# Desarrollo de una metodología para la verificación de la calidad del software crítico en sistemas ferroviarios

Jorge Eterovic; Domingo Donadello; Cintia Gioia; Carlos Maidana; Pablo Pomar; Walter Ureta; Silvina Eterovic

Programa CytMA2 / Departamento de Ingeniería e Investigaciones Tecnológicas Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, (5411) 4480-8900

jeterovic@ing.unlam.edu.ar; ddonadel@ing.unlam.edu.ar; cintiagioia@gmail.com; cemaidana@gmail.com; pablo_pomar@yahoo.com.ar; wureta@gmail.com; silvinaeterovic@gmail.com;

## Resumen

En la industria ferroviaria hay una gran cantidad de sistemas críticos que tienen productos de software. Éste software debe cumplir con los criterios de Confiabilidad, Disponibilidad, Manteni-bilidad y Seguridad (RAMS, por sus siglas en inglés) establecidos en las normas internacionales, en particular en las normas CENELEC EN 50126 /7 /8, utilizadas en la Unión Europea.

Para ello, es necesario desarrollar un proceso de evaluación de la conformidad del software adquirido y/o desarrollado para los sistemas de control y protección ferroviarios.

La conformidad se establecerá de acuerdo con los requisitos establecidos en la norma CENELEC EN 50126.

El proyecto de investigación se propone el desarrollo de una metodología para la verificación de la calidad del software crítico usado en los sistemas de control y protección de los ferrocarriles

**Palabras clave:** Calidad del software; Evaluación de Calidad del Software; Verificación de la Calidad del Software Crítico.

## Contexto

Este proyecto de investigación está inserto en el Programa CyTMA2 del Departamento de Ingeniería e Inves-tigaciones Tecnológicas de la Universidad Nacional de La Matanza.

El tema de estudio y su proyección como objeto de investigación surge como una propuesta del Instituto Argentino de Normalización y Certificación (IRAM).

Dentro del enfoque del proyecto podemos enunciar el uso de tecnologías, la exploración de paradigmas nóveles y su aplicación en el ámbito práctico y académico mediante la producción de las pautas básicas que sirvan de base para el desarrollo de una metodología para la verificación de la calidad del software crítico usado en los sistemas de control y protección de los ferrocarriles.

## Introducción

La gran evolución del Transporte Ferroviario a nivel mundial en las últimas décadas hizo que la demanda de prestaciones y servicios sea cada vez mayor. En este sentido, los requisitos asociados a la Calidad y Seguridad Ferroviaria cada vez son más exigentes. Calidad y Seguridad están directamente relacionados y marcan el nivel de confianza que

ofrece un sistema. Los objetivos de Seguridad y Disponibilidad sólo pueden alcanzarse cumpliendo los requisitos de Confiabilidad y Mante-nibilidad.

Como en la industria ferroviaria hay una gran cantidad de sistemas críticos con un alto contenido de software, es necesario desarrollar un proceso de verificación de la calidad de dicho software crítico a efectos de asegurar la Confiabilidad, la Disponibilidad, la Mantenibilidad y la Seguridad, repre-sentadas por las siglas RAMS [1], acrónimo de Reliability, Availability, Maintainability and Safety.

RAMS representa un indicador, tanto cualitativo como cuantitativo, del grado de confianza que ofrece un sistema para comportarse de acuerdo a la funcionalidad especificada, de forma segura y con una alta disponibilidad. En la Unión Europea se han adoptado los requisitos establecidos en las normas CENELEC (Comité Europeo de Normalización Electrotécnica) [2] en materia de RAMS ferroviaria, y en la mejora de los procesos exigida por dichas normas, en especial en el proceso de desarrollo general del producto.

La normativa CENELEC está compuesta por tres normas de la familia EN, y son las EN 50126 [3], EN 50128 [4] y EN 50129 [5].

