Universidad del Desarrollo
Facultad de Ingeniería

PROPUESTA METODOLOGICA PARA DISEÑO DE UN SISTEMA DE MISIÓN CRÍTICA

CRISTIAN NAVARRO ALVAREZ

PROFESOR GUÍA: HÉCTOR VALDÉS-GONZÁLEZ, PhD

PROYECTO DE GRADO PRESENTADO A LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD DEL DESARROLLO PARA OPTAR AL GRADO ACADÉMICO DE MAGÍSTER EN INGENIERÍA INDUSTRIAL Y DE SISTEMAS

SANTIAGO – CHILE
2020

Universidad del Desarrollo
Facultad de Ingeniería

PROPUESTA METODOLOGICA PARA DISEÑO DE UN SISTEMA DE MISIÓN CRÍTICA

POR: CRISTIAN NAVARRO ALVAREZ

Proyecto de Grado presentado a la Comisión integrada por los profesores:

PROFESORES GUÍA: HÉCTOR VALDÉS-GONZÁLEZ, PhD
OSVALDO BENAVENTE, MIIS

PROFESOR INTEGRANTE 1: JOSÉ LUIS SALAZAR NAVARRETE, PhD

PROFESOR INTEGRANTE 2: CRISTIÁN MEJÍAS CONTRERAS, MBA

Para completar las exigencias del Grado de Magíster en Ingeniería Industrial y de Sistemas.

Diciembre, 2020
Santiago, Chile

DECLARACIÓN DE ORIGINALIDAD

Por medio de la presente, declaro que el trabajo titulado: **PROPUESTA METODOLOGICA PARA DISEÑO DE UN SISTEMA DE MISIÓN CRÍTICA**, que presento a la Universidad del Desarrollo de Chile, es de mi autoría (o co-autoría) y no ha sido publicado previamente, ni está siendo considerado para publicación bajo otra filiación. En igual sentido, declaro que el trabajo de tesis y su contenido, son originales y que todos los datos y referencias a trabajos ya publicados con anterioridad han sido debidamente identificados, referenciados o citados en el documento, y que estas citas han sido incluidas en las referencias bibliográficas. Afirmo, asimismo, que los materiales presentados no se encuentran protegidos por derechos de autor; y en caso de que así lo estuvieran, me hago responsable de cualquier litigo o reclamo relacionado con la violación de derechos de propiedad intelectual, exonerando de toda responsabilidad a la Universidad del Desarrollo de Chile.

Finalmente, me comprometo a no someter este trabajo (o parte de este), a consideración en ninguna revista o congreso para publicación sin contar con la aprobación y haber pasado el debido proceso de revisión en Universidad del Desarrollo. En caso de que un artículo sea aprobado para su publicación, autorizo a la Universidad del Desarrollo a incluir dicho artículo en sus revistas, y a reproducirlo, editarlo, distribuirlo, exhibirlo y comunicarlo en el país y en el extranjero, por medios impresos, electrónicos, Internet o cualquier otro medio, para propósitos científicos y sin fines de lucro.

CRISTIAN NAVARRO ALVAREZ

Firma

A mis padres

Nelda Álvarez y Jaime Navarro

Mis primeros profesores en el aula de la vida, quienes me han brindado su cariño y cuidado incondicional.

A mis hijitas, quienes son la fuente de mi inspiración;

Leonor Sofía, la bebé más pequeñita de papá, mi Sol Radiante que alegra y alumbra mi camino.

y a

María Paz Valentina, mi hija mayor, mi estrella en el firmamento, mi río de paz.

AGRADECIMIENTOS

Primeramente, agradecer a mi familia; mis padres y mis hijas, porque son ellos quienes me han apoyado y motivado a alcanzar los logros de mi vida.

Agradezco a la Universidad del Desarrollo por haberme acogido en sus filas y haberme dado la oportunidad de continuar con mi crecimiento profesional, gracias a todas las personas que participaron de este importante proceso; gracias al Sr. Federico Casanello quien fue director al inicio del programa y a la Srta. Paulina García coordinadora de postgrado quien facilitó el desarrollo de la actividad. Gracias a cada uno de los profesores quienes con paciencia y esfuerzo pusieron su conocimiento a mi disposición.

Quiero agradecer también, a la profesora Alejandra Basualto por las revisiones y observaciones realizadas a mi anteproyecto de grado, sus sugerencias fueron una importante guía y marcaron el destino hacia donde se encaminó este trabajo.

Asimismo, agradezco al Sr. Héctor Valdés González, director de postgrado, y a los profesores Osvaldo Benavente, José Luis Salazar Navarrete y Cristián Mejías Contreras quienes han brindado orientación al desarrollo de la metodología. Sus observaciones han sido una pieza clave para la correcta ejecución de este documento.

Gracias a mis amigos y compañeros de estudios por los momentos que compartimos, tareas que juntos realizamos y la confianza generada en el grupo.

Y muy especialmente agradezco a la ingeniera Mónica Pino por su revisión, aporte y amistad brindada.

Fueron ustedes los responsables, cada uno con su aporte me dieron la fuerza y motivación para llegar al final de este proceso. Gracias por todo.

PROPUESTA METODOLOGICA PARA DISEÑO DE UN SISTEMA DE MISIÓN CRÍTICA

Cristian Navarro Álvarez

Bajo la supervisión del Profesor Héctor Valdés-González en la Universidad del Desarrollo de Chile

Resumen

Este trabajo presenta un sistema de comunicaciones de movilización ferroviaria para trasporte de pasajeros de la ciudad de Santiago, enmarcado en su fase de diseño, caracterizado por poseer alta disponibilidad a pesar de presentar fallos de servicio. El objetivo de este proyecto es proponer un método de desarrollo de la arquitectura del sistema de comunicaciones ferroviario para la entrega de altos niveles de prestaciones. Para lograrlo se utiliza un enfoque cuantitativo, con iteraciones sobre una estrategia basada en definir, medir, analizar, mejorar y controlar, además del método de análisis deductivo conocido como diagramas de bloques de fiabilidad, y el método inductivo para análisis de vulnerabilidades del sistema llamado análisis de efectos y modos de fallos. Los resultados muestran que la arquitectura propuesta para el sistema de comunicaciones logra el nivel de servicios requeridos según especificaciones de contrato. En conclusión, la metodología propuesta resulta viable y de fácil aplicación, permitiendo el diseño de un sistema de comunicaciones de altas prestaciones que contribuye a asegurar la oferta de transporte y reduce las pérdidas por accidentes e indisponibilidad de infraestructura. Esté método, dada sus características genéricas, puede ser utilizado para el diseño de otras prestaciones industriales de misión críticas.

Palabras claves: Transporte ferroviario; DMAIC; RBD; FMEA; Indisponibilidad de infraestructura

ÍNDICE GENERAL

ÍNDICE DE TABLAS

.

ÍNDICE DE FIGURAS

GLOSARIO DE ACRÓNIMOS

Análisis de modos de fallo y efectos (FMEA)

Control de Trenes Basado en Comunicaciones (CBTC)

Controlador de área (DRCU)

Definir, medir, analizar, mejorar y controlar (DMAIC)

Diagrama de bloques de fiabilidad (RBD)

Estación base de radio (RBS)

Red multiservicio de Metro (RMS)

Sistema de misión crítica (SMC)

Tiempo medio entre fallos (MTBF)

Tiempo medio para reparación (MTTR)

Transceptor de estación base (BST)

Transporte guiado urbano (UGT)

1 INTRODUCCIÓN

En los últimos años el aumento de la demanda de transporte y del tránsito vial han traído como consecuencia, particularmente en las ciudades grandes, incrementos en la congestión, demoras, accidentes y problemas ambientales, bastante mayores que los considerados aceptables por los ciudadanos [Bull, A. y Thomson, I. (2001)].

Para responder de modo adecuado a la demanda y evitar el colapso vial y ambiental, se requiere organizar un sistema de transporte público que brinde un servicio efectivo [Bull, A. (2003)]. Un aporte significativo puede provenir de los sistemas de transporte guiado urbano (UGT), ya sean Metro, Tranvía o Trenes de Cercanía, los cuales con una frecuencia de pasada por las estaciones regular y control centralizado, permiten mantener una oferta de transporte controlada y reducir los tiempos de viaje.

A fin de entregar un mayor nivel de servicio a los pasajeros, la operación ferroviaria se debe realizar de forma continua y sin interrupciones involuntarias, es decir, se deben evitar fallos mayores que puedan dejar el sistema UGT indisponible.

Estos avanzados medios de transporte no son ajenos a nuestra realidad, en la ciudad de Santiago de Chile, Metro de Santiago ha desarrollado el proyecto UGT más ambicioso de su historia, la construcción de las Líneas 6 y 3.

Este proyecto supone uno de los mayores hitos de infraestructura en ejecución a nivel nacional, estas dos nuevas líneas, aumentan de 103 kilómetros a 140 kilómetros la red de Metro.

Línea 6 tendrá 16 km de extensión, atendiendo a la Comunas de Cerrillos y Pedro Aguirre Cerda, en tanto, la Línea 3 poseerá 18 estaciones y 21 km de extensión, llegando a las Comunas de Quilicura, Conchalí e Independencia, entre ambas integran más de un millón de usuarios a la red, a través de sus 28 estaciones.

En cuanto a los tiempos de viajes, se reducen entre un 60% y un 70%, esto a través de la incorporación de nuevas tecnologías, por ejemplo, en el caso de los trenes, las

nuevas características guardan relación con un rodado de acero, que además de ser más económico posee una mayor capacidad de transporte.

Otros aspectos importantes en la construcción de estas nuevas líneas son:

- Evacuación Frontal, lo que permite que las personas con disminuida capacidad de movilidad puedan bajar de los trenes de una forma más segura.
- Conducción sin Operador, automatizando los procesos mediante la utilización de tecnología de última generación.
- Trenes más anchos y con aire acondicionado, con el objetivo de dar mayor capacidad de traslado y comodidad a los pasajeros.
- Escaleras mecánicas y ascensores en todas las estaciones y niveles.
- Peajes Bidireccionales.
- Sistemas de pagos automáticos
- Electrificación de altura, lo que otorga una mayor seguridad a los pasajeros en alguna situación de emergencia.
- Comunicación tren-tierra directa desde el pasajero a centro de control de Metro.

Las Líneas 6 y 3 de Metro son construidas bajo la estrategia de línea desatendida, es decir, sin conductores en los trenes, y con muy poco personal de estaciones. Todo es automatizado, desde el movimiento de trenes, hasta la apertura de las puertas de andén.

Este trabajo de grado se enmarca en el proyecto para la construcción del sistema UGT; Líneas 6 y 3 de Metro de Santiago, donde el operador ferroviario ha salido a licitar los sistemas que constituyen el medio de transporte. El alcance específico del trabajo es el sistema de comunicaciones RCOM, el cual ha sido adjudicado para suministro a una empresa contratista especializada.

En las Línea 6 y 3, donde no hay personal de Metro abordo del tren, el sistema RCOM toma un rol preponderante, ya que pasa a constituirse como la interfaz entre los pasajeros a bordo del tren y los operadores del centro de comunicaciones de Metro. Ante una evacuación, desmayo o algún otro evento inesperado, el RCOM es el nexo existente entre los pasajeros y Metro, contribuyendo de esta forma a la seguridad del pasajero sobre todo en condiciones de emergencia.

En este escenario, nace la necesidad de desarrollar una metodología de diseño, llamada desde ahora metodología para diseño de un sistema de misión crítica (SMC). Esta metodología debe asegurar que el sistema RCOM suministrado, cumple los altos estándares de servicios exigidos por el operador en su pliego de licitación y por consiguiente asegura la conectividad entre pasajero y operadores de Metro ante cualquier emergencia.

1.1 Altos niveles de servicio en sistemas de misión crítica

Para razonar de qué forma se debe diseñar un sistema de alto nivel de servicio, es necesario establecer que se entiende por alto nivel de servicio, cuáles son los factores que inciden en esta cualidad y cuáles son las variables que permiten medirla.

Una vez lograda la claridad del concepto y su aplicación, surge el siguiente cuestionamiento: ¿Cuáles son las actividades que deben ser consideradas en un proceso de diseño del sistema de comunicaciones requerido?

En efecto, el contrato de suministro del sistema de comunicaciones licitado establece el nivel de prestaciones requerido, lo que hace necesario establecer dichas actividades con claridad en pos de un diseño óptimo.

1.2 Breve discusión de la literatura

Desde la segunda mitad del siglo XX, los avances científicos y tecnológicos se han desarrollado de forma vertiginosa y consecutiva, la constante evolución en busca de satisfacer necesidades de forma eficiente y segura ha complejizado la tecnología y

los servicios que ella provee. Desde esta perspectiva, un sistema es un compuesto integrado de personas, productos y procesos que permiten satisfacer una necesidad u objetivo declarado [The defense acquisition university press fort belvoir. (2001)], en esta misma línea se entiende por sistemas de misión crítica, a aquellos sistemas considerados de carácter esencial, estos realizan operaciones indispensables, en muchas ocasiones relacionadas con la seguridad, el fallo de estos sistemas incluso puede afectar el bienestar de la sociedad. Algunos ejemplos de sistemas de misión crítica son; centrales eléctricas, gran minería o medios de transportes masivos. Metro de Santiago, con su función primordial de trasladar de forma rápida y segura a miles de pasajeros cada día, puede ser categorizado como sistema de misión crítica. Lo que implica que debe mantener una operación constante y segura en todo momento.

El Sistema ferroviario necesidad de asegurar el correcto funcionamiento.

La Rocket de Stephenson fue una de las primeras locomotoras de vapor, en 1829 se introdujo en Inglaterra y resulto ser la innovación tecnológica precursora del crecimiento ferroviario, desde este punto de la historia se llega a las actuales redes de transporte, las cuales operan haciendo uso de distintas tecnologías en busca de la automatización, mejoras en la operación y reducción de riesgos que puedan afectar la seguridad del sistema [Bracciali A. (2016)].

En este escenario donde existe la necesidad de diseñar, construir y operar sistemas cada día más complejos, la ingeniería de sistema es el proceso interdisciplinario de gestión de la ingeniería que permite desarrollar soluciones considerando el ciclo de vida del sistema y la integración de sus diversas partes [The defense acquisition university press fort belvoir. (2001)].

Por otra parte, cada vez hay más conciencia de que los elementos del sistema tendrán vulnerabilidades conocidas y desconocidas y que a pesar de esta situación, el sistema

debe seguir cumpliendo (posiblemente degradado) con su funcionalidad, rendimiento y objetivos de seguridad.

Con el propósito de abordar dichas vulnerabilidades y prevenir las pérdidas del nivel de servicio del sistema, nace el concepto de aseguramiento.

