MedeSPI: A Software Process Improvement Model for the Medical device industry based upon Automotive SPICE

Fergal Mc Caffery & Ita Richardson
Lero- the Irish Software Engineering Research Centre,
University of Limerick,
Ireland.
Fergal.mcCaffery@lero.ie, Ita.richardson@ul.ie

Abstract
Software is becoming an increasingly important aspect of medical devices and medical device regulation. Software enables highly complex systems to be built. However, complexity is the enemy of safety, therefore strict adherence to well documented processes is important within the domain of medical device software. Medical devices can only be marketed if compliance and approval from the appropriate regulatory bodies (e.g. the Food and Drug Administration (FDA)) is achieved. This paper outlines the development of a software process improvement (SPI) model specifically for the medical device industry. The paper details how medical device regulations may be satisfied by extending relevant practices from Automotive SPICE.

Keywords
Medical device industry, FDA, Regulatory requirements, Automotive SPICE

1 Introduction

Medical device companies must produce a design history file detailing the software components and processes undertaken in the development of their medical devices. Due to the safety-critical nature of medical device software it is important that highly efficient software development practices are in place within medical device companies. The risk of patient injury from software defects is a concern due to the manufacture and deployment of increasing numbers of software-embedded medical devices. There have been a number of major medical device product recalls over this past 25 years that were the result of software defects [1]. For example, four people died and two were left permanently disfigured from massive radiation overdoses due to software defects in the Therac-25 line of medical linear accelerators [2]. A major contributor to

the defects of such faults is the presence of software quality assurance issues [3]. The Center for Devices and Radiological Health (CDRH) reviewed medical device recalls due to software failures between 1983 to 1991 and estimated that 90% were due to inadequate design and 19% were caused by inadequate change contol [4]. It is therefore important that a medical device company has efficient software design and quality assurance procedures in place.

2 SPI within safety-critical domains

Previous research has investigated the suitability of using existing software quality assurance standards in order to achieve FDA [5,6,7,8] compliance related to the areas of process management, requirements specification, design control and change control [1]. However, no specific SPI model has been developed for the industry.

If we investigate other regulated industries such as the automotive and space industries we realise that these domains are not content with satisfying regulatory standards, but have proactively developed SPI models specifically for their domain so that they may continuously improve the development of their information systems to achieve higher levels of safety, greater efficiency, and a faster time to market, whilst seamlessly satisfying regulatory quality requirements. The major SPI models that currently exist, namely ISO/IEC15504 [9] and CMMI [10], do not address the regulatory requirements of either the medical device, automotive or space industries. Therefore, a new SPI model was developed specifically for the automotive industry, this model was based upon ISO/IEC15504 and is referred to as Automotive Spice [11]. Likewise, a new ISO/IEC15504 based SPI model was developed specifically for the space industry, this model is known as SPiCE for SPACE [12]. Both of these models contain reference and assessment information in relation to how companies may improve their practices within their domain.

This paper investigates how thorough current medical device regulations are in relation to specifying what software development practices medical device companies should adopt when developing software. This is achieved through comparing current medical device regulations and guidelines for software development against the formally documented software engineering “best practices” of Automotive SPICE for associated process areas.

Additionally, this paper highlights the need for a SPI model within the medical device industry (MedeSPI). It describes the development of MedeSPI based upon applicable processes from the Automotive SPICE model. The Automotive SPICE model is being used as a foundation upon which to develop this model as it has been designed to assist with the development of safety-critical software (for the automtive industry) which is therefore more applicable to the medical device domain than the generic version of ISO/IEC 15504. This paper will also illustrate high-level mappings that have been performed between medical device regulations and Automotive SPICE.

3 The Development of MedeSPI

The approach for delivering MedeSPI is illustrated in Figure 1. The model is flexible in that relevant elements may be adopted to provide the most significant benefit to the business. We describe how MedeSPI has been developed by extending Automotive SPICE processes with practices from medical device regulations.

