Framework to Assist Healthcare Delivery Organisations and Medical Device Manufacturers Establish Security Assurance for Networked Medical Devices

Anita Finnegan, Fergal McCaffery, and Gerry Coleman

Regulated Software Research Centre, Dundalk Institute of Technology & Lero, Dundalk, Co Louth, Ireland
{anita.finnegan,fergal.mccaffery,gerry.coleman}@dkit.ie

Abstract. This paper introduces an assurance framework for networked medical device development. This work is being conducted to address the ever-increasing concerns of medical device security with a specific focus on medical devices to be incorporated into IT networks. The framework utilises a Process Assessment Model and a Process Reference Model to address system development lifecycle processes, security assurance processes and a focused risk management process. There is currently no governance for the development of secure medical devices in place and so, this work sets out to resolve this problem by increasing the awareness of medical device security risks, threats and vulnerabilities among Medical Device Manufacturers, IT vendors and Healthcare Delivery Organisations.

Keywords: Security Assurance, Networked Medical Device Security, Process Assessment Model, Process Reference Model, Security Capabilities.

1 Introduction

Security of medical devices is a very serious and concerning topic among the medical device domain at present so much so that it has been elevated with the involvement of US Government bodies. One reason for this concern is due to advancements in the design of medical devices in recent years. The introduction of software and then the introduction of interoperable and networked medical devices have presented significant benefits for Healthcare Delivery Organisations (HDOs) and for patient care. The design and functionality of these devices have changed tremendously in the last number of years. However, the development processes have remained unchanged and consideration for new types of risks for such devices with communication capabilities has not yet been adequately built into the development life cycle. This work sets out to change this and to overcome gaps in the development life cycle where security requirements need to be prioritised. This work introduces a Process Assessment Model (PAM) that incorporates the system development life cycle processes and builds upon this to add further assurance for these processes. It then incorporates a very focused security risk management process with a specific set of security controls, requirements and capabilities for consideration.

F. McCaffery, R.V. O'Connor, and R. Messnarz (Eds.): EuroSPI 2013, CCIS 364, pp. 313–322, 2013.

ISO/IEC 15504-2 [1] is an international standard that is often used in the IT and software industry to establish an organisations ability to achieve a particular process or set of processes. It provides a measurement framework for process capabilities and defines the requirements for performing the assessment. In utilising ISO/IEC 15504 the three major outputs are the Process Reference Model (PRMs), PAM and a capability measurement of the assessed processes. Existing generic Software Process Improvement (SPI) models are available which include the Capability Maturity Model Integration (CMMI®) [2] and ISO 15504-6:2006 [3] (SPICE) however these models were not developed to provide sufficient coverage of all areas necessary to assure the security of medical devices being incorporated into an IT network [4]. We achieve this through the development and implementation of an enhanced Process Reference Model (PRM), a Process Assessment Model (PAM) (including a Process Measurement Framework in compliance with IEC/ISO 15504-2 [1]) for the assurance of Medical Device Manufacturers (MDMs) development processes. It is intended that this will impact MDMs in their design decisions during the development of networked medical devices. In developing this framework, another key objective is to strengthen the relationship between MDMs and HDOs with involvement of HDO IT administration staff during the planning stage. This communication will assist MDMs better understand the environment, the intended use and the users of the medical device and, through a predefined set of security capabilities, the HDO will be able to better communicate the security requirements for a particular medical device.

This research aims to address security in networked medical devices and to build an awareness of the types of security vulnerabilities and threats that can negatively impact the safety of patients through the development of a focused security risk management process. Section 1.1 discusses the background to this problem, the reason for this work, and the approach taken. Section two describes process assurance and discusses key standards. Section three concludes the paper and details the expected impact this research will have upon the medical device industry (including the HDOs, MDMs) and in terms of regulatory compliance assessments.

