Ingeniería de software para sistemas críticos ferroviarios

Irrazábal, Emanuel; Bernal, Rubén; Pinto Luft, Cristian; Sambrana, Iván

Departamento de Informática. Facultad de Ciencias Exactas y Naturales y Agrimensura. Universidad Nacional del Nordeste
{eirrazabal}@exa.unne.edu.ar, rbernal73@gmail.com, cristianpl777@gmail.com, sambranaivan@gmail.com

Resumen

Esta línea de investigación aborda temas de ingeniería del software en sistemas tradicionales y su traslado a sistemas críticos con aplicación en el sistema ferroviario argentino. El propósito de esta línea de trabajo es desarrollar los sistemas de gestión para el desarrollo de proyectos software ferroviarios de acuerdo con la normativa europea EN 50128 y la construcción del ecosistema de herramientas que lo instrumenten. Esta nornativa describe un conjunto de buenas prácticas y técnicas opcionales que serán tenidas en cuenta a lo largo del desarrollo software. Debido a ello es necesario analizar las posibles implementaciones de estas buenas prácticas para que sea conforme la normativa. Finalmente, la línea de trabajo plantea la posibilidad de trasladar los resultados a proyectos específicos en conjunto con la Autoridad Ferroviaria Nacional.

Palabras clave: Ingeniería de software, sistemas críticos, EN 50128, desarrollo de procesos.

Contexto

La línea de Investigación y Desarrollo presentada en este trabajo corresponde al proyecto PI-F17-2017 “Análisis e implementación de tecnologías emergentes en sistemas computacionales de aplicación regional.”, acreditado por la Secretaría de Ciencia y Técnica de la Universidad Nacional del Nordeste (UNNE) para el periodo 2018-2021.

Asimismo, parte de la línea de investigación es realizada es desarrollada en el marco de la tesis del maestrando Cristian Pinto Luft perteneciente a la Maestría de Tecnologías de la Información Rs. 764/14 CS UNNE.

Introducción

El sistema público ferroviario argentino se encuentra centralizado, y aunque se percibe como poco importante constituye un eslabón fundamental para la industria. En Argentina cada día tres millones de personas viajan en tren o subte y el 10% del PBI se moviliza por ferrocarril [1]. Sin embargo, todos los sistemas electrónicos para la seguridad vial de trenes y subtes son importados y muy caros. Por ejemplo, un sistema de barrera automático cuesta hasta 200.000 dólares y un sistema de control de velocidad más de 100.000 dólares. Así, en muchos trenes, no hay sistemas de seguridad para pasajeros, conductores, peatones y automovilistas y en otros, se siguen usando tecnologías de hace más de 50 años, que en los países con alto desarrollo tecnológico han sido reemplazadas hace mucho tiempo [2]. Esta situación ha favorecido que ocurran terribles accidentes [3] y ha urgido al Estado a adquirir en el exterior trenes y sistemas de seguridad ferroviaria, lo que implica enormes gastos en dólares y depender de tecnología extranjera [4][5][6] . Pero en la mayoría de los casos los accidentes se podrían haber evitado mediante el uso de sistemas electrónicos apropiados, que hoy en día son habituales en países con alto desarrollo tecnológico. Sin embargo, como se mencionó

anteriormente, en la actualidad estos sistemas no se desarrollan en la Argentina.

Existen, sin embargo proyectos de investigación y de extensión que se encuentran actualmente trabajando en ello. Un ejemplo de ello es el Proyecto Desarrollo de Estratégico UBA Nº23 "Controlador electrónico para barreras automáticas ferroviarias con nivel de integridad de seguridad certificable hasta SIL4" desarrollado por el Dr. Ariel Lutenberg, director del Programa CIAA. El objetivo de este proyecto ha sido desarrollar un prototipo de Monitor de Barrera ferroviaria construido a partir de normas internacionales y componentes electrónicos programables, en este caso la Computadora Industrial Abierta Argentina.

