2013-12-01

Improving Safety in Medical Devices from Concept to Retirements

Martin McHugh
Technological University Dublin, martin.mchugh@tudublin.ie

Fergal McCaffery
Dundalk Institute of Technology, fergal.mccaffery@dkit.ie

Silvana MacMahon
Dundalk Institute of Technology, silvana.macmahon@dkit.ie

See next page for additional authors

Recommended Citation

Mc Hugh, M., McCaffery, F.,& MacMahon, S. (2013). Improving Safety in Medical Devices from Concept to Retirements In Book Chapter in *Handbook of Medical and Healthcare Technologies*, 2013, pg. 453-480. doi:10.1007/978-1-4614-8495-0_21

2013-12-01

Improving Safety in Medical Devices from Concept to Retirements

Martin Mc Hugh

Fergal McCaffery

Silvana Mac Mahon

Anita FInnega

Chapter X

IMPROVING SAFETY IN MEDICAL DEVICES FROM CONCEPT TO RETIREMENT

Martin McHugh, Fergal McCaffery, Silvana Togneri MacMahon and Anita Finnegan
Department of Computing and Mathematics
Dundalk Institute of Technology, Co. Louth, Ireland

1. Introduction

As with many domains the use of software within the healthcare industry is on the rise [1, 2] within the last 20 years. The use of this software ranges from performing administrative tasks such as patient registration to life sustaining tasks such as within a pacemaker. Prior to this, medical devices primarily consisted of hardware with a software component. A significant shift has occurred with medical device manufacturers realizing that functionality can be added to a medical device through the use of software. As the functionality of the medical device grows, so does the complexity and therefore the risk. The risk associated with this complexity applies to both the use of software in standalone devices and also medical devices designed for incorporation into a medical IT network. The incorporation of a medical device into an IT network can introduce risk to the safety, effectiveness and security (data & system) of the device. With an increase in complexity there is an increased risk of harm to the patient, clinician or third party.

The most famous failure of software resulting in harm to a patient within a medical device was with Therac-25 [3]. Therac-25 was a radiation therapy machine which used software to control when a beam spreader plate moved into position to reduce a patient's exposure to radiation. As a result of a failure within the software, this spreader plate did not always move into position when necessary and as a result of this failure, four people died and two were left permanently disfigured. In light of this failure and other significant failures of medical devices as a result of software malfunctions, regulatory bodies introduced regulations to ensure safe and reliable performance of medical devices consisting of software [4].

Within the United States, (US) medical devices are regulated by the Food and Drug Administration (FDA). Within the European Union, they are regulated through the

awarding of the CE mark, which can be awarded by notified bodies within each of the EU member states. Within Canada, medical devices are regulated by Health Canada. Whilst regulations vary between regions, the standards followed for the development of medical device software are typically universal. These standards include EN ISO 13485:2003 – Medical Devices – Quality Management Systems [5], EN ISO 14971:2012: Medical Devices – Application of Risk Management to medical devices [6] and IEC 62304:2006 – Medical Devices – Software Lifecycle Processes [7]. The primary concern of regulatory bodies is that medical devices are safe and reliable. To achieve this, all medical devices, regardless of safety classification marketed for use in the EU, US or Canada, must be developed in accordance with a Quality Management System (QMS). Within the EU and Canada, regulatory bodies recommend that medical device manufacturers develop their devices in accordance with EN ISO 13485. Prior to July 2012, medical devices manufacturers wishing to market a device for use within the US were required to adhere to the FDA Quality System Regulations (QSR) known as FDA 21 CFR Part 820 [8]. However, from July 1st 2012, the FDA began a pilot program in which they offer device manufacturers the option of submitting their quality system audits which are compliant with EN ISO 13485 [9]. This is seen as a step towards a harmonization between FDA regulations and Health Canada; however, it has the knock-on effect of being more beneficial to manufacturers who adhere to EU regulations.

Whilst medical device manufacturers are compliance centric, there is also a shift towards following industry best practices in order to further enhance development practices. However, current frameworks for software development best practices are not domain specific and don't address practices which are specific to the development of medical device software. Therefore, there is a need for a medical device software development specific framework, which aims to combine industry best practices for the entire development and maintenance lifecycles of medical device software with necessary regulations which medical device manufacturers must adhere to.

Section 2, provides a description of the different types of software used within the healthcare domain. Section 3, provides details of the regulations to which medical device manufacturers must adhere when developing medical device software. Section 4, details how medical device software organizations can develop safer and more reliable software by following Capability Maturity Models and discusses the development of a medical device software specific Process Assessment Model (PAM) and Process Reference Model (PRM) This PAM and PRM combine regulations with software development industry best practices that medical device software organizations can follow when developing regulatory compliant software. Section 5, focuses on the development of a PRM and PAM to manage the risks associated with the incorporation of a medical device into a hospital IT network. Section 6, discusses the development of a

Security Assurance PRM and PAM which aims to assess the development process of a medical device and also establish a security capability level for the developed product and finally section 7 presents the summary and conclusions of this chapter.

The primary contribution of this chapter is to provide medical device organizations with information relating to the regulations to which they must adhere and the standards they are recommended to follow. These standards and regulations cover areas including medical device software development, the application of risk management to devices connected to a healthcare network and security use cases for medical devices. Also information regarding the frameworks which combines the requirements of regulations, the guidance of the standards and industry best practices is presented.

2. Types of Software used in Healthcare

Software was first used in healthcare in the 1960's to perform administrative tasks. It was soon realized that introducing software into healthcare could decrease costs, increase patient satisfaction and improve hospital processes which improves patient care. However, since its introduction the use of software has grown exponentially [2]. Whilst the first software used in healthcare was limited to administrative tasks, modern software can be used to perform various tasks ranging from registering patient details on admission into a hospital to controlling a life sustaining device such as defibrillators. As the range of tasks which software could perform was so vast, categorization of that software was required. This categorization is based upon the intended use of the software and in accordance with regulatory requirements. These categories are:

- Software as an accessory to a medical device;
- Software as a medical device in its own right;
- Software as a medical device data system (MDDS); or
- Software currently unclassified and not subject to specific regulations.

2.1 Software as an Accessory to a Medical Device

An accessory to a medical device is an item which in itself is not a medical device but when connected to a medical device assists the medical device to perform its intended function;

The EU regulations define an accessory to a medical device as [10]:

"an article which whilst not being a device is intended specifically by its manufacturer to be used together with a device to enable it to be used in accordance with the use of the device intended by the manufacturer of the device"

Crumpler and Rudolph provided two definitions of software as an accessory to a medical device based upon the FDA's written guidance [11]:

(1) *"a (software) accessory is a (software) unit which is intended to be attached to or used in conjunction with another finished device": or*
(2) *"a software accessory to a medical device either accepts data from the user and modifies it for input to a medical device, or takes the data from a medical device modifies it for presentation to the user".*

It can be seen that whilst the wording between the EU and FDA regulations varies, the definitions are very similar. In essence software is defined as being an accessory to a medical device when it is connected to a medical device to facilitate the operation of that medical device. For example, if a spreadsheet application receives input from a heart rate monitor and calculates averages heart rate over a period of time it is considered an accessory to a medical device.

The key point to note is; where software meets the criteria of an accessory, it assumes the safety classification of the parent device to which it is connected. In our previous example, if the heart rate monitor received a Class III safety classification then the spreadsheet application would automatically assume the Class III safety classification and would undergo the same level of regulatory scrutiny as the heart rate monitor.

2.2 Software as a medical device in its own right

Software is defined as being a medical device if its intended function meets the definition of a medical device. In the EU the definition of medical device is [12]:

"any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application"

The FDA defines a medical device as:

"...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory

which is: recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes."

Health Canada provides a specific definition as to when software is considered a medical device [13]:

"Software regulated as a medical device;

(1) Provides the only means and opportunity to capture or acquire the data from a medical device for aiding directly in diagnosis or treatment of a patient; or

(2) Replaces a diagnostic or treatment decision made by a physician."