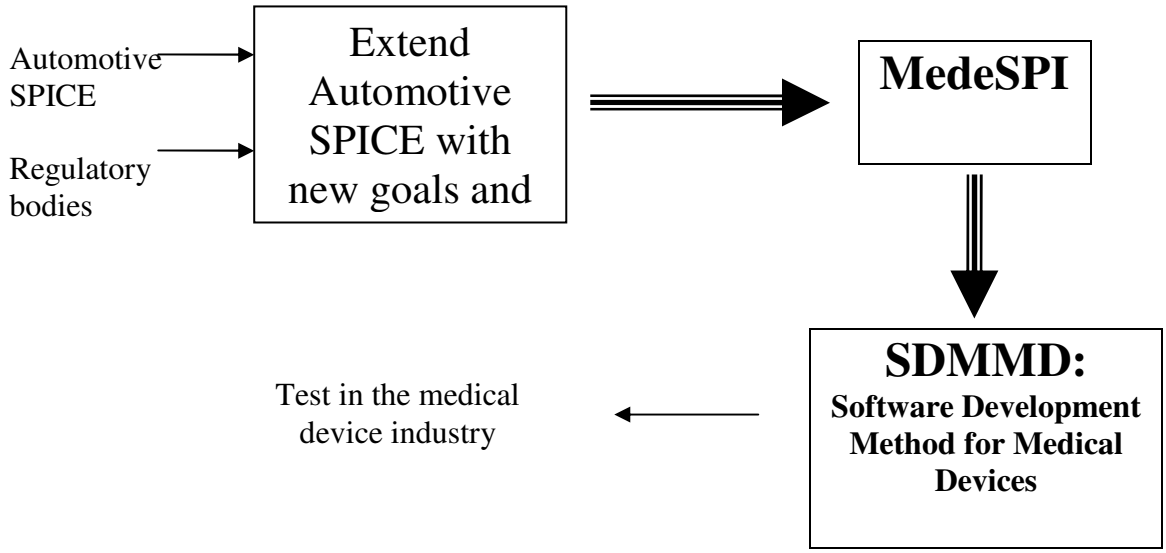


Figure 1: Software framework approach

The Software Development Method for Medical Devices (SDMMD) is a defined set of software process models which when utilised will meet the goals of MedeSPI. SDMMD will cover the complete software development lifecycle. SDMMD will provide a software development roadmap, which addresses the regulatory guidance criteria, while introducing best practices that can be selected as required. MedeSPI will provide a means of assessing software engineering capability in eleven areas that have been defined by the FDA as:

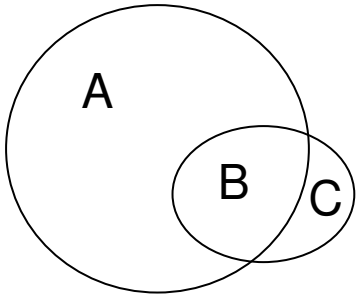
1. Level of Concern
2. Software Description
3. Device Hazard and Risk Analysis
4. Software Requirements Specification
5. Architecture Design
6. Design Specifications
7. Requirements Traceability Analysis
8. Development
9. Validation, Verification and Testing
10. Revision Level History
11. Unresolved Anomalies

MedeSPI is being developed to promote SPI practices into the software development processes of medical device companies. This is an attempt to improve the effectiveness and efficiency of software practices used by medical device companies through investigating the mapping between relevant Automotive SPICE processes and the eleven FDA areas.

