Preface

Software systems are pervasive in all walks of life and have become an essential part of our daily life. Information technology is one major area which provides powerful and adaptable opportunities for innovation, and it seems boundless. However, systems developed using computer-based logic have produced disappointing results. According to stakeholders, they are unreliable, at times dangerous, and fail to provide the desired outcomes. Most significant reasons of system failures are the poor development practices for system designs. This is due to the complex nature of modern software and lack of adequate and proper understanding. Software development provides a framework for simplifying a complex system to get a better understanding and to develop the higher fidelity quality systems at lower cost. Highly embedded critical systems, in areas such as automation, medical surveillance, avionics, etc., are susceptible to errors, which can lead to grave consequences in case of failures.

Formal methods have emerged as an alternative approach to ensuring the quality and correctness of the high confidence critical systems, overcoming limitations of the traditional validation techniques such as simulation and testing. The purpose of this book is to provide the use of formal techniques for the development of computing systems with high integrity. Specifically, it addresses the issue that formal methods are not well integrated into established critical systems development processes by defining a new development life-cycle, and a set of associated techniques and tools to develop highly critical systems using formal techniques from requirements analysis to automatic source code generation using several intermediate layers with a rigorous safety assessment approach. The verification and validation tasks are carried out in intermediate layers for providing a correct formal model with desired system behaviour according to stakeholder needs. This methodology combines the refinement approach with various tools including verification tool, model checker tool, real-time animator and finally, produces the source code into multiple languages using automatic code generation tool. The approach has been realised using Event-B formalism. This book presents a set of tools that helps to verify desired properties, which are undiscovered during the system development. Moreover, this approach helps to identify the potential problems at an early stage of the system development. This book also critically evaluates the proposed life-cycle methodology, and associated techniques and tools through a case study in the medical domain, the cardiac pacemaker.

In addition, the book addresses the formal representation of medical protocols, which is useful for improving the existing medical protocols. We formalise a real-world medical protocol (ECG interpretation) to analyse whether the formalisation complies with certain medically relevant protocol properties. The formal verification process discovers several anomalies in the existing protocols, and provides a hierarchical structure for efficient ECG interpretation that helps to find a set of conditions that can help to diagnose particular diseases at an early stage. The main objective of the developed formalism is to test correctness and consistency of the medical protocol.

Outline

This book proposes an advanced development technique for modelling the critical medical systems using stepwise refinement and introduces the rigorous techniques to analyse the complex behaviour. It covers basic and advanced notions of critical systems, real-time animator to find hidden requirements with the help of domain experts, refinement chart to analyse the refinement structure, automatic code generation, heart-model to provide the biological environment for closed-loop modelling and application scenarios for medical systems verification. Moreover, this book presents advanced notion of critical system development from requirement analysis to implementation. The chapters of this book are organised in a coherent way that will help the reader to understand the development of complex medical systems. The book is structured in 11 chapters. Chapters 2 to 7 cover methodology, and techniques and tools for developing any complex critical system related to medical, automotive or avionic domains. The rest of the chapters have particular emphasis in the medical domain. Chapter 2 presents a basic background and development life-cycle related to the safety critical systems. Chapter 3 describes modelling techniques using the Event-B modelling language. In Chap. 4, we propose a development life-cycle methodology for developing the highly critical software systems using formal methods from requirements analysis to code implementation using rigorous safety assessments. In Chap. 5, we propose a novel architecture to validate the formal model with real-time data set in the early stage of development without generating the source code. This architecture can be used for requirement traceability. In Chap. 6, the refinement chart is proposed to handle the complexity and for designing the critical systems. In Chap. 7, we present a tool that automatically generates efficient target programming language code (C, C++, Java and C#) from Event-B formal specification related to the analysis of complex problems. In this chapter, the basic functionality as well as the design-flow is described, stressing the advantages when designing this automatic code generation tool; EB2ALL. In Chap. 8, we present a methodology to model a biological system, like the heart.

