(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 805 290**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/40 (2006.01)
G06F 21/60 (2013.01)
G06F 21/85 (2013.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.03.2013 PCT/IL2013/050290**

(87) Fecha y número de publicación internacional: **03.10.2013 WO13144962**

(96) Fecha de presentación y número de la solicitud europea: **28.03.2013 E 13720607 (4)**

(97) Fecha y número de publicación de la concesión europea: **20.05.2020 EP 2832070**

(54) Título: **Dispositivo para proteger un sistema electrónico de un vehículo**

(30) Prioridad:

29.03.2012 US 201261617188 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2021

(73) Titular/es:

ARILOU INFORMATION SECURITY TECHNOLOGIES LTD. (100.0%)
7 HaAhim Bejerano St.
Ramat-Gan 5232901, IL

(72) Inventor/es:

LITICHEVER, GIL y
LEVI, ZIV

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Dispositivo para proteger un sistema electrónico de un vehículo

Campo técnico

La presente invención se refiere a sistemas y métodos de seguridad en general, y en particular para proteger un sistema electrónico de un vehículo o sistemas de control industrial de amenazas cibernéticas.

A partir del documento EP 1 309 132 A1 ya se conoce una puerta de enlace en el vehículo interpuesta entre una pluralidad de buses y adaptada para realizar la acción de control apropiada en ciertas situaciones.

Definiciones y antecedentes

DEFINICIONES, TÉRMINOS, ELEMENTOS

Unidad de control electrónico

El término "Unidad de control electrónico" (ECU) indica aquí cualquier sistema electrónico dentro de un vehículo con capacidades de procesamiento (por ejemplo, un sistema de radio es una ECU mientras que un limpiador controlado por un relé no lo es). Una unidad de control electrónico es un tipo de componente electrónico dentro del sistema electrónico de un vehículo.

Algunas ECU incluyen una interfaz de comunicación externa, es decir, una interfaz para comunicarse con componentes fuera del sistema electrónico del vehículo, incluyendo el exterior del propio vehículo. ECU también significa "Unidad de control del motor", que es un caso especial de una Unidad de control electrónico.

Bus

Un bus (también conocido como bus de comunicaciones) es un canal de comunicación inalámbrico o por cable compartido a través del cual diferentes componentes transfieren datos de uno a otro.

Bus de red de área de controlador

Red de área de controlador (CAN o bus CAN) es un estándar de bus de vehículo diseñado para permitir que los sistemas electrónicos se comuniquen entre sí dentro de un vehículo sin un ordenador anfitrión (no se requiere maestro en el bus). Las ECU en un vehículo generalmente se comunican accediendo a un bus CAN. El bus CAN también se usa en sistemas que no son un vehículo, tal como Sistemas de Control Industrial, y la invención abarca los usos del bus CAN o cualquier bus similar en cualquier sistema. Para simplificar la descripción, la mayoría de los ejemplos se referirán a bus CAN y a un vehículo.

Elemento de filtro

El elemento de filtro indica un elemento con dos interfaces que, al recibir un mensaje, lo descarta, lo cambia o lo pasa de acuerdo con varias condiciones, por ejemplo, el valor de ID del mensaje. El elemento de filtro es parte del sistema de seguridad de la invención que se encarga de la lógica del filtrado, por ejemplo, clasificar, analizar y actuar sobre los mensajes recibidos. El elemento de filtro puede ser un módulo de hardware, un módulo de software o un módulo de hardware y software. El elemento de filtro puede contener un módulo lógico adicional para soportar más acciones, tal como generar mensajes por sí mismo, mantener un estado interno o cualquier otra acción.

Elemento proxy

El término elemento proxy al que se hace referencia en el presente documento indica un elemento con al menos una interfaz de comunicación que mantiene el estado actual de acuerdo con una comunicación pasada. El elemento proxy puede enviar mensajes a sus interfaces según su estado actual, la entrada actual (por ejemplo, un mensaje) y el tiempo (por ejemplo, un proceso independiente que envía mensajes de mantenimiento de forma periódica). Este elemento se usa generalmente para permitir que dos partes se comuniquen entre sí indirectamente.

Vectores de ataque

Un vector de ataque es una trayectoria o medios por el cual un atacante puede obtener acceso a un dispositivo computarizado para entregar una carga útil que causará un resultado malicioso. Un automóvil tiene numerosos vectores de ataque, incluyendo la cadena de suministro, acceso físico al bus de comunicación automotriz, reemplazando físicamente una de las ECU del vehículo, utilizando una de las conexiones estándar de la ECU al mundo externo, etc.

La divulgación supone que la mayoría de las amenazas se originan en las conexiones de ECU con el mundo externo. La divulgación asume que cada una de las ECU, excepto el sistema (o dispositivo) de seguridad sugerido, es potencialmente vulnerable a los ataques que podrían ejecutar código malicioso en el mismo y pueden obtener control sobre el mismo. El ataque a cada ECU se puede lograr utilizando cualquiera de sus conexiones de datos (físicas o inalámbricas).

Sistema de seguridad

Sistema de seguridad indica un sistema (que puede implementarse también como un dispositivo) para proteger un componente electrónico o bus dentro de un sistema electrónico de vehículo u otro sistema de control industrial, cuyas realizaciones se describen en la presente divulgación. En algunas realizaciones, el sistema de seguridad es un sistema independiente como se describe en las secciones SISTEMA AUTÓNOMO y SISTEMA DE PASARELA. En algunas realizaciones, el sistema de seguridad está integrado dentro de otro sistema como se describe en la sección SISTEMA INTEGRADO. El sistema de seguridad también se puede indicar por "filtro/proxy de comunicación".

