Gestión de los Requisitos en Sistemas Críticos de Seguridad

Maurizio Palumbo
Julio de 2015
railwaysignalling.eu, UK
maur.palumbo@railwaysignalling.eu

RESUMEN

Un requisito es una declaración que identifica sin ambigüedad a un producto y a sus características o restricciones operacionales, funcionales o de diseño y que es comprobable, medible y necesario para la aceptación del producto o del proceso [3].

La Ingeniería de los Requisitos tiene por objeto la identificación y el monitoreo de las necesidades de las partes interesadas y de las funcionalidades requeridas por los sistemas.

En este contexto, la *Gestión de Requisitos* trata de la organización de esta información como soporte al proceso de implementación, garantizando su integridad durante todo el ciclo de vida del sistema con relación a los cambios que se produzcan en el propio sistema y en su entorno [19].

Los requisitos desempeñan un papel primordial durante todo el ciclo de vida de desarrollo de un sistema. Sin embargo, un proyecto típico de desarrollo de sistemas de mediana complejidad puede generar alrededor de 2500 distintas declaraciones de requisitos, por lo que para tal fin, se han desarrollado y están disponibles herramientas de Gestión de Requisitos (por ej. IBM DOORS) que sirven de soporte al desarrollo de productos y permiten automatizar el proceso.

¿Por qué la Gestión de Requisitos es tan importante para una organización estructurada cuyo objetivo consiste en producir sistemas críticos de seguridad de alta complejidad?

La Gestión de los Requisitos brinda a cada contratista la posibilidad de evaluar de manera progresiva la solución tecnológica dando seguimiento a su progreso, desde las fases iniciales del proyecto (Diseño Conceptual) hasta las pruebas, validación y operación del sistema.

PALABRAS CLAVES: Ingeniería de Sistemas, Gestión de los Requisitos, Ciclo de Vida de los Requisitos, Ciclo V para aplicaciones ferroviarias, IBM Rational DOORS.

1. INTRODUCCIÓN

La Ingeniería de Sistemas (SE - Systems Engineering) es un método multidisciplinario que permite el desarrollo exitoso de sistemas que como producto final logran satisfacer las necesidades, metas y objetivos de los clientes.

La Ingeniería de los Requisitos tiene por objeto la identificación y el monitoreo de las necesidades de las partes interesadas y de las funcionalidades requeridas por los sistemas.

En este contexto, la *Gestión de Requisitos* trata de la organización de esta información como soporte al proceso de implementación, garantizando su integridad durante todo el ciclo de vida del sistema con relación a los cambios que se produzcan en el propio sistema y en su entorno [19].

La cuestión radica en cómo en realidad se realiza la trazabilidad de esa información y qué ventajas tangibles pueden garantizar para el desarrollo de los sistemas.

Este artículo le guiará a través de las diferentes fases del ciclo V para aplicaciones ferroviarias, incluyendo explicaciones relevantes de los requisitos de cada fase, presentando las actividades requeridas por la Ingeniería de Sistemas para el soporte y control del desarrollo de productos.

2. FUNDAMENTOS DE LA INGENIERÍA DE SISTEMAS

2.1 Definiciones

Un Sistema está constituido por un conjunto de elementos, subsistemas y partes ensambladas que de manera combinada contribuyen al logro de determinado objetivo, incluyendo productos, procesos, personal, instalaciones, servicios y elementos de soporte [3].

En un *Sistema Crítico de Seguridad*, la ocurrencia de un fallo o su mal funcionamiento puede conducir a:

- fallecimientos o lesiones graves de las personas,
- pérdida o daños severos de equipos y propiedades,
- afectación al medioambiente.

Generalmente, tales riesgos se manejan mediante métodos y herramientas de la Ingeniería de la Seguridad, y en particular a través de un índice de medición del desempeño que permite determinar la seguridad requerida por un sistema, denominado *Nivel de Integridad de la Seguridad (SIL - Safety Integrity Nivel).*

Para más detalles acerca de la seguridad, véase el Apéndice A.

La Ingeniería de Sistemas (SE) es un método multidisciplinario que permite el desarrollo exitoso de sistemas que como producto final logran satisfacer las necesidades, metas y objetivos de los clientes.

El Ingeniero de Sistemas generalmente juega un papel primordial en el desarrollo de un sistema, definiendo y asignando requisitos, evaluando ventajas e inconvenientes del diseño, buscando el equilibrio de los riesgos técnicos entre los sistemas, definiendo y evaluando interfaces, realizando la

supervisión de actividades de verificación y validación, así como otras muchas tareas.

2.1 Ciclo de Vida del Desarrollo de Sistemas

El ciclo de vida de desarrollo de sistemas se representa muy bien gráficamente mediante el modelo "V", en el cual se describen las actividades a realizar (y los resultados a obtener) durante cada etapa del desarrollo del producto.

El término “V” viene dado por la forma del diagrama (véase la Figura 1 a continuación), el cual primeramente se divide en dos macro-fases principales (fases 1,3) que están interconectadas por una fase intermedia (fase 2):

1) Descomposición y Definición del Sistema (Diseño)

El lado izquierdo de la "V" representa el diseño de la solución, donde se definen las especificaciones del concepto principal que se trascriben a requisitos del sistema para ser asignados a los diferentes subsistemas en la siguiente etapa. Este es un proceso descendente de arriba hacia abajo.