Whilst all Automotive SPICE processes are applicable to the development of safety-critical medical device software, certain processes are essential in terms of satisfying the eleven areas defined by the FDA. Therefore companies must comply with these processes in order to market their medical devices. These processes are as follows:

- Risk Management (applicable to FDA area 1 & 3)
- Requirements Elicitation (applicable to FDA area 4)
- Software Requirements Analysis (applicable to FDA area 4)
- Software Design (applicable to FDA area 5 & 6)
- Software Construction (applicable to FDA area 8)
- Software Integration test (applicable to FDA area 9)
- Software Testing (applicable to FDA area 9)
- System Integration Test (applicable to FDA area 9)
- System Testing (applicable to FDA area 9)
- Verification (applicable to FDA area 9)
- Documentation (applicable to FDA area 2)
- Configuration Management (applicable to FDA area 10)
- Problem Resolution Management (applicable to FDA areas 10 & 11)
- Change Request Management (applicable to FDA area 4 & 7)

The mappings between the FDA regulatory guidelines and the relevant Automotive SPICE processes then produce MedeSPI processes that retain the Automotive SPICE process names. Like Automotive SPICE, each of the MedeSPI processes consist of a purpose, a number of outcomes and a number of base practices that will have to be performed in order to fulfil the outcomes. The performance of the base practices provides an indication of the extent of achievement of the process purpose and process outcomes. Work products are either used, produced or both, when performing the process [13]. The composition of the MedeSPI processes is illustrated in figure 2.



A- Automotive SPICE Practices that are not mandatory for FDA compliance.
B- Automotive SPICE Practices that are required for FDA compliance.
C- Non-Automotive SPICE Practices that are required for FDA compliance.

Figure 2. Composition of MedeSPI processes.

MedeSPI will highlight what additional practices have to be added to the associated Automotive SPICE processes in order to satisfy medical device regulations, as well as any Automotive SPICE outcomes and associated base practices that are not required in order to satisfy medical device regulatory requirements. Due to the scale of the entire MedeSPI model this paper will focus upon the process reference model for the risk management process as this is a very important process in relation to the development of safety-critical software for the medical device industry.

4 MedeSPI Risk Management process

The MedeSPI Risk Management (RM) process seeks to combine the various guidelines and standards within the medical device industry. It does so in the context of the following regulations: ISO 14971 [14], SW68 [15], TIR32 [16] and GAMP 4 [17] and CDRH (FDA specific) [5, 6, 7] guidance documents. The RM process outlined in this paper was developed following an extensive literature review of standards and CDRH guidance papers which govern the medical device software industry. The primary focus of this research area is to investigate if the medical device regulation for RM may be satisfied through adopting the Automotive SPICE RM process. This paper describes an integral part of this research by detailing the development of a MedeSPI RM process that is based upon the Automotive SPICE RM process. Upon development, the MedeSPI RM process will be an extension of the Automotive SPICE RM process that is specifically tailored to fulfil the RM regulations of the medical device software industry. The RM process may then be adopted by medical device companies to improve their software development practices by providing them with a SPI based process that will also ensure that their hazard analysis and risk control procedures satisfy the current medical device regulations and guidelines. The Failure Mode and Effects Analysis (FMEA) method of identifying, mitigating and tracking risk and hazard issues will be used within the RM process [18].

The next section details a mapping of the medical device standards and guidelines (these shall be referred to as medical device regulations throughout the paper) against the Automotive SPICE RM process.

4.1 RMCM DEVELOPMENT

In this section medical device regulations and guidelines, which have a counterpart within the goals and practices of the Automotive SPICE RM process area and are related to the creation of software are identified.

The purpose of the Automotive SPICE RM process is to identify, analyse, treat and monitor the risks continuously. The following outcomes are produced as a result of successful implementation of the RM process [13]:
1) the scope of the risk management to be performed is determined;
2) appropriate risk management strategies are defined and implemented;
3) risks are identified as they develop during the conduct of the project;
4) risks are analysed and the priority in which to apply resources to treatment of these risks is determined;
5) risk measures are defined, applied, and assessed to determine changes in the status of risk and the progress of the treatment activities; and
6) appropriate treatment is taken to correct or avoid the impact of risk based on its priority, probability, and consequence or other defined risk threshold.
NOTE 1: Risks may include technical, economic and timing risks.
NOTE 2: Risks are normally analysed to determine their probability, consequence and severity.
NOTE 3: Major risks may need to be communicated to and monitored by higher levels of management.
NOTE 4: Different techniques may be used to analyze a system in order to understand if risks exist, for example, functional analysis, simulation, FMEA, FTA etc