2.3 Software as a Medical Device Data System

In 2011, the FDA released its rule regarding MDDS known as CFR 21 Part 880.6310 [14]. As part of this rule the FDA released its definition of a MDDS:

"A device that is intended to provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices:

(i) The electronic transfer of medical device data;

(ii) The electronic storage of medical device data;

(iii) The electronic conversion of medical device data from one format to another format in accordance with a pre-set specification; or

(iv)The electronic display of medical device data."

Prior to this rule being introduced by the FDA, software performing any of the functions outlined in the definition of a MDDS was either regarded as an accessory to a medical device which assumed the safety classification of the parent device or was considered a medical device in its own right and was required to undergo a separate process of achieving regulatory approval. However, since the introduction of this rule, if software exclusively performs one or more of the functions as outlined in the definition of a MDDS will automatically receive a Class I safety classification. The FDA has determined that any risk posed by a MDDS would potentially come from inadequate software quality or incorrect functioning of the device. It is expected that poten-

tial issues such as these would be resolved by the use of a QMS in accordance with FDA regulations [15].

There is, however, an exception to this rule. If software exclusively performs one or more of the functions outlined in the definition of a MDDS and is used for active patient monitoring then it cannot be considered a MDDS and must be considered an accessory or medical device.

2.4 Software currently unclassified and not subject to specific regulation

The previous sections have discussed software that is used directly and indirectly with patient care and the category into which they fall. However, there are software applications that are used in healthcare that are currently unclassified and not subject to specific regulation.

Software used within Hospital Information Technology (HIT) which is only used for administrative purposes is currently unclassified [12]. Regulations are primarily concerned with patient safety and as there is no potential risk to patient safety as result of a defect in administrative software, if falls beyond the scope of regulatory scrutiny.

Also Electronic Health Records (EHR) and Computerized Physician Order Entry (CPOE) systems are currently unclassified. Upon reading the functions which these systems perform they do appear to fall into one of the categories previously mentioned. However, regulatory bodies have recognized that in the future these systems have the ability to automatically order tests for patients, therefore initiating the generation of clinical data and as a result would meet the definition of being a medical device [15].

3. Regulating Software in Healthcare

As medical devices can have a direct impact on a person's wellbeing, necessary controls are put in place to ensure the safe and reliable performance of the device. These controls take the form of regulations. Medical device manufacturers wishing to market a device into a region must adhere to the regulations of that region. In this section we describe the regulations within the EU, US and Canada which impact the development of software for use within the healthcare domain.

3.1 European Union Regulations

Medical devices marketed within the EU must carry the CE mark. The awarding of this mark certifies that the device has been developed in accordance with all of the applicable EU regulations. The CE mark is awarded by notified bodies within EU member states and once a device manufacturer receives a CE mark in any member state they are permitted to market their device in all of the member states.

Medical device manufactures must adhere to the Medical Device Directive (MDD) and its latest amendment to achieve the CE mark [16]. The MDD (93/42/EEC) has been amended 5 times with the latest amendment (2007/47/EC) being released in 2007. As part of this amendment, there were 14 significant amendments to the original directive [17]. The most significant of these amendments to impact software is the inclusion of software into the definition of being a medical device. Whilst previous amendments did allow for software to be a component of a medical device, they did not extend to standalone software being recognized as an active medical device. An active medical device is defined in the amendment to the MDD as:

"any medical device operation of which depends on a source of electrical energy or any source of power other than that directly generated by the human body or gravity and which acts by converting this energy…..Stand-alone software is considered to be an active medical device"

As a result of the inclusion of this wording into the amendment, situations may now arise where software can be the only component of a medical device used in a healthcare setting, subject to regulatory scrutiny. Prior to this amendment software was always seen as a component of a hardware device. To ensure the safety of the healthcare software the latest amendment to the MDD states:

"For devices which incorporate software or which are medical software in themselves, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification."

However, the amendment to the MDD does not clarify what is meant by "state of the art", but it is generally accepted that state of the art is referred to as best practice and best practice for medical device software development is achieved by following IEC 62304 and its aligned standards. To accompany this, the EU regulations require that all medical devices are developed in accordance with a Quality Management System

(QMS), such as ISO 13485 and in accordance with a risk management standard such as ISO 14971. These standards are harmonized for use within the EU [18].

When the latest amendment to the MDD was released, confusion arose as to when software would be considered an active medical device. The only clarification provided as part of the amendment was that software used in healthcare for administrative purposes is considered not to be a medical device. It was not until January 2012 when the European Council released the MEDDEV [10] document to accompany the amendment to the MDD that clarified which type of software was subject to regulatory scrutiny.

3.2 FDA Regulations

Medical devices marketed in the US must meet the FDA requirements. Unlike the EU, the FDA is the only regulatory body with the authority to approve a medical device for use within the US. Also unlike the EU the FDA does not specifically regulate software used in healthcare. Rather, if the software meets the definition of being a medical device then it is regulated in the same way as a hardware device that meets the same definition. All medical devices regardless of safety classification marketed in the US must adhere to either the FDA's Quality System Regulations (QSR) or to ISO 13485. However, since the Therac-25 incident, the FDA has recognized the increasingly significant role which software plays in healthcare and as a result has commissioned guidance documents which medical device software organizations can follow. These guidance documents include:

- Design Controls Guidance for Medical Device Manufacturers [19];
- General Principles of Software Validation [20];
- Guidance for Industry and Food and Drug Administration - Mobile Medical

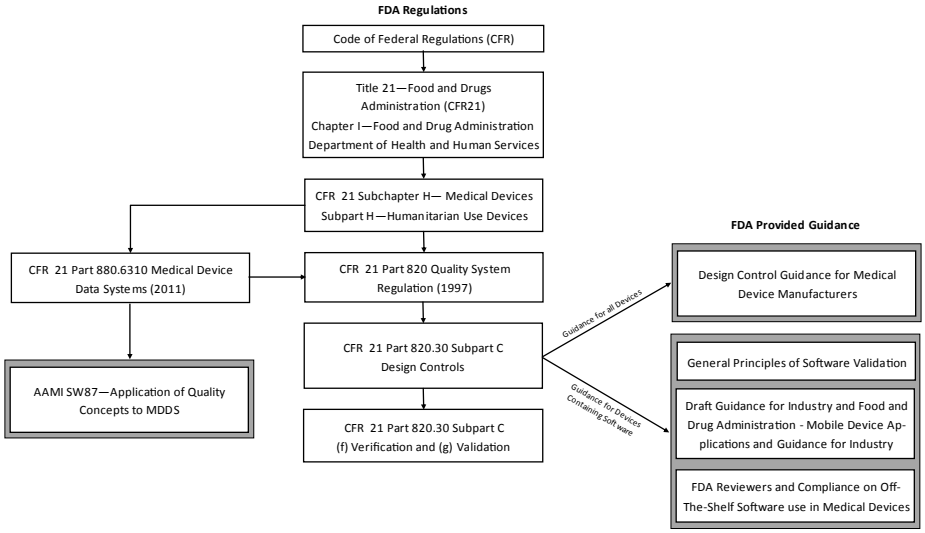

Figure 3 FDA Regulations, Guidance Documents and Rule

Applications [21];
- Guidance for Industry and FDA Reviewers and Compliance on Off-The-Shelf Software use in Medical Devices [22].

Also in conjunction with the regulations and the guidance documents the FDA releases rules. The most recent of these rules which impact on the development of software is the rule on Medical Device Data Systems. Figure 1, shows the relationship between the regulations, guidance documents and rules. As with the EU, the FDA recognizes that IEC 62304 is considered to be medical device software development best practice and has been a consensus standard under FDA guidelines since September 2008. One advantage of following IEC 62304 is that medical device software development organizations following IEC 62304 are not obliged to describe their processes in detail when seeking regulatory approval [23].