1.1 Background

Medical device design innovations over the last number of years have provided significant benefits for patient care and healthcare providers. An increased use of software has allowed MDMs to add sophisticated functionality to devices. More recently medical devices include functionality to communicate via healthcare IT networks, wirelessly, across the Internet and from device to device. Networked medical devices can now provide patients with around-the-clock care outside the healthcare environment. Resource demand for HDOs to administer this care is also significantly reduced. HDOs utilize a wide range of networked devices from hard-wired monitoring devices such as diagnostic equipment (CT scanners) to implanted medical devices such as defibrillators. Clearly the benefits of networking these devices are significant but, in using such technology, a new set of risks arise associated with their use. These are security risks, threats and vulnerabilities. In the last 12 months there have been many published reports highlighting the vulnerabilities of networked medical devices. One report issued by the Department of Homeland

Security [5] highlights common threats associated with each type of device (implantable, external and portable medical devices). As this technology is relatively new, there is fear within the healthcare industry that the security of medical devices is insufficient and has not been thoroughly addressed in terms of research and design. More concerning is that malicious attackers have not yet fully exploited these devices but they do possess the potential to do so. This became evident through a number of controlled hacking demonstrations where security researchers proved the vulnerability of medical devices. One such incident was at the 2011 Black Hat Security Conference in Las Vegas where, a diabetic security researcher, Jerome Radcliffe, hacked his own insulin pump. This enabled him to increase and decrease the dosage levels without a warning that either, the pump had been tampered with or that the dosage levels may be harmful to him. More recently, researchers from Cylance, a stealth security firm based in Irvine, California, hacked into Philips XPER medical management system and allowed them to take control of other pieces of connected equipment [6]. This raised a lot of concern within the medical device domain and led to the interjection of the US government, which prompted a US Government Accountability Office (GAO) inquiry into the FDA's assessment of medical devices in terms of security. The outcome of this was a report published in August 2012 [7] detailing the lack of consideration for both intentional and non-intentional security vulnerabilities during the FDA's PMA and 510k approval processes. This paper outlines work that addresses security issues for medical devices to be incorporated into an IT network. The remainder of section 1 presents an overview of this research and also the approach to address This round of checking takes place about two weeks after the files have been sent to the Editorial by the Contact Volume Editor, i.e. roughly seven weeks before the start of the conference for conference proceedings, or seven weeks before the volume leaves the printer's, for post-proceedings. If SPS does not receive a reply from a particular contact author, within the timeframe given, then it is presumed that the author has found no errors in the paper. The tight publication schedule of LNCS does not allow SPS to send reminders or search for alternative email addresses on the Internet.

1.2 Framework Development – The Approach

The first step in this approach was to select a suitable PRM to build the PAM upon. A system life cycle process standard was most suitable as a foundation for the PAM as it addresses the life cycle of a system (including hardware and software), in 25 processes, from concept through to retirement. In order to place emphasis on security, it was felt that further assurance of particular development processes was required so the PAM was tailored to include additional processes, activities and tasks from another standard. This standard specifically addresses assurance in the system life cycle based on a selected critical property of a system (i.e. dependability, safety, security etc.).

As one of the main objectives of this work is to provide MDMs with a focused security risk management process we have facilitated this by furthering enhancing the PAM to include a list of security controls to be addressed during the development life

cycle of the system. In order to achieve this, a security standard review has been performed. A complete set of controls deemed relevant to these types of medical devices were devised and validated through the use of expert opinion, interested parties within the FDA and the International medical device standards committee (i.e. IEC SC62A JWG7). The outcome of this exercise is a technical report presenting these security controls. This will be raised as a new work item in May 2013 at the IEC SC62A JWG7 International standards meeting. In addition to this another technical report will be published to provide guidance to MDMs for the implementation of the PAM. Upon the preliminary completion of this framework, it will be trialed within MDMs and HDOs within both the EU and the US.

Figure 1 details the overview of this framework for addressing security in the development life cycle stages for networked medical devices.

