Safety Critical Software Development – Extending Quality Management System Practices to Achieve Compliance with Regulatory Requirements

Andrzej Beniamin Bujok[1], Silvana Togneri MacMahon[1], Fergal McCaffery[1], Dick Whelan[2], Bernard Mulcahy[2], William J Rickard[3]

[1]Regulated Software Research Centre at Dundalk Institute of Technology,
Dublin Road, Dundalk, Ireland
{andrzej.bujok, silvana.macmahon, fergal.mccaffery}@dkit.ie
[2]Almir Business Limited, 2 Mungret Street, Limerick, Ireland
{dw, bm}@almir.biz
[3]Dabl Ltd., Carraig Court, Georges Avenue, Blackrock, Co. Dublin, Ireland
wjrickard@dabl.eu

Abstract. Software is increasingly being used to provide functionality in safety critical domains. The complexity involved in the development of software for these domains can bring challenges concerned with safety and security. International standards are published, providing information on practices which must be implemented in order to satisfy the regulations. This paper details an investigation of the relevant standards that companies need to implement in order to satisfy the regulatory requirements. A literature review was conducted which examines the relevant Quality management system, Risk Management and Software development standards across the safety critical domains. To examine the challenges in implementing these standards, interviews were conducted with a medical device software development company having a Quality management system in place and beginning to implement the relevant Software development standards. In addition, an interview was conducted with a consultancy company who have experience in the implementation and maintenance of Quality management systems in small and medium enterprises. Future work will focus on the integration of practices which need to be implemented by companies developing safety critical software.

Keywords: Quality management system, Risk Management, Software development, Standards, Safety critical software development, Regulatory requirements, Integrated use of standards, Small and medium enterprises.

1 Introduction

Software is increasingly being used to provide functionality in safety critical domains such as Medical device; Automotive; or Aviation, Space and Defence. For instance, a premium class car now contains 100 microprocessors and runs on 100m lines of software code. To a software engineer this makes a car like a computer [1]. Safety-critical systems are defined as: *"systems whose failure could result in loss of life, significant property damage, or damage to the environment."* [2] As the use of software, whether embedded or standalone, grows in safety critical domains, functionality also increases thus improving quality of services being provided and the products being produced. For example, software is increasingly being used in medical devices for diagnostic [3] or treatment purposes [4] [5] [6].

However, the increased use of software brings new challenges concerned with safety and security issues. For example attackers have tried to infect medical devices with malware in order to steal confidential data [7]. Another example of a security issue is an instance when a team of computer security researchers was able to gain wireless access to a combination heart defibrillator and pacemaker and were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal if the device had been implanted within a patient. In this case, the researchers were hacking into a device in a laboratory [8]. These examples show the possibility that the confidential data about patient's health could be stolen and misused to cause some damage. As a result a considerable amount of attention is dedicated to these issues, not only on the country government and legal level but also there is a great need to solve them on international level [9] [10].

To have regulatory oversight of the safety critical domains government bodies issue regulatory requirements. In European countries they can be based on the regulatory framework provided by European Union (EU) Council [11], and in United States (US) by Federal Government [12]. In terms of medical devices and the healthcare domain, the EU Council directives [13] and US Code of regulations were issued [14]. If product or service complies with regulatory requirements, a certificate is issued, which entitles the organization to sell products on the market [15].

The paper examines how the use of Quality management system standards can be combined with the use of Software development and Risk management standards in order to implement practices which will allow developers to comply with the relevant regulations. This also ensures that issues concerning the safety and security of the software are avoided. The remainder of this paper is structured as follows. Section 2 presents a literature review of the relevant Quality management system (QMS) standards, Risk Management (RM) and Software development (SD) standards for a number of safety critical domains. This section presents an outline of the relevant standards that were examined for each of the safety critical domains and provides a brief description of the regulatory environments for the Medical; Automotive; and Aviation and Aerospace domains. Section 3 presents two mappings of these standards. One mapping focuses on an examination of QMS standards while the other focuses on SD standards related to safety critical domains. The purpose of the mapping is to identify a core set of requirements which are common across the standards and to identify those requirements which are specific to a certain domain. Section 4 presents the results of the interviews which were conducted to investigate the challenges experienced by companies attempting to integrate and implement the standards. Section 5 describes the research conducted to date and outlines next steps for the future work. Section 6 presents the conclusions of this paper.

