Risk Management of Medical IT Networks: An ISO/IEC 15504 Compliant Approach to Assessment against IEC 80001-1

Silvana Togneri MacMahon, Fergal McCaffery, Frank Keenan
Department of Computing & Mathematics
Dundalk Institute of Technology
Co Louth, Ireland
+ 353 (0) 42 937200
{silvana.macmahon, fergal.mccaffery, frank.keenan}@dkit.ie

ABSTRACT

The incorporation of a medical device into an IT network can introduce risks that may not have been addressed during the design and manufacture of the device. IEC 80001-1 is a lifecycle risk management standard which was developed to address these risks. This paper presents research which has been performed to date which has led to the development of a Process Reference Model (PRM) and Process Assessment Model (PAM) which can be used by Healthcare Delivery Organisations to assess themselves against IEC 80001-1. This paper also presents future work in this area which includes the development of an assessment method for IEC 80001-1 and the validation of the PRM, PAM and assessment method.

Categories and Subject Descriptors

D.2.9 **[Management]**: Software process models (e.g., CMM, ISO, PSP)

General Terms

Management, Measurement, Design, Standardization,Performance

Keywords

Risk Management, Medical IT networks, IEC 80001-1, ISO/IEC 15504-2, Process Assessment.

1. INTRODUCTION

IEC 80001-1: Application of risk management for IT-networks incorporating medical devices [7] was published in 2010 to address the risks associated with the incorporation of a medical device into an IT network. Traditionally, when a medical device was incorporated into an IT network, the medical device manufacturer would not only provide the device but also provide a proprietary network for the device. Proprietary networks were used to allow device manufacturers to exercise control on the configuration of the devices and to make servicing of the device easier [6]. This method of networking medical devices resulted in a proliferation of private networks with a large hospital potentially having hundreds of private networks. Maintenance of these increasingly large numbers of private networks became impractical which has led to medical devices increasingly being designed to be incorporated into the hospitals general IT network.

Medical devices are stringently regulated by authorities in the region where the device is to be marketed. However, the incorporation of a device into a medical IT network may introduce risks that may not have been considered during the design and production of the device. These risks can lead to a host of problems such as incorrect operation or degraded performance of the medical device resulting from combining medical devices and other equipment on the same IT network or incorrect operation of the medical device resulting from combining medical device software and other software applications, such as open email systems or computer games, in the same IT network. IEC 80001-1 seeks to address these risks through the use of a lifecycle approach to risk management. Currently, no method of assessment against IEC 80001-1 exists. Our research to date has focused on the development of a PRM and a PAM which are compliant with the requirements of ISO/IEC 15504-2 to be used for assessment against IEC 80001-1. The PAM which is being developed and validated as part of this work is scheduled for inclusion in the IEC 80001-1 family of standards and as such will be the internationally recognized PAM for assessment against IEC 80001-1. An assessment method to accompany the PAM will also be developed as part of the research. Section 2 of this paper focuses on the origin and applications of IEC 80001-1. Section 3 discusses the approach to the development of a PRM and PAM for assessment against IEC 80001-1 while section 4 discusses the resultant PRM and PAM. Section 5 details future work in terms of the validation of these models and Section 6 presents the conclusions of this paper.

2. IEC 80001-1 ORIGINS & APPLICATION

In 2003, the Food and Drug Administration (FDA) received a cluster of reports of cyber-attacks on US hospitals. As a result of these attacks, the FDA produced guidance on cyber security for medical devices containing off the shelf software [16]. During the development of this guidance, it was recognized that the guidance should not only look at cyber security. The guidance being developed should be widened to address the broader concept of risk management for IT networks which incorporate medical devices. It was recognized by regulators that in order to address this area of risk management that it was not sufficient to aim the guidance at manufacturers. In order to be effective in addressing these risks, the guidance should also address those that have responsibility for the establishment and maintenance of these networks (Responsible Organisations) and also providers of other

ICSSP'13, May 18–19, 2013, San Francisco, USA

IT technology. The resultant standard, IEC 80001-1, aims to be a catalyst for a greater level of communication among these risk management stakeholders [4].

