Universidad Nacional de La Matanza
Departamento de Ingeniería e Investigaciones Tecnológicas

Código del Proyecto de investigación: **C2 ING 018**

Título del Proyecto: **"Propuesta para desarrollar una metodología para estandarizar las auditorias de los productos de software para sistemas de control y protección de ferrocarriles".**

Programa de Investigación: **CyTMA2**

Director del Proyecto: **Jorge Eterovic**

Integrantes del Proyecto: **Domingo Donadello; Cintia Gioia; Pablo Pomar; Walter Ureta; Silvina Eterovic**.

Fecha de inicio: **2014/01/01**

Fecha de finalización: **2015/12/31**

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.

Debido a que el software no envejece ni se degrada con el tiempo, excepto en un cambio de la tecnología donde se procesa el mismo, la calidad de éste dependerá principalmente de los defectos que se introduzcan en las distintas etapas del ciclo de vida del desarrollo del sistema. Por lo tanto contar con una metodología que basada en normativa reconocida internacionalmente, permita auditar cada una de esas etapas del desarrollo, permitirá detectar errores de manera temprana, reduciendo los tiempos y los costos de proyecto y por consiguiente aumentar la calidad del producto.

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.

Se trabajará en una primera parte a partir de exploración bibliográfica para el estudio de las distintas normas internacionales que permitan enmarcar con actualidad el estado del conocimiento de las disciplinas del ámbito de esta investigación. Luego se procederá a desarrollar una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias para auditar los productos de software para sistemas de control y protección del ferrocarril.

Palabras Clave: **Verificación de la Calidad del Software; Calidad del Software; Software crítico; RAMS (Confiabilidad, Disponibilidad, Mantenibilidad y Seguridad).**

Área de Conocimiento: **Ciencias Tecnológicas**

Código de Área de Conocimiento: **33**

Disciplina: **Otras especialidades tecnológicas: Auditoria de software**

Código de Disciplina: **1899**

Campo de Aplicación: **Auditoria del Ciclo de vida de Desarrollo del Software**

Código de Campo de Aplicación: **3399**

Otras dependencias de la UNLaM que intervienen en el Proyecto: **Ninguna**

Otros proyectos con los que se relaciona: **Ninguno**

Propuesta para desarrollar una metodología para estandarizar las auditorias de los productos de software para sistemas de control y protección de ferrocarriles.

1. 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.

Debido a que el software no envejece ni se degrada con el tiempo, excepto en un cambio de la tecnología donde se procesa el mismo, la calidad de éste dependerá principalmente de los defectos que se introduzcan en las distintas etapas del ciclo de vida del desarrollo del sistema. Por lo tanto contar con una metodología que basada en normativa reconocida internacionalmente, permita auditar cada una de esas etapas del desarrollo, permitirá detectar errores de manera temprana, reduciendo los tiempos y los costos de proyecto y por consiguiente aumentar la calidad del producto.

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.

Se trabajará en una primera parte a partir de exploración bibliográfica para el estudio de las distintas normas internacionales que permitan enmarcar con actualidad el estado del conocimiento de las disciplinas del ámbito de esta investigación. Luego se procederá a desarrollar una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias para auditar los productos de software para sistemas de control y protección del ferrocarril.

Palabras Clave: Verificación de la Calidad del Software; Calidad del Software; Software crítico; RAMS (Confiabilidad, Disponibilidad, Mantenibilidad y Seguridad).

2. Desarrollo del Informe Final

2.1. Introducción

- **Selección del Tema**

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 Mantenibilidad.

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, representadas 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 la necesidad de mejora de 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].

- **Definición del Problema**

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.

Para reducir el riesgo, las organizaciones involucradas 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: "Calidad es la totalidad de las características del producto que influyen en la capacidad del producto para satisfacer las necesidades explicitas o implícitas" [9].

- **Justificación del Estudio**

En el marco del sistema que lo contiene, el software es una herramienta, y las herramientas tienen que ser seleccionadas 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 ese sistema. Por lo que podemos inferir que evaluar con la máxima objetividad las características de calidad deseadas, no es una tarea menor, y por ende, se le debe dedicar mucho esfuerzo.

Con la creciente sofisticación de los productos de software y su uso en áreas críticas como medicina, aeronavegación, sistemas de defensa militar, sistemas ferroviarios etc., se ha trabajado mucho en las actividades relacionadas con la evaluación de la calidad de los productos y artefactos de software [11].

El objetivo de este trabajo de investigación es desarrollar una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias para auditar los productos de software para sistemas de control y protección del ferrocarril basado en la aplicación de la norma IRAM-ISO 90003 [12], que da las directrices para la aplicación de la norma IRAM-ISO 9001 [13] para la calidad del software.

- **Limitaciones**

El proyecto busca desarrollar una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias que establezca un proceso de auditoría y control para cada una de las etapas del ciclo de vida de desarrollo del software para 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.

- **Alcance del Trabajo**

El proceso de auditoria se aplicará desde la especificación de requisitos hasta la implantación del producto software, incluso durante toda la vida operativa y en los distintos ciclos de mantenimiento del sistema de control y protección del ferrocarril en que se encuentre instalado.

El proceso de auditoria 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 mismo.

- **Objetivo**

El objetivo de este trabajo de investigación es desarrollar una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias basado en la aplicación de la norma IRAM-ISO 90003 [12], que da las directrices para la aplicación de la norma IRAM-ISO 9001 [13] para la calidad del software.

- **Hipótesis**

La situación actual del sistema ferroviario argentino condiciona la necesidad de renovación de los componentes del mismo, incluyendo material rodante y software de control y protección del ferrocarril. En este contexto de cambio, es fundamental contar con una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias que permita auditar los sistemas de software que vayan a adquirirse y/o desarrollarse.

2.2. Desarrollo

- **Material y Métodos**

De acuerdo al GANTT informado en el Protocolo de presentación del Proyecto:

Actividades / Responsables 1er. Año	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Mes 7**	**Mes 8**	**Mes 9**	**Mes 10**	**Mes 11**	**Mes 12**
1. Fundamentación de la Investigación												
2. Límites y alcance												
3. Formulación de la hipótesis												
4. Lineamientos metodológicos												
5. Contexto de la investigación												
Actividades / Responsables 2do. Año	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**	**Mes 7**	**Mes 8**	**Mes 9**	**Mes 10**	**Mes 11**	**Mes 12**
6. Marco del estudio												
7. Del problema a la solución posible												
8. Validación												
9. Reflexiones finales y futuros trabajos												
10. Armado del trabajo y entrega												

La metodología de investigación comprende las siguientes etapas:

1) Desarrollar la Fundamentación de la Investigación
2) Establecer los Límites y el alcance del Proyecto de Investigación
3) Formular la hipótesis
4) Definir los Lineamientos metodológicos
5) Establecer el Contexto de la investigación
6) Plantear el Marco del estudio
7) Desarrollar las tareas necesarias para llegar desde el planteamiento del problema a la solución posible

8) Hacer la Validación de la solución adoptada
9) Realizar las Reflexiones finales y analizar los futuros trabajos
10) Armar el trabajo y hacer la entrega final del mismo

- **Lugar y Tiempo de la Investigación**

El trabajo de investigación se desarrollará en la UNLaM - Laboratorio Pramin y el tiempo de desarrollo del proyecto fue de 2 (dos) años. Las tareas se llevaron a cabo en base al GANTT descripto en el punto anterior.

- **Descripción del Objeto de Estudio**

Las normas proporcionan una serie de requisitos que se deben cumplir en las fases de desarrollo, implantación y mantenimiento del software crítico destinado a aplicaciones de control y protección de ferrocarriles. Se definen 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. Se proporcionan además los criterios relativos a la calificación, experiencia y competencia del personal.

El concepto clave es el de los niveles de integridad de seguridad del software (SIL). Se identifican cinco niveles de integridad de seguridad del software, 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. Se deben identificar técnicas y medidas para los cinco niveles de integridad de seguridad del software.

En el desarrollo de este trabajo se muestran las técnicas y medidas requeridas para los niveles 0 a 4 de integridad de seguridad del software. Las técnicas requeridas para el nivel 1 son las mismas que para el nivel 2 y las técnicas requeridas para el nivel 3 son las mismas que para el nivel 4. Lo qué no se puede indicar es 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.

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.

De todos modos, 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 razonablemente complejo, especialmente la ausencia de errores de especificación y diseño.

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 del Software, cuyo objetivo es identificar, supervisar y controlar toda actividad, tanto técnica como de gestión, necesaria para garantizar que el software alcanza la calidad requerida.

Esto es necesario para proporcionar la defensa cualitativa necesaria contra errores sistemáticos y para garantizar que se puede establecer una pista de auditoría que permita realizar las actividades de verificación y validación de forma efectiva.

Para ello, las organizaciones involucradas en el desarrollo del software deben implementar y usar un Sistema de Garantía de Calidad conforme con la Norma IRAM-ISO 9000 [14]. Para satisfacer los requisitos de esta norma es altamente recomendable la certificación de conformidad con la Norma IRAM-ISO 9001.

Se debe redactar un Plan de Garantía de Calidad del Software, donde se deberán 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;
    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 seleccionadas 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, como en un Plan de Gestión de la Configuración del Software, en un Plan de Mantenimiento, en un Plan de Verificación del Software y en un Plan de Validación del Software.

Los puntos del Plan de Garantía de Calidad del Software deben proporcionar la referencia de los documentos en los que aparece la información. En cualquier caso, se debe especificar el contenido de cada punto del Plan de Garantía de Calidad del Software, ya sea directamente o mediante referencia a otro documento.

Finalmente se debe redactar un Informe de Verificación de la Garantía de Calidad del Software, pudiéndose usar como base la Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias que se desarrolla en este trabajo.

Ciclo de vida del sistema

El ciclo de vida del sistema es una secuencia de fases, cada una de las cuales contiene tareas que abarcan la vida completa de un sistema desde su concepto inicial hasta la retirada del servicio y la eliminación.

El ciclo de vida proporciona una estructura para la planificación, la gestión, el control y la supervisión de todos los aspectos de un sistema, incluida la RAMS, a medida que el sistema avanza a través de sus fases, con el fin de entregar el producto adecuado al precio correcto dentro del plazo acordado.

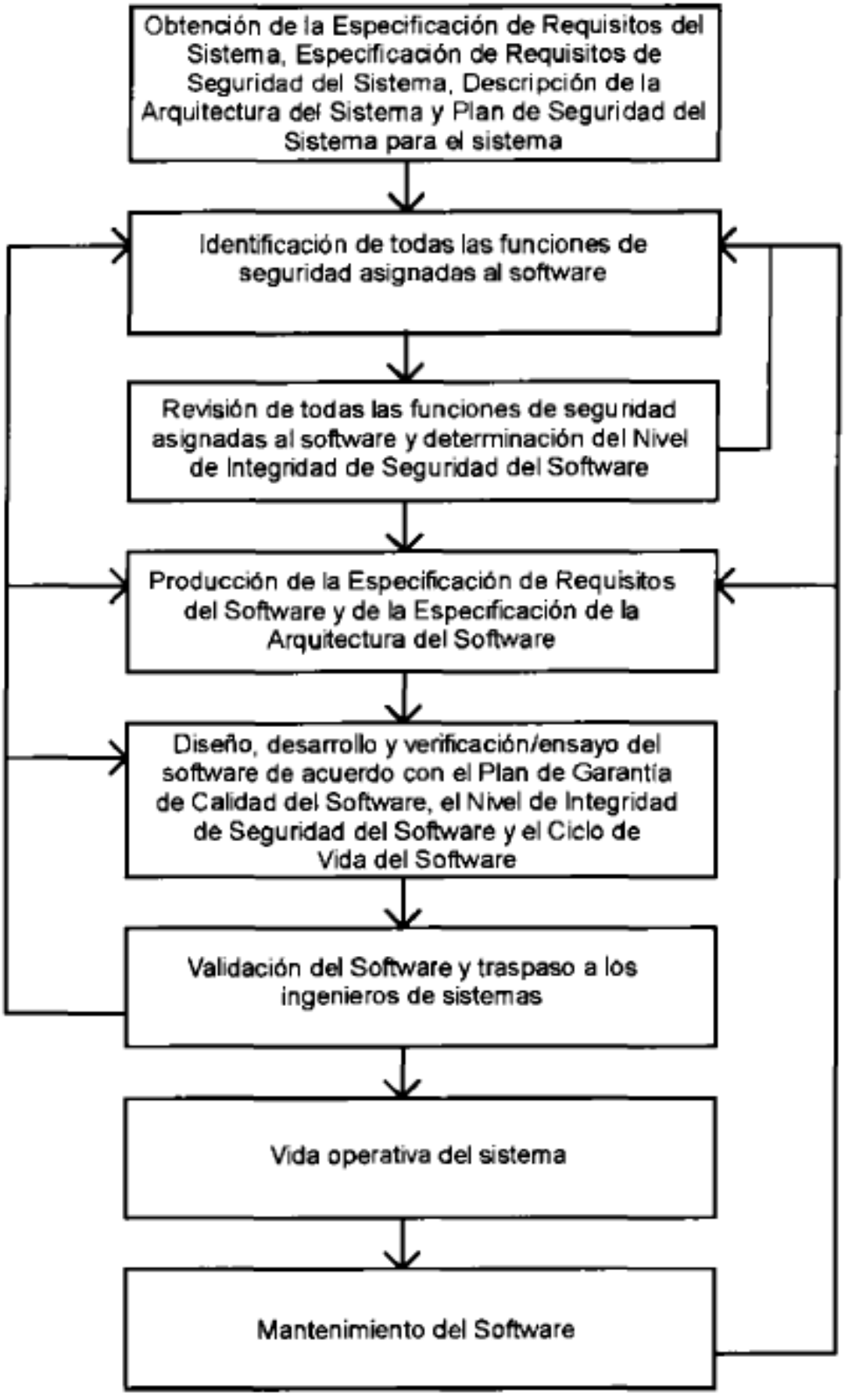


Figura 1- Etapas funcionales

Un ciclo de vida de un sistema, adecuado en el contexto de una aplicación ferroviaria, se muestra en la figura 2.

