A roadmap to ISO 14971 implementation

Derek Flood[*,†], Fergal Mc Caffery, Valentine Casey, Ruth McKeever and Peter Rust

Dundalk Institute of Technology Dundalk, Ireland

ABSTRACT

Medical device standards outline the requirements for developing medical devices. These standards however, do not outline how these requirements should be implemented causing difficulties for organisations entering the medical device domain.

The goal of this study is to validate a roadmap for the implementation of the ISO 14971 standard. The validation examined the arrangement of the milestones within the roadmap and grouping of the goals into milestones.

Five experienced risk management personnel in the medical device domain were asked to complete an on-line questionnaire examining their opinion on the structure and content of the roadmap.

Overall participants found the roadmap in general, to be well structured and well organised and made some recommendations for improving the roadmap through merging of specific goals and rearrangement of the milestones within the roadmap.

The implementation of a risk management process for the medical device domain can be a costly and time consuming process, however this can be alleviated through the use of a software process improvement roadmap for risk management.

Keywords: Medical device software, medical device standards, regulatory compliance, risk management, ISO 14971, software roadmap

1. INTRODUCTION

Medical devices enable medical professionals to increase the level of care to patients. In so doing they are improving the quality and length of life for patients. These devices however, carry with them a significant risk if they malfunction or are used incorrectly. The potential for a medical device to cause harm to patients and/or their operators can be extreme if the manufacturer fails in the implementation of a robust risk management process.

Software has been instrumental in the advancements of medical devices by allowing complex configuration changes to be made without the need for expensive and time consuming hardware changes [1]. In 2006, Faris et al. [2] estimated that over half of the medical devices for sale in the United States of America contained software.

The risk associated with medical devices has led to the need for regulation to ensure that only devices of sufficient quality can be sold [3]. The Food and Drugs Administration (FDA) are responsible for the regulation of medical devices within the USA while the European Commission provides the regulatory framework for countries within the European Union. International standards and guidance documents have been developed and adopted by these regulatory bodies to guide organisations to implement processes that will help ensure quality products are produced.

One such international standard is *ISO 14971 – Medical Devices – Application of risk management to medical devices* [4]. The ISO 14971 standard outlines the requirements for a risk management process which encourages organisations to identify and control risks associated with the medical device under development. This standard however, only specifies what organisations must do without specifying how this is to be done, providing organisations with a degree of freedom with respect to the process that is adopted to meet the requirements of the standard.

This approach however, makes it difficult for organisations inexperienced with risk management to identify a suitable process for performing risk management in a regulatory compliant manner. This work aims to address this issue through the development of a software process improvement roadmap for the implementation of an ISO 14971 compliant risk management process. The roadmap allows organisations to see what requirements of the standard are being addressed, through a high-level view while simultaneously providing them with a customised process, optimised for their organisation.

In this paper we outline the results of a validation of a high level roadmap for the implementation of the ISO 14971 standard. Five people experienced in risk management in the medical device domain were asked to review the roadmap and to determine if the goals of the standard were appropriately grouped into milestones and if these milestones were arranged into a suitable order for implementation.

The remainder of this paper is arranged as follows: Section 2 outlines the role of software within medical devices and outlines how software process improvement is being used in this domain. Section 3 discusses risk and outlines the ISO 14971 standard and describes some of the methods that can be used to fulfil its requirements. Section 4 introduces a high-level roadmap for the implementation of the standard while Section 5 outlines the research method used to validate the high level roadmap. Section 6 then describes the results of this validation. Section 7 outlines the next steps in this work. The paper is then concluded in Section 8.

2. SOFTWARE AND MEDICAL DEVICES

2.1 The role of software in medical devices

Software can offer many benefits to medical devices including efficiency, ease of use and facilitating complex configuration changes that may be needed during the use of the device. For this reason software is becoming a more important component of modern medical devices. In 2006, Faris et al. [2] estimated that software was contained in approximately 50% of the medical devices for sale within the United States.

Although there are many benefits to the use of software, there are also a large number of risks to using software within a medical device. Between 2005 and 2009, 87 infusion pumps were recalled due to safety problems [5]. An analysis of these devices revealed that these problems could be categorized into 3 sections; **software defects,** for example some of these devices failed to activate an alarm when problems occurred, **user interface issues,** such as unclear or confusing on screen instructions and **mechanical or electrical failures**, such as components breaking under routine use. A whitepaper [5] on the use of infusion pumps, produced by the FDA, reports that “many of the problems that have been reported are related to software defects”.

The prevalence of software within the medical device domain has prompted a revision in the Medical Device Directive, 2007/47/EC (Amendment) 2007 [6], to clarify that software in its own right can now be classified as a medical device. This change has meant a number of organisations, who were previously developing software for use within the medical domain, are now developing medical devices and have to adhere to the same standards and regulations as other medical device producers. Prior to this amendment these organisations were under no legal obligation to do so.

2.2 Medical Device Regulations and Standards

If an organisation wishes to market their medical devices within the European Union they must demonstrate compliance with the Medical Device Directive [6]. Similarly if the organisation wishes to sell their device within the USA they must adhere to regulations set forth by the FDA. These regulations recommend that organisations adhere to a number of international standards and guidance documents. If an organisation does not adhere to these standards and guidance documents they may still market their medical device if they can provide strong justification for not following them.

One of the most fundamental requirements of a medical device organisation to achieve regulatory compliance is the implementation of a Quality Management System (QMS). A QMS ensures that the processes used during the development and production of a medical device are defined and monitored to ensure high quality products are developed. The requirements of a QMS for medical devices have been outlined in ISO 13485:2003 [7]. This standard is harmonised in the EU with the Medical Device Directive (MDD) [6] and has recently been accepted by the FDA as adequate fulfilment of the requirements of a QMS.

As part of the QMS, organisations must perform risk management activities. To improve the quality of the medical devices and receive regulatory approval, the organisation should identify all possible risk and take appropriate action to help mitigate them. ISO 14971:2007 [4] describes the requirements of a risk management process for medical device development. This standard identifies six key stages of risk management; Risk Analysis, Risk Evaluation, Risk Control, Evaluation of overall residual risk acceptability, Risk Management Report, and Production and Post-Production information. A full overview of the ISO 14971 risk management process can be found in Section 3.

As part of the risk management process, potential user errors should be considered. To aid organisations in identifying user errors and other usability issues, IEC 62366 [8] outlines a usability engineering process. The usability engineering process defined in IEC 62366 applies not only to the device being developed but also incorporates supporting documentation such as user manuals and on-device markings. The process recommends the use of user profiles and task analysis to identify frequently used functions of the medical device and to identify issues that may occur during the use of the device.