El Aseguramiento aparece dada la necesidad de anticipar el comportamiento del sistema ante la aparición de fallos o eventos inesperados. Para ello, es necesario implementar metodologías que permitan anticipar los errores, fallos y consecuencias antes de que estos se produzcan, de forma tal de garantizar que el sistema cumple con las especificaciones establecidas por el cliente, tanto en operación normal, como degradada o emergencia, de este modo se asegura una calidad continua y a lo largo del tiempo.

El aseguramiento se puede definir desde varios puntos de vista y con foco en diversas áreas de interés, por ejemplo:

- En ingeniería de software y sistema se define el aseguramiento desde la perspectiva de la calidad, como; la parte de la gestión de calidad enfocada en brindar confianza en que los requerimientos especificados serán logrados [ISO/IEC 15288. (2008)].
- El Committee on National Security Systems (EE.UU) describe el aseguramiento como; la medida de la confianza de que las características de seguridad, las prácticas, los procedimientos y la arquitectura de un sistema de información cumplen con rigor la política de seguridad [Consejo Nacional de Seguridad Social (CNSS), (2003)].
- Otra definición, con foco en la seguridad funcional, es la dada por el Ministerio de defensa del Reino Unido en su estándar “Safety Management Requirements for Defence Systems” que muestra el aseguramiento como; la confianza basada en evidencia y procesos, que demuestran que se han cumplido los requisitos de seguridad [MODUK. DEF STAN 00-56. (2007)].

- Desde la perspectiva de la Confiabilidad, la guía de ingeniería de sistemas MITRE, indica que el aseguramiento de la misión significa que los operadores logran la misión, continúan sus procesos críticos y protegen a las personas y bienes bajo ataques internos / externos (físicos y cibernéticos), cambios ambientales u operacionales imprevistos o mal funcionamiento del sistema. A lo largo del ciclo de vida, la ingeniería de sistemas para el aseguramiento permite lograr una misión en diferentes circunstancias [MITRE. (2014)].

En resumen, el aseguramiento del sistema es la confianza justificada de que el sistema funciona como está previsto y está libre de vulnerabilidades durante todo su ciclo de vida [National Defense Industrial Association (NDIA). (2008)].

El aseguramiento de sistema implica abordar las vulnerabilidades del sistema a través de un enfoque de ciclo de vida más completo y reducirlas a través de un conjunto de tecnologías, procesos y actividades.

Ingeniería de Confiabilidad aplicada a los sistemas

La confiabilidad representa la capacidad de un sistema o componente para funcionar en las condiciones establecidas durante un período de tiempo específico, en otras palabras, es la probabilidad de éxito de la función en el tiempo [Creus, A. (2005).]

La ingeniería de confiabilidad permita evaluar el nivel de servicio que se puede esperar de un sistema y proponer acciones orientadas a robustecer el sistema en busca de minimizar las paradas, fallas catastróficas y el mal funcionamiento.

Entre las principales herramientas de la ingeniería de confiabilidad se ubica el diagrama de bloques de fiabilidad (RBD), herramienta que utilizada para modelar la arquitectura del sistema y para evaluar el desempeño esperado [Conradie, P., Fourie, C., Vlok, P. y Treurnicht, N. (2015)]. Otro importante instrumento usado en los estudios de confiabilidad es el análisis de modos de fallo y efectos (FMEA), que es un método orientado a identificar las vulnerabilidades y consecuencias de los fallos sobre la operación del sistema.

Métodos y herramientas de diseño

Teniendo en cuenta la necesidad de modelar, analizar y evaluar la confiabilidad de las arquitecturas que resulten del trabajo de diseño, se han seleccionado por su fácil uso, las siguientes herramientas de la confiabilidad:

RBD desarrolla un modelo que representa la arquitectura del sistema (serie o paralelo) resaltando sus redundancias, el análisis matemático de los diagramas de bloque de fiabilidad utiliza técnicas soportadas en álgebra Booleana y "sets" de combinaciones, entre otros. Además, permite realizar análisis de sensibilidad para identificar los elementos que ante un fallo generan alto impacto en el nivel de servicio.

FMEA es un enfoque paso a paso para identificar las fallas posibles del diseño. Este método es de carácter inductivo, lo que implica que parte desde el fallo de los elementos o funciones del sistema y busca las consecuencias posibles de estos eventos [Moubray, J. (1997)], [Doshi, J. (2017)].

Los estudios de RBD y FMEA se conjugan para generar un modelo de arquitectura preliminar del sistema, luego evaluando el modelo con los datos para medir desempeño; tiempo medio entre fallos (MTBF) y tiempo medio para la reparación (MTTR) se logra estimar la disponibilidad que puede alcanzar el sistema bajo estudio. [Renpenning, F. (2004)].

La metodología definir, medir, analizar, mejorar y controlar (DMAIC) aplicada al diseño permite satisfacer las expectativas y requisitos que debe cumplir el sistema, gracias a la fácil identificación de problemas y a su proceso iterativo de mejora, es la metodología seleccionada para anidar dentro de sus etapas las herramientas de confiabilidad destinadas al análisis, modelamiento y evaluación del rendimiento. [Nedeliaková , E., Štefancová, V. y Hranický, M. (2018)]

Finalmente, este set de herramientas permite la gestión de las principales variables que impactan el nivel de servicio y aplicadas en conjunto con los principios de

aseguramiento de sistemas, hacen posible desarrollar soluciones considerando el ciclo de vida del sistema, la integración de los distintos subsistemas que constituyen el sistema global de transporte y la medición de desempeño [The defense acquisition university press fort belvoir. (2001).]

¿Cómo abordan la problemática en el resto del mundo?

El diseño de sistemas confiables a nivel mundial es abordado generalmente por medio de aplicación de regulaciones que proponen conceptos y principios para la implementación de funciones de seguridad. Una función es relacionada a la seguridad porque ante un fallo de ella, existe riesgo de sufrir un accidente. Por ejemplo, el sistema de frenado de un vehículo es considerado de seguridad técnica, por lo tanto, la probabilidad de fallo del frenado es evaluada y si esta medida es inferior a un objetivo establecido, entonces se deben implementar mitigaciones destinadas a robustecer la función, generalmente dando redundancia a los elementos críticos de ella.

En el ámbito ferroviario internacional, las normas se han venido consignando junto con la evolución del sistema ferroviario. Actualmente, las normativas ferroviarias son las encargadas de entregar los principios y conceptos que debe seguir los distintos actores de la industria ferroviaria, entre las principales normativas a nivel mundial se encuentran las CENELEC (europea) y AREMA (americana).

Cabe destacar que, para no imponer un freno a la evolución de la tecnología, las normas ferroviarias no imponen objetivos, ni procesos rígidos que deban ser realizados por los fabricantes, más bien, proponen conceptos, criterios y principios destinados a alinear a la industria hacia una convergencia de criterios de diseño [Bracciali A. (2016)].

¿Cómo lo abordan en Chile?

En la regulación chilena no existe una norma a cumplir para la implementación de sistemas ferroviarios. Tampoco existe la figura de autoridad ferroviaria, quien dé el visto bueno para la puesta en servicio de un sistema. En la práctica, cada proyecto sigue normas definidas que implementa en los pliegos de licitación y es recibido en conformidad por las propias empresas operadoras quienes dan la aceptación del sistema para salir a explotación. Para el caso de la Empresa de los Ferrocarriles del Estado, utilizan un mix entre normas europeas y americanas. Por otra parte, Metro de Santiago utiliza normas europeas.

Resultados o casos de éxito en Chile y el mundo.

La evolución del transporte ferroviario ha aumentado su eficiencia y seguridad. El rápido desarrollo de tecnologías emergentes como la comunicación, la informática y los sistemas inteligentes se ha integrado a las infraestructuras existentes y se ha adoptado en las nuevas aplicaciones. La nueva generación de transporte ferroviario utiliza en gran medida las redes de comunicaciones para gestionar sus procesos de automatización. Por ejemplo, en la actualidad existen sistemas de Control de Trenes Basado en Comunicaciones (CBTC) para gestionar el tráfico de la línea, en estos el sistema toma conocimiento de la posición exacta de un tren en una línea con mayor precisión que en los sistemas de control tradicionales y, con ello, la gestión del tráfico ferroviario se lleva a cabo de una forma más eficiente y segura [IEEE 1474.1.(1999)].

Los sistemas CBTC modernos permiten diferentes grados de automatización, los cuales van desde un modo de operación manual con protección para operación, hasta la operación desatendida, es decir, sin conductor [Institution of Ralway Signal Engineers (IRSE). (2009)].

En las líneas desatendidas, dada la falta de conductor a bordo del tren, es requisito constar con sistemas de comunicaciones que faciliten la interacción entre el operador ferroviario y los pasajeros. Esta comunicación tiene por función principal

hacer frente a situaciones degradadas y guiar a los pasajeros ante emergencias. Entonces se puede decir que, a mayor nivel de automatización, mayores niveles de seguridad, funcionalidad y rendimiento se hacen necesarios.

Existen varios proyectos de sistemas de UGT con altos requerimientos de comunicaciones implementados en diversos países. La Tabla 1.1 presenta algunos de ellos.

Tabla 1.1: Ejemplos de sistemas ferroviarios con uso intensivo de comunicaciones,

Elaboración propia, 2020.

Lugar	Línea	Proveedor	Solución
Metro de Madrid	1, 6	BOMBARDIER	CITYFLO 650
Metro de Singapur	North-East Line	ALSTOM	Urbalis
Metro de Barcelona	9	SIEMENS	Trainguard MT CBTC
São Paulo Metro	Tiradentes Monorail Extension Line 2	BOMBARDIER	CITYFLO 650
Metro de Santiago	6, 3	THALES	SelTrac RF

Al revisar los casos de sistemas que hacen un uso intensivo de las comunicaciones en su operación, se observa que existen varios de estos implementados en distintos países del globo, sin embargo, a pesar de este hecho, la información acerca de los procesos y metodologías de diseño que poseen sus redes de comunicaciones es confidencial. Lo cual va de la mano con la importancia de los sistemas de misión crítica.

Finalmente, y habiendo revisado las principales contribuciones que aportan o han aportado a la línea de trabajo de este proyecto, es posible indicar que una oportunidad de desarrollo se encuentra en el hecho que no existe, para el caso de sistemas de comunicaciones ferroviarias, información suficiente o certeza, respecto de la disponibilidad de una metodología de desarrollo de la arquitectura de sistemas de alta disponibilidad para transporte ferroviario de personas.

Lo que autoriza la siguiente como contribución para este proyecto de grado.

1.3 Contribución del trabajo

Habiendo recorrido las bases teóricas fundamentales para este estudio, cabe mencionar que la principal motivación para realizarlo ha sido aportar una metodología que permita cumplir con las restricciones que determina el contrato de Comunicaciones considerando el ciclo de vida del sistema y su entorno de diseño. Se propone entonces una metodología de diseño SMC con base en iteraciones sobre estrategias DMAIC, RBD y FMEA aplicadas al transporte ferroviario de pasajeros. En este sentido, el trabajo contribuye a la comprensión de los factores que inciden en el proceso de diseño; las variables claves y consideraciones de entorno para el desarrollo de sistemas de transporte ferroviario.

Adicionalmente, este trabajo podría ser un aporte para un proyecto mucho más ambicioso destinado a la implementación de una normativa Chilena de seguridad ferroviaria.

De acuerdo con lo mencionado anteriormente, este trabajo considera los siguientes puntos como objetivo general y objetivos específicos.

1.4 Objetivo general

Proponer un método para el desarrollo de la arquitectura de un sistema de comunicaciones, con base en iteraciones sobre estrategias DMAIC, usando herramientas RBD y FMEA aplicadas al sistema de transporte ferroviario de pasajeros para el logro de altos niveles de prestaciones, es decir, cumplir objetivos de desempeño cuantitativos basados en la medición de disponibilidad del sistema.

1.4.1 Objetivos específicos

- Investigar los factores que inciden directamente en el diseño del sistema
- Analizar como los factores impactan el desempeño del sistema
- Formular un método de diseño de arquitectura para un sistema de comunicaciones ferroviario que cumpla altos niveles de servicio.

1.5 Propuesta metodológica

Paradigma y Diseño: Se ha optado por utilizar una metodología cuantitativa, basada en la estrategia DMAIC, la cual, por medio de un proceso iterativo de mejora va dando robustez a la arquitectura del sistema. Por otra parte, dentro del proceso DMAIC, se utiliza la herramienta RBD para modelar el desempeño del sistema además se analizan sus debilidades haciendo uso de la herramienta FMEA [Conradie, P., Fourie, C., Vlok, P. y Treurnicht, N. (2015)].

Como paso previo al análisis cuantitativo es necesario conocer acerca los factores que inciden en el diseño desde una mirada de la calidad y con foco en minimizar los errores humanos que podrían ocurrir en el proceso. Por otra parte, también se debe conocer los conceptos básicos asociados a la teoría de confiabilidad de sistemas, sus variables, y técnicas de evaluación.

Población sobre la que se efectuará el estudio: La totalidad de elementos que constituyen el sistema de comunicaciones RCOM, es decir, unidades controladoras de radio, red backhaul, estaciones base, estaciones móviles.

El estudio se realiza en base a las variables que permiten modelar, analizar y evaluar el desempeño del sistema a diseñar; es decir, el tiempo medio entre fallos (MTBF), el tiempo medio para reparar (MTTR) y la disponibilidad del sistema (A) [Alavian, P., Eun, Y., Liu, K., Meerkov, S. y Zhang, L. (2019)].

Los datos de MTBF para los equipos son suministrados por los proveedores, los valores de MTTR están basados en la experiencia y recomendaciones de los fabricantes y la disponibilidad es un parámetro que se calcula en función de las variables MTBF y MTTR [UNE-EN 61703. (2016)].

Entorno: Proyecto de construcción de las Líneas 6 y 3 de Metro de Santiago. Líneas que operan bajo una estrategia desatendida, es decir, trenes sin conductor y un mínimo de personal en estaciones, donde prima la automatización.

Intervenciones: Una vez conocidos los factores y variables que impactan el desempeño del sistema.

El nivel de servicio o desempeño del sistema es evaluado por medio de la disponibilidad, la que se calcula mediante el método de los RBD, este método muestra la arquitectura del sistema a través de bloques (serie o paralelo) que representan los diferentes elementos que constituyen el sistema [Hasan, O., Ahmed, W., Tahar, S. y Salah, M. (2015)]. El diagrama de bloque se establece para la función que debe realizar el sistema y que en caso de falla impacta en el nivel de servicio.

Luego del modelo brindado por RBD, el FMEA estudia de manera sistemática los posibles fallos de los elementos constituyentes del sistema e identifica el impacto de cada una sobre el nivel de servicio ofrecido.