In the following section the MedeSPI RM process is developed through mapping regulatory medical device practices against the seven base practices (BP) specified in Automotive SPICE for RM. These are as follows:

- BP1: Establish risk management scope;
- BP2: Define risk management strategies;
- BP3: Identify risks;
- BP4: Analyse risks;
- BP5: Define risk treatment actions;
- BP6: Monitor risks;
- BP7: Take corrective action.

4.1.1 BP1: Establish risk management scope

The aim of this practice is to determine the scope of the RM to be performed. Both Automotive SPICE and the medical device regulations specify that the RM scope should be defined. Additionally, the medical standards specify that the strategy should include the life-cycle phases for which the strategy is applicable (see table 1).

Table 1: MedeSPI RM Sub-Base Practices for Establishing RM scope

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Determine the scope of risk management to be performed for the project, in accordance with organizational risk management policies.	**Yes**	**Yes**
Define the scope of the strategy and include those life-cycle phases for which the strategy is applicable	No	**Yes**

4.1.2 BP2: Define risk management strategies

The aim of this practice is to define an appropriate RM strategy. Defining a RM strategy involves establishing and maintaining a strategy to be used for RM. Both Automotive SPICE and the FDA require companies to have a RM strategy that is used to define risk analysis and control activities, which should be documented. However, medical device regulations are more stringent in terms of what constitutes a RM strategy and therefore additional activities (other than those detailed in Automotive SPICE) have to be included within this practice in order to fulfil the objectives of the MedeSPI RM process. For example, the FDA guidelines specify that a strategy should include: *potential sources of risk; appropriate techniques for risk analysis of software, electronics, biomaterials etc., such as fault tree analysis, failure modes and effects analysis; risk criteria, parameters and thresholds; risk control methods; & activities used to monitor the risks and whether risk controls were successful* [7]. Table 2, demonstrates that 9 additional medical device specific sub-practices have been added in order to provide full coverage of the medical device regulations.

Table 2: MedeSPI RM Sub-Base Practices for Defining RM strategies

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Define appropriate strategies to identify risks	**Yes**	**Yes**
Define appropriate strategies to mitigate risks	**Yes**	**Yes**
Set acceptability levels for each risk or set of risks, both at the project and organizational level	**Yes**	**Yes**
Include a verification plan as part of the strategy	No	**Yes**
Outline the allocation of responsibilities	No	**Yes**
Outline the requirements for reviewing the RM activities	No	**Yes**
The RM strategy should include Off-The-Shelf Software	No	**Yes**

Post-production queries and bugs be should analysed	No	**Yes**
At least one trained individual directly involved in the software development, with both relevant medical device and RM knowledge shall participate in the RM activity to ensure that risks are adequately addressed. This person(s) shall be identified on the report along with the date of the analysis	No	**Yes**
Determine software hazards	No	**Yes**
Include failure in the OTS software as a potential hazard	No	**Yes**
Include hardware failures as a potential hazard	No	**Yes**

4.1.3 BP3: Identify risks

The aim of this practice is to identify risks as they arise during the development and maintenance of a software development project. From mapping the medical device regulations against Automotive SPICE for this practice, it was discovered that all of Automotive SPICE sub-practices are required in order to achieve medical device regulatory compliance. However, the medical device regulations request additional information in relation to documentation, usage and traceability. Therefore, an additional 3 additional medical device specific sub-practices are required in order to achieve the objectives of the MedeSPI RM process (see table 3).