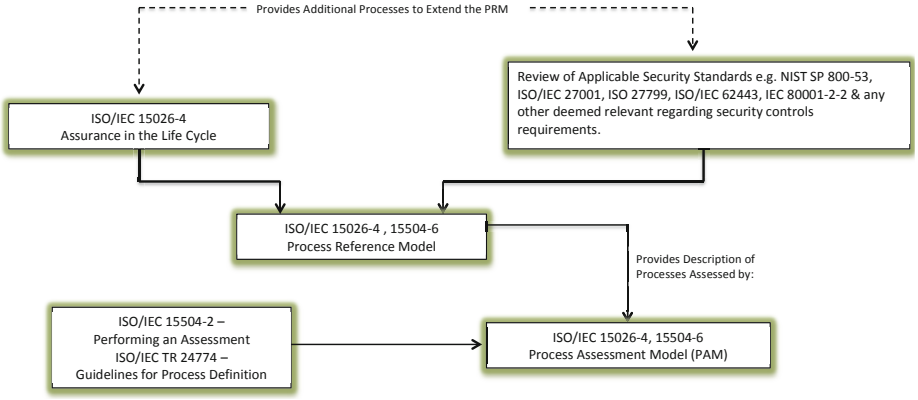

Fig. 1. Process Assurance Overview

2 Security Process Assurance

2.1 ISO/IEC 15504 – Process Assessment Model

The International standard for Software Process Improvement and Capability determination (ISO/IEC 15504) will be utilized to establish the development process capability level. Compliance with IEC/ISO 15504 results in the following outputs; a PRM and a PAM (including an aligned Measurement Framework). The PAM contains two dimensions, which are the Process Dimension and the Capability Dimension. The Process Dimension is developed from an external PRM that presents the processes for assessment in terms of their 'Purpose' and 'Outcome'. The PRM helps support process analysis and design activities as it provides a set of descriptions of the processes to be assessed. The PAM expands the PRM with the use of a set of Performance Indicators called Base Practices and Work Products. The Performance Indicators vary from process to process. Work Products are both, inputs to a process and also the outputs produced by a process. The Work Product Performance

Indicators are the results of performing the process and are used to review the effectiveness of each process. Base Practices are the actions taken to transform the inputs into outputs addressing the purpose of the process. They describe 'what' should be done in order to address the process but do not detail 'how' it should be done. The Base Practices are the basic required activities that specifically address the process purpose. Combined evidence of Work Practice characteristics and the performance of Base Practices provide the objective evidence of achievement of the 'Process Purpose'.

ISO/IEC 15504-2 [1] sets out a Capability dimension that utilizes six Capability Levels from Level 0, 'Incomplete' to Level 5, 'Optimizing'. ISO/IEC 15504-2 defines the measurement framework based upon a set of 9 Process Attributes associated with Levels one through to five. These Process Attributes represent measurable characteristics required to manage and improve each process. The extent of achievement of each attribute is defined on a rating scale. In ISO/IEC 15504-6, these Process Attributes include Generic Practices and Generic Work Products that belong to a set of Process Capability Indicators. These indicators provide the means of achievement of the capability addressed by each of the Process Attributes within each of the associated Capability Levels.

For the solution, the most suitable PRM is defined in ISO/IEC 15288 – *Systems Engineering – System Life Cycle Processes* [8] and forms the foundation for the PAM. ISO/IEC 15288 provides a process framework that covers the entire life cycle of systems from cradle to retirement. A system development life cycle standard is most applicable to networked medical devices as these devices may contain one or more of the following: *"Software, hardware, humans, processes (e.g. review processes), procedures (e.g. operator instructions), facilities and natural occurring entities (e.g. water, organisms, minerals)"*.

Due to the fact that ISO/IEC 15504-6 [3] uses ISO/IEC 15288 as the external PRM, this was then selected as a suitable foundation for the PAM. ISO/IEC 15504-6 details an exemplar PAM that also includes the process attributes that are compliant with ISO/IEC 15504-2. The Process Dimension utilizes the processes as defined in ISO/IEC 15288 and divides these into four groups which are the Agreement, Enterprise, Project and Technical processes. While the foundation PRM and the PAM framework addresses the entire system life cycle it has been extended for the inclusion of additional processes from ISO/IEC 15026-4 [9]. These processes are included as a measure to address security assurance of networked medical devices. This is discussed in the following section.

2.2 Building Additional Assurance into the PAM

Due to advancements in medical device designs and the fact that it is now proven that networked and interoperable medical devices are open to malicious attack, additional steps are required during the development life cycle to address security. An emphasis on security is required and has been achieved through the inclusion of processes in the PRM from ISO/IEC 15026-4 – *Systems and Software Engineering – Systems and Software assurance – 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 ISO/IEC 15288).

Table 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	3rd Party Components in Product Lifecycle Roadmaps	RDMP
18	Transmission Confidentiality	TXCF
19	Transmission Integrity	TXIG
20	Unique User ID	UUID

ISO/IEC 15026-4 is an international standard recently published that provides a process framework (Systems Assurance Process View) for software or a system that requires assurance for a particular aspect. This is usually when additional or careful attention is required for a particular system; otherwise known as a critical property. Critical properties are usually associated with substantial risk concerning safety, dependability, and reliability or, as we have adapted, security. The standard presents a set of add-on processes, activities and tasks with guidance and recommendations.