Antecedentes

Amenaza de piratería

Los automóviles son cada vez más sofisticados y utilizan cada vez más la tecnología computarizada (ECU - unidad de control electrónico) para controlar funciones y componentes críticos, tal como la funcionalidad de los frenos y los airbags. Si bien la tecnología computarizada mejora el rendimiento del vehículo, comprometer el funcionamiento de una de estas ECU críticas para la seguridad puede causar daños graves al vehículo, a sus pasajeros y potencialmente incluso a los alrededores si el vehículo está involucrado en un accidente con otro(s) vehículo(s) o peatones.

Estas ECU generalmente se conectan de manera no segura, tal como a través del bus CAN. Tomar el control del bus de comunicación del vehículo puede comprometer las ECU críticas para la seguridad (ver "Experimental Security Analysis of a Modern Automobile" de Koscher et al., Simposio 2010 de IEEE sobre seguridad y privacidad, www.autosec.org/pubs/cars-oakland2010.pdf).

Algunas de las ECU que están conectadas al bus de comunicación del vehículo tienen conexiones externas, tal como el ordenador telemático y el sistema de información y entretenimiento. Es posible comprometer una de estas ECU mediante un ciberataque. La ECU comprometida sirve como punto de entrada para desplegar el ataque mencionado anteriormente, consulte "Comprehensive Experimental Analyses of Automotive Attack Surfaces", Checkoway et al., (Ver www.autosec.org/pubs/cars-usenixsec2011.pdf).

La figura 1 y la figura 2 presentan una red de comunicación de vehículo simple de la técnica que consiste en un único bus.

La figura 1 muestra un sistema electrónico de vehículo **101** que comprende una pluralidad de ECU **75** conectadas a un bus de comunicación de vehículo **105.** Las ECU **75** se comunican entre sí a través del bus de comunicación **105.** Un sistema electrónico del vehículo **101** puede contener múltiples buses de comunicación **105,** cada uno conectado a una o más ECU **75.**

La figura 2 muestra una vista más detallada de un sistema electrónico de vehículo **101** que comprende una pluralidad de ECU con conexiones externas **104,** ECU críticas para la seguridad **100** y otras ECU **106** (sin conexión externa y no críticas para la seguridad).

ECU es con conexiones externas **104** incluyen (pero no se limitan a) telemática **102,** sistema de información y entretenimiento **112,** Sistema de monitorización de la presión de los neumáticos (TPMS) **113,** ECU de comunicación de un vehículo a otro (V2V) o de vehículo a la infraestructura (V2I) **114** y cualquier combinación de ECU con una conexión externa no mencionada específicamente **109.**

Las ECU críticas para la seguridad **100** incluyen (entre otras) la unidad de control del motor **108,** el módulo de control de frenos (ABS/ESC, etc.) **115,** la unidad de control de airbags (ACU) **116,** la unidad de control de la transmisión (TCU) **117** y cualquier combinación de ECU críticas de seguridad no mencionadas específicamente **110.**

Otras ECU **106** indican el conjunto de ECU que no tienen una conexión externa y no son críticas para la seguridad, que incluyen la unidad de control de conveniencia (CCU) **118** y cualquier combinación de ECU que caiga en esta categoría, pero no se mencionan específicamente **111.** Todas las ECU **75** se comunican usando el mismo bus de comunicación compartido **105.** Hay una conexión externa al sistema electrónico **101** usando la ECU telemática **102.** La ECU telemática **102** se comunica usando la conexión inalámbrica **202** ilustrada con un transceptor inalámbrico **201.**

Un sistema electrónico del vehículo **101** puede ser atacado cuando una fuente de comunicación externa (transceptor) **201** establece una línea de comunicación **202** a una ECU, en este ejemplo, la ECU telemática **102.**

El robo de vehículos utilizando la manipulación del bus CAN se vuelve cada vez más popular como se ve en www.hacka-day.com/2012/07/07/keyless-bmw-cars-prove-to-be-very-easy-to-steal/

Otra amenaza financiera que preocupa a los fabricantes de equipos originales y a los proveedores de nivel 1 es el reemplazo no autorizado de ECU **75**. El propietario de un vehículo puede reemplazar una ECU **75** existente por una no auténtica/no original, por varias razones: La ECU **75** necesitaba ser reemplazada por razones de mantenimiento y el reemplazo no autorizado es más barato (el propietario del vehículo puede o no ser consciente de que la ECU **75** no es auténtica); o
El reemplazo le da al vehículo más capacidades de manera similar al ajuste de chips (por ejemplo, elimina las limitaciones del motor que le da más potencia, aunque no está en las especificaciones del motor, lo que lo hace más propenso al mal funcionamiento y/o lo hace inseguro).

El daño a los fabricantes de equipos originales y a los proveedores de nivel 1 se debe a que no se compró su equipo original y a que el reemplazo no autorizado podría dañar el vehículo que todavía está cubierto por la garantía.

Bus de comunicación de vehículo

El bus de comunicación **105** de un vehículo es una red de comunicación interna que interconecta componentes dentro de un vehículo. Ejemplos de protocolos incluyen CAN, Red de interconexión local (LIN), FlexRay, Red de área de vehículos (VAN) y otros.

La figura 1 y la figura 2 presentan un sistema electrónico de vehículo simple de la técnica que consiste en un solo bus.

La figura 3 y la figura 4 presentan un sistema electrónico de vehículo de la técnica que consiste en varios buses **105** o segmentos de bus **105.** Cada segmento de bus **105** puede consistir en un tipo diferente de protocolo de comunicación o en el mismo protocolo de comunicación, pero posiblemente con una configuración diferente.

La figura 3 ilustra un ejemplo del sistema electrónico interno de un vehículo, que comprende varias ECU **102, 112** y **75** conectadas a un bus de comunicación lento **301** y varias ECU **117, 116, 115, 113, 108** y **75** conectadas a un bus de comunicación rápido **305.** Un puente o una puerta de enlace **302** conecta los dos buses **301** y **305.**

La figura 4 es un ejemplo más general del sistema electrónico interno **101** del vehículo ilustrado en la **figura 3,** donde tres buses de comunicación **105** están conectados por una puerta de enlace o puente **302.** Cada bus de comunicación **105** tiene un conjunto de ECU **75** conectados al mismo.

