A Process Assessment Model for Security Assurance of Networked Medical Devices

Anita Finnegan, Fergal McCaffery, Gerry Coleman
[1] Regulated Software Research Group, Dundalk Institute of Technology & Lero,
Dundalk, Co Louth, Ireland
{anita.finnegan, fergal.mccaffery, gerry.coleman}@dkit.ie

Abstract. The recent introduction of networked medical devices has posed many benefits for both the healthcare industry and improved patient care. However, because of the complexity of these devices, in particular the advanced communication ability of these devices, security is becoming an increasing concern. This paper presents work to develop a framework to assure the security of medical devices being incorporated into an IT network. It begins by looking at the development processes and the assurance of these through the use of a Process Assessment Model with a major focus on the security risk management processes. With the inclusion of a set of specific security controls, both the Healthcare Delivery Organisations and the Medical Device Manufacturers work together to establish fundamental security requirements. The Medical Device Manufacturer reports the achieved security assurance level of their device through the development of a security assurance case. The purpose of this approach is to increase awareness of security vulnerabilities, risks and controls among Medical Device Manufacturers and Healthcare Delivery Organisations with the aim of increasing the overall security capability of medical devices.

Keywords: Process Assessment Model, Security Assurance, and Security Assurance Cases, Networked Medical Devices

1 Introduction

In terms of medical devices, design innovations over the last number of years have led to many outstanding benefits for patient care and healthcare providers. Such innovations include the increased use of software that has allowed Medical Device Manufacturers (MDMs) to add sophisticated functionality to devices such as insulin pumps that automatically detect dangerous glucose levels and administer the required insulin dosage to a diabetic patient. In the last few years we see an increase of interoperable and networked medical devices. Such medical devices have functionality to communicate via healthcare IT networks, wirelessly, across the Internet and from device to device. With this rise in the use and availability of networked medical devices, patients can now receive around-the-clock care even in the comfort of their own home outside the healthcare environment. This also benefits Healthcare Delivery Organizations (HDOs) greatly as the resource demand to administer this care is significantly reduced. HDOs utilize a wide range of networked

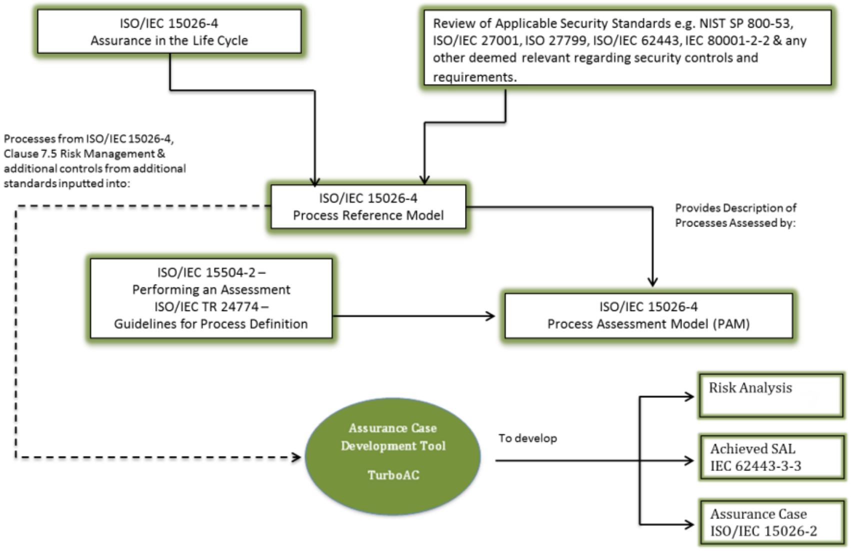
ISO/IEC 15026-4
Assurance in the Life Cycle
Review of Applicable Security Standards e.g. NIST SP 800-53, ISO/IEC 27001, ISO 27799, ISO/IEC 62443, IEC 80001-2-2 & any other deemed relevant regarding security controls and requirements.
Processes from ISO/IEC 15026-4, Clause 7.5 Risk Management & additional controls from additional standards inputted into:
ISO/IEC 15026-4
Process Reference Model
Provides Description of Processes Assessed by:
ISO/IEC 15504-2 – Performing an Assessment
ISO/IEC TR 24774 – Guidelines for Process Definition
ISO/IEC 15026-4
Process Assessment Model (PAM)
Assurance Case Development Tool
TurboAC
To develop
Risk Analysis
Achieved SAL
IEC 62443-3-3
Assurance Case
ISO/IEC 15026-2

