Transforming Requirements of IEC 80001-1 into an ISO/IEC 15504-2 Compliant Process Reference Model and Process Assessment Model

Silvana Togneri MacMahon, Fergal Mc Caffery, Frank Keenan

Regulated Software Research Centre, Department of Computing and Mathematics
Dundalk Institute of Technology, Co. Louth Ireland
{Silvana.MacMahon, Fergal.McCaffery, Frank Keenan}@dkit.ie

Abstract

Efficiencies in patient care can be achieved through interoperability of medical devices. Patient safety is the key concern during the design and manufacture of medical devices with medical devices being subject to stringent regulation in the region in which the device is to be marketed. However, with medical devices increasingly being designed to be incorporated into an IT network, the process of networking the device can introduce risks that may not have been considered during the design and manufacture stage. IEC 80001-1 was developed to address the risks associated with the incorporation of a medical device into an IT network. This paper presents how the requirements of IEC 80001-1 were used to develop a Process Reference Model (PRM) and Process Assessment Model (PAM) which are compliant with the requirements for PRMs and PAMs as outlined in ISO/IEC 15504-2.

Keywords

IEC 80001-1, ISO/IEC 15504-2, ISO/IEC 20000-1, Process Assessment, Risk Management, Medical IT Networks

1 Introduction

In 2003 and 2004, the FDA received reports of a cluster of cyber-attacks on hospitals. The attacks acted as a catalyst for the FDA to produce cyber security guidance for medical device manufacturers for networked medical devices containing off the shelf software [1]. Having developed this guidance to address the cyber security risks, it was recognized that the wider area of risk management of networked medical devices needed to be addressed in a more comprehensive way. Traditionally if a medical device was to be incorporated into a network, the device manufacturer would provide the device and the network. This led to a situation where a hospital could have a plethora of self-contained private networks. In order to allow true interoperability of devices and achieve efficiencies in patient care, medical devices are increasingly being developed to be incorporated into the general IT network of the Healthcare Delivery Organisation (HDO). These networks can carry traffic from life critical patient information to general email traffic. The incorporation of a medical device into the HDOs general network creates a medical IT network which can introduce risks that may not have been considered during the design and manufacture of the device [2] . To address the risks which are specific to the incorporation of a medical device into an IT network, it was recognized that guidance would need to be addressed not only to the manufacturer of the device, but also to the HDO who are responsible for the establishment and maintenance of the medical IT network (referred to in the standard as Responsible

Organisations (RO)) and also to the providers of the HDO networks and other information technology. Guidance in this area would need to focus on promoting a high level of communication among these groups, but also among the various risk management stakeholders within these groups such as IT and clinical staff within a HDO [2]. This was to be the origins of IEC 80001:1 2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities [3]. Section 2 of this paper discusses the requirements as described in IEC 80001-1. Section 3 of this paper discusses the development of the approach to the PRM and PAM while Section 4 discusses the step by step approach of how the requirement of IEC 80001-1 were transformed into the resultant ISO/IEC 15504-2:2003 [4] compliant PRM and PAM. Section 5 presents the conclusions of this paper and future work to be carried out in this area.

2 IEC 80001-1 – Application of Risk Management for IT Networks Incorporating Medical Devices

IEC 80001-1 addresses 3 key properties of a medical IT network – Safety, Effectiveness and (Data and System) Security. Safety is freedom from unacceptable risk of physical injury or damage to the health of the patient or the user of the device or damage to property or the environment. Effectiveness focuses on the ability of the networked device to provide the intended result both for the patient and for the RO. Data and System Security ensures that information assets are reasonably protected from degradation in terms of confidentiality, integrity and availability. IEC 80001-1 takes a lifecycle approach to risk management and applies when a medical IT network is established, when a medical device is added or removed from a network or during any modification or maintenance activities. The lifecycle approach requires the appointment of an appropriately qualified medical IT network risk manager who will ensure that a risk management policy is established and documented and that all risk management activities throughout the lifecycle of the network are carried out in accordance with the risk management policy. All documentation which is produced during the performance of risk management activities must be maintained within the medical IT network risk management file. Roles and responsibilities for each of the stakeholder groups involved in the performance of risk management activities are detailed within IEC 80001-1.While IEC 80001-1 provides guidance on the performance of risk management activities, there is no method available which can be used to allow ROs to assess the capability of their risk management practices with regard to the requirements of IEC 80001-1. Our research to date has focused on the development of a PRM and PAM for IEC 80001-1.