2 Quality Management System, Software Development and Risk Management Standards in Safety Critical domains

Non-government organizations for standardization produce standards which contribute to achieving compliance with the regulatory requirements for safety critical software development [16] [17] such as:

- *ISO 9001:2015 – Quality management systems Requirements* [18]
- *ISO/IEC 15288:2015 Systems and software engineering – System lifecycle processes* [19] *and ISO/IEC 12207:2008 – Systems and software engineering – Software lifecycle processes* [20]
- *ISO 31000:2009 Risk management – Principles and guidelines* [21] and *IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - General requirements*

Many standards are harmonized with respect to US regulations – *"Recognized Consensus Standards"* [22], and European directives [23]. Harmonized standards are:

> *"European Standards, adopted by CEN, CENELEC or ETSI, following a mandate or order issued by the European Commission. Compliance with harmonized standards, for which the reference numbers have been published in the Official Journal of the EU and which have been transposed into national standards, provides a presumption of conformity to the corresponding essential requirements of the EU Directives."* [24]

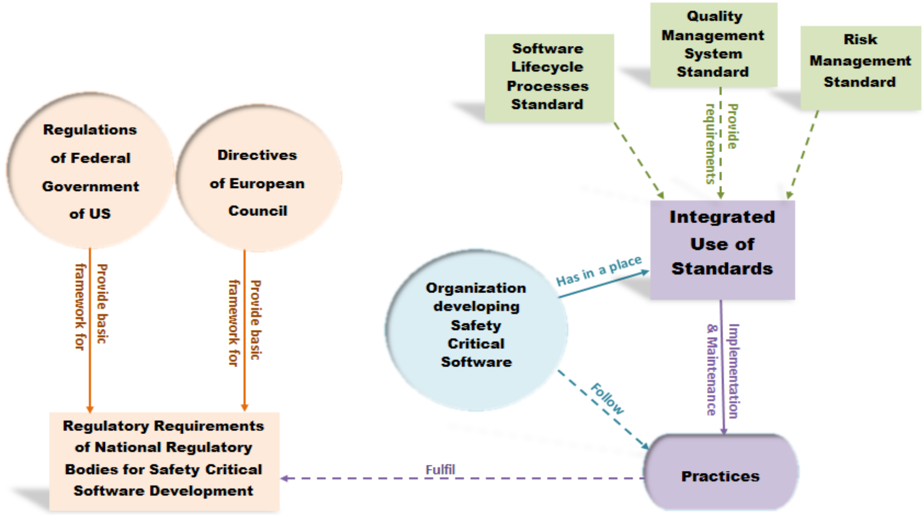

Software Lifecycle Processes Standard
Quality Management System Standard
Risk Management Standard
Provide requirements
Regulations of Federal Government of US
Directives of European Council
Integrated Use of Standards
Has in a place
Organization developing Safety Critical Software
Provide basic framework for
Provide basic framework for
Implementation & Maintenance
Follow
Regulatory Requirements of National Regulatory Bodies for Safety Critical Software Development
Fulfil
Practices

Fig. 1. Integrated requirements of Quality management system, Software development and Risk management standards implemented as required practices in safety critical domains.

The need for implementation of several standards within one domain has resulted in organisations attempting to integrate the requirements of several standards. As a result, ISO organization published guidance on the Integrated use of management system standards [25]. Due to need to integrate an increasing number of standards this publication is currently being revised. Figure 1 shows how Quality management system; Software development; and Risk management standards; represented by the fields at the top right side of diagram, are integrated and consequently implemented as practices. Organizations developing safety critical software need to have Quality management system standard in place and subsequently follow the practices from other standards. Such integrated use of standards provides practices that fulfil the regulatory requirements. In the following subsections there is an explanation of the standards that were examined for each of the listed above safety critical domains. During the initial phases of the research to date, the main focus is on the Medical device domain. This domain will be used as an exemplar of the research approach taken, which can then be applied to the other safety critical domains.

2.1 Standards in the Medical Device Domain

Significant research on Medical device domain has been conducted by other researchers from Regulated Software Research Centre at Dundalk Institute of Technology in Dundalk within last few years. Various fields related to medical device software development were investigated, such as Software process improvement and Roadmaps [26], Integration agile with a Medical device software development [27], Development of process assessment model for assessing medical IT networks against *IEC 80001-1* [28], Investigation of traceability within a medical device organization [29] [30], and others. This paper extends the research being conducted within the centre and through an examination of what standards organizations having *ISO 13485:2012 Medical devices – Quality management systems – Requirements for regulatory purposes* [31] or more generic QMS already in place, need to implement to fulfil the regulatory requirements for the development of software in safety critical domains. This section of the paper examines the standards which are relevant to the medical device domain.

For Medical device developers the *ISO 13485:2012* is seen as the first step in obtaining certification and CE mark for their product. However, QMS is not strictly related to Software development issues, therefore, the *IEC 62304:2006 Medical device software – Software life-cycle processes* [32] standard is also required. The QMS standard addresses the quality management issues but does not address the software lifecycle issues that are addressed by *IEC 62304*. *IEC 62304* is harmonized by the EU and the US and is used as a benchmark for Medical device software development to comply with regulatory requirements. *IEC 62304* standard requires that *ISO 13485:2012*; and *ISO 14971:2012 Medical devices — Application of risk management to medical devices* [33]; are also in place. And additionally there is a Technical report *IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software* [34]. Figure 2 shows the relevant standards, the requirements of which need to be in place to form the Integrated use of standards. Organizations developing medical device software, which are represented in the figure by the circle on the left side, need to have integrated use of standards in place and follow the implemented practices. Through the integrated use of these standards, the regulatory requirements represented by fields placed on the left side of the diagram can be fulfilled.

