Informe Final de Proyecto CSIC

Integración de dos enfoques para la certificación formal de sistemas reactivos

1/7/2001 - 30/6/2002

Gustavo Betarte, Cristina Cornes

18 de Febrero de 2003

En Julio de 2000 CSIC aceptó brindar apoyo económico al proyecto financiando la participación de dos investigadores. Este documento describe las actividades desarrolladas durante el segundo año del proyecto (Julio 2001 - Junio 2002) y presenta la evaluación final de los resultados obtenidos durante todo el proyecto.

1 Antecedentes relativos al primer año

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 Instituo de Computación de la Facultad de Ingeniería (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

[1] www.ccc.com.uy

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.

1.1 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 [7]. 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.

Realizó también un estudio bibliográfico de las normas y estándares internacionales de calidad que aplican a software embebido de seguridad crítica.

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 Institut Nationale de Recherche en Informatique et Automatique (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 [5]. 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.

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).

2 Actividades realizadas durante el segundo año

Durante el segundo año participaron en calidad de responsables del proyecto, Cristina Cornes y Gustavo Betarte (quien se encuentra realizando un post-doc en Francia en la empresa Trusted Logic desde Julio de 2001) Luis Sierra y Alberto Pardo participaron en calidad de investigadores estables.

Las actividades desarrolladas durante el segundo año acompasaron parcialmente las perspectivas de trabajo que quedaron planteadas al finalizar el primero [4]. Se trabajó sobre tres ejes de acción:

- El primer eje fue de investigación entorno la verificación de sistemas informáticos llamados “de tiempo real” (donde el tiempo de respuesta del sistema es crítico) y escritos en lenguajes de programación imperativos (como por ejemplo el lenguaje C y Java).
- El segundo eje fue de acción entorno a la consolidación de un grupo de trabajo en el área de código orientado objetos.Un dominio de aplicación de este tema es el código embarcado en microprocesadores de tarjetas inteligentes y telefonía celular.
- El tercer eje de investigación fue en área no prevista en los objetivos iniciales del proyecto: el estudio de transformaciones de programas recursivos escritos en un lenguaje de programación funcional.

En el área de verificación de sistemas de tiempo real escritos en programas imperativos Luis Sierra estudió la adecuación y complementariedad de varios asistentes de prueba para la verificación de código C. Este estudio está en curso.

Luis Sierra realizó la ponencia *Una cuestión de tiempos* en las Jornadas del InCo, 2001.

También preparó el curso Verificacion y Logica, sobre verificacion de sistemas computacionales, que se dictó en el segundo semestre de 2002.

En el área de verificación de tarjetas inteligentes y de código en lenguaje orientado a objetos, Alberto Pardo y Gustavo Betarte participaron en la redacción de un proyecto de cooperación científica entre los siguientes grupos de investigación:

- Métodos Formales del InCo,
- Métodos Formales de la Facultad de Matemática, Astronomía y Física de la Universidad de Córdoba (Argentina),
- Projet Lemme del laboratorio INRIA de Sophia-Antipolis.

Dicho proyecto fue presentado en agosto de 2001 a la delegación regional francesa del Cono Sur, con el título *Projet de Collaboration Régionale Cône-Sud France: Cartes à Puce*, y obtuvo un finaciamiento de 20.000 (veinte mil) dólares americanos, a ser ejecutados en el período agosto 2001 - agosto 2002.

Alberto Pardo es responsable de coordinación del grupo de trabajo en el tema Tarjetas Inteligentes (JavaCards) del InCo y en particular fue el responsable de la organización de la reunión de trabajo de dicho proyecto Noviembre 2001 en Montevideo.

Gustavo Betarte trabajó en esta área de investigación durante su primer año de pos-doctorado en la empresa Trusted Logic. Su actividad se centró en el desarrollo de la especificación formal y de la demostración de propiedades de seguridad del proceso de verificación estática, carga y ejecución de aplicaciones (*applets*) en una tarjeta inteligente Java Card. En particular estuvo a cargo de la especificación formal y verificación mecanizada, usando el asistente de pruebas Coq, de un Card Manager (runtime environment embebido) para la plataforma Java Card 2.1.1 y de las *Application Programming Interfaces (API)* definidas para esa misma plataforma. Los modelos formales han sido desarrollados para la empresa SchlumbergerSema[2].