Como objetivo final de desarrollo de los sistemas se deberá garantizar que se cumplan en su totalidad los requisitos definidos en esta etapa.

2) Implementación (Desarrollo del Hardware y del Software)

La unión de los dos lados de la "V" representa el proceso, a través del cual se transforma el comportamiento especificado, así como las restricciones de las interfaces y de la implementación en acciones de fabricación para crear un elemento del sistema en correspondencia con las prácticas de la tecnología seleccionada con relación tanto al Hardware como el Software.

3) Integración y Recomposición del Sistema (IVVQ)

El lado derecho de la "V" representa la integración de las partes del sistema (las que fueron descompuestas en la etapa anterior para ser desarrolladas de manera independiente unas de otras), así como la exactitud de los aspectos estáticos y dinámicos de las interfaces entre los diferentes elementos implementados. Este proceso es de abajo hacia arriba.

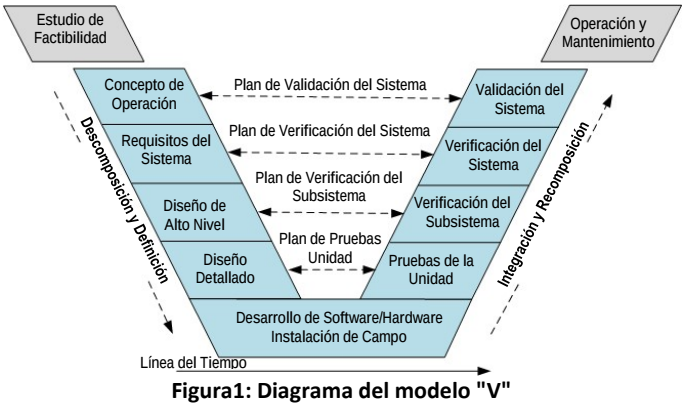

Figura1: Diagrama del modelo "V"

En la Figura 1 se destaca con líneas de flechas bidireccionales cómo las macro fases se enlazan una con otra. La preparación de los planes de verificación y validación es de hecho una tarea que debe ser realizada como parte de la fase de diseño, mientras que las actividades consideradas en estos planes en realidad se ejecutan durante la fase de integración y recomposición.

La descripción detallada de cada subfase del ciclo de vida del sistema no es parte del alcance de este artículo. Para más detalles, véase [1], [9] y [14].

3. GESTIÓN DE LOS REQUISITOS

3.1 ¿Qué es un Requisito?

Un requisito es una declaración que identifica sin ambigüedad a un producto y a sus características o restricciones operacionales, funcionales o de diseño y que es comprobable, medible y necesario para la aceptación del producto o del proceso. [3]

Necesario
El requisito formulado debe ser una característica esencial de carácter físico o de capacidad, o un factor de calidad del producto o proceso.
Conciso
La formulación debe incluir solo un requisito simple y claro. Debe ser conciso, o sea, la declaración no debe incluir explicaciones, fundamentaciones, definiciones o descripciones de uso del sistema.
Completo (de manera independiente)
El requisito formulado debe ser completo sin necesidad de ampliación adicional. El requisito formulado debe ser suficiente.
Coherente
El requisito formulado no debe contradecir otros requerimientos y no puede ser el duplicado de otro.
Inequívoco
Cada requisito debe tener una y solo una interpretación.
Factible
Debe ser posible su implementación a pesar de cualquier limitación del sistema y de su entorno.
Verificable/Comprobable
La formulación de un requisito no debe ambigua o general, sino cuantificable de manera que pueda ser verificable. La verificabilidad de un requisito debe ser consideraba al mismo tiempo que su definición.
Fácil de Seguir
Cada requisito debe ser etiquetado con un único nombre o número de referencia.

Tabla 1: características de un buen requisito

3.3 Tipos de Requisitos de los Proyectos

El conjunto completo de requisitos (técnicos) de un proyecto debe incluir los siguientes tipos de especificaciones:

- **Requisitos Funcionales (FR)**

Los requisitos funcionales describen lo que el sistema debe hacer en términos de funcionalidades:

“El sistema A debe enviar el mensaje <MSG 1> al sistema B”

- **Requisitos No Funcionales (NFR)**

Los requisitos no funcionales describen cómo estas funciones deben ser realizadas. A continuación se presentan algunos NFR típicos:

Desempeño (por ej. Tiempo de Respuesta, Rendimiento, Utilización, Estáticos, Volumétricos), Escalabilidad, Capacidad, Disponibilidad, Confiabilidad, Mantenibilidad, Seguridad, Medioambiental, Integridad de los Datos.

"El Sistema A debe conectarse a la red en 10 segundos desde el momento de su activación"

- **Requisitos de la Interfaz (IR)**

Estos requisitos describen las interfaces entre los elementos de diseño del sistema.

"Los sistemas A y B debe estar conectados físicamente por medio de un cable Ethernet 100baseT"

3.4 Ingeniería y Gestión de los Requisitos

La *Ingeniería de los Requisitos* trata de la identificación, y posteriormente del monitoreo de las necesidades de las partes interesadas y de las funcionalidades requeridas por los sistemas, organizando toda esa información de manera que sirva de soporte a la implementación del sistema.