Para la previsión y evaluación del nivel de servicio, cada equipo es representado en la RBD con sus valores de MTBF y MTTR. Finalmente, en caso de que la disponibilidad del sistema no cumple con los objetivos exigidos, se modifica la arquitectura de la red hasta lograr el desempeño requerido.

Plan de análisis de datos: Con la información de entrada, MTBF y MTTR de los elementos que constituyen el sistema, se da inicio al ciclo iterativo de; modelamiento, análisis y estimación del comportamiento de la arquitectura bajo evaluación. Finalmente, este resultado responde a la problemática y permite identificar cual es la arquitectura del sistema que da cumplimiento a los requisitos contractuales exigidos.

Ética: los datos utilizados como entrada a los modelos son suministrados por los fabricantes de equipos quienes los certifican mediante pruebas. Los métodos y herramientas para el diseño son utilizadas conforme el estado del arte de la técnica. Los datos resultantes de los análisis no han sido manipulados de forma arbitraria para conseguir un resultado particular.

1.6 Organización y presentación de este trabajo

Esta tesis posee 4 capítulos, los cuales en términos generales presentan:

Capítulo 1: Marco conceptual del proyecto, contextualizándolo, proponiendo objetivos y discutiendo desde la literatura la pertinencia del foco de la investigación, su contribución, y presentando a su vez un marco metodológico para su desarrollo e implementación.

Capítulo 2: Se presenta formalmente la problemática del proyecto y la o las metodologías asociadas.

Capítulo 3: Se muestran análisis y resultados de la propuesta del trabajo.

Capítulo 4: Finalmente las conclusiones generales derivadas de este trabajo, y una dirección para la investigación futura, la cual considera aquellas preguntas no contestadas durante el desarrollo de este trabajo, se presentan en este capítulo.

Referencias generales

Anexos

2 PRESENTACIÓN DEL PROBLEMA Y METODOLOGÍA SELECCIONADA

Como se ha mencionado anteriormente, la operación ferroviaria se debe realizar de forma continua y sin interrupciones involuntarias. Por lo tanto, los sistemas que constituyen el UGT deben cumplir altos estándares de disponibilidad y fiabilidad, los cuales están definidos a modo de requisitos contractuales en los pliegos de licitación emitidos por el operador Metro de Santiago.

Este proyecto de grado se enmarca en el proceso de diseño de un sistema de comunicaciones tren-tierra, llamado RCOM, el cual radio transmite mensajes entre vehículos ferroviarios y la sala de control central del operador ferroviario.

El sistema RCOM es parte de un grupo de sistemas –Vías, señalización, Trenes, Energía y Comando y Supervisión– que interactuando en conjunto constituyen un sistema UGT, Línea 6 y 3 de Metro de Santiago.

La Disponibilidad Global del sistema de transporte, es el producto de las disponibilidades de cada uno de los sistemas que lo constituyen [Creus, 2005], es decir, la pérdida de operatividad de cualquiera de dichos sistemas va en detrimento de la oferta de transporte, y por lo tanto, al nivel de servicio ofrecido por el operador.

En esta sección se presenta formalmente el problema, se detallen sus principales componentes, se analiza la metodología y herramientas a utilizar para lograr una solución adecuada.

2.1 Presentación de la problemática del proyecto

Del párrafo anterior se desprende que un fallo en el sistema RCOM puede generar pérdida total o parcial de la operación ferroviaria, por lo tanto, se puede decir que los fallos de dicho sistema son fuente de variabilidad sobre la oferta de transporte entregada por Metro, por consiguiente, la pérdida de RCOM tiene efectos negativos sobre la disponibilidad global del sistema, afectando la regularidad de la circulación de trenes.

No hay que olvidar que el sistema a diseñar permite la comunicación entre los pasajeros y el personal de Metro en una Línea implementada bajo una estrategia desatendida, es decir, donde no hay conductor a bordo del tren para atender a los pasajeros en caso de evacuación, desmayo o algún otro evento inesperado, como por ejemplo; un apagón o incendio. En este escenario el sistema de comunicaciones toma un nivel mayor de importancia, dada su participación en la seguridad del pasajero sobre todo en condiciones de emergencia.

Con la consigna planteada anteriormente, nace la necesidad de diseñar un sistema RCOM que sea suficientemente robusto para lograr el nivel de servicio exigido por contrato, tal de asegurar la conectividad entre tren y centro de comunicaciones en todo momento.

Al analizar la problemática a resolver, se observa que previo a realizar el diseño de RCOM, es necesario conocer los factores que contribuyen al logro de un diseño exitoso. Además de conocer estos factores, también se hace necesario investigar las variables que permiten medir el desempeño del sistema.

Finalmente, se presenta la metodología la cual considera los factores que inciden en el diseño, las variables a gestionar y las actividades a realizar para lograr el sistema de comunicaciones que asegura la conectividad entre pasajero y operadores de metro ante cualquier emergencia o evento inesperado.

2.2 Factores y variables para la metodología de diseño de un SMC

Antes de presentar la Metodología para el diseño de un SMC, es importante investigar los factores y variables que se deben desarrollar para conseguir un diseño adecuado y estructurado, permitiendo que los requisitos de las partes interesadas se logren en todas las etapas del ciclo de vida del proyecto.

La culminación exitosa en calidad, tiempo y costos, con un sistema aceptable, seguro y confiable, depende en gran medida del factor humano, es decir, expectativas y comportamientos que son esenciales durante un proceso de diseño ya que pueden

influir positiva o negativamente en el resultado, por ejemplo; mal entender los requerimientos técnicos, patrones de comportamiento, falta de competencias o sin fin causas más, todos estos errores pueden afectar el proceso de diseño.

Dicho esto, la metodología de diseño debe estar amparada bajo la protección de procesos, procedimientos y buenas prácticas orientadas al logro del aseguramiento de sistema [Engineering Safety Management. (2007)] y por consiguiente a minimizar el error humano.

La gestión de ingeniería, gestión de interfaces, gestión de la configuración, gestión de integración, procesos de verificación y validación, son todas buenas prácticas que soportan el diseño, dan garantía y contribuyen al desarrollo de un sistema óptimo [Government of New South Wales Transport. (2015)].

Los otros factores, de carácter ambiental, operacional y técnicos que influyen el diseño del sistema son considerados en la etapa 1 "definición del sistema" de la metodología de diseño SMC.

Respecto a las variables que permiten evaluar y gestionar el desempeño de un sistema, estas son; fiabilidad, mantenibilidad y disponibilidad [UNE-EN 61703. (2016)].

Fiabilidad: es la capacidad para funcionar de la forma prevista, sin fallos, durante un intervalo de tiempo determinado y en condiciones determinadas. Es representada por la función R(t).

Para equipos electrónicos como los utilizados en este trabajo, la fiabilidad viene dada por la función.

$$\text{Ec. 1: } R(t) = \exp(-\lambda t)$$

De la cual se llega a:

$$\text{Ec. 2: } MTBF = \frac{1}{\lambda}$$

Donde,

MTBF es el tiempo medio entre fallos y λ la tasa de fallos para los elementos.

En este trabajo los valores MTBF para cada elemento que constituye el sistema son suministrados por los fabricantes.

Mantenibilidad: es la capacidad de un elemento, bajo determinadas condiciones de uso, de ser restaurado a un estado en el que pueda realizar la función requerida, cuando el mantenimiento se realiza bajo determinadas condiciones y usando procedimientos y recursos establecidos.

De forma análoga a la medida de fiabilidad, la mantenibilidad se describe por medio del parámetro tiempo medio para reparar (MTTR), descrito por la siguiente ecuación:

Ec. 3: $$MTTR = \frac{1}{\mu}$$

Donde,

MTTR es el tiempo medio entre fallos y μ corresponde a la tasa de reparación.

Disponibilidad: capacidad que tiene un elemento de hallarse en situación de realizar una función requerida en condiciones determinadas en un momento dado o durante un intervalo de tiempo señalado, suponiendo que se faciliten los recursos externos requeridos.

La disponibilidad A es una componente de la fiabilidad y de la mantenibilidad.

Ec. 4: $$\text{Disponibilidad} = \frac{MTBF}{MTBF + MTTR}$$

2.3 Herramientas utilizadas para la construcción de la metodología de diseño SMC

La metodología de diseño SMC, es una integración de tres herramientas destinas para mejorar la calidad de los procesos. Por una parte, tenemos la RBD destinada a modelar el desempeño del sistema, por otra la FMEA, la cual facilita la evaluación de las debilidades de la arquitectura y finalmente se tiene la herramienta DMAIC la cual se encarga de anidar dentro de sus etapas a la RBD y FMEA, permitiendo la necesaria iteración para el logro del sistema óptimo.

2.3.1 DMAIC

El DMAIC es una metodología estructurada para la solución de problemas usada en todo tipo de procesos, es la herramienta de Six Sigma, enfocada en la mejora incremental de procesos e implementación de proyectos de mejora. Es un acrónimo cuyas siglas en inglés significan Definir, Medir, Análisis, Mejorar y Controlar. [Nedeliaková , E., Štefancová, V. y Hranický, M. (2018)].

En este trabajo, el método DMAIC es el pilar sobre el cual se desarrolla la metodología de diseño SMC, y se utiliza a modo de ciclo de vida de diseño, donde se Define el sistema, se Mide su comportamiento en configuración de arquitectura base, luego se Analizan sus debilidades, se Mejora la arquitectura base, y finalmente se Controla la nueva arquitectura mejorada. Este proceso es iterativo, es decir, se realiza hasta conseguir el logro del nivel de servicio requerido.

2.3.2 RBD

Los diagramas de bloques de confiabilidad nos permiten modelar las relaciones (serie, paralelo) de falla de sistemas complejos y sus subcomponentes. Se utilizan ampliamente para cuantificar la fiabilidad del sistema [Hasan, O., Ahmed, W., Tahar, S. y Salah, M. (2015)].

[MIL-HDBK-338B:1998] **sistema serie,** en este todos sus componentes deben funcionar para que el sistema opere. Se representa como muestra la Figura 2.1.

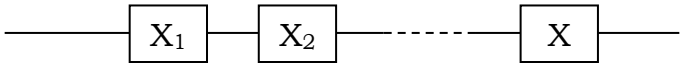


Figura 2.1: Fiabilidad de un sistema serie,

Elaboración propia, 2020

En un sistema serie se cumple que la fiabilidad del sistema viene dada por:

Ec. 5: $$R(t) = \prod_{i=1}^{n} R_i(t)$$

Donde,

R(t) = fiabilidad del sistema

Ri(t) = fiabilidad del elemento I

y las tasas de fallo y de reparación totales de la serie se pueden obtener por medio de las siguientes aproximaciones:

Ec. 6: $$\lambda tot = \sum \lambda i$$ Ec. 7: $$\mu tot = \frac{\sum \lambda i}{\sum \frac{\lambda i}{\mu i}}$$

Siendo $\lambda_1,\ldots,\lambda_n$ las tasas de falla de cada equipo, y $\mu_1,\ldots,\mu_n$ sus tasas de reparación. Si todos los elementos de la serie son iguales, entonces se tiene que:

Ec. 8 $\lambda = n\lambda$.

y por lo tanto, el MTBF de la seria con elementos iguales es:

Ec. 9: $$MTBF = \frac{1}{n\lambda_i}$$

Sistema paralelo en él basta con que una de las ramas esté operativa, para que la función esté disponible, ver Figura 2.2. La fiabilidad del sistema paralelo viene dada por:

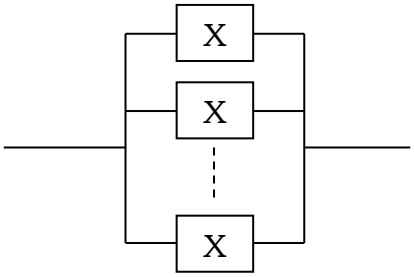


Figura 2.2: Fiabilidad de un sistema paralelo,

Elaboración propia, 2020

Ec. 10 $$1 - R(t) = \prod_{i=1}^{n} (1 - R_i(t))$$

Donde,

R(t) = fiabilidad del sistema

Ri(t) = fiabilidad del elemento I

y las tasas de fallo y de reparación totales del conjunto paralelo se pueden obtener por medio de las siguientes aproximaciones:

Ec. 11: $$\lambda tot = \prod \frac{\lambda i}{\mu i} \sum \mu i$$ Ec. 12: $$\mu tot = \sum \mu i$$

Siendo $\lambda_1, \ldots, \lambda_n$ las tasas de falla de cada equipo, y $\mu_1, \ldots, \mu_n$ sus tasas de reparación.

En este trabajo el RBD se utiliza anidado dentro de la etapa 2 “Medir el desempeño del sistema” de la metodología de diseño de SMC.

2.3.3 FMEA

El análisis de modos de fallos y efectos es una herramienta de calidad que se utiliza para identificar fallas potenciales y efectos relacionados en los procesos y productos.

La investigación demuestra que es posible lograr una mejora continua en la calidad mediante la implementación efectiva de FMEA [Doshi, J. (2017)].

En este trabajo se utiliza para registro del proceso de análisis el formato de FMEA presentado en la Tabla 2.1

Tabla 2.1: Formato FMEA,

Elaboración propia, 2020.

Elemento	Función	Modo de fallo	Efecto en la operación	Categoría de fallo	Mitigación
Nombre del componente a analizar	Descripción de la función que desempeña el	Descripción de la falla del componente /	Efecto del tipo de falla a nivel operativo	Significativo, Mayor, Menor	Descripción de las medidas para limitar el riesgo

La Tabla 2.2 presenta los criterios para la clasificación de los impactos de los fallos sobre la operación. A mayor impacto, se requirieren más medidas de mitigación.

Tabla 2.2: Categoría de fallos,

Elaboración propia, 2020.

Categoria de fallo	Definición
Significativo	Pérdida total de conectividad
Mayor	Pérdida parcial de conectividad
Menor	No cumple los criterios para ser considerado Significativo o Mayor

En resumen, el FMEA es un método para identificar de forma temprana los posibles fallos del sistema, así como sus efectos. Entonces se utiliza para generar cambios de diseño tal de mitigar el efecto de los fallos.

En este trabajo el FMEA se utiliza anidado dentro de la etapa 3 “Análisis del funcionamiento del sistema” de la metodología de diseño de SMC.

2.4 Metodología de diseño de un SMC

Utilizando como marco filosófico los principios del aseguramiento de sistema, y por otra parte, la rigurosidad de la ingeniería de confiabilidad, se da inicio al proceso de diseño con foco en el logro de un sistema con alto nivel de servicio.