IEC 62304:2006 – Medical device software – Software life cycle processes [9], provides specific guidance on the processes to be performed for the development of medical device software. Clause 7 of IEC 62304 describes a software risk management process that is additional to the risk management process described in ISO 14971. IEC 62304:2006 is an EU harmonised standard and is recognised by the

FDA as an approved consensus standard. It is therefore used to develop medical device software for both the European and US markets as well as many other countries.

2.3 Software Process Improvement

There are many reasons why organisations may choose to undertake Software Process Improvement (SPI) initiatives. Studies have shown that SPI can offer a high return on investment in the form of productivity gains, reduced time to market and fewer defects reported by customers [10, 11, 12, 13, 14, 15, 16].

In addition to the benefits outlined above, there are many examples of specific successes achieved by organisations undertaking SPI initiatives. Through peer reviews of software requirements to detect defects prior to coding, one organisation was able to reduce the time spent on rework during the coding phase. In another organisation, improved configuration management practices allowed staff to replicate many errors encountered in the field, reducing the time and expense required to resolve problems [16].

The Software Engineering Institute has set out a roadmap for the undertaking of a software process improvement initiative [17]. This report identifies three main phases in which the software process improvement initiative should progress through. The first phase is to initiate the process improvement initiative which involves learning about SPI, committing initial resources and building a process infrastructure.

The next phase is to baseline the current state of the organisations software processes. This is achieved through the undertaking of a software process improvement assessment, such as ISO/IEC 15504-5:2012 [18] (SPICE) or Capability Maturity Model® Integration (CMMI®) [19]. During an assessment the organisations current processes are assessed and measured, and any weakness or shortcomings are identified. Both ISO/IEC 15504-5 and CMMI® contain capability levels which can allow an organisation to quantify the current state of their processes. These levels also facilitate the setting of targets which the organisation can reach through its process improvement initiative.

Within ISO/IEC 15504-5 [18] an assessment is carried out on specific processes using a conformant Process Assessment Model (PAM) related to one or more Process Reference Models (PRM). In a process assessment model such as ISO/IEC 15504-2 [20], process capability is defined on a six point ordinal scale that enables capability to be assessed from the bottom of the scale, Incomplete (Level 0), through to the top end of the scale, Optimizing Level 5.

The process attribute score and corresponding rating values are defined as:

- N Not achieved - 0 to 15 % achievement, there is little or no evidence of achievement of the defined attributes in the assessed process.
- P Partially achieved - > 15 % to 50 % achievement, there is some evidence of an approach to, and some achievement of, the defined attributes in the assessed process. Some aspects of achievement of the attributes may be unpredictable.
- L Largely achieved - > 50 % to 85% achievement, there is evidence of a systematic approach to, and significant achievement of, the defined attributes

in the assessed process. Some weakness related to these attributes may exist in the assessed process.

- F Fully achieved - > 85 % to 100 % achievement, there is evidence of a complete and systematic approach to, and full achievement of, the defined attributes in the assessed process. No significant weaknesses related to these attributes exist in the assessed process.

The final phase of the software process improvement initiative is to implement or deploy the software process improvements. This stage involves the identification of suitable methods for improving the software processes by addressing the weakness and shortcomings identified during the assessment and then implementing them within the organisation.

Software process improvement is not an overnight activity. It takes long-term commitment from all employees of the organisation, especially senior management, who must provide adequate resources for the implementation of the software process improvement [21]. In describing a usability maturity model developed by Nielsen, the Healthcare Information and Management Systems Society (HIMSS) usability task force noted that it can take decades to reach full maturity [22].

2.4 Software Process Improvement in the medical device domain

As regulatory bodies only outline the regulatory requirements which must be complied with and not how they can be effectively achieved, medical device organisations have been compliance centric in their approach to software development. As a result, there has been very limited adoption of software process improvement within the medical device domain [23].

In addition existing generic SPI models, such as the CMMI® [19] and ISO/IEC 15504-5:2012 [18] (SPICE), do not provide sufficient coverage to achieve medical device regulatory compliance [24]. To address this issue a medical device specific SPI framework, titled Medi SPICE, is being developed [25].

The objective of undertaking a Medi SPICE assessment is to determine the state of a medical device organisation's software processes and practices, in relation to regulatory requirements and best practices with the goal of identifying areas for undertaking process improvement [24]. It can also be used as part of the supplier selection process when an organisation wishes to outsource or offshore part or all of their medical device software development to a third party or remote division [26].

Medi SPICE is based on ISO/IEC 15504-5:2012 [18], IEC 62304:2006 [9] and ISO/IEC 12207:2008 [27]. It is being developed in line with the requirements of ISO/IEC 15504-2:2003 [20] and contains a Process Reference Model (PRM) and Process Assessment Model (PAM). It also incorporates the requirements of the relevant medical device regulations, standards, technical reports and guidance documents.

As well as the Medi SPICE assessment model, a number of other assessment models have been developed to look at specific aspects of the software development process within the medical device domain. Med-Trace [28] is a lightweight software traceability process assessment and improvement method for the medical device

industry. Due to the regulatory nature of medical device software, organisations are required to maintain good traceability from their requirements right the way through design, implementation to testing. In addition to this, other supporting processes such as risk management also require traceability. A Med-Trace assessment can be used to assist companies comply with the traceability requirements of the medical device software standards and regulations.

Med Adept [29] is another process assessment method used in the medical device domain. It is a lightweight assessment method for evaluating an organisations software development processes and has been developed in line with ISO 15504-5, Adept and ANSI/AAMI/IEC 62304:2006.

A risk management capability model (RMCM) [30] is being developed for use in the medical device domain to enable medical device companies produce safe and effective software. The RMCM is based upon a formal SPI model, [1]CMMI®. The standards and guidance documents that are relevant to the medical device domain detail what activities have to be performed to achieve compliance but do not enforce any specific method for performing these activities. The RMCM draws from the CMMI, ISO 14971, SW68 [31], TIR32 [32], GAMP 4 [33] and the Center for Devices and Radiological Health (CDRH) (FDA specific) guidance documents [34,35,36] to provide a means for medical device companies to perform risk management activities at the fundamental capability level.

3. RISK MANAGEMENT

3.1 The nature of risk

Organisations operating in the medical device domain have two distinct risk management processes to conduct, each with its own definition of risk. Project risk – defined as the "*effect of uncertainty on objectives*" and product risk – defined as the *"combination of the probability of occurrence of harm and the severity of that harm"*. There are two distinct sets of stakeholders involved in each process. Considering project risk, the organisation as a business may have shareholders and the risk management process utilised to protect the shareholders interest may be compliant with or based on IS0 31000 [37] or similar.

Today there are comprehensive frameworks and guidelines to help organisations carry out risk management activities and to keep them under review. This however was not always the case. Before 1995 there was no definitive framework or process in existence. There were a small number of competing frameworks which were regarded as unsatisfactory [38]. There was clearly a need to develop a universally acceptable framework.