Es co-autor del artículo "FORMAVIE: Formal Modelling and Verification of the Java Card 2.1.1 Security Architecture", publicado en los Proceedings de la Conferencia *e-Smart 2002*, desarrollada en Cannes, Francia, en setiembre de 2002.

[2]Partner del proyecto OPPIDUM Formavie: proyecto de Investigación y Desarrollo en el dominio de la seguridad de sistemas de información, promovido y parcialmente finaciado por el Ministerio de Economía, Finanzas y de la Industria francés. El partner científico de este proyecto es el instituto de investigación francés INRIA

Dirige actualmente los estudiantes de Maestría en Informática en esta área Daniel Perovich, Andrés Vignaga y Leonardo Rodríguez. La tesis de Perovich tiene por objetivo diseñar un asistente de pruebas para OCL e implementarlo sobre Coq. La tesis de Vignaga tiene por objetivo la definición de una semántica operacional para los operadores del metamodelo UML.

Vinculados a los ejes (1) y (2) y en base al estudio bibliográfico de las normas y estándares internacionales de calidad que aplican a software embebido de seguridad crítica realizado en el primer año del proyecto Cristina Cornes preparó el curso de actualización profesional *Buenas prácticas para mejorar la calidad, seguridad y confiablidad del software* . Dicho curso se dictó en Julio de 2002 en el InCo en el marco de las actividades del Centro de Posgrados del Área del PEDECIBA y de la Facultad de Ingeniería.

En torno al eje (3) trabajó Alberto Pardo estudiando transformaciones de programas recursivos escritos en lenguajes de programación funcional. En particular trabajo en los aspectos finales de su tesis de doctorado [1] que defendió en la Universidad Tecnológica de Darmstadt (Alemania) en Octubre 2001. También escribió el artículo [2] aceptado para publicación en los proceedings de IFIP Working Conference on Generic Programming, realizada en Dagstuhl, Alemania, en Julio 2002.

3 Evaluación de los resultados obtenidos

La verificación de programas imperativos para sistemas de tiempo real por la vía de la integración de los enfoques *verificadores de modelos* y *asistentes de pruebas* ha sido abordada sin que los resultados obtenidos sean aún contundentes. Se ha atacado problema con la estrategia de abstraer la estructura temporal y la no temporal para luego utilizar el enfoque específico a cada estructura. Esta estrategia no está aún validada. Luis Sierra continuará su trabajo de Doctorado en esta área.

La línea de investigación iniciada por Gustavo Betarte en torno a la verificación de propiedades de seguridad aplicadas a tarjetas inteligentes y telefonía móvil está hoy consolidada y tiene su vida propia en el marco de un proyecto específico de cooperación internacional.

Si bien el estudio de transformaciónes de programas recursivos para la incorporación en compiladores de lenguajes funcionales no era parte de los objetivos del proyecto, los resultados obtenidos fueron muy satisfactorios. Alberto Pardo encontró en el marco del proyecto la posibilidad de terminar su tesis de Doctorado y de realizar una publicación internacional.

En consecuencia se considera que los resultados obtenidos durante el desarrollo del proyecto son muy positivos, aún cuando no se cumplieron los objetivos planteados en su totalidad.

En lo que refiere al desarrollo del proyecto cabe señalar que uno de los principales obstáculos enfrentados durante el segundo año fue la dificultad, por parte los investigadores de disponer del tiempo suficiente para dedicarse a tareas de investigación a tiempo completo. En ese sentido es de destacar la importancia que revistió para los investigadores del equipo el poder realizar estadías periódicas en laboratorios externos, durante las cuales poderse consacrar exclusivamente al proyecto.

Referencias

[1] A. Pardo *A Calculational Approach to Recursive Programs with Effects* Tesis de Doctorado, Universidad Tecnológica de Darmstadt (Alemania). Octubre 2001

[2] A. Pardo *Generic Accumulations* IFIP Working Conference on Generic Programming. Julio de 2002

[3] Projet de Collaboration Régionale Cône-Sud France: Cartes à Puce Presentado ante la Delegación Regional Francesa del Cono Sur. Agosto de 2001

[4] G. Betarte, C. Cornes *Informe de estado de avanc de proyecto CSIC. Integación de dos enfoques para la certifiación formal de sistemas reactivos. 1/7/2000-30/6/2001* 19 de Julio de 2001

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

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

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