Puerta de enlace/puente de bus CAN

Una puerta de enlace o puente **302** conecta varios segmentos de bus **105** y permite que pasen mensajes entre los mismos. Un puente **302** se describe, por ejemplo, en la Patente de Estados Unidos n.º 6.292.862 titulada "MÓDULO DE PUENTE". Una puerta de enlace **302** se describe, por ejemplo, en la Solicitud de Patente de Estados Unidos n.º 2009/0198856, titulada "PUERTA

DE ENLACE PARA SISTEMA DE BUS DE DATOS".

Las puertas de enlace y los puentes **302** están diseñados para transferir mensajes entre segmentos de bus **105** de manera fiable, pero no están diseñados desde una perspectiva de ciberseguridad. Una perspectiva del diseño dirigido por ciberseguridad, en oposición al diseño dirigido por fiabilidad, es el filtrado de mensajes. Por lo general, un puente o una puerta de enlace **302** no descartará mensajes por la preocupación de que estos mensajes serán necesarios y su ausencia causará daños. Algunos diseños de pasarela **302** exhiben capacidades de monitorización de mensajes seleccionados como el descrito en la Solicitud de Patente de Estados Unidos n.º 2009/0198856. Al monitorizar las comunicaciones, los mensajes seleccionados se envían a una interfaz de monitorización (que se describe a continuación). La monitorización selectiva a menudo se denomina filtrado; sin embargo, este tipo de filtrado no interfiere con la comunicación original.

Monitorización de bus CAN

Un monitor es un dispositivo que entrega mensajes que se envían en un bus **105** (o sus propiedades) a un dispositivo de diagnóstico. Un monitor es un dispositivo autónomo o un módulo/parte en otro dispositivo, tal como una puerta de enlace **302.** Un monitor autónomo se describe en la Solicitud de Patente de Estados Unidos n.º 2006/0182040, titulada "DISPOSITIVO Y MÉTODO DE DIAGNÓSTICO EN LA APLICACIÓN DE CAN DE MÚLTIPLES CANALES". Algunos de estos monitores monitorizan mensajes selectivamente, pero no intervienen con la comunicación en el bus **105.**

Cifrado de bus

El cifrado es un método común para abordar los problemas de autentificación. Métodos de cifrado para bus CAN **105**

se describen en la Solicitud de Patente de Estados Unidos n.º 2011/0093639, titulada "COMUNICACIONES SEGURAS ENTRE Y VERIFICACIÓN DE DISPOSITIVOS CAN AUTORIZADOS" y la Solicitud de Patente de Estados Unidos n.º 2009/0169007, titulada "SISTEMA Y MÉTODO DE CIFRADO DE DATOS DE RED DE ÁREA DE CONTROL".

Si bien el cifrado puede ser la base de la autentificación, desde la perspectiva del sistema no es una solución viable para el entorno automotriz. El entorno automotriz consiste en muchos proveedores y dispositivos. Estos dispositivos suelen ser simples y tienen poca potencia de procesamiento.

Para un esquema de cifrado efectivo, se requiere un intercambio de claves o claves precargadas específicas. Estos son procesos bastante complicados dadas las limitaciones de la industria automotriz y los dispositivos descritos anteriormente.

El bus CAN **105** suele ser bastante lento y el cifrado requiere un ancho de banda adicional que puede ralentizar aún más la comunicación y afectar el rendimiento general del sistema.

Cortafuegos

La figura 5 es un dibujo esquemático de una integración de cortafuegos de la técnica. Un cortafuegos es un dispositivo, o conjunto de dispositivos, diseñado para permitir o denegar transmisiones de red en función de un conjunto de reglas y se utiliza con frecuencia para proteger las redes del acceso no autorizado y permitir la etapa de comunicaciones legítimas.

La figura 5 ilustra dos redes A y B **501** separadas por un cortafuegos **503.** Cada red **501** tiene al menos un ordenador **500** conectado.

Un cortafuegos **503** generalmente está diseñado para redes basadas en el Protocolo de Internet (IP) **501** y usa las características de IP y Protocolo de Control de Transmisión (TCP) de la comunicación. Actualmente, no hay cortafuegos **503** destinados al bus CAN **105.** Los mensajes CAN difieren de los mensajes IP en muchos aspectos, tal como el tamaño, los encabezados, el contenido, etc.

Los supuestos de los diseñadores de cortafuegos de TI **503** difieren de los supuestos necesarios para diseñar una protección para un sistema crítico de seguridad. Una identificación falsa positiva o falsa negativa de un mensaje en el ámbito de TI generalmente no tiene un impacto físico directo (a diferencia del ámbito de los sistemas de control industrial (ICS) donde los ordenadores controlan procesos físicos tales como la temperatura, la presión, los motores, etc.). Un automóvil implica vidas humanas y las ECU **75** influyen directamente en la funcionalidad del automóvil; por lo tanto, un cortafuegos tradicional **503** no es aplicable en este caso.

La implementación del cortafuegos **503** para un bus de comunicación nativo BUS CAN **105** no existe. En general, las soluciones de seguridad de los sistemas de control industrial (ICS) carecen de filtros y cortafuegos **503** y, por lo general, exhiben una solución de separación de red y diodo (comunicación unidireccional). Estas soluciones no son viables para un automóvil, ya que un automóvil requiere comunicaciones bidireccionales.

Sumario de la invención

La presente invención se define por la materia objetivo de las reivindicaciones independientes. Se definen realizaciones preferidas en las reivindicaciones dependientes.