This work was undertaken jointly by Standards Australia and Standards New Zealand in the early 1990's which culminated in the publication of AS/NZS 4360:2004 [39]

[1] ®CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

that now defines risk as *"the chance of something happening that will have an impact on objectives"*. It is important to note that risk was now understood to have both positive and negative attributes.

In 2005 the International Standards Organisation started work on ISO 31000 using AS/NZS 4360:2004 as its first draft [38]. They published ISO 31000:2009 [37] and defined risk as "*effect of uncertainty on objectives*". Risk was now seen as something that has uncertainty as a compliment – if uncertainty does not exist then there can be no risk. The standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Considering product risk, the organisation as a medical device manufacturer may have patients and users/operators as stakeholders and the risk management process utilised in this sphere of operation requires that it be compliant with ISO 14971 [4].

ISO 12207 [27], introduced in 1995, subsequently amended and republished in 2008, establishes a common framework for software life cycle processes and includes a risk management process that has an application in the general area of software development.

The set of processes, activities, and tasks described in ISO 62304 [9] establishes a common framework for medical device software life cycle processes. ISO 62304 states that *"the manufacturer shall apply a risk management process complying with ISO 14971"* and defines risk as the *"combination of the probability of occurrence of harm and the severity of that harm"*.

The ISO 14971 standard outlines the requirements for a risk management process for use within the medical device domain. The goal of a risk management process is to "*identify the hazards associated with a medical device, to estimate and evaluate the associated risks and to control these risks and to monitor the effectiveness of these controls"*. The risk management process is not a single step to be performed during the development of the medical device, but an on-going activity that is constantly and consistently applied throughout the entire life of the medical device from inception to withdrawal of the medical device from the market.

3.2 Overview of ISO 14971

Requirements concerning the risk analysis component of the risk management process were developed first and published as ISO 14971-1:1998, with the intention that the requirements for risk evaluation, risk control and postproduction information evaluation could be covered in additional parts, but all the requirements were incorporated into International Standard ISO 14971:2000. This standard was amended and republished in 2007 and it is this standard that this roadmap was developed for.

The requirements contained in the current version of ISO 14971 provide manufacturers with a framework within which experience, insight and judgment are applied systematically to manage the risks associated with the use of medical devices [40].

ISO 14971 was developed specifically for medical device/system manufacturers using established principles of risk management. For other manufacturers, e.g., in other healthcare industries, this International Standard could be used as informative guidance in developing and maintaining a risk management system and process [40].

ISO 14971 deals with processes for managing risks, primarily to the patient, but also to the operator, other persons, other equipment and the environment [40].

The six phases of the risk management process are; Risk analysis, Risk evaluation, Risk control, Evaluation of overall residual risk acceptability, Risk management report, and Production and post-production information [4]. During the implementation of risk control measures it is possible that additional risks are introduced to the device and these risks should be subjected to the risk management process like all other risks. In addition it is possible that risks are only identified once the device has entered production and therefore it is necessary to control these risks if and when they arise. The risk management process and its iterative nature is shown in Figure 1.

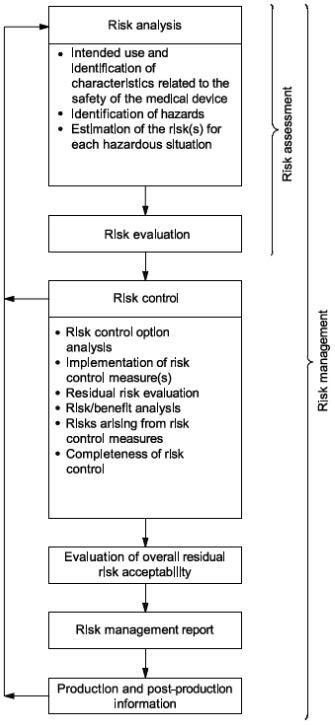

Figure 1 A schematic representation of the risk management process [4]

Each of the phases of the risk management process is outlined below:

Risk analysis. During the risk analysis phase, all possible hazards of the medical device are identified. These hazards are then evaluated in terms of the probability of occurrence and the severity of harm. The standard does not specify metrics to use for evaluating the probability and severity of harm allowing organisations to select a method that is most suited to them. The organisation may choose to do this evaluation either qualitatively or quantitatively depending on the device under development and the organizational culture.

Risk evaluation. Using the probability of occurrence and severity of harm, the organisation must determine if risk control measures are necessary. If there is a low probability of harm and the resulting harm is not severe then an organisation may decide that the risk is acceptable. The level of risk that is acceptable can be dependent on the benefits afforded by the medical device and therefore can vary between devices. For example the level of acceptable risk associated with a computerised tomography scanner would be higher than that of a blood pressure monitor as the benefits afforded by the computerised tomography scanner would be greater.

Risk control. Once it has been determined that a risk is unacceptable, the organisation has a responsibility to implement a risk control measure to address that risk. The standard outlines three broad categories of risk control:

- Inherent safety by design;
- Protective measures in the medical device itself or in the manufacturing process;
- Information for safety.

Each risk that requires control should apply one of these options, using the priority ordering outlined above, i.e. if possible address the risk through inherent safety by design, if not possible then the risk should be controlled with protective measures and finally if this is not possible then the organisation should provide information relating to the risk.

When a risk control measure is implemented, the organisation has a responsibility to ensure that no residual risk is present in the device. If there is residual risk then the organisation should subject these risks to the risk management process.

Evaluation of overall residual risk acceptability. Once all risk control measures have been controlled the organisation must review the remaining risks to determine if they are acceptable. If they are not the organisation should determine if the benefits of the medical device outweigh the risks associated with the device.

Risk management report. Before the product is released the organisation should carry out a review of the risk management process and produce a risk management report. As part of this review the organisation should ensure that the risk management process has been carried out appropriately, the overall residual

risk is acceptable and the appropriate mechanisms are in place to obtain relevant information related to safety during production and post-production.

Production and post-production. During these phases of the product lifecycle the organisation should monitor the medical device to ensure that no previously unrecognized hazards or hazardous situations are present and that the estimated risk arising from a hazardous situation are still acceptable. If this is not the case the information should be fed back into the risk management process.

In addition to the phases outlined above the standard defines a number of requirements in terms of documentation and management responsibilities in relation to the risk management process.

Although the ISO 14971 standard makes no specific references on how to deal with a contractor situation, in most cases it will be implemented in conjunction with ISO 13485 – Medical devices — Quality management systems — Requirements for regulatory purposes [7]. ISO 13485 states that a manufacturer is responsible for the safety of a medical device irrespective of whether they completed the work themselves or outsourced to another organisation/individual.

IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software, [41] recommends that the original manufacturers, by way of contractual agreements, ensure that they maintain sufficient control over the software and its design so that the requirements of ISO 14971 are fully complied with. This may be implemented by requiring the contractor to demonstrate effective risk management themselves by being compliant with ISO 14971. Although a number of other strategies may be utilised, a full description of these strategies is beyond the scope of this work as our focus is on the requirements as detailed in ISO 14971.

