Supervision System for Emergency Brake and Traction-System Isolation on Train Formations

I. Di Vito, P. Gomez, and A. Lutenberg

***Abstract*—In the event of an emergency, railway safety systems typically work by isolating the traction-system and applying the emergency brake, causing logistic problems on the railway line where the train formation remains stopped. This paper presents the design of a supervision system that enables the train formation to be moved in a limited and controlled way to a repair workshop or to a safe place for dropping off passengers (in the case of passenger trains). This supervision system is considered critical, because it operates on the emergency brake and the traction-system. Thus, recommendations of the UNE-EN 50126 standard were followed during its design. In particular, hardware design techniques commonly used in other industries like automotive, aeronautics and aerospace, have been adopted.**

***Index Terms*—Critical systems, Design patterns, Railway systems, UNE-EN 50126.**

I. Introducción

SEGÚN la norma IEC 61508 un sistema causa un daño si se afecta negativamente a la salud a una o más personas de manera directa o indirecta a través de generar grandes pérdidas materiales o al medio ambiente [1]. Un sistema crítico puede definirse como aquel que, en caso de fallar, puede ocasionar daños. Los sistemas críticos se diseñan utilizando técnicas que minimizan el riesgo, que se define como la probabilidad de que el sistema genere daños [2].

Los sistemas críticos tienen requisitos funcionales como cualquier otro equipo electrónico. Sin embargo por su naturaleza también tienen requisitos no funcionales asociados a su capacidad de disminuir los riesgos asociados a un mal funcionamiento. Estos se conocen como requisitos RAMS, cuyas siglas se refieren a la fiabilidad (capacidad del sistema de realizar una función de manera correcta), disponibilidad (capacidad del sistema de ofrecer sus servicios de manera consistente en el tiempo), mantenibilidad (capacidad de un sistema de ser reparado en un tiempo dado) y seguridad (capacidad de un sistema de minimizar el riesgo asociado a generar daños a personas y el medio ambiente) del sistema [3]. La norma UNE-EN 50126 determina una metodología de trabajo y sugerencias que permiten relevar y cumplir estos requisitos no funcionales. Una de estas recomendaciones es la utilización de patrones de diseño.

Los patrones de diseño son técnicas para resolver problemas comunes en una determinada área, aplicando una solución conocida y estandarizada [4]. Estas soluciones tienen la forma de plantillas genéricas que han demostrado ser eficaces y reutilizables [5], [6]. Los patrones de diseño son muy comunes en el desarrollo de software [7] aunque también se aplican al diseño de hardware. Existe un grupo conocido como patrones de diseño híbridos [8], [9]. Los mismos constan de componentes de hardware y firmware que son parte de un mismo patrón de diseño.

I. Di Vito, P. Gomez and A. Lutenberg are with CONICET-GICSAFe and UBA (email: lse@fi.uba.ar).

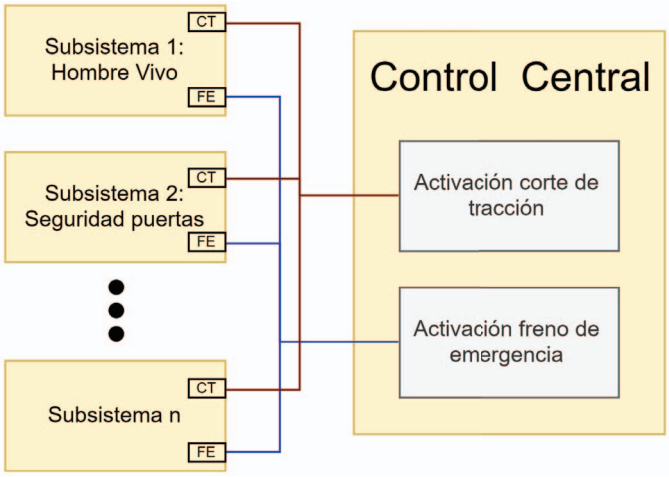

Fig. 1. Diagrama conceptual de la interacción típica de los sistemas de seguridad en una locomotora.

II. Planteo del Problema

En el sistema ferroviario de la República Argentina un número considerable de locomotoras poseen sistemas de seguridad como el que se ilustra en la Fig. 1. En ellos una serie de subsistemas controlan que ciertas funciones específicas estén operando en forma segura. Ejemplo de estos son el subsistema que monitorea el correcto funcionamiento de las puertas, el sistema de hombre vivo y el monitoreo con cámaras de seguridad. Cada uno de estos subsistemas informan su estado a un sistema central. Ante un estado de funcionamiento no seguro, en cualquiera de esos subsistemas, el sistema central activa un mecanismo de seguridad por el cual detiene a la formación cortando la tracción y/o activando el freno de emergencia.

Esta forma de responder a los fallos implica que una sola formación con un problema relativamente menor puede causar la congestión de todo el sistema ferroviario. Por ejemplo, este sería el caso de una formación a la que no le funciona el sistema de cierre de una puerta. Sin embargo, en muchos casos el conductor podría llevar la formación, a una velocidad reducida, a un lugar en donde no afecte la circulación. Además, en el caso de un servicio de pasajeros, se mejoraría la seguridad de los pasajeros permitiendo llegar a un lugar

apropiado donde los mismos desciendan. La única manera en la que el sistema actual permite realizar esta operación es a través de la anulación total de los sistemas de seguridad, lo que se conoce como modo aislado total. Esto soluciona el problema logístico pero compromete seriamente la seguridad al permitirle al conductor operar el material rodante sin ningún sistema de supervisión de la seguridad activado.