3.3 Health Canada Regulations

Health Canada regulates medical devices through its Medical Device Regulations Document SOR/98-282 [24]. Health Canada requires medical device organizations to validate the performance of the software to ensure it performs as intended. Medical device software organizations are required to submit validation studies when seeking regulatory approval. As with the EU, Canada recognizes that software can be a medical device in its own right and as so necessary controls must be put in place to ensure the safe and reliable performance of that medical device software. To achieve this all medical devices marketed in Canada must be developed in accordance with ISO 13485. Health Canada has also released guidance as to when software used in healthcare is considered to be a medical device.

3.4 Safety Classifications

Each region also categorizes medical devices based upon the potential risk the device poses. Table 1, shows the risk classification defined by each region and also shows how the risk classification of each region relates to the classification of the other regions.

The level of risk a device poses will determine the level of regulatory scrutiny applied to the device. For example, in the US class I devices are subject to the least amount of regulatory control. They are subject to “General Controls” which includes provisions that concern issues such as misbranding and premarket notification. Class II devices are subject to “General Controls” also, however they are subject special controls such

as adherence to mandatory performance standards and post market surveillance. Post market surveillance is the practice in which the FDA monitors the device once it has been released onto the market. Finally, class III devices must adhere to "General Controls" and special controls as with Class II, however devices marketed as class III devices must also request premarket approval. The process of achieving premarket approval involves the FDA evaluating the safety of the device prior to it being released onto the market [25].

Table 3. Safety Classification of Medical Devices

Risk	Low	Medium		High
EU	Class I	Class IIa	Class IIb	Class III
Canada	Class I	Class II	Class III	Class IV
US	Class I	Class II		Class III

4. Developing Software for use in Healthcare

The safety of medical device software is determined by the processes followed during development [26]. As a result medical device software manufacturers are advised to follow defined pathways when developing software. The Software Process Improvement (SPI) is gaining momentum in the generic software development industry, but has yet to be widely adopted in the medical device software development industry [27]. SPI methods such as agile software development have shown significant benefits where they have been embraced.

4.1 Capability Maturity Models in Medical Device Software

SPI models exist including the Capability Maturity Model Integration (CMMI®) [28] and ISO 15504-5:2006 [29] (SPICE), but these do not provide sufficient coverage of medical device regulations and standards [30]. In order to address the requirement for a medical device software process assessment and improvement model the Regulated Software Research Group (RSRG) at Dundalk Institute of Technology (DkIT) commenced the development of Medi SPICE a medical device specific SPI model which is being developed in collaboration with the SPICE User Group. This model is being developed similarly to Automotive SPICE [31], which is a domain specific SPI model for the automotive industry.

4.2 What is Medi SPICE?

Medi SPICE is based upon the latest versions of ISO/IEC 15504-5 and ISO/IEC 12207:2008 [32]. It provides coverage of the relevant medical device regulations, standards, technical reports and guidance documents. These include IEC 62304:2006 and its aligned standards, the FDA regulations [33] and guidance documents, and the amendment to the European Medical Device Directive and guidelines. The objective of undertaking a Medi SPICE assessment is to determine the state of a medical device organization's software processes and practices in relation to the regulatory requirements of the industry and to identify areas for process improvement [34]. It can also be used as part of the supplier section process when an organization wishes to outsource part or all of their medical device software development to a third party or a remote division [35].

Medi SPICE contains a Process Reference Model (PRM) which consists of forty two processes and twelve subprocesses which are fundamental to the development of regulatory compliant medical device software. Each process has a clearly defined purpose and outcomes that must be accomplished to achieve that purpose. Medi SPICE also contains a Process Assessment Model (PAM) which is related to the PRM and forms the basis for collecting evidence and the rating of process capability. This is achieved by the provision of a two-dimensional view of process capability. In one dimension, it describes a set of process specific practices that allow the achievement of the process outcomes and purpose defined in the PRM; this is termed the process dimension. In the other dimension, the PAM describes capabilities that relate to the process capability levels and process attributes, this is termed the capability dimension.

In line with ISO/IEC 15504-2:2003 [36] Medi SPICE process capability is defined over 6 levels:

- Level 0 Incomplete;
- Level 1 Performed;
- Level 2 Managed;
- Level 3 Established;
- Level 4 Predictable;
- Level 5 Optimizing.

The Medi SPICE PRM and PAM are being released in stages and each stage is extensively reviewed by interested parties from the SPICE User Group, representatives from international medical device standards bodies (i.e. IEC SC62A JWG3) and industry experts. This collaborative approach is seen as a key element in the development of Medi SPICE to ensure coverage of both the SPI and medical device software

regulatory requirements [34]. The overall objective of Medi SPICE is to provide a conformity assessment scheme to support first, second or third party assessments. It is envisaged that results from these assessments may be recognized by the relevant regulatory bodies.

4.3 Assessing against Medi SPICE

Like other SPI assessments models i.e. CMMI® and IEC 15504-5:2006, a full Medi SPICE assessment will require considerable planning and resources to successfully undertake. While Medi SPICE is being developed with the objective of being as efficient as possible the necessity for rigor dictates the level of planning, resources and analysis required for its successful implementation. While the need for and importance of Medi SPICE is understood [37], it was also appreciated by the RSRG that there was a specific requirement for lightweight assessment methods in the medical device software industry [38]. In particular there was industry led demand for a lightweight assessment method based on Medi SPICE. This was communicated directly to the RSRG by numerous medical device organizations. To address this specific requirement Medi SPICE-Adept was developed. There were two additional objectives in undertaking this task. The first was the opportunity to leverage the extensive research [39] and level of detail which developing Medi SPICE provided. The second was the opportunity to identify and facilitate the use of agile and lean methods. The use of agile and lean methods for medical device software development is an area that the RSRG are also currently researching to assist organizations increase the efficiency of their software development practices [40].

To be effective Medi SPICE-Adept required the employment of a lightweight approach for undertaking software process assessment and improvement. This included the use of a limited number of personnel to carryout and participate in the assessment while also maximizing the benefit of the time and effort of those involved. It was envisaged that Medi SPICE-Adept would eventually encompass all the Medi SPICE processes. It was therefore recognized that an assessment could take place either over 1 day or a number of days depending on how many processes were being assessed. It was also important that organizations could select the specific processes which were of most benefit for achieving their business goals. The focus of the method was on the evaluation of the essential practices, key work products and the achievement of the outcomes which were necessary for the attainment of the specific process purpose being assessed. Medi SPICE-Adept therefore needed to be process dimension centric in its focus.

Finally, the objective of undertaking a Medi SPICE-Adept assessment is not to receive formal certification or a rating, but rather to identify an organization's strengths and

weaknesses and to facilitate process improvement. Having defined the criteria which had to be met the next step was to undertake the development of Medi SPICE-Adept.

4.4 Assessing against Medi SPICE using lightweight assessment models

The RSRG have previously developed and implemented three lightweight software process assessment methods Adept [41], Med-Adept [42] and Med-Trace [43] the objective was to leverage that experience and utilize it for the development of Medi SPICE-Adept. It was in this context that work commenced on the development of Medi SPICE-Adept. It was recognized that this assessment method needed to cover more processes and provide more detailed analysis than those methods which had been previously developed. While this was the case Medi SPICE-Adept was still required to be lightweight to fulfill its purpose. The first task was to identify the initial Medi SPICE processes that would be utilized. The goal was to select a limited number of processes that would be most beneficial and relevant to industry. To achieve this, industry experts were consulted and ten processes were selected:

- Requirements Elicitation;
- System Architectural design;
- Systems Requirements Analysis;
- Software Requirements Analysis,
- Software Construction;
- Software Integration;
- Software Testing;
- Configuration Management;
- Change Request Management;
- Verification.

While these were the initial processes selected Medi SPICE-Adept will additionally provide coverage of all the Medi SPICE processes and subprocesses.