Figure 1 - Approach Overview

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 which are associated with their use. These are security risks, threats and vulnerabilities. In a report issued by the Department of Homeland Security [1], typical threats associated with each type of device (implantable, external and portable medical devices) are highlighted. As this technology is relatively new, the fear among the medical device industry is that the security for these devices is insufficient and has not been thoroughly addressed in terms of research and design. What is probably most concerning is that malicious attackers have not yet fully exploited these devices but do have 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 hacked his own insulin pump during his presentation. This raised a lot of concern among the medical device domain and led to the interjection of the US government, which prompted the 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 [2] 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 being carried out to address security issues for medical devices to be incorporated into an IT network. Subsection 1.1 introduces our approach to address the problem background. Following on from this the paper divides the framework looking at process assurance and product assurance. Section two describes process assurance and discusses key standards. Section three details how the final product assurance in terms of security is addressed. Finally section four concludes the paper detailing next steps and the expected impact this work will have to the medical device industry including the HDOs, MDMs and also in terms of regulatory compliance assessment.

1.1 Overview

This work aims to address security in networked medical devices and build awareness of the types of security vulnerabilities and threats that can negatively impact the safety of patients. A key objective is to strengthen the relationship between MDMs and HDOs and also increase the HDO IT administrations' awareness of the security capability of the medical devices incorporated into their IT network.

This is achieved through the development and use of a Process Reference Model (PRM), a Process Assessment Model (PAM) and a Process Measurement Framework in compliance with IEC/ISO 15504-2 [3] for the assurance of MDMs development processes and establishment of a process capability level. In addition to this, this work will also develop a separate framework to establish security assurance levels of the final product in relation to a series of security controls. This will involve the use of a tool for the risk management process which also incorporates Security Assurance Case development. This will assist HDOs to better understand the suitability of the medical device for installation into their IT network. It will also impact MDMs in their design decisions during development of the medical devices. Figure 1 shows a high-level overview of the research objectives and framework, which is discussed in detail in the following two sections.

2 Security Process Assurance

2.1 The Process Assessment Model in Compliance with ISO/IEC 15504

As previously mentioned, ISO/IEC 15504 will be utilized to establish the development process capability level. Compliance with IEC/ISO 15504 results in the following outputs; a Process Reference Model (PRM), a Process Assessment Model (PAM) and a process capability level.

For the purpose of this research, the most suitable Process Reference Model (PRM) is defined in ISO/IEC 15288 – Systems Engineering – System Life Cycle Processes [4] will form the foundation for the PAM. ISO/IEC 15288 provides a process framework that covers the entire life cycle of systems from cradle to grave. A system is defined in this standard as having one of 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).*

As ISO/IEC 15504-6 [5] uses ISO/IEC 15288 as the external PRM, this has been 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 PAM contains two dimensions; the Process Dimension and the Capability

Dimension. The Process Dimension utilizes the processes as defined in ISO/IEC 15288 and describes these in terms of their 'Process' and 'Outcome' dividing these into four groups. These are Agreement, Enterprise, Project and Technical processes. The PAM expands the PRM with the use of Performance Indicators called Base Practices (BP) and Work Products (WP). Base Practices are the basic required activities that specifically address the process purpose. They describe 'what' should be done in order to address the process but do not detail 'how' it should be done. Work Product performance indicators are the result of performing the process and are used to review the effectiveness of each process. Combined evidence of Work Practice characteristics and the performance of Base Practices provide the objective evidence of achievement of the 'Process Purpose'.