La metodología para diseño SMC, se establece en base a iteraciones sobre la estrategia DMAIC, modelamiento del desempeño con RBD y análisis de las consecuencias de los fallos por FMEA. Estas tres herramientas actuando en conjunto, permiten estimar el comportamiento del sistema, tanto en operación normal, como degradada, asegurando de esta forma el comportamiento del sistema ante eventos inesperados. Ver Figura 2.3.

La aplicación de este método de diseño permite evaluar de forma cuantitativa, hasta qué punto se puede confiar en que el sistema funcione correctamente, garantizando la operación y seguridad del sistema ferroviario, por consiguiente, la metodología propuesta permite asegurar que el diseño realizado alcanza el nivel de servicio exigido por Metro.

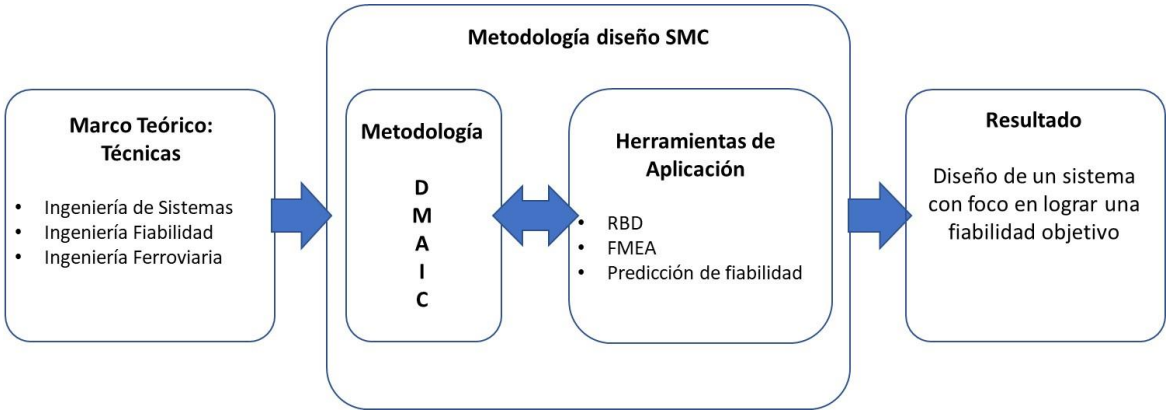


Figura 2.3: Técnicas, métodos y herramientas,
Elaboración propia, 2020

La metodología de diseño SMC se plantea de forma jerárquica en tres niveles: nivel método, nivel etapas y nivel detalle.

Esta estructura permite una fácil identificación de todos los procesos involucrados partiendo desde una visión general hasta llegar a un nivel específico donde se estudia el detalle de la implementación.

La metodología empieza con una definición conceptual de la técnica a utilizar en el trabajo, dada la necesidad de utilizar un enfoque iterativo y hacia la calidad, se selecciona la aplicación de DMAIC.

Luego se expone el desglose del concepto DMAIC, dando origen al segundo nivel, llamada “Etapas”. En este punto se desarrolla, a modo general, cada una de las etapas que constituyen al DMAIC, y se observa la aplicación metodológica como un proceso integrado desde la etapa 1 a la etapa 5.

Finalmente, se llega al nivel de detalle, donde cada una de las etapas definidas en el nivel anterior, es examinada de forma desagregada y planteada como proceso independiente con sus respectivos; objetivos, entradas, salidas y herramientas a utilizar. Ver Figura 2.4

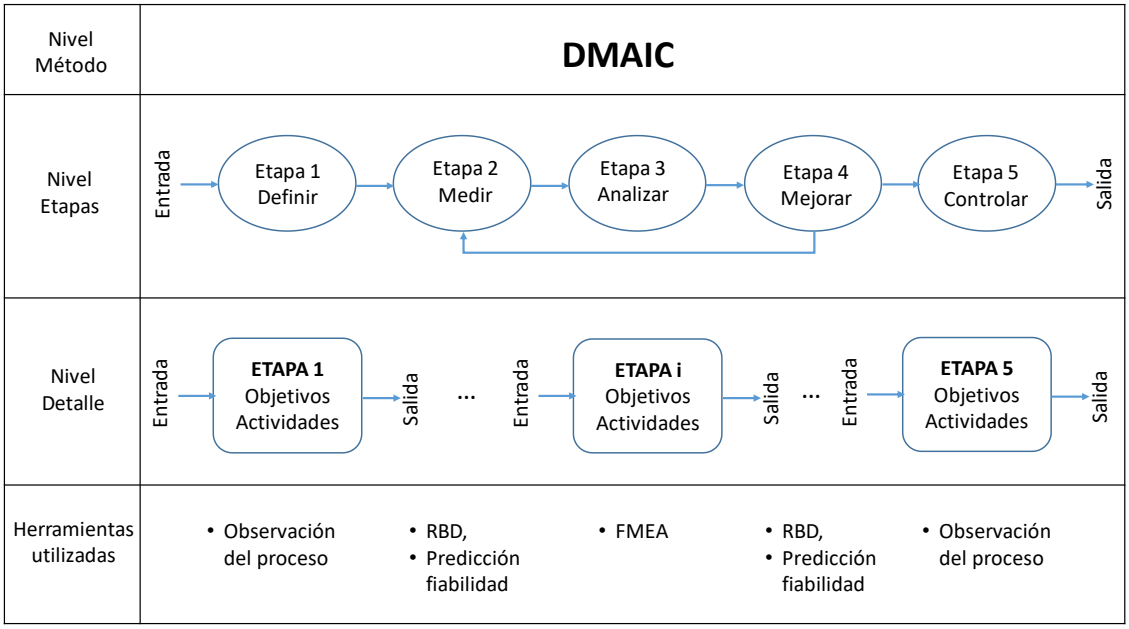


Figura 2.4: Desglose metodología diseño SMC,

Elaboración propia, 2020.

DMAIC es una metodología enfocada en la mejora incremental de procesos. Por lo tanto, esta herramienta permite realizar varias iteraciones en el proceso de diseño del sistema, hasta alcanzar el objetivo o nivel de servicio establecido.

La metodología DMAIC se estructura en 5 etapas, las cuales, en este caso particular, han sido definidas de forma tal de permitir el diseño de sistema deseado. Ver Figura 2.5

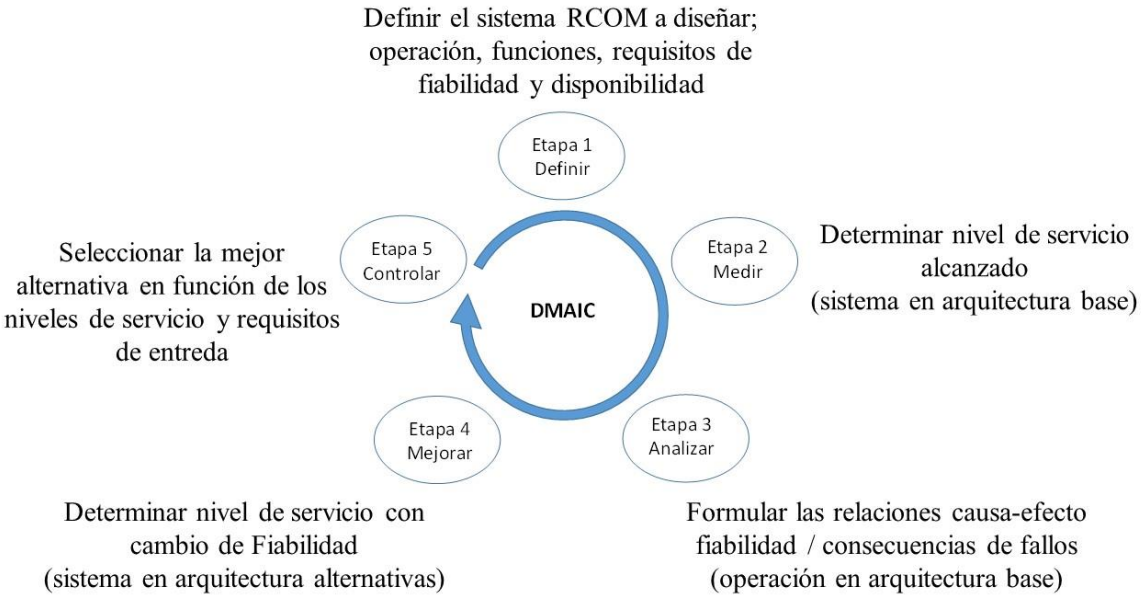


Figura 2.5: DMAIC adaptada al método de diseño SMC,
Elaboración propia, 2020.

Basado en el estándar [ISO/IEC 15288:2008], cada una de las etapas de la metodología DMAIC es redefinida como un proceso que es descrito en términos de los siguientes atributos:

- Título, el cual transmite el alcance de la etapa como un todo.
- Objetivo de la etapa, meta a alcanzar en la etapa.
- Entradas, son los requisitos que deben estar cubiertos para permitir el desarrollo de la etapa.
- Salidas, los resultados esperados para alcanzar los objetivos de la etapa.
- Actividades, conjunto de tareas necesarias para el desarrollo de la etapa.
- Herramientas, corresponde a los instrumentos (RBD, FMEA, Poisson) utilizados en la ejecución de las actividades de la etapa.

Ver Figura 2.6

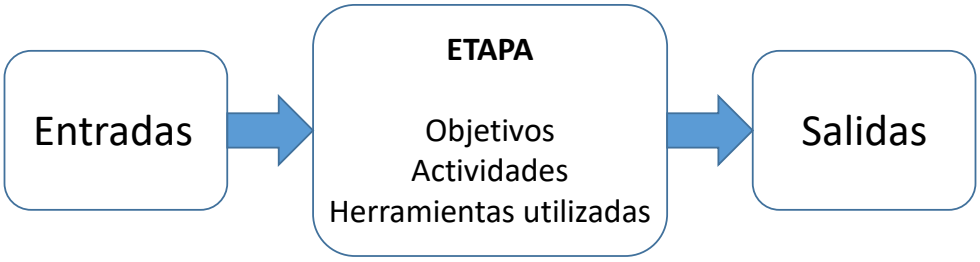


Figura 2.6: Etapas DMAIC descritas como proceso,
Elaboración propia, 2020

2.4.1 Etapa 1: Definir el sistema

Objetivo E1

Describir el sistema RCOM a diseñar, a fin de conocer su operación, funciones y objetivos de disponibilidad a alcanzar.

Entradas

Toda la información y los datos relevantes necesarios para cumplir las actividades definidas para la etapa, por ejemplo, declaraciones de alcance, especificaciones técnicas y finalidad del proyecto.

Actividades

Describir el sistema en relación a:

- Alcance, contexto y objetivos
- Vida útil
- Supuesto de operación
- Criticidad
- Perfil de misión
- Descripción funcional del sistema

Salidas

- Descripción conceptual del sistema

Herramientas

- Observación del proceso

2.4.2 Etapa 2: Medir desempeño del sistema base

Objetivo E2

Determinar la disponibilidad del sistema en arquitectura base.

Se entiende por arquitectura base a la arquitectura preliminar, sobre la cual se realizan iteraciones a fin de dar robustez al sistema.

Entradas

- Toda la información y datos relevantes provenientes de la etapa 1
- Descripción conceptual del sistema

Actividades

- Definir variables y parámetros a utilizar para el modelo y medición de la disponibilidad del sistema
- Modelar el funcionamiento del sistema
- Estimar la fiabilidad que alcanza el sistema en la arquitectura base

Salidas

Caracterización del sistema;

- Arquitectura base
- Tasa de fallo de sistema

Herramientas

RBD, predicción de fiabilidad.

2.4.3 Etapa 3: Analizar el funcionamiento del sistema

Objetivo E3

Formular las relaciones causa-efecto existentes entre la fiabilidad y las consecuencias de los fallos sobre la operación del sistema en arquitectura base

Entradas

Descripción conceptual del sistema

Caracterización del sistema

Actividades

Realizar un análisis de modos de fallos y sus efectos sobre la operación.

Salidas

Efectos de los fallos sobre la operación y mantenimiento

Herramientas

FMEA

2.4.4 Etapa 4: Mejorar el sistema

Objetivo E4

Brindar robustez al sistema.

Establecer cumplimiento de objetivos de desempeño.

Entradas

Descripción conceptual del sistema

Caracterización del sistema en arquitectura base

Efectos de los fallos de la arquitectura base

Actividades

Establecer arquitecturas alternativas con niveles de fiabilidad mejores a la arquitectura base.

Para las arquitecturas alternativas:

- Modelar el funcionamiento del sistema
- Estimar el desempeño que alcanza el sistema en la arquitectura alternativa

Salidas

Niveles de servicio alcanzados para las arquitecturas alternativas

Herramientas

RBD, predicción de fiabilidad

2.4.5 Etapa 5: Selección de la arquitectura a implementar

Objetivo E5

Seleccionar la arquitectura final en función de los niveles de servicio a alcanzar

Entradas

Caracterización de sistemas en arquitectura alternativas

Efectos de los fallos sobre la operación y mantenimiento

Niveles de servicio alcanzados por las arquitecturas alternativas

Actividades

- Evaluar los resultados de las diferentes arquitecturas alternativas
- Seleccionar la mejor arquitectura en función del desempeño

Salidas

Arquitectura a implementar

Herramientas

Observación del resultado

Finalmente, el método para diseño de SMC realiza las iteraciones necesarias hasta logra una arquitectura con un alto nivel de servicio que de cumplimiento a los requerimientos exigidos al sistema.

2.5 Conclusión y análisis del capítulo

Luego de investigar los factores; humanos, ambiental, operacional y técnicos que influyen el diseño del sistema y las variables que permiten medir su desempeño; MTBF, MTTR y Disponibilidad. Se opta por componer la metodología de diseño de SMC, la cual se construye sobre un proceso DMAIC.

Por otra parte, anidando dentro del proceso DMAIC, se utiliza la herramienta RBD para modelar el desempeño del sistema en la arquitectura bajo evaluación. Después de realizar el modelo, se analizan las debilidades de la arquitectura por medio de la herramienta FMEA.

Una vez conocido el desempeño y las debilidades de la arquitectura bajo evaluación, el proceso DMAIC genera una nueva iteración a fin de corregir las debilidades detectadas.

Finalmente, las metodologías seleccionadas para el proceso de diseño son de fácil aplicación y permiten lograr una arquitectura robusta que cumpla las exigencias definidas en los contratos de Metro respecto al nivel de servicio del sistema y por consiguiente asegure la conectividad entre pasajero y operadores de metro ante cualquier emergencia o evento inesperado.

3 RESULTADOS

Este capítulo presenta los resultados de la aplicación de la metodología para diseño SMC al sistema RCOM.

A fin de lograr una visión a nivel de Línea del desempeño requerido, antes de iniciar el análisis especifico al sistema RCOM, se presentar un resumen del sistema UGT y los sistemas que lo constituyen.