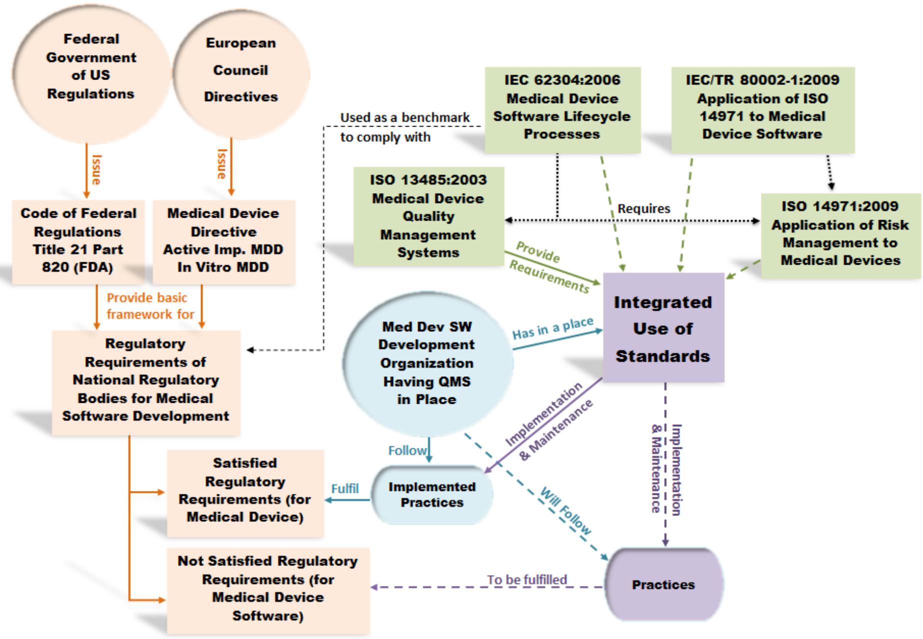

Federal Government of US Regulations
European Council Directives
Issue
Issue
Code of Federal Regulations Title 21 Part 820 (FDA)
Medical Device Directive Active Imp. MDD In Vitro MDD
Provide basic framework for
Regulatory Requirements of National Regulatory Bodies for Medical Software Development
Used as a benchmark to comply with
IEC 62304:2006 Medical Device Software Lifecycle Processes
IEC/TR 80002-1:2009 Application of ISO 14971 to Medical Device Software
ISO 13485:2003 Medical Device Quality Management Systems
Requires
ISO 14971:2009 Application of Risk Management to Medical Devices
Provide Requirements
Integrated Use of Standards
Med Dev SW Development Organization Having QMS in Place
Has in a place
Implementation & Maintenance
Implementation & Maintenance
Follow
Satisfied Regulatory Requirements (for Medical Device)
Fulfil
Implemented Practices
Will Follow
Not Satisfied Regulatory Requirements (for Medical Device Software)
To be fulfilled
Practices

Fig. 2. Integrated requirements of ISO 13485, IEC 62304 and ISO 14971 implemented as required practices for Medical device software domain.

2.2 Standards in the Automotive Domain

The Automotive domain can be illustrated by diagram similar to the general one in Figure 1, but there are specific standards for automotive domain, that are considered for integration in the general diagram.

- For QMS: *ISO/TS 16949:2009 Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations* [35]
- for SD: *ISO 15497:2000 Road vehicles – Development guidelines for vehicle based software* [36] and *ISO 26262-6:2011 Road vehicles — Functional safety Part 6 : Product development at the software level* [37] together with *ISO 26262-8:2011 Road vehicles — Functional safety Part 8 : Supporting processes* [38]
- for RM: *ISO 26262-9:2011 Road vehicles — Functional safety Part 9 : Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses* [39].

2.3 Standards in the Aviation and Aerospace Domain

Similarly for the Aviation, Space and Defence domain there are specific standards:

- for QMS: *EN 9100: 2009 Quality Management Systems — Requirements for Aviation, Space and Defence Organizations* [40] and *EN 9115 : 2013 Quality Management Systems — Requirements for Aviation , Space and Defence Organizations — Deliverable Software* [41]
- for SD: *RTCA DO-178C:2011 Software Consideration in Airborne Systems and Equipmqnt Certification* [42]
- for RM: *EN 16601-80:2014 Space project management Risk management* [43]

2.4 Challenges of Software Development for Safety Critical Domains

The introduction of this paper identifies challenges faced by organizations developing software in safety critical domain related to safety and security issues and in compliance with regulations. For some of the safety critical domains there is a need for implementation of more than one standard. The need for knowledge of different standards and practices to be implemented, and of standards integration, gives another challenge to software developers. Following the completion of the literature review of the relevant standards related to each of the safety critical domains, two additional phases of the research process were completed as follows:

- A comparison of the QMS standards and related SD standards across the safety critical domains was performed
- An investigation of the challenges experienced by companies implementing these standards was conducted

The comparison of the standards was conducted to identify a core set of requirements which are common across the standards and to identify those requirements which are specific to a certain domain. Following the literature review and the mapping of the standards, the focus of the research was then to gain an understanding of the challenges that are experienced by companies when trying to integrate and implement these standards. The following section of this paper discusses the approach to and the results of the mapping of the standards. The results of the investigation of the challenges in implementing the standards are presented in section 4.