The heart model is mainly based on electrocardiography analysis, which models the heart system at the cellular level. The main objective of this methodology is to model the heart system and integrate it with the medical device model like the cardiac pacemaker to specify a closed-loop system. Chapter 9 shows a complete formal development of a cardiac pacemaker using proposed techniques and tools from requirements analysis to automatic code generation. The methodology and techniques are presented in previous chapters. All the essential properties are proven according to the domain experts. In Chap. 10, we present a new application of formal methods to evaluate real-life medical protocols for quality improvement. In this study, we consider a real-life reference protocol (ECG Interpretation) which covers a wide variety of protocol characteristics related to several heart diseases. Chapter 11 summarises this book. The formal development of industrial size case studies, illustrations, and formalisation throughout the text will help the reader to understand the complexity of medical systems and master the intricacies of the more subtle aspects in critical systems analysis.

Acknowledgement

This book is based on my Ph.D. thesis and would not have been possible without the support of a number of people. I would like to express my deep and sincere gratitude to my supervisor Prof. Dominique Méry for his inspiring discussions, enduring supervision and encouragement. His wide knowledge and his logical way of thinking have been of great value for me. His extensive discussions, critical suggestions and interesting explorations around my work have been very helpful for this study. He has also been a kind and effective advisor, allowing me a great amount of freedom while being actively involved in my research and nudging me in the right directions. I thank to the French Ministry of University and Research for grant funding for my Ph.D. study.

I would like to thank the external referees of my Ph.D. thesis, Prof. John Fitzgerald from the University of Newcastle and Prof. Yamine Ait-Ameur from the LISI/ENSMA. It is an honour for me that they were willing to invest their valuable time and effort in the careful reviewing of my thesis. In fact, I am thankful to all members of my Ph.D. committee, Prof. Catherine Dubois, Dr. Yann Guermeur, Dr. Isabelle Perseil, Prof. Olivier Roux and Prof. Dr. Etienne Aliot for fruitful discussions and for the highest support they offered for my work. I am also very thankful to Dr. Isabelle Perseil and Prof. Dominique Méry, who encourage me to publish a book based on my thesis work. I thank Mr. Ben Bishop and Mrs. Beverley Ford from Springer for helping to facilitate the publication of this book.

My sincere thanks also goes to Dr. S. Ramesh, and Dr. Manorajan Satpathi, for offering me the summer internship opportunities in their group (India Science Lab, General Motor, Bangalore, India) and leading me working on diverse exciting projects. I would like to thank Amel Amblard (Clinical Research Manager, Sorin Group-ELA Medicals) and research team of Sorin Group, Paris to demonstrate current challenging problems and to show the development process of a cardiac pacemaker. Furthermore, I thank Prof. Dr. Etienne Alliot, Head of the Cardiology Department of CHU Nancy, and all his colleagues MD doctors, who share their experiences for implanting a cardiac pacemaker and give me an opportunity to learn about the heart system through their fruitful discussions. Furthermore, I am grateful to cardiologist experts Prof. Yves Juillière (MD, Cardiology) and Dr. Frédérique Claudot and biomedical experts Dr. Didier Fass from the INRIA/LORIA, who shared their experiences to discuss and to verify the correctness of the heart model.

I would like to extend my gratitude to Prof. Tom Maibaum and Assoc. Prof. Alan Wassyng from the McMaster University for their advices in the area of certification and pacemaker challenges. Furthermore, I want to acknowledge to Prof. Dominique Cansell, Dr. Stephan Merz, Dr. Pascal Fontaine and Dr. Denis Roegel from the INRIA/LORIA for their advice and time. I also thank Prof. P.K. Kalra from IIT Rajasthan, Prof. Prabhat Munshi from IIT Kanpur and Asst. Prof. M.H. Khan from IET Lucknow for their inspiration.