Un sistema Ferroviario se puede definir como un conjunto de sistemas y componentes, unidos de forma organizada, para lograr una funcionalidad especificada de transporte. El sistema responde a entradas para generar salidas especificadas, mientras actúa recíprocamente con el entorno.

De acuerdo a su tecnología, funcionalidades y condiciones ambientales en las cuales opera, cada sistema ferroviario instalado posee sus particularidades, es decir, es una aplicación específica. A pesar, de la existencia de dichas particularidades, los sistemas ferroviarios poseen funciones comunes, las cuales permiten realizar modelos que buscan asegurar el comportamiento del sistema.

Basado en [CLC/TR 50126-2. (2007)], se presenta una estructura típica para un sistema de transporte ferroviario, esta es esencialmente un desglose de los subsistemas físicos. Los subsistemas propuestos en el segundo nivel suelen ser los que a menudo se obtienen de forma independiente en el mercado ferroviario tradicional. Ver Figura 3.1

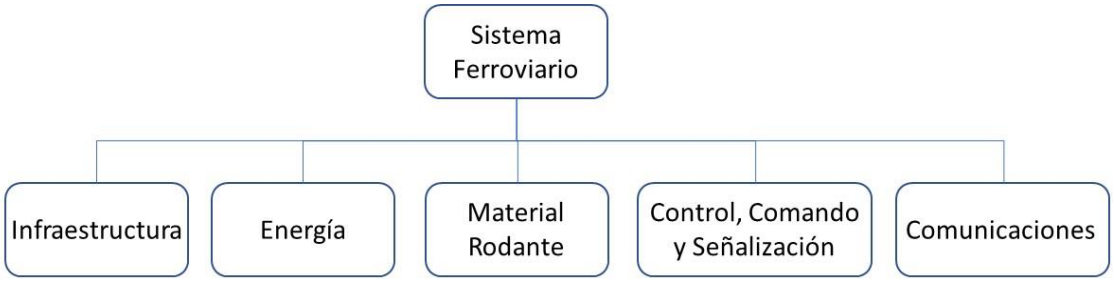


Figura 3.1: Desglose Sistema de Transporte Ferroviario,

Fuente [CLC/TR 50126-2. (2007)].

Este enfoque basado en una descomposición funcional ofrece una estructura genérica del sistema de transporte, donde se define un nivel de servicio objetivo para cada uno de los sistemas que constituyen el UGT, y en consecuencia, se puede calcular la disponibilidad técnica global objetivo para la Línea en operación.

Siguiendo esta lógica, el Sistema UGT debe mantener un nivel de servicio objetivo y dicho nivel de servicio se alcanza, mediante el cumplimiento de objetivos de Disponibilidad, Fiabilidad y Mantenibilidad definidos para cada uno de los sistemas que lo constituyen.

3.1 Aplicación de la metodología de diseño SMC al sistema RCOM

El sistema RCOM es uno de los constituyentes de UGT y es el sistema que cubre las necesidades de comunicaciones tren-tierra. La Figura 3.2 muestra asignación de confiabilidad para el sistema de transporte global y para RCOM.

Los objetivos planteados son parte de los requisitos contractuales que el operador impone al constructor del sistema RCOM, para dichos requisitos el constructor debe demostrar cumplimiento.

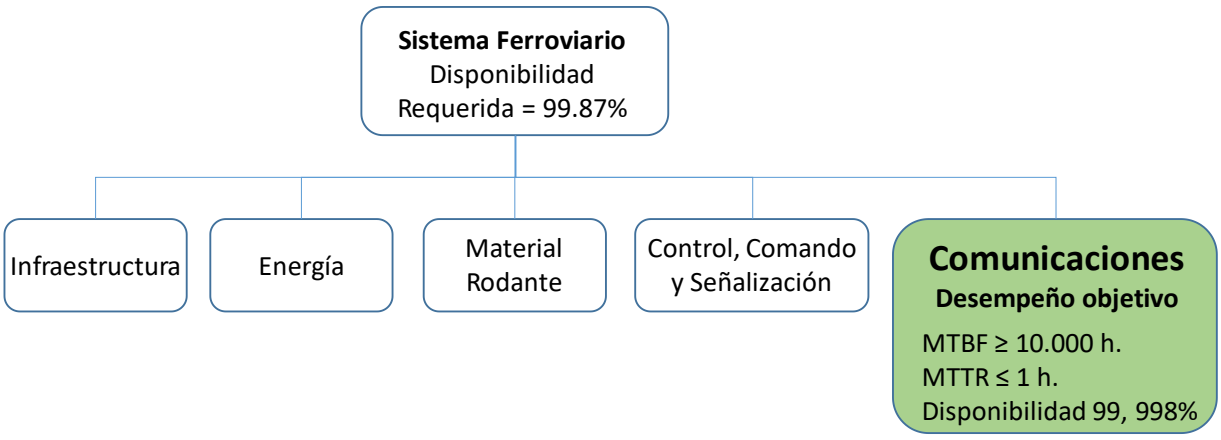


Figura 3.2: Objetivos de confiabilidad del sistema,

Elaboración propia, 2020

En los siguientes párrafos se aplica la metodología de diseño SMC expuesta en el § 2, para el desarrollo del sistema de comunicaciones ferroviario RCOM, considerando requisitos de fiabilidad, mantenibilidad y disponibilidad.

3.1.1 Etapa 1: Definir el sistema RCOM a diseñar

El objetivo de esta etapa es describir el sistema RCOM, a fin de conocer sus condiciones de operación, perfil de misión, funciones y características, las que posteriormente servirán como información de entrada para elaborar los modelos y análisis del venideros.

3.1.1.1 Descripción del sistema

El sistema de radio RCOM es una plataforma de comunicaciones inalámbrica entre el tren y tierra que tiene como objetivo final disponer una comunicación fiable de datos, más específicamente proporcionar una comunicación entre los sistemas en tierra conectados a la RMS y los sistemas conectados en al interior del del tren.

El sistema RCOM brinda una plataforma de comunicaciones IP transparente para los distintos sistemas de comunicaciones embarcados en los trenes, como por ejemplo CCTV, Telefonía y Sistema de anuncios al pasajero (SIP), con los sistemas en tierra.

La arquitectura comprende componentes a nivel de línea, cocheras y equipamiento embarcado garantizando una cobertura en todo momento en que el tren se encuentre operativo, ver Figura 3.3.

Condiciones climáticas de operación

La ciudad de Santiago tiene un clima templado cálido con lluvias invernales, según definición de Koeppen. En verano se producen variaciones de 20 oC entre las temperaturas mínimas y máximas. Estas variaciones en invierno llegan a menos de 10 oC. En condiciones extremas, las precipitaciones alcanzan una intensidad de 40 mm en 24 horas.

Estos parámetros son utilizados como línea base en el proceso de diseño de la aplicación específica, por lo tanto, si el clima sufriera grandes cambios (tormentas, tsunamis, etc) el efecto de estos eventos queda excluido del alcance del análisis del sistema a suministrar y deben ser considerado por el operador ferroviario en sus análisis de seguridad operacional.

Compatibilidad electromagnética

El sistema debe garantizar la compatibilidad electromagnética en el entorno de uso, es decir, instalaciones de Metro de Santiago

Perfil de misión: 24 horas / día

Vida útil: 15 años

Objetivos de desempeño a lograr

- MTBF ≥ 10.000 h.
- MTTR ≤ 1 h.
- Disponibilidad ≥ 99, 998%

3.1.1.2 Estructura funcional de la solución

RCOM posee infraestructura operacional y funcional desplegada a lo largo de todos los lugares por donde circula el tren. Esta infraestructura constituye un área de radio.

El área de radio es una zona de cobertura específica del sistema de radio, que ofrece servicios inalámbricos a los trenes. Esta zona está delimitada por factores operativos y de rendimiento del sistema.

Cada área de radio está compuesta por:

- Controladores de área
- Red Backhaul
- Estaciones base de radio (RBS)

Controlador de área de radio

El controlador de área está constituido por un servidor que administra y opera un conjunto de RBS instaladas a lo largo de la vía cubriendo una zona definida.

El controlador de área realiza las funciones relacionadas con el control y acceso a la red multiservicio de Metro (RMS) de todos los dispositivos de su zona.

El controlador de área es denominado DRCU (Distributed Radio Control Unit). Cada DRCU poseerá dos interfaces de red Ethernet, una conectada a la RMS para proporcionar acceso a los recursos externos de RCOM y la otra a la red Backhaul de la RCOM, permitiendo la comunicación con las RBS dispuestas en el área.

La interfaz física de cada DRCU, con el anillo Backhaul, es implementada mediante un switch de acceso dispuesto especialmente para estos fines. Este switch posee las interfaces de fibra óptica necesarias para ser parte del anillo de fibra. A partir de ahora este switch será denominado Switch DRCU.

Red Backhaul

La red Backhaul se encarga de ofrecer una plataforma de comunicaciones de alta velocidad, disponibilidad y fiabilidad, implementando mecanismos de recuperación de la red de comunicaciones en caso de corte o falla de equipos.

Por cada RBS y DRCU existirá un Switch que permitirá a estos dispositivos incorporarse a la red.

Debido a que la red Backhaul posee una arquitectura de anillo, tiene tolerancia ante un corte de de fibra óptica (FO) o falla de un switch, pudiendo seguir operando de forma completamente normal, sin penalización en el rendimiento de la red.

Estación base de radio

Este es el componente responsable de proporcionar cobertura inalámbrica a los equipos embarcados en los trenes. Este dispositivo es quien emite señales inalámbricas que proporciona la cobertura efectiva a lo largo de las rutas del tren y en talleres.

El área de radio posee un número determinado de RBS, el que es establecido por el dimensionamiento realizado en base a los requerimientos de transmisión/recepción y las capacidades propias de los equipos que la constituyen.

Cada RBS está compuesta por:

- Un (1) transceptor de estación base (BST) o equipo de transmisión inalámbrica de 2 canales
- Cuatro (4) antenas, Dos (2) por canal
- Un (1) tablero de conexión que posee un (1) switch (parte de la red Backhaul) y una serie de accesorios complementarios como fuente de alimentación y cabecera de FO.

En el proyecto se ha considerado la instalación de una RBS con capacidad para manejar 2 canales de forma simultánea, denominados canal A y canal B, utilizando frecuencias diferentes.

Cada RBS posee una zona de cobertura determinada, denominada celda, y cuando una o varias estaciones móviles (instaladas en el tren) estén bajo el área de cobertura de la RBS, las estaciones móviles se asociarán a sus servicios de conectividad de forma automática, lo que será estrictamente controlado por la DRCU.

Estación móvil

La estación móvil es el equipo que proporciona la interfaz inalámbrica a cada tren de la Línea 63, la que permite la comunicación con las RBS ubicadas a lo largo del trayecto y tiene por objetivo ser la puerta de enlace para los datos provenientes desde los dispositivos ubicados en el interior del tren.

Cada tren contendrá dos estaciones móviles, una en cada cabina de este, las que operarán en canales diferentes, teniendo así cada tren comunicación con el canal A y canal B.

Estas estaciones móviles o MST (Mobile Station Transceiver) operarán de forma agregada en cada tren, realizando transmisión o recepción de datos de forma simultánea.

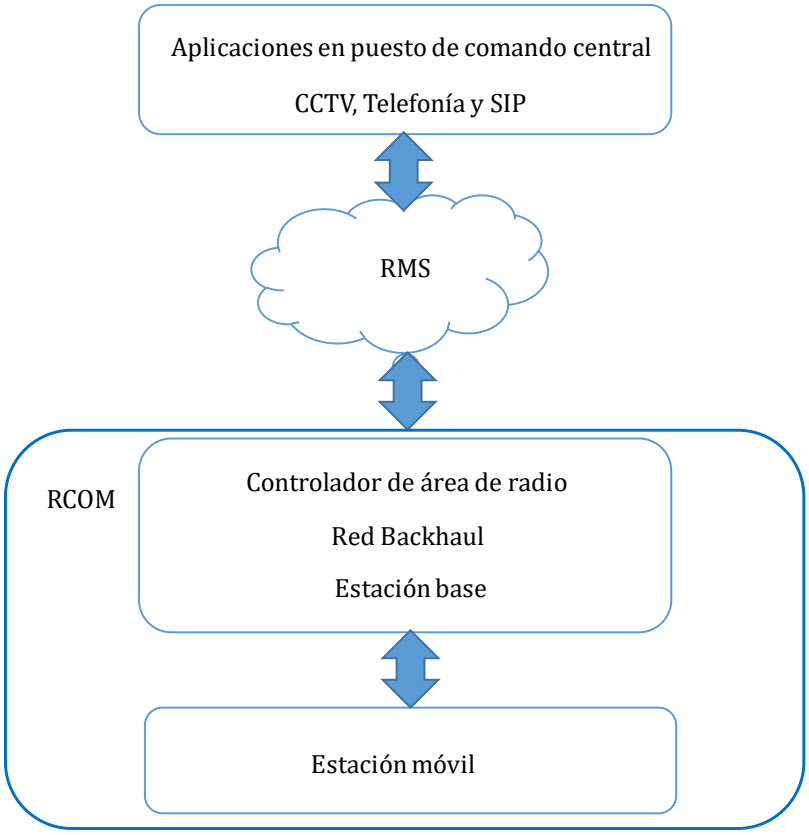


Figura 3.3: Estructura RCOM,

Elaboración propia, 2020

3.1.1.3 Interfaces

El sistema RCOM tiene interfaces, es decir, conexión funcional con otros sistemas, las cuales deben ser gestionadas desde inicio del proyecto para asegurar la integración de los distintos sistemas que constituyen el UGT. Las siguientes son las interfaces a ser aseguradas para lograr el correcto funcionamiento de RCOM.

- Material Rodante, conexión de MTS a bordo del tren.

- Vías, posición del equipamiento en túnel.
- Energía, suministro de energía
- Red Multiservicio del operador, transporte de la data desde la RCOM al puesto de comando central del operador.

3.1.2 Etapa 2: Medir el desempeño de RCOM en arquitectura preliminar

Esta etapa tiene por objetivo modelar y estimar el desempeño del sistema en una arquitectura preliminar, llamada arquitectura base. Esta es el pilar sobre el cual inicia el proceso de diseño.

3.1.2.1 Modelamiento de la arquitectura

Utilizando como entrada la definición de sistema proveniente de la etapa 1, se elabora la Tabla 3.1 que muestra el desglose de los elementos y funciones que constituyen a RCOM.

Tabla 3.1: desglose del sistema RCOM,

Elaboración propia, 2020.