Table 3: MedeSPI RM Sub-Base Practices for Identifying Risks

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Identify risks to the project both initially within the project strategy and as they develop during the conduct of the project, continuously looking for risk factors at any occurrence of technical or managerial decisions.	**Yes**	**Yes**
Identify risks associated with cost, schedule, effort, resource and technical areas.	**Yes**	**Yes**
Review environmental elements that may impact the project - Risks may include technical, economic and timing risks	**Yes**	**Yes**
Document the context, conditions, and potential consequences of the risk	No	**Yes**
Include a description of the intended use and any foreseeable misuse	No	**Yes**
Provide risk traceability: Identify risk traceability from the device level down to the specific cause within the software	No	**Yes**

4.1.4 BP4: Analyse risks

The aim of this practice is to analyse risks to determine the priority in which to apply resources to the treatment of these risks. From mapping the medical device regulations against the Automotive SPICE base practice for analysing risks, it was

discovered that the medical device regulatory requirements for this practice will be fully satisfied through adopting the corresponding Automotive SPICE base practice (see table 4). Therefore the MedeSPI base practice for analysing risks will contain 3 sub-base practices that are applicable to both Automotive SPICE and the medical device regulations.

Table 4: MedeSPI RM Sub-Base Practices for Analysing Risks

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Evaluate the identified risks using the defined risk parameters	**Yes**	**Yes**
Analyse risks to determine their probability, consequence and severity.	**Yes**	**Yes**
Prioritise risks for mitigation based upon the probability and impact of each identified risk.	**Yes**	**Yes**

4.1.5 BP5: Define risk treatment actions

The aim of this practice is to define actions to correct or avoid the impact of risk. Additionally, this practice also seeks to define risk measures to determine changes in the status of risk and the progress of risk treatment activities. From mapping the medical device regulations against the Automotive SPICE base practice for defining risk treatment actions, it was discovered that the medical device regulatory requirements for this practice will not be satisfied through adopting the corresponding Automotive SPICE base practice (see table 5). In fact, the MedeSPI base practice for defining risk treatment actions requires 2 additional sub-practices to be added to the Automotive SPICE sub-practices in order to satisfy the medical device regulations. Sub-practices had to be added to ensure that resources were committed to risk-handling activities and that all risk mitigations should be verified. Therefore, the MedeSPI RM practice for defining risk treatment actions contains 4 sub-practices – all 4 are required in order to fulfil regulatory medical device requirements, but only 2 are required in order to satisfy Automotive SPICE in relation to this practice.

Table 5: MedeSPI RM Sub-Base Practices for Defining risk treatment actions

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Determine the levels and thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation or contingency plan	**Yes**	**Yes**
Develop mitigation & contingency plans for all risks	**Yes**	**Yes**
Provide continued commitment of resources for each plan to allow successful execution of the risk-handling activities	No	**Yes**
Mitigations should be verified	No	**Yes**

4.1.6 BP6: Monitor risks

The aim of this practice is to apply and monitor risk metrics to determine changes in the status of risks and the progress of risk treatment activities. From mapping the medical device regulations against the Automotive SPICE base practice for defining risk treatment actions, it was discovered that the medical device regulatory requirements for this practice would almost be satisfied through following the sub-practices of the corresponding Automotive SPICE base practice (see table 6). However, the MedeSPI RM base practice for monitoring risks requires an additional sub-practice to be added to the Automotive SPICE sub-practices in order to satisfy the medical device regulations. A sub-practice had to be added to ensure that the results of mitigation verification are verified. Therefore, the MedeSPI RM practices for monitoring risks contains 4 sub-practices – all 4 are required in order to fulfil regulatory medical device requirements, but only 3 are required in order to satisfy Automotive SPICE in relation to this practice.

