ARGSAFE: Usando Argumentación para Garantizar Seguridad en Sistemas Técnicos Complejos

Sergio Alejandro Gómez[†], Adrian Groza[‡], Carlos Chesñevar[†], Ioan Alfred Letia[‡], Anca Goron[‡], Mauro Gómez Lucero[†]

[†]Laboratorio de Investigación y Desarrollo en Inteligencia Artificial (LIDIA)[*]
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Av. Alem 1253, (8000) Bahía Blanca, Argentina
E-mail: {sag, cic, mjg}@cs.uns.edu.ar
[†]Department of Computer Science,
Technical University of Cluj-Napoca
Baritiu 28, 400391, Cluj-Napoca, Romania
E-mail: {Adrian.Groza, letia, Anca.Goron}@cs.utcluj.ro

Resumen

En este trabajo, se presenta la problemática asociada al Proyecto Bilateral MINCYT-MECTS Argentina-Rumania llamado *ARGSAFE* que tiene como objetivo estudiar cómo utilizar argumentación rebatible para garantizar seguridad en sistemas técnicos complejos. Los resultados de la investigación se espera que sean aplicables a dominios tales como manejo de autos autónomos, aviación, ciencias médicas y redes de computadores.

Palabras clave: Inteligencia Artificial, Razonamiento no-monótono, Argumentación rebatible, Programación en Lógica Rebatible, Ontologías, Lógicas para la Descripción, Lógicas Híbridas, Razonamiento Normativo, Seguridad, Agentes inteligentes

Contexto

Esta línea de investigación está enmarcada en el Proyecto Bilateral Argentina-Rumania MINCYT-MECTS Código RO/12/05 "Usando Argumentación para Garantizar Seguridad en Sistemas Técnicos Complejos" (ARGSAFE: Using Argumentation for Justifying Safeness of Complex Technical Systems). El proyecto está financiado por el Programa de Cooperación Científico-Tecnológica entre el Ministerio de Ciencia, Tecnología e Innovación Productiva de la República Argentina (MINCYT) y el Ministerio de Educación, Investigación y Deportes de Rumania (MECTS), cabe acotar que las instituciones huésped en estos casos son (por la Argentina) la Universidad Nacional del Sur en Bahía Blanca y (por Rumania) la Technical University of Cluj-Napoca en Cluj-Napoca.

Objetivos, Metodología y Plan de Trabajo

Objetivos y Metodología

El software usado en diferentes tecnologías para toma de decisión (redes de comunicaciones, aviones, automóviles, etc.) se ha vuelto cada más complejo sin posibilidad de realizar una verificación exhaustiva y una incapacidad, en muchos casos, de aplicar métodos formales. Basados en la experiencia de los equipos rumanos y argentinos, proponemos investigar un método para garantizar la seguridad de sistemas de software críticos basados en avances en teoría de argumentación [2] y representación de conocimiento. El tema de investigación involucra dos ejes: (1) cómo las ontologías y las reglas pueden ser usadas para describir requerimientos de seguridad en sistemas complejos, y (2) cómo la teoría de la argumentación puede detectar y resolver inconsistencias.

La integración de teoría de argumentación con las garantías necesarias para definir políticas de seguridad [11] puede considerarse como un tópico de investigación prometedor en varios dominios ([4];[1]). Un caso de seguridad se define en el estándar de Defen-

[*]LIDIA es un miembro del IICyTI (Instituto de Investigación en Ciencia y Tecnología Informática).

sa Inglés 00-56 como [18]: "Un argumento estructurado, soportado por un cuerpo de evidencia que brinda un caso convincente, comprensible y válido indicando que un sistema es seguro para una aplicación dada en un ambiente dado de operación". Así, un caso de seguridad debe presentar argumentos fuertes que un sistema es aceptablemente seguro para operar en un contexto particular [11]. En esta línea de razonamiento, el proyecto propuesto utiliza teoría de argumentación como la instrumentación técnica para soportar seguridad. La argumentación tendrá el rol de integrar la evidencia recolectada a partir de los métodos formales y será presentada a agentes humanos en posición de decidir acerca de la seguridad de sistemas técnicos complejos.