Breve descripción de los dibujos

La figura 1 ilustra un ejemplo del sistema electrónico de un vehículo de la técnica, que comprende ECU y un bus de comunicación;
La figura 2 ilustra un ejemplo más detallado del sistema electrónico de un vehículo de la técnica, que comprende ECU con comunicaciones externas, ECU de seguridad crítica y otras ECU, todas las ECU conectadas a un bus de comunicación. Se establece una conexión externa al sistema electrónico desde una fuente de comunicación externa a la ECU telemática;
La figura 3 ilustra un ejemplo del sistema electrónico interno de un vehículo de la técnica, que comprende ECU conectadas a dos buses de comunicación con diferentes velocidades, y un puente o una puerta de enlace que conecta los dos buses;
La figura 4 es un ejemplo más general del sistema electrónico interno del vehículo de la técnica ilustrado en la **figura 3**, en el que una puerta de enlace o un puente están conectados a múltiples buses de comunicación;
La figura 5 ilustra dos redes de la técnica separadas por un cortafuegos;
La figura 6 es una ilustración del sistema electrónico ilustrado en la **figura 2** en el que todas las ECU con una conexión externa están protegidas por sistemas de seguridad autónomos (filtro/proxy de comunicación), de acuerdo con una realización de la invención;
La figura 7 ejemplifica la integración del sistema de seguridad (filtro/proxy de comunicación) como una puerta de

enlace entre tres buses de comunicación, de acuerdo con una realización de la presente invención;
La figura 8 ilustra la integración del sistema de seguridad (filtro/proxy de comunicación) conectado en serie a una puerta de enlace existente, de acuerdo con una realización de la presente invención;
La figura 9 ilustra la integración del sistema de seguridad (filtro/proxy de comunicación) como un sistema de seguridad integrado dentro de una ECU, de acuerdo con una realización de la presente invención;
La figura 10 ilustra un flujo general de mensajes entre dos buses de comunicación conectados a un sistema de seguridad (filtro/proxy de comunicación), y una conexión a un ordenador de configuración y diagnóstico, de acuerdo con una realización de la presente invención;
La figura 11 es una ilustración en vista superior de los diversos módulos de una realización del sistema de seguridad (filtro/proxy de comunicación), de acuerdo con una realización de la presente invención;
La figura 12 es una ilustración de diagrama de flujo de un ejemplo de gestión de mensajes realizado por la realización ilustrada en la **figura 11,** de acuerdo con una realización de la presente invención;
La figura 13 ilustra un gestor de mensajes de una interfaz básica sin una interfaz de configuración. Este es un ejemplo de una unidad integrada de recepción y transmisión de mensajes, sin la interfaz de configuración, de acuerdo con una realización de la presente invención;
La figura 14 ilustra un gestor de mensajes de una interfaz, que también funciona como unidades de recepción y transmisión de mensajes. Es un ejemplo de una unidad integrada de recepción y transmisión de mensajes, de acuerdo con una realización de la presente invención;
La figura 15 es un diagrama de flujo que ilustra un ejemplo de la gestión de mensajes en un gestor de mensajes tal como se ilustra en la **figura 14,** de acuerdo con una realización de la presente invención;
La figura 16 es un diagrama de bloques que ilustra un ejemplo de un elemento de filtro/proxy (unidad combinada de clasificación de mensajes/analizador de mensajes), de acuerdo con una realización de la presente invención;
La figura 17 es un diagrama de bloques que ilustra un ejemplo del elemento filtro/proxy (unidad combinada de clasificación de mensajes/analizador de mensajes) ilustrada en la **figura 16,** según una realización de la presente invención;
La figura 18 es una ilustración de diagrama de flujo de un ejemplo de una lógica de gestión de mensajes implementada por un elemento de filtro/proxy (unidad combinada de clasificación de mensajes/analizador de mensajes) ilustrada en la **figura 17,** de acuerdo con una realización de la presente invención;
La figura 19 es una ilustración del diagrama de bloques de un ejemplo de una regla de temporización. Una regla de temporización es una regla que puede integrarse en un elemento de filtro/proxy (en la unidad de análisis de mensajes) como una de las reglas utilizadas, de acuerdo con una realización de la presente invención;
La figura 20 es una ilustración de diagrama de flujo de un ejemplo de mensaje gestionado por una regla de temporización ilustrada en la **figura 19,** de acuerdo con una realización de la presente invención;
La figura 21 es una ilustración de diagrama de bloques de un ejemplo de un elemento proxy (en el sistema de seguridad), de acuerdo con una realización de la presente invención;
La figura 22 es una ilustración de diagrama de bloques de un ejemplo de un emulador de enlace tal como el emulador de enlace A de la **figura 21,** de acuerdo con una realización de la presente invención;
La figura 23 es una ilustración de diagrama de bloques de un ejemplo del elemento proxy ilustrado en la **figura 21**. Esta ilustración ejemplifica el uso de un sistema de seguridad que contiene un proxy para proteger un vehículo de los ataques originados por el sistema de información y entretenimiento, de acuerdo con una realización de la presente invención;
La figura 24 es un diagrama de bloques que ilustra un ejemplo de un sistema de seguridad de la invención que consiste en una unidad de recepción de mensajes, una unidad de clasificación de mensajes, una unidad de análisis de mensajes y una unidad de transmisión de mensajes; y
La figura 25 ilustra un ejemplo de dos ECU con sistemas de seguridad integrados de la invención que comprenden unidades de autentificación y conectadas en el mismo bus de comunicación.

MODOS PARA LLEVAR A CABO LA INVENCIÓN

En la siguiente descripción detallada de varias realizaciones, se hace referencia a los dibujos adjuntos, que forman parte de la misma, y en los cuales se muestran, a modo de ilustración, realizaciones específicas en las que la invención puede ponerse en práctica. Se entiende que otras realizaciones se pueden utilizar y se pueden hacer cambios estructurales sin apartarse del alcance de la presente invención.

Las figuras descritas en el presente documento ilustran bloques. Cada bloque puede representar cualquier combinación de hardware, software y/o firmware que realice las funciones como se definen y se explican en el presente documento.