Table 1 - ISO/IEC 15504-2, Rating Scale

Indicator	Meaning	Value
N	Not Achieved	0 to 15% achievement
P	Partially Achieved	>15% to 50% achievement
L	Largely Achieved	>50% to 85% achievement
F	Fully Achieved	>85% to 100% achievement

The Capability Dimension, as set out in ISO/IEC 15504-2, utilizes six Capability Levels from Level 0, 'Non Performing' to Level 5, 'Optimizing'. As defined in ISO/IEC 15504-2, the measurement framework is based upon a set of Process Attributes of which there are a total of nine associated with Levels 1 through to 5. 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 indicated in ISO/IEC 15504-2 and represented in Table 1. In ISO/IEC 15504-6, these Process Attributes include Generic Work Practices, which belong to a set of Process Capability Indicators. These indicators are the means of achievement of the capability addressed by each of the Process Attributes within each of the associated Capability Levels.

The PAM is being developed in compliance with ISO/IEC 15504-2. ISO/IEC 15504-6 will form the foundation of the model as it contains the processes necessary for compliance with ISO/IEC 15288. To further extend the PRM and the PAM, additional processes from ISO/IEC 15026-4 [6] will also be included in order to address security assurance. 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.

2.1 Building Additional Assurance into the PAM

Due to the criticality of medical device security, additional assurance during the development life cycle is achieved through the inclusion of ISO/IEC 15026-4 – Systems and Software Engineering – Systems and Software assurance – Assurance in the life cycle - processes in the PRM.

ISO/IEC 15026-4 is a relatively new standard providing a process framework (Systems Assurance Process View) for software or systems that require an assurance claim for particular systems aspects that require additional attention, otherwise known as critical properties. Critical properties are usually in areas where substantial risk is involved such as safety, dependability, reliability and in this case, 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 relates and integrates well with the Process Assessment Model as set out in ISO/IEC 15026-4. Table 2 presents the relationship between ISO/IEC 15288, ISO/IEC 15504-6 and ISO/IEC 15026-4. The black cells represent the family of processes addressed in ISO/IEC 15288. The grey shaded cells indicate processes that include additional recommendations for the assurance of the final product in terms of security being the critical property. With the successful implementation of ISO/IEC 15026-4, the following expected outcomes are:

a) *A subset of requirements for the achievement of critical properties is defined.*
b) *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.*[1]
c) *A strategy for achieving these assurance claims and showing their achievement is defined.*
d) *The extent of achievement of the assurance claims is communicated to affected stakeholder.*

[1] Assurance claims, the framework and reasoning for use is detailed in section 3.2 of this paper.

Table 2 – Standards Process Relationship

Agreement Processes		
ISO/IEC 15288	**ISO/IEC 15504-6**	**ISO/IEC 15026-4**
Acquisition Processes	AGR.1	7.1
Supply Processes	AGR.2	
Enterprise Resources		
ISO/IEC 15288	**ISO/IEC 15504-6**	**ISO/IEC 15026-4**
Enterprise Environment Management Process	ENT.1	
Investment Management Process	ENT.2	
System Life Cycle Processes Management Process	ENT.3	
Resource Management Process	ENT.4	
Quality Management Process	ENT.5	
Project Resources		
ISO/IEC 15288	**ISO/IEC 15504-6**	**ISO/IEC 15026-4**
Project Planning Process	PRJ.1	7.3
Project Assessment Process	PRJ.2	
Project Control Process	PRJ.3	
Decision-Making Process	PRJ.4	7.4
Risk Management Process	PRJ.5	7.5
Configuration Management Process	PRJ.6	7.6
Information Management Process	PRJ.7	7.7
Technical Resources		
ISO/IEC 15288	**ISO/IEC 15504-6**	**ISO/IEC 15026-4**
Stakeholder Requirements Definition Process	TEC.1	7.8
Requirements Analysis Process	TEC.2	7.9
Architectural Design Process	TEC.3	
Implementation Process	TEC.4	
Integration Process	TEC.5	
Verification Process	TEC.6	7.10
Transition Process	TEC.7	
Validation Process	TEC.8	
Operation Process	TEC.9	7.11

3 Security Product Assurance

To specifically address security as the system critical property, the PAM again, will be further extended. In this section we focus on the Security Risk Management Processes and introduce new considerations and tools to be utilized during security risk management activities (Process Reference PRJ.5 from ISO/IEC 15504-6). Section 3.1 discusses security standards, security controls and the development of a validated expert reviewed set of security controls to be adopted by this framework in assuring the security of medical devices. Section 3.2 then discusses security assurance cases, the benefits of developing security assurance cases and how security assurance cases are employed in this framework. Finally, section 3.3 introduces a schema for generating a security assurance value for the final product and discusses the benefits of generating such a value to the medical device industry.