En este contexto la empresa estatal Trenes Argentinos Operaciones (SOFSE) encargó al Grupo de Investigación en Calidad y Seguridad de las Aplicaciones Ferroviarias (GICSAFe) del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) el desarrollo de un sistema embebido crítico capaz de solucionar este problema.

En la bibliografía se encuentran equipos que abordan este problema, con un enfoque similar al del modo aislado total, como el Emergency Bypass Switch (EBS) [10]. El EBS permite al conductor aislar por completo las funciones de seguridad del material rodante para poder llevarlo a un lugar donde pueda repararse [11], [12]. Sin embargo, el EBS no supervisa al material rodante durante el modo aislado total [13]. Un ejemplo de las consecuencias de esto se presenta en un reporte de un accidente de trenes sucedido en Chicago, Illinois en 1976. Allí se reporta que los sistemas de control automático de trenes fallaban en promedio 6,5 veces al día y los conductores se veían obligados a utilizar el modo aislado provisto por el EBS [14]. El sistema propuesto, al supervisar el material rodante, es capaz de detectar automáticamente estados inseguros durante el funcionamiento en modo aislado, como por ejemplo una velocidad excesiva, y en ese caso aplicar el freno de emergencia y/o el corte de tracción, sin la intervención del conductor. A su vez implementa una conexión inalámbrica con una central operativa que debe otorgar un permiso de circulación.

III. Solución Propuesta

En la Fig. 2 se puede ver como interactúa el sistema diseñado, denominado SAL/T (Sistema de Aislamiento Limitado/Total), con los sistemas de seguridad de la formación. En una situación de falla de un subsistema asociado a la seguridad, luego de la activación del freno de emergencia y/o del corte de tracción, el SAL/T permite al maquinista activar un modo de funcionamiento limitado del material rodante conocido como modo aislado limitado. En esta situación el SAL/T toma el control de las señales de corte de tracción y freno de emergencia mediante los relés K_2 y K_4 permitiendo al conductor mover la formación siempre que no se supere una velocidad máxima y que exista un permiso de circulación emitida por la central operativa. Si alguna de estas condiciones no se cumplen el equipo utiliza los relés K_1 y K_3 para activar el corte de tracción y/o freno de emergencia, según corresponda.

El SAL/T está diseñado para ser instalado en la locomotora, sobre el pupitre, para que el conductor pueda activar el modo aislado limitado si fuera necesario. Mientras esté activado el SAL/T muestra la velocidad medida por el material rodante así como su estado a través de indicadores LED.

Otras función que debe cumplir el SAL/T es reportar a la central operativa el estado de la formación. Esto incluye

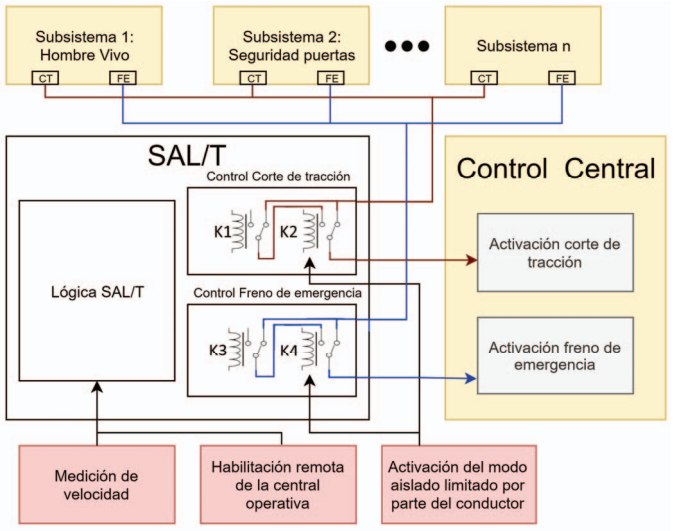

Fig. 2. Diagrama conceptual de la interacción del SAL/T con los sistemas de seguridad en una locomotora.

una indicación de modo aislado activado/desactivado y la velocidad a la que circula el material rodante además de una serie de parámetros internos de la lógica del programa. Dichos parámetros también deben ser configurables a través de los comandos remotos emitidos por la central operativa. La central debe tener la capacidad de alterar el comportamiento del equipo a través del envío de comandos de cambio de modo. Estos modos hacen que el equipo active o desactive las diferentes señales críticas sin importar la velocidad medida. Un ejemplo de esto es el denominado modo aislado total donde se permite la circulación sin restricciones de velocidad. Estos comandos de cambio de modo son válidos sólo durante un corto periodo, por lo que el equipo vuelve al modo normal si luego de transcurrido determinado intervalo de tiempo no recibe el comando que le indica que debe mantenerse en modo aislado limitado o modo aislado total, según corresponda.

IV. Diseño del Sistema

Para el diseño del sistema se siguieron las primeras cinco fases planteadas en la norma UNE-EN 50126 [3]. Estas fases consisten en implementar y documentar una serie de pasos que incluyen una definición conceptual del proyecto, una definición de las políticas RAMS, un análisis de riesgos y por último la definición de los requisitos del sistema y los subsistemas que lo componen.