I thank colleagues, friends, and family members for their support, encouragement, patience, and ideas throughout my studies, including: Late Mr. Kamleshwar Singh, Mr. Jitendra Singh, Mr. Rajkumar Singh, Mr. Shankar Singh, Late Mr. Ratneshwar Singh, Mr. Ravindra Singh, Mr. Surendra Singh, Mr. Sikander Singh, Mr. Updesh Singh, Mr. Manoj Singh, Dr. Pramod, Dinesh, Anurag, and Yogendra.

Especially, I thank my parents, Mrs. Lalita Devi and Mr. Ram Babu Singh, my brothers, Er. Sanjay Singh and Mr. Ranjay Singh, for their continuous support and encouragement, and I thank my wife, Arti, for her valuable support.

Further Sources

This book is based on several sources, particularly chronicles three years of working towards the author's Ph.D. thesis [10]. Chapter 4 covers some material from an article in the Innovations in Systems and Software Engineering [3] and also covers some material from previous work at SoICT [6]. Chapter 5 is an extended version of a previous paper at CSDM [1] and ISoLA [2]. Chapter 6 is a derived version of an article in the ACM Transactions on Embedded Computing Systems [9]. Chapter 7 is a substantially extended version of a previous paper at SoICT [4] that presents the basic framework and development of plug-ins for automatic code generation. In Chap. 8, we extend a previous paper at FHIES [7]. Chapter 9 is a significantly improved and detailed case study on the cardiac pacemaker in the International Journal of Discrete Event Control Systems [5]. Chapter 10 is also detailed version of an article at FHIES [8].

References

1. Méry, D., & Singh, N. K. (2010). Real-time animation for formal specification. In M. Aiguier, F. Bretaudeau, & D. Krob (Eds.), *Complex systems design & management* (pp. 49–60). Berlin: Springer.

2. Méry, D., & Singh, N. K. (2010). Trustable formal specification for software certification. In T. Margaria & B. Steffen (Eds.), *Lecture notes in computer science: Vol. 6416. Leveraging applications of formal methods, verification, and validation* (pp. 312–326). Berlin: Springer.
3. Méry, D., & Singh, N. (2011). A generic framework: From modeling to code. In *Innovations in systems and software engineering* (pp. 1–9).
4. Méry, D., & Singh, N. K. (2011). Automatic code generation from Event-B models. In *Proceedings of the second symposium on information and communication technology*, SoICT'11 (pp. 179–188). New York: ACM.
5. Méry, D., & Singh, N. K. (2011). Functional behavior of a cardiac pacing system. *International Journal of Discrete Event Control Systems*, *1*(2), 129–149.
6. Méry, D., & Singh, N. K. (2012). Critical systems development methodology using formal techniques. In *Proceedings of the third symposium on information and communication technology*, SoICT'12 (pp. 3–12). New York: ACM.
7. Méry, D., & Singh, N. K. (2012). Formalization of heart models based on the conduction of electrical impulses and cellular automata. In Z. Liu & A. Wassyng (Eds.), *Lecture notes in computer science: Vol. 7151. Foundations of health informatics engineering and systems* (pp. 140–159). Berlin: Springer.
8. Méry, D., & Singh, N. K. (2012). Medical protocol diagnosis using formal methods. In Z. Liu & A. Wassyng (Eds.), *Lecture notes in computer science: Vol. 7151. Foundations of health informatics engineering and systems* (pp. 1–20). Berlin: Springer.
9. Méry, D., & Singh, N. K. (2013). Formal specification of medical systems by proof-based refinement. *ACM Transactions on Embedded Computing Systems*, *12*(1), 15:1–15:25.
10. Singh, N. K. (2011). *Reliability and safety of critical device software systems*. PhD thesis, Department of Computing Science, Université Henri Poincaré-Nancy 1.

York, UK
April 2013

Neeraj Kumar Singh

http://www.springer.com/978-1-4471-5259-0

Using Event-B for Critical Device Software Systems
Singh, N.K.
2013, XVIII, 326 p., Hardcover
ISBN: 978-1-4471-5259-0