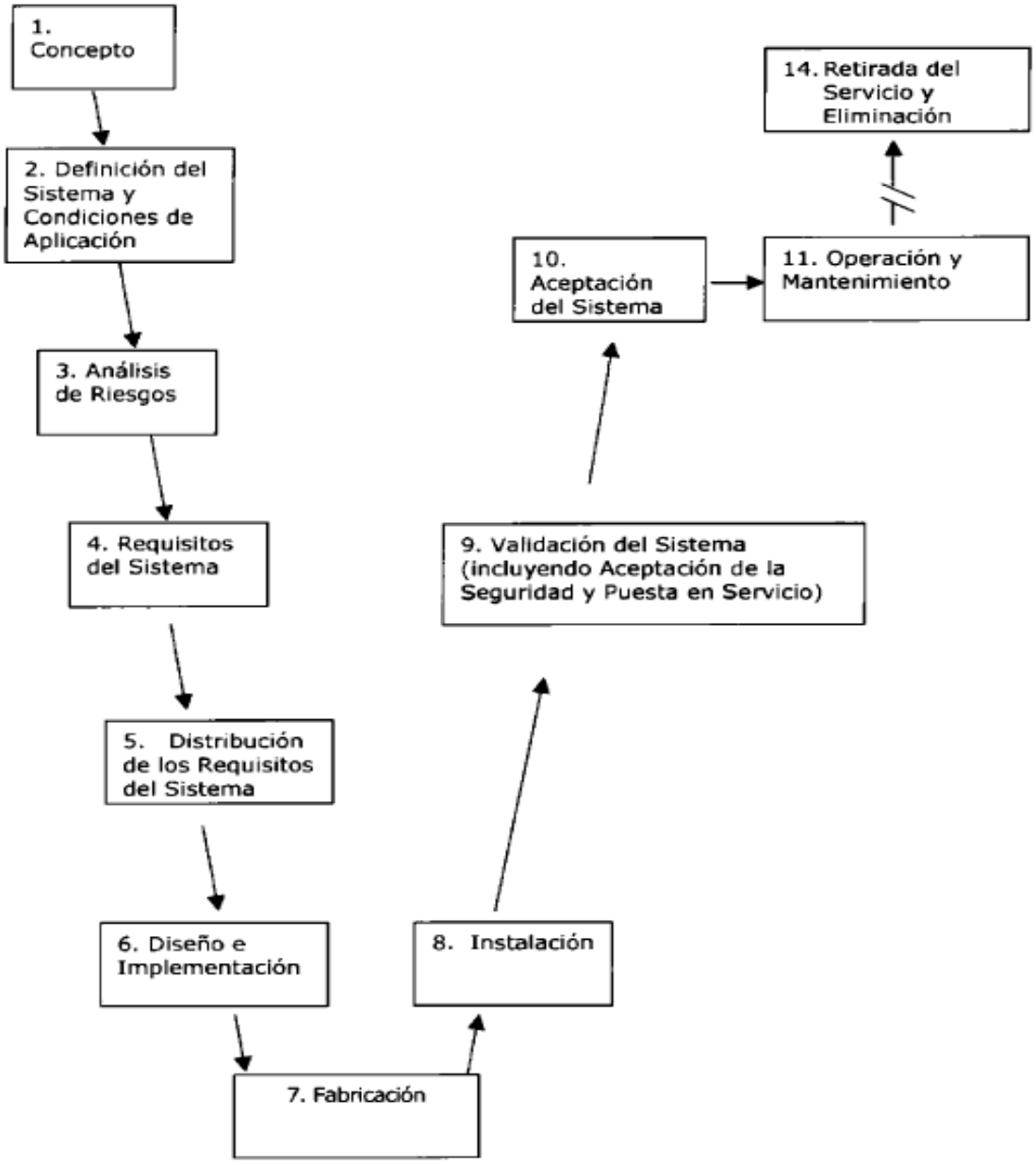


Figura 2 – Ciclo de vida (representación en V)

La figura 2 representa el ciclo de vida del sistema en el modelo en “V”, donde la rama descendente (lado izquierdo) se llama generalmente Desarrollo y consiste en un proceso de perfeccionamiento que finaliza con la fabricación de componentes del sistema. La rama ascendente (lado derecho) está relacionada con el montaje, la instalación, la recepción y el funcionamiento de todo el sistema.

La representación en “V” supone que las actividades de aceptación están intrínsecamente vinculadas a las actividades de desarrollo, dado que lo que es realmente diseñado tiene que ser finalmente comprobado en relación con los requisitos.

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 3.

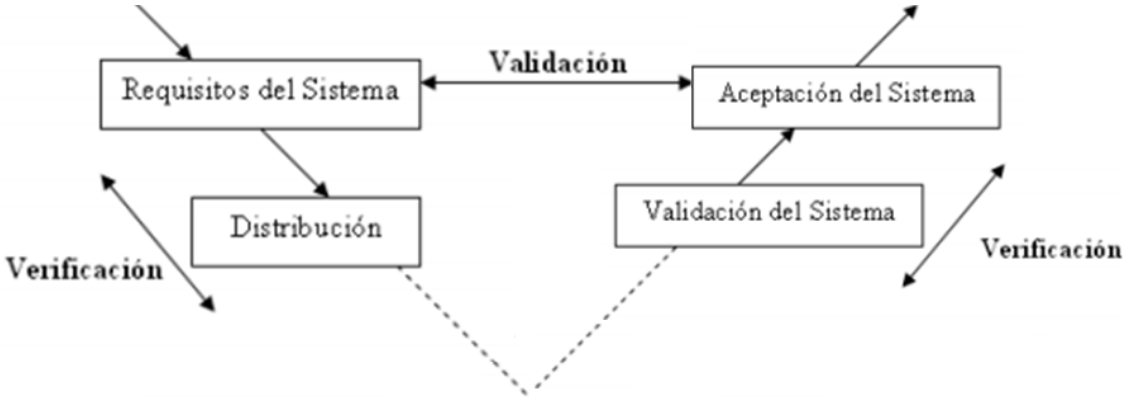


Figura 3 - Validaciones

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 entregas 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 sus requisitos en todos los aspectos.

Las tareas de verificación están incluidas dentro de cada fase del ciclo de vida. Si buscamos el aseguramiento del sistema en el contexto RAMS, las tareas de verificación y validación forman parte integral de la demostración global de aseguramiento de los sistemas.

- **Diseño de la Investigación**

Para la realización de estas tareas se debe definir el Rol “Validador”, cuyas responsabilidades serán:

1) debe desarrollar una comprensión del sistema de software dentro del entorno previsto de aplicación;
2) debe desarrollar un plan de validación y especificar las tareas y actividades esenciales para la validación del software y ponerse de acuerdo sobre este plan con el evaluador;
3) debe revisar los requisitos del software en relación a su uso/entorno previsto;
4) debe revisar el software en relación a los requisitos del software de forma que se garantice que se cumplen todos ellos;
5) debe evaluar la conformidad del proceso del software y del software desarrollado en relación a los requisitos de la normativa incluyendo el SIL asignado;
6) debe revisar la corrección, coherencia y adecuación de la verificación y de los ensayos;
7) debe comprobar la corrección, coherencia y adecuación de los casos de ensayo y de los ensayos realizados;
8) debe garantizar que se realizan todas las actividades del plan de validación;
9) debe revisar y clasificar todas las desviaciones en términos de riesgo (impacto), registrarlas y comunicarlas al organismo competente de la gestión de las modificaciones para su evaluación y toma de decisiones;
10) debe proporcionar una recomendación sobre la idoneidad del software para su uso previsto e indicar cualquier restricción de la aplicación según sea apropiado;
11) debe registrar las desviaciones a partir del plan de validación;
12) debe realizar auditorías, inspecciones o revisiones del proyecto global (como instancias del proceso de desarrollo genérico) según sea apropiado, en varias fases del desarrollo;
13) debe revisar y analizar los informes de validación relativos a aplicaciones previas según sea apropiado;
14) debe revisar si las soluciones desarrolladas son trazables hasta los requisitos del software;
15) debe garantizar que se revisan los registros de situaciones peligrosas asociadas y los casos de no conformidad y que se resuelven todas las situaciones peligrosas de manera adecuada, ya sea mediante medidas que las eliminen o con medidas de control/transferencia de los riesgos;
16) debe desarrollar un informe de validación y
17) debe expresar su acuerdo/desacuerdo sobre la versión del software publicada

- **Instrumentos de Recolección y Medición de Datos**

Para cada fase de este ciclo de vida, se han definido las principales tareas a ser auditadas. Se resumen en la siguiente tabla (figura 4):

Fase del ciclo de vida	**Tareas a ser auditadas**
1. Concepto	Ámbito y propósito del proyecto Ferroviario. Definición del concepto del proyecto ferroviario. Análisis Financiero y estudios de viabilidad. Existencia del equipo de gestión. Las implicaciones de seguridad del proyecto. La política y objetivos de la seguridad.
2. Definición del sistema y condiciones de aplicación	El perfil de la misión del sistema. La descripción del sistema. La estrategia de Operación y Mantenimiento. Las condiciones de operación y mantenimiento. La influencia de las restricciones de la infraestructura existente. El análisis preliminar de las amenazas. El plan de seguridad. Definición de las condiciones de operación y mantenimiento a largo plazo. Identificar la influencia en RAM de las restricciones en la infraestructura existente.
3. Análisis de riesgos	El Análisis de riesgos relacionado con el proyecto. El análisis amenazas y riesgos de la seguridad del sistema. El registro de las amenazas. La evaluación de riesgos.
4. Requisitos del Sistema	El análisis de requisitos. Especificaciones del sistema. Especificación el entorno. Los criterios de Demostración y Aceptación del sistema. El plan de Validación. Los requisitos de Gestión, Calidad y Organización. El procedimiento de control de cambios. Los requisitos de Seguridad del Sistema. Los criterios de aceptación de la Seguridad. Los requisitos relacionados con la segundad Funcional. La Gestión de Seguridad.
5. Distribución de los Requisitos del Sistema	Especificación de los requisitos de los subsistemas y componentes. Especificación de los criterios de aceptación de subsistemas y componentes. Los requisitos de seguridad de los subsistemas y componentes. Los criterios de aceptación de seguridad de los subsistemas y componentes. El Plan de Seguridad del Sistema.
6. Diseño e implementación	La planificación. El Diseño y desarrollo. El análisis del diseño y pruebas. La Verificación del diseño- La implementación y validación. El diseño de los recursos de apoyo logísticos.

	El Registro de amenazas. El Análisis de amenazas y evaluación de riesgos. La Gestión de la Seguridad. El Control de subcontratos y proveedores. Un Caso de Seguridad.
7. Producción	El plan de producción. La fabricación de código. La fabricación y prueba del montaje de componentes. La documentación. La capacitación. La implementación del plan de seguridad. El uso del registro de amenazas.
8. Instalación	El montaje del sistema La instalación del sistema. El programa de instalación. La implementación del programa de instalación.
9. Validación del sistema	La puesta en servicio. El período de pruebas de operación. La capacitación. El programa de puesta en servicio. La implementación del programa de puesta en servicio. El Caso de Seguridad específico de la aplicación.
10. Aceptación del sistema	Los procedimientos de aceptación, basados en criterios de aceptación. La recopilación de las pruebas para la aceptación. La entrada en servicio. El periodo de pruebas de operación. El Caso de Seguridad específico de la aplicación.
11. Operación y mantenimiento	La operación del sistema a largo plazo. El mantenimiento. La capacitación en el mantenimiento centrado en segundad. El control de la ejecución de segundad y mantenimiento del registro de las amenazas.
12. Supervisión de la ejecución	La recopilación estadística de la ejecución operacional. La adquisición, el análisis y la evaluación de los datos. La recopilación, el análisis, la evaluación el uso de las estadísticas de Seguridad y ejecución.
13. Modificación y realimentación	Los procedimientos de cambio de requisitos. Los procedimientos de modificación y realimentación. Las implicaciones de Seguridad para la modificación y realimentación.
14. Retirada de servicio y eliminación	El plan de retirada de servicio y eliminación. La retirada de servicio. La eliminación. El plan de Seguridad. El análisis de amenazas y la evaluación de riesgos. La implementación del plan de Seguridad.

Figura 4 – Tareas a auditar

Además de lo expresado, en todas las fases se deberían auditar las siguientes tareas:

1) Control de Cambios

2) Gestión de la Configuración
3) Verificación y Validación
4) Análisis de riesgos

Los procesos del sistema de gestión se deben evaluar de acuerdo a la norma IRAM-ISO 9000, teniendo que considerar los siguientes temas:

1) Identificación y comunicación de los requisitos del cliente;
2) Identificación de la vinculación (secuencia e interrelación) con otros procesos;
3) Identificación de los objetivos del proceso;
4) Definición de responsabilidad y autoridad;
5) Competencia del personal;
6) Adecuación de recursos y ambiente de trabajo;
7) Adecuación de la documentación que describe las prácticas de operación;
8) Seguimiento del desempeño del proceso y control de no conformidades;
9) Aplicación de acciones correctivas y preventivas;
10) Evidencia de mejora continua;
11) Disponibilidad de registros;
12) Divulgación de la certificación. Uso de logos. (Aplica sólo en auditorías de seguimiento o recertificación) y
13) Gestión del cumplimiento de requisitos legales del producto.