Table 6: MedeSPI RM Sub-Base Practices for Monitoring risks

Sub-Practice	**Specified in Automotive SPICE**	**Specified in the Medical device regulations**
Results of the mitigation verification should be documented	No	**Yes**
Monitor risk status;	**Yes**	**Yes**
Provide a method for tracking open risk-handling options when monitored risks exceed the defined thresholds	**Yes**	**Yes**
Collect performance measures on the risk-handling activities.	**Yes**	**Yes**

4.1.7 BP7: Take corrective action

The aim of this practice is for appropriate treatment to be taken to correct or avoid the impact of risks based upon priority, probability, and consequence. Appropriate corrective action should be taken when expected progress has not been achieved. From mapping the medical device regulations against the Automotive SPICE base practice for taking corrective actions, it was discovered that the medical device regulatory requirements for this practice would not be satisfied through following the sub-practices of the corresponding Automotive SPICE base practice (see table 7). The MedeSPI RM base practice for taking corrective action requires an additional sub-practice to be added to the Automotive SPICE sub-practices in order to satisfy the medical device regulations. A sub-practice had to be added to ensure that the results of all the RM activities should be recorded and maintained in a RM file mitigation. The MedeSPI RM practice for taking corrective action contains 2 sub-practices – both are required in order to fulfil regulatory medical device requirements, but only one is required in order to satisfy Automotive SPICE in relation to this practice.

Table 7: MedeSPI RM Sub-Base Practices for Taking corrective action

Sub-Practice	Specified in Automotive SPICE	Specified in the Medical device regulations
Invoke selected risk-handling options when monitored risks exceed the defined thresholds	**Yes**	**Yes**
The results of all the RM activities should be recorded and maintained in a RM file	No	**Yes**

4.2 Summary of the MedeSPI RM

Table 8, illustrates that there are 33 sub-practices within MedeSPI RM. Each of these sub-practices are required within the medical device industry whereas only 16 are required within the Automotive SPICE RM process. Only one of the seven Automotive SPICE base practices fully satisfies the requirements of the associated MedeSPI RM practice. Therefore, the mappings highlight that MedeSPI needs to be more comprehensive in its coverage of the RM process than Automotive SPICE in order to satisfy the regulatory requirements of the medical device industry.

Table 8: Summary of MeDeSPI RM

Practice	Automotive SPICE Sub-Practices	Automotive SPICE Sub-Practices required to meet regulatory medical device requirements	Additional Sub-Practices required to meet regulatory medical device requirements
BP1: Establish risk management scope	1	1	1
BP2: Define risk management strategies	3	3	9
BP3: Identify risks	3	3	3
BP4: Analyse risks	3	3	0
BP5: Define risk treatment actions	2	2	2
BP6: Monitor risks	3	3	1
BP7: Take Corrective action	1	1	1
Total	**16**	**16**	**17**

5 Conclusions

With respect to the practices of the MedeSPI RM process, it is clear that following the base practices of the Automotive SPICE RM process will at best, only partially meet the regulatory requirements of the medical device industry in relation to RM. For RM, the existing Automotive SPICE specification of outcomes and base practices can be carried over, with the extension mentioned above into the MeDeSPI framework.

We are still developing MedeSPI. Our approach is to examine all of the appropriate processes that have listed in section 3, and investigate the extent to which the Automotive SPICE framework needs to be extended to create MeDeSPI. Our vision is

to provide a framework that will encourage medical device companies to distance themselves from the concept of developing the software first and then completing the necessary documentation that is required to achieve FDA compliance, to instead pursuing a continuous SPI path that will produce more efficient software development and safer medical devices. In this paper we have focused upon RM which is a key process within the medical device industry and therefore requires comprehensive coverage, however in other processes we may discover that the associated Automotive SPICE base practices will more than satisfy the regulatory medical device requirements and in these cases the medical device industry may be able to adopt some of the additional Automotive SPICE sub-practices to increase the efficiency of that process.