3.1 Security Controls for the Risk Management Process

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* [7] 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. This technical report presents 20 security capabilities that both the HDOs use to communicate their security requirements prior to acquisition of a medical device and the MDMs use to communicate the final status of the product in relation to those security capabilities. This technical report will form the foundation for the security risk management process in that; the 20 capabilities here will be included in the risk management process. Reasons for exclusion of capabilities or those deemed unnecessary for a particular product must still be justified and documented. For example, in 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 extends this with the inclusion of Base Practice '*PRJ.4.BP.2: Identify Risks'* as a performance indicator. These processes are further adapted to address security risks in addition to project or product risks. The outcome of this work will be the inclusion of a list of security risks here, which a MDM must address during the security risk management process in order to ensure the desired security capability of the medical device is achieved. For each of these security risks, evidence must be provided to prove that the Base Practices were carried out with the full list of controls considered. For example, consider the security capability from IEC/TR 80001-2-2, *Automatic Log Off,* the MDM must consider this control and establish whether there is a risk associated with the elimination of the control. If no risk is associated, evidence will be provided and documented to prove this. If, however, a risk is identified due to the elimination of this control then the MDM must follow through the rest of the Base Practices for the Security Risk Management Process. These are:

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*

Base Practice PRJ.4.BP.6, Select Risk Treatment Strategy will be the security control, *Automatic Log Off* functionality.

One of the first steps in this work was to determine the security controls that should be included in the security risk management process. This was done by carrying out a cross-standard review of all security controls to establish if there are gaps in the 20 capabilities of IEC 80001-2-2. The standards reviewed were ISO/IEC 27001 [8], ISO/IEC 27799 [9], ISO 15408 [10], IEC 62443-3-3 [11] and NIST SP 800-53 [12]. Each of these standards and guidance documents similarly highlight security classes and controls and, as a result many controls are presented in numerous standards. For this reason a security control matrix has been developed to map the controls from each standard and identify those similar to compile a complete set of controls addressed in all standards. Those controls that relate will be rated in terms of their similarity. Following on from this, a gap analysis will be conducted in order to identify further capabilities that should be included in IEC 80001-2-2. This will be achieved through the use of expert opinion. The expert users from industry plus the FDA will validate the controls. The validated security controls 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. The architecture of this framework will then be somewhat consolidated to use only the capabilities outlined in IEC 80001-2-2 as opposed to a multitude of standards. This will provide benefits for MDMs and HDOs in that they only need update their security risk management processes in line with one source standard.

3.2 Security Assurance Cases – Building-In Assurance

In support of IEC/TR 80001-2-2, development of security assurance cases are a key element of this framework for the interchange of security assurance information between MDMs and HDOs. Traditionally, assurance cases in the medical device domain have been used to address safety concerns. Since April 2010, Infusion Pump manufacturers have been operating under the Infusion Pump Improvement Initiative where a draft guidance document [13] recommends the use of assurance cases for use during the approval process for new Infusion Pumps entering the market. The FDA recommends the use of assurance cases to communicate information about the safety of the device and how risks have been identified and mitigated [13].

> *"In making this demonstration of substantial equivalence for your infusion pump, FDA recommends that you submit your information through a framework known as an assurance case or assurance case report."*

Assurance cases can be defined as “a reasoned and compelling argument, supported by a body of evidence, that a system, service or organization will operate as intended for a defined application in a defined environment [14]. They are most often used when the requirement to demonstrate that a system or software exhibit a critical property that is usually risk-related and requires additional assurance such as safety, dependability or, in this case, security. Assurance cases are quite often compared to legal cases where a claim is supported by a comprehensive argument showing how evidence supports the overall claim. Therefore, the three main components of an assurance case as defined in the GSN standard [14] are:

1. **Claim** A proposition being asserted by the author that is a true or false statement i.e. the system is adequately secure.
2. **Argument** A body of information presented with the intention to establish one or more claims through the presentation of related supporting claims, evidence and contextual information.
3. **Evidence** Information or objective artifacts being offered in support of one or more claims. Evidence may include component test results, policies, code reviews, training records, good processes among others.