Si bien las normas CENELEC nos permiten identificar los requerimientos para la verificación de la calidad del software crítico en sistemas ferroviarios de manera que en la norma EN 50126 se define el ciclo de vida, en la norma EN 50128 las técnicas de software y en la EN 50129 las técnicas de hardware, podríamos plantear un requisito para cada nivel de integridad de seguridad del software (SIL) para cada técnica o medida de la Garantía de la Calidad del Software en función del Nivel de Integridad de la Seguridad (SIL) de la siguiente manera:

Donde los requisitos para los niveles de integridad de seguridad del software 1 y 2 son los mismos para cada técnica. Del mismo modo, cada técnica tiene los mismos requisitos en los niveles de integridad de seguridad del software 3 y 4. Estos requisitos pueden ser:

- M: mandatorio;
- AR: altamente recomendable:
- R: recomendable

Técnica/Medida	SIL O	SIL 1	SIL 2	SIL3	SIL4
Acreditada según la Norma ISO 9001	R	AR	AR	AR	AR
Conforme con la Norma ISO 9001	M	M	M	M	M
Conforme con la Norma ISO/IEC 90003	R	R	R	R	R
Sistema de Calidad de la Compañía	M	M	M	M	M
Gestión de la Configuración del Software	M	M	M	M	M
Listas de Comprobación	R	AR	AR	AR	AR
Trazabilidad	R	AR	AR	M	M
Registro y Análisis de Datos	AR	AR	AR	M	M

La combinación de técnicas o medidas se deberán incluir en el Plan de Garantía de Calidad del Software.

- **Métodos de Análisis Estadísticos**

A lo largo del proyecto no se han utilizado métodos de análisis estadísticos.

- **Resultados**

Se ha desarrollado una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias. La misma tiene la finalidad de ser un Referencial en la especificación y demostración de la confiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS) según lo establecido en la norma UNE-EN 50126.

A continuación se desarrolla la Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias que se debería implementar en las auditorias del software:

LISTA DE VERIFICACIÓN PARA LA AUDITORÍA

Aplicaciones Ferroviarias

REFERENCIAL

Especificación y demostración de la confiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS) UNE-EN 50126

ORGANIZACIÓN:	
REFERENCIAL:	**UNE-EN 50126**
TIPO DE AUDITORÍA:	**1. REVISIÓN DOCUMENTAL** **2. CERTIFICACIÓN**
FECHAS DE AUDITORÍA:	
AUDITOR:	

ANÁLISIS DE DOCUMENTACIÓN

Manual del Sistema RAMS

Verificar:

- ✓ Alcance del sistema de gestión de la RAMS, incluyendo los detalles y la justificación de cualquier exclusión del alcance.
- ✓ Los procedimientos documentados establecidos para el sistema de gestión de la RAMS, o referencia a los mismos.
- ✓ Una descripción de la interacción de los procesos del sistema de gestión de la RAMS.

Hallazgos:

ENTREVISTA CON LA CONDUCCIÓN DEL PROYECTO RAMS

Temas a considerar:

- ✓ Los elementos RAMS (confiabilidad, disponibilidad, mantenibilidad y seguridad) en el contexto de los sistemas ferroviarios.
- ✓ Gestión de fallas y defectos y modos de funcionamiento
- ✓ Los conceptos técnicos de seguridad
- ✓ Efectos de los fallos
- ✓ Factores que influyen en la RAMS Ferroviaria
- ✓ Categorías de los factores
- ✓ Gestión de factores
- ✓ Medios para alcanzar los requisitos de la RAMS Ferroviaria – evaluación y tipificación de fallas
- ✓ Riesgos – conceptos de riesgos – análisis de riesgos – frecuencia de riesgos
- ✓ Evaluación y aceptación de riesgos- categorías cualitativas de riesgos

Hallazgos:

ENTREVISTA CON EL RESPONSABLE DE LA GESTIÓN DEL PROYECTO RAMS

Temas a considerar:

- ✓ Proceso de gestión: requisitos, control de peligros, planificación y tareas del RAMS, cumplimiento de requisitos, supervisión cumplimiento de requisitos en el ciclo de vida
- ✓ Ciclo de vida del sistema, tareas generales y RAMS relacionadas con el proyecto
- ✓ Requisitos obligatorios: responsabilidad, competencia, gestión de conflictos, soporte y uso del ISO 90003, Métodos, herramientas y técnicas utilizadas.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 1: Concepto

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Alcance, contexto y finalidad;
  - ✓ Entorno del sistema; Implicaciones generales RAMS para el sistema.
  - ✓ Implicaciones RAMS para cualquier análisis financiero y estudio de viabilidad del sistema.
  - ✓ Fuentes de Peligro: interacción con otros sistemas y con seres humanos.
  - ✓ Anteriores requisitos y rendimiento RAMS en sistemas similares;
  - ✓ Política y los Objetivos de seguridad actuales de la Autoridad Ferroviaria; Legislación en materia de seguridad.
  - ✓ Alcance de los requisitos de gestión para sucesivas tareas RAMS del ciclo de vida del sistema.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados: las entregas deben incluir una estructura de gestión adecuada para poner en práctica los requisitos RAMS correspondientes a las fases 2, 3 y 4 del ciclo de vida
- ✓ Verificación:
  - ✓ Idoneidad de la información para tareas RAMS dentro de esta fase.
  - ✓ Idoneidad de la declaración de entorno del sistema.
  - ✓ Integridad de la relación de fuentes de peligros.
  - ✓ Idoneidad de los métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 2: Definición del Sistema

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Perfil de la misión del sistema;
  - ✓ Entorno;
  - ✓ Alcance de las condiciones de aplicación;
  - ✓ Alcance del análisis de peligros del sistema.
  - ✓ Análisis preliminar RAM para apoyar objetivos;
  - ✓ Identificar subsistemas asociados a peligros y tipos de acontecimientos asociados con accidentes;
  - ✓ Definir criterios iniciales de tolerabilidad de riesgos.
  - ✓ Política general del RAMS.
  - ✓ Plan de seguridad del sistema.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados.
  - ✓ Política de Seguridad.
  - ✓ Plan de Seguridad del sistema.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Consistencia con la entrega de la fase 1.
  - ✓ Integridad del proceso de análisis RAM y de identificación de peligros.
  - ✓ Evaluación del Plan de Seguridad.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 3: Análisis de Riesgos

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Identificar y priorizar peligros asociados al entorno de aplicación (por uso incorrecto, por defectos, por factores humanos, etc.);
  - ✓ Identificar secuencias de acontecimientos que conducen a peligros;
  - ✓ Evaluar frecuencia con que sucede cada peligro;
  - ✓ Evaluar probable gravedad de las consecuencias de cada peligro;
  - ✓ Evaluar riesgo que supone cada peligro para el sistema.
  - ✓ Determinar y clasificar la aceptabilidad del riesgo asociado a cada peligro.
  - ✓ Establecer un Registro de Peligros.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados.
  - ✓ Análisis de riesgos recogidos en el Registro de Peligros.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Consistencia con la entrega de la fase 2.
  - ✓ Integridad de la gestión de riesgos.
  - ✓ Clasificación de la aceptabilidad de los riesgos.
  - ✓ Idoneidad la idoneidad del proceso del Registro de Peligros.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 4: Requisitos del Sistema

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Requisitos globales: Definición y límites del sistema; Perfil de la misión; Requisitos funcionales, de rendimiento, de seguridad; Requisitos de integridad de la seguridad para cada función de seguridad; Requisitos de apoyo logístico; Interfaces; Niveles tolerables de riesgo; Medidas externas necesarias para cumplir los requisitos; Requisitos de soporte; Límites del análisis.
  - ✓ Especificación de requisitos globales: Criterios de aceptación; Plan de validación del sistema RAMS.
  - ✓ Programa detallado RAM correspondiente a las restantes tareas del ciclo de vida, debe acordarse por la Autoridad Ferroviaria y la industria ferroviaria: Gestión; Confiabilidad; Mantenibilidad; Disponibilidad.
  - ✓ Corrección del Plan de Seguridad para garantizar que todas las tareas futuras planeadas sean coherentes con los requisitos emergentes RAMS del sistema.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Plan de Seguridad y Plan de Aceptación actualizados.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Consistencia con las entregas de las fases 2y 3.
  - ✓ Requisitos de Seguridad comparados con los objetivos y políticas RAM de la Autoridad Ferroviaria
  - ✓ Requisitos RAM comparados con los objetivos y políticas RAM de la Autoridad Ferroviaria
  - ✓ Idoneidad e integridad del Plan de Aceptación y del Plan de Validación
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 5: Distribución de los Requisitos

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Asignar requisitos funcionales a los subsistemas, componentes y equipos externos; Asignar los requisitos de seguridad a los subsistemas, componentes y equipos externos de reducción de riesgos; especificar los subsistemas, componentes y equipos externos;
  - ✓ Examinar programa RAM.
  - ✓ Especificar los requisitos para cumplir los requisitos, criterios de aceptación, demostración y aceptación de procesos y procedimientos de los subsistemas, componentes y equipos externos.
  - ✓ Examinar y actualizar el Plan de Seguridad y el Plan de Validación.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados, incluyendo requisitos de los sistemas asignados a los subsistemas, componentes y equipos externos designados.
  - ✓ Plan de Seguridad actualizado.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Consistencia con las entregas de las fase 4.
  - ✓ Arquitectura.
  - ✓ Trazabilidad de requisitos RAMS correspondientes a subsistemas, componentes y equipos externos, con los requisitos RAMS del sistema.
  - ✓ Integridad y coherencia entre funciones.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 6: Diseño e Implementación

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Diseñar subsistemas y componentes.
  - ✓ Llevar a cabo el diseño de subsistemas y componentes.
  - ✓ Planificar futuras tareas del ciclo de vida: Instalación; Puesta en servicio; Operación y mantenimiento; Adquisición y evaluación de datos durante el funcionamiento.
  - ✓ Definir, verificar y establecer un proceso de fabricación capaz de producir subsistemas y componentes validados por la RAMS.
  - ✓ Desarrollar Caso de Seguridad genérico.
  - ✓ Desarrollar Caso de Seguridad de aplicación.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados;
  - ✓ Registro de tareas de validación;
  - ✓ Planes de futuras tareas del ciclo de vida;
  - ✓ Procedimientos de funcionamiento y mantenimiento;
  - ✓ Caso de Seguridad genérico;
  - ✓ Caso de Seguridad de aplicación.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Consistencia con las entregas de las fases 4 y 5.
  - ✓ Diseño de subsistemas y componentes.
  - ✓ Consistencia de la realización de los subsistemas y componentes con el diseño.
  - ✓ Conformidad de la realización de los subsistemas y componentes con los criterios de aceptación RAMS.
  - ✓ Capacidad de los procesos de fabricación para producir subsistemas y componentes validados por la RAMS.
  - ✓ Coherencia de planes para futuras actividades con los requisitos RAMS.
  - ✓ Idoneidad e integridad del caso genérico de seguridad, y, de corresponder, del caso de seguridad de aplicación.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.
  - ✓ Aplicabilidad de plan de validación.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 7: Fabricación

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Verificar y aplicar el proceso de fabricación.
  - ✓ Establecer planes de apoyo para subsistemas y componentes: documentación, procedimientos y material de formación.
  - ✓ Planificar la fabricación para que cumpla los requisitos;
  - ✓ Aplicar la fabricación;
  - ✓ Poner en práctica la garantía de los procesos RAMS a fin de evitar potenciales modos de fallo.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Registro de las tareas de validación RAMS emprendidas durante la fase.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Adecuación y coherencia de la documentación de apoyo RAMS.
  - ✓ Conformidad de los productos fabricados con los requisitos del sistema.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 8: Instalación

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Instalación del sistema completo, de acuerdo con el Plan de Instalación.
  - ✓ Documentar el proceso de instalación.
  - ✓ Examinar y actualizar el Plan de Seguridad.
  - ✓ Formación del personal;
  - ✓ Disponibilidad de los procedimientos de apoyo;
  - ✓ Establecer el aprovisionamiento de piezas de repuesto y de herramientas.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Registro de las tareas de validación RAMS emprendidas,
  - ✓ Plan de Seguridad actualizado.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Concordancia de la instalación con el Plan de Instalación.
  - ✓ Aplicabilidad del Plan de Seguridad
  - ✓ Conformidad de los sistemas instalados con los requisitos RAMS.
  - ✓ Eficacia de los planes de apoyo del sistema.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 9: Validación del Sistema

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Ejecutar el Plan de validación y registrar el proceso.
  - ✓ Ejecutar el Plan de puesta en servicio y registrar el proceso;
  - ✓ Si es necesario establecer un período de funcionamiento a prueba.
  - ✓ Elaborar un Caso de seguridad (solo si no se ha elaborado en la fase 6)
  - ✓ Adquisición y evaluación de datos operativos como información aportada a un proceso de mejora del sistema.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Tareas de validación RAMS registradas,
  - ✓ Un Caso de Seguridad Específico de la Aplicación para el sistema dentro de esta fase
  - ✓ Registro de todas las tareas de Aceptación.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Verificación y validación, de que el sistema instalado cumpla los requisitos RAMS.
  - ✓ Verificación de que la puesta en servicio se conforma con el Plan de Puesta en Servicio.
  - ✓ Idoneidad y eficacia del sistema de recogida de datos operativos.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 10: Aceptación del Sistema