Los sistemas ferroviarios son complejos, compuestos por distintos componentes software, hardware y humanos, que interactúan con su entorno de maneras muy variadas. Un fallo en uno de estos componentes o subsistemas puede llegar a tener asociados distintos niveles de peligros, pudiendo causar pérdidas financieras, daño al equipamiento, daños ambientales, lesiones a personas o en los peores casos pérdidas de vidas humanas. Por estos motivos dichos sistemas se encuentran regulados con distintas leyes y normativas cuyo fin es preservar los recursos anteriormente mencionados [7]. Algunos de los principales organismos que regulan esta actividad son el Comité Européen de Normalisation Electrotechnique (CENELEC) en Europa o la International Electrotechnical Commission (IEC) en América.

Una de las características más importantes de los sistemas que estas normas intentan reforzar durante todo su ciclo de vida son las de fiabilidad, disponibilidad, mantenibilidad y seguridad (RAMS por sus siglas en inglés).

Las principales normas propuestas por el CENELEC orientadas a la resolución de la problemática explicada anteriormente son las siguientes:

- EN 50126 [8]: Aplicaciones ferroviarias. La especificación y demostración de Fiabilidad, Disponibilidad, Mantenibilidad y Seguridad (RAMS). Esta norma se orienta principalmente al cumplimiento de las características RAMS del sistema en general.
- EN 50128 [9]: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Software para sistemas de control y protección del ferrocarril. Esta norma se centra principalmente en la calidad de los aspectos software de los sistemas de ferrocarriles.
- EN 50129 [10]: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización. Esta norma se centra principalmente en los aspectos de calidad del hardware de los sistemas de ferrocarriles.

Una de las características principales de los sistemas críticos es la seguridad de la que estos deben estar dotados por naturaleza, debido a las consecuencias que pueden provocar sus fallos. Para dotarlos de seguridad, una de las metodologías utilizadas en su diseño es el aseguramiento de los mismos desde su concepción, es decir, desde el análisis y definición de sus requerimientos. Para esto se utilizan enfoques que integran las disciplinas de ingeniería de requerimientos con la ingeniería de seguridad, lo cual está comprobado que aumenta significativamente la seguridad del sistema en sí [11].

En la actualidad, grandes organizaciones como la NASA [12], Ansaldo Signal o Siemens Rail Transportation [13] utilizan una combinación de metodologías y formas de trabajo provenientes de distintos campos del conocimiento para lograr dicha vinculación, y de esta manera mejorar la calidad y seguridad de los sistemas críticos que desarrollan, dedicando tiempo, recursos y esfuerzo a esta tarea. Esta línea de trabajo utilizará principalmente los enfoques

propuestos por las normas UNE-EN 50126:2005 y UNE-EN 50128:2012, gestionando las políticas RAMS vinculadas a los requerimientos de los subsistemas software que componen a los sistemas ferroviarios, y haciendo hincapié en los aspectos de seguridad de las mismas.

Para ello es indispensable el desarrollo de procedimientos y un sistema de gestión de calidad conforme la normativa UNE-EN 50128. Esta normativa detalla las buenas prácticas de las diferentes fases en el desarrollo de los sistemas software ferroviarios en las aplicaciones de señalización y control.

Centrándose en la gestión de la seguridad de los requisitos software, existen una amplia variedad de técnicas con las que se intenta, en distintos niveles y bajo diferentes enfoques, dotarlos de dicho atributo de calidad. Entre ellas se pueden encontrar Preliminary Hazard Analysis (PHA) [14], Software Failure Modes and Effect Analysis (SFMEA) [15], Software Effect and Criticality Analysis (SFMECA) [15], Software Failure Tree Analysis (SFTA) [15], Software Common Cause and Failure Analysis (SCCFA) [15], Hardware-Software Integration Analysis (HSIA) [15], Software Subsystem Hazard Analysis (SSHA) [12], Deductive Cause Consequence Analysis (DCCA) [16], entre otras.

Asimismo, existen diferentes herramientas que intentan dar soporte a dicha gestión, cubriendo determinados aspectos relacionados al modelado, control y chequeo de cuestiones relativas a la seguridad, como ser por ejemplo SCADE [17], Matlab [18], CodeCheck [18], StackAnalyzer [19], aiT WCET Analyzer [19], Astrée [19], OVADO [20], Atelier B [21], Rodin [21], Verasis [21], Eclipse Modeling Framework [22], MOFScript [22], PolySpace [23], entre otras. Además de utilizarse herramientas para realizar estos procesos, también se desarrollan y utilizan diversos modelos y meta-modelos de procesos, tratando de abarcar todas las sub áreas que componen al tema en cuestión [16][24][25][26].