Durante la fase 1 “Definición Conceptual del Proyecto” se relevaron las diferentes características del proyecto. Quienes son los principales actores, cuál es el alcance del proyecto, los supuestos y el contexto, así como los criterios de aceptación de los resultados y los riesgos. También se relevaron los requisitos y se generó la solución propuesta.

En la fase 2 “Políticas RAMS” se definieron los criterios con los que en la fase 3 “Análisis de Riesgos” se analizaron los diferentes riesgos asociados a la solución propuesta. Dadas las recomendaciones de la norma se analizó para cada uno de los riesgos tanto su probabilidad como la gravedad de sus consecuencias. En la Tabla I se puede ver un extracto de la

TABLA I
EXTRACTO DE LA TABLA DE ANÁLISIS DE RIESGOS DEL DOCUMENTO DE FASE 3 "ANÁLISIS DE RIESGOS"

Situación identificada	Característica particular	Análisis peligro	Es peligro
Falla en los actuadores de las señales de FE y CT.	Fallo no seguro de los actuadores	Si existe un fallo en los actuadores de salida que evita su desactivación, entonces el material rodante se encuentra en un modo no seguro	SI

documentación de la fase 3 donde se deja registro del resultado del análisis de un riesgo en particular.

En las fases 4 "Requisitos del sistema" y 5 "Distribución de los requisitos del sistema" se determinaron los diferentes módulos que componen el sistema. En la Fig. 3 se puede ver un diagrama del resultado de esta división en módulos así también la forma en la que se decidió agruparlos en la implementación del hardware en dos placas diferentes. Luego se determinaron los requisitos funcionales que cada uno de estos módulos debe cumplir de forma tal que todos los requisitos de la primera etapa queden cubiertos.

Utilizando los resultados del análisis de riesgo, se definieron distintos requisitos que mejoren los parámetros RAMS de los subsistemas más críticos. En los siguientes párrafos de esta sección se explican dichos requisitos. Los mismos surgen de aplicar en estos subsistemas patrones de diseño de hardware o híbridos que mejoran las características deseadas [15].

En algunos subsistemas no fue necesaria la aplicación de estos patrones para llegar a los niveles establecidos en la fase 2 de la norma 50126. Esto se debe a que un mal funcionamiento de la lógica del sistema, la interfaz con el registrador de eventos, la fuente y/o la interfaz hombre-maquina del SAL/T no afecta la seguridad de la formación. Ante una falla en cualquiera de esos subsistemas el conductor puede desactivar el SAL/T mediante la misma llave rotativa con la que lo activó. En ese caso, los sistemas de seguridad presentes en la formación vuelven a activarse, devolviendo a la formación a un estado seguro. La implementación de esta característica del sistema es a través de un circuito mecánico por lo que su funcionamiento no depende de la alimentación ni de la lógica del SAL/T. Además en este caso el conductor está en estado de alerta, porque al activar el SAL/T se pasa a un modo de trabajo bajo supervisión de la central operativa.

Es fundamental para el correcto funcionamiento del sistema tener una medición confiable de la velocidad del material rodante. Un error en esta medición puede generar que el sistema funcione incorrectamente afectando su fiabilidad, como por ejemplo la circulación de una formación a una velocidad superior a la velocidad máxima permitida. Por esto se decidió usar el patrón de diseño de *hardware dúplex heterogéneo* [4]. El mismo consiste en utilizar más de un circuito de hardware con idéntico objetivo de forma tal de evitar errores de modo común. El diseño contempla el uso de tres fuentes de información independientes: la referencia de velocidad medida por el propio equipo de seguridad del material rodante, un contador de pulsos conectado a un tacómetro y un sistema de GPS. El SAL/T utiliza estas tres fuentes de información para buscar inconsistencias en las mediciones y así evitar fallos.

Otro desafío en el diseño es la actuación segura sobre las señales críticas del material rodante. Dado que las mismas controlan el corte de tracción y el freno de emergencia, un error en su operación conlleva un gran riesgo. Para mitigar esto se decidió aplicar el patrón de diseño *canal simple protegido* [4]. El mismo consiste en que un sistema que actúa sobre una señal, en simultáneo mida el efecto de su accionar con el objetivo de comprobar que se logró el efecto deseado. En particular la aplicación de este patrón consiste en utilizar relés dobles de forma tal de poder medir el estado del mismo, compararlo con el valor esperado y en caso de detectar una inconsistencia llevar al equipo a una condición segura.

El tercer desafío es la necesidad de contar con una conexión inalámbrica entre el material rodante y la central operativa de manera fiable. Pueden generarse problemas logísticos si un equipo, debido a un error de conexión, no recibe la señal de permiso que habilita el modo aislado. Es un requisito del sistema que esta conexión se realice a través de la red celular con la tecnología GPRS. Por esto se decidió utilizar nuevamente el patrón de diseño de *hardware dúplex heterogéneo* [4]. En este caso se implementaron dos conexiones en paralelo con diferentes proveedores de servicio para minimizar la posibilidad de que existan zonas sin cobertura.