Los vehículos modernos utilizan cada vez más componentes y subsistemas electrónicos e informatizados más eficientes en lugar de piezas mecánicas. Dichos sistemas están controlados por ECU **75,** que están conectadas a través de uno o más buses de comunicación **105.** En caso de que exista más de un bus de comunicación **105**, los buses **105** generalmente están conectados usando puentes o puertas de enlace **302.** Algunos de estos sistemas controlados de ECU **75** son sistemas críticos de seguridad **100,** tal como la unidad de control del motor **108** o el módulo de control de frenos **115,** y algunos son sistemas menos críticos o no críticos, como sistemas de información y entretenimiento **112** y sensores inalámbricos de presión de neumáticos **113.** Algunos de los sistemas mencionados anteriormente son ECU con interfaces externas **104,** por ejemplo, los sensores de presión de los neumáticos **113** se

comunican de forma inalámbrica con un receptor en el bus **105,** la radio **112** tiene conexión inalámbrica (radio, sistema de datos de radio (RDS), etc.) y las interfaces locales (por ejemplo, archivos multimedia) y la telemática **102** (por ejemplo, On-Star™) tienen una interfaz celular **202.**

Aunque estos sistemas computarizados interconectados **75** ofrecen al usuario un mayor rendimiento del vehículo y servicios adicionales, existe un peligro heredado en dicha arquitectura en el que cualquier persona que tenga acceso a un bus de comunicación **105** del vehículo puede interferir maliciosamente con el funcionamiento adecuado de los sistemas **75** comunicando a través del bus **105,** entre ellos los sistemas críticos de seguridad **100.** Hay muchas maneras en que tales ataques pueden lograrse una vez que se obtiene acceso a un bus de comunicación **105.** Algunos ejemplos incluyen: atacar cualquier sistema **75** directamente; enviar mensajes constantemente por el bus **105** evitando que otros se comuniquen (denegación de servicio); hacerse pasar por otros dispositivos **75** que envían mensajes falsos; enviar mensajes que tendrán un efecto nocivo (presione los frenos, desactive el sistema de antibloqueo de frenos **115,** etc.); enviar mensajes para limitar la funcionalidad de una parte 75 (velocidad límite, etc.), etc. En la arquitectura actual del vehículo, no existe un aislamiento seguro entre los sistemas críticos de seguridad **100** y los otros sistemas **104** y **106.**

Algunas realizaciones de la presente invención se refieren a un diseño dirigido por ciberseguridad que interviene selectivamente en la ruta de comunicación para evitar la llegada de mensajes maliciosos a las ECU **75** (en particular, a las ECU críticas para la seguridad **100**). La perspectiva de seguridad sugiere que más daños pueden ser causados por pasar un mensaje potencialmente no deseado que bloqueándolo o cambiándolo. Sin embargo, puede haber implicaciones de fiabilidad. En un diseño dirigido por ciberseguridad, los problemas de fiabilidad se pueden resolver utilizando métodos descritos en el presente documento.

En algunas realizaciones, el sistema de seguridad de la invención incluye un filtro que evita que los mensajes ilegales enviados por cualquier sistema o dispositivo **75** que se comuniquen a través del bus de comunicaciones **105** lleguen a su destino. El filtro de la invención puede, a su discreción, de acuerdo con las reglas preconfiguradas, cambiar el contenido de los mensajes o limitar la velocidad a la que se pueden entregar dichos mensajes, almacenando los mensajes en la memoria intermedia y enviándolos solo en intervalos preconfigurados. Las reglas en el filtro de la invención, que determinan qué mensajes están permitidos y cuáles no, y la velocidad de los mensajes, pueden configurarse usando una interfaz externa del filtro. El sistema de seguridad puede ubicarse, por ejemplo, entre cada componente del sistema que tiene una interfaz externa **109** y el bus de comunicación **105,** protegiendo el bus **105** y los dispositivos electrónicos **75** conectados al componente **109.**

En algunas realizaciones, el sistema de seguridad de la invención tiene al menos dos interfaces de bus **105** y puede filtrar mensajes en cada dirección. El filtrado se realiza de cualquier manera apropiada, por ejemplo, de acuerdo con las propiedades del mensaje (tales como encabezados de mensajes, datos, etc.) y/o de acuerdo con las propiedades del estado interno del sistema de seguridad (tal como la interfaz física a través de la cual el mensaje fue enviado, los horarios, etc.) o cualquier combinación de lo anterior.

En algunas realizaciones, el sistema de seguridad tiene capacidades de proxy. Un proxy guarda el estado de los protocolos de comunicación en una o más de sus interfaces físicas. También gestiona de forma independiente el protocolo de comunicación a través de cada una de sus interfaces (como enviar mensajes de mantenimiento a la radio sin involucrar a otros componentes **75**).

En algunas realizaciones, el sistema de seguridad tiene capacidades de puerta de enlace **302**. Puede conectar dos o más buses de comunicación **105** que pueden tener diferentes propiedades físicas.

En algunas realizaciones, el sistema de seguridad puede guardar sus configuraciones en una memoria no volátil, y las configuraciones y la memoria no volátil pueden actualizarse desde una fuente externa.

En algunas realizaciones, el sistema de seguridad puede guardar estadísticas, datos de monitorización, etc. internamente para su uso posterior, por ejemplo, cuando dichos datos se leen externamente más tarde.

En algunas realizaciones, el sistema de seguridad puede actualizar internamente el contenido de la memoria no volátil.

En algunas realizaciones, el sistema de seguridad puede integrarse dentro de las ECU actuales **75,** entre el controlador físico y la parte lógica de la ECU **75,** ahorrando la necesidad de interfaces físicas adicionales para el sistema de seguridad. En otras realizaciones, el sistema de seguridad puede ser un sistema de seguridad autónomo. El sistema de seguridad autónomo de la invención se puede acoplar a una sola ECU **75,** acoplarse a una pluralidad de ECU **75** o no acoplarse a ninguna ECU **75.**

En algunas realizaciones, el sistema de seguridad puede integrarse en un sistema que contiene uno o más buses de comunicación **105** y ECU **75.** Puede aprender las propiedades de comunicación de las diferentes partes **75** del sistema, construir reglas de filtrado de forma autónoma y filtrar cuando finaliza la fase de aprendizaje.