La *Gestión de los Requisitos* es la actividad a la que concierne el control efectivo de la información relacionada con los requerimientos del sistema, garantizando de manera particular su integridad durante todo el ciclo de vida del sistema en lo que respecta a los cambios que se produzcan tanto en el propio sistema como en su entorno [19].

¿Por qué la Gestión de Requisitos es tan importante para una organización estructurada cuyo objetivo consiste en producir sistemas de alta complejidad? En [9] se menciona un análisis de costo interesante el cual se resume en la Figura 2.

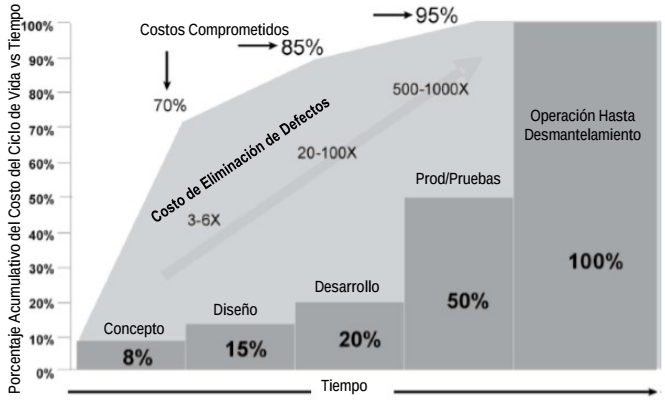

Figura 2: Costo Asignado al Ciclo de Vida vs. Tiempo

La Gestión de los Requisitos brinda a cualquier contratista de proyecto la posibilidad de evaluar de manera progresiva la solución tecnológica del sistema dando seguimiento a su progreso desde la concepción y hasta la operación.

Tal método permite detectar cualquier defecto en etapas tempranas del desarrollo, reduciendo los riesgos y los costos asociados.

3.5 Gestión de los requisitos a lo largo del ciclo de vida

3.5.1 Diseño del Sistema

Los requisitos desempeñan un papel primordial desde las etapas más tempranas de un proyecto. Se deben considerar en orden cronológico las siguientes actividades:

1) Adquisición de los Datos de las Partes Interesadas

Se refiere a la práctica de obtención de la información relativa a los requisitos de un sistema de parte de los usuarios, clientes y de otras partes interesadas (de cualquier entidad que tenga un interés legítimo sobre el sistema), constituyendo las bases de diseño el sistema.

SALIDA

Al final de este proceso se deben entregar de manera formal los siguientes dos documentos:

- La *Especificación de los Requisitos del Cliente y de las Partes Interesadas* que regirán el desarrollo del sistema, las cuales el producto final deberá satisfacer.
- El *Concepto de Operación* que describirá el modo de funcionamiento desde el punto de vista de los operadores y en el cual se resumirán las necesidades, objetivos y características de la comunidad de usuarios del sistema.

2) Formalización de los Requisitos del Sistema

El propósito de esta fase consiste en transformar los requerimientos de las partes interesadas (conjunto de servicio deseados) en requisitos técnicos de un producto específico que podría proveer dichos servicios.

SALIDA

- *La Especificación de los Requisitos del Sistema (SRS - System Requirements Specification)* debe declarar las funcionalidades a lograr por el sistema.

3) Diseño Arquitectónico del Sistema

El desarrollo del diseño arquitectónico se refiere a la síntesis de la organización de los componentes de manera que el sistema pueda satisfacer los requisitos del sistema.

SALIDA

- Se debe entregar una *Descripción de la Arquitectura del Sistema (SyAD - System Architecture Description)* como representación de su estructura, comportamiento e interfaces con otros sistemas externos. Este documento debe incluir la descripción detallada de los componentes del sistema (subsistemas) y de las interfaces (internas y externas), además de un diagrama en bloques (Estructura Desglosada del Sistema, véase la Figura 3) mostrando los componentes principales, las interconexiones y las interfaces externas.

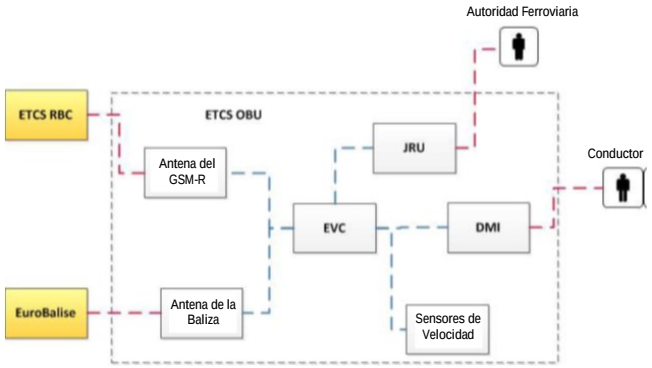

Figura 3: SyAD Simplificado del OBU del ETCS

4) Formalización de los Requisitos de los Subsistemas

Una vez que la arquitectura del sistema ha sido definida, es hora de evaluar los requisitos del sistema contra la estructura de los componentes, analizando la naturaleza de estos requisitos y comprendiendo cuáles funcionalidades deben ser cumplimentadas por un subsistema (A) en lugar de otro (B).

"El sistema ETCS a bordo debe automáticamente informar al maquinista durante el arranque si el ETCS no está apto para el servicio".