V. IMPLEMENTACIÓN DE HARDWARE

En la etapa de diseño de hardware se definió que el sistema cuente con dos placas. La placa principal contiene los módulos de lógica, comunicación, medición de la velocidad y accionamiento seguro sobre las señales del material rodante. La placa secundaria se encarga de la interfaz hombre máquina (HMI). En la Fig.4 se pueden ver ambas placas.

El diseño de los módulos planteados se realizó siguiendo las especificaciones determinadas en las etapas de diseño. Para la actuación sobre las señales críticas se decidió utilizar relés de seguridad TE Connectivity V23047A1024A501. Los mismos, además de estar certificados para aplicaciones críticas, constan de dos pares de contactos vinculados mecánicamente. Esto habilita aplicar el patrón de *canal simple protegido* [4] al utilizar un par de contactos para accionar sobre la señal crítica y el otro para medir si efectivamente el circuito está funcionando correctamente. Esto habilita que el firmware reaccione ante errores en el hardware protegiendo la integridad del sistema. En las señales particularmente críticas, como el corte de tracción y frenado de emergencia, este circuito de relés está redundado siguiendo el patrón de diseño de *hardware dúplex homogéneo* [4]. Este consiste en duplicar un circuito con una función crítica de forma tal que la misma se sigue cumpliendo aunque uno de los dos circuitos falle.

Para cumplir con la especificación de conexión GPRS redundada se utilizaron dos módulos SIM 808. El mismo utiliza un chip GSM para conectarse a la red celular. Esto permite utilizar el servicio de dos empresas distintas mejorando la disponibilidad de la conexión. A la vez cada uno de estos módulos cuentan con funcionalidad GPS brindando redundancia en la medición de la velocidad del sistema.

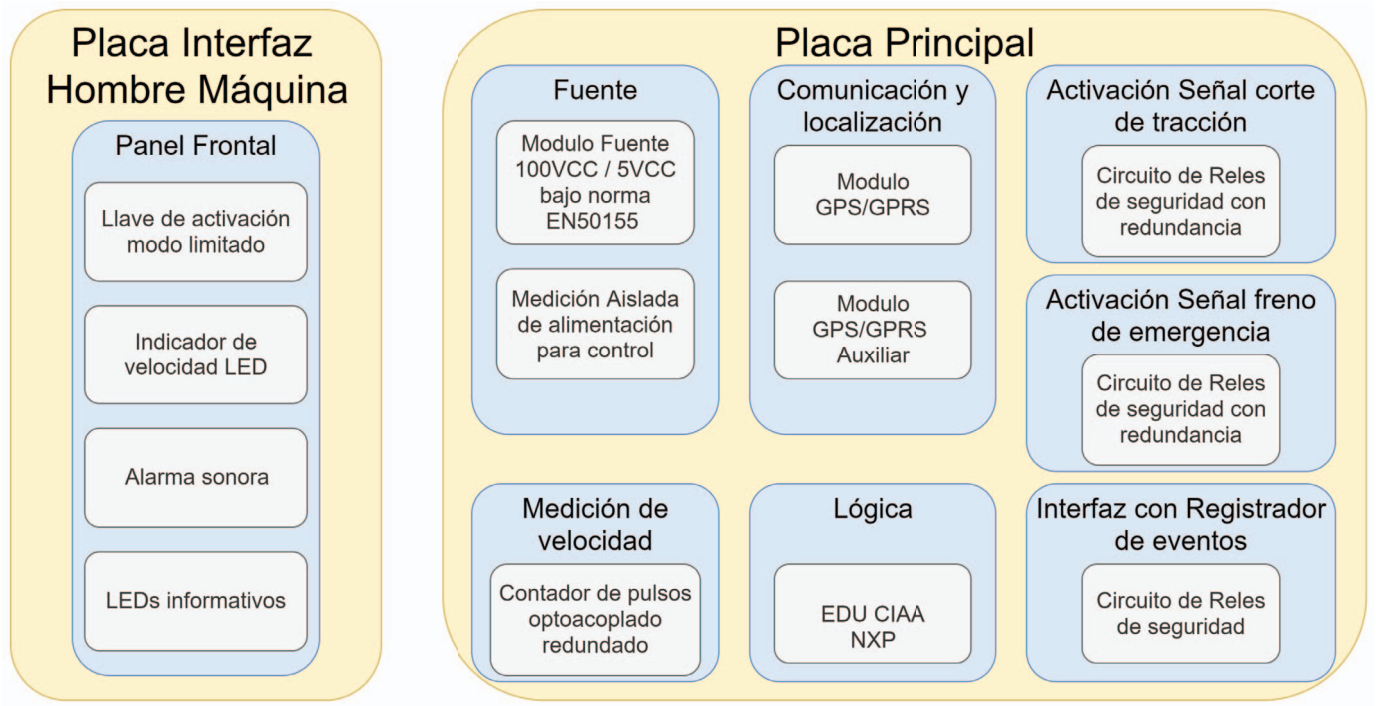

Fig. 3. Diagrama de los módulos que componen el diseño del SAL/T y su agrupación en 2 placas.