El grado de integridad de las funciones de seguridad se mide y tabula mediante el SIL, Nivel de Integridad de la Seguridad (Safety Integrity Level) [6]. El SIL mide y tabula la confianza que nos merece que una función de seguridad se vaya a ejecutar adecuadamente. Es una unidad de medida para cuantificar la reducción del riesgo.

Por ello, las organizaciones involu-cradas en el desarrollo del software crítico, deben implementar un Sistema de Garantía de Calidad. El concepto de “Calidad” es muy ambiguo, y también lo es el de “Calidad de Producto de Software” [7], [8], [9], [10]. Una de las definiciones más aceptada es [9]: "Calidad es la totalidad de las características del producto que influyen en la capacidad del producto para satisfacer las necesidades explicitas o implícitas".

En el marco del sistema que lo contiene, el software es una herramienta, y las herramientas tienen que ser selec-cionadas por su calidad y pertinencia.

El software determina el rendimiento de los procesos a los que brinda apoyo, impactando en el desempeño del sistema global, por lo tanto es importante para la calidad de este sistema. Por ello no es una tarea menor evaluar con la máxima objetividad posible las características de calidad deseadas, y debe dedicársele mucho esfuerzo.

Cabe agregar que con la creciente sofisticación de los productos de software y su uso en áreas críticas como medicina, aeronavegación, militar, ferroviaria etc., se han incrementado las actividades de evaluación de la calidad de los productos y artefactos de software [11].

El objetivo de este trabajo es el desa-rrollo de una metodología para la verifica-ción de la calidad del software crítico en sistemas ferroviarios basado en la aplica-ción de la norma IRAM-ISO 90003 [12], que da las directrices para la aplicación de norma IRAM-ISO 9001 [13].

## Líneas de Investigación, Desarrollo e Innovación

El proyecto busca desarrollar una metodología para la verificación de la calidad para cada una de las etapas del ciclo de vida de desarrollo del software de los sistemas de control y protección del ferrocarril basado en una serie de normas y estándares reconocidos y utilizados internacionalmente.

Las normas proporcionan una serie de requisitos que se deben cumplir en las fases de desarrollo, implantación y mantenimiento del software crítico.

El concepto clave es el de los niveles de integridad de seguridad del software. Se identifican cinco niveles, siendo 0 el nivel mínimo y 4 el máximo. Cuanto más peligrosas

sean las consecuencias de un fallo del software, mayor será el nivel requerido de integridad de seguridad del mismo.

La Especificación de Requisitos de Seguridad del Sistema identifica todas las funciones de seguridad asignadas al software y determina el nivel de integridad de seguridad del sistema para dichas funciones. En la figura 1 se muestran las etapas funcionales.

Se debe seleccionar un modelo de ciclo de vida para el desarrollo del software y se debe detallar en el Plan de Garantía de Calidad, cuyo objetivo es identificar, supervisar y controlar toda actividad, tanto técnica como de gestión, necesaria para garantizar que el software alcanza la calidad requerida.

Se debe redactar un Plan de Garantía de Calidad del Software, donde se deben especificar los siguientes elementos:

a) Definición del modelo del ciclo de vida:
   1) actividades y tareas básicas compatibles con los planes, por ejemplo, el Plan de Seguridad que se ha establecido a nivel del sistema;
   2) criterios de entrada y salida de cada actividad;
   3) entradas y salidas de cada actividad;
   4) principales actividades de calidad;