IEC 80001-1 applies when a medical IT network is established. A medical IT network is defined within IEC 80001-1 as an IT network that contains a medical device. IEC 80001-1 also applies when a medical device is placed on an existing medical IT network, when a change or modification to a device on a medical IT network takes place, when maintenance activities are performed on a device on a medical IT network and finally when a device is removed from a medical IT network. The standard addresses 3 key properties of the medical IT network. Safety deals with the prevention of harm to the patient, user or the environment. Effectiveness is concerned with the ability of the device to provide the intended result for the patient and the Responsible Organization. Data and System security seeks to maintain an operational state where information items are protected from degradation in terms of confidentiality, integrity, and availability.

IEC 80001-1 advocates a lifecycle risk management approach and gives guidance on the role, responsibilities and activities that should be carried during the management of these risks. However, there is currently no method to assess how well these processes are being performed and to highlight areas where process improvement could be implemented. The following section discusses the approach to the development of the PRM and PAM for IEC 80001-1.

3. APPROACH TO THE DEVELOPMENT OF THE PRM AND PAM

In order to develop the PRM and PAM, a review of relevant standards was completed. The individual requirements of IEC 80001-1 were reviewed. In addition to this a review of standards related to process assessment was performed. Finally, our research focused on reviewing standards which are similar to IEC 80001-1 and also examined how assessment methods were developed to assess against this standard. These methods were then reviewed to ascertain if they could be applied to IEC 80001-1. Each of these steps is discussed in detail within this section.

3.1 Review of Process Assessment Standards

ISO/IEC 15504-2:2003 Information technology - Process assessment - Part 2: Performing an assessment [8] is an international standard which defines the requirements for performing process assessment as a basis for use in process improvement and capability determination. The standard provides guidance on performing an assessment and focuses on aspects of the assessment such as the roles and responsibilities, defining the scope of the assessment and recording the output of the assessment. A measurement framework for use during assessments is prescribed. Requirements for models for process assessment are outlined with specific requirements for PRMs and PAMs being described in detail. Finally, methods for verifying the conformity of PRMs and PAMs are outlined.

The aim of the requirements as outlined in ISO/IEC 15504-2 is to provide a structure that will allow for self-assessment, producing a process rating which is based on the ability of the process to achieve its purpose and which can be used as a basis for capability determination and to facilitate process improvement. Assessments which follow the requirements of ISO/IEC 15504-2 are applicable across all application domains and sizes of organization and consider the context in which the assessed process is implemented. This standardized approach allows for objective benchmarking across organizations.

In order to achieve these benefits, ISO/IEC 15504-2 requires that PRMs should include a declaration of the domain of the PRM, should contain a description of the processes within the PRM, a description of the relationship between the PRM and its intended context of use and a description of the relationship between the processes within the PRM. The PRM should also state the community of interest of the PRM and how consensus within that community was achieved with regard to the processes contained within the PRM. Within the PRM the process should be described in terms of a statement explaining the purpose of the process and should also details the outcomes that will be observable as a result of performing the process.

A PAM is related to one or more PRMs and forms the basis for the collection of evidence and rating of process capability. The PAM extends the processes as defined in the PRM with the addition of a measurement framework. This allows the PAM to provide a two dimensional view of process capability – the process dimension which relates to the processes as defined within the PRM and the capability dimension which is related to the measurement framework as described in ISO/IEC 15504-2. The description of process in the PRM is extended in the PAM to make reference to base practices and work products. Base practices are the activities which must be performed to achieve the process purpose. Work products are either used or produced in the performance of the process. Part 5 of the ISO/IEC 15504 [14] family of standards provides an exemplar PAM showing the requirements of ISO/IEC 15504-2 as applied to the processes outlined in ISO/IEC 12207:2008 [10]. The PRM and PAM which are being developed as part of this research comply with the requirements for assessment models as described in ISO/IEC 15504-2.

3.2 Review of Standards Identified as Similar to IEC 80001-1

In order to define the approach to the development of the an ISO/IEC compliant PRM and PAM, a review of standards similar to IEC 80001-1 for which ISO/IEC 15504-2 compliant models have been developed was undertaken. ISO/IEC 20000-1 Information technology - Service management - Part 1: Service management system requirements [13] is a generic Service Management standard which is identified within Annex D of IEC 80001-1 as being similar to IEC 80001-1. This standard is similar to IEC 80001-1 in that it also describes a lifecycle approach to Service Management. This annex examines ISO/IEC 20000-1 and ISO/IEC 20000-2 [9] and identifies the processes which are common to these standards and IEC 80001-1. The annex also identifies areas where, while the terminology appears different, the underlying role, document or process is similar.

