Assessing against IEC 80001-1

Silvana Togneri MacMahon[1], Fergal Mc Caffery[1], Sherman Eagles[2], Frank Keenan[1], Marion Lepmets[3], Alain Renault[3]

[1]Regulated Software Research Group, Department of Computing & Mathematics, Dundalk Institute of Technology & Lero, Dundalk Co. Louth, Ireland
{silvana.macmahon, fergal.mccaffery, frank.keenan}@dkit.ie

[2]SoftwareCPR, Saint Paul, MN 55114, USA
seagles@softwarecpr.com

[3]Public Research Centre Henri Tudor, Luxembourg
{alain.renault, marion.lepmets}@tudor.lu

Keywords: Keywords- IEC 80001-1; ISO/IEC 15504 – Process Assessment; Service Management; ISO/IEC 20000-1; TIPA; ITIL.

Abstract: Medical devices are designed and produced subject to various standards. These standards are recognized by the regulatory authorities within the region in which they are going to be marketed. Traditionally medical devices were placed on a proprietary network; however emergent technology is increasingly seeing medical devices being included on to the general hospital IT network. The incorporation of a medical device into an IT network can introduce risks which can impact the safety, effectiveness & security of the medical device. 80001-1: Application of Risk Management for IT networks incorporating Medical Devices addresses the risk that healthcare can be compromised when a medical device is incorporated into an IT network. In order to address these risks, an assessment of the network against IEC 80001-1 must be performed. To perform an assessment which is compliant with ISO/IEC 15504-2 of an IT network against IEC 80001-1, a process assessment model is required. This paper examines how a process assessment model could be developed to assess against IEC 80001-1.

1 INTRODUCTION

IEC 80001-1 (IEC, 2010) "represents a catalyst for a new level of IT and clinical technology cooperation to ensure network changes don't negatively impact biomedical systems" (Cooper et al., 2011) . When a medical device is incorporated into an IT network, a medical device network is established. Medical Devices are subject to regulations as prescribed by the various regulatory authorities of the regions in which the device is to be marketed. When a medical device is incorporated into an IT network which contains other IT components, this creates a new system in which the medical device has not been validated. New hazards may emerge that are directly related to the interaction of the networked components that were not considered when the device was being designed and validated (Cooper et al., 2011). Prior to the introduction of IEC 80001-1, no standard addressed the risks of incorporating a medical device into an IT network. IEC 80001-1 extends the definition of harm and identifies three main areas of risk – safety, effectiveness and (Data & System) security. IEC 80001-1 takes a life cycle approach to risk management. This paper examines how a Process Assessment Model (PAM) (which is compliant ISO/IEC 15504-2 Information technology - Process assessment (ISO/IEC, 2003)) may be developed to be used to assess against IEC 80001-1. The remainder of this paper examines the requirements contained in IEC 80001-1 and how IEC 80001-1 is related to ISO/IEC 20000-1 Information technology - Service management (ISO/IEC, 2011). ISO/IEC 15504 is examined in terms of its requirements for the development of process models. Finally the paper focuses on how current PAMs (which comply with ISO/IEC 15504-2) were developed to assess against service management standards and examines how these methods could be used to develop PAMs to assess against IEC 80001-1.

2 IEC 80001-1- APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES

IEC 80001-1 identifies 3 main areas of risk – safety, effectiveness & (Data & System) security. IEC 80001-1 covers the entire life cycle of the medical IT network, incorporating the principle that a risk management process should be implemented not only when creating a medical device network or but also when removing, maintaining or changing/modifying equipment on a medical device network. IEC 80001-1 uses a risk based approach based on the approach as outlined within ISO 14971 Application of risk management to medical devices (ISO, 2007) .

In order to address the variety of approaches to risk management among Responsible Organisations (RO), IEC 80001-1 outlines the specific roles, responsibilities and activities that must be performed with regard to the risk management of the incorporation of medical devices into IT networks. The standard is addressed to ROs, Medical Device Manufacturers (MDM) and to the providers of other information technology. An RO is defined within the standard as "an entity responsible for the use and maintenance of a Medical IT network". IEC 80001-1 recognizes that the overall responsibility for the Medical IT network belongs to the RO. The RO must establish a risk management policy for the incorporation of medical devices into an IT network and must appoint a medical IT risk manager. The risk manager must maintain the risk management file which must contain sufficient documentation as to support the risk management activities required by IEC 80001-1.