Los casos de seguridad basados en argumentación están siendo aceptados progresivamente en los dominios de la defensa, industria automotriz, extracción gas y petróleo en plataformas marinas, y dispositivos médicos. Consecuentemente, esta investigación busca: (a) identificar los enlaces entre la teoría de argumentación y la ingeniería de sistemas seguros, (b) desarrollar métodos argumentativos para transferir confianza en sistemas de software donde la seguridad es crítica, (c) aplicar la instrumentación técnica a casos de estudio (tales como la seguridad en software para manejo de automóviles autónomos [7], asistencia a controladores de vuelo y control de dispositivos médicos de alta complejidad).

Plan de Trabajo

Primera etapa: Se procederá a la recopilación bibliográfica y realización de contacto e intercambio de ideas entre los investigadores argentinos y rumanos. Se definirán pautas para la caracterización de un sistema argumentativo para razonar sobre garantía de la seguridad en el contexto de una línea de desarrollo automotriz. Se estudiará y definirá un marco para conceptualizar el razonamiento sobre ontologías que describen los estándares de seguridad

Segunda etapa: Se trasladarán los resultados obtenidos sobre la integración de técnicas de razonamiento argumentativo utilizando Programación en Lógica Rebatible al razonamiento con ontologías potencialmente inconsistentes expresadas en Lógicas para la Descripción. Se aprovecharán en tal sentido los razonadores existentes sobre Lógicas para la Descripción y sobre Programación en Lógica Rebatible. En particular, este último brinda la posibilidad de razonar sobre bases de conocimiento inconsistentes con un compromiso óptimo entre expresividad y eficiencia computacional.

Tercera etapa: Se avanzará en el desarrollo de un marco de razonamiento que permita evaluar el aseguramiento de la seguridad en líneas de producción de software embebido de la industria automotriz, sistemas de soporte a la toma de decisiones en el contexto de pilotaje de aviones tripulados y no tripulados. Las políticas de aseguramiento de la seguridad y disminución del riesgo serán representadas con ontologías como las propuestas por la iniciativa de la Web Semántica. Se utilizará un acercamiento argumentativo para modelar el razonamiento sobre las ontologías potencialmente contradictorias que modelen los criterios de aseguramiento de la seguridad con el objetivo que agentes humanos puedan utilizar las respuestas generadas por el marco de razonamiento para poder decidir sobre cuestiones de disminución del riesgo. Se definirán experimentos para evaluar el rendimiento del modelo en casos prototípicos.

Cuarta etapa: Se procederá a la evaluación del sistema desarrollado, recurriendo a experimentos a través de problemas representativos. Se realizará una comparación de rendimiento con otros acercamientos. Se concluirá una especificación definitiva que incorpore los elementos propuestos en el plan de investigación, y se desarrollarán aplicaciones prototípicas para su evaluación experimental.

Resultados Esperados al Término de la Investigación

En forma creciente, los cuerpos reguladores de la seguridad requieren que los desarrolladores de sistemas críticos de software brinden casos explícitos de seguridad –definidos en términos de argumentos estructurados basados en evidencia objetiva– para probar que el sistema es aceptablemente seguro.

Los argumentos de seguridad típicos deben resolver al menos dos problemas: (1) mostrar que todos los riesgos han sido analizados y cómo las medidas de control contribuyen a la mitigación de riesgos, y (2) probar la conformidad con los estándares o lineamientos de seguridad. El modelado de peligros y los riesgos que implican constituyen la bases para los requerimientos de riesgo y los niveles de integridad de la seguridad. En dominios críticos como el software embebido en la industria automotriz, como AUTOSAR, OSEK, Flex-