A review of SO/IEC 15504-2 compliant assessment methods to assess against ISO/IEC 20000-1 was completed. Research focused on the Tudor IT Service Management Process Assessment (TIPA) [1] which was developed by CRP Henri Tudor and which can be used to perform assessments against both ISO/IEC 20000-1 and the Information Technology Infrastructure Library (ITIL). ITIL [15] is a widely accepted approach to service management which was developed by the Cabinet Office , the latest versions of which have been closely aligned to ISO/IEC 20000 [5]. The benefits of the combination of the use of ISO/IEC 15504-2 and ITIL in the management of services have been recognised by CRP Henri Tudor [2] who have developed TIPA in a manner which is compliant with ISO/IEC 15504-2 requirements. In reviewing models for assessing against ISO/IEC 20000-1, an examination of the method of developing these models was conducted. Our research focused on the TIPA transformation process which was used to develop TIPA.

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 [3]. The transformation process advocates identifying elementary requirements and organising these requirements into requirement trees. These requirement trees are then oriented around the business goals to which they are related and form goal trees. The transformation process uses the requirements of ISO/IEC 15504-2 combined with the requirements of ISO/IEC TR 24774 to develop the final PRM and PAM. ISO/IEC TR 24774 Systems and software engineering - Life cycle management - Guidelines for process description [12] 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 TIPA transformation process was used in the development of the IEC 80001-1 PRM and PAM.

4. IEC 80001-1 PRM AND PAM

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 20000-4 [11] was reviewed. ISO/IEC 20000-4 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” approach could also be used to address the lifecycle approach advocated in IEC 80001-1. This approach has been maintained as illustrated in Fig. 1 Using the ISO/IEC 20000-4 PRM as a template, the next stage of the development of the IEC 80001-1 PRM was to structure the requirements according to the TIPA transformation process. Two process categories were identified – Primary processes and Organisational processes. The primary process group is concerned with processes related to the performance of risk management activities, such as risk analysis & evaluation, while the organizational process category is concerned with the planning of risk management activities and deals with specific output such as documentation produced as a result of the performance of risk management activities. The primary process category contains three process groups with a total of nine processes. The organizational process category contains a single process group which contains five processes. The processes were developed around domain goals. Various approaches were taken to organizing requirements around domain goals but the final approach taken was to follow the sections within the standard. Processes are expressed in terms of the of the process purpose and process outcome as per the requirements of ISO/IEC TR 24774. During the development of the PRM, traceability to the specific requirements within IEC 80001-1 to each of the processes which have been developed was maintained.

According to ISO/IEC 15504-2, a process assessment cannot be carried out using a PRM alone. In order for an assessment to take place, a PAM must be developed. The PAM extends the process definitions as described in the PRM and requires the addition of a measurement framework. The processes within the PRM are extended to include base practices and work products. The 14 processes which are contained in the PRM have been extended to include 70 base practices. A base practice is an activity which must be carried out to achieve the purpose of the process and achieve the outcomes. A work product is used or produced as a result of performing the process. Traceability to the original requirements of IEC 80001-1 is maintained with each work product being associated with the relevant base practice and each base practice being related to the expected result that will be achieved as a result of performing the base practice. A list of work products is included in the PAM. As per ISO/IEC 15504-2, the PAM must include a statement of the conformance of the PAM with the PRM which outlines which processes within the PRM are being assessed by the PAM. In the IEC 80001-1 PAM, the PAM assesses all processes within the PRM. The PAM also contains two annexes, one of which shows the relationship between the requirements under the standard and the associated base practices and the other which relates base practices to the specific requirement.

In order to perform an assessment against the processes outlined within the PAM, an assessment method is required. An assessment method ensures a standard approach to the performance of an assessment and deals with organisational aspects of performing the assessment such as defining roles and responsibilities during the assessment and the scope of the assessment. The assessment method also contains a set of questions related to each of the processes to determine the capability level that is associated with the performance of each process. The capability levels which will be determined for each process will be the standard capability levels which are used in ISO/IEC 15504-2. There are 6 capability levels in this standard as follows: Level 0: Incomplete, Level 1: Performed, Level 2: Managed, Level 3: Established, Level 4: Predictable & Level 5: Optimised. These levels reflect the capability of the performance of the process and the level is determined by reference to 9 process attributes which are associated with the 5 capability levels.