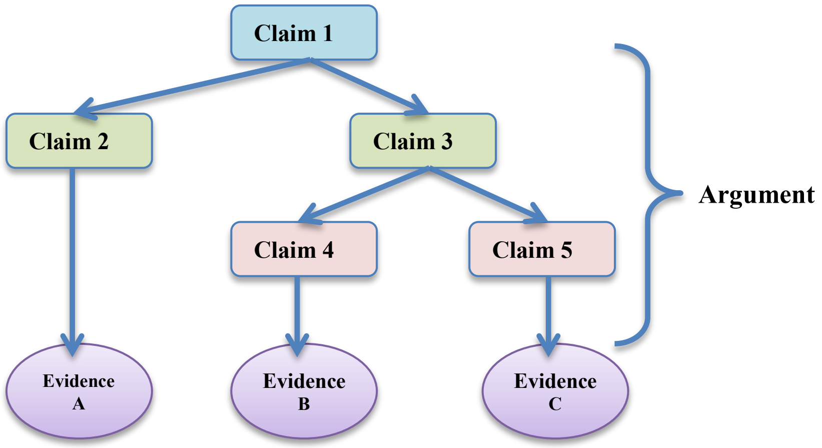

Figure 2 – Assurance Claim Structure

Looking at Figure 2 (a simplistic layout of an assurance case) we can now say:

If Evidence A **then** Claim 2
If Evidence B **then** Claim 4
If Evidence C **then** Claim 5
If Claim 4 **&** Claim 5 **then** Claim 3
If Claim 2 **&** Claim 3 **then** Claim 1

For this work, the proposed method for development of the security assurance cases focuses fundamentally on the security capability requirements as agreed between the HDO and the MDM (section 3.3). During the security risk management process, the manufacturer will utilize a software tool for the development of the risk analysis and the FMEA. This tool has been specifically developed for manufacturers of safety critical products to assist in the development, management and maintenance of the risk management processes. This particular tool works quite well with the artifacts of this framework as it automatically generates an assurance case through the progression of the FMEA process. The security assurance case arguments and evidence will relate directly to the achievement of each of the security capabilities and so for example, if 'Authentication' is defined as a requirement by the HDO then the evidence could detail login and password controls as implemented by the MDM. The assurance case will clearly identify the relationships between the claims to assist manufacturers in developing a meaningful and thorough argument resulting in adequate evidence to support a higher level claim stating that the system is acceptably.

To further ensure the strength of the argument, guidelines will also be published to assist the MDMs in establishing the security assurance level of their product based on the evidence gathered. This is discussed in more detail in the following subsection.

3.3 – Establishment of the Final Product Security Assurance Level

Communication of a Security Assurance Level (SAL) to HDOs will provide a simple and meaningful method for establishing suitability of the device for the users need and its environment. To do this, IEC 62443-3-3 is being used as a guide for establishing the system security assurance level by the MDMs. As previously stated, the HDO will determine the appropriate security capabilities from within IEC/TR 80001-2-2 along with any other validated capabilities from other standards should they not be included here. The communication of the security capabilities from the HDO is used as a means to open discussion only between the HDO and the MDM. The purpose of this is to build awareness of security risks, threats and vulnerabilities among HDOs. MDMs carry out the security risk management processes thereafter. With regards the different types of SAL, the critical value is the achieved SAL (SAL-A) since this is most valuable to the HDO and the FDA when establishing the security capability of the product. Post product development, the MDM will communicate the SAL-A to the HDO which will be based on the agreed target SAL (SAL-T) level (0-4) as determined by both the MDM and HDO at the start of the acquisition process. The SAL vector detailing the assurance level and security capabilities is presented here:

SAL-A = (FR, domain) = {AC UC DI DC RDF TRE RA}
SAL-A = (FR, domain) = {3 3 3 3 2 1 0}