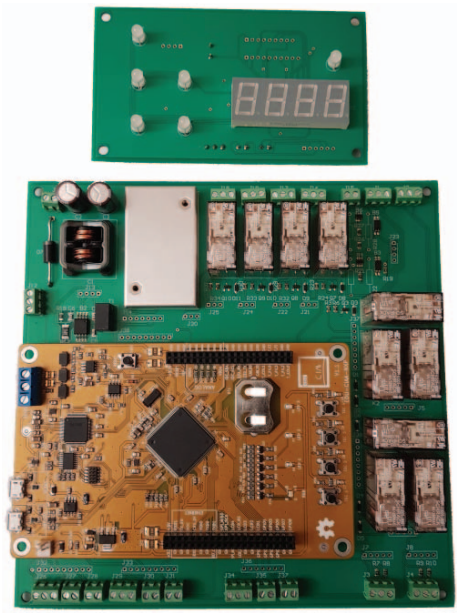

Fig. 4. Hardware del SAL/T, arriba placa interfaz hombre máquina, abajo placa principal.

Fig. 5. Banco de pruebas utilizado para el relevamiento de las tramas emitidas por el equipo Hasler Teloc 1500.

Un desafío técnico que se presentó durante esta implementación fue cómo obtener la información de la velocidad actual del material rodante medida por el equipo Hasler Teloc 1500. Este equipo contiene la medición más confiable de velocidad presente en el sistema ya que es la que se utiliza para informar al conductor y para ser registrada en la caja negra del material rodante. Dicha información se encuentra codificada en un bus RS-485 que une al equipo principal con el display de velocidad. Dada la falta de documentación de dicho bus se procedió a realizar un trabajo de relevamiento de las tramas enviadas para su posterior análisis. En la Fig. 5 se puede observar el banco de medición con el que se obtuvo.

VI. Implementación de Firmware

Para el diseño del firmware del sistema se utilizó una técnica de modelado basada en diagramas de estado. La misma consiste en el diseño de varias máquinas de estados que encapsulan el comportamiento de los diferentes módulos del

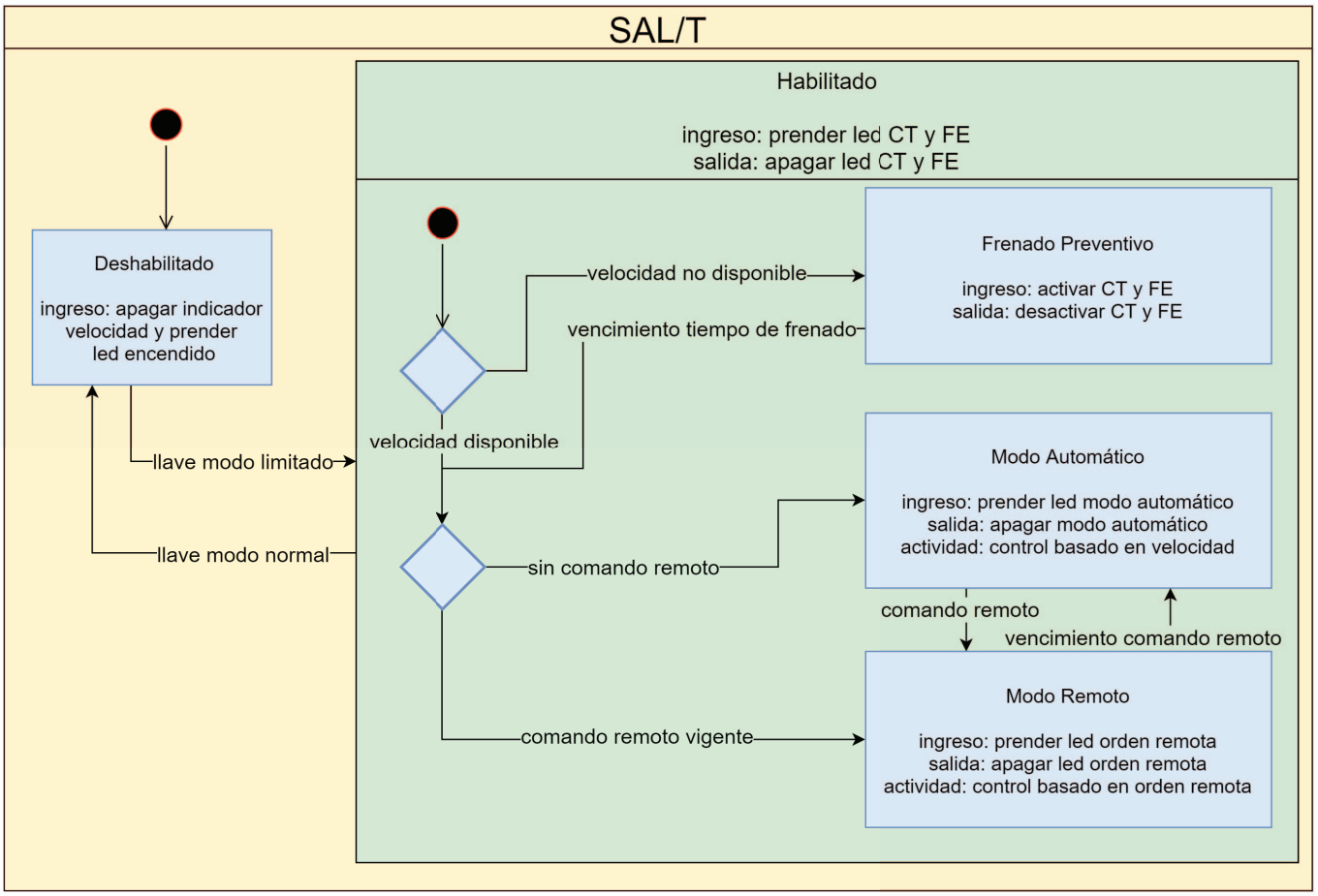

Fig. 6. Representación de la máquina de estados asociada a la lógica de alto nivel del SAL/T.