3 Approach to the Development of the PRM and PAM

To develop the PRM and PAM for IEC 80001-1, a review of the following areas was undertaken:

- A detailed review of the requirements of IEC 80001-1
- A review of Process Assessment standards focusing on ISO/IEC 15504-2 and ISO/IEC 15504-5 [5]
- A review of Process Assessment models that have been developed to assess against similar standards and how they were developed

The approach to the review of the requirements of IEC 80001-1 is detailed in section 4 below which was undertaken using the Tudor IT service management Process Assessment (TIPA) [6] transformation process. The TIPA transformation process is a goal oriented requirements engineering technique which was developed by CRP Henri Tudor to develop the TIPA framework which is used to assess service management processes. The TIPA transformation process provides guidance on how to transform domain requirements into PRMs and PAMs which are compliant with the requirements of ISO/IEC 15504-2 and ISO/IEC TR 24774 [7]. TIPA can be used to assess the capability of Service Management processes against the requirements of ISO/IEC 20000-1 [8] or the IT Infrastructure Library (ITIL) [9]. The TIPA transformation process was analysed during a review of models which have been developed for similar standards for its ability to be applied to the requirements of IEC 80001-1.

The TIPA transformation process has been used for the development of the PRM and PAM for IEC 80001-1 due to the similarities between IEC 80001-1 and ISO/IEC 20000-1 which are identified in Annex D of IEC 80001-1. Both IEC 80001-1 and ISO/IEC 20000-1 take a lifecycle approach to addressing the requirements of the standard. Annex D of IEC 80001-1 details process areas which are common to both standards such as "Configuration Management" and also highlights areas where while the terminology appears to be different the underlying role, document or process is similar. The TIPA transformation process is discussed in detail in section 4

4 Development of the PRM and PAM using the TIPA transformation process

4.1 The TIPA transformation Process

The TIPA transformation process is a goal oriented requirements engineering technique. The TIPA transformation process was developed in recognition of the fact that while ISO/IEC 15504-2 is detailed in its description of the requirements for PRMs and PAMs, it does not provide guidance on how to transform the input - the domain requirements into the output – the PRM and PAM [10]. The transformation process advocates identifying elementary requirements and organising these requirements into requirement trees. These requirement trees are then then oriented around the business goals to which they are related to form goal trees. The transformation process uses the requirements of ISO/IEC 15504-2 [4] combined with the requirements of ISO/IEC TR 24774 to develop the final PRM and PAM. ISO/IEC TR 24774 Systems and software engineering - Lifecycle management - Guidelines for process description is a standard which provides guidelines for the elements used most frequently in describing a process as a means to ensuring consistency in standard process reference models. The guidelines expressed in this standard can be applied to any process model developed for any purpose.

The steps in the TIPA transformation process are summarised below:

1. Identify elementary requirements in a collection of requirements.
2. Organise and structure the requirements.
3. Identify common purposes upon those requirements and organise them towards domain goals.
4. Identify and factorise outcomes from the common purposes and attach them to the related goals.
5. Group activities together under a practice and attach it to the related outcomes.
6. Allocate each practice to a specific capability level.
7. Phrase outcomes and process purpose. (Apply ISO/IEC TR 24774 guidelines)
8. Phrase the Base Practices attached to the Outcomes. (Apply ISO/IEC TR 24774 guidelines)
9. Determine Work Products among the inputs and outputs of the practices.