The assessment method for IEC 80001-1 has not been developed to date, but development will take place as part of on-going research. When an assessment is completed using the assessment method, the results will determine the current capability level of the process which can identify areas of strengths, weaknesses, opportunities and threats to the process which can be used to identify areas which are suitable for process improvement. The next section of this paper will discuss the approach that will be taken to the validation of the PRM, PAM and assessment method which is also part of the future work of this project.

5. VALIDATION OF THE PRM, PAM AND ASSESSMENT METHOD

In order to ensure that the PRM, PAM and assessment method are suitable for assessment against IEC 80001-1, both models will need to be validated. There will be a number of stages of validation of the PRM and PAM. The validation will mainly take a Design Research approach which focuses on real world problems and refines the artifacts which are developed to address these problems by situating the artifact or solution in its context of use [17].

The first step in the validation of the PRM and PAM will be from a structural point of view. This validation will be carried out by the developers of the TIPA assessment method. The developers of this model have extensive experience in the development of PRMs and PAMs and will validate the model with its compliance to the requirements of ISO/IEC 15504-2 in terms of the structural requirements for PRMs and PAMs as outlined in this standard. The model will be reviewed in terms of the definition of the processes and in terms of the process attributes which have been assigned to each of the processes. The definition of base practices and work products within the PAM will also be reviewed. Any structural issues with the models will be addressed and the model will be updated based on the feedback.

The next stage of validation will be performed by the International Standards Community. The PAM for IEC 80001-1 has been raised as a New work item Proposal (NP) by IEC 62A JWG7 for inclusion in the IEC 80001-1 family of standards. This NP was raised following the circulation and presentation of the latest draft of the IEC 80001-1 PAM at the September 2012 meeting of JWG7 in Vienna which was very well received. As part of the NP process, the PAM will be circulated to member states, representing 82 countries as full or associate members, who will have the opportunity to comment on the PAM. Representatives from the member states are experts in the area such as representatives from medical device manufacturers, representatives from Healthcare delivery organisations (such as systems engineers and physicists from large hospitals), academics who are performing research in this area and representatives from the standards authorities of the individual member states who have been involved in the development of the IEC 80001-1 standard. At the NP stage, there is a 3 month period during which comments can be made and voting takes place. Once the NP has been approved, it enters the preparatory stage and a Working Draft (WD) is prepared. The preparatory stage ends when a working draft is available for circulation to the members of the technical committee or subcommittee as a first Committee Draft (CD). At this stage, the CD is submitted to the national committees for comment. During this time, national bodies carefully study the text of the CDs and make comments which are taken into consideration. Appropriate adjustments are made to the CD until consensus is reached. After this stage the draft enters a period where voting takes place. If approved, the draft will form part of the standard. The comments which are raised during this process will validate the models from the perspective of its ability to be used to assess against IEC 80001-1. The comments made during this period will be incorporated into the model and the final PAM will be included in the IEC 80001-1 family of standards. As all processes which are in the PRM are being assessed though the PAM this will validate both the PRM and PAM.

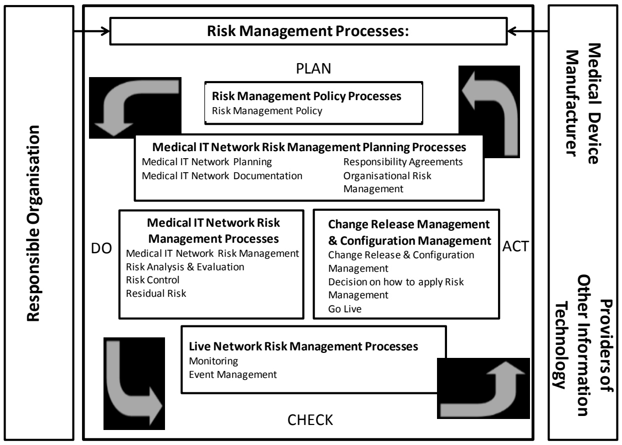
Responsible Organisation
Risk Management Processes:
Medical Device Manufacturer
PLAN
Risk Management Policy Processes
Risk Management Policy
Medical IT Network Risk Management Planning Processes
Medical IT Network Planning
Medical IT Network Documentation
Responsibility Agreements
Organisational Risk Management
DO
Medical IT Network Risk Management Processes
Medical IT Network Risk Management
Risk Analysis & Evaluation
Risk Control
Residual Risk
Change Release Management & Configuration Management
Change Release & Configuration Management
Decision on how to apply Risk Management
Go Live
ACT
Providers of Other Information Technology
Live Network Risk Management Processes
Monitoring
Event Management
CHECK