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Evaluar todas las tareas de verificación y validación del sistema.
  - ✓ Si corresponde, aceptar formalmente el sistema para su entrada en servicio.
  - ✓ Examinar y actualizar el Registro de Peligros.
  - ✓ Adquisición y evaluación de datos operativos como información aportada a un proceso de mejora del sistema.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Tareas de aceptación registradas
  - ✓ Registro de Peligros actualizado.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Aceptación, mediante análisis y pruebas, de que el sistema cumpla los requisitos RAMS.
  - ✓ Verificación que la aceptación se conforma con el Plan de aceptación.
  - ✓ Evaluación de la ininterrumpida aplicabilidad del plan de seguridad revisado.
  - ✓ Garantizar la gestión de cualquier peligro residual.
  - ✓ Idoneidad e integridad del caso de seguridad específico de la aplicación.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 11: Funcionamiento y Mantenimiento

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Supervisar la puesta en práctica del sistema (aplicación de procedimientos de funcionamiento y mantenimiento).
  - ✓ Garantizar cumplimiento de requisitos RAMS: examen y actualización de los procedimientos de funcionamiento y mantenimiento, del Registro de Peligros y del Caso de Seguridad;
  - ✓ Examen de la documentación de formación del sistema;
  - ✓ Apoyo logístico (repuestos, herramientas, calibración, etc.);
  - ✓ Mantenimiento del Sistema de comunicación de Fallos y Medidas Correctoras (FRACAS).
- ✓ Entregas:
  - ✓ Registro de todas las tareas de seguimiento del rendimiento emprendidas durante la fase, junto con las suposiciones y justificaciones realizadas durante la fase.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Coherencia de los cambios introducidos en los planes de apoyo con los requisitos RAMS y con los de coste del ciclo de vida.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 12: Seguimiento de la Ejecución

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Establecer, aplicar y examinar regularmente un proceso para: recoger estadísticas de rendimiento operativo y RAMS;
  - ✓ Análisis y evaluación de datos de rendimiento y RAMS;
  - ✓ Comprobar validez del caso de seguridad.
  - ✓ Analizar los datos del rendimiento y la RAMS para influir en: nuevos procedimientos de funcionamiento y mantenimiento;
  - ✓ Cambios en el apoyo logístico del sistema.
- ✓ Entregas:
  - ✓ Registro de todas las tareas de seguimiento del rendimiento emprendidas durante la fase, junto con las suposiciones y justificaciones realizadas durante la fase.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Coherencia de los cambios introducidos en los planes de apoyo con los requisitos RAMS y con los de coste del ciclo de vida.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 13: Modificación y Retroalimentación

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Establecer un plan de seguridad.
  - ✓ Establecer, aplicar y examinar regularmente un proceso destinado a controlar la modificación y realimentación del sistema, en el contexto RAMS.
- ✓ Entregas:
  - ✓ Sistema modificado y validado,
  - ✓ Resultados de la fase documentados,
  - ✓ Registro de Peligros actualizado,
  - ✓ Plan de Seguridad para hacer frente a las tareas de retirada del servicio y eliminación,
  - ✓ Caso de Seguridad de la Aplicación actualizado.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Idoneidad de cualquier documentación correspondiente a sistemas afectados por las actividades de retirada del servicio y eliminación.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LA ESTRUCTURA DEL SISTEMA RAMS

Procesos. Fase 14: Retirada de Servicio y Eliminación

- ✓ Objetivos
- ✓ Entradas
- ✓ Requisitos:
  - ✓ Establecer el impacto de la retirada del servicio y la eliminación sobre cualquier sistema o equipo externo asociado con el sistema que vaya a ser retirado del servicio;
  - ✓ Planificar la retirada del servicio.
  - ✓ Facilitar un análisis del rendimiento del ciclo de vida RAMS para transmitir dicha información, incluido el cálculo de costes del ciclo de vida, a futuros sistemas.
- ✓ Entregas:
  - ✓ Resultados de la fase documentados,
  - ✓ Registro de todas las tareas de retirada del servicio y eliminación emprendidas dentro de la fase.
  - ✓ Registro de Peligros actualizado.
  - ✓ Plan de Seguridad para hacer frente a las tareas de retirada del servicio y eliminación,
  - ✓ Caso de Seguridad de la Aplicación revisado.
- ✓ Verificación:
  - ✓ Idoneidad de la información.
  - ✓ Idoneidad de cualquier documentación correspondiente a sistemas afectados por las actividades de retirada del servicio y eliminación.
  - ✓ Idoneidad de métodos, herramientas y técnicas utilizadas.
  - ✓ Competencia del personal.

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE CONVOCATORIA DE LICITACIÓN

Temas a considerar:

- ✓ Realizar un análisis preliminar RAMS (caso peor).
- ✓ Distribución de los requisitos RAMS del sistema (Subsistemas / equipos, otros sistemas relevantes, etc.).
- ✓ Realizar un análisis de peligros y seguridad del sistema.
- ✓ Realizar análisis de riesgos relacionados con RAM.
- ✓ Preparar futuras evaluaciones de datos RAMS.
- ✓ Comentarios capítulo por capítulo con respecto RAMS.

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE NEGOCIACIONES DEL CONTRATO
Temas a considerar: ✓ Revisar / actualizar el análisis preliminar RAMS y la distribución RAMS.
Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE TRAMITACIÓN DEL PEDIDO: DEFINICIÓN DE LOS REQUISITOS DEL SISTEMA

Temas a considerar:

- ✓ Establecer la gestión RAMS específica del proyecto.
- ✓ Especificar los requisitos RAMS del sistema (global).
- ✓ Establecer el programa RAMS (¿es suficiente el programa RAMS estándar?).
- ✓ Asignar los requisitos RAMS a los subcontratistas, proveedores.
- ✓ Definir el criterio de aceptación RAMS (global).

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE TRAMITACIÓN DEL PEDIDO: DISEÑO E IMPLEMENTACIÓN

Temas a considerar:

- ✓ Análisis de Fiabilidad (FMEA).
- ✓ Análisis de Seguridad (FMECA), si es aplicable.
- ✓ Análisis de Mantenimiento / reparos; definir la política de mantenimiento/ reparación.
- ✓ Análisis de disponibilidad basado en la política de mantenimiento / reparación.
- ✓ Revisiones RAMS.
- ✓ Estimación del coste del ciclo de vida.
- ✓ Demostración RAMS, evidencia de recopilación.
- ✓ FMEA de Diseño / fabricación.
- ✓ Pruebas de fiabilidad y mantenibilidad, si son aplicables.

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE COMPRAS

Temas a considerar:

- ✓ Facilitar la especificación RAMS a subcontratistas / proveedores.

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE FABRICACIÓN / REALIZACIÓN DE PRUEBAS
Temas a considerar: ✓ Garantía de calidad / garantía de proceso relacionadas con RAMS.
Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE PUESTA EN SERVICIO / ACEPTACIÓN

Temas a considerar:

- ✓ Realizar una demostración RAM.
- ✓ Elaborar un Caso de Seguridad específico de la Aplicación.
- ✓ Poner en marcha la evaluación de datos RAMS.
- ✓ Realización de pruebas RAM durante las primeras etapas de funcionamiento; selección y evaluación de datos.

Hallazgos:

EVALUACIÓN DE LOS PROCESOS DEL PROYECTO RAMS

Proceso: FASE OPERACIÓN Y MANTENIMIENTO

Temas a considerar:

- ✓ Operación provisional y mantenimiento (política de Mantenimiento / reparación).
- ✓ Formación del personal de operación y mantenimiento.
- ✓ Evaluación de los datos RAMS.
- ✓ Evaluación del coste del ciclo de vida.
- ✓ Revisión de la ejecución.

Hallazgos:

COMENTARIOS SOBRE TEMAS A VERIFICAR EN LA PRÓXIMA AUDITORÍA
Hallazgos:

- **Discusión**

La Especificación de Requisitos de Seguridad del sistema identifica todas las funciones de seguridad asignadas al software y determina el nivel de Integridad de la Seguridad del mismo para dichas funciones.

Las etapas funcionales sucesivas en la aplicación de las normas europeas son las que se detallan a continuación:

a) Definir la Especificación de Requisitos del Software y en paralelo considerar la arquitectura del software. La arquitectura del software es donde se desarrolla la estrategia de seguridad para el software y para el nivel de Integridad de la Seguridad del software;

b) Diseño, desarrollo y ensayo del software de acuerdo con el Plan de Garantía de la Calidad del Software, el nivel de Integridad de la Seguridad del software y el ciclo de vida del software;

c) Integrar el software en el hardware objetivo y verificar su funcionalidad;

d) Aceptar e implantar el software;

e) Si se requiere el mantenimiento del software durante su vida operativa, entonces se ha de hacer de acuerdo con las normas europeas descriptas en éste trabajo.

Durante el Ciclo de Vida del desarrollo del software se deberán realizar varias actividades. Estas incluyen: ensayos, verificación, validación, evaluación, aseguramiento de la calidad y modificación y control de las modificaciones.

Se deberán establecer requisitos para las herramientas de soporte y para los sistemas configurados mediante datos de aplicación o algoritmos.

Se deberán establecer también requisitos en lo que concierne a la independencia de roles y a la competencia del personal implicado en el desarrollo del software.

Si bien las normas no obligan a utilizar un Ciclo de Vida específico para el desarrollo del software, es muy conveniente adoptar uno y su correspondiente conjunto de documentación asociada.

2.4. Conclusiones

Una conclusión importante a la que se arribó, luego del análisis de los niveles de Integridad de la Seguridad del software crítico en sistemas ferroviarios, es que el SIL depende de la integridad ante fallas sistemáticas y ante fallas aleatorias.

A las fallas aleatorias, inherentes a la fiabilidad de los equipos, fallas debido a la fatiga, deterioro por el tiempo de uso, etc. no los hemos considerado, ya que éste trabajo de investigación se basó en la identificación de los requisitos de Integridad de la Seguridad del software para el desarrollo de una Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias.

Como las fallas sistemáticas son causadas por errores humanos durante el diseño, fabricación, verificación, validación, implantación o mantenimiento del software, una forma de minimizar éstas fallas sistemáticas es adoptar un adecuado Ciclo de Vida de desarrollo y técnicas o medidas del software adecuadas para el diseño y desarrollo del producto.

Para cada nivel SIL, las normas EN 5012X son más o menos exigentes, determinando la forma de minimizar las fallas sistemáticas.

Para minimizar los riesgos debidos a las fallas sistemáticas, las técnicas o medidas del software deberán ser de aplicación Mandatoria (M) o Altamente Recomendable (AR) para sistemas con requerimientos de un SIL elevado, como es el caso del software crítico en sistemas ferroviarios.

La Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias 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.

Como representante de la Universidad Nacional de La Matanza ante el IRAM - Instituto Argentino de Normalización y Certificación, se ha presentado la Lista de Verificación para la Auditoría de Aplicaciones Ferroviarias al Sub-Comité de Seguridad en Tecnologías de la Información. La misma ha despertado el interés del Sub-Comité y será sujeta a evaluación por parte del mismo a fin de ser adoptada.

2.5. Bibliografía

1. Zárate Fraga, Marta. Análisis RAMS. Proyecto Fin de Carrera. Universidad Carlos III de Madrid; Febrero de 2012.
2. CENELC: 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 9000. Sistemas de gestión de la calidad. Fundamentos y vocabulario. 2000.

2.6. Anexos

- **Publicaciones**

d) Anexo 1: Asistencia a Congresos Nacionales

- Certificado WICC 2014
- Certificado CoNaIISI 2014
- Certificado WICC 2015
- Certificado CoNaIISI 2015

d) Anexo 2: Artículos presentados en Congresos Nacionales

- AUTORES: Eterovic, Jorge; Donadello, Domingo; Gioia, Cintia; Maidana, Carlos; Pomar, Pablo; Ureta, Walter; Eterovic, Silvina.
- TÍTULO: Desarrollo de una metodología para estandarizar las auditorias del software para sistemas de control y protección del ferrocarril.
- TIPO: Comunicación libre (póster)
- REUNIÓN: WICC 2014 - XVI Workshop de Investigadores en Ciencias de la Computación.
- LUGAR: Ushuaia.
- FECHA REUNIÓN: 7 y 8 de mayo de 2014.
- RESPONSABLE: Universidad Nacional De Tierra del Fuego. RedUNCI.
- TIPO DE TRABAJO: Artículo completo
- FUENTE: Anales del WICC 2014. Mayo de 2014. Ushuaia. Páginas: 816-821; ISBN: 978-950-863-101-5.
  Link: http://sedici.unlp.edu.ar/handle/10915/43265

- AUTORES: Eterovic, Jorge; Donadello, Domingo.
- TÍTULO: Desarrollo de una Guía de Auditoria para la Verificación de la Calidad del Software Crítico en Sistemas Ferroviarios.
- TIPO: Ponencia
- REUNIÓN: CoNaIISI 2014 – 2do Congreso Nacional de Ingeniería Informática / Sistemas de Información.
- LUGAR: San Luis.
- FECHA REUNIÓN: 13 y 14 de noviembre de 2014.
- RESPONSABLE: Universidad Nacional de San Luis. CONFEDI – RIISIC.

- TIPO DE TRABAJO: Artículo completo.
- FUENTE: Anales del CoNaIISI 2014. Noviembre de 2014. San Luis. Páginas 1372-1379. ISSN: 2346-9927.