The Medi SPICE PAM had been developed for each of the initial processes which were based on best practice as outlined by the latest version of ISO/IEC 15504-5 and the specific requirements of the medical device regulations, standards, technical reports and guidance documents. As a result each process had a defined purpose and outcomes, specific practices and work products were also included for the achievement of these outcomes and purpose. Additionally, each outcome and specific practice was mapped to the regulations, standards etc. on which it was based. To facilitate the assessment each of the initial processes were evaluated and specific questions identified based on the Medi SPICE PAM. Questions relating to the current or potential use of agile and lean software methods were also identified and included. This

work was undertaken by five members of the RSRG team with extensive experience of SPI and knowledge of medical device software development and included two experts in the area of lean and agile methods. The next step was to develop the specific procedure for implementing a Medi SPICE assessment.

4.5 Implementing a Medi SPICE Assessment

Based on the RSRG's previous experience of developing and undertaking lightweight software process assessments [38] a seven stage procedure for undertaking a Medi SPICE Assessment was defined. The assessment team should normally consist of two assessors who share responsibility for conducting the assessment. The seven stages of the procedure are as follows: Prior to undertaking an assessment a preliminary meeting between the lead assessor and the company takes place. This is the first stage in the procedure and during this meeting the lead assessor discusses the main drivers for the company wishing to undertake an assessment. In this context the expectations regarding what can be realistically achieved are discussed and the procedure for undertaking the assessment is outlined. Then a schedule is developed. At the second stage the lead assessor meets with the staff and management from the company who will be participating in the assessment. Here an overview of the Medi SPICE assessment method is presented and details of what staff participation will involve. The onsite assessment is the third stage in the procedure. During the onsite assessment the lead assessor conducts interviews with relevant staff based on scripted Medi SPICE-Adept questions. The second assessor who also participates in the interviews prepares interview notes and may ask additional questions when clarification is required. Work products may also be requested and briefly reviewed at this stage. A maximum of five processes are assessed in a single day with the interviews for each process taking approximately one hour. At the fourth stage the findings report is prepared off-site based on the data gathered at stage three. Each process is reviewed in turn and where relevant particular strengths and issues (weaknesses) are identified based on the evaluation and interview notes. Suggested actions to address these issues are then outlined and discussed. The possibility for the use of appropriate agile and lean practices is also considered. These are then documented and included in the findings report. This is a joint effort between the assessors and may include other SPI and/or lean and agile experts if required. The findings report is then presented to the management and staff who took part in the assessment which is the fifth stage in the procedure. Having provided adequate time for the findings report to be read and considered by the organization at the sixth stage the contents of the report is discussed in detail with the relevant management and staff. At this point specific objectives for process improvement are collaboratively defined based on the findings report which results in the development of a process improvement plan. Given the lightweight nature of Medi SPICE-Adept improvements that offer the greatest benefits in terms of compliance, quality and the

achievement of business goals are selected for inclusion in this plan. At the seventh stage in the procedure the organization having implemented the process improvement plan have the opportunity of having the processes reassessed. Based on this, a final detailed report is prepared which highlights what has been achieved and an updated improvement plan is also provided.

5. Risk Management of IT Networks Incorporating Medical Devices

Traditionally, when medical devices were connected to a network, the network would be a proprietary network that would be provided, installed and supported by the medical device vendor. This allowed the medical device vendor to have control over configuration such as IP addressing which made support and service of the network easier. With the medical device vendor providing the network, this relieved the hospital of the responsibility of supporting life critical applications themselves. However use of proprietary networks in this way presented a number of disadvantages in that, as medical devices increasingly were designed to be incorporated into a network, the result was a proliferation of these networks resulting in the situation where large hospitals could have a large number of private networks. The maintenance of a large number of private networks is impractical and increasingly devices are being designed to be incorporated into a hospitals general IT network. General hospital IT networks are highly flexible and highly configurable. Incorporating a medical device into a general IT network can introduce additional risks that are particular to the incorporation of the device into the IT network and which may not have been considered during the design and manufacture of the device [44].

In order to address these risks, IEC 80001-1: Application of risk management for IT-networks incorporating medical devices [45] was published in 2010 which outlines the roles, responsibilities and activities that are required for the risk management of a medical IT network. IEC 80001-1 advocates a life cycle approach to risk management. The standard looks at the medical IT network from the perspective of maintaining 3 key properties of the network – Safety, Effectiveness and (Data & System) Security. Safety deals with ensuring that the device does not cause harm to the patient, the user of the device or the environment. Effectiveness is concerned with ensuring that the device continues to provide the intended result for the patient and the Responsible Organization. A Responsible Organisation is defined within the standard as an entity accountable for the use and maintenance of a medical IT network. Data & System Security ensures that information assets are reasonably protected from degradation of confidentiality, integrity, and availability. A medical IT network is defined within IEC 80001-1 as an “an IT network that incorporates at least one medical device”.

5.1 Assessment against IEC 80001-1

While IEC 80001-1 outlines the roles, responsibilities and activities that are required for risk management, there is currently no method which allows for assessment against IEC 80001-1. In order to address this, a Process Assessment Model (PAM) has been developed to allow for assessment against IEC 80001-1. The PAM was developed in accordance with the requirements for Process Assessment as described in ISO/IEC 15504-2 [46]. According to these requirements a PAM must be developed by extending a Process Reference Model (PRM) with the addition of a measurement framework. This measurement framework is described in ISO/IEC 15504-2 and contains 6 capability levels ranging from "incomplete" to "optimized".

Once the requirements for the development of PRMs and PAMs as described in ISO/IEC 15504-2 had been reviewed, it was necessary to determine an approach to the development of the PRM and PAM for assessment against IEC 80001-1. In order to do determine this approach, a review of standards similar to IEC 80001-1 was undertaken in order to determine what assessment methods were available for assessment against these standards and to determine how these assessment methods were developed. The research focused on ISO/IEC 20000-1 [47] which is a generic Service Management standard which is identified in Annex D of IEC 80001-1 as being similar to IEC 80001-1. While a medical IT network is set up to fulfill a specific purpose, it shares a number of characteristics with a general IT network [48]. Recognising this, in Annex D of IEC 80001-1 the requirements of ISO/IEC 20000 were reviewed to see if they could fulfill the requirements of IEC 80001-1. While it was recognized that IEC 20000-1 could not fulfill all of the requirements of IEC 80001-1, Annex D highlights areas where there are common processes between the two standards and areas where though the terminology is different, the underlying role, document or process is similar. The research focused on the Tudor IT Service Management Process Assessment (TIPA)[49] method which can be used to assess against ISO/IEC 20000-1 and another Service Managements standard, the Information Technology Infrastructure Library (ITIL) [50].

During the development of the TIPA assessment method it was noted that while ISO/IEC 15504-2 is clear in its requirements for process assessment in terms of the development of PRMs and PAMs, it does not provide guidance on how to transform the input or the domain requirements into the output or the PRM and PAM [51]. To address this need the TIPA transformation process, a goal oriented requirements engineering technique, was developed to give guidance ion the development of PRMs and PAMs which are consistent with the requirements as expressed in ISO/IEC 15504-2. The TIPA transformation technique also ensures that the processes within the PRM and PAM are described in a way which is consistent with ISO/IEC TR 24774 [52]

which gives guidelines for process description. Given the similarities between ISO/IEC 20000-1 and IEC 80001-1 as previously discussed, the TIPA transformation process was used in the development of the PRM and PAM for assessment against IEC 80001-1. The transformation process was used in the development of the PRM which was then extended with the addition of a measurement framework to form the PAM. The PRM & PAM for assessment against IEC 80001-1 is discussed in the next section.