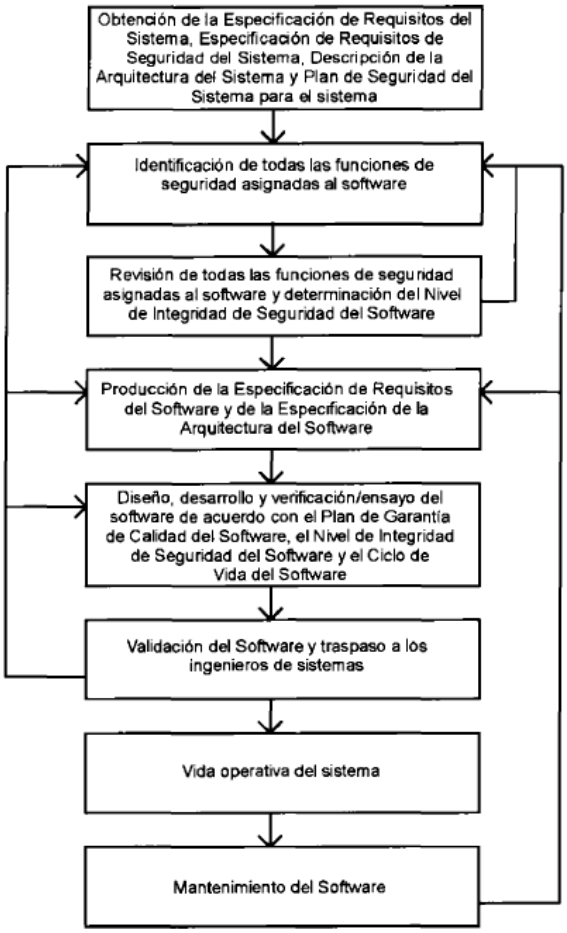


**Figura 1- Etapas funcionales**

   5) entidad responsable de cada actividad.

b) Estructura de la documentación.

c) Control de la documentación:
   1) roles de aquellos implicados en su redacción, control y aprobación;

2) campo de aplicación de la distribución;
3) archivo.

d) Seguimiento y trazabilidad de las desviaciones.
e) Métodos, medidas y herramientas para la garantía de calidad en función de los niveles de integridad de seguridad asignados.
f) Justificaciones de que cada combinación de técnicas o medidas seleccionada es apropiada para cada nivel definido de integridad de seguridad del software.

Cierta información requerida en el Plan de Garantía de Calidad del Software puede aparecer en otros documentos, tales como en el Plan de Gestión de la Configuración del Software, en el Plan de Mantenimiento, en el Plan de Verificación del Software o en el Plan de Validación del Software.

Las actividades de validación correspondientes a la aceptación en varias etapas de un sistema, se basan en la especificación del sistema y deben ser planificadas en las primeras etapas; es decir, empezando en las fases correspondientes de desarrollo del ciclo de vida, como se muestra en la figura 2, donde se muestran por separado las tareas de verificación y validación dentro del ciclo de vida.

El objetivo de la verificación consiste en demostrar que, para las entradas de información específicas, las salidas de cada fase cumplen, en todos los aspectos, los requisitos de dicha fase.

El objetivo de la validación consiste en demostrar que el sistema de que se trate, en cualquier momento de su desarrollo y después de su instalación, cumple con sus requisitos en todos los aspectos.

La metodología para la verificación de la calidad del software crítico no se basará en la utilización de un ciclo de vida de desarrollo específico, pero sí establecerá puntos de control, validaciones, verificaciones, evaluacio-nes, criterios de aceptación y documentación como parte de un proceso myor como lo es el de auditoría y control en el desarrollo de dichos productos de software, de manera de poder garantizar la calidad del mismo desde las diferentes etapas del desarrollo, reduciendo los defectos y los riesgos.

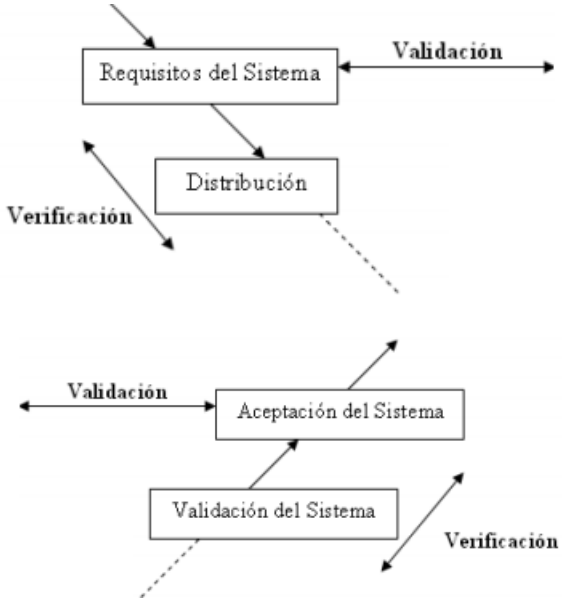


**Figura 2 - Validaciones**

## Resultados y Objetivos

Se ha logrado constituir un grupo de investigación multidisciplinario, donde los resultados esperados se pueden describir en tres aspectos distintos