3.3 Approaches to risk management

Risk Identification

One of the key aspects of the risk management process is to identify the risks that the device poses to not only the user of the device, but also the patient (if different from the user) and the environment in which the device is to be used. The identification of these risks is a complex process and there are a number of methods that can be used by medical device manufacturers.

Bartoo [42] identifies one of the most common methods of risk identification used in the medical device domain, “brainstorming sessions”. During brainstorming sessions a multidisciplinary group brainstorm to identify risks of a proposed medical device. Bartoo recommends that the multidisciplinary group should contain representatives

from a diverse range of backgrounds such as hardware and software engineers, system engineers, regulatory and clinical staff and marketing and service personnel.

Research [43] has shown that members from different backgrounds can offer different perspectives and thus identify different types of risks. In a controlled study Lindholm and Host [43] have shown that the risk overlap between three groups of participants from different backgrounds (medical device software developers, general software developers and clinicians) was rather small and the best results can be obtained through utilization of personnel from multiple disciplines. This approach is also recommended in a number of other studies [42, 44]

An alternative approach that can be used for risk identification is Fault Mode and Effect Analysis (FMEA). The following description is adopted and abbreviated from [45] to provide a high level overview of the main points of a FMEA analysis:

1. Identify all possible failure modes
2. For each failure mode identify the possible consequences of that failure
3. Estimate the severity of harm for each failure. If more than one severity is identified for each failure then the highest severity level is recorded.
4. Determine the root cause of each failure and estimate the probability of occurrence for each root failure.
5. Determine the detectability (how well a root cause can be detected) of each failure.
6. Calculate a Risk Priority Number (RPN) by finding the product of severity, probability and detectability.
7. Prioritize the risks using the RPN.

One study conducted by Fetcher & Barba, [46] applied FMEA to infusion pumps and found the process to be time-consuming but worthwhile and concluded that *"the exercise would have a positive impact on overall patient safety"*.

Risk Estimation

An important consideration of the risk management process is the estimation of severity of harm and probability of occurrence of each risk. These values can be used to determine if the medical device requires risk control measures to be implemented or if it is sufficient to alert users to the risk. Although there are many scales that can be used to measure these two values, they can be broadly categorized into two types; qualitative and semi-quantitative.

In a qualitative approach each risk is rated using one of a variable number of textual descriptions. For example the ISO 14971 standard suggests estimating severity of harm arising from each risk using one of the following severity levels:

- **Significant**: - Death or loss of function or structure

- **Moderate**: - Reversible or minor injury
- **Negligible**: - Will not cause injury or will injure slightly

Similarly the probability of harm can be estimated using a qualitative scale. One example from Bartoo [42] estimates the probability of harm using a 5-point scale:

- **Frequent**: - Likely to occur at least once a month in the operating life of the system
- **Probable**: - Likely to occur less than 12 times per year in the operating life of the system
- **Occasional**: - Likely to occur at least once in the life of the system
- **Remote**: - May occur in the life of the system
- **Improbable**: - unlikely to occur in the life of the system

In contrast to the qualitative approach mentioned about, a semi-quantitative approach may also be used. In a semi-quantitative approach exact probability of harm may not be known but it may be known the probability is within a specific range. For example

- **Frequent**: >= 10^{-3}
- **Probable**: <10^{-3} and >= 10^{-4}
- **Occasional**: <$10^{-4}$and >= 10^{-5}
- **Remote**: <$10^{-5}$and >= 10^{-6}
- **Improbable:** < 10^{-6}

Risk Evaluation

Risk evaluation is used to determine if a risk is acceptable or further risk control measures are necessary. The ISO 14971 standard does not define what level of risk is acceptable leaving this decision up to the manufacturers of the device. On deciding on what level of risk is acceptable the organisation should consider levels of risk evident in similar devices, applicable standards and evaluation of clinical study data.

Typically medical device organisations use a risk matrix to indicate the level of acceptable risk. Using a combination of severity of harm and probability of occurrence of harm, an organisation can indicate in the matrix which combinations are acceptable and which are not. Table 1 shows an example of a risk evaluation matrix. In the matrix below the shaded area indicates risks that are unacceptable while the clear area indicates acceptable risks.

Although the example above only differentiates between acceptable and unacceptable risk, manufacturers may choose to use more fine grained categories of acceptability. For example Bartoo [42] defines three levels of risk acceptability; High (where risk must be reduced before distribution to customers), Moderate (where risk must be reduced before distribution to customers however, risk benefit analysis can be considered if risk reduction is impractical) and Low (Risk control measures are not required).

4. ROADMAP FOR ISO 14971 COMPLIANT RISK MANAGEMENT

Although the ISO 14971 standard specifies what needs to be accomplished by a risk management process, the standard does not specify how this is to be achieved. Supporting appendices of the standard provides some guidance on this, however some organisations inexperienced with risk management find it difficult to implement a suitable risk management process. To address this issue this work introduces a software process improvement roadmap for performing risk management of medical devices.

4.1 Software Process Improvement Roadmaps

In the context of this work, a software process improvement roadmap is defined as "A series of milestones, comprised of goals, that will guide an organisation, through the use of specific activities, towards compliance with regulatory standards."

The roadmap is divided into two levels. The first level defines the goals, grouped into milestones, that the organisation should achieve throughout the SPI initiative. The first level of the roadmap is presented at a high level and does not contain any detail relating to how the goals should be achieved. This is done for two reasons. Firstly, by presenting the roadmap as a series of goals, traceability to the relevant standard can be easily achieved. Secondly, the high-level roadmap can form a basis for communication across the industry as the same high-level roadmap can be applied to all organisations.

The second level roadmap contains specific guidance for organisations on how to achieve the goals outlined in the high level roadmap. The activities performed, to meet the goals of the high level roadmap, can vary from organisation to organisation due to their nature, different abilities and resources. Each roadmap is comprised of multiple activities that can achieve each goal so that the most suitable activity can be presented to an organisation wanting to implement the roadmap.

The goal of the roadmap is to introduce a process that will meet the requirements of the ISO 14971 standard. To this end each goal is introduced into the organisation at the earliest appropriate point in the development process. Although the activities may be performed at several points during the development process they are only introduced once and repeated as required.

4.2 Development Methodology

The methodology used for the development of the roadmaps is as follows:

1. **Identify requirements of the standard.** The first step in the process of developing the roadmap is to identify all of the required activities of the standard. This step is similar to the first step in the transformation process presented in [47].