The TIPA transformation process was used in the development of the PRM and PAM which will be discussed in the next two sections of this paper.

4.2 Development of the PRM

To provide a template to inform the development of the PRM for IEC 80001-1, the PRM for ISO/IEC 20000-1 which is contained in ISO/IEC TR 20000-4 [11] was reviewed. The document was reviewed to assess if the set of processes contained within the PRM for ISO/IEC 20000 could be used to assess against IEC 80001-1. While both standards follow a lifecycle approach, the processes detailed within ISO/IEC 20000-4 do not adequately address the aspects of risk management that are particular to the incorporation of a medical device into an IT network. On this basis, ISO/IEC 20000-4 was used to inform the structure of the PRM for IEC 80001-1 while not using the same set of processes. In reviewing ISO/IEC 20000-4, it was clear that the lifecycle approach of using a "Plan, Do, Check, Act" ap-

proach, as used in ISO/IEC 20000-4, could also be used to address the lifecycle approach advocated in IEC 80001-1. This approach has been maintained as illustrated in Figure 1.0.

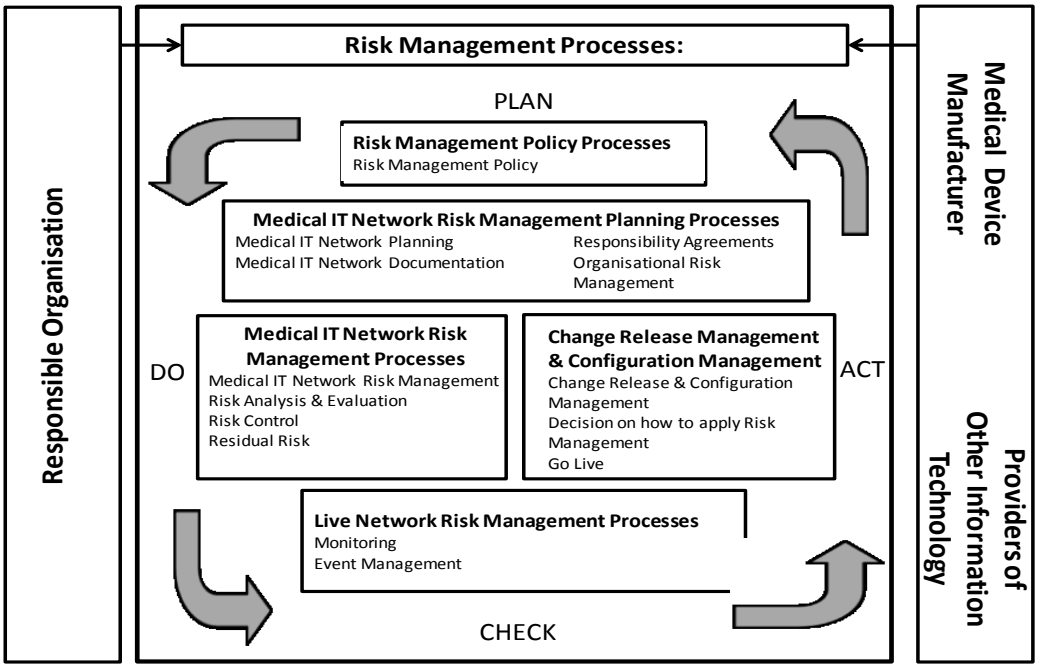

Figure 1.0 IEC 80001-1 Processes

Using the ISO/IEC 20000-4 as a template, the next stage of the development of the PRM was to structure the requirements according to the TIPA transformation process. Step 1 of the transformation process requires that elementary requirements are identified within the collection of requirements. In order to isolate elementary requirements, IEC 80001-1 was reviewed line by line and each item that was considered to be a requirement was identified and placed in a requirement catalogue. Elementary requirements have a single verb, object and complement and do not contain conjunctions. One hundred and sixty one requirements were initially identified. In order to maintain traceability, the source of each requirement was noted making reference to the section of the standard and the line number. The requirements catalogue was updated as required to ensure that only requirements that would form the PRM were included. For example initially requirements were noted that prescribed that certain actions should be carried out by the holder of a specific role. However these requirements had to be updated in order to comply with the requirements of ISO/IEC 15504-2 that requires that processes within the PRM are defined in term of the purpose and the outcome of the process and are not concerned with who performs the process.