sistema. Cada máquina de estado está asociada a una función lógica del sistema. Ejemplos de esto son el control de la conexión con los módulos GPS/GPRS, la recepción y envío de información con la central operativa y la lógica de alto nivel del sistema que coordina las diferentes funcionalidades. Una representación gráfica de este último ejemplo puede verse en la Fig. 6, donde se observa la máquina de estados que controla la lógica de alto nivel del sistema. Estas máquinas de estado reaccionan a eventos generados tanto por señales externas al equipo como a los generados por las otras máquinas.

Para la implementación de este firmware se utilizó el framework RKH [16]. El mismo permite implementar la arquitectura mediante objetos activos cuyo comportamiento es representado mediante máquinas de estado. Para la política de planificación de ejecución de las tareas asociadas a estas máquinas de estados se adoptó el planificador nativo provisto por el framework que es del tipo cooperativa no apropiativa. Todo el código fue escrito en C compatible con C99 y mayoritariamente es independiente de la plataforma. El mismo fue hecho utilizando el paradigma de la programación reactiva o dirigida por eventos y principios de la programación basada en objetos.

El framework RKH ya ha sido utilizado en otros desarrollos de sistemas en la industria ferroviaria [17]. Este framework fue desarrollado utilizando patrones de diseño de software como los test unitarios y metodologías de desarrollo como Test-Driven Development (TDD) para mejorar la calidad del mismo [18]. De todas formas, como se explicó en la sección IV, una falla en el firmware no compromete la seguridad de la formación, solo afecta la disponibilidad del SAL/T.

Dentro de estas máquinas de estado es necesario implementar el firmware asociado a los patrones de diseño híbridos planteados durante el diseño del sistema. Un ejemplo de esto es el uso de múltiples fuentes de velocidad. Para esto se definió una sub-máquina de estados que recibe las señales de velocidad de las diferentes fuentes y emite una señal única con la información de la fuente más confiable disponible. La lógica implementada consiste en jerarquizar las diferentes fuentes y utilizar la que se considera más confiable, siempre y cuando la misma sea un valor válido y la última emisión de esta señal se haya recibido dentro de una ventana de tiempo configurable. En caso de que se venza el periodo de validez de una fuente se pasa inmediatamente a tomar como válida la siguiente fuente en la jerarquía. En caso de que se reciba una señal válida de una fuente más confiable se vuelve al estado asociado a dicha fuente.

Para poder obtener la información de la velocidad medida por el equipo Hasler Teloc 1500 fue necesario analizar la trama

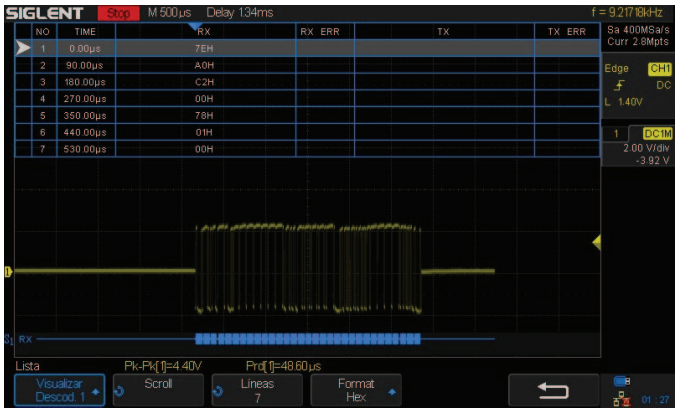

Fig. 7. Trama emitida por el equipo Hasler Teloc 1500 con la información necesaria para el funcionamiento del SAL/T.

de datos del equipo tal como se comentó en la sección V. En la Fig. 7 se puede observar la medición de un paquete de datos completo. Cada trama enviada está formada por 31 bytes de datos, cada uno compuesto por 8 bits en formato LSB. El bus utiliza 1 bit de stop, no usa bits de paridad y tiene una frecuencia de 115200 Hz. Cada una de las tramas empieza y finaliza con un byte con valor hexadecimal 7E. Este flag de inicio y fin es muy útil para la implementación del firmware ya que se puede utilizar para marcar el inicio y fin de una trama y analizarla independientemente del resto. Al simular en el banco de pruebas la velocidad medida por el equipo Hasler se pudo encontrar que tanto los bytes 7 y 8 como los 9 y 10 contienen la información necesaria en formato hexadecimal. Por ejemplo para una velocidad simulada de 120 Km/h el valor de estos bytes era 0x00 0x78 (120 en representación hexadecimal). Otro dato importante para la implementación del firmware es que los bytes 29 y 30 de la trama contienen un código de redundancia cíclica (CRC). Esto permite que la implementación los utilice para decidir si la trama fue leída correctamente y por lo tanto la información de velocidad es válida. Analizando múltiples tramas se dedujo que el algoritmo utilizado para el cálculo de este código CRC es la variante CRC-16/IBM-3740.