These processes, activities and tasks are intended to build upon the Agreement, Project and Technical processes as set out in ISO/IEC 15288. Therefore, conformance to this standard is achieved through the demonstration of these additional processes as well as conformance with the Agreement, Project and Technical processes of ISO/IEC 15288. For this reason, demonstration of additional assurance specifically addressing security, through the use of this standard, is suited for integration with the Process Assessment Model as set out in ISO/IEC 15504-6. The expected outcomes incorporating processes from IEC/ISO 15026-4 are [9]:

1. A subset of requirements for the achievement of critical properties is defined.
2. Assurance claims, their justification, and the body of information showing the achievement of the assurance claims for the critical properties are established as an element of the system.
3. A strategy for achieving these assurance claims and showing their achievement is defined.
4. The extent of achievement of the assurance claims is communicated to affected stakeholder.

3 Security Process Assurance

As we have developed this framework to specifically address security as the system critical property we have enhanced the PAM to focus on the Risk Management Processes where we introduce new considerations to be utilized during risk management activities (Process Reference PRJ.5 from ISO/IEC 15504-6). This paper discusses the security risk management process only and so this is additional to the normal practices for project and product risk management. This subsection looks at security standards and the development of a set of security controls for assuring the security of medical devices that will be validated and approved by medical device security experts in the domain and the FDA.

3.1 IEC/TR 80001-2-2

IEC/TR 80001-2-2 - Application of risk management for IT-networks incorporating medical devices - Guidance for the communication of medical device security needs, risks and controls [10] is a technical report which sets out to promote the communication of security controls, needs and risks of medical devices to be incorporated into IT networks between MDMs, IT vendors and HDOs. In this technical report there are a total of 20 security capabilities (Table 1) presented. These security capabilities provide a base template for a HDO to communicate their security requirements for a given medical device based on their needs. Prior to the acquisition of a medical device, HDO IT administrators may use this technical report to assist MDMs in establishing the HDO requirements. The benefit in adapting this approach is that the HDOs then become more aware of their requirements in order to securely incorporate a medical device into their network. It assists MDMs to better understand the intended use and environment in which the medical device will be utilized. However, the security requirements as indicated by the HDO are for guidance purposes only. The MDM will continue to carry out the usual risk analysis steps and upon completion of this will communicate back and agree with the HDO the necessary security capabilities for the product. This technical report will form the foundation for the security risk management process. The 20 security capabilities defined in IEC/TR 80001-2-2 will be included in the risk management process. A set of sub requirements, called Security Capability Requirements (SCRs) for each security capability will be required. These sub requirements present alternatives for implementation of a particular security capability. The security capabilities and their SCRs are intended to act as a template for communicating high level security requirements between the HDOs and MDMs. SCRs for each of the 20 security

capabilities in IEC/TR 80001-2-2 have been developed and will be validated through untilising the opinion of expert users, security researchers and also interested personal within the FDA. An example of a set of sub requirements for security capability Automatic Logoff is show in Table 2.

Table 2. Security Capability Requirements ALOF ALOF

Implementation Identifier	Capability
ALOF.01	A screensaver starts automatically 5 minutes after last keystroke/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 15504-6, Process PRJ.5 - Risk Management Process, the process purpose is to identify and assess threats and monitor the risks throughout the life cycle. The PAM further builds on this with the inclusion of the Base Practice 'PRJ.4.BP.2: Identify Risks' as a performance indicator. The MDM will conduct the risk assessment, considering the type of networked medical device, the design, its operational environment, the user and the users' needs (as communicated by the HDO). For each of these risks, the following Base Practices must be performed:

- PRJ.4.BP.3 Determine the Risk Occurrence Probability
- PRJ.4.BP.4 Evaluate the Risk Consequence
- PRJ.4.BP.5 Prioritize Risks
- PRJ.4.BP.6 Select Risk Treatment Strategies

The Base Practice PRJ.4.BP.6, Select Risk Treatment Strategy will detail the implementation of the SCRs for each security capability (such as Automatic Log Off, Unique User ID etc.) as communicated and agreed between the HDO and the MDM.

