Kenneth J. Turner. Formally-Based Testing of Radiotherapy Accelerators. In Robert N. Procter and Mark Rouncefield, editors, Proc. Dependability in Healthcare, Edinburgh, pages 97-99, March 2001.

Formally-Based Testing of Radiotherapy Accelerators

Kenneth J. Turner
Department of Computing Science and Mathematics, University of Stirling
Stirling FK9 4LA, UK
Email kjt@cs.stir.ac.uk

20th March 2001

Abstract

The paper presents the aims and research plan of the CONFORMED project (Conformance Of Radiological/Medical Devices). This three-year project will develop tools and techniques for modelling and testing radiotherapy equipment. Formal specifications in LOTOS (Language Of Temporal Ordering Specification) will be used to model accelerators formally and to derive tests rigorously based on these specifications.

Keywords: Accelerator, Formal Method, LOTOS (Language Of Temporal Ordering Specification), Radiotherapy, Testing

1 Introduction

This paper briefly introduces the CONFORMED project (Conformance Of Radiological/Medical Devices). The three-year project is being undertaken from October 2000 at the University of Stirling, with funding from the NCC (National Computing Centre). The research is being undertaken in conjunction with the Oncology Physics Department, Western General Hospital, Edinburgh. Since the project started only recently, the paper concentrates on the goals of the work.

1.1 Project Aims

The project aims to combine scientific investigation of conformance testing with a practical application to the safety of radiotherapy equipment. A number of radiation accidents due to software failures have been well documented (e.g. [14, 15]). Existing results from testing theory and conformance testing will be significantly extended during the project for the evaluation of radiotherapy equipment. Formal specifications in LOTOS (Language Of Temporal Ordering Specification [8]) will be used to ensure that functional and performance aspects of this equipment are accurately captured. These specifications will be used to derive and apply tests in a rigorous manner. This will ensure that testing is systematic, thorough and objective. Testing is necessary when medical equipment is commissioned (to check the integrity of design and implementation), and also during its operational lifetime (to check for deterioration or changes due to system upgrades).

The general aim is to develop and demonstrate methods and tools for formulating specifications of radiotherapy equipment, and for conducting tests based on these specifications. The types of radiotherapy equipment typically used in UK hospitals will be studied. Computer-controlled radiotherapy equipment is widespread. Clearly its correct design and operation are safety-critical. Modern accelerators are entirely dependent on software to control beam settings and movement. Increasingly complex demands are being placed on the software (e.g. high dosage with pinpoint accuracy, real-time control of treatment in three dimensions). Software problems for accelerators include real-time demands, quality assurance, configuration control and handling periodic upgrades. Typical guidelines for accelerators [16] recommend rigorous specification and testing, but note that such procedures need to be developed.

Medical equipment is a significant industry within the UK, though sadly the major radiotherapy machines manufacturers (International General Electric/CGR, Philips Medical, Siemens, Varian Medical Systems) undertake R&D elsewhere. This creates a major problem because radiotherapy equipment is developed *outside* the

UK but has to be tested *in* the UK. As an indication of the scale of the problem, around 300 radiotherapy accelerators are currently used in this country. There is an opportunity for the UK to develop specialist expertise in radiotherapy equipment testing, and to establish norms for this.

Technical spin-offs from the project will be methods, tools and specifications for testing equipment such as that used in radiation treatment. More widely, these methods and tools will be applicable to safety-critical and quality-critical computer-controlled systems. The results of the project will have impact on the communities dealing with radiotherapy and oncology, formal methods, and safety-critical systems.

1.2 Related Work

A review of standards for software-controlled medical devices is given in [12]. The main international standards of relevance to the project are those in the IEC 601 series. This is a very large collection of standards, specifically including programmable electrical medical systems [5, 6]. A number of subsidiary standards concern accelerators [7]. The US FDA (Food and Drug Administration) has published guidelines on Good Manufacturing Practice [2] that are relevant to software-controlled medical devices. Radiotherapy machines are typically certified by the FDA before they are sold anywhere in the world. The American Association of Physicists in Medicine has laid down a code of practice specifically for radiotherapy accelerators [16]. The Canadian Atomic Energy Authority also plays an active role in regulating radiotherapy devices. In Europe, the EC is defining standards for safety of medical equipment (e.g. the Medical Devices Directive [1]). More general software development standards are also relevant to the project, such as the ISO/IEC 9000 series on quality assurance and its European EN equivalents.

Many projects in the UK and elsewhere have worked on the development of formal methods. A number of formal languages, including LOTOS, have been internationally standardised as FDTs (Formal Description Techniques [20]). As far as the author knows, radiotherapy equipment has attracted surprisingly little attention from the formal methods community. [18] is one of few contributions, having made use of LOTOS to investigate equipment characteristics. The only other work known to the author has used Z [17] in the development (not testing) of software for a radiation therapy machine [11]. The application of conformance testing methods to performance is largely uninvestigated.