Haciendo mención al ERTMS/ETCS, el requisito de sistema anterior guarda relación con el subsistema "DMI", el cual constituye la pantalla de a bordo, o sea, el medio principal de interacción entre el conductor y el sistema.

Esta relación entre el requerimiento original y su evolución natural en un requisito más detallado es parte del proceso de control conocido como "Trazabilidad de los Requisitos". En la sección §4.1 de este artículo está disponible una descripción detallada acerca de la trazabilidad.

SALIDA

Para componente definido, en la Especificación de los Requisitos del Subsistema (SSRS - Sub-System Requirements Specification) se deben declarar las funcionalidades que el subsistema requiere cumplir.

3.5.2 Sistema IVVQ

La finalidad de esta fase se puede resumir como sigue:

- Ensamblaje completo de los elementos que han sido implementados para asegurarse de que son compatibles unos con otros.
- Demostrar que los conjuntos de elementos implementados realizan las funciones previstas y cumplen con los criterios de desempeño y efectividad.
- Detectar defectos/fallos relacionados con las actividades de diseño y ensamblaje, sometiendo los agregados a un enfoque de acciones V&V [14].

La actividad de ensamblaje se une y enlaza físicamente con los elementos implementados. Cada elemento implementado es verificado y validado de manera individual antes de entrar en la fase de integración.

Respecto a los requisitos, la clave radica en la relación que guarda cada aspecto del diseño con relación al procedimiento de prueba que debe ser capaz de garantizar la efectividad de las funcionalidades a que va dirigido. En la sección §4.1 de este artículo se trata con mayor detalle este aspecto de la trazabilidad. (Conformidad con la Trazabilidad).

Sin embargo, ¿cuál es la diferencia entre los conceptos de Verificación y Validación? Los ingenieros generalmente se esfuerzan por unir ambos procesos y términos, que tienen diferentes significados. Véase en el Apéndice B información más detallada sobre la Verificación y la Validación desde el punto de vista de un sistema.

4. PROCESOS DE SOPORTE DE LA INGENIERÍA DE SISTEMAS

La eficiencia de Gestión de los Requisitos guarda relación con la implementación de un número de procesos de soporte de la Ingeniería de Sistemas (SE - Systems Engineering), lo cual contribuye al control del producto en proceso de desarrollo durante su ciclo de vida.

4.1 TRAZABILIDAD DE LOS REQUISITOS

La *Trazabilidad de los Requisitos* se ocupa de proporcionar vínculos entre los diversos requerimientos asociados. Es común diferenciar los conceptos Conformidad y Trazabilidad de la Conformidad.

Trazabilidad de la Conformidad

La trazabilidad de la conformidad se ocupa de proporcionar vínculos entre requisitos de origen y de destino.

Una de las prácticas más comunes de la SE consiste en desarrollar una jerarquía de requerimientos que contribuya a la evolución de cada requisito desde un concepto de alto nivel y hacia una especificación más detallada de las funcionalidades que deben ser cumplidas.

La Figura 4 siguiente constituye un ejemplo genérico de estructura desglosada de los requisitos. La jerarquía se compone de los siguientes niveles:

- Nivel 0: Requisitos de las Partes Interesadas
- Nivel 1: Requisitos del Sistema
- Nivel 2: Requisitos del Subsistema
- Nivel 3: Requisitos de la Unidad

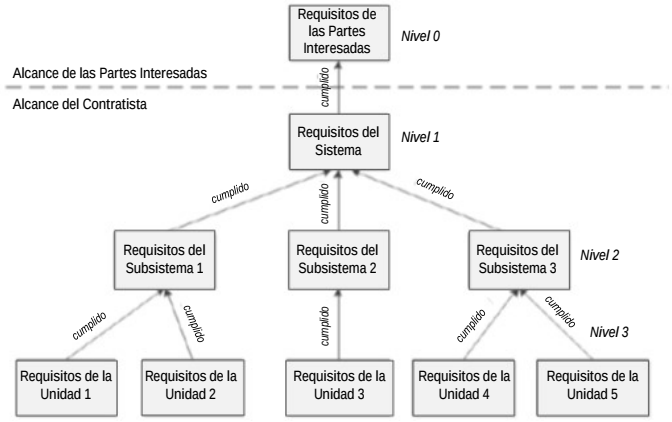

Figura 4: Estructura Desglosada de los Requisitos

Como era de esperar, la ruta (Nivel 0) de la estructura está representada por la Especificación de las Partes Interesadas

que constituye el punto de partida para el desarrollo del producto.

Un Requerimiento de las Partes Interesadas debe ser satisfecho por un requisito de más bajo nivel (Nivel 1) del sistema, el cual a su vez se enlaza con otro requisito del Nivel 2, y así sucesivamente hasta que se alcancen las hojas del árbol (en este caso, el nivel 3).

SALIDA

La *Matriz de Cobertura de los Requisitos* ayuda a mantener la trazabilidad y la actualización del origen de cada requisito.

Cada requerimiento (a menos que sea el de una barra de pan) estará vinculado a un requisito de nivel inferior en el árbol. Por tanto, la matriz es también útil para identificar cualquier falta de conformidad (requisitos no implementados) entre una especificación de requisitos y el destino con que guarda relación.