- AUTORES: Eterovic, Jorge; Donadello, Domingo; Gioia, Cintia; Pomar, Pablo; Ureta, Walter; Eterovic, Silvina.
- TÍTULO: Desarrollo de una metodología para la verificación de la calidad del software crítico en sistemas ferroviarios.
- TIPO: Comunicación libre (póster)
- REUNIÓN: WICC 2015 - XVI Workshop de Investigadores en Ciencias de la Computación.
- LUGAR: Salta.
- FECHA REUNIÓN: 16 y 17 de abril de 2015.
- RESPONSABLE: Universidad Nacional De Tierra del Fuego. RedUNCI.
- TIPO DE TRABAJO: Artículo completo
- FUENTE: Anales del WICC 2015. Abril de 2015. Salta. ISBN: 978-987-633-134-0

- AUTORES: Eterovic, Jorge; Donadello, Domingo.
- TÍTULO: Desarrollo de una Guía de Auditoria para la Verificación de la Calidad del Software Crítico en Sistemas Ferroviarios.
- TIPO: Ponencia
- REUNIÓN: CoNaIISI 2015 – 3er Congreso Nacional de Ingeniería Informática / Sistemas de Información.
- LUGAR: CABA.
- FECHA REUNIÓN: 19 y 20 de noviembre de 2015.
- RESPONSABLE: Universidad Tecnológica Nacional – Facultad Regional Buenos Aires. CONFEDI – RIISIC.
- TIPO DE TRABAJO: Artículo completo.
- FUENTE: Anales del CoNaIISI 2015. Noviembre de 2015. CABA. ISSN: 978-987-1896-47-9.

Mag. Jorge E. Eterovic

Anexo 1

Certificados de Asistencia a Congresos Nacionales

RedUNCI

WICC2014 USHUAIA
XVI Workshop de Investigadores en Ciencias de la Computación

UNTDF
Universidad Nacional de Tierra del Fuego, Antártida e Islas del Atlántico Sur

Se certifica que Cintia Gioia (UNLaM), Carlos Maidana (UNLaM), Pablo Pomar (UNLaM), Walter Ureta (UNLaM), Silvina Eterovic (UNLaM), Domingo F Donadello (UNLaM), Jorge E. Eterovic (UNLaM) ha/n participado en calidad de autor/es del artículo 6200 + "Desarrollo una metodología para estandarizar las auditorias del software para sistemas de control y protección del ferrocarril" en el **XVI WORSHOP DE INVESTIGADORES EN CIENCIAS DE LA COMPUTACIÓN**, realizado en la ciudad de Ushuaia, Tierra del Fuego, Antártida e Islas del Atlántico Sur, durante los días 7 y 8 de mayo de 2014.

Ing. Armando E. De Giusti
Coordinador RedUNCI

Lic. Guillermo E. Feierherd
Coordinador XVI WICC

2° Congreso Nacional de Ingeniería Informática / Sistemas de Información

CoNaIISI 2014

Se certifica que ***Jorge Esteban Eterovic*** ha participado en carácter de expositor del artículo: ***"Desarrollo de una guía de auditoria para la verificación de la calidad del software crítico en sistemas ferroviarios"***, en el 2° Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI 2014), organizado por la Red de Ingeniería Informática / Sistemas de Información de CONFEDI (RIISIC), realizado en la Universidad Nacional de San Luis los días 13 y 14 de noviembre de 2014.

Se extiende el presente a los 14 días del mes de noviembre de 2014 en la ciudad de San Luis, Argentina.

Dr. Daniel Riesco
Universidad Nacional de San Luis
Coordinador de CoNaIISI

Dr. Germán Montejano
Universidad Nacional de San Luis
Coordinador de CoNaIISI

Ing. Andrés Burgetyn
Universidad Tecnológica Nacional
Facultad Regional Buenos Aires
Coordinador RIISIC 2014

UNIVERSIDAD NACIONAL DE SALTA

WICC 2015

RedUNCI

XVII Workshop de Investigadores en Ciencias de la Computación

Se certifica que ***Jorge E. Eterovic (UNLaM), Cintia Gioia (UNLaM), Carlos Maidana (UNLaM), Pablo Pomar (UNLaM), Walter Ureta (UNLaM), Silvina Eterovic (UNLaM)*** ha/n participado en calidad de autor/es del artículo ***Desarrollo de una metodología para la verificación de la calidad del software crítico en sistemas ferroviarios***, aceptado en el **XVII Workshop de Investigadores en Ciencias de la Computación** - **WICC 2015**, llevado a cabo los días 16 y 17 de Abril de 2015 en la ciudad de Salta, Argentina.

Ing. Armando E. De Giusti
Coordinador RedUNCI

Ing. Carlos E. Puga
Decano de la Facultad de Ciencias Exactas
Universidad Nacional de Salta

19 y 20 de Noviembre
Universidad Tecnológica Nacional, Facultad Regional Buenos Aires

CONAIISI2015

3er Congreso Nacional de Ingeniería Informática / Sistemas de Información

confedi · RIISIC · UTN.BA · UNIVERSIDAD TECNOLÓGICA NACIONAL

TRABAJO ACEPTADO PARA PRESENTACIÓN

Por cuanto:

JORGE ESTEBAN ETEROVIC Y DOMINGO DONADELLO

han participado como autores del trabajo titulado "***Identificación de los niveles de Integridad de la Seguridad en el desarrollo de software crítico para sistemas ferroviarios***" en el 3er Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI 2015), organizado por la red de carreras de Ingeniería Informática / Sistemas de Información (RIISIC) perteneciente al CONFEDI y realizado en la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires, los días 19 y 20 de noviembre del 2015.

Se extiende el presente certificado a los veinte días del mes de noviembre del 2015 en la ciudad de Buenos Aires, Argentina.

Ing. Andrés Bursztyn
UTN FR. Buenos Aires

Dr. Daniel Riesco
UN San Luis

Anexo 2

Artículos presentados en Congresos Nacionales

– **Artículo presentado en el WICC 2014**

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 organi-zativa, 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 metodológi-cos.
- Establecer el contexto de la investiga-ción.
- 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 método-logía 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.

– **Artículo presentado en el CoNaIISI 2014**

Desarrollo de una guía de auditoria para la verificación de la calidad del software crítico en sistemas ferroviarios

Eterovic, Jorge Esteban
Donadello, Domingo
Universidad Nacional de La Matanza,
Departamento de Ingeniería e Investigaciones Tecnológicas

Abstract

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, Mantenibilidad y Seguridad (RAMS, por sus siglas en inglés) establecidos en las normas internacionales, en particular en la norma EN 50126, utilizada en la Unión Europea.
Para ello, es necesario desarrollar un proceso de evaluación de la conformidad del software adquirido y/o desarrollado para el control ferroviario. La conformidad será de acuerdo con los requisitos establecidos en la norma EN 50126.
Considerando que ésta norma describe las fases del desarrollo del software, y que las organizaciones involucradas en el desarrollo de software deben implementar y usar un Sistema de Garantía de Calidad conforme con la Norma ISO 9000, es *altamente recomendable la certificación de conformidad con ésta norma.*
El objetivo de este trabajo es el desarrollo de una guía de auditoria para la verificación de la calidad del software crítico en sistemas ferroviarios, basada en la aplicación de la norma ISO 90003, que da las directrices para la aplicación de norma ISO 9001.
De esta manera, una empresa que desarrolle software para sistemas ferroviarios, al certificar la calidad del proceso con las normas ISO 9001 y 90003, estaría en condiciones de certificar su producto con la norma EN 50126.

Palabras Clave

Software crítico. RAMS. Calidad del software. Proceso de evaluación de calidad. Verificación de la calidad del software.

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 Mantenibilidad.
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, representadas 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 la necesidad de mejora de 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 involucradas 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 seleccionadas 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 lo tanto, evaluar con máxima objetividad las características de calidad deseadas, no es una tarea menor, y debe dedicarse mucho esfuerzo.

Con la creciente sofisticación de los productos de software y su uso en áreas críticas como en medicina, cirugía, aeronavegación, militar, ferroviaria etc., se han intensificado las actividades de evaluación de la calidad de los productos y artefactos de software [11].

El objetivo de este trabajo es el desarrollo de un guía de auditoria para la verificación de la calidad del software crítico en sistemas ferroviarios basado en la aplicación de la norma IRAM-ISO 90003 [12], que da las directrices para la aplicación de norma IRAM-ISO 9001 [13].

Elementos del Trabajo y metodología

Las normas proporcionan una serie de requisitos que se deben cumplir en las fases de desarrollo, implantación y mantenimiento del software crítico destinado a aplicaciones de control y protección de ferrocarriles. Se definen 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. Se proporcionan además los criterios relativos a la calificación, experiencia y competencia del personal.

El concepto clave es el de los niveles de integridad de seguridad del software. Se identifican cinco niveles de integridad de seguridad del software, 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.

Se deben identificar técnicas y medidas para los cinco niveles de integridad de seguridad del software.

Como resultado de este trabajo se muestran las técnicas y medidas requeridas para los niveles 0 a 4 de integridad de seguridad del software. Las técnicas requeridas para el nivel 1 son las mismas que para el nivel 2 y las técnicas requeridas para el nivel 3 son las mismas que para el nivel 4. Lo qué no se puede indicar es 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.

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.

De todos modos 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 relacionado con la seguridad razonablemente complejo, especialmente la ausencia de errores de especificación y diseño.

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:

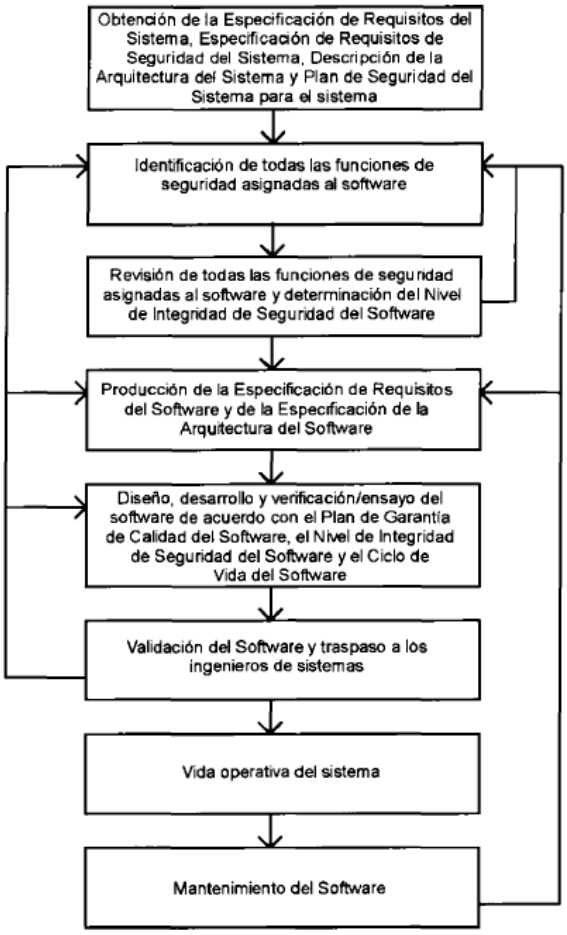


Figura 1- Etapas funcionales

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 del Software, cuyo objetivo es identificar, supervisar y controlar toda actividad, tanto técnica como de gestión, necesaria para garantizar que el software alcanza la calidad requerida.

Es necesario para proporcionar la defensa cualitativa necesaria contra errores sistemáticos y para garantizar que se puede establecer una pista de auditoría que permita realizar las actividades de verificación y validación de forma efectiva.

Las organizaciones involucradas en el desarrollo del software deben implementar y usar un Sistema de Garantía de Calidad conforme con la Norma IRAM-ISO 9000 [14], para satisfacer los requisitos de esta norma europea. Es altamente recomendable la certificación de conformidad con la Norma IRAM-ISO 9001.

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

g) Definición del modelo del ciclo de vida:
   6) actividades y tareas básicas compatibles con los planes, por ejemplo, el Plan de Seguridad que se ha establecido a nivel del sistema;
   7) criterios de entrada y salida de cada actividad;
   8) entradas y salidas de cada actividad;
   9) principales actividades de calidad;
   10) entidad responsable de cada actividad.

h) Estructura de la documentación.

i) Control de la documentación:
   4) roles de aquellos implicados en su redacción, control y aprobación;
   5) campo de aplicación de la distribución;
   6) archivo.

j) Seguimiento y trazabilidad de las desviaciones.

k) Métodos, medidas y herramientas para la garantía de calidad en función de los niveles de integridad de seguridad asignados.

l) 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, como en un Plan de Gestión de la Configuración del Software, un Plan de Mantenimiento, un Plan de Verificación del Software y un Plan de Validación del Software separados. Los apartados del Plan de Garantía de Calidad del Software deben proporcionar la referencia de los documentos en los que aparece la información. En cualquier caso, se debe especificar el contenido de cada apartado del Plan de Garantía de Calidad del Software, ya sea directamente o mediante referencia a otro documento.
Finalmente se debe redactar un Informe de Verificación de la Garantía de Calidad del Software, pudiéndose usar como base la guía de auditoria que se desarrolla en este trabajo.

Ciclo de vida del sistema

El ciclo de vida del sistema es una secuencia de fases, cada una de las cuales contiene tareas que abarcan la vida completa de un sistema desde su concepto inicial hasta la retirada del servicio y la eliminación. El ciclo de vida proporciona una estructura para la planificación, la gestión, el control y la supervisión de todos los aspectos de un sistema, incluida la RAMS, a medida que el sistema avanza a través de sus fases, con el fin de entregar el producto adecuado al precio correcto dentro del plazo acordado.
Un ciclo de vida de un sistema, adecuado en el contexto de una aplicación ferroviaria, se muestra en la figura 2.
La figura 2 representa el ciclo de vida del sistema en el modelo en "V", donde la rama descendente (lado izquierdo) se llama generalmente Desarrollo y consiste en un proceso de perfeccionamiento que finaliza con la fabricación de componentes del sistema. La rama ascendente (lado derecho) está relacionada con el montaje, la instalación, la recepción y el funcionamiento de todo el sistema.