Once all elementary requirements had been identified, the next step in the TIPA transformation process is to organize and structure the requirements. The process groups within ISO/IEC 20000-4 were reviewed to understand if these groups could also be used to structure the requirements for IEC 80001-1. While there are some process areas which are common to both standards (e.g. Release Management and Configuration Management), the structure of the processes needed to be adapted to take into account that IEC 80001-1 solely contains requirements for risk management activities throughout the lifecycle while risk management is a single process in the lifecycle approach to Service Management within the ISO/IEC TR 20000-4 PRM. Various approaches were taken to the organization of the requirements. The approach that was considered most suitable was to follow the structure of the IEC 80001-1 standards and to use the different sections of the standard to isolate the domain goals which would eventually form the processes. The domain goals informed the definition of the process purpose. In structuring the requirements in this way, step 3 of the transformation was completed simultaneously. The requirements of ISO/IEC TR 24774 were also considered during this stage and process descriptions were formulated accordingly.

Having defined the processes and process purpose through steps 1, 2 and 3, step 4 focused on the definition of the outcomes to be attached to each of the identified process purposes. A process outcome is a measurable, tangible technical or business result that is produced as a result of the performance of the process. In order to ensure the completeness of the list of outcomes associated with any process, the complete set of outcomes were reviewed to ensure that the achievement of all of the

outcomes would result in the fulfillment of the process purpose. This step was completed in conjunction with step 7 of the transformation process which ensures that outcomes and purposes of the process are phrased in a manner which is compliant with the requirements of ISO/IEC TR 24774. The completion of steps 1, 2, 3, 4 and 7 were necessary for the development of the PRM. The remaining steps of the transformation process are associated with the development of the PAM.

4.3 Development of the PAM

In order to develop the PAM for IEC 80001-1, the process within the PRM are extended with the addition of a measurement framework. This framework consists of 5 levels which range from “Incomplete“ to “Optimising“ and is defined in ISO/IEC 15504-2. In order to be able to make an assessment against this measurement framework, the remaining steps of the TIPA transfomation process were carried out to complete the development of the PAM. Step 5 of the TIPA transformation process consists of grouping activities under a practice. In order to complete this step, the process outcome and purpose were reviewed and a practice was defined that would result in the production of each outcome. Practices consist of base practices and generic practices. A base practice is an activity that addresses the purpose of a particular process. Base practices are also process performance indicators that indicates the extent of achievement of the process purpose and process outcomes. Generic practices are the principal indicators of process capability and practices that are established to support the process performance as it is characterized at level 1.

Once the practices had been identified, to complete step 6, each of the identifed practices was reviewed and was assigned to a specific capability level. This was done by reviewing the outcome of each parctice and the effect its perfomrnce would have on the process purpose. On the basis of this review, each practice was determined to be either a base practice, and related to a process performance and a capability level of 1, or a generic practice, and related to process capability and the achievement of a capability level upper than 1. For generic practices, the specific capability level was detemined by a review of the 9 process attributes associated with each capability level. Capability levels are based on the achievement of these process attributes. Process attributes and the evidence required to achieve them are defined in Clause 4.3.2 of ISO/IEC 15504-5. Capability levels are detailed in Table C.2 of Annex C of the IEC 80001-1 PAM which detailes the association of IEC 80001-1 requirements with capability levels and base practices.