2. **Logically group all requirements**. The next step is to group the requirements. Requirements can be grouped based on the stage of the software development lifecycle at which they will occur. Some activities are performed throughout the lifecycle, independent of specific phases. In those cases these activities should be grouped together in a logical manner.
3. **Separate grouped activities in line with ISO/IEC 15504 capability levels.** Once the requirements have been grouped, these groups should be separated based on the capability level at which the requirements should be performed. These groups form the milestones of the roadmap
4. **Order the milestones based on the capability level and logical groups**. All Level 1 milestones, as defined in ISO 15504-2 should be implemented first in the order in which they will occur in the development process, followed by all Level 2 activities, and subsequently by all Level 3 activities until all of the milestones are in a suitable order.
5. **Validate generated roadmap.** The generated roadmap should be validated with industry experts. These experts could be individuals working in industry implementing the standards, assessors regulating organisations using the standards or academics with the appropriate expertise. Members of the standards committee could also assist with the validation.
6. **Identify activities that can meet the identified goals**. The next step in the generation of the roadmap is to identify appropriate activities that can be used to fulfil the requirements of each goal in the roadmap. This can be done through a systematic literature review and/or case studies with organisations already implementing the standard.
7. **Validate activities in host organisation**. The final stage of the roadmap development methodology is to validate the roadmap within a host organisation. This will involve the generation of a roadmap for the host organisation and then undertaking a software process improvement initiative to implement the roadmap.

For a full description of the roadmap development methodology please refer to Flood et al. (2013) [48].

4.3 Roadmap to ISO 14971 compliance

The roadmap resulting from the application of the roadmap development methodology to the ISO 14971 standard contains 14 milestones and 52 goals. The 14 milestones contain all of the requirements from the 6 phases of the risk management process and all supporting requirements from the standard. The 14 identified milestones are as follows:

M1. Initial Planning: Before the risk management process can commence, organisations must plan the implementation of the process. This involves defining the policy for defining risk acceptability, defining the criteria for risk acceptability, defining the verification activities to be used, establishing the risk management file

and document the system that will be used for categorization of probability of harm and severity of harm. (6 goals)

M2. Risk Analysis: The risk analysis milestone is predominantly concerned with the identification and documentation of hazards and hazardous situations. As part of this process the organisation must identify and document the intended use and any foreseeable misuse of the medical device. (4 goals)

M3. Risk Evaluation: During the risk evaluation milestone the organisation introduces the estimation of probability of occurrence and severity of harm and then based on the criteria for risk acceptability the organisation determines if risk control is necessary. As part of this milestone the organisation must document the results of risk evaluation. (3 goals)

M4. Risk Control: The risk control milestone introduces control of the risks to the organisation. As part of this milestone the organisation must identify and implement suitable risk control measures for all risks that are identified as requiring risk control. In addition the organisation should document the risk control measures implemented. (3 goals)

M5. Verification of Risk Control: Once the risk control measures have been implemented, the organisation has a responsibility to ensure that they have been implemented correctly and that the implemented risk control measure is effective. If the risk control measure does not ensure that the risk is effective then they must re-subject the risk to the risk management process. (5 goals)

M6. Residual Risk: The organisation should evaluate all residual risks after all risk control measures have been put in place. If any new risks are identified then the organisation must subject these risks to the risk management process. In addition they should conduct a risk/benefit analysis to ensure that the benefits of the medical device outweigh the risks. (8 goals)

M7. Pre-Release: Before the release of the medical device the organisation should conduct a final review of the risk posed by the medical device and ensure that all risks from identified hazards have been considered and to determine if the residual risk is acceptable. In addition the organisation must carefully consider how to disclose the residual risk, i.e. the level of detail needed, the wording of the residual risk to ensure easy understanding and the means and media to use. (6 goals)

M8. Pre-Production: Prior to the commencement of production, the organisation should establish a system for collecting and reviewing information about the medical device during production and post-production. A schedule for the review of this information for its relevance to safety should be established. (1 goal)

M9. Post-Production: The next milestone should be introduced after the medical device has gone into production. During this milestone the organisation begins to

review collected data on the medical device and other similar devices to evaluate their relevance to safety and the risk management process. (2 goals)

M10. Management Planning: In establishing the risk management process, management must perform certain activities. These activities include the establishment of the scope of the risk management process, defining the requirements for regular reviews of the risk management process, establishment of the risk management plan and the documentation of the risk management plan. The goals included in this milestone were all determined to have an ISO 15504-2 capability level of 2 and therefore are introduced later in the roadmap. (4 goals)

M11. Staff Planning: As part of the planning process, the organisation should ensure that all staff are appropriately qualified and have the authority to perform their duty. This milestone ensures that staff and other resources are available for the risk management process. (4 goals)

M12. Final Review: Prior to release of the medical device the organisation should perform a final review of the risk management process to ensure that the risk management plan has been appropriately implemented. (2 goals)

M13. Risk Management System Review: In addition to the final review of the risk management process the organisation should regularly review the risk management process to ensure that it is performing optimally. If this is not the case the risk management process should be altered to address the issues identified. (3 goals)

M14. Traceability: As part of the risk management process, traceability should be ensured for all risks. This should include traceability from each hazard to risk analysis, risk evaluation, implementation and verification of risk control measures and the assessment of the acceptability of any residual risk. (1 goal)

The following table, Table 2, outlines the number of goals per milestone.

5. ROADMAP VALIDATION METHODOLOGY

The aim of this study is to validate the roadmap for ISO 14971 implementation. To meet this aim two objectives were set:

1. To determine if the goals are appropriately grouped into milestones
2. To determine if the ordering of the milestones is appropriate for implementation in a medical device organisation.

To meet these objectives, 17 people experienced in risk management for the medical device domain were asked to complete an online questionnaire. Personnel with experience in the area of medical device standards, and particularly the use of ISO 14971, were approached and asked to identify individuals they felt would be experienced with the standard and could participate in the study. From these four participants completed the online questionnaire and a fifth participant reviewed the material and emailed their opinion to the lead author.

The questionnaire, illustrated in Figure 2, showed participants each milestone in turn and asked them to state whether they thought each goal belonged in the milestone it was included in. In addition the participants were asked to rate on a 5 point Likert scale whether they agreed with the following statement (where 1 = strongly disagree and 5 = strongly agree): *The order of this milestone within the roadmap is correct.* The participants were also provided with the opportunity to add any additional comments they felt were relevant.

