, ad hoc etc). It should be possible to find and recommend quality assurance techniques that are especially suitable for the medical device organisations. When it comes to risk analysis it is also frequently performed by the organisations however some of the organisations do not use established and systematic techniques as HazOp or FMEA to analyse the risks of the medical devices. A reason for that is may be that is too much effort to use these techniques in relation to the safety risk. It was not mentioned during the interviews how the manufacturers actually prove that their medical devices are safe. It would be interesting to investigate the real reason why systematic techniques are not used and based on the results maybe tailor make a technique that fits the organisation’s way of working, are easy to use, cost effective and adapted to what are requested by laws and regulation.

The interviewed persons stated that the software is safety critical work on management level in the organisations as for example quality assurance manager, clinical affairs manager, strategy manager, development or technical manager and they are well aware of the classification of the medical device, maybe the developers have another opinion regarding the software. In the previously conducted survey [15] there were participants that did not consider their medical device as safety critical even if the classification indicated the opposite. The reason can be that the participant’s apprehend the part of the medical device he/she is working with not to be safety critical and this maybe effect the way of working.

Only one of the organisations procure all their software from third part and one organisation pointed out that use of third part software increases and this is also a trend seen among developing organisations in other areas [22]. The question is how the use of third part software affects the organisations way of working with quality assurance, can the organisations guarantee that laws, regulations, standards and work procedures are followed, how the inspections shall be done and who has the responsibility.

6. REQUIREMENTS ON DEVELOPED TECHNIQUES AND PROCESSES

Software process improvement is, as in other fields, important in development of medical systems. However, there are a number of important issues to think about when new procedures, processes, techniques and methods are developed in every domain. Based on

[1] http://www.ghtf.org/

the findings from the interview studies we have identified a number of requirements on techniques and processes, which are intended to be used in software development of medical systems. The requirements are presented in table 5-6 below. These requirements can serve as guidance to, for example, researchers aiming at developing methods that are used in this domain.

The requirements are divided into requirements on process level, requirements on quality systems and requirements on individual techniques.

The development process and other processes over time for example the document process; quality assurance process and validation process must fulfil these two key requirements for medical device organisations found in Table 4.

Table 4. Requirements for processes

PROCESS	
Requirements	**Cause**
1) Must fulfil laws in different countries	Medical devices that are marketed in several countries have to be inspected and obey the law in these different countries
2) Must be designed to be able to fulfil several different standards	A medical device organisation are often certified according to several different standards

The two requirements in Table 4 have been derived from the interviews in this study where the organisations state that they have to follow different laws according to the different countries they are marketed in and that they are certified according to several different standards. Most of the interviewed medical device organisations state that they are certified according to three to five different standards. Since these two requirements are key requirements they will also be found in Table 5 and 6.

Many of the development processes used by the interviewed medical device organisation focus on quality, risk, validation traceability and design control. These areas can be found in Table 5 and Table 6 as requirements if for example a new quality system, validations process or a new method or technique should be developed. Example of new methods or techniques could be a new quality assurance method or a new risk analysis technique.

Table 5. Requirements for quality system

QUALITY SYSTEM	
Requirements	**Cause**
1) Must fulfil laws in different countries	Medical devices that are marketed in several countries have to be inspected and obey the law in these different countries
2) Must be designed to be able to fulfil several different standards	A medical device organisation are often certified according to several different standards
3) Must cover the whole development process	The whole development process must be covered by the quality system according to law
4) Must be documented	All the quality assurance activities must be documented according to law
5) Quality improvements over time must be documented	According to law and standards the medical device organisations must document all quality improvements.
6) Must have focus on producing safe and effective medical devices	Safety and efficiency are key areas for the medical device organisations
7) Must include design control	According to law the medical device organisations must have design control that are an interrelated set of practices and procedures that are incorporated into the design and development process
8) Must include process control	According to standards the medical device organisation must monitor, measure and analyse processes
9) Must secure that the customers requirements are established and fulfilled	According to standards it is the top management of the medical device organisations that have the responsibility to secure the customers requirements.
10) Must include procedures for risk analysis	All medical device organisations must perform risk analysis according to law
11) Must have traceability for example from requirements to design to development to product and backwards	All quality activities must be able to trace during to whole development process according to law.
12) Must be available in a inspectable format for third part	Most of the medical device organisations quality systems are inspected by Notify Body

The requirements in Table 5 and Table 6 are derived from both laws and regulations and from the interviews made by the medical device organisations. All the organisations pointed out that the laws and standards really affect their way of working very much. They have to have these standards and laws in mind in every thing they do.