Otras herramientas muy utilizadas en este campo de investigación y desarrollo son los métodos formales de modelado, como ser: Formal Failure Model [16], redes de Petri [27], método formal B (lenguaje B) [20][21] o Abstract Interpretation [19][23] entre otros. Mediante los mismos se pretende disminuir la ambigüedad de las distintas fases relacionadas a la gestión de seguridad de los requerimientos software, partiendo desde su análisis, pasando por el diseño y llegando a la verificación formal de los productos a desarrollar.

El propósito de esta línea de trabajo es, por tanto, desarrollar los sistemas de gestión y la construcción del ecosistema de herramientas que lo instrumenten, así como su verificación y validación en ensayos junto con la Autoridad Ferroviaria Nacional, valiéndose de las investigaciones realizadas en el marco del proyecto.

Líneas de investigación y desarrollo

En la línea de Ingeniería de Software para Sistemas Críticos se propone:

- Estudiar las normativas de sistemas críticos ferroviarios para el desarrollo de firmware y software certificables.
- Desarrollar el conjunto de procedimientos para la gestión de requerimientos en entornos críticos y de seguridad funcional.
- Desarrollar un sistema de gestión de calidad adaptados a entidades que construyen sistemas embebidos y sistemas críticos de acuerdo con la norma internacional EN 50128 e ISO 9001.
- Validar los procedimientos construyendo prototipos de sistemas a ser utilizados por la Autoridad Ferroviaria Nacional.

Resultados obtenidos

El grupo de investigación es de reciente formación, por lo cual los resultados son preliminares y, en parte, se enumeran antecedentes llevados adelante en el marco de otros grupos de trabajo. A continuación se indican:

En la línea de Ingeniería de Software para Sistemas Críticos:

- Se está trabajando en el desarrollo de un Ecosistema de Calidad de Software para Sistemas Críticos a partir de las herramientas Jenkins, SONAR, Eclipse Process Framework (EPF), Redmine y Testlink. Estas herramientas sirven como soporte para la gestión colaborativa de los proyectos, la descripción de los procedimientos y el análisis del código fuente [28].
- Se está trabajando en la construcción de los procedimientos de desarrollo software de acuerdo con la norma UNE-EN 50128 soportado por EPF [29].

Formación de recursos humanos

En el Grupo de Investigación en Innovación en Software y Sistemas Computacionales (GIISSC) están involucrados 4 docentes investigadores, 1 becario de investigación de pregrado, 1 tesista de doctorado y 3 tesistas de maestría. Cinco alumnos de la carrera están realizando sus proyectos finales vinculado a estos temas.

Para el caso de esta línea de investigación se encuentran trabajando dos docentes investigadores, un tesista de maestría y dos tesistas de pregrado.

Referencias

[1] Sitio web con estadísticas CNRT: https://www.cnrt.gob.ar/content/estadisticas, Visitado: 19/02/2018.

[2] Ingeniería y gestión del mantenimiento en el sector ferroviario (Spanish Edition) Paperback – 2010, Arques Paton José Luis.

[3] Sitio web con ejemplos de accidentes ferroviarios argentinos:: https://es.wikipedia.org/wiki/Categor%C3%ADa:Accidentes_ferroviarios_en_Argentina. Visitado: 19/02/2018,

[4] Sitio web com ejemplo de licitación: https://www.clarin.com/ciudades/trenes-china-compra-licitacion-reestatizacion_0_rJduN7cwXe.html. Visitado:19/02/2018.

[5] https://www.clarin.com/ieco/china-trenes_de_carga-randazzo-inversiones_0_rJygK8mKP7l.html

[6] https://www.argentina.gob.ar/noticias/japon-comenzara-fabricar-la-tecnologia-para-el-frenado-automatico-de-trenes

[7] J. L. Boulanger, “CENELEC 50128 and IEC 62279 Standards”, Control, Systems and Industrial Engineering Series, John Wiley & Sons, Inc., 2015, p. 13.