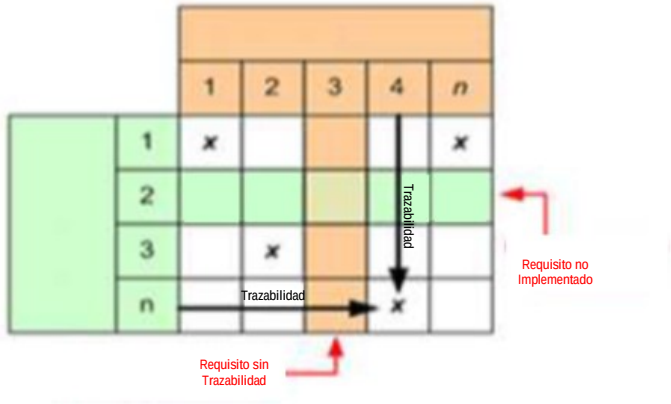

Figura 5: Identificación de requisitos no implementados

Trazabilidad de la Conformidad

Una vez que los requisitos han sido escritos, se deben especificar los métodos para asegurar que el sistema contenga las funciones especificadas para su desarrollado. Existen diferentes métodos que permiten verificar y validar las funcionalidades y determinar si el sistema reacciona de la forma prevista: pruebas, inspecciones, análisis y demostraciones.

Para verificar y validar los requisitos se escriben planes de las pruebas a realizar que incluyen múltiples casos, cada uno de los cuales guarda relación con un estado del sistema para comprobar funciones relacionadas con un conjunto de requisitos.

La conformidad de la trazabilidad garantiza la capacidad de los elementos de la solución técnica para satisfacer los requisitos asignados, mediante uno de los métodos de validación anteriormente mencionados.

SALIDA

La *Matriz de Conformidad de los Requisitos* asocia cada requerimiento particular a uno o más casos de pruebas (o con otros métodos de verificación y validación), con el fin de garantizar la plena conformidad de cualquiera de las especificaciones de requisitos.

4.2 GESTIÓN DE LA CONFIGURACIÓN Y LOS CAMBIOS

La Gestión de la Configuración (CM - Configuration Management) trata de "etiquetar" cada versión sin cambios (congelada) de un sistema, subsistema, documento o cualquier elemento de configuración con un único identificador de configuración, que sirve de base para la definición e implementación de cambios durante el ciclo de vida de desarrollo del producto.

En la gestión de la configuración, la Línea Base constituye una versión congelada del sistema en proceso de desarrollo.

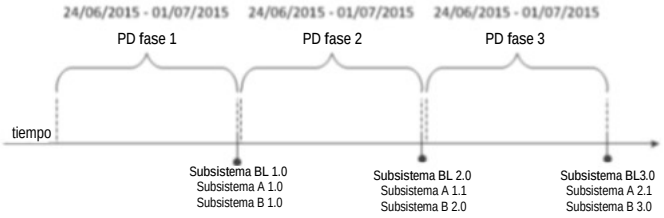

Figura 6: Línea base a lo largo del ciclo de vida del proyecto

La Figura 6 anterior presenta un sistema compuesto por dos subsistemas A y B. Cada uno de ellos se considera un elemento de configuración, por lo tanto, la configuración del sistema será:

- Línea Base del Sistema ***x.y***
  - Subsistema A ***z.w***
  - Subsistema B ***i.q***

Para cada versión de la línea base del sistema, es posible proponer (abrir) una Solicitud de Cambio (CR - Change Request).

El análisis de los cambios permite determinar su impacto sobre los trabajos relacionados con el producto, con la información, con el cronograma y con los costos.

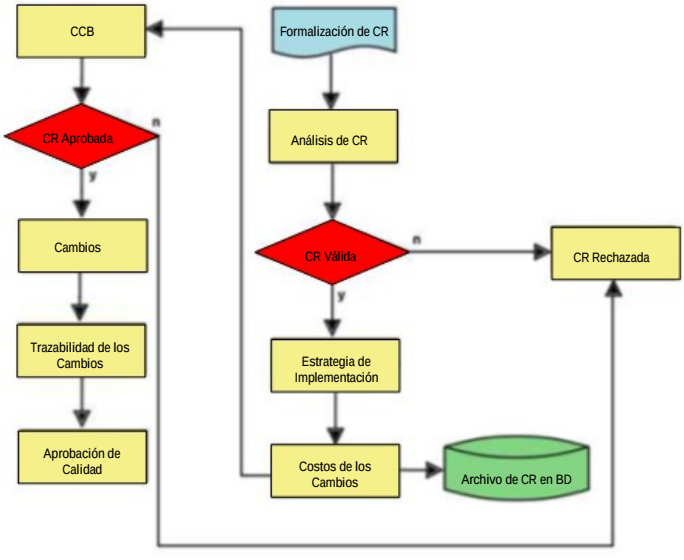

Figura 7: Proceso de Solicitud de Cambio

Posteriormente, en el Consejo de Control de los Cambios (CCB - Change Control Board), al discutir y validar la CR, le será asignado un implementador quien se encargará de realizar la modificación. El cambio realmente tendrá lugar y se aplicará en la siguiente línea base del sistema.

Además, de esta manera, es posible evaluar la separación detallada existente entre dos líneas base del sistema.