Algunas realizaciones pueden incluir una combinación de cualquiera de las realizaciones mencionadas anteriormente.

Otros aspectos de la materia objeto actualmente divulgada se harán evidentes al considerar la descripción detallada y los dibujos adjuntos.

INTEGRACIÓN Y COLOCACIÓN DEL SISTEMA

Hay varias realizaciones potenciales de la invención desde el punto de vista de la integración del sistema. En algunas realizaciones, el sistema de seguridad actuará como un sistema o dispositivo de protección entre al menos dos buses de comunicación **105** o componentes **75.**

Atacar un automóvil (sin alterar físicamente o preinstalar una puerta trasera) requiere acceso lógico a sus componentes electrónicos **75.** Las posiciones de integración sugeridas del sistema de seguridad de la invención, de acuerdo con algunas realizaciones, evitan que un acceso lógico incorrecto que se origina desde las interfaces externas **202** alcance los componentes críticos de seguridad **100.** Por lo tanto, la integración del sistema de seguridad puede proteger contra ataques cibernéticos que amenazan la vida. Suponiendo que el sistema de seguridad está configurado correctamente, se logra una protección potencialmente hermética.

En algunas realizaciones, cuando se trata de ajuste de chips, reemplazo no autorizado de ECU **75** y robo de vehículos, el sistema de seguridad de la invención se puede acoplar con ECU **75** que deben protegerse y/o autentificarse (por ejemplo, ECU antirrobo **75,** inmovilizador **110,** unidad de control del motor **108,** etc.)

Si el sistema de seguridad tiene un puerto de configuración, en algunas realizaciones, el puerto de configuración no se conectará a ningún bus de comunicación no fiable **105.**

En algunas realizaciones, el puerto de configuración se puede conectar en banda, es decir, a uno o más de los buses de comunicación **105,** dado que está protegido de alguna manera. En algunas realizaciones, esta configuración en banda es opcional y puede desactivarse después de que se complete la etapa de configuración inicial (por ejemplo, durante la fabricación o montaje del vehículo). En algunas realizaciones, los mensajes de configuración especiales enviados a través del bus de comunicación **105,** se transferirán a la interfaz de configuración para su procesamiento, y provocarán un cambio en la configuración.

DISPOSITIVO AUTÓNOMO

La figura 6 ilustra la integración del sistema de seguridad autónomo, de acuerdo con algunas realizaciones. **La figura 6** es una ilustración del sistema electrónico **101** ilustrado en la **figura 2** protegido por sistemas de seguridad autónomos (referido como dispositivo de filtro de comunicación/proxy) **703** de la invención. Todas las ECU con interfaces de comunicación externa **104** están protegidas por dispositivos de protección de proxy/filtro de comunicación autónomo **703.** Las ECU **104** están conectadas al sistema de seguridad **703** a través de una interfaz **119.** La interfaz **119** puede ser cualquier interfaz de comunicación, incluyendo un bus de comunicación **105.**

En la invención, el sistema de seguridad **703** es un sistema o dispositivo autónomo. El sistema de seguridad **703** tiene al menos dos interfaces de comunicación y además puede tener un puerto de configuración.

En algunas realizaciones, el sistema de seguridad **703** se coloca entre una ECU que tiene una interfaz externa **109** (física o inalámbrica, por ejemplo, radio o telemática) y el bus de comunicación **105.** Cada ECU que tiene una conexión externa **109** puede conectarse en serie al sistema de seguridad **703** para proteger otras ECU **75** de la comunicación que se origina en el mismo.

En algunas realizaciones, el sistema de seguridad **703** está integrado con ECU que no tienen una interfaz externa **106** para hacer frente a amenazas tales como robo de vehículos, ajuste de chips, reemplazo no autorizado de ECU **75,** etc.

En algunas realizaciones, la fuente de alimentación para el sistema de seguridad **703** es externa o se origina en las interfaces de comunicación (una línea dedicada o arrancada desde el bus de comunicación **105**).

Opcionalmente, el sistema de seguridad autónomo **703** puede accionar eléctricamente el bus de comunicación **105** conectado al mismo (por ejemplo, proporcionar tensión negativa y terminación en un bus CAN **105**). Esta opción puede ser configurable para cada uno de los puertos de comunicación, dependiendo de la implementación. Esta opción emula las propiedades físicas del bus **105** hacia cualquier segmento al que esté conectado. En caso de actualización; ahorra la necesidad de instalar un controlador físico adicional en el bus **105.**

En algunas realizaciones, esta integración permite la adaptación de un automóvil, sin reemplazar las ECU existentes **75.**

En algunas realizaciones, cuando cada sistema de seguridad **703** generalmente gestiona solo una ECU **75,** su configuración y operación es bastante simple, y puede implementarse con una arquitectura de hardware simple (en

comparación con otras alternativas).

DISPOSITIVO DE PUERTA DE ENLACE

En la invención, el sistema de seguridad **703** es un sistema o dispositivo autónomo. El sistema de seguridad **703** tiene al menos dos interfaces de comunicación y además tiene un puerto de configuración.

En algunas realizaciones, el sistema de seguridad reemplaza una puerta de enlace/puente existente **302,** como se muestra en la **figura 7,** o está integrado entre una puerta de enlace/puente **302** y uno de sus buses de comunicación conectados **105** como se muestra en la **figura 8.**

Opcionalmente, el sistema de seguridad **703** puede conducir eléctricamente el bus de comunicación **105 de** manera similar al sistema de seguridad autónomo o dispositivo **703** descrito anteriormente.