3 Mapping of QMS and SD standards related to different domains

This section provides a description of the mappings of the standards that have been completed as part of this research. One mapping focuses on an examination of QMS standards while the other focuses on SD standards related to different safety critical domains. The future work will include also the mapping of RM standards. The purpose of the mapping was to examine areas which are common among the standards and also to investigate the differences among them. Initially the focus of the research was on Medical device domain and medical device software development, but was then expanded to examine the use of QMS, RM and aligned SD standards in other safety critical domains, like Automotive; and Aviation, Space & Defence.

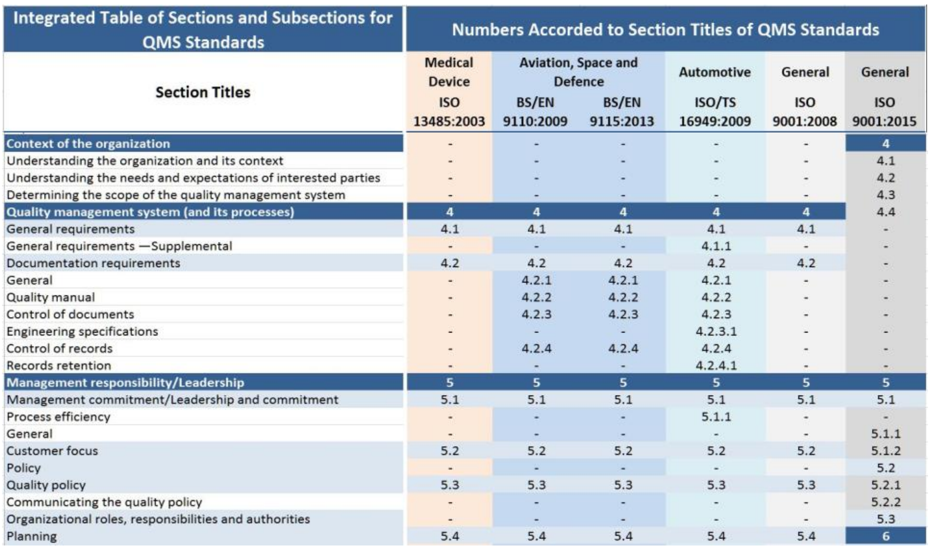
It has been observed that the set of standards, which is necessary for medical device software development, as QMS, SD and RM, is common for other safety critical domains and that each domain has corresponding standards related to this domain. Accordingly, there is specific QMS for Medical device, specific QMS for Automotive, and specific QMS for Aviation, Space and Defence domains. As a next step of the research on standards integration we need to define, what is common for these standards and develop common core.

Consequently the research subject has been expanded to:

- What are the required practices of integrated use of standards for safety critical software development domain to comply with regulatory requirements
- How can the implementation of integrated use of standards become more feasible for software developers in terms of small and medium enterprises

For the indicated domains – Medical device; Automotive; Aviation, Space and Defence; the cross industry cross reference mapping of sections and subsections for QMS standards has been conducted as a first step of standards mapping. As an outcome the cross reference table has been created presenting differences and what is common for researched industries. The sample of the table for QMS standards is introduced on Table 1. There are six different QMS standards represented in the table: *General ISO 9001 QMS*, which is foundation QMS and is used as a base for development of domain specific QMS standards, *Medical Device 13485 QMS*, *Aviation, Space and Defence EN 9100 AND EN 9115 QMS* and *Automotive ISO 16040 QMS*.

Table 1. The sample of mapping conducted of QMS standards for different safety critical domains.



Integrated Table of Sections and Subsections for QMS Standards	Numbers Accorded to Section Titles of QMS Standards					
Section Titles	Medical Device	Aviation, Space and Defence		Automotive	General	General
	ISO 13485:2003	BS/EN 9110:2009	BS/EN 9115:2013	ISO/TS 16949:2009	ISO 9001:2008	ISO 9001:2015
Context of the organization	-	-	-	-	-	4
Understanding the organization and its context	-	-	-	-	-	4.1
Understanding the needs and expectations of interested parties	-	-	-	-	-	4.2
Determining the scope of the quality management system	-	-	-	-	-	4.3
Quality management system (and its processes)	4	4	4	4	4	4.4
General requirements	4.1	4.1	4.1	4.1	4.1	-
General requirements —Supplemental	-	-	-	4.1.1	-	-
Documentation requirements	4.2	4.2	4.2	4.2	4.2	-
General	-	4.2.1	4.2.1	4.2.1	-	-
Quality manual	-	4.2.2	4.2.2	4.2.2	-	-
Control of documents	-	4.2.3	4.2.3	4.2.3	-	-
Engineering specifications	-	-	-	4.2.3.1	-	-
Control of records	-	4.2.4	4.2.4	4.2.4	-	-
Records retention	-	-	-	4.2.4.1	-	-
Management responsibility/Leadership	5	5	5	5	5	5
Management commitment/Leadership and commitment	5.1	5.1	5.1	5.1	5.1	5.1
Process efficiency	-	-	-	5.1.1	-	-
General	-	-	-	-	-	5.1.1
Customer focus	5.2	5.2	5.2	5.2	5.2	5.1.2
Policy	-	-	-	-	-	5.2
Quality policy	5.3	5.3	5.3	5.3	5.3	5.2.1
Communicating the quality policy	-	-	-	-	-	5.2.2
Organizational roles, responsibilities and authorities	-	-	-	-	-	5.3
Planning	5.4	5.4	5.4	5.4	5.4	6

