MÉTODOS FORMALES PARA VERIFICAR LOS NUEVOS DESARROLLOS EN SISTEMAS DE TRANSPORTE

FORMAL METHODS FOR VERIFY THE NEW DEVELOPMENTS IN TRANSPORTATION SYSTEMS

MÉTHODES FORMELLES POUR VERIFIER LES NOUVEAUX DEVELOPPEMENTS DANS SYSTEMES DE TRANSPORT

Joseph A. Kinirty
University College Dublin
jakinirty@ucd.ie

(Tipo de artículo: **REFLEXIÓN**. Recibido el 24/01/2011. Aprobado el 14/05/2011)

RESUMEN
El acelerado desarrollo de los sistemas ciber-físicos modernos y el incremento en la complejidad de su diseño y análisis, requiere nuevas tecnologías para realizar los procesos de verificación e integración. Debido a la base matemática que los sustenta y al incremento constante en la efectividad de sus procedimientos, los métodos formales son los llamados a proporcionar esas tecnologías. En este artículo se comparan los procesos de verificación formal y la tradicional herramienta de simulación para verificar sistemas ciber-físicos.

Palabras clave
Métodos formales, verificación formal, sistemas ciber-físicos de transporte.

ABSTRACT
The rapid development of modern cyber-physical systems and the increasing complexity of its design and analysis requires new technologies to make the process of verification and integration. Because of the mathematical basis that supports them and the steady increase in the effectiveness of its procedures, formal methods are called to provide such technologies. This paper compares the processes and the traditional formal verification simulation tool to cyber-physical systems.

Keywords
Formal methods, formal verification, transportation cyber-physical systems.

RÉSUMÉ
Le développement accéléré des systèmes cyber-physiques modernes et la complexité croissante de la conception et l'analyse, nous demande nouvelles technologies pour réaliser les processus de vérification et intégration. À cause de l'accroissement constante dans l'effectivité de ses procèdes et sa base mathématique, les méthodes formelles sont les élus pour fournir ces technologies. Dans cet article on compare les processus de vérification formelle et l'outil traditionnel de simulation pour vérifier des systèmes cyber-physiques.

Mots-clés
Méthodes formelles, vérification formelle, systèmes cyber-physiques de transport.

1. INTRODUCCIÓN

Los sistemas de transporte –automóviles, aviación, y ferrocarril– involucran interacciones entre controladores de software, redes de comunicación y dispositivos físicos. Estos sistemas se encuentran entre los sistemas ciber-físicos más complejos diseñados por humanos, pero las limitaciones de tiempo y costo que los caracteriza hacen que su desarrollo sea una tarea técnica desafiante. Las tecnologías automatizadas para verificación y validación son indispensables para desarrollar sistemas de transporte seguros y fiables [1].

La tecnología de verificación formal complementa el enfoque tradicional basado en simulación para probar modelos de sistemas ciber-físicos, proporcionando una cobertura completa y exhaustiva. El análisis formal automatizado también se puede utilizar para mejorar el soporte para el diseño, las pruebas y la generación de código; además, las técnicas formales son cada vez más reconocidas como esenciales en el ahorro de tiempo y dinero, y los enfoques formales para la verificación están empezando a ser aceptados como argumentos de certificación [1].

2. REQUISITOS Y DESAFÍOS TÉCNICOS

La nueva tecnología de verificación y validación formal es necesaria para hacer frente a los siguientes desafíos específicos que plantea el sector del transporte:

- **Complejidad**. Los sistemas de transporte son sistemas complejos, y la actual tecnología de verificación formal no es suficiente para el tamaño de estos sistemas, ya que necesitan analizarse en varios niveles de abstracción. Con sólo una técnica de verificación es poco probable que se satisfagan todos los niveles, por lo que es necesario una colección de técnicas que integren adecuadamente los resultados. Los sistemas de transporte son sistemas de tiempo crítico, y su seguridad depende de la capacidad para generar respuestas con garantías en tiempo real; además, la especificación y verificación de los requisitos de sincronización incrementa su complejidad [3]. Los sistemas de transporte consisten en sistemas de control embebidos en el interior del vehículo (V) y en la infraestructura circundante (I), así como en la interacción entre vehículos (V2V) y entre el vehículo y la infraestructura (V2I). Las dinámicas de estas interacciones incrementan la complejidad y plantean nuevos desafíos para la verificación formal.

- **Componentes no confiables o desconocidos**. Los modelos detallados de algunos componentes del sistema de transporte pueden no estar disponibles porque, por ejemplo, los construyen proveedores externos o son parte de algún subsistema heredado. Garantizar la fiabilidad y robustez del sistema obtenido mediante una integración incompleta de los componentes especificados es un reto para la verificación composicional [4].

- **Flexibilidad**. Se espera que los sistemas de transporte evolucionen, por lo que pueden ser actualizados o ampliados con nuevos componentes externos, que se necesitan para asegurar que esos sistemas modificados continúen cumpliendo con su correcta especificación a nivel de sistema.