6 Acknowledgements

This research is supported by the Science Foundation Ireland funded project, Global Software Development in Small to Medium Sized Enterprises (GSD for SMEs) as part of Lero - the Irish Software Engineering Research Centre (http://www.lero.ie).

7 References

1. M.W. Bovee, D. L. Paul, K. M. Nelson, “A Framework for Assessing the Use of Third-Party Software Quality Assurance Standards to Meet FDA Medical Device Software Process Control Guidelines”, In: IEEE Transactions on Engineering Management, Vol. 48, No. 4, pp. 465-478.
2. N.G Leveson, C. S Turner, “An investigation of the Therac-25 accidents”, Computer, Vol. 26, No. 7, pp. 18-41, July 1993.
3. H. Bassen, J. Silberberg, F. Houston, W. Knight, C. Christman, M.D. Greberman, “Computerized medical devices: Usage trends, problems and safety technology”. In Proc. IEEE 7th Annual Conference Engineering in Medicine and Biology Society, 1985, pp. 180-185.
4. “Software related recalls for fiscal years 1983-91”, CDRH, FDA, US Department of Health and Human Services, 1992
5. FDA’s Mission Statement - http://www.fda.gov/opacom/morechoices/mission.html
6. CDRH, General Principles of Software Validation; Final Guidance for Industry and medical device Staff. January 11, 2002
7. CDRH, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices; Guidance for Industry and medical device Staff. May 11, 2005
8. CDRH, Off-The-Shelf Software Use in Medical Devices; Guidance for Industry, medical device Reviewers and Compliance. Sept 9, 1999
9. ISO/IEC 15504, Information Technology – Process Assessment – Part 5: An exemplar Process Assessment Model, ISO/IEC JTC1/SC7, International Standards Organisation, October 2003.

10. Capability Maturity Model® Integration (CMMISM) for Software Engineering (CMMI-SW, V1.1, Version 1.1, August 2002)
11. Automotive SIG, The SPICE User Group Automotive Special Interest Group, Automotive SPICE Process Reference Model, 2005, available from http://www.automotivespice.com
12. A. Cass, and C. Volcker, SpiCE for SPACE: A method of Process Assessment for Space Projects, SPICE 2000 Conference Proceedings, http://www.synspace.com
13. Automotive SIG, The SPICE User Group Automotive Special Interest Group, Automotive SPICE Process Assessment Model, 2005, available from http://www.automotivespice.com
14. ANSI/AAMI/ISO 14971, Medical devices – Application of risk management to medical devices. 2000
15. ANSI/AAMI SW68, Medical device software – Software life cycle processes. 5 June, 2001
16. AAMI TIR32:2004, Medical device software risk management, 2005
17. ISPE, GAMP Guide for Validation of Automated Systems. GAMP 4, Dec 2001
18. IEC 60812, Analysis technique for system reliability - Procedure for failure modes and effects analysis (FMEA), 1985.

8 Authors' biographies

Dr Fergal Mc Caffery

Dr. Fergal Mc Caffery is a senior research fellow with Lero - the Irish Software Engineering Research Centre. He has both an industrial and academic background. His current research interests include the development of a software development framework for the medical device industry, software process improvement frameworks and assessments, and global software development. He is a member of the programme committee for various International Software Engineering Journals and Conferences.

Dr.Ita Richardson

Dr. Ita Richardson is a senior lecturer in the Department of Computer Science and Information Systems at the University of Limerick where she lectures to undergraduate and postgraduate students. Her main research interests are in Software Process Improvement with a specific focus on small to medium sized enterprises and on Global Software Development. She is a project leader on the GSD for SMEs project, which is funded by Science Foundation Ireland and operates within Lero - the Irish Software Engineering Research Centre. Her research involves qualitative research with companies, and some of her post-

[SM] SCAMPI is a service mark of Carnegie Mellon University

graduate students are in full-time employment with software development companies. In early 2007, she was guest editor of IEEE Software special issue on 'Software Engineering Challenges in Small Companies'.