5.2 IEC 80001-1 Process Reference Model & Process Assessment Model

The PRM for assessment against IEC 80001-1 contains 2 main process categories – Primary Processes and Organizational Processes. The Primary Processes category is concerned with the performance of risk management activities and contains 3 process groups which contain 9 processes in total. The process groups in the Primary Processes category are Medical IT Network Risk Management Process Group, Change Release Management & Configuration Management Process Group and finally the Live Network Risk Management Process Group. The Organizational Process category is concerned with the planning and management or risk management activities and contains a single process group called the Medical IT Network Documentation and Planning Process Group which contains 5 Processes. The PRM maintains the "Plan, Do, Check, Act" approach which is used in ISO/IEC TR 20000-4[53] (which is the PRM

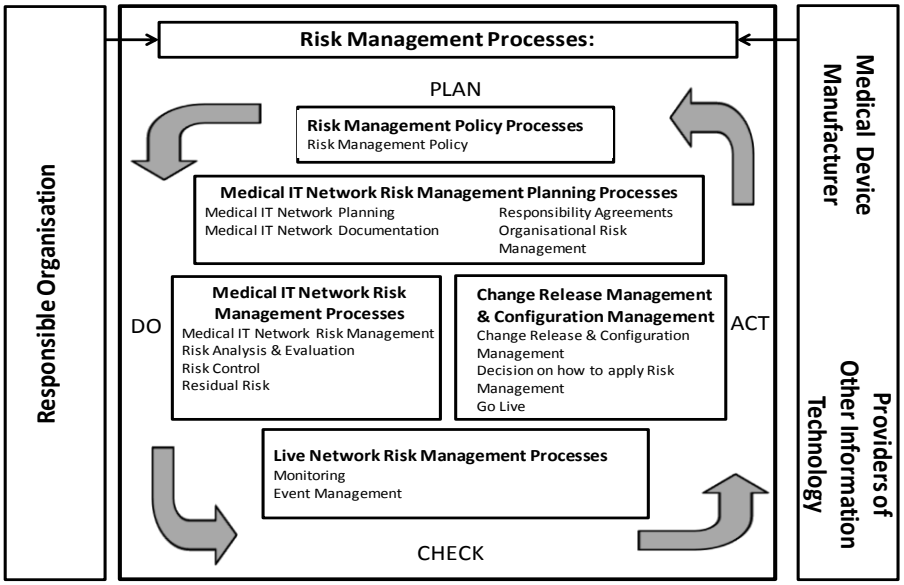

Figure 5 – IEC 80001-1 PRM Process Map

for ISO/IEC 20000-1). The 14 processes as defined in the PRM are shown below.

The descriptions of the processes shown in Figure 5 were extended to include base practices and work products which together with the addition of the measurement framework formed the PAM.

5.3 Future Validation and Development of the Assessment Framework

The next stage once complete will allow for assessment against IEC 80001-1 using an assessment method. The assessment method will be follow a staged process which will deal with aspects of the management of the assessment and which will provide a comprehensive list of questions related to each process within the PAM which will allow the assessor to establish the capability level associated with each process which will be the main stage of the assessment method. On the basis of this stage of the assessment, areas for improvement will be identified which will be communicated. A plan for these improvements will be delivered and a further assessment against this plan will be completed at a later date. Work on the development of this assessment method is ongoing.

The PRM and PAM which have been developed are currently being validated. Validation will be carried out in three ways. The PRM and PAM which are described in this chapter will be reviewed by the developers of the TIPA framework who will review the PRM and PAM in terms of their conformance with the requirements of ISO/IEC 15504-2 using experience gained during the development of a ISO/IEC 15504-2 compliant PAM for assessment against ISO/IEC 20000-1.The PAM has been raised as a new work item proposal for inclusion in the IEC 80001 family of standards. In the second stage of validation, the PAM will be reviewed by members of the international standards community, who have developed the IEC 80001-1 standard, in terms of its ability to assess against the requirements contained within IEC 80001-1. The final stage of validation will be the use of the PAM and assessment method within a hospital environment. The validated PAM and assessment method will then be used to perform a trial assessment within another hospital. The final PRM, PAM and assessment method will allow for assessment against IEC 80001-1. The PAM will be included in the IEC 80001 family of standards and as an international standard will provide an internationally recognized way to assess against the requirements as outlined in the IEC 80001-1 standard.

6. Security Assurance of Medical Devices

In the last number of years, there has been substantial advancement in the design and functionality of medical devices to offer patients a more sophisticated, reliable means

of medical care. These advancements are mainly due to the growing use of software in medical devices. With the inclusion of software in medical devices, the next step in advancement came with the introduction of interoperable and connected medical devices incorporating technology to communicate wirelessly and across networks. The advantage of this development in medical device design is that patients can now receive around the clock monitoring and real-time treatment outside the healthcare environment without a consultant present. As for the healthcare providers, these devices alleviate the need for additional resources to monitor and administer the care or treatment to their patients. The downside to this is that while these design advancements do benefit the healthcare industry and patient care in many ways, it also introduces new risks to patient safety. These are security risks, vulnerabilities and threats.

Traditionally medical devices were designed to be stand-alone devices but we see many different types of devices that communicate wirelessly and over networks in today's world with each device type presenting different security concerns. While there have been no malicious attacks on medical devices recorded to date there have been a number of controlled hacks on medical devices. Implantable medical devices (IMDs) have been targets of some of the controlled hacks in the last year or so. One such incident was at the Black Hat Security Conference in Las Vegas in 2011. The diabetic security researcher carried out a controlled hack on his own insulin pump during his presentation and gained sufficient access to allow him to increase and decrease the insulin dosage. On both occasions, there was no warning that the device had been tampered with and there was no warning that the patient could possibly die. External medical devices also pose problems with regard security. Many devices have built in

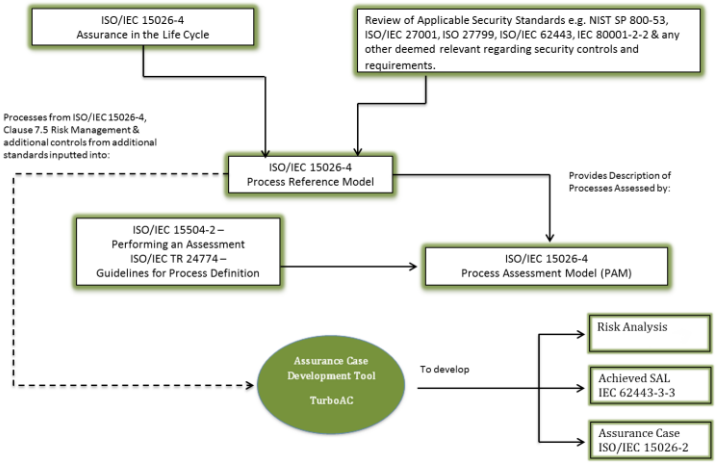

Figure 6 - Approach Overview

commercial operating systems, which were designed by software developers but, because these are widely used operating systems, they are more susceptible to malicious attacks. The other types of medical devices which are of concern are the increasingly portable medical devices and Bring Your Own Devices (BYODs). More and more practitioners are using smartphones and iPads to retrieve electronic patient health information (EPHI) in patient consultations [54].

The age of interoperability and connected medical devices has just begun and so the area of security in such devices is not fully exploited as yet by the medical device community and researchers but more worryingly by malicious attackers. As of yet, there is no formal governance for the assessment of such medical devices process capability or for the establishment of medical device product capability with regard security. Over the last number of years there has been a lot of concern among the medical device community in regard to interoperable and connected medical devices and their communication abilities in terms of security vulnerabilities, threats and risks. This has been reflected through the many publications, technical reports and guidance documents released such as IEC/TR 80001-2-2 [55]. In August 2012, the Government Accountability Office (GAO) published a report [56] that clearly indicated the need for the FDA to enhance their assessment of security medical devices and concluded with the recommendation that the FDA address these issues.

This section discusses research that sets out to address this problem by establishing a methodology to assure the security of connected and interoperable medical devices on IT networks. Figure 6 outlines the architecture of the solution that is discussed in more detail in the following sections.

