Informe de estado de avance del proyecto CSIC

Integración de dos enfoques para la certificación formal de sistemas reactivos

1/7/2000 - 30/6/2001

Gustavo Betarte, Cristina Cornes

19 de Julio de 2001

1 Introducción

Durante el período 1/7/2000 - 30/6/2001 trabajaron como investigadores estables en el proyecto Gustavo Betarte y Cristina Cornes en tanto que responsables del proyecto y Luis Sierra realizando su trabajo de doctorado bajo la dirección de Cristina Cornes.

En 1999 los investigadores del InCo establecieron contacto con la empresa uruguaya *Centro de Construcción de Cardioestimuladores del Uruguay*[1]. Esta empresa fabrica y exporta estimuladores cardíacos implantables y diseña prototipos de dispositivos médicos a pedido de equipos de investigadores en medicina. Los ingenieros de CCC manifestaron interés en verificar formalmente el código embarcado en sus marcapasos. En este marco, CCC posibilitó a los investigadores del InCo, acceso al programa fuente escrito en lenguaje C. Esta aplicación representa un caso de estudio típico de la clase de programas en los que se interesa este proyecto: código embarcado, reactivo, escrito en un lenguage imperativo, con interrupciones por hardware y manejo de tiempo real.

Las actividades de Cristina Cornes y Luis Sierra se centraron en torno a la verificación de sistemas reactivos, tomando como caso de estudio el código embarcado en un microcontrolador para marcapasos.

La actividad de Gustavo Betarte se centró en torno a la verificación de código embarcado en tarjetas inteligentes y telefonía.

[1] `www.ccc.com.uy`

2 Actividades realizadas durante el primer año

Cristina Cornes comenzó la modelización del código embarcado en un microcontrolador para marcapasos utilizando `Correctness`, la herramienta de representación de programas imperativos en Coq desarrollada por Jean-Cristophe Filliatre [3]. Esta herramienta permite modelar y razonar sobre las estructuras de control y las estructuras de datos básicas de un lenguaje de programación imperativo. Sin embargo no contempla en forma directa la modelización relojes, ni el manejo de hardware ni de interrupciones por hardware, características típicas del caso de estudio. Una propuesta para modelar estos aspectos en Coq es considerar una extensión del lenguaje manejado por `Correctness` con primitivas de control específicas para relojes y manejo de interrupciones por hardware. Dichas primitivas son especificadas a través de pre y pos condiciones. Este trabajo de modelización está actualmente en curso.

Cristina Cornes realizó también un estudio bibliográfico de las normas y estándares internacionales de calidad que aplican a software embebido de seguridad crítica. Una parte de esta revisión bibliográfica será volcada al dictado de un curso para profesionales sobre buenas prácticas para mejorar la seguridad y confiabilidad del software a ser dictado en el segundo semestre del 2001 o primer semestre del 2002.

Luis Sierra realizó, en el marco de su de su plan de doctorado, una misión de un mes en Francia del 1 al 28 de Octubre del 2000. Durante la misma, trabajó dos semanas en el Laboratorio de Especificación y Verificación (LSV) de la ENS de Cachan y dos semanas en el seno del proyecto Coq del Inria-Rocquencourt.

Durante su estadía en Cachan, Luis Sierra dictó un seminario a los estudiantes de posgrado del LSV sobre el análisis del código de microcontroladores con tiempo real empleando verificadores de modelo.

También trabajó con la Dra. Bérard en el tema de comparación de herramientas de verificación de modelos. Un trabajo preliminar sobre dicha comparación fue reportado en [1]. Las actividades desarrolladas comprendieron la elaboración de juegos de prueba comparativos para los verificadores de modelos Uppaal, Hytech, Kronos y la realización de las pruebas correspondientes. Los criterios de comparación fueron la eficiencia de los sistemas y el tamaño (número de estados) de los sistemas que pueden ser tratados con cada herramienta.

En el INRIA Rocquencourt, Luis Sierra presentó el trabajo "On the verification of a pacemaker code" en el seminario del proyecto Coq. Durante su estadía Sierra continuó trabajando sobre la verificación del código fuente del marcapaso, con un enfoque alternativo al de Cristina Cornes. En este enfoque se emplean técnicas de análisis estático a fin de simplificar el problema. Las mismas han sido utilizadas en la literatura, pero solamente en sistemas sin restricciones temporales. Luis Sierra modeló en Kronos la porción del código correspondiente al manejo del tiempo de respuesta para dos modos de funcionamientos simples de un marcapasos unicameral. Sobre estos modelos probó dos propiedades de diferente naturaleza. Una primera propiedad prueba que el modelo realizado del programa describe correctamente la evolución del tiempo. Esta propiedad, general a todo sistema informático de tiempo real, garantiza la coherencia del modelo. La segunda propiedad demostrada muestra que, bajo ciertas condiciones, el marcapasos realiza los estímulos eléctricos adecuados en los tiempos esperados. Esta segunda propiedad certifica el correcto funcionamiento del programa que controla el marcapasos.