La representación en "V" supone que las actividades de aceptación están intrínsecamente vinculadas a las actividades de desarrollo, dado que lo que es realmente diseñado tiene que ser finalmente comprobado en relación con los requisitos.

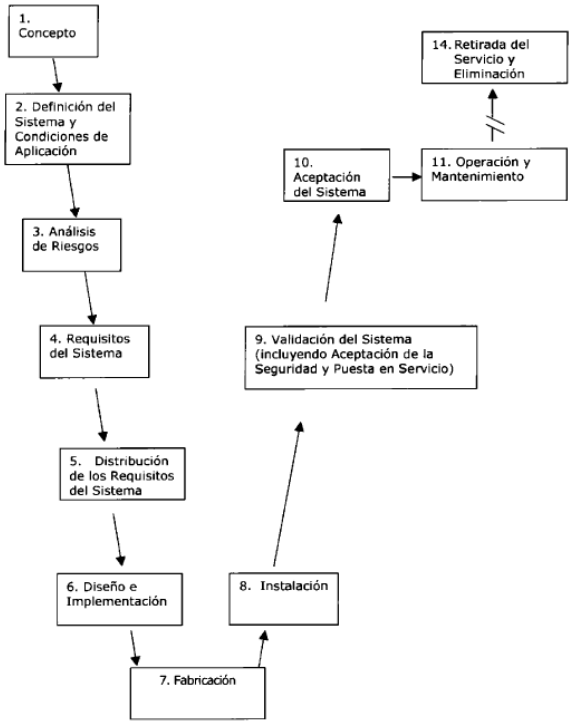
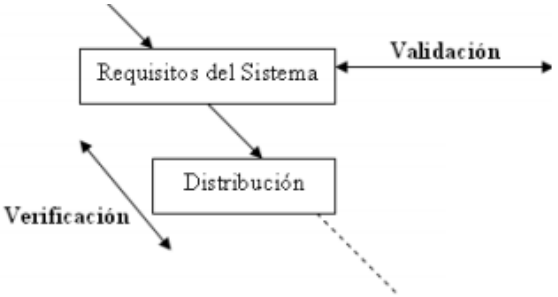


Figura 2 – Ciclo de vida (representación en V)

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 3.



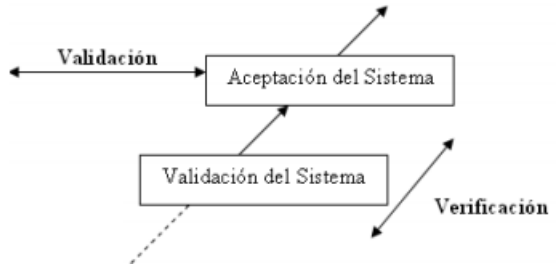


Figura 3 - Validaciones

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 entregas 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 sus requisitos en todos los aspectos.

Las tareas de verificación están incluidas dentro de cada fase del ciclo de vida. Si buscamos el aseguramiento del sistema en el contexto RAMS, las tareas de verificación y validación forman parte integral de la demostración global de aseguramiento de los sistemas.

Para la realización de éstas tareas se debe definir el Rol "Validador", cuyas responsabilidades serán:

- debe desarrollar una comprensión del sistema de software dentro del entorno previsto de aplicación;
- debe desarrollar un plan de validación y especificar las tareas y actividades esenciales para la validación del software y ponerse de acuerdo sobre este plan con el evaluador;
- debe revisar los requisitos del software en relación a su uso/entorno previsto;
- debe revisar el software en relación a los requisitos del software de forma que se garantice que se cumplen todos ellos;
- debe evaluar la conformidad del proceso del software y del software desarrollado en relación a los requisitos de la normativa incluyendo el SIL asignado;
- debe revisar la corrección, coherencia y adecuación de la verificación y de los ensayos;
- debe comprobar la corrección, coherencia y adecuación de los casos de ensayo y de los ensayos realizados;
- debe garantizar que se realizan todas las actividades del plan de validación;
- debe revisar y clasificar todas las desviaciones en términos de riesgo (impacto), registrarlas y comunicarlas al organismo competente de la gestión de las modificaciones para su evaluación y toma de decisiones;
- debe proporcionar una recomendación sobre la idoneidad del software para su uso previsto e indicar cualquier restricción de la aplicación según sea apropiado;
- debe registrar las desviaciones a partir del plan de validación;
- debe realizar auditorías, inspecciones o revisiones del proyecto global (como instancias del proceso de desarrollo genérico) según sea apropiado, en varias fases del desarrollo;
- debe revisar y analizar los informes de validación relativos a aplicaciones previas según sea apropiado;
- debe revisar si las soluciones desarrolladas son trazables hasta los requisitos del software;
- debe garantizar que se revisan los registros de situaciones peligrosas asociadas y los casos de no conformidad y que se resuelven todas las situaciones peligrosas de manera adecuada, ya sea mediante medidas que las eliminen o con medidas de control/transferencia de los riesgos;
- debe desarrollar un informe de validación y
- debe expresar su acuerdo/desacuerdo sobre la versión del software publicada

Resultados

Para cada fase de este ciclo de vida, se han definido las principales tareas a ser auditadas. Se resumen en la siguiente tabla (figura 4):

Fase del ciclo de vida	**Tareas a ser auditadas**
1.Concepto	Ámbito y propósito del proyecto Ferroviario. Definición del concepto del proyecto ferroviario. Análisis Financiero y estudios de viabilidad. Existencia del equipo de gestión. Las implicaciones de seguridad del proyecto. La política y objetivos de la seguridad.
Fase ciclo del de vida	**Tareas a ser auditadas**
2.Definición del sistema y condiciones de aplicación	El perfil de la misión del sistema. La descripción del sistema. La estrategia de Operación y Mantenimiento. Las condiciones de operación y mantenimiento. La influencia de las restricciones de la infraestructura existente. El análisis preliminar de las amenazas. El plan de seguridad. Definición de las condiciones de operación y mantenimiento a largo plazo. Identificar la influencia en RAM de las restricciones en la infraestructura existente.
3.Análisis de riesgos	El Análisis de riesgos relacionado con el proyecto. El análisis amenazas y riesgos de la seguridad del sistema. El registro de las amenazas. La evaluación de riesgos.
4.Requisitos del Sistema	El análisis de requisitos. Especificaciones del sistema. Especificación el entorno. Los criterios de Demostración y Aceptación del sistema. El plan de Validación. Los requisitos de Gestión, Calidad y Organización. El procedimiento de control de cambios. Los requisitos de Seguridad del Sistema. Los criterios de aceptación de la Seguridad. Los requisitos relacionados con la segundad Funcional. La Gestión de Seguridad.
5.Distribución de los Requisitos del Sistema	Especificación de los requisitos de los subsistemas y componentes. Especificación de los criterios de aceptación de subsistemas y componentes. Los requisitos de seguridad de los subsistemas y componentes. Los criterios de aceptación de seguridad de los subsistemas y componentes. El Plan de Seguridad del Sistema.
6.Diseño e implementación	La planificación. El Diseño y desarrollo. El análisis del diseño y pruebas. La Verificación del diseño- La implementación y validación. El diseño de los recursos de apoyo logísticos. El Registro de amenazas. El Análisis de amenazas y evaluación de riesgos. La Gestión de la Seguridad. El Control de subcontratos y proveedores. Un Caso de Seguridad.
Fase ciclo del de vida	**Tareas a ser auditadas**
7.Producción	El plan de producción. La fabricación de código. La fabricación y prueba del montaje de componentes. La documentación. La capacitación. La implementación del plan de seguridad. El uso del registro de amenazas.
8.Instalación	El montaje del sistema La instalación del sistema. El programa de instalación. La implementación del programa de instalación.
9.Validación del sistema	La puesta en servicio. El período de pruebas de operación. La capacitación. El programa de puesta en servicio. La implementación del programa de puesta en servicio. El Caso de Seguridad específico de la aplicación.
10.Aceptación del sistema	Los procedimientos de aceptación, basados en criterios de aceptación. La recopilación de las pruebas para la aceptación. La entrada en servicio. El periodo de pruebas de operación. El Caso de Seguridad específico de la aplicación.
11.Operación y mantenimiento	La operación del sistema a largo plazo. El mantenimiento. La capacitación en el mantenimiento centrado en segundad. El control de la ejecución de segundad y mantenimiento del registro de las amenazas.
12.Supervisión de la ejecución	La recopilación estadística de la ejecución operacional. La adquisición, el análisis y la evaluación de los datos. La recopilación, el análisis, la evaluación el uso de las estadísticas de Seguridad y ejecución.
13.Modificación	Los procedimientos de cambio de

y realimentación	requisitos. Los procedimientos de modificación y realimentación. Las implicaciones de Seguridad para la modificación y realimentación.
14.Retirada de servicio y eliminación	El plan de retirada de servicio y eliminación. La retirada de servicio. La eliminación. El plan de Seguridad. El análisis de amenazas y la evaluación de riesgos. La implementación del plan de Seguridad.

Figura 4 – Tareas a auditar

Además de lo expresado, en todas las fases se deberían auditar las siguientes tareas:

- Control de Cambios
- Gestión de la Configuración
- Verificación y Validación
- Análisis de riesgos

Los procesos del sistema de gestión se deben evaluar de acuerdo a la norma IRAM-ISO 9000, teniendo que considerar los siguientes temas:

1. Identificación y comunicación de los requisitos del cliente (5.4, 7.2);
2. Identificación de la vinculación (secuencia e interrelación) con otros procesos (4.1);
3. Identificación de los objetivos del proceso (7.1);
4. Definición de responsabilidad y autoridad (5.5.1);
5. Competencia del personal (6.2);
6. Adecuación de recursos y ambiente de trabajo (6.3, 6.4, 7.1);
7. Adecuación de la documentación que describe las prácticas de operación (Cap. 7);
8. Seguimiento del desempeño del proceso y control de no conformidades (8.3, 8.4);
9. Aplicación de acciones correctivas y preventivas (8.5.2, 8.5.3);
10. Evidencia de mejora continua (8.5.1);
11. Disponibilidad de registros (4.2.4, 7.1d);
12. Divulgación de la certificación. Uso de logos. (Aplica sólo en auditorías de seguimiento o recertificación) y
13. Gestión del cumplimiento de requisitos legales del producto.

Discusión

Si bien las normas CENELEC nos permiten identificar los requerimientos para la verificación de la calidad del software crítico en sistemas ferroviarios de manera que en la norma EN 50126 se define el ciclo de vida, en la norma EN 50128 las técnicas de software y en la EN 50129 las técnicas de hardware, podríamos plantear y un requisito para cada nivel de integridad de seguridad del software (SIL) para cada técnica o medida de la Garantía de la Calidad del Software en función del Nivel de Integridad de la Seguridad (SIL) de la siguiente manera:

Técnica/Medida	**SIL O**	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
Acreditada según la Norma ISO 9001	R	HR	HR	HR	HR
Conforme con la Norma ISO 9001	M	M	M	M	M
Conforme con la Norma ISO/IEC 90003	R	R	R	R	R
Sistema de Calidad de la Compañía	M	M	M	M	M
Gestión de la Configuración del Software	M	M	M	M	M
Listas de Comprobación	R	HR	HR	HR	HR
Trazabilidad	R	HR	HR	M	M
Registro y Análisis de Datos	HR	HR	HR	M	M

Donde los requisitos para los niveles de integridad de seguridad del software 1 y 2 son los mismos para cada técnica. Del mismo modo, cada técnica tiene los mismos requisitos en los niveles de integridad de seguridad del software 3 y 4. Estos requisitos pueden ser:

- M: mandatorio;
- HR: altamente recomendable:
- R: recomendable

La combinación de técnicas o medidas se deberán incluir en el Plan de Garantía de Calidad del Software.

Conclusión

Una conclusión importante a la que se arribó, luego del análisis de la guía de auditoria para la verificación de la calidad del software crítico en sistemas ferroviarios, es que el Nivel de Integridad de la Seguridad (SIL) depende de la integridad ante Fallos Sistemáticos y ante Fallos Aleatorios.

A los Fallos Aleatorios, inherentes a la fiabilidad de los equipos, fallos debidos a la fatiga, deterioro por el tiempo de vida, etc. no los hemos considerado, ya que la investigación se basó en la verificación de la calidad del software.

Los Fallos Sistemáticos son causados por errores humanos durante el diseño, fabricación, verificación, validación o mantenimiento del software.

Una forma de minimizar fallos sistemáticos es utilizar un adecuado ciclo de vida y técnicas de software y hardware adecuadas para el diseño y desarrollo del producto.

Para cada nivel SIL, las normas EN 5012X son más o menos exigentes, determinando la forma de minimizar los fallos sistemáticos. En los Fallos sistemáticos las características del ciclo de vida, de las tareas a realizar, de las técnicas software y hardware a aplicar etc. deberán ser más exigente para sistemas con funciones de un SIL elevado.

Referencias

1. Zárate Fraga, Marta. Análisis RAMS. Proyecto Fin de Carrera. Universidad Carlos III de Madrid; Febrero de 2012.
2. CENELC: 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 9001. Sistemas de gestión de la calidad. Requisitos. 2008.
13. Norma IRAM-ISO 90003. Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software. 2004.
14. Norma IRAM-ISO 9000. Sistemas de gestión de la calidad. Fundamentos y vocabulario. 2000.