En algunas realizaciones, si el sistema de seguridad **703** reemplaza una pasarela/puente **302** existente, también funcionará como uno solo (por ejemplo, convirtiendo protocolos, conectando los buses **105**).

Para que este tipo de integración sea efectiva, debe implementarse una arquitectura apropiada de los buses de comunicación **105** de los automóviles. En algunas realizaciones, el diseño puede tener que incluir un sistema de seguridad de la invención **703** en cada ruta entre una ECU crítica de seguridad **110** y una ECU con una interfaz externa **109** (por ejemplo, todas las ECU con una conexión externa **104** están conectadas a un solo segmento **105,** separados de las otras ECU **75** por un sistema de seguridad **703**).

En algunas realizaciones, dicha integración permite la adaptación de un automóvil sin reemplazar las ECU existentes **75.**

En algunas realizaciones, cada sistema de seguridad **703** tiene que manejar la comunicación de varias ECU **75** conectadas al bus. Por lo tanto, la configuración e implementación es potencialmente más compleja y se requiere hardware más complicado. Tal diseño puede requerir la integración de un único sistema de seguridad **703.** Por un lado, dicho sistema de seguridad **703** puede ser más complejo y costoso. Por otro lado, sustituye a múltiples sistemas de seguridad más simples **703;** por lo tanto, puede valer la pena financieramente. Además, el diseño requiere un único punto de configuración que puede ser más conveniente para el diseño y el mantenimiento.

SISTEMA DE SEGURIDAD INTEGRADO

En algunas realizaciones, el sistema de seguridad **703** está integrado dentro de una ECU **905** como se representa en la **figura 9.** El sistema de seguridad **703** tiene al menos dos puertos de comunicación **901** y **903,** uno **903** conectado al controlador de capa física **904** y el otro **901** conectado al resto de la lógica **900** de la ECU (por ejemplo, el controlador de la ECU) utilizando su capa física nativa (por ejemplo, óxido de metal complementario (CMOS) o lógica de transistor-transistor (TTL)). El controlador de capa física **904** está conectado al bus de comunicación **105.**

En algunas realizaciones, la integración del sistema de seguridad **703** dentro de una ECU **905** existente ahorrará muchos componentes (por ejemplo, fuente de alimentación, carcasa mecánica, controladores físicos, etc.) haciendo así que el diseño sea más barato y más robusto.

En algunas realizaciones, el sistema de seguridad **703** se integrará en las mismas ECU **905** (aquellas con interfaces externas **104**) y con las mismas configuraciones que en el caso de un sistema de seguridad autónomo **703.**

En algunas realizaciones, la integración permitirá a un proveedor de ECU **75** integrar una solución de seguridad **703** realizada por un tercero fiable, proporcionando así una ECU completa y segura **905.**

En algunas realizaciones, esta solución no permitirá la adaptación a las ECU existentes **75.** Sin embargo, será viable para nuevos diseños. Esta solución incorpora todas las ventajas del sistema de seguridad autónomo **703.**

Cuando se hace referencia a una ECU 75 acoplada con un sistema de seguridad, también puede referirse a una ECU con un sistema de seguridad integrado como en el caso de **905.**

DISEÑO INTERNO

Por razones de claridad, el núcleo del sistema de seguridad **703** que es responsable de los aspectos de seguridad del sistema de seguridad **703** (por ejemplo, filtrado o que sirve como proxy) se denomina en algunas realizaciones descritas en el presente documento como "elemento de filtro" o "elemento proxy". Sin embargo, es posible que un elemento designado como "elemento de filtro" también pueda proporcionar funcionalidad proxy, y/o un elemento designado como "elemento proxy" también pueda proporcionar funcionalidad de filtro. Todas estas variaciones y combinaciones están abarcadas por la presente invención.

Además, por motivos de simplicidad, el flujo de mensajes se representa en algunas realizaciones en el presente documento como si se usara un filtro simple basado en reglas, aunque puede aplicarse un filtro basado en reglas más complejo y está abarcado por la presente invención. Por ejemplo, se pueden aplicar varias reglas al mismo mensaje.

VISTA SUPERIOR

La figura 10 ilustra la descripción general del sistema de seguridad **703**, en el que el elemento de filtro/proxy **1304** (que funciona como la unidad de clasificación de mensajes y la unidad de análisis de mensajes) se conecta a dos buses de comunicación **105** usando dos gestores de mensajes **1801,** de acuerdo con algunas realizaciones de la presente invención. En algunas realizaciones, el elemento de filtro/proxy **1304** recibe mensajes desde uno de estos buses **105** a través de una memoria intermedia de entrada **1302** (del gestor de mensajes **1801**), filtra estos mensajes y envía los mensajes filtrados a través de la memoria intermedia de salida apropiada **1303** (del gestor de mensajes **1801**), al otro bus de comunicación **105.** El sistema de seguridad **703** también puede servir como una puerta de enlace de filtrado entre dos buses **105** diferentes y realizar las conversiones necesarias (tales como conversiones de protocolo) entre los buses **105,** como se ve en la **figura 7.**

En la invención, como se ve en la **figura 10,** el sistema de seguridad **703** está configurado por un dispositivo externo (por ejemplo, ordenador de configuración/diagnóstico) **1408,** a través de una interfaz fuera de banda (OOB) tal como una conexión en serie (por ejemplo, RS-232). La configuración afecta el comportamiento del sistema de seguridad **703**, los mensajes que deja pasar, los cambios o los bloqueos, y cualquier otra de sus propiedades configurables. La nueva configuración se puede guardar, de modo que la próxima vez que se reinicie el sistema de seguridad **703**, la nueva configuración se ejecutará al inicio.