3. DESAFÍOS EN INVESTIGACIÓN

Los enfoque de verificación formal tradicionales, basados en la comprobación de modelos y prueba de teoremas, son insuficientes para hacer frente a la complejidad de los sistemas ciber-físicos de transporte. Se requiere una nueva matemática y un nuevo soporte computacional para tratar con espacios de estado híbrido y para razonar acerca de combinaciones lineales, no lineales y booleanas, y con las limitaciones de dominio finitas. Debido a que las herramientas existentes no son escalables, se requieren nuevas herramientas y enfoques para sistemas híbridos –discretos + continuos– [4].

La verificación de sistemas ciber-físicos complejos requiere un portafolio de técnicas: desde métodos ágiles e invisibles que verifiquen las propiedades superficiales del modelo detallado hasta métodos robustos que verifiquen las propiedades profundas de una abstracción adecuada del modelo. Por otra parte, las técnicas de verificación formal estáticas, que validan el modelo, el diseño o la implementación, necesitan complementarse con técnicas dinámicas que monitoreen el sistema que está en ejecución. Las técnicas formales de tiempo de ejecución pueden, probabilísticamente, garantizar la seguridad en la línea de tiempo.

La verificación composicional es un importante enfoque para verificar sistemas complejos conformados de varios componentes interconectados; se basa en el análisis de componentes individuales para luego verificar el sistema con una composición del análisis de componentes. El análisis composicional se habilita si los componentes especifican sus interfaces –las restricciones o presunciones en sus entradas y las propiedades o garantías en sus salidas. Un componente debe ser verificado contra su especificación, que incluye la especificación del tiempo y la interfaz [5]. Estas especificaciones, en forma de interfaces e invariantes, pueden ser desde muy simples hasta muy complejas, por lo que se necesitan técnicas formales para generar y controlar interfaces e invariantes.

La verificación formal y las pruebas basadas en simulación deben complementarse entre sí, ya que las primeras utilizan métodos simbólicos lentos pero proporcionan una cobertura exhaustiva, mientras que los enfoques basados en simulación utilizan solucionadores numéricos rápidos pero proporcionan una cobertura limitada. Las técnicas formales se pueden utilizar para desarrollar nuevos enfoques para la generación automática de vectores de prueba –tanto para pruebas de unidad como de sistema–, y para mejorar la cobertura de las pruebas.

Contrariamente, las tareas de verificación y de generación de invariantes se pueden dirigir mediante resultados de simulación [6].

Un enfoque fundamental para construir y verificar sistemas ciber-físicos de transporte complejos se basará en preservar la separación, o más generalmente y de menor privilegio, en las interacciones entre componentes. Los modelos de simulación de sistemas ciber-físicos contienen algunos detalles de la dinámica de bajo nivel que no siempre requieren verificarse mediante algoritmos de control de alto nivel. El modelo de reducción y abstracción es el proceso de simplificar un modelo de simulación a un modelo más para utilizarse en la verificación y el análisis de otros [7]. Realizar el modelo de abstracción automatizado de grandes sistemas híbridos de alta dimensión, y caracterizar y cuantificar la aproximación y/o función de extracción utilizada para crear el modelo más simple, son tareas técnicas desafiantes. Los modelos formales abstractos, en contraste con los modelos de simulación, son simples pero más robustos, y son más adecuados para la verificación. Las técnicas automatizadas para la abstracción de modelos también son necesarias para soportar un modelado multi-escala.

4. CONCLUSIONES

Los sistemas de transporte ciber-físicos se diseñan utilizando herramientas de diseño de sistemas de control asistidas por computador, como Matlab, y el análisis actualmente se soporta sólo en forma de simulación. Para incrementar la confianza en la seguridad y fiabilidad del sistema diseñado, y debido a que el tiempo de desarrollo disponible es limitado, es imprescindible que se desarrolle un portafolio de nuevas tecnologías formales que puedan soportar el diseño, la prueba y la implementación de los sistemas ciber-físicos complejos. Sin embargo, para hacer frente a la complejidad de los sistemas de transporte, estos nuevos enfoques para la verificación y la composición deben ajustarse para que puedan ofrecer mayor garantía a la inversión de más recursos.

REFERENCIAS

[1] J. A. Stankovic, I. Lee, A. Mok & R. Rajkumar. “Opportunities and obligations for physical computing systems”. *Computer*, Vol. 38, No. 11, pp. 23-31. 2005.

[2] B. Brosgol & C. Comar. “DO-178C: A New Standard for Software Safety Certification”. *SSTC 2010*, Salt Lake City, Utah, USA. 2010.

[3] E. A. Lee. “Cyber-Physical Systems - Are Computing Foundations Adequate?” *NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*. Austin, USA, Oct. 16-17. 2006.

[4] E. A. Lee. “Cyber Physical Systems: Design Challenges”. Invited Paper *International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC)*. Orlando, USA, May 5-7. 2008.

[5] J. Wegener & F. Mueller. “Comparison of static analysis and evolutionary testing for the verification of timing constraints”. *Real-Time Systems*, Vol. 21, No. 3, pp. 241-268. 2001

[6] M. Broy. “Functional specification of time-sensitive communicating systems”. *ACM Transactions on Software Engineering and Methodology*, Vol. 2, No. 1, pp. 1-46. 1993

[7] R. Venkatasubramanian, J. P. Hayes & B. T. Murray. “Lowcost on-line fault detection using control low assertions”. *International On-Line Testing Symposium*. Kos Island, Greece, pp. 137-143. 2003.