Development and Evaluation of a Risk Management Capability Model (RMCM) for the Medical Device Industry

[1]Fergal Mc Caffery, [2]John Burton, [2]Ita Richardson
[1]Dundalk Institute of Technology, Dundalk, Ireland
[2]Lero – the Irish Software Engineering Research Centre
Fergal.McCaffery@dkit.ie, John.Burton@ul.ie, Ita.Richardson@ul.ie

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 [1], therefore strict adherence to 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 of the Food and Drug Administration (FDA), and the European Commission under its Medical Device Directives is achieved. Medical device companies must produce a design history file detailing the software components and processes undertaken in the development of their products. Due to the safety-critical nature of medical device software it is important that a highly efficient risk management process is 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 devices [2]. In 2006, there were 325,742 reports of medical device associated injuries, deaths and malfunctions, which represents a 77% increase over 2005 [3]. The Center for Devices and Radiological Health take the matter of software related defects so seriously that they have recently made a significant investment in upgrading their “software forensics lab”, whose primary goal is to determine the root cause of the medical device software failures [4]. To reduce the risk of failure it is important that the software design process includes efficient risk management practices. Consequently, regulators penalise medical device manufacturers who cannot demonstrate sufficient attention has been devoted to the area of risk management throughout the software lifecycle.

The presentation will have four main parts. The first part will illustrate how thorough current medical device regulations are with relation to the Capability Maturity Model Integration (CMMI®) in specifying what risk management practices medical device companies should adopt when developing software. The second part will present a Risk Management Capability Model (RMCM) that has been developed by the authors specifically for the medical device software industry. The third part will explain how a five phase multi-cyclical action research approach was used within an organisation to evaluate the effectiveness of the RMCM in assisting medical device companies improve their software risk management procedures and practices. Finally, we will present the results of this evaluation.

[1] J. McDermid, “Issues in the development of safety-critical systems”, In: “F. Redmill and T. Anderson (eds) Safety-Critical Systems: Current Issues, Techniques and Standards (Chapman and Hall, London) pp. 16-43, 1993.

[2] 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.

[3] Shawn M. Schmitt, “Medical Device Reports To FDA Rose 77% In 2006”, "The Silver Sheet", August, 2007

[4] Chloe Taft, “CDRH Software Forensics Lab: Applying Rocket Science To Device Analysis”, “The Gray Sheet”, October 15, 2007

This research is supported by Science Foundation Ireland through the Stokes Lectureship Programme, grant number 07/SK/I1299 and the Global Software Development in Small to Medium Sized Enterprises project (GSD for SMEs) grant number 03/IN3/1408C within Lero - the Irish Software Engineering Research Centre.