Table 3 - IEC 62443-3-3 Foundational Requirements

Foundational Requirement	Code
Identification and Authentication Control	IAC
Use Control	UC
Data Integrity	DI
Data Confidentiality	DC
Restricted Data Flow	RDF
Timely Response to Events	TRE
Resource Availability	RA

For each of the parameters within the vector (refer to table 3 for Foundational Requirements (FR) descriptions), a value of zero to four will be used to represent the SAL level for that particular requirement. A SAL Level 4 represents medical devices that have undergone most rigour in terms of security assurance. Following on from this, the MDM will then verify the selected SAL level through the use of the SAL Mapping Matrix as shown in Annex B of IEC 62443-3-3, which will also be included in the PRM. This information, prior to a HDO installing the medical device into their IT network will be communicated to them by the MDM.

4 Conclusion

This paper presents a two-step framework for the assurance of networked and interoperable medical devices in terms of security. The framework combines an array of standards, guidance documents and processes to create a step by step process for MDMs to use during development. The objective is to decrease the risk of potential security vulnerabilities associated with the use of networked medical devices. As one component of the framework is a process assessment model with an associated measurement framework it provides great benefits to the FDA and for external assessors in establishing process quality. The framework presented in this paper is twofold, addressing process assurance and also final product security assurance separately.

The output for the process assurance component is:

1. The development of an extended PAM and PRM.
2. A validated set of applicable and meaningful security controls to be adopted and included in the Risk Management process of the PAM.
3. The publication of a technical report detailing the security controls required for consideration in using this framework.

The expected output for the product assurance component is:

1. A technical report detailing the strategy and framework for carrying out the Risk Management process with the use of a software tool.
2. A framework for addressing the security controls and building a security assurance case around these controls.
3. A framework for the assignment of achieved security assurance levels for a networked medical device.

It is expected that this framework will be trialled with MDMs and HDOs in both Europe and the US. In applying this, MDMs will have three major outputs upon application.

These outputs are:

1. A process maturity level for the development of the product.
2. An achieved security assurance level (SAL-A) for the final product.
3. A security assurance case detailing in depth, the arguments and evidence supporting the security claim for the medical device. This assurance case will be used to communicate the security assurance of the product to the HDO where the medical device will be installed.

Currently no such framework exists to address both the development processes and the security product capabilities of networked medical devices. This is the primary focus of this work, hence, it is envisaged that the output of this work will positively impact the medical device domain by building awareness of security vulnerabilities, threats and related risks for HDOs and MDMs [15].

5 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.

References

1. DHS, Attack Surface: Healthcare and Public Heath Sector. 2012.
2. Government Accountability Office, Medical Devices, FDA Should Expland Its Consideration of Information Security for Certain Types of Devices, GAO, Editor 2012.
3. ISO/IEC, 15504-2: 2003 Software Engineering - Process Assessment - Performing an Assessment, 2003.
4. ISO/IEC, 15288 - Systems engineering — System life cycle processes, 2008.
5. ISO/IEC, 15504-6:2008 Information technology — Process assessment — An exemplar system life cycle process assessment model, 2008.
6. ISO/IEC, 15026-4: Systems and Software Engineering - Systems and Software Assurance - Assurance in the Life Cycle, 2012.
7. IEC, TR 80001-2-2 - Application of risk management for IT-networks incorporating medical devices - Guidance for the disclosure and communication of medical device security needs, risks and controls, 2011, International Electrotechnical Committee,. p. Page 30.
8. ISO/IEC, 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements, 2005.
9. ISO, EN ISO 27799:2008 Health informatics. Information security management in health using ISO/IEC 27002, 2008.
10. ISO/IEC, 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT Security, in Introduction and General Model2009.
11. 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.
12. NIST, 800-53 Recommended Security Controls for Federal Information Systems and Organisations, U.S.D.o. Commerce, Editor 2009.
13. FDA, Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions - Draft Guidance, 2010.
14. Consulting (York) Ltd, GSN Community Standard Version 1, 2011.
15. Finnegan, A., F. McCaffery, and G. Coleman, Development of a process assessment model for assessing security of IT networks incorporating medical devices against ISO/IEC 15026-4, in Healthinf 2013: Barcelona, Spain.