Step 8 requires that base practices were linked to the outcome that would be achieved by the performance of the practice. These practices should be phrased according to the requirements of ISO/IEC TR 24774 and it should be noted that a single practice may produce and therefore be linked to a number of outcomes. The previous steps were completed for each of the 14 processes resulting in the identification of 70 base practices.

Having identified the practices associated with each of the proceses, step 9 required that each of the processes were reviewed in order to determine work products among the inputs and the outputs of the practices. A review was undertaken of specific and generic practices contained in ISO/IEC 15504-5. Applicable work products were used within the IEC 80001-1 PAM with additional work products related to specific risk management activities as per the requirements of IEC 80001-1 being added as required. A list of generic and specific inputs and outputs and their characteristics are contained within Annex B of the IEC 80001-1.

The competion of all 9 steps of the TIPA transformation process allowed the domain requirements as expressed in IEC 80001-1 to be developed into a PRM and PAM. A sample process from the PAM is shown in Table 1.0. The resultant PRM and PAM are compliant with the requirements of ISO/IEC 15504-2 and ISO/IEC TR 24774. The PAM can be used for assessment against IEC 80001-1 and can be used to determine the capability levels of risk management processes for the incorporation of medical devices into an IT network. These capability levels can then be used as a basis for process improvement which will inturn increase the safety, effectiveness and security of the medical IT network.

Process ID:	CRCM.3
Name:	Go-Live
Context:	The process is to allow the responsible organisation to manage the Go-Live Phase of the project and to consider the decision to go live in terms of the residual risk.
Purpose:	The purpose of the Go-Live Process is to allow the responsible organisation to manage the transition of the IT network to the live environment and to allow the responsible organisation to manage the risk management activities associated with the Go-Live phase of the project.
Outcomes:	As a result of the successful implementation of Go-Live Process: 1. Medical IT-network residual risk is reviewed prior to going live. [[IEC 80001-1, 4.5.3]]. 2. Residual risk summaries are reviewed for acceptability of risks associated with interactions of recent or pending projects or changes. [[IEC 80001-1, 4.5.3]]. 3. The specified change to the medical IT-network is approved prior to go-live by the medical IT-network risk manager. [[IEC 80001-1, 4.5.3]]. 4. The approval of the medical-IT network residual risk is documented in the medical IT-network risk management file. [[IEC 80001-1, 4.5.3]].
Base Practices:	CRCM.3.BP1: Review residual risk. Review Medical IT Network residual risk summaries for acceptability of risk associated with interactions of recent or pending projects or changes, prior to going live. [IEC 80001-1, 4.5.3] [IEC 80001-1, 4.5.3] [Expected Result: 1, 2]. CRCM.3.BP2: Approve specified change. Approval is given for the specified change by the medical IT Network Risk Manager prior to go-live. [IEC 80001-1, 4.5.3] [Expected Result: 3]. CRCM.3.BP3: Document approval of residual risk. Document the approval of the medical IT Network residual risk in the Medical IT network risk management file. [IEC 80001-1, 4.5.3] [Expected Result: 4].
Inputs:	
13-03 Risk Benefit Analysis Record [CRCM.3, BP1, 2] [Expected Result 1, 2, 3]	
Outputs:	
08-02 Change Request Approval Record [CRCM.3, BP.2, 3] [Expected Result 3, 4] 16-02 Medical IT network Risk Management File [CRCM.3, BP.3] [Expected Result 4]	

Table 1.0 – Sample Process from IEC 80001-1 PAM

5 Conclusions and Future Work

The focus of research to date has been on the development of an ISO/IEC 15504-2 compliant PRM and PAM for assessment against IEC 80001-1. This will allow HDOs to assess the capability of their risk management processes against the requirements of IEC 80001-1 with regard to the incorporation of a medical device into an IT network which can then be used as a basis for process improvement. The PRM and PAM which have been developed as part of this research have been presented at a meeting of IEC SC62A JWG7 in September 2012. The PRM and PAM have been raised as a new work item proposal and will be published as a technical report as part of the IEC 80001-1 family of standards. This will establish the PAM as the standards method of assessment against IEC 80001-1.