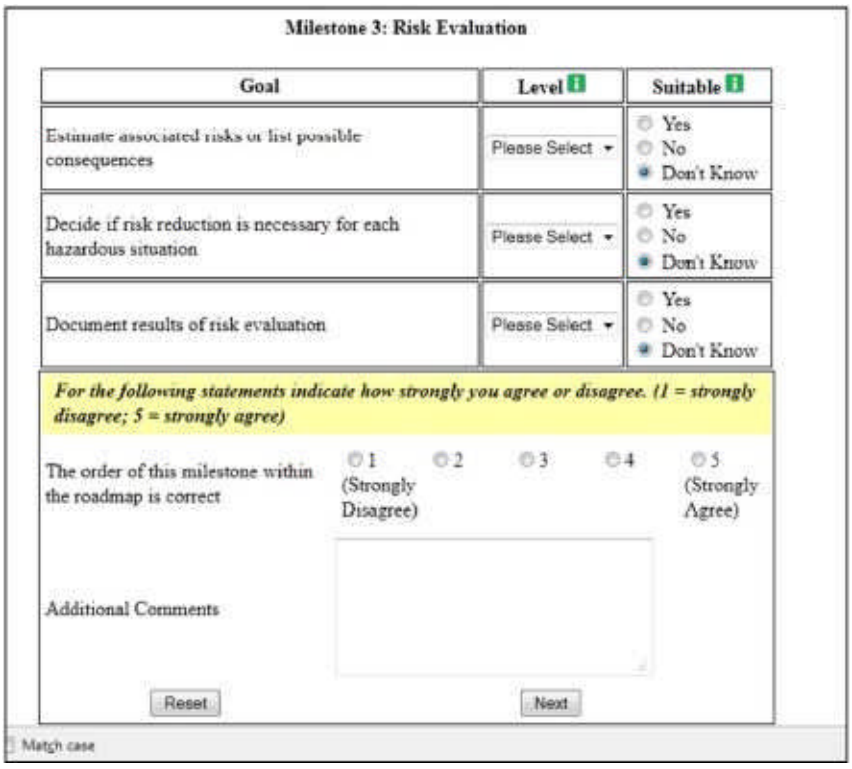

Figure 2: Screenshot from online questionnaire

In addition to this the online questionnaire also provides the user with the opportunity to state at what capability level, in line with 15504-2, each goal should be accomplished at. As the participants who took part in the study were experts in medical device risk management and not software process improvement these results were not included in the study.

Subsequently, the roadmap was reviewed with a number of experts in ISO 15504-2 and it was found that all of the goals of the roadmap should be found at level 1 of a risk management process assessment model. The experts remarked that as the requirements have been derived from the ISO 14971 standard, which must be implemented in full in order to achieve regulatory compliance, that any process assessment model would consider these as being necessary to meet the purpose of the process and therefore should all be found at level 1.

Figure 3: Navigation Panel

During the study participants could move freely through the roadmap using a navigation panel on the top of the screen as illustrated in Figure 3. The navigation panel was colour coded to allow participants monitor their progress during the study:

- **White** indicated milestones the user had not yet completed,
- **Light green** indicated the milestone they were currently on
- **Dark green** indicated milestones for which they had completed the survey.

6. RESULTS

6.1 Grouping of the Milestones

The first objective of the study was to determine if the goals were appropriately grouped into milestones. To meet this objective each participant was asked if each goal belonged to the milestone. The participants could select one of three possible answers: Yes, No, or Don't know. To determine if a goal belonged in the milestone the participants answers were grouped and the majority answer selected by participants was determined to be correct. If less than two of the participants selected a given answer the goal was determined to be inappropriately grouped.

As can be seen in Figure 4 the majority of participants felt that the goals were appropriately grouped into milestones. For 55% of the goals all participants agreed that they were in the correct milestone. It can be seen that for Goal 51, included in Milestone 13 (M13 in the graph), that half of the participants felt that this milestone was out of place. One participant remarked *"Record changes to the risk management plan seems to be out of place here. Perhaps it is because I am used to the requirement*

of needing a quality system and the other goals listed here go with quality system review”.

This comment indicates that this is not specifically a risk management activity but part of a larger quality management system. However, the roadmap presented here is focused purely on the risk management process of which monitoring the risk management process is a part. For this reason it was decided that the goal should remain as part of this milestone as it forms part of the risk management process review.

In the remainder of the goals it can be seen that only one participant felt any goal was out of place therefore the majority of participants felt that the goals were well grouped into milestones, indicating that no changes were necessary.

During the analysis of the comments provided by the participants, it was remarked that *“Shouldn't need 2 questions for Verify & Document. If it is not documented it was not done.”* For this reason all of the goals were reviewed and where documentation is a separate goal from the activity that is being documented, the goals were merged to form a single goal. For example in Milestone 5, Goal 17 states “*Verify implementation of the risk control measure”* and Goal 18 states “*Document the verification of the risk control measure”*. In the revised roadmap these two goals were merged to form a new goal *“Verify and document the verification of the risk control measure”*.

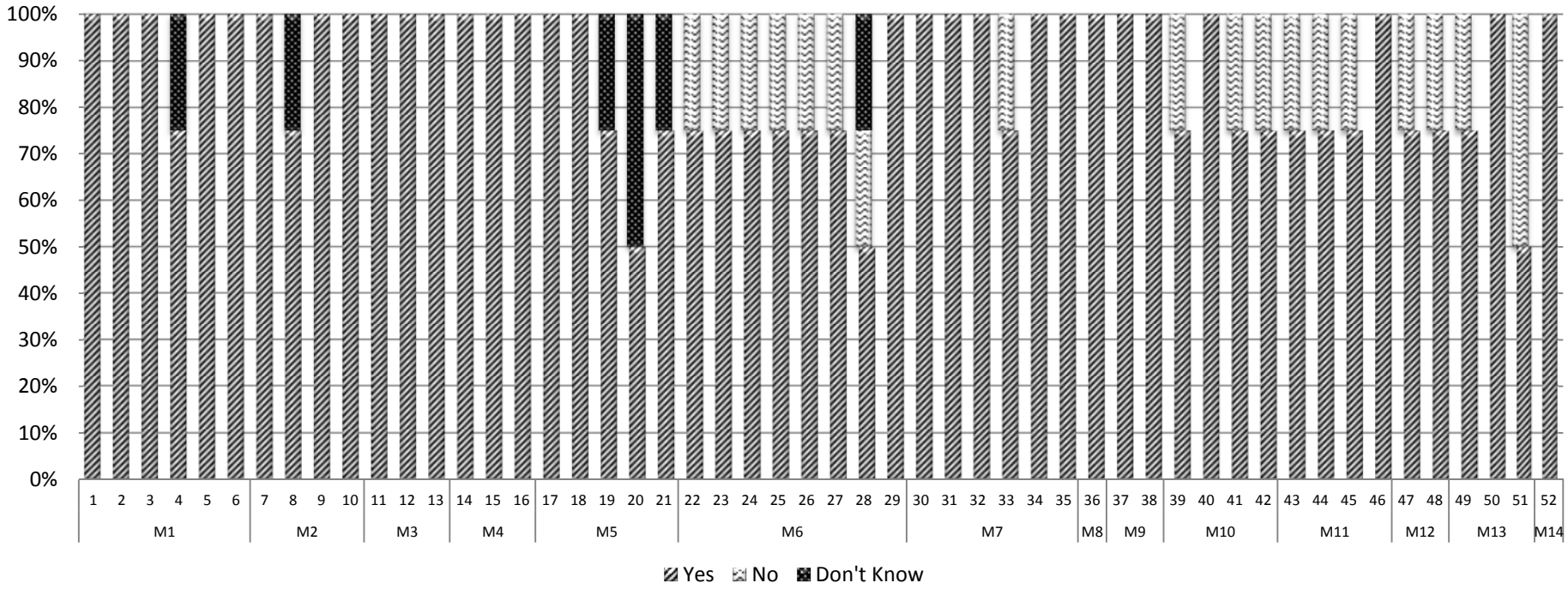

Figure 4: Grouping of Goals into milestones

6.2 Order of the milestones

The second aspect of the validation of the roadmap was *To determine if the ordering of the milestones is appropriate for implementation in a medical device organisation*. To determine if the ordering was appropriate, each participant was asked to state on a five point Likert scale (where 1 = strongly disagree and 5 = strongly agree) if "*The order of this milestone within the roadmap is correct.*"