Datos de Contacto:

Mag. Jorge Esteban Eterovic.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail. jeterovic@hotmail.com
jeterovic@ing.unlam.edu.ar

Mag. Domingo Donadello.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail.ddonadel@ing.unlam.edu.ar

– **Artículo presentado en el WICC 2015**

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;

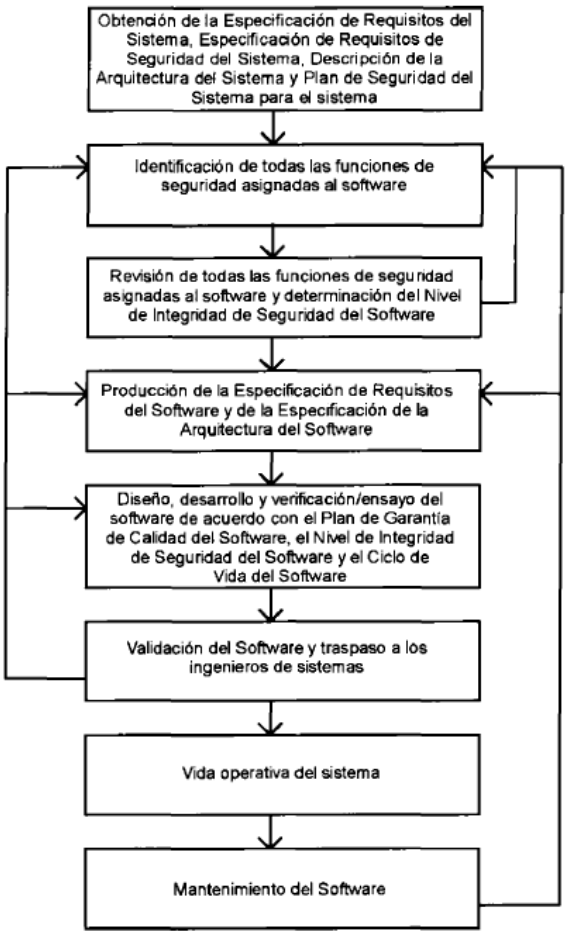


Figura 1- Etapas funcionales

   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 documen-tación 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.

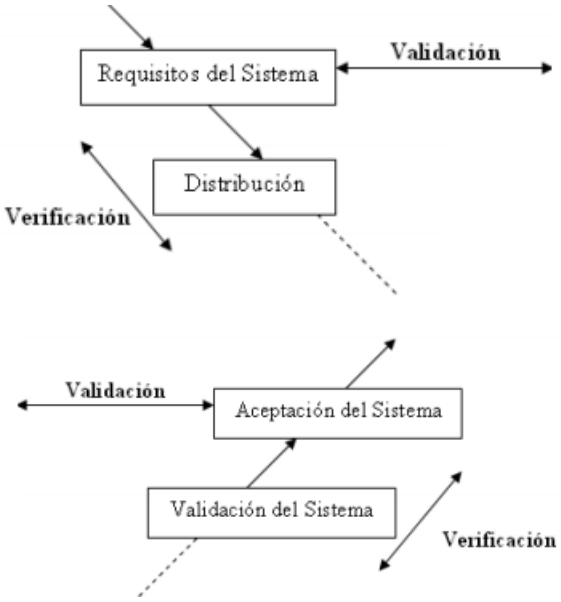


Figura 2 - Validaciones

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.

– **Artículo presentado en el CoNaIISI 2015**

Identificación de los niveles de Integridad de la Seguridad en el desarrollo de software crítico para sistemas ferroviarios

Eterovic, Jorge Esteban
Donadello, Domingo
Universidad Nacional de La Matanza,
Departamento de Ingeniería e Investigaciones Tecnológicas

Abstract

Los sistemas críticos, cuyo buen funcionamiento condiciona nuestra vida cotidiana, necesitan cumplir con determinados niveles de Integridad de la Seguridad (SIL), antes de su puesta en funcionamiento. La criticidad de estos sistemas reside cada vez más en los productos de software que contienen.
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, Mantenibilidad y Seguridad (RAMS, por sus siglas en inglés) establecidos en las normas internacionales, en particular en la norma EN 50126 [1], utilizada en la Unión Europea.
Cuanto más peligrosas sean las consecuencias de una falla del software, mayor será el nivel requerido de Integridad de Seguridad del mismo.
El objetivo de este trabajo es identificar éstos niveles de Integridad de la Seguridad en el desarrollo de software crítico para sistemas ferroviarios.

Palabras Clave

Software crítico ferroviario. Niveles de Integridad de la Seguridad. SIL.

Introducción

El desarrollo de sistemas para la industria ferroviaria debe ser llevado a cabo con ciertas premisas relativas a la seguridad, tratando de identificar los riesgos para controlarlos y llevarlos a un nivel aceptable. Los requisitos de seguridad pueden ser cuantitativos o cualitativos.
En algunas áreas, tales como el software, donde se pueden producir fallas sistemáticas, las buenas prácticas de ingeniería señalan que para cumplir con los requisitos de integridad se deben establecer y aplicar adecuados niveles de Integridad de la Seguridad (SIL) [2].
Existen técnicas estandarizadas para evaluar y controlar el riesgo derivado de las fallas aleatorias. El riesgo derivado de las fallas sistemáticas se controla, en distintas actividades de la ingeniería, a través de la comprobación rigurosa y la aplicación de normas, códigos y del uso de las buenas prácticas generalmente aceptadas.
Sin embargo, como la complejidad de los diseños aumenta, las fallas sistemáticas contribuyen, en una mayor proporción, en el incremento del riesgo.
Para el software, todas las fallas son sistemáticas. En el software y algunas otras áreas donde los diseños pueden ser particularmente complejos, tales como el diseño de la electrónica, las mejores prácticas actuales aconsejan hacer uso de niveles de Integridad de la Seguridad para controlar dichas las fallas sistemáticas.
Los SILs se describen en la serie de normas IEC 61508 [3], ampliamente utilizadas en el desarrollo de software crítico. Además, específicamente para la industria ferroviaria, las normas EN 50128 [4] y EN 50129 [5] definen los sistemas o partes de sistemas para los cuales es aplicable el uso de los SILs.
Los SILs representan diferentes niveles de rigurosidad en el proceso de desarrollo. Se definen cinco niveles, que van desde SIL 4, el más riguroso, al SIL 1, el menos riguroso. Las funciones que no se basan en

los SILs para controlar el riesgo, pueden ser descriptas como SIL 0.
Cada nivel de Integridad se asocia con una probabilidad de falla. En la Tabla 1 se muestra la probabilidad de falla para cada uno de los SILs, de acuerdo con la norma IEC 61508.

Modo de Operación de baja demanda (probabilidad de falla en la demanda)	**Modo de Operación de Continua / Alta demanda (tasa por hora de falla peligrosa)**	**Nivel de Integridad de Seguridad (SIL)**
$\geq 10^{-5}$ a 10^{-4}	$\geq 10^{-9}$ a 10^{-8}	4
$\geq 10^{-4}$ a 10^{-3}	$\geq 10^{-8}$ a 10^{-7}	3
$\geq 10^{-3}$ a 10^{-2}	$\geq 10^{-7}$ a 10^{-6}	2
$\geq 10^{-2}$ a 10^{-1}	$\geq 10^{-6}$ a 10^{-5}	1

Tabla1

En la mayoría de los casos, se debe utilizar la columna "**Modo de Operación Continua / Alta demanda**". La columna "**Baja demanda**" sólo se debería utilizar si se espera que la demanda se produzca:

- No más de 1 vez al año; y
- No es mayor a 2 veces que cuando la función se pone a prueba.

No se establecen probabilidades para SIL 0. Luego, deberían establecerse las probabilidades de falla para las funciones sistemáticas a efectos de lograr un nivel de riesgo aceptable para el sistema en general.
Para los sistemas ferroviarios, las funciones que el software debería realizar estarán definidas en las Especificaciones de Requisitos.
De la misma manera que los requisitos de seguridad se fijan a nivel de sistema y forman parte de los requisitos generales del mismo, es habitual establecer una Especificación de Requisitos de Seguridad del Software ya sea como un subconjunto de la Especificación de Requisitos del Software o como un documento separado.
La norma EN 50128 proporciona una guía sobre las características de tolerancia a fallas.

Como el software no se desgasta ni se rompe, todas las fallas de software serán sistemáticas. La mayoría de las fallas de software son el resultado de errores en la programación, que a su vez son el resultado de fallas en el proceso de desarrollo, tales como una especificación incorrecta, o un error en la implementación de una especificación.
En general, si un sistema ferroviario incluye software, entonces la Integridad de la Seguridad del sistema dependerá de la Integridad de la Seguridad del software. Entonces, la confiabilidad del sistema deberá ser tratada mediante la especificación del SIL del software, que será el mismo que el SIL para el sistema.
Se requiere una Especificación de Requisitos de Seguridad del Software y una Especificación de Requisitos del Software para el software. Siempre los requisitos relacionados con la seguridad deberán ser claramente identificados.
La Especificación de Requisitos de Seguridad del Software tendrá un papel fundamental en los casos de seguridad del sistema. Tendrá que demostrar que los requisitos de seguridad del software son suficientes y que el software cumple con sus requisitos de seguridad.
Para lograr esto, la Especificación de Requisitos de Seguridad del Software debe ser completa, precisa e inteligible tanto para aquellos que desarrollan el software como para los que los usuarios.
Idealmente se debería poder asegurar que la Especificación de Requisitos del Software tenga todos estos atributos. Sin embargo, no se ha encontrado un consenso dentro de la comunidad de la ingeniería del software sobre métodos de predicción de la probabilidad de fallas de software [6].
Por lo tanto, si no se puede estimar la probabilidad de falla del software, no es posible estimar la probabilidad de falla del sistema que contiene el software.
Es posible, sin embargo, estimar la probabilidad de falla del sistema por causas que no sean del software y presentar este cálculo, cuidadosamente explicado, junto

con los SILs de las funciones del sistema en un “Caso de Seguridad” [7]. Si se utilizaran árboles de fallas, la probabilidad que el sistema falle por causas que no sean del software, pueden ser calculados estableciendo que la probabilidad de falla de software sea cero, aunque debe entenderse que se trata de un una forma de excluir la falla del software en el proceso de cálculo, y no que el software no falla.
El objetivo de este trabajo es identificar los niveles de Integridad de la Seguridad en el desarrollo de software crítico para sistemas ferroviarios.

Elementos del Trabajo y metodología

La documentación del sistema debe identificar las funciones del sistema relacionado con la seguridad tanto para el software, como para las interfaces del mismo. El sistema en el cual el software está integrado debe estar totalmente definido en relación a los siguientes elementos:

- funciones e interfaces;
- condiciones de aplicación;
- configuración o arquitectura del sistema;
- situaciones peligrosas a controlar;
- requisitos de Integridad de Seguridad;
- asignación de requisitos y del SIL al software y al hardware;
- restricciones de tiempo

La Integridad de la Seguridad del software debe especificarse como uno de cinco niveles, que como se vió anteriormente, van desde el SIL 0 al SIL 4.
El nivel requerido de Integridad de la Seguridad del software se debe decidir y evaluar a nivel del sistema, tomando como base el nivel de Integridad de la Seguridad del sistema y el nivel de riesgo asociado con el uso del software en el sistema.
Según las normas europeas, para la parte de software de un sistema que tengan un impacto en la seguridad por debajo del SIL 1, se deben cumplir, por lo menos, los requisitos asociados al SIL 0. Esto ocurrirá cuando exista una incertidumbre en la evaluación del riesgo, e incluso en la identificación de situaciones peligrosas.
Si trabajamos con un alto grado de incertidumbre en la evaluación del riesgo, es recomendable aplicar un nivel bajo de Integridad de la Seguridad, representado por SIL 0, en lugar de no utilizar ninguno.
Para trabajar de acuerdo con las normas europeas, se debe demostrar que se ha satisfecho cada uno de los requisitos definidos respecto al nivel de Integridad de la Seguridad del software y que por lo tanto se ha cumplido con el objetivo en cuestión.
En los casos en los que se califique a un requisito con las palabras "dentro del alcance requerido por el nivel de Integridad de Seguridad del software", se estará indicando que se han utilizado una serie de técnicas y medidas para satisfacer dicho requisito.
En los casos en los que se aplique el punto anterior, se deberán usar las Tablas 2, 3, y 4 para hacer la selección de las técnicas y medidas adecuadas al nivel de Integridad de Seguridad del software. Dicha selección debe documentarse en el Plan de Garantía de Calidad del Software o en otro documento al que haga referencia el Plan de Garantía de Calidad del Software [8].
A modo de ejemplo, en los Anexos A, se describen cada una de las técnicas o medidas referenciadas en las tablas.
Si no se utiliza una técnica o medida calificada como altamente recomendable (AR) en las tablas, se deben detallar entonces las razones que justifiquen el uso de técnicas alternativas y se deben registrar en el Plan de Garantía de Calidad del Software. Esto no será necesario si se utiliza una combinación homologada de técnicas que estén especificadas en la tabla correspondiente. Se debe demostrar que se han aplicado las técnicas seleccionadas de forma correcta [9].
Si se propone utilizar una técnica o una medida que no aparezca en las tablas, se debe justificar entonces su efectividad e idoneidad para cumplir los requisitos

particulares y los objetivos globales del apartado.
Debe verificarse, mediante la inspección de los documentos requeridos por las normas europeas, la conformidad con los requisitos de cada apartado en particular y sus técnicas y medidas respectivas detalladas en

DOCUMENTACIÓN	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
Planificación					
1. Plan de Garantía de Calidad del Software	AR	AR	AR	AR	AR
2. Informe de Verificación de la Garantía de Calidad del Software	AR	AR	AR	AR	AR
3. Plan de Gestión de la Configuración del Software	AR	AR	AR	AR	AR
4. Plan de Verificación del Software	AR	AR	AR	AR	AR
5. Plan de Validación del Software	AR	AR	AR	AR	AR
Requisitos del Software					
6. Especificación de Requisitos del Software	AR	AR	AR	AR	AR
7. Especificación de Ensayos del Software en Conjunto	AR	AR	AR	AR	AR
8. Informe de Verificación de los Requisitos del Software	AR	AR	AR	AR	AR
Arquitectura y diseño					
9. Especificación de la Arquitectura del Software	AR	AR	AR	AR	AR
10. Especificación del Diseño del Software	AR	AR	AR	AR	AR
11. Especificación de las Interfaces del Software	AR	AR	AR	AR	AR
12. Especificación de Ensayos de Integración del Software	AR	AR	AR	AR	AR
13. Especificación de Ensayos de Integración del Software / Hardware	AR	AR	AR	AR	AR
14. Informe de Verificación de Diseño y Arquitectura del Software	AR	AR	AR	AR	AR
Diseño de Componentes					
15. Especificación de Diseño de los Componentes Software	R	AR	AR	AR	AR
16. Especificación de Ensayos de los Componentes Software	R	AR	AR	AR	AR
17. Informe de Verificación del Diseño de los Componentes Software	R	AR	AR	AR	AR
Implementación y Ensayos de Componentes					
…..					
…..					