5. HERRAMIENTAS PARA LA INGENIERÍA DE REQUISITOS

Para cualquier proyecto de ingeniería de sistemas de dimensiones realistas, la gestión de los requisitos constituye una tarea administrativa intensa, lo cual implica estar en capacidad de:

- Relacionar disímiles documentos;
- Obtener una vista sinóptica de estas relaciones de documentos
- Recuperar información contenida en esos documentos;
- Controlar los cambios realizados en el conjunto de los documentos de una manera coherente.
- Acomodar diversos requisitos para reestructurar diferentes tipos de documentos de requisitos.

A fin de comprender el nivel de la administración de requisitos, debe tenerse en cuenta que un proyecto típico de mediana complejidad de desarrollo de sistemas puede requerir de unas 2.500 declaraciones de distintos requisitos, cada uno de los cuales puede a su vez dar lugar a una serie de documentos de desarrollo y fundamentación [20].

Gestionar manualmente estas cantidades enormes de datos puede ser aún una opción disponible, aunque resulta natural que hoy en día muchas organizaciones estén adoptando herramientas para la gestión de los requisitos que sirvan de soporte al proceso de desarrollo de los sistemas.

Una herramienta de gestión de los requisitos permite:

- Organizar los requisitos en una base de datos compartida, proporcionando acceso a todos los participantes para garantizar el control de los requisitos durante todo el ciclo de vida del proyecto.
- Crear vínculos entre los requisitos relevantes de sistemas y subsistemas;
- Desarrollar análisis de deficiencias, identificar posibles inconsistencias entre lo que se requiere y lo que será satisfecho;
- Dar seguimiento progresivo a los cambios sobre el desarrollo del producto, la vinculación de cualquier actualización de los requisitos y sus impactos con relación al diseño global y los plazos de entrega.
- Verificar que el diseño propuesto satisfaga el desempeño previsto;
- Hacer que las evidencias de conformidad (mediante análisis, dibujos, cálculos, prototipos y los resultados de las pruebas) lleguen hasta los requisitos.

5.1 IBM DOORS

Entre los disímiles software que están disponibles, vale la pena dedicar algunas palabras a DOORS (Dynamic Object Orientated Requirements System), la herramienta de mayor uso en el mundo de desarrollo de los sistemas críticos de seguridad.

DOORS es una herramienta de gestión de requisitos basada en una Arquitectura Cliente-Servidor que incluye funciones para la captura, seguimiento y administración de los requisitos del proyecto.

Los requisitos pueden ser introducidos en una base de datos para darles seguimiento y gestionarlos a lo largo de su ciclo de vida mediante la utilización de una variedad de características, tales como vistas, enlaces y análisis de trazabilidad.

La descripción detallada de esta herramienta no forma parte del alcance de este artículo. Para cualquier información, consulte [11].

6. NOMENCLATURA

CCB	Change Control Board (Consejo de Control de Cambio)
CM	Configuration Control (Control de la Configuración)
DOORS	Dynamic Object Oriented Requirements System
DMI	Display Machine Intefrace (Interfaz Pantalla-Máquina)
ERTMS	European Railway Traffic Management System (Sistema Europeo de Gestión de Tráfico Ferroviario)
ETCS	European Traffic Control System (Sistema Europeo de Control de Tráfico)
EVC	European Vital Computer (Computadora Vital Europea)
FR	Functional Requirements (Requisitos Funcionales)
GSM-R	Global System for Mobile Communications - Railway (Sistema Global de Comunicaciones Móviles - Ferrocarril)
ICD	Interface Control Document (Documento de Control de Interfaz)
IR	Interface Requirements (Requisitos de la Interfaz)
IVVQ	Integration Verification Validation and Qualification (Integración, Verificación, Validación y Cualificación)
JRU	Juridical Recording Unit (Unidad de Grabación Jurídica)
NFR	Non Functional Requirements (Requisitos no Funcionales)
OBU	On-Board Unit (Unidad A Bordo)
RM	Requirements Management/Manager (Gerente/Gestión de Requisitos)
RMP	Requirements Management Plan (Plan de Gestión de Requisitos)
RSM	Requirements Status Metrics (Parámetros del Estado de los Requisitos)
RTM	Requirements Traceability Matrix (Matriz de Trazabilidad de los Requisitos)
RE	Requirements Engineering/Engineer (Ingeniero/Ingeniería de los Requisitos)
SE	System Engineering/Engineer (Ingeniero/Ingeniería de Sistemas)

SIL	Safety Integrity Level (Nivel de Integridad de Seguridad)
SRS	System Requirements Specification (Especificación de los Requisitos del Sistema)
SSRS	Subsystem Requirements Specification (Especificación de los Requisitos del Subsistema)
SyAD	System Architecture Description (Descripción de la Arquitectura del Sistema)
SysML	System Modelling Language (Lenguaje de Modelación de Sistemas)
UML	Unified Modelling Language (Lenguaje de Modelación Unificado)

7. REFERENCIAS

[1] National Aeronautics and Space Admrinstration (NASA) – "NASA Systems Engineering Handbook" (Manual de Ingeniería de Sistemas de la NASA), 2007

[2] Atkins Rail Ltd – "Railway Systems Engineering in Action" (La Ingeniería de Sistemas Ferroviarios en Acción), 2006

[3] ISO/IEC 15939:2007 – "Systems and software engineering - Measurement process" (Los Sistemas y la Ingeniería de Software), 2007

