Desarrollo de una Guía de Auditoria para Verificar la Calidad del Software Crítico en los Sistemas Ferroviarios

Jorge Esteban Eterovic[1], Domingo Donadello[2]
Departamento de Ingeniería e Investigaciones Tecnológicas, Universidad Nacional de La Matanza,
Florencio Varela 1903, (1754) San Justo, Argentina.
[1]Prof. Mag. Jorge Esteban Eterovic - e-mail: jeterovic@ing.unlam.edu.ar
[2]Prof. Mag. Domingo Donadello - e-mail: ddonadel@ing.unlam.edu.ar
Teléfono: +54-11-4480-8900

Resumen: *En la industria ferroviaria hay una gran cantidad de sistemas críticos que tienen productos de software. Éste 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 esta 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 esta 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 y certifica la calidad del proceso con las normas ISO 9001 y 90003 estaría en condiciones de certificar su producto con la norma EN 50126.*

Palabras Claves: *Software crítico. RAMS. Calidad del software. Proceso de evaluación de calidad. Verificación de la calidad del software.*

Abstract: *In the railway industry there are a lot of critical systems with software products. This software must meet the criteria of RAMS (Reliability, Availability, Maintainability and Safety), under international standards, particularly in EN 50126, used in the European Union. It is therefore necessary to develop a process for evaluating software compliance acquired and / or developed for railway control. Compliance shall be in accordance with the requirements of EN 50126. Whereas this standard describes the stages of software development, and that the organizations involved in the development of software must implement and use a Quality Assurance System in accordance with the ISO 9000, certification is highly recommended in accordance with this standard. The aim of this work is the development of an audit guide to verify the quality of critical software in railway systems, based on the application of the ISO 90003 standard, which provides the guidelines for the application of ISO 9001. This way, a company that develops software for railway systems, and certifies process quality with ISO 9001 and ISO 90003 standards, would be able to certify their product with EN 50126.*

Keywords: *Critical software. RAMS. Software quality. Quality assessment process. Verification of software quality.*

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 (Zárate Fraga, 2012), 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; http://www.cenelec.eu) 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: las EN 50126, EN 50128 y EN 50129 (Norma EN 50126, 2005; Norma EN 50128, 2012; Norma EN 50129, 2005).

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) (Charlwood et al., 2004). 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 de 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" (Brosseau, 2010; Kitchenham et al., 1996; Dromey, 1996; Wallace and Reeker, 2001). Una de las definiciones más aceptadas es (Dromey, 1996): "Calidad es la totalidad de las características del producto que influyen en la capacidad del mismo para satisfacer las necesidades explicitas o implícitas".

En el marco del sistema que lo contiene el software es una herramienta, y ellas deben 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 y, por lo tanto, es importante para la calidad de este 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 en medicina, cirugía, aeronavegación, militar, ferroviaria etc., se han intensificado las actividades de evaluación de la calidad de los productos y artefactos de software (Murphy et al., 2013).

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 basado en la aplicación de la norma IRAM-ISO 90003 (Norma IRAM-ISO 9001, 2008) que da las directrices para la aplicación de norma IRAM-ISO 9001 (Norma IRAM-ISO 90003, 2004).

ELEMENTOS DE 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 inherentes a las actividades de desarrollo, implantación y mantenimiento. Se proporcionan además los criterios correspondientes 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 que 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