Resultados en cuanto a la producción de conocimiento: Desarrollar una metodología que se pueda utilizar en la verificación de la calidad del software crítico en sistemas ferroviarios.

Resultados en cuanto a la formación de recursos humanos: Propuesta de capacitación a personal de empresas ferroviarias que daban auditar software de aplicaciones ferroviarias y a alumnos universitarios que puedan desarrollar capacidades de colaboración en audito-rias de sistemas ferroviarios.

Resultados en cuanto a la difusión de resultados: Difusión de la normativa internacional referida a sistemas de control y protección del ferrocarril para promover su adopción. Se ofrecerá la publicación de un Referencial de auditoria de sistemas ferroviarios a través del IRAM.

La metodología una vez desarrollada, servirá como base para la evaluación de la calidad del software crítico de las aplicaciones ferroviarias, y eventualmente permitiría certificar en base a la Norma EN 50128:2011.

## Formación de Recursos Humanos

El equipo está integrado por docentes/ investigadores que pertenecen a la cátedra de Auditoria y Seguridad Informática de la carrera de Ingeniería en Informática de la UNLaM, más otro docente/ investigador especializado en sistemas de control y una alumna de la carrera de Ingeniería en Informática que está haciendo sus primeras experiencias en proyectos de investigación.

Dos de los miembros del equipo de investigación se encuentran desarrollando su trabajo de tesis de posgrado de la Maestría en Informática de la UNLaM. Ambos están siendo tutoreados por el Mag. Jorge Eterovic, director del proyecto de investigación.

El presente trabajo se enfoca en un dominio tecnológico incipiente, por ende, es posible extender nuevas líneas de investigación y desarrollo para ampliar los alcances de nuestra propuesta a otros escenarios.

## Referencias

[1] Zárate Fraga, Marta. Análisis RAMS. Proyecto Fin de Carrera. Universidad Carlos III de Madrid; Febrero de 2012.

[2] CENELEC: Comité Européen de Normalisation Electrotechnique-. http://www.cenelec.eu.

[3] Norma EN 50126. Aplicaciones Ferroviarias. Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS). 2005.

[4] Norma EN 50128. Aplicaciones Ferroviarias. Sistemas de comunicaciones, señalización y procesamiento. Software para sistemas y protección del ferrocarril. 2012.

[5] Norma EN 50129. Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización. 2005.

[6] Mark Charlwood, Shane Turner and Nicola Worsell. A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines. Health and Safety Executive. 2004

[7] Brosseau, Jim. Software Quality Attributes: Following All the Steps, Clarrus Consulting Group Inc. Noviembre de 2010.

[8] Kitchenham, B., Lawrence, Pfleeger, S.L.: Software Quality: The Elusive Target, Software, IEEE (Volume:13, Issue: 1, pp. 12-21), Enero de 1996.
[9] Dromey, R.G.: Cornering the Chimera, Software, IEEE (Volume: 13, Issue: 1, pp. 33-43), Enero de 1996.
[10] Wallace, D. and Reeker L., Software Quality, in Guide to the Software Engineering Body of Knowledge SWEBOK, A. Abram and P. Bourque, Eds.: IEEE, pp. 165 – 184, 2001.
[11] Thomas E. Murphy, Nathan Wilson. Gartner: Magic Quadrant for Integrated Software Quality Suites. Julio de 2013.
[12] Norma IRAM-ISO 90003. Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software. 2004.
[13] Norma IRAM-ISO 9001. Sistemas de gestión de la calidad. Requisitos. 2008.