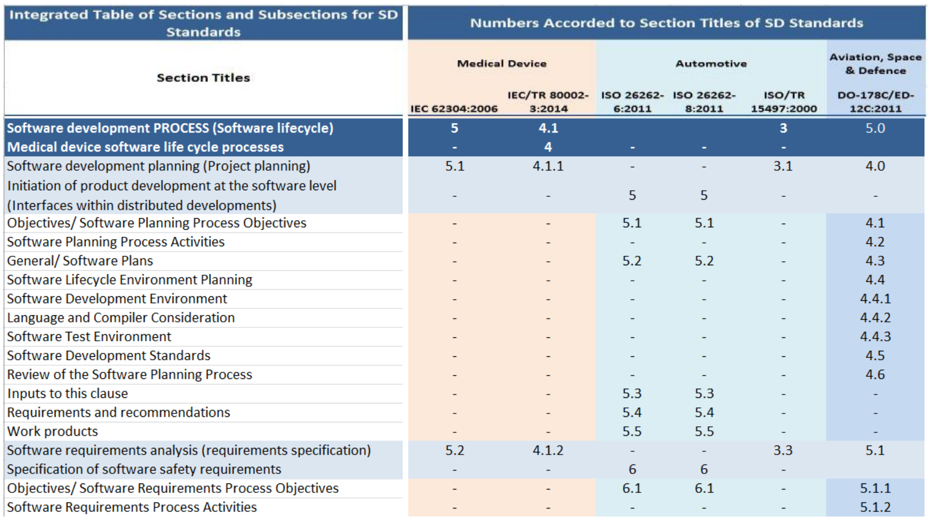
There are two vertical segments of the table. The left segment – *"Integrated Table of Sections and Subsections for QMS Standards"* has one column for Section Titles (titles). In the right segment – "*Numbers Accorded to Section Titles of QMS Standards"* there are six columns and each column represents one QMS standard. The column of titles has been populated with section titles from Medical device QMS standard first, followed by section titles from QMS standards of other domains. If, in some of the QMS standards, the new title of main section or sub/sub-sub section appeared, a new line was added to the table in order to include the new title. If the examined QMS standard contains inserted title then in the related line the number of title is inserted to the column representing this QMS standard, if not, the dash mark is inserted.

This mapping is an initial stage of developing common core for QMS standards and common core for SD standards. This approach corresponds to the fact that also ISO have seen that organizations have had challenges in implementing multiple standards. To this end they published Annex SL within *ISO/IEC Directives, Part 1* publication [44]. This Annex SL provides framework for the future Management systems that will make them more generic, more easily applicable and more consistent and therefore their integration should be easier. This common framework consists of high level structure, identical core text and common terms and core definitions. There is number of standards including ISO 9001:2015 that already employed Annex SL [45]. ISO also addressed the challenges of multiple risk standards. They introduced *ISO 31000 Risk management – principles and guidelines* [21] that provides common framework that can be applied to any type of risk and is not specific to any industry or sector [21]. This attempt of ISO to harmonize Management systems and to harmonize Risk management processes by introducing common framework can be seen as a model for development of common framework for safety critical software standards. The presented mapping of QMS and SD standards is s first step of developing common core for these standards.

For all considered domains it was noticed that for the QMS standards the structure of main sections and first subsections is exactly the same, except of ISO 9001:2015. The differences were found in the second and higher subsections. The unified structure of QMS standards for different safety critical domains provides a good foundation for their integration. The presence of a common set of requirements in these standards allows for the identification of core set of QMS requirements which can then be extended to allow the additional requirements of a specific safety critical domain to be implemented.

Using the same approach the cross industry cross reference mapping of sections and subsection for SD standards has been conducted and subsequently the cross reference table was created. The sample of the table is presented on Table 2. The structure of the table for SD standards is similar to the table for QMS standards. There are six columns representing different domains and SD standards related to these domains, and there is column for integrated section titles. The sample of the table shows that there are sections with significant differences. It has been realized that for SD there are more differences in section structure then for QMS. Therefore the development of common core appears more challenging comparing to QMS standards.

Table 2. The sample of mapping conducted of SD standards for different safety critical domains.