Life cycle risk management must be performed in a way that allows the RO to support effective healthcare delivery. When making changes to or performing maintenance activities on medical devices, ROs must follow strictly formal approaches directly involving the manufacturer of the device. This establishes an on-going relationship between the RO and the device manufacturer which continues for the entire life cycle of the medical IT network. In this context, we review in the next section the relationship between IEC 80001-1 and the generic Service Management standard ISO/IEC 20000-1.

3 RELATIONSHIP BETWEEN IEC 80001-1 AND ISO/IEC 20000-1.

Annex D of IEC 80001-1 examines the relationship between ISO/IEC 20000-1 (and ISO/IEC 20000-2), highlighting the processes that are common to both such as Change Management or Release Management. Annex D also highlights a number of areas within the 2 standards where the terminology differs but the underlying process areas are the same. For example, what is referred to as "Risk Management Process" in IEC 80001-1 appears as "Security Risk Assessment Practices" within ISO/IEC 20000. Due to the common life cycle approach, the concepts of Service Management as described in ISO/IEC 20000-1 and ISO/IEC 20000-2 (ISO/IEC, 2005) have been examined for their ability to meet the requirements outlined in IEC 80001-1 (IEC, 2010) .

4 ISO/IEC 20000 – SERVICE MANAGEMENT STANDARDS

ISO/IEC 20000-1 requires "an integrated process approach" when the service provider "plans, establishes, implements, operates, monitors, reviews, maintains and improves a service management system (SMS)". In order to follow this integrated process approach, ISO/IEC 20000 promotes a "Plan, Do, Check, Act" procedure. The "Plan" phase involves establishing, documenting and agreeing the SMS policies plans and objectives. The "Do" phase involves implementing and operating the SMS. The "Check" phase involves monitoring, measuring and reviewing the SMS to ensure that it meets the agreed policies and objectives. The "Act" phase involves taking actions to continually improve the performance of the SMS (ISO/IEC, 2011). :

ISO/IEC 20000-2 (ISO/IEC, 2005) describes the best practices for Service Management within the scope of ISO/IEC 20000-1. Guidance is provided on the 5 process categories identified in Part 1 of the standards namely Service Delivery Processes, Control Processes, Release Processes, Resolution Processes and Relationship Processes. ISO/IEC 20000-4(ISO/IEC, 2010a) ISO/IEC 20000-4 provides the Process Reference Model (PRM) for IT Service Management based on the requirements of ISO/IEC 20000-1.

Best practices for Service Management are also outlined within the Information Technology Infrastructure Library (ITIL) (Cartlidge et al., 2007). ITIL was developed in the United Kingdom at the end of the 1980's. ITIL has become the world wide

"de facto" standard for IT Service Management (Barafort et al., 2009) and is now owned by the Cabinet Office . ITILv3 consists of 5 publications which cover – Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

As both ISO/IEC 20000-4 and ITIL deal with a life cycle approach to Service Management, they are very similar standards. The relationship between ITILv3 and ISO/IEC 20000 is close - to the extent that ISO/IEC 20000 has become known as the "ITIL standard". In the latest version of the standard ISO/IEC 20000-1:2011, there have been steps taken to ensure that ISO/IEC 20000 is more closely aligned with ITILv3 (Dugmore and Taylor, 2008) .

5 ISO/IEC 15504 AND THE DEVELOPMENT OF PROCESS ASSESSMENT MODELS

ISO/IEC 15504-2 defines the requirements for performing process assessment as a basis for use in process improvement and capability determination. ISO/IEC 15504-2 defines a measurement framework for the process capability and defines the requirements for performing an assessment. It also defines requirements for building PRMs, building PAMs and verifying conformity of process models and of process assessment. Process assessment is viewed on the basis of a two dimensional model containing both a process dimension and a capability dimension. The process dimension is provided by reference to an external PRM in which processes are characterized in terms of their purpose and their outcomes. Further guidelines for process description are outlined in ISO/IEC TR 24774:2010 (ISO/IEC, 2010b) . The capability dimension is based on 6 capability levels. The achievement of these capability levels is based on the achievement of the associated process attributes.

In order to perform an assessment which is compliant with ISO/IEC 15504-2, a PAM is required. ISO/IEC 15504-5 (ISO/IEC, 2006) provides an exemplar PAM which can be used to perform an assessment compliant with the requirements defined in ISO/IEC 15504-2. The PAM extends the PRM process definitions by including a measurement framework.

Process assessment contains 2 aspects, capability determination and process improvement. Once process capability has assessed the current state of a set of processes (against a target capability level determined in advance of the assessment), the results of the assessment are then analysed to determine the strengths, weaknesses, opportunities and threats in the process context and process improvement can be undertaken on this basis.

