Reduciendo la Ambigüedad en el Modelo del Dominio mediante Especificaciones Formales Ligeras en VDM++

Elizabeth Vidal-Duarte[1], César Mogrovejo Ramirez[1], Eveling Castro Gutierrez[2]
[1] Universidad Católica San Pablo
[2] Universidad Nacional de San Agustín

Resumen

Una de las herramientas más utilizadas para modelar los requerimientos funcionales es el Modelo del Dominio. Muchas veces, dependiendo de la complejidad de los requerimientos a ser modelados, no es posible que dicho modelo capture todos los detalles y restricciones relacionados. Esto puede causar que el Modelo del Dominio sea sujeto de interpretaciones subjetivas que conlleven a errores de implementación más adelante. Este artículo presenta una forma de reducir la ambigüedad en el Modelo del Dominio mediante el uso de especificaciones formales ligeras en VDM++. A modo de ejemplo, presentamos la especificación formal de un electrocardiógrafo digital. La especificación está basada en la descripción de las características del funcionamiento del electrocardiógrafo. Se pone especial atención en las características de la captura de la señal electrocardiográfica. Se ha identificado propiedades y restricciones importantes que permiten incrementar la confiabilidad al momento de la implementación. Las propiedades y restricciones se han especificado en forma de invariantes y precondiciones. La validación de la propuesta se realizó con la herramienta VDM++ToolBox.

Palabras clave:

VDM++ToolBox, desarrollo de software, electrocardiógrafo

Abstract

One of the most used tools for modeling the functional requirements is the Domain Model. Many times, depending on the complexity of the requirements to be modeled is not possible that this model captures all the details and restrictions related. This can cause the Domain Model is subject to subjective interpretations that lead to implementation errors later. This article presents a way to reduce ambiguity in the domain model by using lightweight formal specification in VDM++. As an example, we present the formal specification of a digital electrocardiograph. The specification is based on the description of the operation of the electrocardiograph. It pays special attention to the characteristics of the capture of the electrocardiogram. Properties have been identified and significant restrictions that increase reliability at the time of implementation. The properties and restrictions are specified as invariants and preconditions. The validation of the proposal was made VDM++ tool ToolBox.

Keywords:

VDM ++ Toolbox, software development, electrocardiograph

Introducción

Es ampliamente conocido que la parte más crítica del desarrollo de software corresponde a la identificación y especificación de requerimientos [Sommerville, 2001]. Para facilitar el proceso de desarrollo de software, muchos desarrolladores trabajan con una variedad de métodos y herramientas reconocidos, por ejemplo el Lenguaje de Modelado Unificado (UML) [Rumbaugh etal, 1998]. Aunque UML es el lenguaje estándar para modelamiento aún no está suficientemente refinado como para proveer toda la información relevante en una especificación [Aicherning, 2001]. Los diagramas UML están sujetos muchas veces a interpretaciones subjetivas. Esto podría llevar a implementaciones que corren el riesgo de no cumplir con los requerimientos reales.

Existe la necesidad de describir restricciones adicionales acerca de los objetos en el modelo, sobre todo si el sistema a describir es de carácter crítico, como es el caso de un Electrocardiógrafo. Dichas restricciones son descritas por lo general en lenguaje natural. La experiencia ha mostrado que esto siempre resulta en ambigüedades. Para evitar dichas ambigüedades, se hace necesario el uso de los llamados lenguajes formales [Fitzgerald and Gorm Larsen, 1998].

Si queremos que los métodos formales sean utilizados en el desarrollo de proyectos de software, necesitamos habilitar a los desarrolladores en el uso de especificaciones formales. En este artículo, se muestra una forma de especificación formal ligera [Jones, 1996]. Para este propósito, haremos uso de VDM++ (Vienna Development Method++) [CSK SYSTEMS a, 2009]. VDM++ permite expresar restricciones adicionales en los modelos orientados a objetos. Permite la especificación de restricciones formales en el contexto de diagramas de clase de UML [Booch etal, 1998].

El resultado de este trabajo no nos proporciona una especificación completa del electrocardiógrafo, sino brinda una descripción razonable de la especificación de una de las funcionalidades consideradas como críticas: la correcta captura de la señal electrocardiográfica.

El principal aporte del presente trabajo es mostrar que la aplicación de especificaciones formales ligeras contribuye a incrementar la confiabilidad en la correctitud para la implementación.

El resto del artículo está organizado de la siguiente manera: en la sección 2, se presenta las principales características del electrocardiógrafo. En la sección 3, se presenta la definición de métodos formales y especificaciones formales ligeras. En la sección 4, se explica las principales características de VDM++, así como la sintaxis que será utilizada en nuestro caso de estudio. En la sección 5, se describe la metodología seguida. En la sección 6, se presenta, como caso de estudio, la especificación formal del electrocardiógrafo. Se describen los requerimientos funcionales de manera informal para luego modelar la clase UML junto con la especificación formal VDM++. Además, se presenta el análisis y validación del modelo propuesto utilizando la herramienta VDMToolBox. En la sección 7, se exponden nuestras conclusiones y el trabajo futuro.