Integrated Table of Sections and Subsections for SD Standards	Numbers Accorded to Section Titles of SD Standards					
Section Titles	Medical Device		Automotive			Aviation, Space & Defence
	IEC 62304:2006	IEC/TR 80002-3:2014	ISO 26262-6:2011	ISO 26262-8:2011	ISO/TR 15497:2000	DO-178C/ED-12C:2011
Software development PROCESS (Software lifecycle)	5	4.1			3	5.0
Medical device software life cycle processes	-	4	-	-	-	
Software development planning (Project planning)	5.1	4.1.1	-	-	3.1	4.0
Initiation of product development at the software level (Interfaces within distributed developments)	-	-	5	5	-	-
Objectives/ Software Planning Process Objectives	-	-	5.1	5.1	-	4.1
Software Planning Process Activities	-	-	-	-	-	4.2
General/ Software Plans	-	-	5.2	5.2	-	4.3
Software Lifecycle Environment Planning	-	-	-	-	-	4.4
Software Development Environment	-	-	-	-	-	4.4.1
Language and Compiler Consideration	-	-	-	-	-	4.4.2
Software Test Environment	-	-	-	-	-	4.4.3
Software Development Standards	-	-	-	-	-	4.5
Review of the Software Planning Process	-	-	-	-	-	4.6
Inputs to this clause	-	-	5.3	5.3	-	-
Requirements and recommendations	-	-	5.4	5.4	-	-
Work products	-	-	5.5	5.5	-	-
Software requirements analysis (requirements specification)	5.2	4.1.2	-	-	3.3	5.1
Specification of software safety requirements	-	-	6	6	-	
Objectives/ Software Requirements Process Objectives	-	-	6.1	6.1	-	5.1.1
Software Requirements Process Activities	-	-	-	-	-	5.1.2

4 The Challenges of Compliance with Regulatory Requirements Related to Safety Critical Domains

The introduction of this paper identified challenges faced by organizations developing software in safety critical domains related to safety and security issues and to regulatory requirements. The research conducted on standards and their implementation shows the complexity of existing standards and how they relate to software development and to each other. The next phase of the research, presented in this section, examined the challenges faced by organizations developing software for a safety critical domain.

4.1 Medical Device Software Development & Compliance with Regulatory Requirements

Using Medical device software as an example of safety critical software domains that faces challenges related to compliance with regulatory requirements, an interview was conducted with an organization developing medical device software. The purpose of the interview was to examine their experience with standards implementation and main challenges that they face.

Previously, for the purpose of their activity they implemented QMS and they were *ISO 9001:2008 Quality management system* [46] compliant. The regulatory amendment issued in 2010 changed the classification of software meaning that software used for treatment and diagnosis as per the established definition of Medical device, could now be classified as a medical device in its own right [47]. This amendment changed their situation significantly. The amendment meant that they now needed to obtain the CE mark for their software as a proof of compliance with regulatory requirements. For this reason, the Quality assurance (QA) department was created and a QA specialist was employed within the organization. They had ISO 9001:2008 in place but, because of the classification of their software as a Medical device, they then implemented the ISO 13485:2012 standard as a first step in obtaining CE mark. In order to implement ISO 13485:2012, the company initially conducted a gap analysis between the requirements of ISO 9001:2008 and those additional requirements, which would need to be implemented in order to comply with ISO 13485:2012. In this way an integration of two systems, ISO 9001 and ISO 13485 was achieved and presently there are not two separate QMS in place and no duplicated requirements implemented.

The company is now beginning to implement the requirements of IEC 62304:2006. They identify the implementation of this standard as challenging. They see standard as being open to interpretation, and not specific in terms of which software development life-cycle should be used in order to comply with regulatory requirements. They find the requirements of this standard to be unclear and are not certain if their understanding is correct. In their opinion, with the many different software development lifecycles which are available for use there is continuous discussion within the company as to which of these lifecycles is appropriate for use for medical device software development. The company stated that even the opinions from specialist consultants on which of the lifecycles are suited for use were contradictory.

The company would like to follow the agile software lifecycle but because of the perceived lack of clarity regarding its suitability in terms of compliance with regulatory requirements, they follow the Waterfall lifecycle. From their point of view the regulations and directions are ambiguous and there are no guidelines provided on what is necessary. They find that the requirements of the standard are expressed at a high level and implementation can be challenging. They advised that a check-list which details an approach to the implementation of the requirements would be most helpful. They consider the implementation of the IEC 62304:2006 as a very robust approach, the implementation of which would be very challenging for small and medium enterprises (SME). Given constrains on SMEs the company feel that there is an issue with identifying the minimum requirements of standard that has to be implemented in order to comply with regulations.

Another issue for the company is concerned with safety classification. In their opinion, in the EU the regulations pertaining to the classification of devices is open for interpretation and not specific enough. The company noted that in the US on the FDA website there is a “Product Code Classification Database” where you can look at other products registered and compare, as a code classification guide. They stated that a similar site would be helpful which provides examples of the safety classification of devices under EU regulations. An incorrect safety classification of a device can have serious consequences for the company.

The interview confirmed that in the medical device domain there is presently no unified framework for safety critical software development that incorporates all of the best practices for safety critical software development. The selection of appropriate standards and necessary requirements, integration and implementation of these standard requirements causes significant challenges for SMEs.