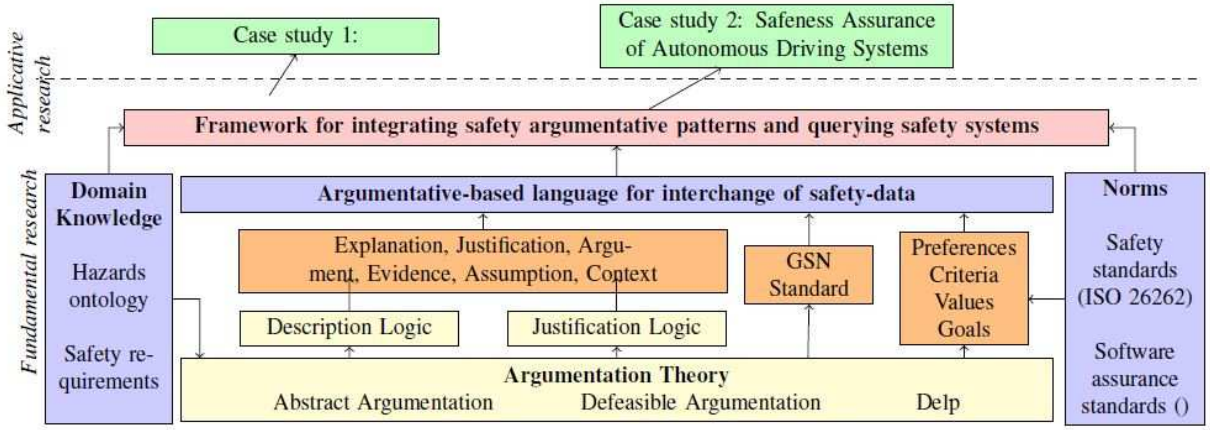

Figura 1: Dominio de investigación

Ray, CAN y LIN están ampliamente utilizados. En esta línea, ISO 26262 y MISRA son dos estándares de software que aplican a la verificación y validación de software para vehículos. Desde una perspectiva socioeconómica, los beneficios para las entidades de negocios involucra la mejora de la comprensión de los argumentos de seguridad entre los involucrados (desarrolladores de software, ingenieros de seguridad, auditores técnicos, cuerpos de certificación). El modelo desarrollado actuará como un contrato formal entre los desarrolladores de software y el cuerpo de certificación de seguridad. Como subproducto, el desarrollador podrá determinar a priori qué evidencia espera el certificador basado en los estándares activos. Se espera que los costos de certificación decrezcan porque: (a) la evidencia requerida es recolectada durante el desarrollo del sistema seguro y (b) se necesita menos tiempo para la auditoría pues el caso de seguridad está organizados de acuerdo a los estándares activos. Entonces, nuestra propuesta tenderá a mejorar el negocio a partir de mejorar la seguridad.

Como objetivo científico principal se espera lograr un marco integrador (framework) en lo que concierne a la seguridad de sistemas de software por medio de una teoría argumentativa. Como objetivo transversal a la ejecución del proyecto, se espera aprovechar y fortalecer las capacidades complementarias de los grupos de investigación de la Universidad Técnica de Cluj-Napoca (Rumania) y de la Universidad Nacional del Sur (Argentina). Desde la perspectiva rumana, cabe señalar que la propuesta se enmarca en el área conducida por el grupo de Sistemas Inteligentes (director: I. Letia, http://cs-gw.utcluj.ro/letia/publications.html), y el escenario de vehículos autónomos se vincula con el grupo de *Image Processing* dirigido por Sergiu Nedevschi (http://users.utcluj.ro/nedevski), lo que provee un incentivo adicional para colaborar con el grupo argentino. Desde la perspectiva argentina, el trabajo realizado en Rumania se vincula complementariamente con el desarrollo de software utilizando argumentación, área en la cual el grupo argentino ha trabajado con resultados prometedores, principalmente a través de la denominada Programación en Lógica Rebatible (DeLP) (ver http://lidia.cs.uns.edu.ar) ([8]; [9]).

Los esfuerzos actuales de investigación están centrados en realizar un cruce de las temáticas investigadas por ambos grupos y viendo cómo ambos acercamientos se pueden combinar para atacar el problema de garantizar seguridad en sistemas complejos como por ejemplo sistemas de navegación en autos. La navegación en automóviles es un tema de impacto tanto en el ámbito científico como en el periodístico ([3]; [15]; [7]). En particular el proyecto Obstacle Avoidance System de Ford es un caso paradigmático junto con aplicaciones de lógica difusa al control de vehículos ([6]; [12]), aplicaciones de ontologías para vehículos de búsqueda y rescate ([19] desarrollan una ontología para lograr una representación neutral que capture la información relevante acerca de robots y sus capacidades para asistir en el desarrollo, testing y certificación de tecnologías para sensado, movilidad, navegación, planificación, integración e interacción con operadores en el contexto de robots de búsqueda y rescate).