Conclusiones

En este artículo, se ha presentado una forma de incrementar la confiabilidad en la correctitud para la captura de la señal electrocardiográfica. Para ello, se han aplicado especificaciones formales ligeras. Nos hemos centrado en la especificación de restricciones que no son evidentes en el diagrama de clases UML. Se ha aplicado invariantes y precondiciones utilizando VDM++.

Las especificaciones fueron ejecutadas en VDM++ToolBox para validar la propuesta. Los casos de prueba fueron elegidos de acuerdo con la técnica de Clases de Equivalencia. Los resultados obtenidos nos permitieron incrementar la confiabilidad en la correctitud para la implementación de la captura de señales del electrocardiógrafo.

Si bien, VDM++ presenta muchas más características que las descritas en este artículo, hemos tomado solo una pequeña parte para mostrar cómo especificar restricciones de manera formal para complementar los diagrama de clases. Nuestro objetivo es incrementar el uso de especificaciones formales en el proceso de desarrollo. Creemos

que el uso de especificaciones formales en las primeras etapas del desarrollo nos permite incrementar la correctitud del software que estamos desarrollando.

Como trabajo futuro, pretendemos ampliar la especificación del electrocardiógrafo centrándonos un poco más en la especificación de la señal.

Referencias

[1] [Aicherning, 2001] B. K. Aichernig (2001).Systematic Black-Box Testing of Computer-Based Systems through Formal Abstraction Techniques. Doctoral Thesis. Technischen Universitat Graz.

[2] [Bjørner and Jones, 1982] D. Bjørner and C.B. Jones. Formal Specification and Software Development. Prentice-Hall International.

[3] [Booch etal, 1998] G. Booch, J. Rumbaugh, and I. Jacobson (1998). The Unified Modeling Language User Guide, Addison-Wesley.

[4] [CSK SYSTEMS a, 2009] CSK SYSTEMS a (2009). The VDM++ Language. Technical Report.

[5] [CSK SYSTEMS b, 2009] CSK SYSTEMS b (2009). VDM Tools User Manual. Technica Report.

[6] [CSK SYSTEMS c, 2009] CSK SYSTEMS b (2009). The VDM++ Method Guideline. Technica Report.

[7] [Dubin, 1986] D. Dubin (1986). Electrocardiografía Práctica: Lesión Trazado e Interpretacion, 3ra Ed; Mc-Graw hill Interamericana

[8] [Easterbrook et al, 1998] S. M. Easterbrook, R. Lutz, R. Covington, J. Kelly, Y. Ampo, and D. Hamilton. (1998) Experiences using lightweight formal methods for re-quirements modeling. IEEE Transactions on Software Engineering, 24(1), January 1998.

[9] [Fitzgerald and Gorm Larsen,1998] J. Fitzgerald and P.Gorm Larsen (1998). Modelling Systems Practical Tools and Techniques in Software Development. Cambridge University Press, The Edinburgh Building, Cambridge CB2 2RU, UK.

[10] [Fitzgerald etal, 2005] J. Fitzgerald, P. Gorm Larsen, P. Mukherjee, N. Plat, and M. Verhoef (2005). Validated Designs for Object-oriented Systems. Springer, New York.

[11] [Gom Larser etal,1996] P. Gorm Larsen, J. Fitzgerald, and T. Brookes (1996). Applying Formal Specification in Industry. IEEE Software, 13(3):48–56.

[12] [Garcia and Yavar, 2007]D. O. Garcia and L.F. Yavar (2007). Captación y Visualización de Señales ECG Bipolares: Diseño y Desarrollo. VII Congreso de la Sociedad Cubana de BioIngenieria.

[13] [Jackson and Wing,1996] D. Jackson and J. Wing (1996). Formal methods light: Lightweight formal methods. IEEE Computer, 29(4):21–22, April 1996

[14] Jones, 1996] C. B. Jones. (1996). Formal methods light: A rigorous approach to formal methods. IEEE Computer, 29(4):20–21, April 1996.

[15] [Kurita et al, 2008] T. Kurita, Y. Nakatsugawa & M. Chiba (2008). Application of a Formal Specification Language in the Development of the "Mobile FeliCa" IC Chip Firmware for Embedding in Mobile Phone. FM'08 Proceedings of the 15th international symposium on Formal Methods.

[16] [Rumbaugh etal, 1998] J. Rumbaugh, I. Jacobson, and G. Booch, (1998). The Unified Modeling Language Reference Manual, Addison-Wesley.

[17] [Sommerville, 2001] I. Sommerville (2001). Software Engineering, Sixth Edition, Addison Wesley.

[18] [The UK Ministery of Defence, 1989] The UK Ministry of Defence (1989). Defence standard for military safety-critical software 00-59. draft.

[19] [Wartak, 1985] J. Wartak (1985). Interpretación de Electrocardiogramas. 2 Ed., Nueva Editorial Interamericana.