4.2 Issues with Compliance with Regulatory Requirements Seen by Consultancy Company

Another interview was conducted with a Consultancy Company. This company provides assistance with the implementation and maintenance of QMS standards in SMEs. They have insight into the challenges concerned with QMS standard implementation that the SMEs face, and also they have experience with their approach to address these challenges. The purpose of the interview was to see their experience with QMS standard implementation and how they perceive the challenges with QMS implementation that the SMEs face. Building on their experience of implementing QMS in SMEs the consultancy company is now focussing on: how these systems can be expanded to include the required best practices in order to comply with the requirements for the development of software in safety critical domains. The other purpose of interview, based on their broad insight into the field of different international standards, was to investigate the challenges that the organization having QMS standard in place and developing software in safety critical domain have to face with implementing requirements of Software standards.

The Managing Director of the company said that from their experience the quality management systems are: *"well practised, they are well written and tangible"*. But in their opinion the software standards assume unlimited resources for implementation and maintenance of all standard procedures, but this is not the case of SMEs. From their experience there are number of small enterprises with limited human and financial resources, with experts in software development but without knowledge of regulatory requirements and about standard implementation. The other issue is concerned with the need for implementation of several standards which is the case of safety critical software development. They say that implementation of all standard requirements produces lots of overlying separate processes in place. The interview confirmed again that SME face the challenges related to the lack of resources which are necessary for standard implementation and maintenance. They have also insufficient knowledge about regulations and standards.

5 Future Works

To date the literature review and interviews with companies were conducted to identify the challenges that SMEs developing software in safety critical domains have to face. A cross industry mapping of section titles has been completed for QMS standards and for SD standards. A detailed mapping of standard requirements will be conducted as the next phase of the research process. Three different standard categories will be investigated. One mapping will be conducted for QMS standards, another mapping for Software development standards and another one for Risk management standards related to safety critical domains. For each of the standard categories, the outcome of the mapping will define the common requirements across the investigated domains and identify the requirements which are specific to each domain. Based on the defined common requirements for each standard category, a common core will be developed, one for QMS, one for SD and one for RM. These common cores will be a foundation for development of the Integrated use of standards. In the next stage the mapping of common cores will be conducted to investigate overlaying requirements and procedures. Based on this mapping the core of Integrated use of standards will be developed. This core of Integrated use will provide practices that include all investigated domains and all related standard categories. The further work will focus on standard requirements which are specific for different domains. The goal of this research is to develop the integrated use of management system standards as a unified framework for safety critical software development that incorporates all of best practices.

Conclusion

This paper has presented the results of a literature review which has examined how the integrated use of QMS and SD standards can address the challenges concerned with safety critical software development. To extend the results of the literature review and investigate the challenges in integrating and implementing the requirements of various standards, interviews were conducted with companies assisting in the implementation of QMS standards and with a company developing software in the medical device domain. These interviews combined with the results of the literature review revealed that organisations, particularly SME, struggle to integrate and implement the practices outlined in standards which are necessary for compliance with the regulations for software development in safety critical domains.

The research conducted to date has focused on an initial investigation of the challenges experienced by SMEs in the integration of QMS, RM and SD standards. The next phase of the research will focus on identifying requirements which are common within standard categories across safety critical domains and identifying which requirements are domain specific. This will form the basis for the development of a framework which can be used by SME already having a QMS in place to implement the requirements for software development in safety critical domains. The mapping of standards conducted to date will be expanded to examine the requirements of the standards. The mapping approach will cover all of investigated safety critical domains and related standard categories. The framework which will be developed as part of this research will assist organisations in addressing the challenges of complying with the regulatory requirements for software development across safety critical domains.

Acknowledgments

This research is supported by the Science Foundation Ireland 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 by Lero - the Irish Software Research Centre (http://www.lero.ie) grant 10/CE/I1855 & 13/RC/20194.

References

[1] J. Gapper, "Software is steering auto industry - FT.com," *Financ. Times*, 2016.

[2] J. Knight, "Safety Critical Systems: Challenges and Directions," *Int. Conf. Softw. Eng.*, 2002.

[3] M. M. Monti, A. Vanhaudenhuyse, M. R. Coleman, M. Boly, J. D. Pickard, L. Tshibanda, A. M. Owen, and S. Laureys, "Willful Modulation of Brain Activity in Disorders of Consciousness," 2010.

[4] M. McHugh, F. McCaffery, and S. T. MacMahon, "Improving Safety in Medical Devices from Concept to Retirement."

[5] Next Generation PDT, "Next Generation PDT - New Generation Cancer Treatment Therapy." [Online]. Available: http://www.nextgenerationpdt.com/?loc=gbl. [Accessed: 15-Feb-2016].

[6] National Cancer Institute, "Radiation Therapy for Cancer." [Online]. Available: http://www.cancer.gov/about-cancer/treatment/types/radiation-therapy/radiation-fact-sheet#q1. [Accessed: 15-Feb-2016].

[7] TrapX Labs, "ANATOMY OF AN ATTACK MEDJACK (Medical Device Hijack)," 2015.

[8] K. Fu, "ARCHIMEDES Ann Arbor Research Center for Medical Device Security." [Online]. Available: http://www.secure-medicine.org/. [Accessed: 15-Feb-2016].

[9] European Council, "MD Directives."