Otros autores están enfocados en la producción de marcos de control cognitivo para sistemas robóticos y en particular en la generación de ontologías para tal aplicación (por ejemplo, CORBYS se enfoca en sistemas robóticos que tienen que lidiar con ambientes altamente dinámicos; en este caso CORBYS [5] pretende implementar una arquitectura de control de ro-

bots que permita la integración de (1) módulos de robots cognitivos de alto-nivel, y (2) un módulo con self-awareness). En este contexto, un tópico de la investigación está dado por la implementabilidad del marco de definiciones que desarrollarámos como fruto de la investigación; así, se muestran atractivos resultados de otros autores respecto de la posibilidad de usar ambientes virtuales de prueba y su relación con robots físicos en el mundo real (ver [14]). Otras avenidas de investigación se focalizan en estudiar cómo afecta un cambio en la documentación de un proyecto a la seguridad del mismo; en este sentido OMoC [13]) desarrolla un acercamiento para la gestión del cambio basada en ontologías para soportar la evolución, revisión y adaptación de colecciones de documentos técnicos.

Para permitir la verificación de normas en procesos de negocios integrados, Letia & Groza [17] desarrollaron el marco NJL-ALC para cerrar la brecha entre las normas abstractas y los procesos de negocios concretos. Para razonar sobre los permisos y obligaciones activas, extendieron la Lógica Temporal Normativa (NJL) al aplicar operadores deónticos de obligación y permiso en la lógica para la descripción $\mathcal{ALC}$ (Attribute Language with Complements). Como prueba de concepto de sus resultados, han usado el estándar de análisis de riesgos en puntos críticos (Hazard Analysis at Critical Points), para prevenir la ocurrencia de riesgos en la industria de la comida.

Letia & Goron [16] introdujeron justificaciones en sistemas normativos con elobjeto de entender mejor el cumplimiento de normas, incluyendo las situaciones de conflicto entre normas que pudieran surgir. Para mantenerse al nivel de las explicaciones sobre la justificación, emplearon la Lógica Híbrida de Justificación (Hybrid Justification Logic). Aplicaron estos conceptos a un caso de estudio para un sistema de manejo de tránsito. Las relaciones entre normas es juzgada con respecto a los valores de una sociedad multi-agente a través Argumentación Basada en Valores (Value-Based Argumentation). La justificación para la manera en que los agentes cumplen o no con las normas, relativas a sus valores sociales, ha sido implementada en el ambiente argumentativo CaSAPI.

Resultados Obtenidos y Trabajo en Progreso

Al momento actual los resultados obtenidos incluyen una publicación en una conferencia internacional. En [10], Goron et al. proponen un acercamiento basado en argumentación para la actualización de modelos en lógicas híbridas. La teoría de argumentación es usada para asistir el proceso de actualización del modelo. Un modelo de Kripke Híbrido es visto como una descripción del mundo en el que estamos interesados. Esta actualización en tal modelo Kripke ocurre cuando el sistema tiene que acomodar nuevas propiedades deseables o restricciones normativas. Cuando el modelo falla en verificar una propiedad, un programa lógico rebatible es usado para analizar el estado corriente. Dependiendo del estado de aceptación de los argumentos, el sistema puede garantizar cuatro acciones primitivas en el modelo: actualizar variables de estado, agregar una nueva transición, remover una transición, o agregar un nuevo estado. Un escenario de prueba es presentado mostrando la verificación de un vehículo aereo no tripulado, al interlazar razonamiento en Programación en Lógica Rebatible y verificación de modelos en el Hybrid Model Checker. Como parte de nuestro trabajo en progreso, estamos tratando de extender las ideas de dicho trabajo a un sistema multiagente contemplando la comunicación entre vehículos no tripulados.

Formación de Recursos Humanos

El proyecto cuenta con un director argentino (Sergio Gómez), uno rumano (Adrian Groza), profesores (Carlos Chesñevar e Ioan Letia) y dos becarios de posgrado o posdoctorado (Anca Goron y Mauro Gómez Lucero). Este proyecto involucra dos misiones de estancias de investigación para investigadores argentinos hacia Rumania y tres estancias de investigadores rumanos hacia Argentina. Durante 2013 se realizó una pasantía de investigación del becario rumano en Argentina y una misión del director argentino en Rumania. Durante 2014, se esperan realizar dos misiones de director e investigador rumano en Argentina junto con una pasantía de investigación del becario argentino en Rumania.