6.1 Establishing Meaningful Security Controls

The first step in developing this model is to conduct a comprehensive review of existing security standards and guidance documents. These will include ISO/IEC 27001 [57], ISO/IEC 27799 [58], ISO 15408 [59], IEC 62443-3-3 [60], and NIST SP 800-53 [61]. Each of these standards and guidance documents similarly present security classes and controls. A list of applicable security controls to be addressed during the development risk assessment process will be derived from the previously mentioned sources through the use of expert opinion. The FDA and carefully selected expert users will validate this derived set of controls. The outcome of this will be a published technical report with a cross-standard mapping of security controls to be considered in regard to interoperable medical devices communicating over an IT network.

IEC/TR 80001-2-2 [55] is a technical report that sets out to promote the communication of security controls, needs and risks of medical devices to be incorporated into IT

networks between Medical Device Manufacturers (MDMs), IT vendors and Healthcare Delivery Organisations (HDOs). This technical report presents 20 security capabilities (See Table 6.1). It is anticipated that the upcoming technical report outlining a set of mandatory security controls will be reflected in a new revision of IEC 80001-2-2 should the technical report highlight gaps with the existing 20 security capabilities.

6.2 Process Assurance

This research presents a methodology to address security concerns in the medical device domain specifically looking at networked medical devices. As a way to assure medical devices, the methodology takes an approach from the development process capability and also the final product quality assurance. In establishing a process capability level for the development of a medical device, MDMs gain better control over their processes and output. This also proves beneficial from a compliance assessment point of view when there are clearly defined and measurable processes in place.

Table 6.1 - IEC/TR 80001-2-2 Capabilities

	Security Capability	Code
1	Automatic Logoff	ALOF
2	Audit Controls	AUDT
3	Authorization	AUTH
4	Configuration of Security Features	CNFS
5	Cyber Security Product Upgrades	CSUP
6	Data Backup and Disaster Recovery	DTBK
7	Emergency Access	EMRG
8	Health Data De-Identification	DIDT
9	Health Data Integrity and Authentication	IGAU
10	Health Data Storage Confidentiality	STCF
11	Malware Detection/Protection	MLDP
12	Node Authentication	NAUT
13	Person Authentication	PAUT
14	Physical Locks on Device	PLOK
15	Security Guides	SGUD
16	System and Application Hardening	SAHD
17	Third-Party Components in Product Lifecycle Roadmaps	RDMP
18	Transmission Confidentiality	TXCF
19	Transmission Integrity	TXIG
20	Unique User ID	UUID

For the problem solution a PAM will be used. These are widely used in software /I.T. businesses to measure the capability of an organization to achieve particular processes. The two most widely used models are CMMI [62] and the ISO/IEC 15504 family . We have selected the international standard for process assessment, ISO/IEC 15504-2 [63] that sets out requirements for defining process assessment models and for performing process assessments.

In using this standard, the two major outcomes will be a PRM and PAM. A PAM contains two dimensions; these are the Process Dimension and the Capability Dimension. The Process Dimension is developed from an external PRM that provides the processes for assessment in terms of 'Purpose' and 'Outcome'. The PAM expands the PRM with the use of Performance Indicators called Base Practices and Work Products. Work Products are both the inputs and outputs to each process and the Base Practices describe the process activities that convert these inputs to process outputs.

The Capability Dimension is based upon six capability levels ranging from Level 0 'Incomplete' to Level 5 'Optimizing'. Achievement of a capability level is based upon the achievement of Process Attributes (of which there are a total of nine) for Capability Levels 1 through to 5. A Process Attribute is the measurement characteristic of each process. For example, in achieving capability level 1, 'Performed', the Process Attribute is Process Performance, for capability level 2, 'Managed', one Process Attribute is Process Management, and so on.

ISO/IEC 15504-6 [64] describes an exemplar PAM and will form the foundation of the model as it utilizes ISO/IEC 15288 [65] as the PRM. This international standard (ISO/IEC 15288) has been selected as it addresses system life cycle processes. As these networked medical devices can contain a combination of hardware, software, people, processes etc. it is deemed the most suitable foundation for the PAM. ISO/IEC 15288 is a framework to improve the communication and cooperation among parties that design, develop, use and maintain systems. It covers the entire life cycle of systems development from concept straight through to retirement and also including acquisition and supply processes.

Due to the criticality of networked medical devices, this PAM will be extended to include additional processes from ISO/IEC 15026-4 [66]. This is yet another international standard specifically addressing assurance in the life cycle. ISO/IEC 15026-4 is mainly utilized where additional assurance for a critical property, such as dependability, safety or security, is required for a system or software. The standard is used as an add-on to an already existing life cycle process standard such as that of ISO/IEC 15288. Therefore, this extension of the PAM lines up with ISO/IEC 15504-6 building upon existing processes addressed here.

Finally, the PAM will be further extended to include the 20 security capabilities presented in IEC/TR 80001-2-2 (Table 6.1). This will be included in the system risk management process. In developing a networked medical device, MDMs will be required to specifically address all 20 security capabilities and determine which of those are applicable to the medical device. Justification of non-applicable security capabilities will be required.

6.3 Product Assurance

Having established the process assurance for the development of medical devices to be incorporated into an IT network, the research will further assure the medical device by addressing the security assurance of the deliverable. This means assurance starts at the beginning of the acquisition process between the HDO and the MDM. In support of IEC/TR 80001-2-2, the outcome of this methodology will be the communication of the target security capability requirement of a device by the HDO to the MDM and then a justification of an achieved security capability requirement from the MDM to the HDO. This is the first input in the product assurance strategy of this model. In communicating this information a vector schema will be utilised. Table 6.1 presents the security capabilities. In order to better define the requirements of the HDO this will be further broken down. Each security capability will have a sub set of requirements. Table 6.2 shows an example break down for security capability *Automatic Logoff* (ALOF). Each of the security capability requirements will be displayed on a vector as follows:

$$T\text{-}ALOF = \{1, 0, 1, 1, 0\}$$

This vector indicates the HDO's target security capability requirement (T) for *Automatic Logoff* to have in place the sub requirements ALOF.01, ALOF.03 and ALOF.04. Zero on the vector indicates that that particular sub requirement is not required. This format will be used for all security capabilities and their sub requirements. During the risk management process, required security controls will be identified. These controls will be the second input to the product assurance element of this methodology. This will be achieved through the utilisation of a tool. This tool will be used to further build on the risk management processes. Each security capability will be addressed in the FMEA or risk analysis builder within the tool. In turn the tool will automatically build an assurance case and outline in detail the evidence gathered to support the achievement of each security assurance level. To date, assurance cases have mainly be used within in the medical device domain to address safety and are recommended to MDMs as part of the infusion pump initiative [67]. A similar type methodology will be adapted here addressing security as the critical property.

Table 6.2 - Security Capability Requirements for ALOF

Implementation Identifier	Capability
ALOF.01	A screensaver starts automatically 5 minutes after last key-stroke/mouse movement operation
ALOF.02	The screensaver clears all displayed health data from the screen.
ALOF.03	The screensaver does not log-off the user / does not terminate the session.
ALOF.04	User has to log-in after occurrence of the screensaver
ALOF.05	The user-session terminates automatically 60 minutes after last keystroke/mouse movement/touchscreen operation.

ISO/IEC 15026-2 [68] defines requirements for the structure and content of an assurance case. An assurance case is a body of evidence organized into an argument demonstrating some claim that a system holds i.e. is acceptably secure. An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability. Security assurance cases are often compared with a legal case where there are two elements to the case, the argument and the evidence to support a claim. For an assurance case to be effective it must satisfy the following points:

- Must make a claim or set of claims about a property of a system;
- Produce the supportive evidence;
- Provide a set of arguments;
- Make clear the assumptions and judgements underlying the arguments;
- Associate different viewpoints and level of detail.