In addition, to the inclusion of the security capabilities presented in IEC/TR 80001-2-2, work has been carried out to survey an array of security standards and best practices. The standards reviewed were ISO/IEC 27001 [11], ISO/IEC 27799 [12], ISO 15408 [13], IEC 62443-3-3 [14] and NIST SP 800-53 [15]. Each of these standards and guidance documents similarly highlight security classes and controls with many repeating controls existing between standards. A security control matrix has been developed to map the controls across each standard and to identify cross over controls. An exhaustive list of security controls from all security standards has been compiled for review in terms of their relevance to networked medical devices. With this complete list of security controls from the above standards, a mapping has been done to link the security capabilities from IEC/TR 80001-2-2 to their attributing

security control(s). This will assist with the development of guidance documents for suitable security controls for networked medical devices. In addition to this, a gap analysis is being conducted in order to identify further capabilities/controls that should be included in IEC/TR 80001-2-2. This will be achieved through the use of expert opinion (i.e. expert users from industry and the FDA). The validated security controls, plus the existing IEC/TR 80001-2-2 security capabilities, will form the foundation for the security risk management process. A Technical Report will be published in the coming months detailing this security matrix gap analysis with the anticipation that IEC/TR 80001-2-2 will be revised based on this.

4 Conclusions and Future Work

This paper presents a framework for the assurance of networked medical devices in terms of security. The solution combines an array of international standards, guidance documents and processes to create a step-by-step process for MDMs. MDMs will follow this during development to decrease the risk of potential security vulnerabilities associated with the use of networked medical devices. As a PAM forms the foundation of this framework, with an associated measurement framework, it provides great benefits to the FDA and for external assessors in establishing the efficiency, thoroughness and quality of processes used to develop networked medical devices. This also benefits HDO's with supplier selection activities. The approach discussed in this paper focuses on development process assurance with the aim of positively impacting the overall security capability of networked medical devices. The remainder of this section describes the expected outputs from both the process and product assurance components of the approach. The output for the process assurance component is:

1. The development of a PAM based on the international standard ISO/IEC 15504-6 model that has been specifically developed for the international system life cycle process standard, ISO/IEC 15288. This PAM will be extended to include additional processes based on security being the critical property in line with yet another international standard for security assurance in the life cycle, ISO/IEC 15026-4.
2. A published technical report detailing the application and use of this extended PAM.
3. A validated set of applicable and meaningful security controls to be adopted and included in the Risk Management process of the PAM.
4. The publication of a technical report detailing the security controls required for consideration in using this approach. This is fully supported by the FDA and a Standard Committee Conveyor. It is expected that this be prioritised as a new work item within one of the Standard Committee Joint Working Groups. The expectation is the development of an international standard on the basis of this.

This framework will be trialed with MDMs and HDOs in both Europe and the US. Medical device security assurance driven development is a new concept and so future work will be to further build upon this to develop product specific SCRs following the

trialing of this with MDMs. Currently there is no method to specifically address security assurance for the development processes for networked medical devices. This is the primary focus of this research and so it is expected that the output of this 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 [4].

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 and supported in part by Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855.

References

1. ISO/IEC, 15504-2: 2003 Software Engineering - Process Assessment - Performing an Assessment (2003)
2. SEI, CMMI-DEV, CMMI for Development (2010)
3. ISO/IEC, 15504-6:2008 Information technology — Process assessment — An exemplar system life cycle process assessment model (2008)
4. Finnegan, A., McCaffery, F., Coleman, G.: Development of a process assessment model for assessing security of IT networks incorporating medical devices against ISO/IEC 15026-4. In: Healthinf 2013, Barcelona, Spain, pp. 250–255 (2013)
5. DHS, Attack Surface: Healthcare and Public Heath Sector (2012)
6. Rashid, F.Y.: Researchers Uncover Privilege Escalation Bug in Philips Medical Devices (2013), http://www.securityweek.com
7. GAO, Medical Devices, FDA Should Expland Its Consideration of Information Security for Certain Types of Devices (2012)
8. ISO/IEC, 15288 - Systems engineering — System life cycle processes (2008)
9. ISO/IEC, 15026-4: Systems and Software Engineering - Systems and Software Assurance - Assurance in the Life Cycle (2012)
10. 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 control, International Electrotechnical Committee (2011)
11. ISO/IEC, 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements (2005)
12. ISO, EN ISO 27799:2008 Health informatics. Information security management in health using ISO/IEC 27002 (2008)
13. ISO/IEC, 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT Security, in Introduction and General Model (2009)
14. IEC, 62443-3-3 – Security for industrial automation and control systems - Network and system security – System security requirements and security assurance levels Introductory Note (2011)
15. NIST, 800-53 Recommended Security Controls for Federal Information Systems and Organisations, U.S.D.o. Commerce, Editor (2009)