Agradecimientos

Parte de esta investigación está apoyada por el Proyecto Bilateral Argentina-Rumania MINCYT-MECTS RO/12/05 (“Usando Argumentación para Garantizar Seguridad en Sistemas Técnicos Complejos” (ARG-SAFE: Using Argumentation for Justifying Safeness of Complex Technical Systems), por la Universidad Nacional del Sur, y por la Universidad Técnica de Cluj-Napoca. Adrian Groza es apoyado por el proyecto de la Universidad Técnica de Cluj-Napoca, Romania “Green-Vanets: Improving transportation using

Car-2-X communication and multi-agent systems".

Referencias

[1] Andy Applebaum, Karl N. Levitt, Jeff Rowe, and Simon Parsons. Arguing about firewall policy. In Bart Verheij, Stefan Szeider, and Stefan Woltran, editors, *COMMA*, volume 245 of *Frontiers in Artificial Intelligence and Applications*, pages 91–102. IOS Press, 2012.

[2] T. J. M. Bench-Capon and Paul E. Dunne. Argumentation in artificial intelligence. *Artif. Intell.*, 171(10-15):619–641, 2007.

[3] Terry Bennett. Google's Plan for Autonomous Cars Doesn't Go Far Enough. 30 Sep 2013, 2013.

[4] Paul W. H. Chung, Larry Y. C. Cheung, and Colin H. C. Machin. Compliance flow - managing the compliance of dynamic and complex processes. *Know.-Based Syst.*, 21(4):332–354, May 2008.

[5] Corbys. CORBYS: Cognitive Control Framework for Robotic Systems. Deliverable D4.1 Generalisation of Ontology Hierarchy Specification, 2012.

[6] T. Fraichard and P. Garnier. Fuzzy control to drive car-like vehicles. *Robotics and Autonomous Systems*, 34(1):1–22, 2001.

[7] Silberg G., Wallace R., Matuszak G., Plessers J., Brower C., and Subramanian D. Self-driving cars: The next revolution. KMPG and The Car Group, 2012.

[8] A. García and G. Simari. Defeasible Logic Programming: An Argumentative Approach. *Theory and Prac. of Logic Program.*, 4(1):95–138, 2004.

[9] Alejandro Javier García, Nicolás D. Rotstein, Mariano Tucat, and Guillermo Ricardo Simari. An Argumentative Reasoning Service for Deliberative Agents. In Zili Zhang and Jörg H. Siekmann, editors, *KSEM*, volume 4798 of *Lecture Notes in Computer Science*, pages 128–139. Springer, 2007.

[10] Anca Goron, Adrian Groza, Sergio Alejandro Gómez, and Ioan Alfred Letia. Towards an argumentative approach for repair of hybrid logics models. In *Eleventh International Workshop on Argumentation in Multi-Agent Systems (ArgMAS 2014)*, page (Accepted), 2014.

[11] Patrick J. Graydon, Ibrahim Habli, Richard Hawkins, Tim Kelly, and John C. Knight. Arguing conformance. *IEEE Software*, 29(3):50–57, 2012.

[12] A. El Hajjaji and S. Bentalba. Fuzzy path tracking control for automatic steering of vehicles. *Robotics and Autonomous Systems*, 43(4):203–213, 2003.

[13] D. Hutter and M. Kohlhase. OMoC - Ontology-Driven Management of Change. Jacobs University, Bremen, Germany, 2012.

[14] Alex Juarez. *Semantic Web for Robots: Applying Semantic Web technologies for interoperability between virtual worlds and real robots*. PhD thesis, Technische Universiteit Eindhoven, 2012.

[15] Leo Kelion. Los autos del futuro maniobrarán solos para evitar choques. La Nación (via BBC Mundo) 15 Oct 2013, 2013.

[16] I.A. Letia and A. Goron. Towards justifying norm compliance. *Coordination, Organizations, Institutions, and Norms in Agent System VII*, 7254:110–128, 2012.

[17] I.A. Letia and A. Groza. Compliance Checking of Integrated Business Processes. *Data & Knowledge Engineering*, 87:1–18, 2013.

[18] UK Ministry of Defence. 00-56 safety management requirments for defence systems. *UK Ministry of defence*, 4(9), 2007.

[19] C. Schlenoff and Messina. E. A robot ontology for urban search and rescue. In *Proc. of the 2005 CIKM Conference: Workshop on Research in Knowledge Representation for Autonomous Systems*, pages 27–34, 2005.