Nivel	Grupo	Elemento	Función
Equipos de suelo	Grupo DRCU	DRCU Server PC	controla y gestiona intercambio de datos entre red de campo y RMS
		Base Station power Supply	Provisión de energía CC a BST y Switches RBS
		RBS Backhaul Access Switch	Trasporte de datos de red de campo hacia DRCU
	Grupo red backhaul	Base Station Network Switch	Transporte de datos dentro de red de campo hacia RBS
		Base Station power Supply	Provisión de energía CC a BST y Switches RBS
	Grupo BST	Base Station Transceiver	Intercambio de datos entre tren y tierra
Equipos móviles	Grupo MST	Mobile Station Transceiver	Intercambio de datos entre tren y tierra

El desempeño del sistema es medido en términos de disponibilidad, la cual, a su vez, está en función del MTBF y MTTR, ver ecuación 4.

La disponibilidad del sistema se obtiene por medio del uso de RBD, según se indica en § 2.3.2.

La Figura 3.4 muestra la RBD que representa al sistema RCOM en arquitectura base. El diagrama solo considera redundante a nivel de equipos de suelo, el grupo de red backhaul (por ser un anillo tolerante a fallos). Las funciones DRCU y BST no se encuentran redundadas en esta fase inicial. Respecto a los equipos móviles, el tren está equipado con 2 MST las cuales funcionan en redundancia.

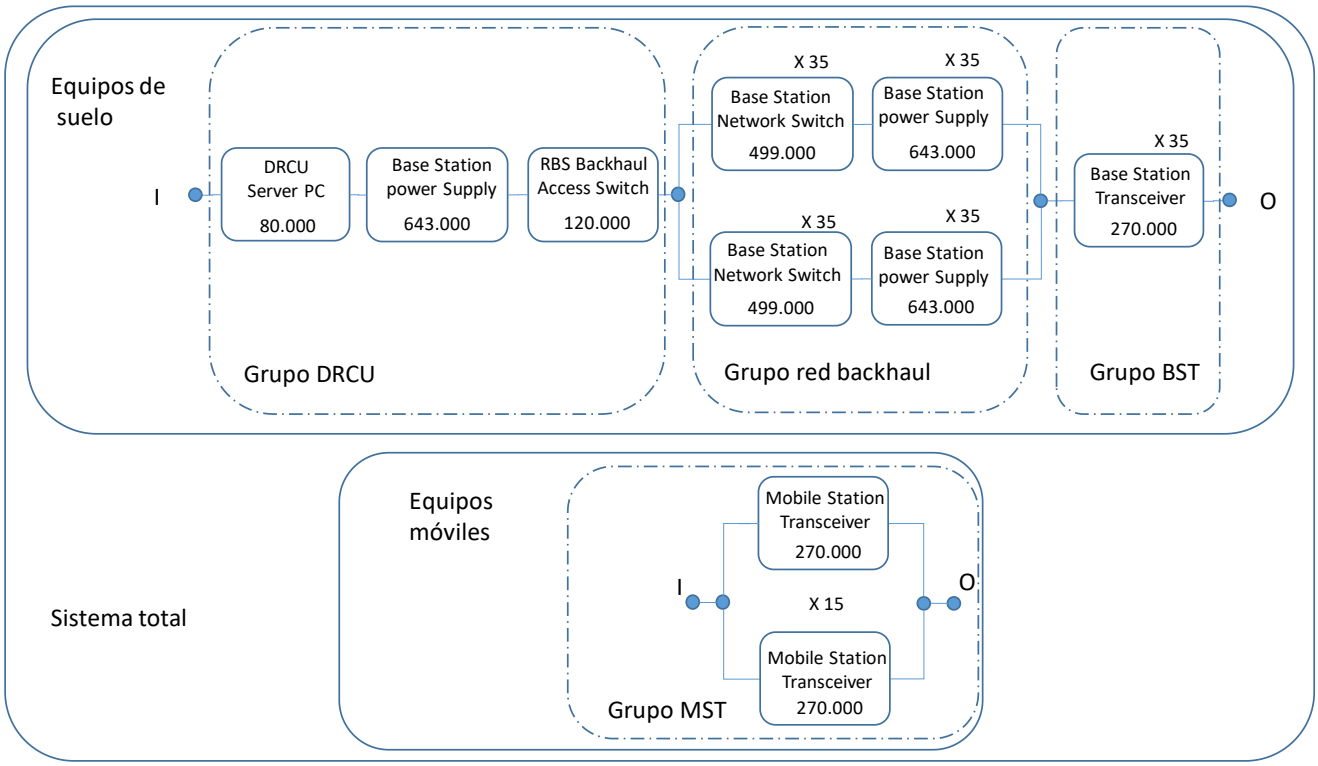


Figura 3.4: RBD sistema RCOM en arquitectura base,

Elaboración propia, 2020

3.1.2.2 Estimación de desempeño

El nivel de servicio o desempeño del sistema es medido evaluando el diagrama de bloques presentado en la Figura 3.4.

Los valores MTBF utilizados en el análisis son informados por los fabricantes en sus hojas técnicas, el anexo 6.1 presenta un ejemplo al respecto. Los valores MTTR están basados en la experiencia y recomendaciones del fabricante.

La estimación de desempeño sigue el siguiente proceso:

- Cálculo de fiabilidad y mantenibilidad de cada grupo
- Cálculo de fiabilidad y mantenibilidad equipos de suelo
- Cálculo de fiabilidad y mantenibilidad equipos móviles

- Cálculo de fiabilidad, mantenibilidad y disponibilidad del sistema en arquitectura base

Luego haciendo uso de las ecuaciones 2, 3, 4, 6, 7, 11 y 12 se obtienen los resultados presentados en la Tabla 3.2

Tabla 3.2: Cálculos de desempeño estimado para RCOM en arquitectura base, Elaboración propia, 2020

Nivel	Grupo	MTBF (h)	MTTR (h)	Elemento	N°_elementos	MTBF (h)	MTTR (h)
Equipos de suelo	DRCU	44,666	1.00	DRCU Server PC	1	80,000	1.00
				Base Station power Supply	1	643,000	1.00
				RBS Backhaul Access Switch	1	120,000	1.00
	Red backhaul	10,525,181	0.75	Base Station Network Switch	35	499,000	1.50
				Base Station power Supply	35	643,000	1.50
	BST	7,714	0.67	Base Station Transceiver	35	270,000	1.50
Equipos móviles (15 trenes)	MST	1,620,000,000	0.75	Mobile Station Transceiver	30	270,000	1.50
	MTBF	**6,574**			**138**		
Total sistema	**MTTR**	**0.716**					
	Disponibilidad	**99.98911%**					

Resultado

En base a lo observado en la tabla anterior, el desempeño estimado en arquitectura base cumple con brindar la funcionalidad de comunicación, sin embargo, no cumple con los objetivos de nivel de servicio requeridos por el operador. Ver Tabla 3.3.

Tabla 3.3: Resultado desempeño de RCOM en arquitectura base, Elaboración propia, 2020

Parámetro	Desempeño estimado	Objetivo contractual	Cumple / No Cumple
MTBF	6,574	≥ 10.000 h.	No Cumple
MTTR	0.716	≤ 1 h	Cumple
Disponibilidad	99.98911%	99, 998%	No Cumple

3.1.3 Etapa 3: Analizar las vulnerabilidades de RCOM en arquitectura preliminar

A fin de identificar y mitigar las vulnerabilidades del sistema RCOM en arquitectura base, se utiliza la herramienta FMEA, según se indica en § 2.3.3.

Del análisis se observa que la arquitectura base cumple con brindar la funcionalidad de comunicación en el área de radio definida, sin embargo, es una arquitectura frágil, donde la ocurrencia de un fallo generalmente afecta el servicio. La Tabla 3.4 muestra el detalle del análisis.

Tabla 3.4: FMEA para RCOM en arquitectura base,

Elaboración propia, 2020

Elemento	Función	Modo de fallo	Efecto en la operación	Categoría de fallo	Mitigación
DRCU Server PC	controla y gestiona intercambio de datos entre red de campo y RMS	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	asignar redundancia
Base Station power Supply	Provisión de energía CC a BST y Switches RBS	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	asignar redundancia
RBS Backhaul Access Switch	Trasporte de datos de red de campo hacia DRCU	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	asignar redundancia
Base Station Network Switch	Transporte de datos dentro de red de campo hacia RBS	Pérdida de conectividad 1 sentido del anillo	Sin efecto en la operación	Menor	
Base Station power Supply	Provisión de energía CC a BST y Switches RBS	Pérdida de conectividad 1 sentido del anillo	Sin efecto en la operación	Menor	
Grupo red Backhaul	Conectividad RMS a BST	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	Operador ferroviario debe establecer procedimientos para el caso.
Base Station Transceiver	Intercambio de datos entre tren y tierra	BST fuera de servicio	Pérdida parcial de la comunicación tren-tierra, solo el sector cubierto por las BST en falla	Mayor	asignar redundancia
Mobile Station Transceiver	Intercambio de datos entre tren y tierra	Pérdida de 1 MST del tren	Tren sigue en operación modo degradado	Menor	
Grupo MST	Intercambio de datos entre tren y tierra	Pérdida de ambas MST del tren	Tren declarado fuera de servicio	Significativo	Operador ferroviario debe establecer procedimientos para el caso.

3.1.4 Etapa 4: Mejorar el desempeño de RCOM

Una vez conocido el desempeño y las debilidades del sistema en arquitectura base, se inicia un proceso de mejora destinado a robustecer el sistema con foco en lograr el cumplimiento de los objetivos de desempeño establecidos por el operador ferroviario.

3.1.4.1 Modelamiento de la arquitectura

Utilizando como entrada la definición de sistema proveniente de la etapa 1, el modelo de desempeño y análisis de debilidades provenientes de las etapas 2 y 3 de la metodología se da inicio al proceso de optimizar el sistema.

Del análisis de vulnerabilidades presentado en la Tabla 3.4, se observa que:

El grupo DRCU es crítico para la operación del sistema, un fallo en cualquiera de sus elementos impacta directamente la funcionalidad de RCOM, generando la pérdida total de la comunicación tren-tierra en toda el área de radio (Línea 6 de Metro de Santiago). A fin de robustecer este grupo, se asigna una redundancia física a toda la rama constituida por el DRCU Server PC, Base Station power Supply y RBS Backhaul Access Switch.

Por otra parte, un fallo a nivel de BST genera la pérdida parcial de comunicación tren-tierra en la zona específica de cobertura (celda) de la BST fuera de servicio. Por lo tanto, se asigna una redundancia a nivel de celdas, es decir, se opta por instalar las BST a menor distancia entre ellas. Con esa acción se genera traslape de las zonas de cobertura y en consecuencia ante el fallo de una BST, siempre se logra conectividad por una BST adyacente.

Las mejoras establecidas en los párrafos anteriores dan origen a la RBD de la Figura 3.5.

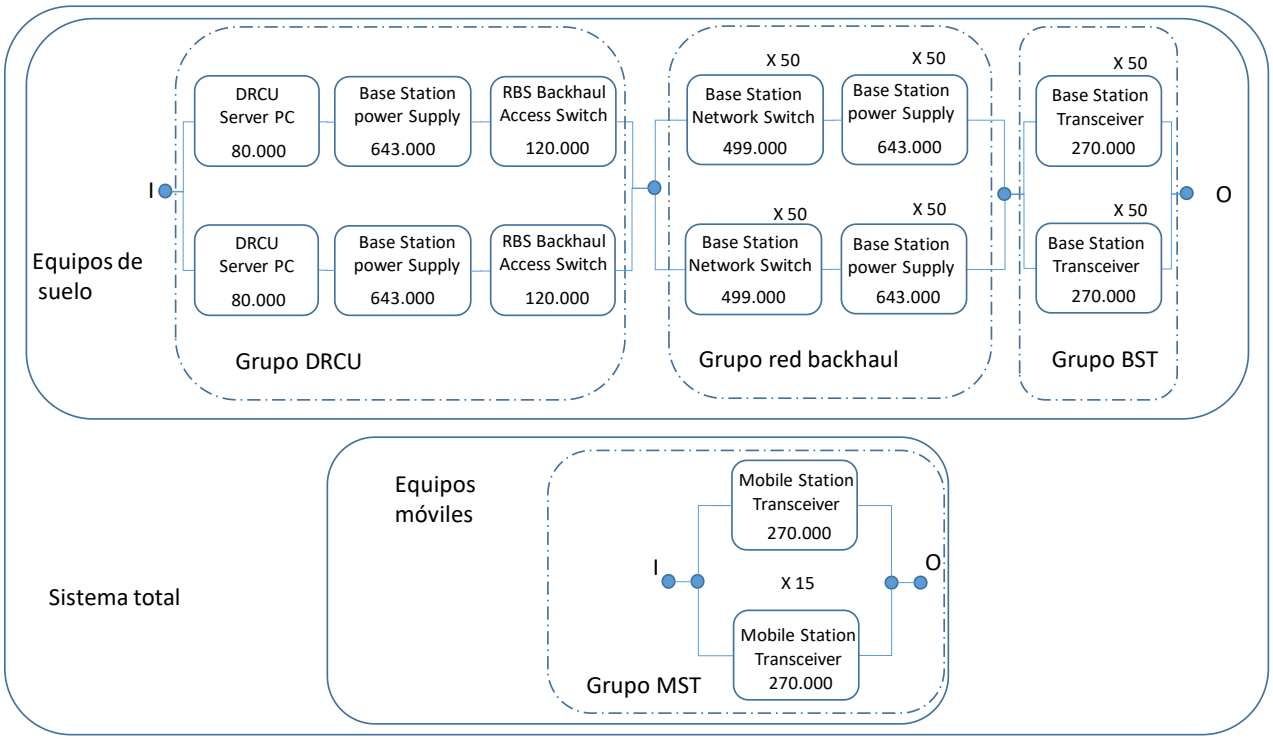


Figura 3.5: RBD sistema RCOM en arquitectura mejorada,

Elaboración propia, 2020

3.1.4.2 Estimación de desempeño

La estimación del desempeño sigue el mismo procedimiento que el utilizado en la etapa 2 de esta metodología.

El nivel de servicio o desempeño del sistema es medido evaluando el diagrama de bloques presentado en la Figura 3.5

Los valores MTBF utilizados en el análisis son informados por los fabricantes en sus hojas técnicas, el anexo 6.1 presenta un ejemplo al respecto. Los valores MTTR están basados en la experiencia y recomendaciones del fabricante.

La estimación de desempeño sigue el siguiente proceso:

- Cálculo de fiabilidad y mantenibilidad de cada grupo
- Cálculo de fiabilidad y mantenibilidad equipos de suelo

- Cálculo de fiabilidad y mantenibilidad equipos móviles
- Cálculo de fiabilidad, mantenibilidad y disponibilidad del sistema en arquitectura mejorada.