In the interviews it appeared, for example, discussions about focus on customer, safety and risks. It was stated that the organisations focus more and more on the customers and users in different

ways. This seems to be a relatively new issue for the organisations but an area they have to work with according to standards.

All the medical devices in the study are classified according to the MDD [3] and/or FDA [6] as safety critical and all the organisations state in the interviews that they consider the software in their medical devices as safety critical. All the organisation point out that they focus on safety and that safety is a very important area for this type of organisation.

All interviewed organisations do risk analysis on a regularly basis and also in this area different processes and standards effects the organisations way of working and this fact is very obvious to them.

Table 6. Requirements for validation, methods and techniques

VALIDATION, METHODS AND TECHNIQUES	
Requirements	**Cause**
1) Must fulfil laws in different countries	Medical devices that are marketed in several countries have to be inspected and obey the law in these different countries
2) Must be designed to be able to fulfil several different standards	A medical device organisation are often certified according to several different standards
3) Must be carried out before delivery or use	Validation and risk analysis must be done before delivery or use
4) Must be documented	All validation and use of methods and techniques must be documented according to law
5) Must have clinical evaluation and/or evaluation of performance for the whole product including software	All medical device organisations must evaluate performance and/or do clinical evaluation

Since systematic techniques and tool not seems to be used as widely in the domain as could be expected this requirements above can hopefully be a help in the process of developing such techniques and tools.

7. CONCLUSION

There are no global laws and regulations so the developers and manufactures of medical devices have many different rules, laws, regulations and standards to adjust to depending on what market they are interested in. This leads for example to duplication of registration procedures, which takes a lot of effort, and that external inspections of more than one third part are needed. It had been facilitated for all developers and manufacturers of medical devices, if the laws and regulations were the same over the whole world and no duplication of registration procedures and many external inspections of different third part were needed.

The medical devices are often short term embedded systems, defined as normally indented for continuous use for not more than 30 days, this by MDD [3] labelled with the CE-mark and classified according to MDD in Class IIa or IIb. The developing organisations consider their software to be safety critical and this corresponds well to the classifications of the medical devices according to MDD. All the organisations follow development processes for their software; they have for example the V-model, and Design Control but it could be possible to design special development processes, especially adapted to handle the difficulties of developing medical devices and also a development process that fulfils the requirements from laws and regulations.

In accordance with available laws and regulations all organisations have quality systems. They are all certified according to ISO standards such as ISO 9001, ISO 13485. ISO 13485 is a standard specific to medical device quality systems where as ISO 9001 is quality system standards applicable to many kinds of industries. According to the standards the organisations have to work with quality improvement and focus on the customers. The organisations do that by, for example, working with user feedback, classification of problems, and special forms for quality remarks and complaints. To guarantee the quality they have internal inspections of the requirements or the quality system. They have reviews of requirements specification, design reviews and reviews of their quality system. A Notified body also performs external inspections of the quality system documentation on regular bases. As part of the quality assessment process the organisations do risk analysis and they are oblige to do so according to law. The used risk analysis techniques differ between the organisation and the area in which the risk analysis is performed differs from organisation to organisations. The organisations are very eager to follow the law so risk analysis is frequently performed but it is a little bit surprising to notice that some or the organisations do not use established and systematic techniques as for example HazOp and FMEA to analyse the risk of the medical devices, not in that extent as it is expected.

This interview study is an exploratory study. The objective has been to try to get an understanding of the organisations developing safety critical medical devices containing software and their developing and quality processes. The medical device organisations have to focus more on safety and risks than other kind of industries and they are at a large extent managed by laws and regulations, this taken together makes the requirements on the development process for the medical devices more specific and more work can be done in this area to help the organisations.