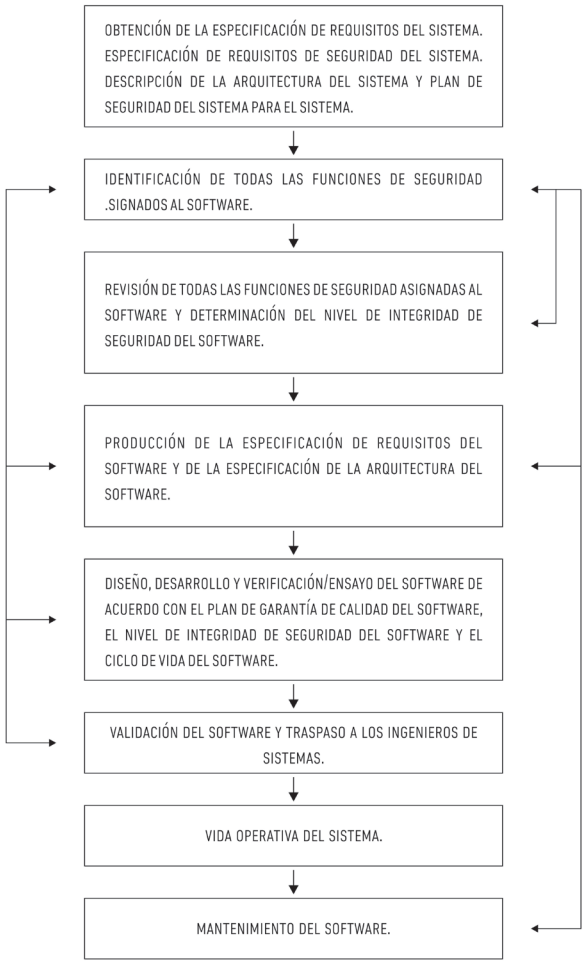

Figura 1 - Etapas funcionales,

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.

Es necesario para proporcionar la defensa cualitativa necesaria contra errores sistemáticos y garantizar que se puede establecer una pista de auditoría

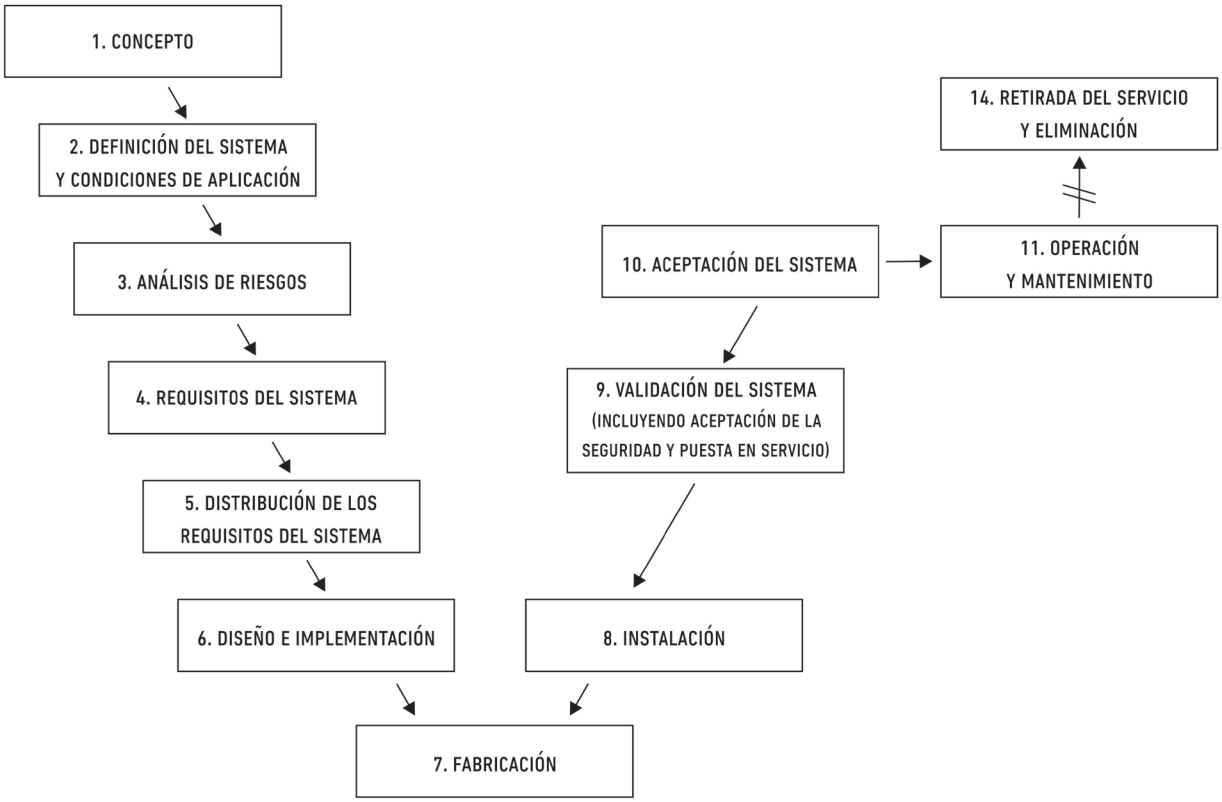

Figura 2 - Ciclo de vida (representación en V).