LOTOS is a flexible specification language that has been used in a variety of industrial sectors including safety-critical ones (e.g. avionics, railway signalling, vehicle control and medical devices). An enhanced version, E-LOTOS (Enhancements to LOTOS), is currently being standardised [10]. For the project, the most relevant enhancements being developed in E-LOTOS concern the specification of time and hence performance. The project will therefore exploit E-LOTOS in its work. However because E-LOTOS is relatively recent, it will be necessary to develop a new theory of conformance testing for it. Tools for LOTOS are readily obtainable, but for E-LOTOS are only now being produced [3]. The project therefore expects to undertake its own tool development for conformance testing.

2 Project Workplan

2.1 Goals

The aim of the project is to support a safer environment for treatment of patients through radiation therapy. The main goals are:

- to define a method for specifying the functional and performance characteristics of radiotherapy accelerators
- to develop a method for deriving and applying rigorous tests based on formal accelerator specifications
- to develop prototype tool support for the methods
- to demonstrate the methods and tools through realistic case studies.

The secondary goals of the project are:

- to generalise from the project results to safety-critical systems generally
- to establish links with relevant health authorities and national committees
- to establish links with radiotherapy equipment suppliers in the UK.

2.2 Research Activities

The following tasks will be performed, in iterative steps where possible. This will allow early experience of the approach as it develops, feeding back into later enhancements of the techniques and tools. The project is currently at the stage of a literature and tools survey. The main topics of interest are formalising (non-)functional requirements using LOTOS, conformance testing based on LOTOS, radiotherapy accelerators and treatment practices.

Radiotherapy machines are quite different in functionality and characteristics from most computer-controlled systems. It will be necessary to identify clearly the functions that radiotherapy machines perform and the performance requirements that they must meet. Although there has been some standardisation of what radiotherapy machines must do, this has mainly dealt with outputs rather than inputs. The specifications written by manufacturers are necessarily proprietary and are not generic. It will therefore be necessary to 'reverse engineer' the requirements for radiotherapy machines in general. A proper relation between inputs and outputs will need to be established, and performance characteristics will have to be defined. The work will concentrate on functionality and performance rather than ergonomic aspects. It will be necessary to consider the behaviour of radiotherapy machines if they are misoperated, the extent to which partial failures in a machine may compromise its correct operation, and where fail-safe recovery is required. A major improvement needed in the current understanding of radiotherapy machines is clarifying the sources and severity of potential problems. It is also important to ensure that the machine manipulates reality and not just some internalisation of it. The aim is to define a high-level statement of requirements that can be specialised for any particular radiotherapy machine.

The requirements definition for radiotherapy machines will be formalised using LOTOS – a language that has proved very suitable for compactly and precisely describing system architecture and behaviour. The LOTOS community has already gained experience of specifying medical devices (e.g. [18, 19]). It will be important, however, to describe performance aspects of radiotherapy machines. For this reason, the project will use E-LOTOS that is currently being standardised by ISO. E-LOTOS offers new features for specifying performance and timing aspects. Other extensions such as improved data types and modularity will also be useful to the project. The result of this work will be formal specifications in E-LOTOS of the functionality and performance expected of a radiotherapy machine.

The notion of conformance testing is well developed in data communications [9]. Formal methods for conformance testing have also been investigated, including techniques based on LOTOS (e.g. [4, 13]). The scientific challenges facing the project are to adapt such approaches to the field of radiotherapy, to devise testing techniques for E-LOTOS, and to develop a means of testing performance based on E-LOTOS. Conventional methods for testing radiotherapy machines will need to be reconciled with a formally-based approach. Current radiotherapy practice is very thorough in validating machine outputs, but less so in validating inputs and the input-output relationship. Various techniques are known for deriving tests from a LOTOS specification. These will need to be extended to deal with E-LOTOS, since formal derivation of tests for performance as well as functionality has not yet been investigated for E-LOTOS. The outcome of this task will be test suites derived from the formal specifications of radiotherapy machines. Because of the complexity of this task, tools will be developed for automated test derivation based on the theory. Tools will also be developed for automatically applying and evaluating these tests on actual equipment.

Two case studies will be performed using different accelerators. It is hoped to involve equipment manufacturers in the case studies, since the manufacturers have an intense interest in the safety of their products. The case studies will involve producing specialised LOTOS specifications that reflect the characteristics of each machine. From these, machine-specific test suites will be derived. The test suites will be used in various ways: in a simulated commissioning test, to validate correct operation after a system upgrade (of software or hardware), and for routine maintenance checks. The case studies will allow the applicability and usability of the method and tools to be assessed.

3 Conclusion

Although the CONFORMED project has just started, it has real potential to introduce formal methods in testing radiotherapy accelerators. As the project unfolds, it is hoped that it will effectively complement the careful testing already undertaken by manufacturers.