Resta por analizar la porción "no temporal" del código, sobre la cual interesa demostrar propiedades de corrección vinculadas al valor de las variables del programa en ciertos estados del marcapasos. Para esta parte de su trabajo se piensa utilizar la herramienta *Correctness* de Coq, siguiendo la línea de trabajo comenzada por Cristina Cornes. De obtener buenos resultados con este enfoque, Luis Sierra abordará otros modos más complejos de marcapasos unicamerales.

Un reporte técnico con los resultados obtenidos hasta el momento está siendo redactado.

Gustavo Betarte trabajó con investigadores del Inria-Sophia Antipolis en torno a la verificación de código embarcado. En particular estudió sobre cómo pasar de una formalización directa del código embarcado a una formalización más abstracta y menos operacional de la aplicación a verificar. Para eso se tomó como caso de estudio los intérpretes del lenguaje Java embarcados en los microprocesadores de tarjetas inteligentes (smart cards), como por ejemplo las tarjetas de crédito utilizadas en Francia o las tarjetas al interior de los teléfonos celulares.

Este trabajo permitió extender el área de estudio del proyecto a ejemplos que, si bien no corresponden enteramente a un sistema reactivo, sí comparten varios puntos en común (aplicaciones embarcadas, escasez de recursos de memoria, programación en lenguajes imperativos). Se espera que esta nueva área de investigación del Inco pueda desarrollarse más gracias a un post-doc de un año que ha sido propuesto a Gustavo Betarte por parte de la empresa francesa Trusted Logic (`www.trusted-logic.fr`). Trusted Logic es una start-up creada por el INRIA y Bull CP8 que se especializa en la verificación de propiedades de seguridad de aplicaciones Java embarcadas en tarjetas inteligentes.

3 Evaluación de los resultados obtenidos durante el primer año

El trabajo de Cristina Cornes y de Luis Sierra en el primer año permitió avanzar en la verificación del código de marcapasos. El trabajo de Gustavo Betarte permitió definir nuevas líneas de investigación a desarrollar con investigadores del proyecto OASIS del Inria-Sophia Antipolis, en torno al área de verificación de propiedades de seguridad aplicadas a tarjetas inteligentes y telefonía móvil. Si bien queda aún mucho trabajo a realizar en ambas direcciones, se espera que los resultados del proyecto redundarán en una transferencia directa de nuevas tecnologías del ámbito científico a la industria uruguaya.

En lo que refiere al desarrollo del proyecto cabe señalar que uno de los principales obstáculos enfrentados durante el primer año fue la dificultad, por parte los investigadores con mayor experiencia, de disponer del tiempo suficiente para dedicarse a tareas de investigación a tiempo completo. En ese sentido es de destacar la importancia que reviste para los investigadores del equipo el poder realizar estadías periódicas en laboratorios externos, durante las cuales pueden consacrarse exclusivamente al proyecto. Sin embargo, esta dificultad no impidió que el cronograma de actividades llevadas a cabo coincida globalmente con el cronograma planteado.

En resumen, los participantes del proyecto consideran positivo este primer año del proyecto.

4 Perspectivas para el año siguiente

La continuación inmediata del trabajo realizado en el primer año es avanzar en la verificación del código del marcapasos, utilizando en ciertas etapas de la misma, la herramienta `Correctness` de verificación de programas imperativos provista por el sistema Coq. Este trabajo será realizado por Cristina Cornes y Luis Sierra.

A partir de Julio del año 2001 y hasta Abril del 2002 Gustavo Betarte realizará un post-doc en la empresa Trusted Logic. Se espera que esto sea el punto de partida para el desarrollo de una nueva área en torno a la verificación de propiedades de seguridad en el área de tarjetas inteligentes y telefonía en el InCo.

Referencias

[1] B. Bérard, L.Sierra *Comparing verification with HyTech, Kronos and Uppaal on the railroad crossing example* Research Report LSV-00-2, January 2000

[2] L.Sierra *Verifying Electronic Devices. Case Study: A Pacemaker* 2do. Congreso Uruguayo de Informática, Agosto, 1999. `http://www.info-uy.org/ponencias/ponencias.htm`

[3] J.C. Filliâtre *Preuve de programmes impératifs en théorie des types* Thse de Doctorat, Université de Paris-Sud, May 1999.