[4] ISO – "ISO 900:2005, Quality Management Systems – Fundamentals and vocabulary" (Sistemas de Gestión de la Calidad - Fundamentos y Vocabulario), 2015

[5] CDC Unified Process Practices Guide – "Requiremets Management" (Guía de la Prácticas de los Procesos Unificados CDC - Gestión de Requisitos),

[6] Dr. Steve Easterbrook (Institute for Software Research) –" Verification and Validation of Requriements for Mission Critical Systems" (Verificación y Validación de Requisitos en Sistemas de Misiones Críticas), 2004

[7] Holt, "UML for Systems Engineering: watching the wheels" (UML para Ingeniería de Sistemas: Observando las Ruedas), Segunda Edición, 2004

[8] Alexander & Stevens - "Writing Better Requirements" (Escribiendo Mejores Requisitos) - Addison-Wesley, 2002

[9] INCOSE – "System Engineering Handbook, a guide for system life-cycle (INCOSE - Manual de Ingeniería de Sistemas, guía para los procesos y actividades del ciclo de vida del sistema - 2010)

[10] Andrew Bourne (Tube Lines Ltd) – "System Requrirements (Gestión de los Requisitos de Sistemas), 2007

[11] IBM – "Software lifecycle management" (Gestión de Ciclo de Vida del Software) disponible: http://www.ibm.com/developerworks/rational/slmoverview.html

[12] Larry A. Fellows (Compliance Automation Inc.) - "10 Steps to Better Requirements" (10 Pasos para Mejores Requisitos), 2003

[13] Department of Computer Science University of Missouri-Rolla - Integrated Analysis of Functional and Non-Functional Requirements", (Análisis de Conflictos entre Requisitos no Funcionales Usando el Análisis Integrado de Requisitos Funcionales y no Funcionales), 2007.

[14] INCOSE –Guide to the Systems Engineering body of knowledge (INCOSE - Guía Informativa sobre Ingeniería de Sistemas), disponible en: http://sebokwiki.org/wiki/System_Requirements

[15] IBM – Rational DOORS getting started (Introducción a Rational DOORS), 2013

[16] Ivy Hooks – "What Happens with Good Requirements Practices" (Qué Pasa con las Buenas Prácticas de los Requisitos) - 2001

[17] T. Hammer, L. Rosenberg, L. Huffman, L. Hyatt (IEEE) – "Measuring Requirements Testing" (Medición de las Pruebas de los Requisitos), 2005

[18] Requirements Experts – Checklist for Common Requirements Risk Factors (Expertos en Requisitos - Lista de Chequeo de los Factores de Riesgo Más Comunes en los Requisitos), 2012

[19] A. Finkelstein (UCL) – "Requirements Management" (Gestión de los Requisitos), disponible en: (http://www0.cs.ucl.ac.uk/staff/A.Finkelstein /talks/ rmfsetut.pdf)

[20] A. Finkelstein (UCL) – "The future of Requirements Management Tools" (El Futuro de la Gestión de los Requisitos), 2010.

[21] EN 50120 – Railway Applications – Communication, signaling and processing systems – Safety related electronic systems for signalling (Aplicaciones Ferroviarias - Sistemas de Comunicaciones, Señalización y Procesamiento - Sistemas electrónicos relacionados con la seguridad para la señalización)

7. BIOGRAFÍA DEL AUTOR

Maurizio Palumbo es el fundador de railwaysignalling.eu, donde también es conocido como *Vesuvius*. Nació en Nápoles (Italia) el 26 de septiembre de 1986. Es un ingeniero en sistemas informáticos, joven curioso, risueño y entusiasta, especializado en señalización ferroviaria y ERTMS/ETCS (Sistema Europeo de Gestión de Tráfico Ferroviario / Sistema Europeo de Control de Tráfico). Ha estado involucrado en actividades relacionadas con sistemas e ingeniería de aplicaciones para tres esquemas de ERTMS (Italia, Dinamarca y Reino Unido) y en un proyecto de metro (Londres, Reino Unido).

8. BIOGRAFÍA DEL TRADUCTOR

José Colón González, graduado de Ingeniero Eléctrico especializado en Señalización y Comunicaciones por la Universidad Estatal de Ingeniería Ferroviaria de Moscú en 1980, donde también obtuvo el grado de PhD en 1988. Trabajó durante más de 25 años en la Empresa de Ingeniera del Ministerio de Transporte de Cuba vinculado a proyectos de ingeniería, consultoría e I+D. En la actualidad trabaja como consultor y traductor técnico independiente especializado en temas ferroviarios.

APÉNDICE A: Nivel de Integridad de Seguridad

La ingeniería de seguridad es una disciplina mediante la cual se garantiza que los sistemas alcancen niveles aceptables de seguridad.

Durante la fase de diseño del sistema, la especificación de los requisitos del sistema se presenta al equipo de ingeniería de seguridad para la realización de un *Análisis de Riesgos*.

Un riesgo se define como una condición, evento o circunstancia que podría provocar o contribuir a un suceso no planificado o indeseable.

Se deberá crear y mantener un *Registro de Riesgos* para todo el ciclo de vida de la seguridad, en el cual se deberá incluir una lista de los riesgos identificados, junto con su clasificación y la información de control [21].