[10] U.S. FDA, "Inspection, Compliance, Enforcement, and Criminal Investigations."

[11] M. M. Hugh, F. M. Caffery, and V. Casey, "How amendments to the medical device directive affects the development of medical device software," 2011.

[12] M. Mc Hugh, F. Mc Caffery, and V. Casey, "US FDA releases final rule on Medical Device Data Systems- what does this mean for device manufacturers?," 2011.

[13] European Commission, *COUNCIL DIRECTIVE 93/42/EEC*, vol. L 269, no. September 2000. 2000.

[14] U.S. FDA, "Code of Federal Regulations Title 21."

[15] U.S. FDA, "FDA Agents - FDA Registration and U.S. Agent Representation."

[16] ISO, "ISO - International Organization for Standardization." [Online]. Available: http://www.iso.org/iso/home.htm. [Accessed: 15-Feb-2016].

[17] IEC, "Welcome to the IEC - International Electrotechnical Commission." [Online]. Available: http://www.iec.ch/index.htm. [Accessed: 15-Feb-2016].

[18] ISO, *ISO 9001 : 2015 Quality management systems Requirements ... making excellence a habit* . 2015.

[19] ISO/IEC, *ISO/IEC 15288:2015 Systems and software engineering — Life cycle processes*. 2015.

[20] ISO/IEC, *ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes*. 2008.

[21] ISO, *ISO 31000:2009 Risk management – principles and guidelines*. 2009.

[22] U.S. FDA, "Recognized Consensus Standards."

[23] European Comission, "Harmonised Standards - European Commission."

[24] NSAI, "Standards Supporting EU Directives." [Online]. Available: http://www.nsai.ie/Our-Services/Standardization/Standards-Supporting-EU-Directives.aspx. [Accessed: 17-Feb-2016].

[25] ISO, "ISO publishes book+CD on integrated use of management system standards (2008-07-15) - ISO," 2008. [Online]. Available: http://www.iso.org/iso/news.htm?refid=Ref1144. [Accessed: 15-Jan-2016].

[26] D. Flood, F. M. Caffery, V. Casey, and G. Regan, "A Methodology for Software Process Improvement Roadmaps for Regulated Domains - Example with IEC 62366."

[27] M. M. Hugh, F. M. Caffery, V. Casey, and M. Pikkarainen, "Integrating agile practices with a medical device software development lifecycle," *EuroSPI 2012*, pp. 1–8, 2012.

[28] S. T. MacMahon, F. M. Caffery, S. Eagles, F. Keenan, M. Lepmets, and A. Renault, "Development of a Process Assessment Model for assessing Medical IT Networks against IEC 80001-1."

[29] G. Regan, F. McCaffery, K. McDaid, and D. Flood, "Investigation of Traceability within a Medical Device Organization."

[30] F. McCaffery and V. Casey, "Med-Trace," pp. 208–211, 2011.

[31] ISO, *EN ISO 13485:2012 Medical devices — Quality management systems — Requirements for regulatory purposes*, no. July. 2012.

[32] IEC, *IEC 62304:2006 Medical device software—Software life cycle processes*. 2006.

[33] ISO, *EN ISO 14971:2012 Medical devices — Application of risk management to medical devices (ISO 14971:2007, Corrected version 2007-10-01)*. 2012.

[34] IEC, *IEC/TR 80002-1:2009 Medical device software Part 1 : Guidance on the application of ISO 14971 to medical device software*. 2009.

[35] ISO, *ISO/TS 16949 : 2009 Quality management systems — Particular requirements for the application of ISO 9001 : 2008 for automotive production and relevant service part organizations*. 2009.

[36] ISO, *ISO/TR 15497:2000 Road Vehicles — Development guidelines for vehicle based software*. 2000.

[37] ISO, *ISO 26262-6:2011 Road vehicles — Functional safety Part 6 : Product development at the software level*. 2011.

[38] ISO, *ISO 26262-8:2011 Road vehicles — Functional safety Part 8 : Supporting processes*. 2011.

[39] ISO, *ISO 26262-9:2011 Road vehicles — Functional safety Part 9 : Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*. 2011.

[40] EN, *EN 9100 : 2009 Quality Management Systems – Requirements for Aviation, Space and Defense Organizations*. 2009.

[41] EN, *EN 9115 : 2013 Quality Management Systems — Requirements for Aviation , Space and Defense Organizations — Deliverable Software*. 2013.

[42] RTCA, *RTCA DO-178C:2011 Software Consideration in Airborne Systems and Equipmqnt Certification*. 2011.

[43] EN, "BS EN 16601-80:2014 Space project management. Risk management," 2014. .

[44] ISO, *ISO/IEC Directives , Part 1 Consolidated ISO Supplement — Procedures specific to ISO*. 2014.

[45] The 9000 Store, "What is the New Annex SL Platform?" [Online]. Available: http://the9000store.com/iso-9001-2015-annex-sl.aspx. [Accessed: 25-Feb-2016].

[46] ISO, *EN ISO 9001 : 2008 Quality management systems Requirements*. 2008.

[47] European Commission, *DIRECTIVE 2007/47/EC*, no. November 2000. 2007.