SOFL THREE-STEP APPROACH TO CONSTRUCT THE FORMAL SPECIFICATION OF A BRAIN TUMOR TREATMENT SYSTEM

A Rahman Mat* & Cheah Wai Shiang
Fac. of Computer Science & IT, Universiti Malaysia Sarawak, Kota Samarahan, Sarawak, MALAYSIA
{marahman, wscheah}@fit.unimas.my

Shaoying Liu
Dept. of Computer & Information Sciences, Hosei University, Tokyo, JAPAN
sliu@hosei.ac.jp

ABSTRACT

The SOFL three-step approach to the construction of formal specifications has been proposed and applied in information systems, but its effectiveness and applicability have not yet been demonstrated in developing safety critical systems. In this paper, we describe an application of the SOFL approach to the construction of a formal specification for the brain tumor treatment system. This case study demonstrates the suitability of SOFL for safety-critical system developments and provides us with an insight into the knowledge of how the SOFL three-step specification approach can be effectively supported.

KEYWORDS

Formal Engineering Method, Formal Specification, SOFL, Brain Tumor Treatment System

1 INTRODUCTION

The Structured Object-Oriented Formal Language (SOFL) three-step approach to the construction of formal specifications for software systems has been developed and applied in information systems over the last nineteen years [1][2]. Compared to well-known formal methods, such as VDM [3], B method [4] and Larch [5], SOFL has many distinct advantages, mainly because it offers effective ways to integrate formal methods into the entire process of software engineering, which allows practitioners to easily apply formal methods in real software projects. In particular, the SOFL three-step specification approach is one of the many important features of the SOFL method. It emphasizes the fact that constructing a formal specification for design of a system significantly contributes to the quality assurance of the system and the importance of a progressive process for achieving it. According to the progressive process, the formal design specification can be achieved in three steps [1]. The first is to build an informal specification, documenting the major functions, necessary data resources, and constraints (e.g., safety, security, policy). The second is to transform the informal specification to a semi-formal specification which is more precise than the informal one and organized in a modular fashion. The third step is to build a completely formal specification for design on the basis of the semi-formal specification by first defining the architecture of the system and then defining all the components involved in the architecture using a mathematically-based notation.

While there is sufficient evidence, resulting from many applications, to suggest that the SOFL three-step specification approach be effective in ensuring software quality and reducing development cost for information systems, it has not been sufficiently demonstrated that SOFL is also suitable for the development of safety-critical systems. In this paper, we present a case study applying SOFL three-step approach to formally specify the brain tumor treatment system [6]. Particularly, we concentrate on the description of how to write the informal specification, how to transform it into the semi-formal specification, and finally how to form the formal design specification based on the semi-formal one. The case study demonstrates the suitability of SOFL for safety-critical system development and provides us with an insight into the knowledge of how the SOFL three-step specification approach can be effectively supported.

The remainder of the paper is organized as follows. Section 2 describes the background of a brain tumor treatment system. Section 3 gives a brief introduction to the SOFL three-step specification approach which we used in the case study. A brief overview of related work is given in Section 4. Section 5 discusses how the SOFL approach is applied in writing the specifications for the brain tumor treatment system. Section 6 describes our experience and

* The author is currently doing his doctorate study at the Department of Computer & Information Science, Hosei University, Koganei Campus, Tokyo, Japan and can be contacted via email: arman.mat@gmail.com