A cada nivel de integridad de la seguridad (SIL) le corresponde un valor relativo de reducción de riesgos que proporciona una función de seguridad y se usa para especificar un nivel objetivo de reducción de riesgos. En términos sencillos, el SIL es una medición del desempeño requerido por una función instrumentada de seguridad".

Las normas de seguridad para aplicaciones ferroviarias se especifican completamente en [21].

APÉNDICE B: Verificación y Validación

La verificación se encarga de demostrar si un producto de cualquier modelo de sistema y dentro de su estructura ha sido realizado conforme a los requisitos. En otras palabras, la finalidad del proceso de verificación es la de confirmar si los ***requisitos del diseño*** especificado han sido cumplidos por el sistema.

Este proceso también proporciona la información requerida para las medidas correctivas que deben corregir las no conformidades detectadas en el sistema realizado.

La validación es la confirmación, a través de evidencias objetivas, de que los ***requisitos de las partes interesadas*** para un uso o aplicación específica han sido cumplidos.

Un sistema validado, por lo tanto, es capaz de cumplir su uso final previsto, así como sus objetivos generales y específicos (es decir, satisfacer los requisitos de las partes interesadas) en el entorno operacional.

Una acción de validación aplicada a un elemento de ingeniería incluye lo siguiente:

- La identificación del elemento en el que la acción de validación se realizará.
- La identificación de la referencia que define el resultado esperado de la acción de validación.
- Cualquier elemento de ingeniería puede validarse mediante una referencia específica por comparación (véase la Figura 8 siguiente).

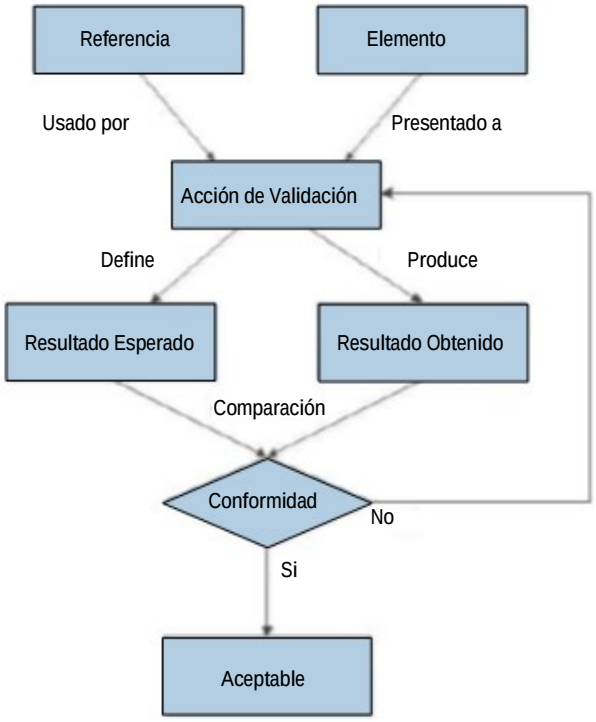

Figura 8: Proceso de Validación

Según estas definiciones, desde el punto de vista del proceso, las dos actividades pueden ser de naturaleza similar, pero los objetivos son en esencia diferentes.

Desde el punto de vista de la ingeniería, es esencial confirmar que el producto ha sido realizado conforme a sus especificaciones de diseño ***(¿fue realizado correctamente?***), mientras que desde el punto de vista del cliente, el interés radica en si el producto final hará lo que el cliente espera ***(¿se realizó el producto correcto?***) [1].

Además, es importante comprender la naturaleza interactiva de estas actividades que pueden repetirse en cada etapa del ciclo de vida del sistema, a fin de proporcionar una evidencia progresiva de la satisfacción de los requisitos (y las medidas correctivas para la solución de las no conformidades) durante el desarrollo del producto (véase la Figura 9 siguiente).

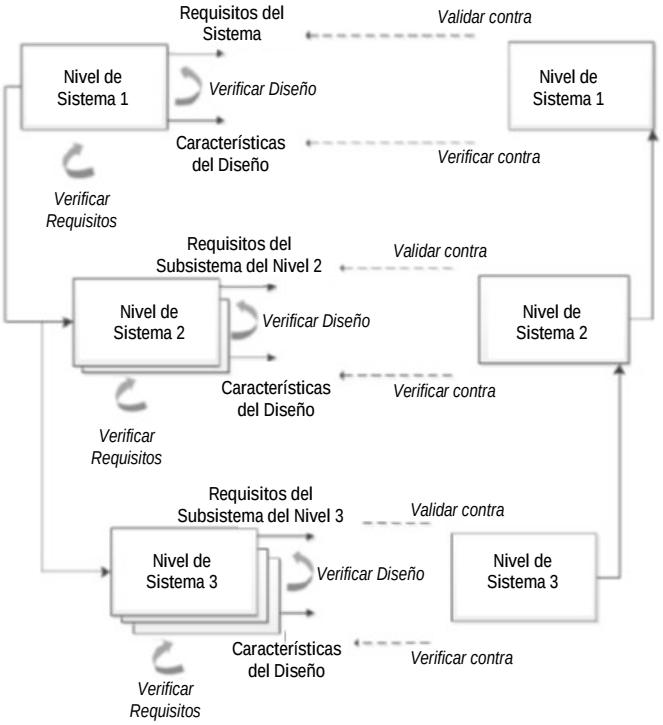

Figura 9: Interacciones de los Procesos de Validación y Verificación