Figure 1 – IEC 80001-1 PRM Process Map

An additional stage in the validation of the PAM will be to validate the PAM in the context of its use within a Healthcare Delivery Organisation (HDO). This validation will be performed in St James's Hospital in Dublin. This will involve a review of the processes within the PAM by the principal physicist and the Informatics Team within the hospital. The processes will be mapped onto previous medical IT network projects which have been completed within the hospital. The review will focus on a number of projects of different sizes such as the large scale installation of a medical IT network within the Intensive Care Unit and a smaller installation within a specialist clinic setting. This will allow us to gain insight into how the model can be used to address HDOs of varying sizes and will also serve to inform the development of the assessment method. All feedback from this stage of validation will be included in the WD versions of the PRM, PAM that will be included in the IEC family of standards and into the final version of the assessment method. This stage of validation will allow us to ensure that the models can be used in a real HDO setting.

The final stage of validation will be to perform a trail assessment using the assessment method which has been developed and validated for use against the IEC 80001-1 PAM. The trail assessment will be completed in a small hospital in Ireland and a larger hospital in America. Any amendments which are required as a result of performing the assessment will be incorporated into the final version of the assessment method.

6. CONCLUSIONS

The result of this research will be the production of a validated PRM, PAM and assessment method which will allow HDOs to assess themselves against IEC 80001-1. The PAM which is being developed as part of this research is scheduled for inclusion in the IEC 80001-1 family of standards. The PAM and assessment method can be used to perform an assessment which can be used to determine the current capability levels of the risk assessment process which are currently in place within the HDO to address the risks associated with incorporation of a medical device into an IT network. The results of the assessment can be used as a basis for process improvement. The implementation of effective risk management processes will ensure that risk management activities preserve the key properties to ensure that the safety, effectiveness and data and system security are not impacted by the incorporation of a medical device into an IT network. Validation of the PRM, PAM and assessment method will ensure that the models can be scaled for use in HDOs of varying sizes and will ensure that the models can be used in the context of a HDO setting.

7. ACKNOWLEDGMENTS

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

8. REFERENCES

[1] Barafort, B., Betry, V., Cortina, S., Picard, M., St Jean, M., Renault, A., Valdés, O., and 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*. Van Haren, Zaltbommel, Netherlands.

[2] Barafort, B., Di Renzo, B., and Merlan, O., 2002. Benefits Resulting from the Combined Use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL) Product Focused Software Process Improvement. In (2002), Springer Berlin / Heidelberg, 314-325. DOI= http://dx.doi.org/10.1007/3-540-36209-6_27.

[3] Barafort, B., Renault, A., Picard, M., and Cortina, S., 2008. A transformation process for building PRMs and PAMs based on a collection of requirements – Example with ISO/IEC 20000. In *Proceedings of the SPICE* (Nuremberg, Germany2008).

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

[5] Dugmore, J. and Taylor, S., 2008. ITILv3 and ISO/IEC 20000 - Alignment White Paper - March 2008. In *Best Management Practice for IT Service Management* OCG,TSO and BSI.

[6] Gee, T., 2008. Medical Device Networks Trouble Industry Medical Connectivity.

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

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

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

[10] ISO/IEC, 2008. ISO/IEC 12207:2008 - System and Software Engineering - Software Life Cycle Processes, Geneva, Switzerland.

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

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

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

[14] ISO/IEC, 2012. ISO/IEC 15504-5:2012 Information technology -- Process assessment -- Part 5: An exemplar software life cycle process assessment model, Geneva,Switzerland.

[15] The Cabinet Office, 2011. ITIL 2011 - Summary of Updates Crown Copyright, Norfolk, England.

[16] U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of Compliance, and Evaluation, O.o.D., 2005. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, FOOD AND DRUG ADMINISTRATION Ed., 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD, 20852.

[17] Zimmerman, J. and Forlizzi, J., 2008. The role of design artifacts in design theory construction. *Artifact 2*, 1, 41-45.