Upon completion of the risk management process, the MDM will have established the achieved security capability requirements for the product and developed a security assurance case with proof, through evidence, of the security assurance of the networked medical device. This will be detailed on the security assurance case, which will be held by the MDM for third party regulatory assessment. It may be the communication article between the MDM and the HDO in which, the HDO IT Administration staff may include in their risk management file should the medical device be installed into their IT network. Upon completion of the security assurance case, the MDM will then follow the same format as the HDOs to highlight the security capability requirements as was done at the start of the acquisition process by the HDO. They too will use a vector format to present the achieved security capability requirements of the medical device. Using the previous example, the achieved security capability requirements (A)

for *Automatic Logoff* could be as shown below. This example shows that ALOF.02, although not stated as a target security capability requirement, is also shown as being implemented. Again, for each of the 20 security capabilities, the achieved security capability requirements will be communicated to the HDO.

$$A\text{-}ALOF = \{1, 1, 1, 1, 0\}$$

7. Conclusions and Summary

Medical devices have a direct impact on an individual's wellbeing. Therefore to ensure the safe and reliable performance of medical devices regulations have been put in place. These regulations dictate what information a medical device manufacturer should produce as evidence as to how safe the device is. However, regulatory bodies do not provide comprehensive guidance as to how this objective evidence must be produced.

Traditionally, a medical device was considered a hardware device with a software component. In this case, the safety of the device could be proved through the hardware functioning of the device. However, recent changes to regulations now mean that a medical device may consist solely of software. As a result there is no hardware element which can produce evidence to support the safety of the device. To overcome this, medical device software organizations are recommended to follow the latest state of the art development processes and standards such as IEC 62304; however, IEC 62304 has not been updated since the recent changes to regulations and as a result it is not sufficiently comprehensive to provide coverage of all of the necessary stages of development.

To fill this void and to draw upon the software industry best practices, Medi SPICE is currently under development by the RSRG. Medi SPICE will act as a single point of reference for medical device software organizations when developing regulatory compliant software. Medi SPICE combines international regulations, medical device software standards and software development best practices to a single point. Medi SPICE aims to provide coverage of all of the stages of medical device software development and maintenance.

While Medi SPICE is under development to respond to the needs of the medical device software industry an emerging area causing concerns regarding medical device safety, is the connecting of medical device to networks. This creates a new level of concern with regards to the impact other devices on the same network will have on the medical device and also the potential security implications of a device being accessed

by an unauthorized user. To address these risks two frameworks are currently under development by the RSRG which aim to address these risks.

IEC 80001-1 takes a life cycle approach to risk management of IT networks which incorporate medical devices. The incorporation of a device into an IT network can introduce risks that may not have been considered during the design and manufacture of the medical device. While HDOs may perform risk management activities, there is no method that exists to allow a HDO to assess the capability of their risk management processes against the requirements of IEC 80001-1 which outlines risk management activities which are specific to the incorporation of a medical device into an IT network. Research to date has focused on the development of a PRM and PAM for assessment against IEC 80001-1. The PRM and PAM have been raised as a new work item proposal and will be part of a technical report within the IEC 80001-1 family of standards. When an assessment is performed using the IEC 80001-1 PAM, this will allow the HDO to assess the capability of risk management processes and will provide an insight into areas where process improvement can take place and a higher capability level can be achieved. IEC/TR 80001-2-2 defines the security capabilities that a MDM or IT vendor must communicate to the HDO in order to enhance knowledge of security risks and controls the HDO IT administration staff should consider and vice versa. The outcome of this research will provide many benefits for both the HDOs and the MDMs. For the HDOs some of the benefits will include:

1. A common framework to assist in the selection of suppliers through process capability levels.
2. Guidance for the communication of medical device security needs.
3. Better understanding of the security capability of the devices.
4. Knowledge of the security assurance of the device through the use of a vector for the target and achieved security capability requirements.

The MDMs also benefit through:

1. Better knowledge of the capability level of their life cycle processes with clear insight for process improvement.
2. A method to add additional assurance to their processes through the extension of the PRM using the international standard ISO/IEC 15026-4, Assurance in the Life Cycle.
3. A focused security risk management process with the inclusion of a defined set of security capabilities and further requirements.
4. A method and tool for the automatic development of security assurance cases

Currently, there is no methodology to address both the development processes and the product capabilities of medical devices in terms of security. Hence, it is envisaged that the output of our research will positively impact the medical device domain in both the EU and the US by building awareness of security vulnerabilities, threats and related risks between the HDO and the MDM [69].

Whilst the research presented in this chapter is on-going, there is a clear need for the models which have been presented. This need has been identified through collaboration with the medical device industry, the standards community and regulatory bodies such as the FDA. Once completed, each of the models presented will have a direct impact on the safe and reliable performance of medical devices which are also secure.

References

1. I. Lee and O. Sokolsky, "Medical cyber physical systems," presented at the 47th Design Automation Conference, Anaheim, California, 2010.
2. R. K. Bhaskar and G. Somu, "Adoption Of Information Technology (IT) In Healthcare Delivery- Experience At A Tertiary Level Hospital " *International Journal of Medical Informatics,* vol. 5, 2011.
3. L. Ash, *The Web Testing Companion: The Insider's Guide to Efficient and Effective Tests*. New York: John Wiley & Sons, 2003.
4. N. Leveson, *Safeware: System Safety and Computers*: Addison Wesley, 1995.
5. ISO, "*ISO/IEC 13485:2003 Medical devices -- Quality management systems -- Requirements for regulatory purposes*," ed. International Organisation for Standards - Geneva, Switzerland, 2003.
6. ISO, "*ISO/IEC 14971:2007 Medical devices -- Application of risk management to medical devices*," ed. International Organisation for Standards - Geneva, Switzerland 2007.
7. AAMI, "ANSI/AAMI/IEC 62304, Medical device Software - Software life cycle processes," ed. Association for the Advancement of Medical Instrumentation, 2006.
8. FDA, "Title 21--Food and Drugs Chapter I --Food and Drug Administration Department of Health and Human Services subchapter h--Medical Devices part 820 Quality System Regulation," ed: *U.S. Department of Health and Human Services*, 2007.
9. *Guidance for Industry, Third parties annd Food and Drug Administration Staff, Medical Device ISO 13485:2003 Voluntary Audit Report Submission Program*, 2012.
10. *Medical Devices Guidance Document - Qualification and Classification of stand alone software MEDDEV 2.1/6*, 2012.

11. E. S. Crumpler and H. Rudolph, "FDA Software Policy and Regulation of Medical Device Software," *Food and Drug Law Journal*, vol. 52, 1997.
12. *Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007*, 2007.
13. Health Canada. (2011, 10/01/2013). *Software Regulated as a Medical Device* Available: http://www.hc-sc.gc.ca/dhp-mps/md-im/activit/announce-annonce/md_qa_software_im_qr_logicels-eng.php
14. FDA, "21 CFR Part 880 Medical Devices; Medical Device Data Systems Final Rule.," *Federal Register* vol. 76, pp. 8637 - 8649, 2011.
15. M. McHugh, F. McCaffery, and V. Casey, "US FDA releases final rule on Medical Device Data Systems - What does this mean for device manufacturers," *Journal of Medical Device Regulation*, vol. 8, pp. 35-40, 2011.
16. M. Klumper and E. Vollebregt, "The Regulation of Software for Medical Devices in Europe," *Journal of Medical Device Regulation*, vol. 7, pp. 5-13, 2010.
17. M. McHugh, F. McCaffery, and V. Casey, "Changes to the International Regulatory Environment," *Journal of Medical Devices*, vol. 6, 2012.
18. *Commission communication in the framework of the implementation of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (Publication of titles and references of harmonised standards under the directive)*, 2010.
19. *FDA Design Control Guidance for Medical Device Manufacturers*, 1997.
20. FDA, "General Principles of Software Validation: Final Guidance for Industry and FDA Staff," ed: *Centre for Devices and Radiological Health*, 2002.
21. FDA, "Draft Guidance for Industry and Food and Drug Administration - Mobile Device Applications," ed: *Centre for Devices and Radiological Health*, 2011.
22. FDA, "Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software use in Medical Devices," ed: *U.S. Department of Health and Human Services*, 1999.
23. P. Jordan, "Standard IEC 62304 - Medical Device Software - Software Lifecycle Processes," presented at the The Institution of Engineering and Technology Seminar on Software for Medical Devices London, 2006.
24. Minister of Justice, "Medical Device Regulations SOR/98-282," in *http://laws-lois.justice.gc.ca*, ed, 2012.
25. D. M. Zuckerman, P. Brown, and S. E. Nissen, "Medical device recalls and the fda approval process," *Archives of Internal Medicine*, vol. 171, pp. 1006-1011, 2011.