Acknowledgements

The research is being undertaken by Qian Bing (email qb@cs.stir.ac.uk) at the University of Stirling, under the author's supervision. Stirling gratefully acknowledges the support of the National Computing Centre and its project coordinator, Daniel Dresner. Thanks are also due to Dr. Hamish Porter of the Western General Hospital, Edinburgh, for his collaboration and helpful discussions.

References

[1] EC. Medical devices directive. Technical Report 93/42/EEC, European Commission, Brussels, Belgium, June 1993.

[2] FDA. Medical devices: Current good manufacturing practice. Technical Report 61 FD 195, US Food and Drug Administration, New York, USA, Oct. 1996.

[3] H. Garavel and M. Sighireanu. Towards a second generation of Formal Description Techniques – Rationale for the design of E-LOTOS. In J.-F. Groote, B. Luttik, and J. van Wamel, editors, *Proc. 3rd. International Workshop on Formal Methods for Industrial Critical Systems*, pages 187–230, Amsterdam, Netherlands, May 1998. University of Nantes.

[4] T. Higashino and G. von Bochmann. Automatic analysis and test case derivation for a restricted class of LOTOS expressions with data parameters. *IEEE Trans. on Software Engineering*, 20(1), Jan. 1994.

[5] IEC. *Medical Electrical Equipment – Part 1: General Requirements for Safety*. IEC 601-1. International Electrotechnical Commission, Geneva, Switzerland, 1988.

[6] IEC. *Medical Electrical Equipment – Part 1: General Requirements for Safety – 4. Collateral Standard: Programmable Electrical Medical Systems*. IEC 601-1-4. International Electrotechnical Commission, Geneva, Switzerland, 1988.

[7] IEC. *Medical Electrical Equipment – Part 2: Particular Requirements for Safety*. IEC 601-2. International Electrotechnical Commission, Geneva, Switzerland, 1988.

[8] ISO/IEC. *Information Processing Systems – Open Systems Interconnection – LOTOS – A Formal Description Technique based on the Temporal Ordering of Observational Behaviour*. ISO/IEC 8807. International Organization for Standardization, Geneva, Switzerland, 1989.

[9] ISO/IEC. *Information Processing Systems – Open Systems Interconnection – Conformance Testing Methodology and Framework*. ISO/IEC 9646. International Organization for Standardization, Geneva, Switzerland, 1991.

[10] ISO/IEC. *Information Processing Systems – Open Systems Interconnection – Enhanced LOTOS – A Formal Description Technique based on the Temporal Ordering of Observational Behaviour*. ISO/IEC 15437. International Organization for Standardization, Geneva, Switzerland, Apr. 2000.

[11] J. Jacky, J. Unger, M. Patrick, D. Reid, and R. Risler. Experience with Z developing a control program for a radiation therapy machine. In J. P. Bowen, editor, *Proc. 10th. International Conference of Z Users*, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany, Dec. 1996.

[12] J. Jacobson and O. Andersen. Software controlled medical devices. Technical Report SP-Rapport 1997:11, European Network of Clubs for Reliability and Safety of Software, Apr. 1997. ISBN 91-7848-669-6.

[13] Ji He and K. J. Turner. Protocol-inspired hardware testing. In G. Csopaki, S. Dibuz, and K. Tarnay, editors, *Proc. Testing Communicating Systems XII*, pages 131–147, London, UK, Sept. 1999. Kluwer Academic Publishers.

[14] E. J. Joyce. Accelerator linked to fifth radiation overdose. *American Medical News*, 1, Feb. 1987.

[15] C. J. Karzmark. Procedural and operator error aspects of radiation accidents in radiotherapy. *International Journal of Radiation Oncology Biological Physics*, 13:1599–1602, Jan. 1987.

[16] R. Nath, P. J. Biggs, F. J. Bova, C. C. Ling, J. A. Purdy, J. van de Geijn, and M. S. Weinhous. AAPM code of practice for radiotherapy accelerators. *Medical Physics*, 21(7):1093–1121, July 1994.

[17] J. M. Spivey. *The Z Notation: A Reference Manual*. Prentice-Hall, Englewood Cliffs, New Jersey, USA, Second edition, 1992.

[18] M. H. Thomas. The story of the Therac-25 in LOTOS. *High Integrity Systems Journal*, 1(1):3–15, Feb. 1994.

[19] P. Trafford. *The Use of Formal Methods for Safety-Critical Systems*. PhD thesis, School of Computer Science and Electronic Systems, Kingston University, Kingston-upon-Thames, UK, Oct. 1997.

[20] K. J. Turner, editor. *Using Formal Description Techniques — An Introduction to ESTELLE, LOTOS and SDL*. Wiley, New York, Jan. 1993.