En el caso del patrón *canal simple protegido* que se aplicó a los relés que actúan sobre las señales críticas existe una tarea en el sistema que cada un tiempo configurable (por defecto 100 ms) busca discrepancias entre la posición que deberían tener los relés (según el estado del sistema) y la que el sistema mide mediante. En el caso de reiteradas discrepancias en un relé se considera que el mismo se encuentra fallado y se informa que el equipo se encuentra en un estado peligroso.

El módulo de firmware que controla la comunicación entre el SAL/T y la central operativa utiliza el protocolo MQTT. La máquina de estados encargada de esta comunicación fue implementada de forma tal que en caso de cierto número de errores de comunicación entre el equipo y la central operativa la comunicación se realiza mediante el otro módulo GPRS disponible en el SAL/T. De esta forma se puede mejorar la comunicación en zonas donde se encuentran disponibles diferentes proveedores de servicio de datos.

Todos los módulos de firmware comentados en los párrafos anteriores cuentan con diferentes parámetros configurables. Los mismos deben ajustarse según el caso de uso del equipo. Un ejemplo de esto es el parámetro que determina por cuánto tiempo un comando de permiso de cambio de modo es válido. Este parámetro tiene que tener distintos valores para una formación que circula por un área urbana que otra que lo hace por una zona rural. Para maximizar la flexibilidad con la que la central operativa determina la configuración de cada equipo el firmware es capaz de recibir a través del canal MQTT comandos de modificación de estos parámetros. A su vez el SAL/T envía periódicamente a la central operativa su estado completo. El mismo consiste en el valor actual de todos los parámetros configurables, la velocidad actual de la formación y la fuente de dicha información y el número de serie del equipo.

VII. Resultados

Se realizaron pruebas de funcionamiento del sistema emulando las señales del material rodante. Se simularon condiciones normales y de fallas de forma reiterada de modo tal de realizar una prueba de estrés del SAL/T. Durante estas pruebas se utilizó una versión del firmware modificada que reporta los errores a través de una conexión serie local. Ejemplos de posibles errores son la medición de inconsistencias entre la salida teórica y real de los relés que operan sobre señales críticas o la falla de uno de los módulos GPS/GPRS que genera que el sistema utilice el módulo secundario. Durante estas pruebas no se registró ninguno de estos eventos de error.

También se realizó una primera prueba de campo del equipo en el taller de material rodante eléctrico de Victoria del ramal Tigre del tren Mitre. En la Fig. 8 puede verse el banco de medición utilizado durante esta prueba. Allí se conectó al SAL/T un equipo Hasler Teloc 1500 que se encuentra instalado en su banco de pruebas. Durante esta prueba el SAL/T logró medir correctamente las señales del material rodante y reflejar la información simulada por el banco de pruebas en el display del equipo. Esta información fue transmitida a la central operativa periódicamente y se comprobó que la misma era correcta. También se recibieron comandos remotos y se pudo comprobar en el banco de medición que los mismos generaban el efecto esperado. Esta prueba de laboratorio con resultados exitosos es un primer paso necesario para realizar las pruebas de campo en una formación ferroviaria completa.

VIII. Conclusiones

En esta trabajo se presentan las principales características del diseño de un sistema de supervisión de la seguridad del material ferroviario. El mismo se basa en las etapas planteadas en la norma UNE-EN 50126 y en la aplicación de patrones de diseño de hardware para mejorar las características RAMS del sistema. Aplicar esta metodología lleva a un diseño que permite su uso en sistemas críticos como los asociados a la industria ferroviaria.

La correcta utilización de patrones de diseño híbridos requiere de un detallado diseño previo del sistema ya que tiene grandes implicancias en el posterior desarrollo del hardware y

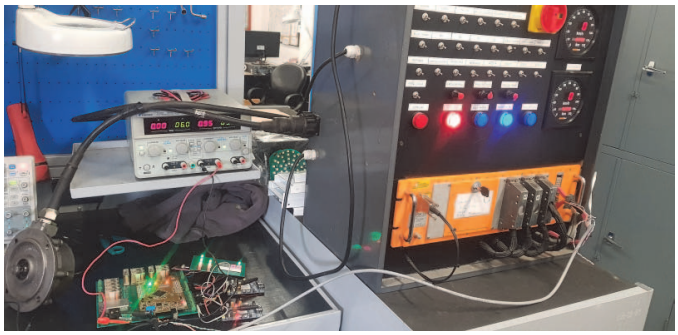

Fig. 8. Banco de pruebas de la primera prueba de campo integral del SAL/T.

el firmware de un sistema embebido al estar integrados no solo en las cuestiones funcionales sino también en las funciones de seguridad.

El desarrollo del primer prototipo del SAL/T fue exitoso dado que se generó un equipo que ha demostrado cumplir con los requisitos pedidos por las especificaciones relevadas tanto en pruebas de laboratorio como de campo. El seguimiento de las normas y la utilización de patrones de diseño desde la concepción del proyecto facilitaron que el mismo se pudiera llevar a cabo exitosamente.