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 (Norma IRAM-ISO 9000, 2000) 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:

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. Xriterios 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 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.

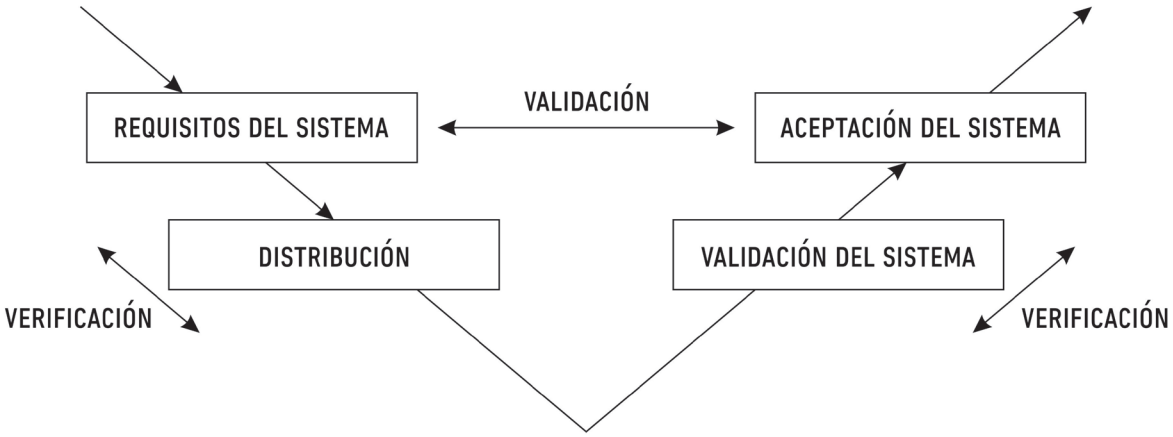

Figura 3 - Validaciones.

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 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 que 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 mismo 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.

Se muestran por separado las tareas de verifica-

ción 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 mismos.

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 resuelvan 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.

RESULTADOS Y DISCUSIÓN

Para cada fase de este ciclo de vida se han definido las principales tareas a ser auditadas. Se resumen en la Tabla 1.

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:

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 MANTENIMIENTOLA 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 EJECUCIÓNLA 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 REALIMENTACIÓNLOS 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 ELIMINACIÓNEL 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.

Tabla 1 - Tareas a auditor.

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.

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:

TÉCNICA/MEDIDA	SIL 0	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 CONFIG. 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	MTO

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.

CONCLUSIONES

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 éstos 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.

AGRADECIMIENTOS

Se agradece a los organizadores del CoNaIISI 2014 por la selección de este trabajo para su publicación y al DIIT – Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza por el apoyo y financiamiento del Proyecto de Investigación.

REFERENCIAS

Zárate Fraga, "Análisis RAMS". Proyecto Fin de Carrera. Universidad Carlos III de Madrid; (Febrero de 2012).

CENELC: Comité Européen de Normalisation Electrotechnique-. http://www.cenelec.eu.

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

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

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

Charlwood, Turner and 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).

Brosseau, Software Quality Attributes: Following All the Steps, Clarrus Consulting Group Inc., (Noviembre de 2010).

Kitchenham, Pfleeger, S. L.: Software Quality: The Elusive Target, Software, IEEE (Volume 13, Issue: 1, pp. 12-21), (Enero de 1996).

Dromey, Cornering the Chimera, Software, IEEE (Volume: 13, Issue: 1, pp. 33-43), (Enero de 1996).

Wallace and Reeker, Software Quality, in Guide to the Software Engineering Body of Knowledge SWEBOK, Abram and Bourque, Eds.: IEEE, pp. 165 - 184, (2001).

Murphy, Wilson, Gartner: Magic Quadrant for Integrated Software Quality Suites, (Julio de 2013).

Norma IRAM-ISO 9001. Sistemas de gestión de la calidad. Requisitos, (2008).

Norma IRAM-ISO 90003. Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software, (2004).

Norma IRAM-ISO 9000. Sistemas de gestión de la calidad. Fundamentos y vocabulario, (2000).

Fecha de Presentación: 15/05/15
Fecha de Aprobación: 08/06/15