6 THE DEVELOPMENT OF A PROCESS ASSESSMENT MODEL TO ASSESS AGAINST IEC 80001-1.

In order to perform an assessment against IEC 80001-1, our research to date has focused on investigating how other ISO/IEC 15504-2 compliant process models have been developed to assess against other similar standards. Given the relationship between IEC 80001-1 and ISO/IEC 20000-1, we have investigated how the PAM for this standard was developed. We also investigated how the TIPA PAM was developed. We discovered that the TIPA framework which was developed by Public Research Centre Henri Tudor can be used to assess against both ISO/IEC 20000 and ITIL. The TIPA PAM which is used to assess against ITIL continues to be updated to assess against the latest versions of ITIL. It should be noted that the TIPA PAM which was developed to assess against ISO/IEC 20000 is no longer being updated but is being further developed in JTC1 ISO/IEC SC7 under the title ISO/IEC 15504-8.

In developing the TIPA PAM for ITIL and the TIPA PAM for ISO/IEC 20000, the TIPA transformation process was used. The TIPA transformation process was developed to address the fact that while ISO/IEC 15504 provides a detailed description of the process assessment approach and provides an exemplar PAM in ISO/IEC 15504-5, there is no guidance to support the transformation from the input (domain requirements) to the output (process model). This gap was identified by Barafort et al. (Barafort et al., 2008) and the TIPA transformation process was developed as a means to develop ISO/IEC 15504-2 compliant PAMs using goal driven requirement engineering techniques.

Due to the similarities between ISO/IEC 20000 and IEC 80001-1., it is clear that using the TIPA transformation process; a process assessment model could be built to assess medical IT networks against IEC 80001-1

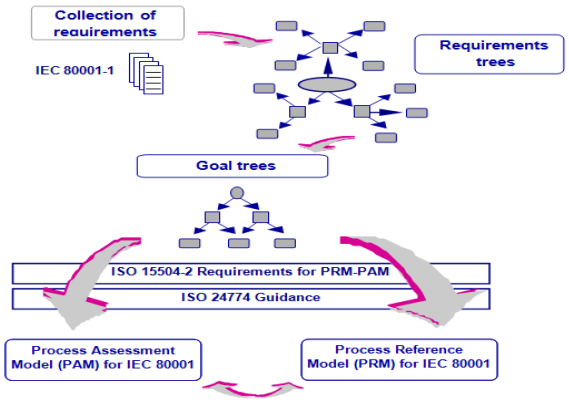

Fig. 1. Shows how the TIPA transformation process may be used to create a PRM and PAM to assess medical IT networks against IEC 80001-1.

7 CONCLUSIONS AND FUTURE WORK

It is proposed that a PAM could be developed, using the TIPA transformation process, to assess against IEC 80001-1. Future research will focus on the development of a PRM and PAM based on the TIPA transformation process. Each process will be validated by industry experts and amended according to the consensus. Once the PRM and PAM have been fully developed, the model will then be validated through trials.

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.
ITIL® is a registered trade mark of the Cabinet Office. TIPA® is a Registered Trade Mark of the CRP Henri Tudor

REFERENCES

Barafort, B., Betry, V., Cortina, S., Picard, M., St Jean, M., Renault, A., Valdés, O. & Tudor, P. R. C. H. 2009. *ITSM Process Assessment Supporting ITIL : Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification,* Zaltbommel, Netherlands, Van Haren.

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

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. 2007. An introductory Overview of ITILv3. The UK Chapter of the itSMF.

Cooper, T., David, Y. & Eagles, S. 2011. *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks*, AAMI.

Dugmore, J. & Taylor, S. 2008. ITILv3 and ISO/IEC 20000 - Alignment White Paper - March 2008. *Best Management Practice for IT Service Management* [Online]. [Accessed 02/01/2012].

IEC 2010. IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities. Geneva, Switzerland: International Electrotechnical Commission.

ISO 2007. ISO 14971:2007 - Medical Devices - Application of Risk to Medical Devices. Geneva, Switzerland: International Organisation for Standardization.

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

ISO/IEC 2005. ISO/IEC 20000-2:2005 - Information technology -- Service management -- Part 2: Code of Practice. Geneva, Switzerland.

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

ISO/IEC 2010a. ISO/IEC TR 20000-4:2010 - Information technology — Service management - Part 4: Process reference model. Geneva, Switzerland.

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

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