Tabla 2. SILs relativos al Ciclo de Vida y la Documentación

las tablas.
Cuando sea procedente, se deberán tener en cuenta también otras pruebas objetivas, auditorías y ensayos.

Criterios para la selección de técnicas y medidas

Para establecer los niveles de SIL requeridos, se comienza trabajando con la documentación asociada al Ciclo de Vida del desarrollo del software.
En la Tabla 2, a manera de ejemplo, se muestran los SILs para las primeras 4 etapas del Ciclo de Vida.
Luego se desarrollan tablas de nivel inferior para cada apartado de la tabla anterior. Por ejemplo, el apartado "6. Especificación de

Requisitos del Software" de la Tabla 2 se desarrolla en la Tabla 3.

TÉCNICA / MEDIDA	Ref.	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Métodos Formales	A.1	-	R	R	AR	AR
2. Modelado	Tabla 3	R	R	R	AR	AR
3. Metodología Estructurada	A.2	R	R	R	AR	AR
4. Tablas de Decisión	A.3	R	R	R	AR	AR

Requisitos:
1) La Especificación de Requisitos del Software debe incluir una descripción del problema en lenguaje natural y todas las notaciones formales o semiformales necesarias.
2) La tabla refleja requisitos adicionales para definir la especificación de forma clara y precisa. Se deben seleccionar una o más de estas técnicas para satisfacer el nivel de Integridad de Seguridad del software utilizado.

Tabla 3. Especificación de Requisitos del Software

TÉCNICA / MEDIDA	Ref.	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Modelado de Datos	A.4	R	R	R	AR	AR
2. Diagrama de Flujo de Datos	A.5	-	R	R	AR	AR
3. Diagrama de Flujo de Control	A.6	R	R	R	AR	AR
4. Máquinas de Estado Finitos o Diagramas de Transición de Estados	A.7	-	AR	AR	AR	AR
5. Redes de Petri Temporizadas	A.8	-	R	R	AR	AR
6. Tablas de Decisión/Tablas de Verdad	A.9	R	R	R	AR	AR
7. Métodos Formales	A.10	-	R	R	AR	AR
8. Modelado de las Prestaciones	A.11	-	R	R	AR	AR
9. Prototipado/Animación	A.12	-	R	R	AR	AR
10. Diagramas de Estructura	A.13	-	R	R	AR	AR
11. Diagramas de Secuencias	A.14	R	AR	AR	AR	AR

Requisitos:
1) Se deben definir y utilizar directrices de modelado.
2) Se debe seleccionar al menos una de las técnicas “AR”.

Tabla 4. Modelado

En ésta tabla tenemos la Técnica/Medida “2. Modelado”, que se desarrolla en la Tabla 4.

En cada una de las tablas se hace referencia a un anexo “A”, que es de carácter informativo. A manera de ejemplo se muestra en el Anexo A.4 la descripción del apartado “Modelado de Datos” de la Tabla 4.

Junto a cada técnica o medida que aparece en las tablas, habrá un requisito para cada nivel de Integridad de Seguridad del software. En este ejemplo, los requisitos para los niveles 1 y 2 de Integridad de Seguridad del software son los mismos para cada técnica. Del mismo modo, cada técnica tiene los mismos requisitos en los niveles 3 y 4 de Integridad de Seguridad del software.

Estos requisitos pueden ser:

– "M" este símbolo significa que el uso de una técnica es obligatoria (Mandatorio).
– "AR" este símbolo significa que la técnica o la medida es altamente recomendable (Altamente Recomendado) para ese nivel de Integridad de la Seguridad. Si no se utiliza esa técnica o medida, se debe proporcionar una justificación detallada en el Plan de

Garantía de Calidad del Software de por qué se han utilizado técnicas

– alternativas.

Objetivo:
Crear un modelo de datos.
Descripción
En informática se llama modelado de datos al proceso de creación de un modelo de datos mediante la aplicación de descripciones de modelos de datos formales utilizando las técnicas de modelado de datos. En ingeniería del software, un modelo de datos es un modelo abstracto que describe los modos de representación y acceso a los datos. Los modelos de datos definen formalmente objetos de datos y las relaciones entre los objetos de datos para un ámbito de interés determinado. Algunas aplicaciones típicas de modelos de bases de datos incluyen soportar el desarrollo de bases de datos y permitir el intercambio de datos para un ámbito de interés determinado. Los modelos de datos se especifican en un lenguaje de modelado de datos.

Anexo A.4. Modelado de Datos

– "R" este símbolo significa que la técnica o la medida es recomendable (Recomendado) para ese nivel de Integridad de la Seguridad. Éste es un nivel de recomendación inferior al "AR", y se pueden combinar dichas técnicas para formar parte de un paquete.
– "-" este símbolo significa que no existen recomendaciones ni a favor ni en contra relativas a la utilización de esa técnica o medida.
– "NR" este símbolo significa que la técnica o la medida NO es recomendable (No Recomendado) para ese nivel de integridad de la seguridad. La utilización de esta técnica o medida debe justificarse de forma detallada en el Plan de Garantía de Calidad del Software.

La combinación de técnicas o medidas se expondrá en el Plan de Garantía de Calidad del Software, seleccionando una o más técnicas o medidas, a menos que las notas adjuntas a la tabla impongan otros requisitos.
Dichas notas pueden incluir referencias a técnicas homologadas o a combinaciones homologadas de técnicas. Si se utilizan éstas técnicas o combinaciones de técnicas, más todas las técnicas de carácter obligatorio, entonces se deberán aceptar como válidas y solo se deberá verificar que se apliquen correctamente.
Si se utiliza un conjunto de técnicas diferente y puede justificarse su uso, entonces puede considerarlas aceptables.

Resultados

Trabajando de ésta manera se establecen 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 de ferrocarriles.
Se definen los requisitos relativos a cada una de las etapas del Ciclo de Vida del desarrollo del software que incluyen las actividades de desarrollo, implantación y mantenimiento.
El concepto clave es el de los niveles de Integridad de Seguridad del software. Se identifican cinco niveles de integridad de seguridad del software, siendo 0 el nivel mínimo y 4 el máximo.
Se establece como norma que cuanto más peligrosas sean las consecuencias de una

falla del software, mayor será el nivel requerido de Integridad de la Seguridad del software.
Se han identificado técnicas y medidas para los cinco niveles de Integridad de la Seguridad del software. En las Tablas 1, 2 y 3 se muestran las técnicas y medidas requeridas para dichos niveles de SIL.
En este ejemplo y para simplificar la identificación de los requisitos, las técnicas requeridas para el nivel 1 son las mismas que para el nivel 2 y las técnicas requeridas para el nivel 3 son las mismas que para el nivel 4.
No se dan indicaciones sobre qué nivel de Integridad de la Seguridad del software es apropiado para un riesgo determinado. Este análisis 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 ello se requiere que se adopte un enfoque sistemático para:

a) identificar peligros, evaluar riesgos y tomar decisiones en función de los criterios de riesgo;
b) identificar la reducción de riesgo necesaria para cumplir con los criterios de aceptación de riesgos;
c) definir una Especificación global de Requisitos de Seguridad del sistema con las protecciones necesarias a efectos de conseguir la reducción de riesgo requerida;
d) seleccionar una arquitectura del sistema adecuada;
e) 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 a partir de las características validadas de Integridad de la 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 la Seguridad. Y finalmente se llegará a los niveles de Integridad de la 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 de demostrar la ausencia de errores en un software razonablemente complejo, especialmente la ausencia de errores de especificación y diseño.
Por ello, las buenas prácticas aplicadas al desarrollo de software de alta complejidad, recomiendan el uso de:

- métodos de diseño descendentes (arriba-abajo);
- la modularidad;
- la verificación de cada fase del Ciclo de Vida del desarrollo;
- la verificación de los componentes y de las librerías de los componentes;
- una documentación y trazabilidad claras;
- documentos auditables;
- la validación;
- la evaluación;
- la gestión de la configuración y el control de las modificaciones; y
- el estudio apropiado de las competencias del personal y de la organización.

Discusión

La Especificación de Requisitos de Seguridad del sistema identifica todas las funciones de seguridad asignadas al software y determina el nivel de Integridad de la Seguridad del mismo para dichas funciones.
Las etapas funcionales sucesivas en la aplicación de las normas europeas son las que se detallan a continuación:

a) definir la Especificación de Requisitos del Software y en paralelo considerar la

arquitectura del software. La arquitectura del software es donde se desarrolla la estrategia de seguridad para el software y para el nivel de Integridad de la Seguridad del software;

b) diseño, desarrollo y ensayo del software de acuerdo con el Plan de Garantía de la Calidad del Software, el nivel de Integridad de la Seguridad del software y el ciclo de vida del software;
c) integrar el software en el hardware objetivo y verificar su funcionalidad;
d) aceptar e implantar el software;
e) si se requiere el mantenimiento del software durante su vida operativa, entonces se ha de hacer de acuerdo con la norma europea.

Durante el Ciclo de Vida del desarrollo del software se deberán realizar varias actividades. Estas incluyen: ensayos, verificación, validación, evaluación, aseguramiento de la calidad y modificación y control de las modificaciones.

Se deberán establecer requisitos para las herramientas de soporte y para los sistemas configurados mediante datos de aplicación o algoritmos.

Se deberán establecer también requisitos en lo que concierne a la independencia de roles y a la competencia del personal implicado en el desarrollo del software.

Si bien las normas no obligan a utilizar un Ciclo de Vida específico para el desarrollo del software, es muy conveniente adoptar uno y su correspondiente conjunto de documentación asociada.

Conclusión

Una conclusión importante a la que se arribó, luego del análisis de los niveles de Integridad de la Seguridad del software crítico en sistemas ferroviarios, es que el SIL depende de la integridad ante fallas sistemáticas y ante fallas aleatorias.

A las fallas aleatorias, inherentes a la fiabilidad de los equipos, fallas debido a la fatiga, deterioro por el tiempo de uso, etc. no los hemos considerado, ya que la investigación se basó en la identificación de los requisitos de Integridad de la Seguridad del software.

Las fallas sistemáticas son causadas por errores humanos durante el diseño, fabricación, verificación, validación, implantación o mantenimiento del software.

Una forma de minimizar éstas fallas sistemáticas es adoptar un adecuado Ciclo de Vida de desarrollo y técnicas o medidas del software adecuadas para el diseño y desarrollo del producto.

Para cada nivel SIL, las normas EN 5012X son más o menos exigentes, determinando la forma de minimizar las fallas sistemáticas.

Para minimizar los riesgos debidos a las fallas sistemáticas, las técnicas o medidas del software deberán ser de aplicación Mandatoria (M) o Altamente Recomendable (AR) para sistemas con requerimientos de un SIL elevado, como es el caso del software crítico en sistemas ferroviarios.

Referencias

15. Norma EN 50126:2005. Aplicaciones Ferroviarias. Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS). 2005.
16. Engineering Safety Management Guidance. The yellow book. Fundamental and Guidance. Volume 2. Published by Rail Safety and Standards Board. 2007
17. Norma BS EN 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. BSI Standards Publication. 2010
18. Norma EN 50128:2012. Aplicaciones Ferroviarias. Sistemas de comunicaciones, señalización y procesamiento. Software para sistemas y protección del ferrocarril. 2012.
19. Norma EN 50129:2005. Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización. 2005.
20. Engineering Safety Management (The Yellow Book). Volumes 1 and 2 Fundamentals and Guidance. Publicado por Rail Safety and Standards Board. 2007.
21. 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
22. Brosseau, Jim. Software Quality Attributes: Following All the Steps, Clarrus Consulting Group Inc. Noviembre de 2010.
23. Kelly T. A Systematic Approach to Safety Case Management, 04AE-149, 2003.

Datos de Contacto:

Mag. Jorge Esteban Eterovic.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail. jeterovic@ing.unlam.edu.ar

Mag. Domingo Donadello.
Universidad Nacional de La Matanza.
Departamento de Ingeniería e Investigaciones Tecnológicas.
Florencio Varela 1903, (B1754JEC) San Justo, Prov. de Buenos Aires, Argentina.
Tel: (54 11) 4480-8900
E-mail.ddonadel@ing.unlam.edu.ar