Future work in this area will focus on the development of an assessment method for IEC 80001-1. A PAM cannot be used in isolation to perform an assessment against IEC 80001-1. To allow an assessment to be carried out, an assessment method will be developed which will allow for a standardised approach to performing the assessment and provides a set of questions which will allow a capability level to be determined for each of the practices related to the processes.

The PRM, PAM and assessment method will be validated in a number of ways. The PRM and PAM will be validated for structure and content with regard to their ability to assess against IEC 80001-1 requirements and their compliance with the requirements of ISO/IEC 15504-2. This validation will be conducted through expert opinion by eliciting feedback from the developers of the TIPA framework and through the resolution of comments made by members of JWG7 during the comment resolution phase of the technical report. Validation of the PRM, PAM and assessment method will also be carried out from the HDO perspective and medical device manufacturer perspective. Validation will be performed form the HDO by mapping of the processes within the PRM and PAM processes to a previously implemented network project within a large ICU and in a smaller clinical context. A medical device manufacturer will be asked to provide feedback on the processes which are addressed to medical device manufacturers. The research will take a design research approach by placing the artifact, in this case the PRM, PAM and assessment method in the context in which they will ultimately be used in order to assess their effectiveness. The required changes, based on feedback during the validation process, will be incorporated into the final model.

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

6 Author CVs

Silvana Togneri MacMahon

Silvana Togneri MacMahon received a Higher Diploma in Science in Computing in 2011 from Dundalk Institute of Technology having worked as a User Acceptance Test Lead in the Retail Banking sector. She is currently undertaking research for her PhD in the area of risk management of networked medical devices focusing on the development of a process reference model, process assessment model and assessment method for IEC 80001-1.

Fergal Mc Caffery

Dr Fergal Mc Caffery is the leader of the Regulated Software Research Group in Dundalk Institute of Technology and a member of Lero. He has been awarded Science Foundation Ireland funding through the Stokes Lectureship, Principal Investigator and CSET funding Programmes to research the area of software process improvement for the medical device domain. Additionally, he has received EU FP7 and Enterprise Ireland Commercialisation research funding to improve the effectiveness of embedded software development environments for the medical device industry.

Frank Keenan

Dr Frank Keenan lectures in Software Engineering in the Computing Department at Dundalk Institute of Technology. His current research interests include requirements engineering, agile development and context analysis. A particular interest is the transfer of knowledge gained to form innovative delivery approaches to subjects taught.

7 *References*

[1] *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software,* Food and Drug Administration, 2005.

[2] T. Cooper*, et al.*, *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks*: AAMI, 2011.

[3] 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.

[4] ISO/IEC, "ISO/IEC 15504-2:2003 - Software engineering — Process assessment — Part 2: Performing an assessment," ed. Geneva, Switzerland, 2003.

[5] ISO/IEC, "ISO/IEC 15504-5 - Information technology — Process Assessment — Part 5: An exemplar Process Assessment Model," ed. Geneva, Switzerland, 2006.

[6] B. Barafort*, et al.*, *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.

[7] ISO/IEC, "ISO/IEC TR 24774:2010 - Systems and software engineering — Life cycle management — Guidelines for process description," ed. Geneva, Switzerland, 2010.

[8] ISO/IEC, "ISO/IEC 20000-1:2011 - Information technology —Service management Part 1: Service management system requirements," ed. Geneva, Switzerland, 2011.

[9] The Cabinet Office, "ITIL 2011 - Summary of Updates," ed. Norfolk, England: Crown Copyright, 2011.

[10] B. Barafort*, et al.*, "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.

[11] ISO/IEC, "ISO/IEC TR 20000-4:2010 - Information technology — Service management - Part 4: Process reference model," ed. Geneva, Switzerland, 2010.