CORE
Metadata, citation and similar papers at core.ac.uk
Provided by El Servicio de Difusión de la Creación Intelectual

Desarrollo una metodología para estandarizar las auditorias del software para sistemas de control y protección del ferrocarril

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

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

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

Resumen

El software es un elemento clave en todos los sistemas que se utilizan actualmente en la gestión de las organizaciones, en particular los sistemas de control, incluidos los de seguridad crítica, tales como los de control y protección de las aplicaciones ferroviarias, en los que una falla puede causar daños irreparables a personas y/o al entorno. Ésta dependencia ha hecho que el nivel de fiabilidad requerido para este tipo de software sea muy alto.

La forma de conseguir un software de calidad suficiente es sometiéndolo a un proceso de auditoría y control en cada una de las etapas del ciclo de vida de su desarrollo, basado en una serie de normas y estándares reconocidos y utilizados internacionalmente.

El proyecto de investigación se propone el desarrollo de una metodología para estandarizar las auditorias del software para sistemas de control y protección del ferrocarril.

Palabras clave: Auditoria de software; sistemas de control del ferrocarril; sistemas de protección del ferrocarril.

Contexto

Este proyecto de investigación está inserto en el Programa CyTMA2 del Departamento de Ingeniería e Investigaciones 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 una metodología que sirva de base para el desarrollo las auditorias del software para sistemas de control y protección del ferrocarril.

Introducción

Luego del extracto planteado en el resumen, se desprende que los objetivos del presente trabajo están centrados esencialmente en identificar las diferentes normas y estándares internacionales que permitan compilar los requerimientos para auditar el ciclo de vida del desarrollo del software para uso en el ferrocarril. Estos serán considerados como requerimientos funcionales de los sistemas de control y protección del ferrocarril.

A continuación se realizará el análisis y selección de los puntos de control para diseñar la metodología para auditar los productos de software para sistemas de control y protección del ferrocarril.

Y finalmente se trabajará en el desarrollo de la propuesta para diseñar y documentar una metodología para auditar los sistemas de control y protección del ferrocarril.

La situación actual del sistema ferroviario argentino condiciona la necesidad de renovación de los componentes del mismo, incluyendo el material rodante y el software de control y protección del ferrocarril. En este contexto de cambio, es fundamental contar con un método que permita auditar los sistemas de software que vayan a adquirirse y/o desarrollarse localmente.

La metodología para estandarizar la auditoría proporcionará una serie de requisitos que se deben cumplir en el desarrollo, implantación y mantenimiento de cualquier software relacionado con la seguridad, destinado a aplicaciones de control y protección del ferrocarril.

En los alcances se definirán los requisitos relativos a la estructura organizativa, a la relación entre organizaciones y a la división de responsabilidades relativas a las actividades de desarrollo, implantación y mantenimiento. Deberá proporcionar además los criterios relativos a la calificación, experiencia y competencia del personal.

El concepto clave en esta metodología es el de los niveles de integridad de seguridad del software. En las normas se identifican cinco niveles de integridad de seguridad del software, siendo O 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 software.

En la metodología se deberán identificar técnicas y medidas para los cinco niveles de integridad de seguridad del software. Sin embargo, no se darán indicaciones sobre qué nivel de integridad de seguridad del software es apropiado para un riesgo determinado. Esta decisión dependerá de muchos factores, incluyendo la naturaleza de la aplicación, del grado en que otros sistemas llevan a cabo funciones de seguridad y de factores sociales y económicos.

Para el desarrollo se requiere que se adopte un enfoque sistemático para identificar peligros, evaluar riesgos y tomar decisiones en función de los criterios de riesgo; identificar la reducción de riesgo necesaria para cumplir con los criterios de aceptación de riesgos; definir una especificación de requisitos de seguridad del sistema global con las protecciones necesarias para conseguir la reducción de riesgo requerida; seleccionar una arquitectura del sistema adecuada y planificar,

supervisar y controlar las actividades técnicas y de gestión necesarias para convertir la especificación de requisitos de seguridad del sistema en un sistema relacionado con la seguridad con unas características validadas de integridad de seguridad.

A medida que se descompone la especificación en un diseño que incluye sistemas y componentes relacionados con la seguridad, se produce una nueva asignación de niveles de integridad de seguridad. Finalmente, se llega a los niveles de integridad de seguridad requeridos para el software.