26. P. L. Jones, J. Jorgens, A. R. T. Jr, and M. Weber, "Risk Management in the Design of Medical Device Software Systems," *Biomedical Instrumentation & Technology: July 2002*, vol. 36, pp. 237-266, 2002.
27. C. Denger, R. L. Feldman, M. Host, C. Lindholm, and F. Schull, "A Snapshot of the State of Practice in Software Development for Medical Devices," presented at the First International Symposium on Empirical Software Engineering and Measurement, 2007. ESEM 2007, Madrid, 2007.
28. *Capability Maturity Model® Integration for Development Version 1.2*, 2006
29. ISO/IEC 15504-5:2006, "Information technology - Process Assessment - Part 5: An Exemplar Process Assessment Model," ed. Geneva, Switzerland: ISO, 2006.
30. F. Mc Caffery and A. Dorling, "Medi SPICE Development," *Software Process Maintenance and Evolution: Improvement and Practice Journal* vol. 22 pp. 255 – 268, 2010.
31. Automotive SIG, "Automotive SPICE Process Assessment V 2.2," ed, 21 August 2005.
32. ISO/IEC 12207:2008, "Systems and software engineering - Software life cycle processes," ed. Geneva, Switzerland: ISO, 2008.
33. US FDA, "21 CFR Part 820 Quality System Regulations," *Code of Federal Regulations, Title 21*, vol. 8, Revised April 1, 2011
34. F. Mc Caffery, A. Dorling, and V. Casey, "Medi SPICE: An Update," in *International Conference on Software Process Improvement and Capability Determinations (SPICE)*, Pisa, Italy, 2010, pp. 195 -198.
35. V. Casey, "Virtual Software Team Project Management," *Journal of the Brazilian Computer Society*, vol. 16, pp. 83 – 96, August 2010 2010.
36. ISO/IEC 15504-2:2003, "Software engineering - Process assessment - Part 2: Performing an assessment," ed. Geneva, Switzerland: ISO, 2003
37. F. Mc Caffery and A. Dorling, "Medi SPICE: An Overview," in *International Conference on Software Process Improvement and Capability Determinations (SPICE)*, Turku, Finland, 2009, pp. 34 - 41.
38. F. Mc Caffery, V. Casey, and M. Mc Hugh, "How Can Software SMEs become Medical Device Software SMEs," in *European Systems & Software Process Improvement and Innovation Conference, (EuroSPI)*, Copenhagen 2011, pp. 247 – 258.
39. F. Mc Caffery, J. Burton, V. Casey, and A. Dorling, "Software Process Improvement in the Medical Device Industry," in *Encyclopedia of Software Engineering*. vol. 1, P. Laplante, Ed., ed New York: CRC Press Francis Taylor Group, 2010, pp. 528 - 540.
40. O. Cawley, I. Richardson, and X. Wang, "Medical Device Software Development - A Perspective from a Lean Manufacturting Plant," in *11th International SPICE Conference on Process Improvement and Capability dEtermination 2011*, Dublin City University, Ireland,, 2011, pp. 84 – 96.

41. F. Mc Caffery, I. Richardson, and G. Coleman, "Adept – A Software Process Appraisal Method for Small to Medium-sized Irish Software Development Organisations," in *European Systems & Software Process Improvement and Innovation (EuroSPI 2006)*, Joensuu, Finland, 2006, pp. 7.12-7.21.
42. F. Mc Caffery and V. Casey, "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, pp. 1.9 - 1.16.
43. V. Casey and F. Mc Caffery, "A lightweight traceability assessment method for medical device software," *Journal of Software Maintenance and Evolution Research and Practice*, October 2011 2011.
44. T. Gee. (2008, 27/1/2012). *Medical Device Networks Trouble Industry*. Available: http://medicalconnectivity.com/2008/12/18/medical-device-networks-trouble-industry/
45. IEC, "IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities," ed. Geneva, Switzerland: International Electrotechnical Commission, 2010.
46. ISO/IEC, "ISO/IEC 15504-2:2003 - Software engineering — Process assessment — Part 2: Performing an assessment," ed. Geneva, Switzerland, 2003.
47. ISO/IEC, "ISO/IEC 20000-1:2011 - Information technology —Service management Part 1: Service management system requirements," ed. Geneva, Switzerland, 2011.
48. M. Janssen and R. Schrenker, "Guidelines From 80001: Maintaining a Medical IT Network," *Biomedical Instrumentation & Technology*, vol. 45, pp. 295-299, 2011/07/01 2011.
49. B. Barafort, V. Betry, S. Cortina, M. Picard, M. St Jean, A. Renault, O. Valdés, and P. R. C. H. Tudor, *ITSM Process Assessment Supporting ITIL : Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification* vol. 217. Zaltbommel, Netherlands: Van Haren, 2009.
50. The Cabinet Office, "ITIL 2011 - Summary of Updates," ed. Norfolk, England: Crown Copyright, 2011.
51. B. Barafort, A. Renault, M. Picard, and S. Cortina, "A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000," presented at the SPICE Nuremberg, Germany, 2008.
52. ISO/IEC, "ISO/IEC TR 24774:2010 - Systems and software engineering — Life cycle management — Guidelines for process description," ed. Geneva, Switzerland, 2010.

53. ISO/IEC, "ISO/IEC TR 20000-4:2010 - Information technology — Service management - Part 4: Process reference model," ed. Geneva, Switzerland, 2010.
54. DHS, "Attack Surface: Healthcare and Public Heath Sector," 2012.
55. IEC, "TR 80001-2-2 - Application of risk management for IT-networks incorporating medical devices - Guidance for the disclosure and communication of medical device security needs, risks and controls," ed: International Electrotechnical Committee,, 2011, p. Page 30.
56. Government Accountability Office, "Medical Devices, FDA Should Expland Its Consideration of Information Security for Certain Types of Devices," 2012.
57. ISO/IEC, "27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements," ed, 2005.
58. ISO, "EN ISO 27799:2008 Health informatics. Information security management in health using ISO/IEC 27002," ed, 2008.
59. ISO/IEC, "15408-2 Information Technology - Security Techniques - Evaluation Criteria for IT Security," in *Security Functional Components*, ed, 2008.
60. IEC, "62443-3-3 -- Security for industrial automation and control systems - Network and system security -- System security requirements and security assurance levels Introductory," ed, 2011.
61. NIST, "800-53 Recommended Security Controls for Federal Information Systems and Organisations," U. S. D. o. Commerce, Ed., Revision 3 ed, 2009.
62. SEI, "CMMI for Development," 2006.
63. ISO/IEC, "15504-2: 2003 Software Engineering - Process Assessment - Performing an Assessment," ed, 2003.
64. ISO/IEC, "15504-6:2008 Information technology — Process assessment — An exemplar system life cycle process assessment model," ed, 2008.
65. ISO, "Systems and software engineering -- System life cycle processes," ed, 2008.
66. ISO/IEC, "15026-4: Systems and Software Engineering - Systems and Software Assurance - Assurance in the Life Cycle," ed, 2012.
67. FDA, "Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions - Draft Guidance," ed, 2010.
68. ISO/IEC, "15026-2: 2011 Systems & Software Engineering, Systems & Software Assurance, Part 2: Assurance Case," ed, 2011, p. 28.
69. A. Finnegan, F. McCaffery, and G. Coleman, "Development of a process assessment model for assessing security of IT networks incorporating medical devices against ISO/IEC 15026-4," presented at the Healthinf 2013, Barcelona, Spain.

Index terms (alphabetically):