Luego haciendo uso de las ecuaciones 2, 3, 4, 6, 7, 11 y 12 se obtienen los resultados presentados en la Tabla 3.5

Tabla 3.5: Cálculo de desempeño estimado para RCOM en arquitectura mejorada, Elaboración propia, 2020

Nivel	Grupo	MTBF (h)	MTTR (h)	Elemento	N°_elementos	MTBF (h)	MTTR (h)
Equipos de suelo	DRCU	997,512,462	0.50	DRCU Server PC	2	80,000	1.00
				Base Station power Supply	2	643,000	1.00
				RBS Backhaul Access Switch	2	120,000	1.00
	Red backhaul	10,525,181	0.75	Base Station Network Switch	50	499,000	1.50
				Base Station power Supply	50	643,000	1.50
	BST	486,000,000	0.75	Base Station Transceiver	50	270,000	1.50
Equipos móviles (15 trenes)	MST	1,620,000,000	0.75	Mobile Station Transceiver	30	270,000	1.50
		MTBF	**10,132,982**		**186**		
Total sistema		**MTTR**	**0.747**				
		Disponibilidad	**99.99999%**				

Resultado

En base a lo observado en la tabla anterior, el desempeño estimado en arquitectura mejorada cumple con brindar la funcionalidad de comunicación tren-tierra de forma robusta, es decir, tolerante a fallos. Por otra parte, la arquitectura mejorada cumple con los objetivos de nivel de servicio requeridos por el operador. Ver Tabla 3.6

Tabla 3.6: Resultado desempeño de RCOM en arquitectura mejorada, Elaboración propia, 2020

Parámetro	Desempeño estimado	Objetivo contractual	Cumple / No Cumple
MTBF	10,132,982	≥ 10.000 h.	Cumple
MTTR	0.747	≤ 1 h	Cumple
Disponibilidad	99.99999%	99, 998%	Cumple

3.1.4.3 Analizar el funcionamiento del sistema RCOM

Utilizando el mismo procedimiento que el utilizado en la etapa 3 de esta metodología. Se emplea la herramienta FMEA para analizar las debilidades del sistema RCOM post proceso de mejora.

Del análisis se observa que:

- La arquitectura mejorada cumple con; brindar la conectividad tren-tierra necesaria, es muy robusta y tolerante a fallos en todos sus niveles.
- A pesar de lograr la robustez necesaria para alcanzar el desempeño exigido, aún existe la posibilidad de fallo, sin embargo, ante estos casos la responsabilidad del tratamiento de la contingencia es traspasada al operador ferroviario, quien por medio de procedimiento operacionales debe establecer los pasos a seguir para evitar riesgos inaceptables.

Tabla 3.7: FMEA para RCOM en arquitectura mejorada,

Elaboración propia, 2020

Elemento	Función	Modo de fallo	Efecto en la operación	Categoría de fallo	Mitigación
DRCU Server PC	controla y gestiona intercambio de datos entre red de campo y RMS	Pérdida de una rama DRCU	Sin efecto en la operación	Menor	
Base Station power Supply	Provisión de energía CC a BST y Switches RBS	Pérdida de una rama DRCU	Sin efecto en la operación	Menor	
RBS Backhaul Access Switch	Trasporte de datos de red de campo hacia DRCU	Pérdida de una rama DRCU	Sin efecto en la operación	Menor	
Grupo DRCU	Gestión de comunicación RMS a BST	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	Operador ferroviario debe establecer procedimientos para el caso.
Base Station Network Switch	Transporte de datos dentro de red de campo hacia RBS	Pérdida de conectividad 1 sentido del anillo	Sin efecto en la operación	Menor	
Base Station power Supply	Provisión de energía CC a BST y Switches RBS	Pérdida de conectividad 1 sentido del anillo	Sin efecto en la operación	Menor	
Grupo red Backhaul	Conectividad RMS a BST	Pérdida de conectividad con RMS	Pérdida total de comunicación tren-tierra	Significativo	Operador ferroviario debe establecer procedimientos para el caso.
Base Station Transceiver	Intercambio de datos entre tren y tierra	BST fuera de servicio	Sin efecto en la operación	Menor	
Grupo BST	Intercambio de datos entre tren y tierra	Pérdida de 2 BST contiguas	Pérdida parcial de la comunicación tren-tierra, solo el sector cubierto por las BST en falla	Mayor	Operador ferroviario debe establecer procedimientos para el caso.
Mobile Station Transceiver	Intercambio de datos entre tren y tierra	Pérdida de 1 MST del tren	Tren sigue en operación modo degradado	Menor	
Grupo MST	Intercambio de datos entre tren y tierra	Pérdida de ambas MST del tren	Tren declarado fuera de servicio	Significativo	Operador ferroviario debe establecer procedimientos para el caso.

3.1.5 Etapa 5: Selección de la arquitectura a implementar

Después de realizada la iteración sobre la arquitectura base con foco en mejorarla, se tienen dos alternativas de arquitectura que cumplen la función de comunicación tren-tierra, la arquitectura base y la mejorada.

3.1.5.1 Comparación de arquitecturas

El criterio de decisión para la selección de la arquitectura a utilizar es dar fiel cumplimiento al contrato adjudicado y en consecuencia a los requisitos de desempeño en él establecidos. La Tabla 3.8 muestra una comparación de los parámetros más representativos de las arquitecturas evaluadas.

Tabla 3.8: Comparación de arquitecturas,
Elaboración propia, 2020

Parámetro	Arquitectura base	Arquitectura mejorada
MTBF	6,574	10,132,982
MTTR	0.716	0.747
Disponibilidad	99.98911%	99.99999%
Tolerancia a fallos	baja	alta
N° equipos instalados	108	156

En todo proyecto los costos son una variable fundamental al momento de tomar decisiones, sin embargo, en el caso de sistemas de misión crítica, prima el criterio de desempeño por sobre el económico.

Por lo anterior, a pesar de que la arquitectura mejorada implica la compra de un mayor número de elementos, y, por consiguiente, mayores costos de suministro. Es esta la arquitectura seleccionada para ser implementada en Línea 6 de Metro de Santiago.

3.1.5.2 Arquitectura para implementar

Finalmente, la arquitectura a implementar se traduce en el esquema que muestra la Figura 3.6, donde se aprecian las redundancias destinadas a robustecer los diferentes niveles del sistema.

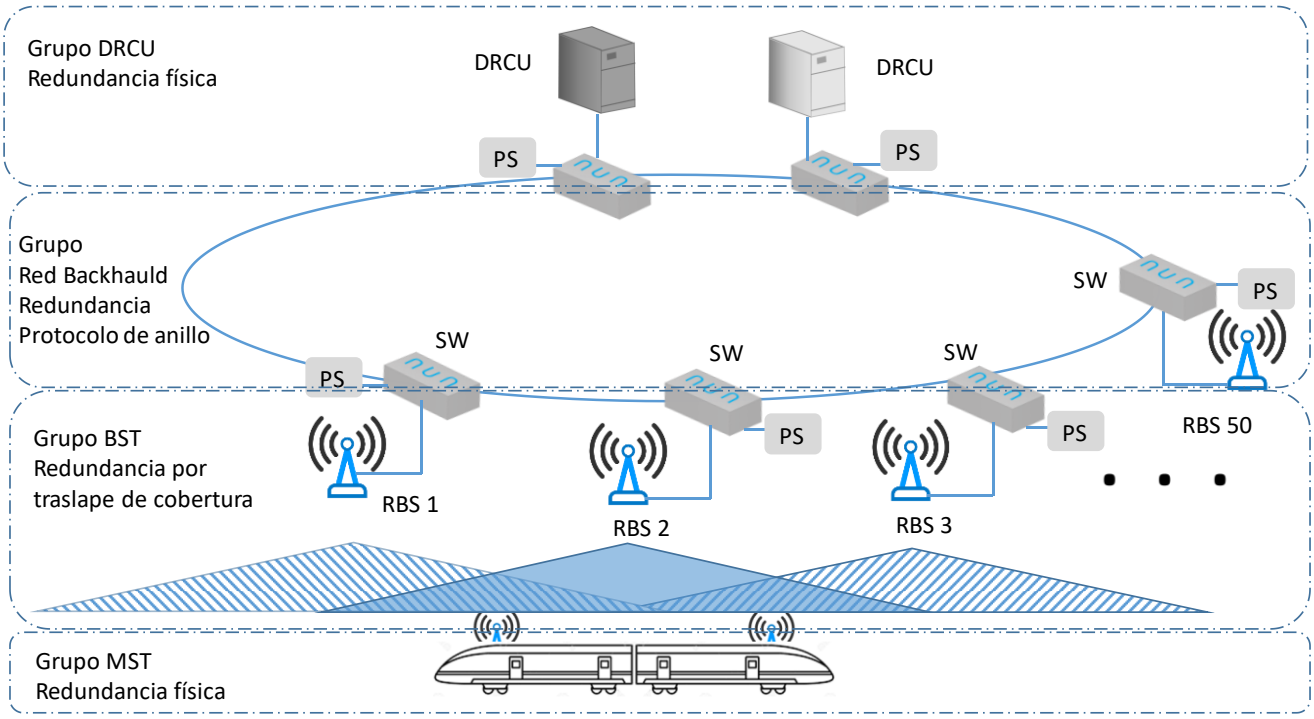


Figura 3.6: Arquitectura seleccionada,

Elaboración propia, 2020

3.2 Conclusión y análisis del capítulo

Los resultados muestran que la metodología propuesta para diseño de SMC es una secuencia de actividades, destinadas a gestionar los factores y variables que deben ser considerados en el proceso de diseño de un sistema que requiere alto nivel de servicio.

Las actividades para el diseño se ordenan dentro de un proceso DMAIC, el cual anida en su interior las herramientas; RBD para modelar el desempeño del sistema y FMEA para analizar las debilidades de la arquitectura.

La elaboración de la metodología de diseño de SMC, se puede visualizar desde el punto de vista de la gestión de innovación (Design Thinking), donde luego de un proceso de inmersión en diferentes diciplinas (Ingeniería; ferroviaria, de sistemas, confiabilidad, por nombrar algunas) y definición de necesidades (diseñar un sistema), se diverge en búsqueda de técnicas, métodos y herramientas conocidas (DMAIC, FMECA y RBD), las cuales al ser integradas convergen para generar la nueva metodología de diseño propuesta. Al aplicar esta metodología al sistema RCOM se consigue construir una arquitectura robusta que logra el desempeño exigido por el operador ferroviario.

La gestión de operaciones de Metro tiene como fin último optimizar la productividad de la Línea, con este objetivo busca gestionar parámetros como; regularidad de la circulación de los trenes, seguridad y afluencia de pasajeros, entre otros. La aplicación de la metodología de diseño de SMC, permite suministrar el sistema de comunicaciones RCOM, el cual con su alto nivel de desempeño, favorece a la gestión de la operación de la Línea de Metro. La arquitectura redundante permite mantener la operación a pesar de la ocurrencia de fallos. Además, RCOM toma especial relevancia ante emergencias y operación degradada de Línea, contribuyendo directamente a mantener la regularidad de la circulación de trenes y aportar en la seguridad en casos de emergencia.

Desde el punto de vista de la gestión de negocio, Metro y sus finanzas se centran principalmente en la venta de boletos, es decir, la afluencia de pasajeros. Como ya se ha mencionado, el sistema RCOM favorece a la gestión de operación de la Línea de Metro, minimizando las detenciones y aportando a cumplir con el intervalo planificado entre trenes. Por lo tanto, se puede inferir que el sistema RCOM de alta disponibilidad impacta de forma positiva a la gestión del negocio de Metro

contribuyendo a mantener un sistema operativo y por consiguiente mantener la venta de boletos necesaria para financiar la operación de Metro.

4 CONCLUSIONES GENERALES

La investigación muestra que las actividades a ser consideradas en el proceso de diseño de un sistema de misión crítica son: la definición, medición, análisis, mejora y control de los factores y variables que afectan el desempeño del sistema. En este sentido se propone un método para desarrollo de un sistema de comunicaciones que posee alto nivel de servicio, es decir, cumple objetivos de desempeño cuantitativos basados en la medición de disponibilidad del sistema. En efecto los resultados muestran que una metodología para diseño construida sobre un proceso DMAIC se adapta a la secuencia de actividades que se requiere realizar. Por lo tanto, se establece la metodología para diseño de SMC, la cual anida en su interior, a las herramientas; RBD para modelar el desempeño del sistema y FMEA para analizar las debilidades de la arquitectura. La metodología para diseño de SMC genera iteraciones sobre una arquitectura preliminar a fin de corregir las debilidades detectadas en pos de un diseño óptimo. Esta metodología permite estimar el desempeño del sistema, tanto en operación normal, como degradada, asegurando de esta forma el comportamiento del sistema ante eventos inesperados, tales como; un apagón, corte en la fibra óptica de la red, fallos en una estación radio base, etc.

Se realizó una revisión de literatura especializada en temas relativos a; ingeniería de sistemas, confiabilidad, aseguramiento de sistemas y normativas tanto del mundo ferroviario, como militar y se identificó al error humano como el principal factor que incide directamente en el proceso de diseño, en esta clasificación se encuentran; la interacción entre personas, competencias, motivación, calidad de la información, interfaces entre humanos y herramientas automatizadas, por nombrar algunas. Otro importante factor que resulta relevante para conseguir con éxito un sistema que cumpla con los requisitos especificados es la condición de explotación, en esta clasificación se encuentran; temperatura, humedad, compatibilidad electromagnética, interfaces, perfil de la misión, en general, las tareas que realiza el sistema y las condiciones y entorno en que se realizan dichas tareas.

Desde la información revisada se analizó como estos dos factores impactan en el proceso de diseño, llegando a la determinar que el error humano puede generar desviaciones entre lo esperado por el operador ferroviario y lo realizado por el contratista. Este factor está estrechamente relacionado con la actividad de las personas que participan directa o indirectamente en el proceso de ingeniería y diseño. El error humano se puede dar por mal entender los requerimientos, patrones de comportamiento, falta de competencias o sin fin de causas más. Con el propósito de minimizar el error humano, la actividad de diseño debe ser realizada bajo la protección de; procesos, procedimientos y buenas prácticas orientadas al logro del aseguramiento de sistema.

Por otra parte, las condiciones de explotación deben ser identificadas de forma temprana en el proceso de diseño. Las funciones, requisitos y entorno en el cual opera el sistema, son claves para su correcta definición y por consiguiente para el logro del objetivo de desempeño definido.

En este contexto se generó el método de diseño SMC el cual sistematiza el proceso de diseño, para minimizar posibles desviaciones entre lo solicitado y lo emitido. Este método fue utilizado en el diseño del sistema de comunicaciones RCOM de Metro de Santiago, donde lleva operativo 3 años sin mayores inconvenientes.