Some areas of special interest have been found were improvements can be made. These findings could lead to further research in the quality, process and risk areas that in the end could give the medical device organisations specially adopted processes and techniques that further could lead to more cost effective work for the organisations. As a guide to e.g. researchers and based on the findings from the interview studies we have identified a number of requirements on processes and techniques. The intension is that these requirements can serve as guidance to researchers aiming at developing methods and techniques that are used in this domain.

8. ACKNOWLEDGMENTS

The authors would like to gratefully acknowledge the persons and their companies involved in the interviews. The authors would also like to acknowledge Gyllenstiernska Krapperupstiftelsen for funding the research studies of Christin Lindholm

9. REFERENCES

[1] ISO/IEC-9126-1 Software engineering— Product quality Part 1: Quality model, 2001.

[2] F. Brooks, No Silver Bullet Essence and Accidents of Software Engineering, IEEE Computer, Vol 20, No 4, 1987 pp 10-19.

[3] Commission of the European Communities, Council Directive 93/42/EEC EEC concerning medical devices.

[4] Software Engineering Institute, CMMI for Development, technical report CMU/SEI-2006-TR-008, ESC-TR-2006-008, 2005.

[5] Swedish Code of Statutes *The Act* (1993:584) Medical Devices. www.riskdagen.se (2008-09-16)

[6] U.S. Food and Drug Administration, Federal Food, Drug and Cosmetic Act section 201(h).

[7] U.S. Food and Drug Administration, 1995. Premarket Notification 510 (k), Regulatory Requirements for Medical Devices, HHS Publication, FDA 95-4158

[8] J. C. Knight, "Safety Critical systems: Challenge and Directions", In proceedings of the 24th International Conference on Software Engineering, 2002. ICSE 2002, IEEE Computer Society, 2002, pp 547-550.

[9] R.Hewett, R. Seker, "A Risk assessment Model of Embedded Software Systems", In proceedings of the 29th Annual IEEE/NASA Software Engineering Workshop, IEEE Publication, 2005

[10] K. Nilsen, "Stringent certification requirements for safety-critical software", Embedded Control Europe, pp. 18-21. 2004

[11] H. Doernemann, "Tool-based risk management made practical", Proceedings of the IEEE Joint International Conference on Requirements Engineering (RE´02), 2002.

[12] S. R. Rakitin, "Coping with Defective Software in Medical Devices", IEEE Computer, volume 39, 2006, pp 40-45.

[13] S. Prakash, A. Aurum, K. Cox, "Requirements engineering in pharmaceutical and healthcare manufacturing" In proceeding of 11th Asia-Pacific Software Engineering Conference (APSEC´04), pp. 402-409.

[14] V.M. Brannigan, "The SAFE MEDICAL DEVICES ACT OF 1990: New directions for FDA software regulation", In proceeding of Fourth Annual IEEE Symposium on Compute-Based Medical Systems, 1991, pp 350-357.

[15] C. Denger, R. Feldman, M. Höst, C. Lindholm, F.Shull, "State of the practice in software development for medical device production" IESE-Report No. 071.07/E, Fraunhofer Institut

[16] C. Robson, *Real world research*, second edition, Blackwell Publishers Ltd, Oxford, 2002.

[17] T.C. Lethbridge, S.E. Sim, J. Singer, "Studying software engineering: data collection techniques for software field studies", In proceedings of the 10th Empirical Software Engineering Conference, 2005, Spring Science pp 311-341.

[18] R.K. Yin *Case study research design and methods*, third edition, Sage, Thousand Oaks Calif. 2003.

[19] Nigel Hyatt, *Guidelines for Process Hazards Analysis (PHA, HAZOP), Hazards Identification, and Risk Analysis,* CRC Press LCC, Florida 2000

[20] D.H Stamatis, *FMEA from theory to execution,* second edition, ASQ, Milwaukee, 2003

[21] IEC 61025 Ed. 1.0 b:1990, Fault tree analysis (FTA), 1990

[22] T. Hazel, "*Outsourced IT-projects from the vendor perspective: different goals and different risks"* Journal of Global Information Management Vol 15, No 2, 2007.