Figure 5: Milestone Order

Figure 5 shows the mean response of the participants. From the data it can be seen that overall, participants had a favourable opinion of the order of the milestones presented. The results show that 3 of the milestones (M10, M11 and M14) were found to be in an inappropriate order for implementation.

Milestone M10, Management Planning, outlines the responsibilities of management in relation to the risk management process. As this process establishes the scope of the risk management process and establishment of the risk management plan the participants felt that this milestone should come earlier in the process. In addition one participant, who emailed their opinion of the roadmap, states that this milestone should occur second, after the initial planning. Similarly M11, staff planning, should be performed at the start of the risk management process.

Although traceability can be done retrospectively, best practice recommends that it is performed throughout the process. For this reason it is believed M14 Traceability should be introduced earlier in the process, before Risk Analysis. In starting traceability here the organisation can maintain traces easier throughout the risk management process.

6.3 Summary of Changes

In response to the results obtained during the validation of the roadmap a number of changes were made:

- Documentation of activities performed and the activities themselves were merged to form a single goal.
- Milestone 10 and Milestone 11 were moved to become Milestone 2 and Milestone 3 respectively.
- Milestone 14, Traceability was moved to become Milestone 4.

The resulting roadmap now contains 44 goals divided into 14 milestones as outlined below:

1. Initial Planning (6 goals)
2. Management Planning (3 goals)
3. Staff Planning (3 Goals)
4. Traceability (1 Goal)
5. Risk Analysis (4 goals)
6. Risk Evaluation (3 goals)
7. Risk Control (2 goals)
8. Verification of Risk Control (3 goals)
9. Residual Risk (7 goals)
10. Pre-Release (6 goals)
11. Pre-Production (1 goal)
12. Post-Production (1 goal)
13. Risk Management System Review (3 goals)
14. Final Review (1 goal)

7. FUTURE WORK

Currently the focus of this work is on the identification of suitable activities for the achievement of the goals outlined in the roadmap. To do this a literature review is being conducted to identify studies that have implemented the ISO 14971 standard and to extract methods used for the achievement of the goals included within the roadmap. In addition experts in the area of risk management implementation will be approached to help identify other suitable activities

The next phase then will be to trial the roadmap within a medical device organisation. For the trial the organisations existing processes will be examined and all goals that the organisation currently meets will be identified. Next, the authors will produce a roadmap customized for the organisation which will outline how the organisation should meet the remaining goals.

The customization of the roadmap will use the structure of the roadmap validated by the experts to guide the customized roadmap. Each goal that the organisation currently has in place will be removed from the generic roadmap and the milestones will be

reorganized, if necessary, to increase the efficiency with which the organisation can implement the remaining goals.

Next a meeting between the authors and the organisation will outline the roadmap and an agreement on the timeframe for the implementation of the roadmap will be reached. Specific guidance on how to implement the goals within the first milestone will also be provided at this meeting. Regular meetings between the authors and the organisation will take place to evaluate the organisations progress with the implementation and to outline the next milestone to be implemented until the entire roadmap has been implemented.

8. CONCLUSIONS

Risk management is a key activity for organisations developing medical devices. ISO 14971 outlines the requirements for performing risk management within the medical device domain. For some organisations new to the medical device domain identifying suitable activities to meet the requirements of ISO 14971 can be a difficult and time consuming task. To assist these organisations this work presents a roadmap to implement ISO 14971.

The proposed roadmap has been validated with five experienced risk management personnel within the medical device domain. Each participant was presented with the roadmap and asked to determine if the goals within each milestone are appropriately grouped and if the order in which the milestones are implemented would be suitable for implementing the ISO 14971 standard within a medical device organisation.

During the validation the majority of participants found that the goals in each milestone were well grouped and that none of the goals should be moved. However, it was identified that in a number of cases two goals could be merged into a single goal. These cases occurred when a specific practice and the documentation of that practice were separate goals. The participants also found that the positioning of some of the milestones was inappropriate for implementation. Based on this feedback these milestones were re-ordered into a more appropriate order for implementation.

Acknowledgements

This research is supported by the Science Foundation Ireland (SFI) Stokes Lectureship Programme, grant number 07/SK/I1299, the SFI Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by Science Foundation Ireland under a co-funding initiative by the Irish Government and European Regional Development Fund), and supported in part by Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855.

REFERENCES

[1] Lee, I., Pappas, G., Cleaveland, R., Hatcliff, J., Krogh, B., Lee, P., Rubin, H., and Sha, L., High-Confidence Medical Device Software And Systems. Computer, 2006. 39(4): p. 33 - 38

[2] Faris, T. H., (2006) “Safe and Sound Software: Creating an Efficient and Effective Quality System for Software Medical Device Organizations” ASQ Quality Press, 2006

[3] Burton, J., Mc Caffery, F., and Richardson, I., (2009) “Improving Software Risk Management in a medical device Company”, International Conference on Software Engineering (ICSE) 2009, Vancouver, Canada pp 152 - 162

[4] ISO 14971 (2007) – Medical Devices – Application of risk management to medical devices, Switzerland, ISO.

[5] Food and Drugs Administration (FDA) (2010) “Infusion Pumps Improvement Initiative”, http://www.fda.gov/medicaldevices/productsandmedicalprocedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm205424.htm [07/12/2012]

[6] European Council, Council Directive 2007/47/EC (Amendment). 2007, Official Journal of The European Union: Luxembourg

[7] ISO 13485:2003 (2003) Medical devices — Quality management systems — Requirements for regulatory purposes. Second ed. Geneva, Switzerland, ISO.

[8] IEC 62366:2007 “Medical Devices – Application of usability engineering to medical devices”

[9] IEC 62304:2006 (2006) Medical device software—Software life cycle processes. Geneva, Switzerland, IEC.

[10] Humphrey W. S., Snyder T. R., Willis R R. 1991. Software process improvement at Hughes Aircraft. IEEE Software 8(4): 11–23.