En este sentido la metodología de diseño SMC, contribuye a la comprensión de los factores que inciden en el proceso de diseño del sistema, además define una secuencia de actividades, de fácil implementación y gestionables.

Finalmente, al aplicar la metodología de diseño de SMC sobre el sistema de comunicaciones ferroviario RCOM, se logra construir una arquitectura robusta que supera los objetivos de desempeño fijados, es decir, posee un alto nivel de servicio. Esta cualidad contribuye a asegurar la oferta de transporte y reduce las pérdidas por accidentes e indisponibilidad de infraestructura y por sobre todo asegura la

conectividad entre pasajeros y operadores de metro ante cualquier emergencia o evento inesperado.

4.1 Propuesta para trabajos futuros

El análisis de fiabilidad de sistemas es una disciplina que tiene varias aristas y mucho por recorrer aún, a continuación, se presentan algunas líneas de investigación que quedan abiertas y podrían ser objeto de futuros trabajos.

- La investigación para implementar un proyecto normativo que busque asegurar la puesta en servicio de los futuros proyectos ferroviarios en Chile.

  Por ejemplo, en Europa, cada país posee la figura de "Autoridad Ferroviaria", este organismo es responsable de dar la autorización para la explotación de cada sistema que entra en operación en el país. Esta entidad es independiente de los operadores locales y vela por asegurar que cada modificación o nuevo proyecto se realice dando cumplimiento a la normativa de Seguridad, también es requisito de dicha norma, que exista el rol de Autoridad Ferroviaria.

  Otros países como; Estados Unidos y Australia, utilizan una estrategia similar a la Europea para la gestión de su Seguridad Ferroviaria.

  Por otra parte, Chile tiene en carpeta proyectos de actualización de infraestructura existente, nuevos proyectos y estudios para futuros proyectos, como los son; Santiago Batuco, Coquimbo la Serena, Santiago Valparaíso, Línea 7 de Metro, Extensión L3, Extensión L2, renovación de la señalización de la red de EFE, por nombrar algunos. Ante este hecho y sumada la falta de la figura de la una Autoridad Ferroviaria en Chile, parece razonable promover la investigación destinada a la implementación de una normativa Chilena destinada a garantizar la Seguridad Ferroviaria.

- La evaluación de la fiabilidad desde la fase de diseño del ciclo de vida abre la puerta a los análisis centrados en el costo del ciclo de vida. La gestión de proyectos tradicional se ha centrado principalmente en los costos de adquisición de los sistemas, sin embargo, la experiencia indica que la falta de previsión ante la aparición inesperada de fallos y/o obsolescencia tecnología, podría generar grandes incrementos en los costos totales durante el ciclo de vida del sistema. En el ámbito ferroviario esta situación toma especial fuerza, al ser los repuestos construidos a pedido y de tecnología propietaria, los costos de las piezas y partes de sistemas y trenes tienen elevado costo y largos tiempos de producción.
- Actualmente, los sistemas incluyen por lo menos hardware y software destinados a cumplir la función para la cual han sido concebidos, sin embargo, el término fiabilidad en sí mismo, no es directamente aplicable al caso del software, puesto que la fiabilidad se define como una probabilidad de ocurrencia de un evento. A diferencia del software (de entorno ferroviario) el cual utiliza modelos determinísticos que ante una combinación definida de entradas y eventos, siempre responden de la misma forma, es decir, la existencia de un fallo de diseño residual en el software hace que, ante unas determinadas condiciones se produzca siempre un fallo (probabilidad 1), mientras que, para otras condiciones, nuca se producirá (probabilidad 0). Lo anterior lleva a preguntarse qué métodos se puede utilizar para medir el desempeño y seguridad del software.
- Evaluación de los modelos RBD por medio de software especializados, por ejemplo; blocksim reliasoft, Raptor, etc.

5 REFERENCIAS BIBLIOGRAFICAS

Asociación Española de Normalización. (2018). Aplicaciones ferroviarias Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS). UNE 50126-1,2018

Bull, A. (2003). Congestión de tránsito: el problema y cómo enfrentarlo. CEPAL, p-14.

Bull, A. y Thomson, I. (2001). La congestión del tránsito urbano: causas y consecuencias económicas y sociales. DOI:10.18356/FD4A1F83-ES

Bracciali A. (2016) Railway Wheelsets: History, Research and Developments, p-23, p-30. DOI: 10.4203/ijrt.5.1.2.

Conradie, P., Fourie, C., Vlok, P. y Treurnicht, N. (2015) Quantifying system reliability in rail transportation in an ageing fleet environment, p-2. DOI: 10.7166/26-2-1076.

Consejo Nacional de Seguridad Social (CNSS), (2003). National Information Assurance (IA) Glossary. N° 4009.

Creus, A. (2005). Fiabilidad y seguridad, Iberoamericana, p-30

Doshi, J. (2017). Application of failure mode & effect analysis (FMEA) for continuous quality improvement - multiple case studies in automobile SMEs, p-1-6. DOI: 10.18421/IJQR11.02-07.

Engineering Safety Management (The Yellow Book), Rail Safety and Standards Board on behalf of the UK Rail industry, 2007

Government of New South Wales Transport. (2015). Systems Engineering. T MU AM 06006 ST.

Hasan, O., Ahmed, W., Tahar, S. y Salah, M. (2015). Reliability block diagrams based analysis: A survey. DOI: 10.1063/1.4913184

IEC 61078. (2016). Diagramas de bloques de confiabilidad.

IEEE 1474.1. (1999). Standard for Communication Based Train Control Performance Requirements and Functional Requirements.

Institution of Ralway Signal Engineers (IRSE). (2009). Semi-automatic, driverless, and unattended operation of trains. International Technical Committee.

ISO/IEC 15288:2008(E) (2008) IEEE Std 15288™-2008, Systems and software engineering - System life cycle processes.

MacDonald, M. (2007). Application of Systems Engineering to Railway Projects. Vol. 3, 1, pp. 25-34.

MITRE, (2014). Systems Engineering Guide, p-155.

MODUK. DEF STAN 00-56 (PART 1) /4. (2007). Safety Management Requirements for Defence Systems.

Moubray, J. (1997). Reliability-centered Maintenance.

National Defense Industrial Association (NDIA), (2008). Engineering for System Assurance. System Assurance Committee. Arlington, VA: NDIA, p-1.

Nedeliaková , E., Štefancová, V. y Hranický, M. (2018). Implementation of Six Sigma methodology using DMAIC to achieve processes improvement in railway transport, p-2. DOI: 10.30657/pea.2019.23.03.

Papen, V., Harvey, R., Qaasim, H. Y Spielholz, P. (2010). Systems Assurance Management in Railway through the Project Life Cycle.

Renpenning, F. (2004). Reliability Prediction in Railway Signalling, p-2. DOI:10.1007/978-0-85729-410-4_363.

The defense acquisition university press fort belvoir. (2001). Systems Engineering Fundamentals. p3-p7.

UNE-EN 61703. (2016). Expresiones matemáticas para los términos de fiabilidad, disponibilidad, mantenibilidad y de logística de mantenimiento

United States Department of Defense. (1991). MILITARY HANDBOOK RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT. MIL-HDBK-217F

6 ANEXOS

6.1 Swicth DRCU

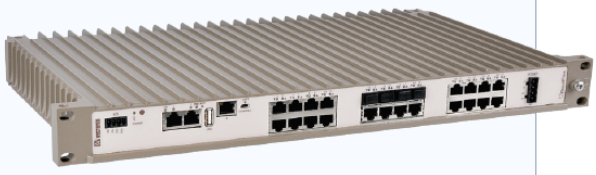
Swicth DRCU utilizado en la RCOM, posee certificación EN 50121-4 para uso en aplicaciones ferroviarias e informa un MTBF de 120.000 hrs bajo MIL-HDBK-217K

westermo RedFox

19" Industrial Routing Switch

RFIR-227-F4G-T7G-AC

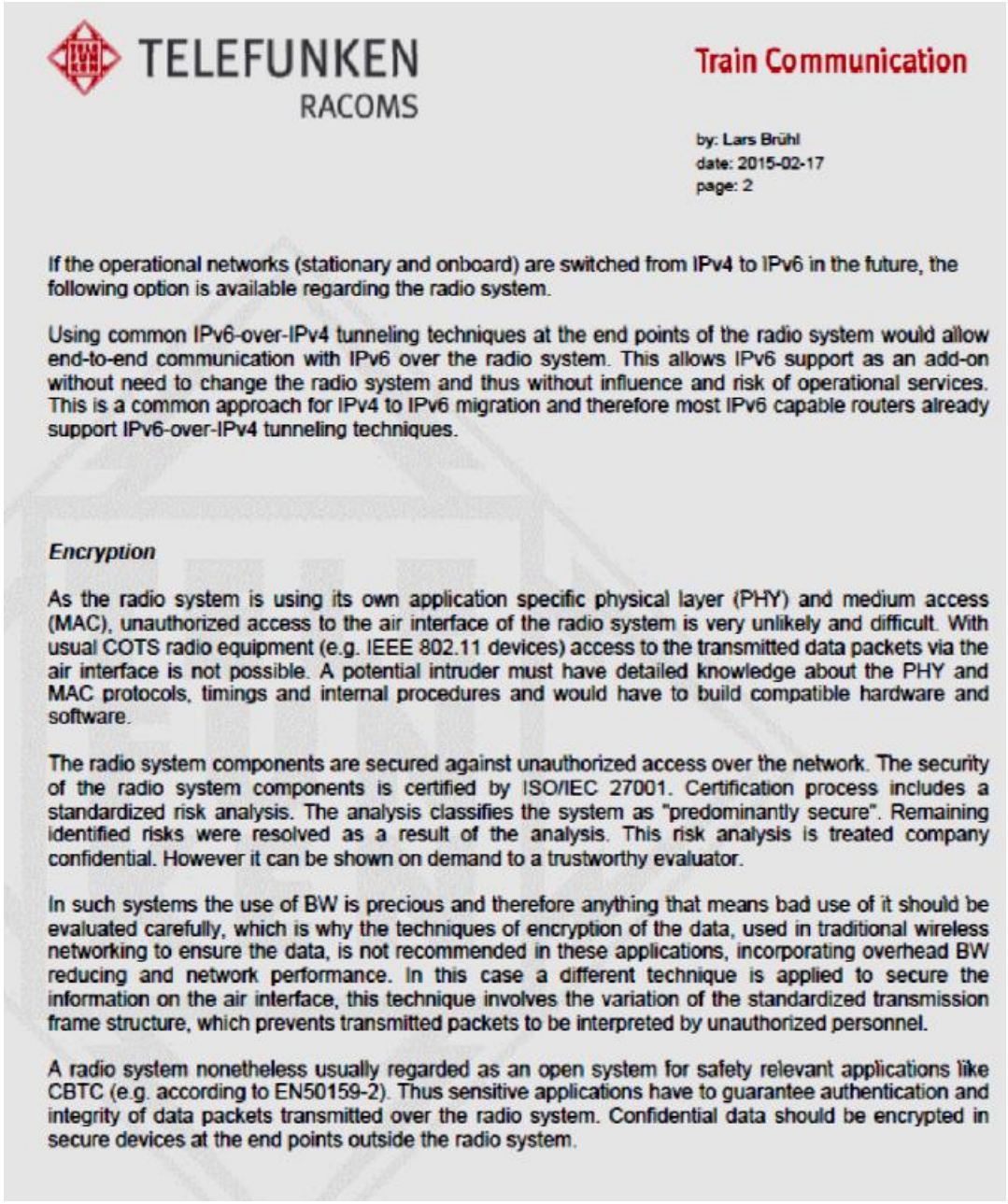
- High performance and configurable
  - 27 ports including 11 gigabit ports
  - Powerful dual core CPU
  - Advanced WeOS layer3 functionality
- Designed for demanding Edge Network applications
  - Low power consumption AC power supply
  - Highly configurable fault I/O contact
  - Ultra-robust IP40 19" rack/wall-mount housing
- Robust and reliable for long service life
  - 120 000 hours MTBF to MIL-HDBK-217K
  - -40 to +55°C without ventilation holes
  - Industrial and trackside type tested
- Unique future proof industrial networking solutions
  - Simple web configuration with professional CLI
  - Network IP Security and remote access
  - Multiple network resilience solutions



CE FC Part 15 | EN 50121-4 Railway Trackside | EN 55022 ITE Emission | EN 55024 ITE Immunity | EN 61000-6-1 Residential Immunity | EN 61000-6-2 Industrial Immunity | EN 61000-6-4 Industrial Emission

6.2 BST Telefunken

Certificado de la BST para equipo de radio comunicación ferroviaria.



TELEFUNKEN
RACOMS

Train Communication

by: Lars Brühl
date: 2015-02-17
page: 2

If the operational networks (stationary and onboard) are switched from IPv4 to IPv6 in the future, the following option is available regarding the radio system.

Using common IPv6-over-IPv4 tunneling techniques at the end points of the radio system would allow end-to-end communication with IPv6 over the radio system. This allows IPv6 support as an add-on without need to change the radio system and thus without influence and risk of operational services. This is a common approach for IPv4 to IPv6 migration and therefore most IPv6 capable routers already support IPv6-over-IPv4 tunneling techniques.

Encryption

As the radio system is using its own application specific physical layer (PHY) and medium access (MAC), unauthorized access to the air interface of the radio system is very unlikely and difficult. With usual COTS radio equipment (e.g. IEEE 802.11 devices) access to the transmitted data packets via the air interface is not possible. A potential intruder must have detailed knowledge about the PHY and MAC protocols, timings and internal procedures and would have to build compatible hardware and software.

The radio system components are secured against unauthorized access over the network. The security of the radio system components is certified by ISO/IEC 27001. Certification process includes a standardized risk analysis. The analysis classifies the system as "predominantly secure". Remaining identified risks were resolved as a result of the analysis. This risk analysis is treated company confidential. However it can be shown on demand to a trustworthy evaluator.

In such systems the use of BW is precious and therefore anything that means bad use of it should be evaluated carefully, which is why the techniques of encryption of the data, used in traditional wireless networking to ensure the data, is not recommended in these applications, incorporating overhead BW reducing and network performance. In this case a different technique is applied to secure the information on the air interface, this technique involves the variation of the standardized transmission frame structure, which prevents transmitted packets to be interpreted by unauthorized personnel.

A radio system nonetheless usually regarded as an open system for safety relevant applications like CBTC (e.g. according to EN50159-2). Thus sensitive applications have to guarantee authentication and integrity of data packets transmitted over the radio system. Confidential data should be encrypted in secure devices at the end points outside the radio system.

6.3 Fotos instalación de BST

Instalación de BST en túnel y talleres