AGRADECIMIENTOS

Este trabajo fue financiado parcialmente mediante el subsidio UBA-PDE Nº8 2018.

REFERENCIAS

[1] IEC 61508-4. “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Part 4: Definitions and abbreviations”. 2010.
[2] Christopher Preschern, Nermin Kajtazovic, Christian Kreiner. ”Catalog of Safety Tactics in the light of the IEC 61508 Safety Lifecycle”. 2013.
[3] UNE-EN 50126-1. “Aplicaciones ferroviarias. Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS). Parte 1: Requisitos básicos y procesos genéricos”. 2005.
[4] Ashraf Armoush. “Design Patterns for Safety-Critical Embedded Systems”. RWTH Aachen University. 2010.
[5] Humberto Luiz Valdivia de Matos, Adilson Marques da Cunha, Luiz Alberto Vieira Dias. “Using design patterns for safety assessment of integrated modular avionics”. 2014.
[6] Tiago Amorim, Helmut Martin, Zhendong Ma. “Systematic Pattern Approach for Safety and Security Co-engineering in the Automotive Domain”. 2017.
[7] UNE-EN 50128. “Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Software para sistemas de control y protección del ferrocarril”. 2012.
[8] Christopher Preschern, Nermin Kajtazovic, Christian Kreiner. ”Building a Safety Architecture Pattern System”. 2015.
[9] Dulcineia Penha, Gereon Weiss, Alexander Stante. ”Pattern-Based Approach for Designing Fail-operational Safety-Critical Embedded Systems”. 2015.
[10] Peter Mann. ”Train Protection & Warning System (TPWS)”. 2011. [Online]. Disponible: https://tinyurl.com/y3vdw4fj
[11] RIS-3437-TOM. ”Defective On-Train Equipment”. 2018. [Online]. Disponible: https://tinyurl.com/y5hljb39
[12] Northern. ”Class 323 drivers manual”. 1992. [Online]. Disponible: http://www.ttweb.co.uk/tra/323tm.pdf
[13] RSSB. ”Preparation and movement of trains: Defective or isolated vehicles and on-train equipment”. 2018. [Online]. Disponible: https://cutt.ly/GERT8000-TW5-Rule-Book
[14] National Transportation Safety Board. ”Railroad accident report: Chicago Transit Authority, collision of trains no. 104 and no. 315 at Addison Street Station, Chicago, Illinois, January 9, 1976”. 1976. [Online]. Disponible: https://tinyurl.com/y2lxjgbg
[15] Bruce Powel Douglass. “Real-Time Design Patterns: Robust Scalable Architecture for Real-Time Systems”. Addison Wesley. 2002.
[16] Leandro Francucci. “RKH framework”. 2010. [Online]. Disponible: https://vortexmakes.com/rkh/
[17] Adrián Laiuppa, Martín Amado, Sergio Gallina, Irrazábal, Emanuel, Iván Sambrana, Hugo Ferrari, Dario Baliña, Leandro Francucci, María de los Ángeles Gómez López, Juan Manuel Cruz, Pablo Gomez, Ariel Lutenberg. “Sistema de monitoreo remoto de barreras ferroviarias automáticas”. 2018.
[18] Vortexmakes ”RKH: State machine framework for reactive embedded systems” [Online]. Disponible: https://github.com/vortexmakes/RKH

Ivan Mariano Di Vito es estudiante de ingeniería electrónica de la UBA. Se encuentra en desarrollo de su tesis de grado en el laboratorio de sistemas embebidos de la FIUBA trabajando en el área de sistemas críticos ferroviarios.
Actualmente se desempeña como CTO y socio fundador de Lab-A Tecnología Asistiva, una empresa dedicada al desarrollo de tecnología para las personas con discapacidad.

Pablo Martín Gomez es Ingeniero Electrónico graduado de la UBA en 2007. En 2015 obtuvo su diploma de Doctor en Ingeniería de la misma universidad, con mención de honor “Summa Cum Laude”.
Actualmente es Jefe de Trabajos Prácticos con dedicación exclusiva en la FI-UBA y Director de la Carrera de Especialización en Sistemas Embebidos y la Maestría (a distancia) en Sistemas Embebidos de la misma Universidad. A su vez, es Secretario de la Asociación Civil para la Investigación, Promoción y Desarrollo de los Sistemas Electrónicos Embebidos.

Ariel Lutenberg es ingeniero electrónico graduado de la UBA en 2006. En 2009 obtuvo su diploma de Doctor en Ingeniería de la misma universidad, con mención de honor “Summa Cum Laude”. En 2018 recibió el Gran Premio INNOVAR por el desarrollo de un sistema de monitoreo remoto de barreras ferroviarias automáticas, y desde 2019 forma parte del jurado del Premio INNOVAR. Por ese proyecto también recibió el primer premio del Concurso “Desafío Eureka”.
Actualmente es Profesor Adjunto con dedicación exclusiva en la FI-UBA, Investigador Adjunto del CONICET, Director del Laboratorio de Sistemas Embebidos de la UBA y Director de la Carrera de Especialización en Sistemas Embebidos y la Maestría en Sistemas Embebidos de la misma Universidad. A su vez, es Presidente de la Asociación Civil para la Investigación, Promoción y Desarrollo de los Sistemas Electrónicos Embebidos.