[8] EN 50126. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 2005.

[9] EN 50128. Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems. 2011.

[10] EN 50129. Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling. 2005.

[11] J. Vilela, J. Castro, L. E. G. Martins, T. Gorschek, “Integration between Requirements Engineering and Safety Analysis: A Systematic Literature Review”, The Journal of Systems & Software, Vol. 125, Pp. 68-92, Marzo, 2017.

[12] NASA Software Safety Guidebook. NASA Technical Standard. NASA-GB- 8719.13. Marzo, 2004. [15] Ansaldo STS. Website, última visita 11/07/2017. http://www.ansaldo-sts.com/en/index

[13] [Siemens Rail Transportation. Website,. http://w3.siemens.com/mcms/industrial-controls/en/railway/Pages/overview.aspx Visitado 19/02/2018

[14] J. kotti, S. Panchumarthy, "The Quantitative Safety Assessment and Evaluation for Safety-Critical Computer Systems", SIGSOFT Softw. Eng. Notes, Vol. 41, pp. 1-8, Enero, 2016.

[15] R. Pietrantuono, S. Russo, "Introduction to Safety Critical Systems", Innovative Technologies for Dependable OTS-Based Critical Systems, pp. 17-27, Enero, 2013.

[16] F. Ortmeier, M. Güdemann, W. Reif, "Formal Failure Models", IFAC Proceedings Volumes, Vol. 40, pp. 145-150, Junio, 2007.

[17] M. Huhn, S. Milius, "Observations on formal safety analysis in practice", Science of Computer Programming, vol. 80, pp. 150-168, Febrero, 2014.

[18] T. L. Johnson, H. A. Sutherland, B. Ingleston, B. H. Krogh, "Dependable Software in Railway Signalling", IFAC Proceedings Volumes, vol. 38, pp. 42-49, 2005.

[19] D. Kästner, C. Ferdinand, "Applying Abstract Interpretation to Verify EN-50128 Software Safety Requirements", Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification, LNCS, vol. 9707, pp. 191-202, Junio, 2016.

[20] R. Abo, L. Voisin, "Formal Implementation of Data Validation for Railway Safety-Related Systems with OVADO", Software Engineering and Formal Methods, LNCS, vol. 8368, pp. 221-236, Marzo, 2014.

[21] A. G. Russo Jr., "Formal Methods as an Improvement Tool", Industrial Deployment of System Engineering Methods, pp. 81-95, 2013.

[22] A. Svendsen, G. K. Olsen, J. Endresen, T. Moen, E. Carlson, K.-J. Alme, Ø. Haugen, "The Future of Train Signaling", Model Driven Engineering Languages and Systems, LNCS, vol. 5301, pp. 128-142, 2008.

[23] A. Ferrari, D. Grasso, G. Magnani, A. Fantechi, M. Tempestini, "The Metrô Rio ATP Case Study", Formal Methods for Industrial Critical Systems, LNCS, vol. 6371, pp. 1-16, 2010.

[24] J. L. de la Vara, A. Ruiz, K. Attwood, H. Espinoza, R. Kaur Panesar-Walawege, Á. López, I. del Río, T. Kelly, "Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel", Information and Software Technology, vol. 72, pp. 16-30, Abril, 2016.

[25] M. Huhn, H. Hungar, "8 UML for Software Safety and Certification", Model-Based Engineering of Embedded Real-Time Systems, LNCS, vol. 6100, pp. 201-237, 2010.

[26] D. Fowler, P. Bennett, "IEC 61508 - A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems", Computer Safety, Reliability and Security, LNCS, vol. 1943, pp. 250-263, 2000.

[27] M. S. Durmus, U. Yildirim, O. Eris, M. T. Söylemez, "Safety-Critical Interlocking Software Development Process for Fixed-Block Signalization Systems", IFAC Proceedings Volumes, vol. 45, pp. 165-170, Septiembre, 2012.

[28] Diapositivas y explicaciones del funcionamento del Ecosistema de Calidad em www.linsse.com.ar. Visitado: 18/02/2018

[29] Sitio web construído en EPF www.linsse.com.ar/epf. Visitado: 18/02/2018