El estado actual de la técnica es tal que ni la aplicación de métodos para garantizar la calidad (como las medidas para evitar y detectar errores) ni la aplicación de soluciones de software tolerante a errores, pueden garantizar la seguridad absoluta del sistema No hay manera conocida para demostrar la ausencia de errores en un software complejo relacionado con la seguridad, especialmente la ausencia de errores de especificación y diseño.

Por ello la auditoría deberá comprender los procedimientos y requisitos técnicos para el desarrollo de software para sistemas electrónicos programables para su uso en aplicaciones de control y protección del ferrocarril. Se podrá aplicar en cualquier área del ferrocarril que tenga relación con la seguridad. Además se debe tener en cuenta que estos sistemas pueden implementarse utilizando microprocesa-dores dedicados, controladores lógicos programables, sistemas multiprocesadores distribuidos, sistemas de procesador central de gran escala u otras arquitecturas.

La auditoría se aplicará al software y a la interacción entre el software y el sistema del que forma parte. Se debe tener presente que el software relacionado con la seguridad utilizado en sistemas de control y protección del ferrocarril incluye: la programación de aplicaciones, sistemas operativos, herramientas de soporte y el firmware.

La programación de aplicaciones comprende la programación de alto nivel, de bajo nivel y la programación de propósito específico (por ejemplo, la de un controlador lógico programable).

El desarrollo de este proyecto de investigación se considera asequible en cuanto a que no se requieren recursos extraordinarios, tanto tecnológicos como económicos, sino más bien, el estudio de las normas disponibles y el trabajo del desarrollo de una metodología para estandarizar las auditorias del software para sistemas de control y protección del ferrocarril.

Líneas de Investigación, Desarrollo e Innovación

El proyecto busca desarrollar una metodología que establezca un proceso de auditoría y control 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.

La investigación no se basará en la utilización de un ciclo de vida de desarrollo específico, pero sí establecerá puntos de control, validaciones, verificaciones, evaluaciones, criterios de aceptación y documentación como parte

del proceso de auditoría y control en el desarrollo de dichos productos de software, de manera de garantizar la calidad del mismo en las diferentes etapas del desarrollo, reduciendo los defectos y los riesgos.

El proceso de auditoria se aplicará desde la especificación de requisitos hasta la implantación del producto software, incluso durante la vida operativa del sistema y el mantenimiento del mismo.

Este proceso se aplicará a todo el ciclo de vida de desarrollo, considerando la aplicación de un plan de garantía de la calidad del software y la integridad de seguridad del software.

La metodología de investigación propuesta comprende las siguientes etapas:

- Desarrollar la Fundamentación de la Investigación.
- Establecer los Límites y el alcance del Proyecto de Investigación.
- Formular la hipótesis.
- Definir los lineamientos metodológicos.
- Establecer el contexto de la investigación.
- Plantear el Marco del estudio.
- Desarrollar las tareas necesarias para llegar desde el planteamiento del problema a la solución posible.
- Hacer la validación de la solución adoptada.
- Realizar las Reflexiones finales y analizar los futuros trabajos.
- Armar el informe final del trabajo y hacer la entrega del mismo.

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: Escribir una metodología que se pueda utilizar en auditorias de sistemas de control y protección del ferrocarril.

Resultados en cuanto a la formación de recursos humanos: Capacitación a personal de empresas ferroviarias que daban auditar software de aplicaciones ferroviarias y a alumnos universitarios que puedan desarrollar capacidades de colaboración en auditorias 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 la adopción de la normativa de respaldo a la metodología 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 de 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 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

- Norma EN 50128:2011. Aplicaciones Ferroviarias. Sistemas de comunicaciones, señalización y procesamiento. Software para sistemas y protección del ferrocarril.
- Norma EN 50126-1:1999. Aplicaciones Ferroviarias. Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS). Parte 1: Requisitos básicos y procesos genéricos.
- Norma EN 50129:2003. Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización.
- Norma EN ISO 9000. Sistemas de gestión de la calidad: Fundamentos y vocabulario. (ISO 9000:2005).
- Norma EN ISO 9001. Sistemas de gestión de la calidad. Requisitos (ISO 9001:2008).
- Norma ISO/IEC 90003:2004. Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software.
- Norma ISO/IEC 9126, serie Ingeniería del software. Calidad del producto software.