[11] Dion R. 1993, Process Improvement and the Corporate Balance Sheet, IEEE Software, 10 (4): 28 - 35

[12] Herbsleb J., A. Carleton, Rozum J., Siegel J., Zubrow D., 1994, Benefits of CMM-Based Software Process Improvement: Executive Summary of Results, Software Engineering Institute

[13] Diaz, M., Sligo, J. 1997 How software process improvement helped Motorola, IEEE Software 14 (5): 75 – 81

[14] Harter D., E., Krishnan M., S., 2000, Slaughter, S., A., Effects of Process Maturity on Quality, Cycle Time, and Effort in Software Product Development, Management Science 46 (4): 451-466

[15] Paulisch F., Ebert C., 2008, Business Impact of Process Improvements Workshop ICSE Companion ’08, Companion of the 30th international conference on Software Engineering 1073-1074.

[16] Ziehe, T., Wohlwnd, H., Gettel, G., McGowan, D., (1995) “Software Process Improvement (SPI) guidance for Improving software: Release 4.0” SEMATECH report, Technology Transfer # 95082943A-ENG; October 31st 1995.

[17] McFeeley, R., and McKeehan, D., "Software Process Improvement Roadmap," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, User's Guide CMU/SEI-95-UG-001,

[18] ISO/IEC 15504-5:2012 (2012) Information technology - Process Assessment - Part 5: An Exemplar Process Assessment Model. Geneva, Switzerland, ISO.

[19] CMMI Product Team (2006) Capability Maturity Model® Integration for Development Version 1.2. Software Engineering Institute, Pittsburch PA.

[20] ISO/IEC 15504-2 (2003) - Software engineering — Process assessment — Part 2: Performing an assessment. 2003: Geneva, Switzerland, ISO.

[21] Casey V., Richardson I, A Practical Application of the IDEAL Model, Software Process Improvement and Practice, vol. 9, no. 3, pp 123 - 132, July/September 2004

[22] HIMSS Usability Task Force (2011) "Promoting usability in Health Organisations: Initial Steps and Progress towards a Healthcare Usability Maturity Model" Health Information and Management Systems Society.

[23] Denger, C., Feldmann, R., Host, M., Lindholm, C. & Shull, F. (2007) A Snapshot of the State of Practice in Software Development for Medical Devices. First International Symposium on Empirical Software Engineering and Measurement. Madrid, Spain

[24] McCaffery, F. & Dorling, A. (2010) Medi SPICE Development. Software Process Maintenance and Evolution: Improvement and Practice Journal, 22, 255 – 268.

[25] Casey V., Mc Caffery, F. "Development of the Medi SPICE PRM", International SPICE Conference on Process Improvement and Capability dEtermination, 30th to 31st May 2012, Majorca, Spain, 265 -268

[26] Casey, V. (2010) Virtual Software Team Project Management. Journal of the Brazilian Computer Society, 16, 83 – 96.

[27] ISO/IEC 12207:2008 (2008) Systems and software engineering - Software life cycle processes. Geneva, Switzerland, ISO.

[28] Casey, V. and Mc Caffery, F. (2011) Med-Trace: Traceability Assessment Method for Medical Device Software Development. In: European Systems and Software Process Improvement and Innovation Conference, EuroSPI 2011, 27th - 29th June 2011, Roskilde University, Denmark.

[29] Mc Caffery, F., Casey, V.: Med-Adept: A Lightweight Assessment Method for the Irish Medical Device Software Industry. In: European Systems & Software Process Improvement and Innovation Conference (EuroSPI), Grenoble, France (2010)

[30] Burton, J., Mc Caffery, F., and Richardson, I., "A Risk Management Capability Model for use in Medical Device Companies" In: 4th Workshop on Software Quality, ICSE 2006, 21st May 2006, Shanghai.

[31] ANSI/AAMI SW68, Medical device software – Software life cycle processes. 5 June, 2001

[32] AAMI TIR32:2004, Medical device software risk management, 2005

[33] ISPE, GAMP Guide for Validation of Automated Systems. GAMP 4, Dec 2001

[34] CDRH, General Principles of Software Validation; Final Guidance for Industry and medical device Staff. January 11, 2002

[35] CDRH, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices; Guidance for Industry and medical device Staff. May 11, 2005

[36] CDRH, Off-The-Shelf Software Use in Medical Devices; Guidance for Industry, medical device Reviewers and Compliance. Sept 9, 1999

[37] ISO 31000:2009, Risk management – Principles and Guidelines, Geneva, Switzerland.

[38] Newdick, D., Risk Management and ISO 31000, http://www.slideshare.net/dougnewdick/risk-management-and-iso-31000. htm. [18/08/2014].

[39] Standards Australia and Standards New Zealand (2004) AS/NZS 4360:2004, Risk Management, Sydney, NSW. ISBN 0 7337 5904 1.

[40] http://shop.bsigroup.com/ProductDetail/?pid=000000000030268035. [18/08/2014].

[41] IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software, Geneva, Switzerland, IEC.

[42] Bartoo, G., (2003) "Risk management", IEEE Eng. Med. Biol. Mag., vol. 22, no. 4, pp.166 -,170, 2003

[43] Lindholm, C., Host, M., "Risk identification by physicians and developers - differences investigated in a controlled experiment," Software Engineering in Health Care, 2009. SEHC '09. ICSE Workshop on , vol., no., pp.53,61, 18- 19 May 2009

[44] Rakitin, R., "Coping with defective software in medical devices," Computer , vol. 39, no. 4, pp.40 - 45, April 2006

[45] http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html. [17/10/2013]

[46] Fechter, R.J., Barba, J.J., "Failure Mode Effect Analysis Applied to the Use of Infusion Pumps," Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE , vol.2, no., pp.3496,3499, 1-5 Sept. 2004

[47] Barafort, B., Renault, A., Picard, M., and Cortina, S., A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000, in SPICE 2008: Nuremberg, Germany.

[48] Flood, D, Mc Caffery, F, Casey, V, Regan, G.: A Methodology for Software Process Improvement Roadmaps for Regulated Domains – Example with IEC 62366, in: European Systems & Software Process Improvement and Innovation Conference (EuroSPI), Dundalk, Ireland (2013).

Table 1: Example Risk Evaluation Matrix

	Significant	**Moderate**	**Negligible**
High			
Medium			
Low			

Acceptable Unacceptable

Table 2: # of goals per milestone

Milestone	**# of Goals**	**Milestone**	**# of Goals**
Initial Planning	6	Pre-Production	1
Risk Analysis	4	Post-Production	2
Risk Evaluation	3	Management Planning	4
Risk Control	3	Staff Planning	4
Verification of Risk Control	5	Final Review	2
Residual Risk	8	Risk Management System Review	3
Pre-Release	6	Traceability	1