El gestor de mensajes **1801** incluye (1) una unidad de recepción de mensajes para recibir un mensaje a su memoria intermedia de entrada **1302** desde el bus de comunicación **105;** y (2) una unidad de transmisión de mensajes para transmitir un mensaje desde su memoria intermedia de salida **1303** al bus de comunicación **105.**

La figura 11 ilustra la vista superior del sistema de seguridad **703** con más detalle que el ilustrado en la **figura 10,** de acuerdo con algunas realizaciones de la presente invención. Los mensajes que llegan al gestor de mensajes **1801** (descrito con más detalle en la **figura 14,** y también funciona como la unidad de recepción de mensajes y la unidad de transmisión de mensajes) a través de la interfaz física E/S **1800,** o cualquier otra interfaz de la misma, se envían a la interfaz adecuada. Si se envía a la interfaz de configuración, será manejado por el módulo de configuración, estadísticas y control **1807** que puede manejarlo de cualquier forma configurada (por ejemplo, enviarlo a través de la interfaz OOB E/S **1806** fuera del sistema para el registro, inspección o cualquier otro propósito). Si el mensaje se envía al elemento de filtro/proxy **1304,** lo inspecciona y decide si lo envía a la interfaz de destino o no. Si el elemento de filtro/proxy **1304** (unidad combinada de clasificación de mensajes y unidad de análisis de mensajes) debe enviar el mensaje a la interfaz de destino, se enviará al gestor de mensajes apropiado **1801.** El gestor de mensajes **1801** gestiona el mensaje en algunas realizaciones como se representa en la **figura 14** y la **figura 15,** y lo envía a la interfaz de destino adecuada (por ejemplo, la interfaz física E/S B 1800). Las interfaces **1808** entre los gestores de mensajes **1801** y el elemento de filtro/proxy **1304** se denominan "interfaz de proxy" y se ajustan tanto a los filtros como a los proxies (también pueden denominarse "interfaz de filtro" o "interfaz de filtro y/o proxy").

Algunas realizaciones del proceso descrito se ilustran en la **figura 12.** En la etapa **3200,** se recibe un mensaje en la unidad de recepción de mensajes de la interfaz **1801** del gestor de mensajes, por ejemplo, por su interfaz física, y se envía a una o más de sus interfaces en la etapa **3201.** Si el mensaje se debe enviar a la interfaz física, se envía a su interfaz física en la etapa **3202.** Si el mensaje se va a enviar a la interfaz de configuración **1602,** es gestionado por la interfaz de configuración **1605** de acuerdo con su funcionalidad, por ejemplo, impreso en la pantalla del operador, escrito en un registro, etc. en la etapa **3204.** Si el mensaje se debe enviar a la interfaz de filtro/proxy **1604,** se envía al elemento de filtro apropiado **1304,** y se clasifica por su unidad de clasificación de mensajes en la etapa **3203,** que lo envía a la unidad de análisis de mensajes del elemento de filtro. El elemento de filtro **1304** comprueba entonces la legalidad del mensaje (mediante el analizador de mensajes) en la etapa **3205.** Si el mensaje es ilegal, se descartará en la etapa **3206.** Si el mensaje es legal, se envía a su destino (que puede ser el gestor de mensajes opuesto **1801**) en la etapa **3207.**

GESTOR DE MENSAJES

La figura 13 representa la forma simple del mecanismo de tratamiento de mensajes **1801** que cada interfaz (elemento de filtro/proxy **1304**) tiene, según algunas realizaciones de la presente invención. En algunas realizaciones, cada mensaje que llega desde una interfaz física **1800** es procesado por una unidad de recepción de mensajes de un gestor de mensajes **1801** y enviado a la memoria intermedia de entrada **1302** del elemento de filtro/proxy **1304.** Cada mensaje que se origina en el gestor de mensajes de otra interfaz y está destinado a la interfaz **1800** y permitido por el elemento de filtro/proxy **1304** se envía a la memoria intermedia de salida apropiada **1303.** Desde la memoria intermedia de salida **1303** se envía a la unidad de transmisión de mensajes del gestor de mensajes **1801** y se envía a la interfaz física **1800.** La unidad de recepción de mensajes y la unidad de transmisión de mensajes pueden ser unidades separadas o integradas juntas en un gestor de mensajes **1801** para comunicaciones bidireccionales más eficientes con un bus de comunicación **105.**

La figura 14 describe una forma más compleja del gestor de mensajes de interfaz **1801** que la descrita en la **figura 13,** de acuerdo con algunas realizaciones de la presente invención. Cada mensaje que llega desde una interfaz física de E/S **1800** a la interfaz física **1602** a través del transceptor **1301** va al componente de enrutamiento **1603.** El componente de enrutamiento puede determinar los encabezados internos del mensaje (tal como la fuente del mensaje o cualquier otra información sobre el mensaje) y a continuación decide hacia qué destino enviar el mensaje, de acuerdo con su algoritmo de enrutamiento. Los destinos posibles incluyen, entre otros, cero o más de las interfaces ilustradas en la figura a través de sus respectivas memorias intermedias de entrada, tales como: la interfaz física **1602,** la interfaz de filtro/proxy **1604** o la interfaz del módulo de configuración **1605.** También puede haber muchas otras interfaces similares. El mensaje se envía a la interfaz adecuada que lo gestiona. El componente de enrutamiento **1603** se puede configurar a través del módulo de configuración **1807** (el flujo de datos de configuración no se dibuja explícitamente), para cambiar su comportamiento, tal como cambiar sus tablas de enrutamiento o algoritmo de enrutamiento. Los mensajes que llegan del elemento de filtro/proxy **1304** a través de su interfaz de E/S **1808** se envían al componente de enrutamiento que los envía a la interfaz adecuada como se describe anteriormente. Los mensajes que llegan a la interfaz del módulo de configuración **1605** desde el componente de enrutamiento se envían al módulo de configuración **1807** a través de la memoria intermedia de salida de configuración **1607** y el transceptor de interfaz externo **1608.** El transceptor de interfaz externo **1608** puede implementarse como un módulo de software y/o hardware. En algunas realizaciones, el transceptor de interfaz externo **1608** es opcional y puede omitirse. El módulo de configuración **1807** gestiona mensajes de varias maneras, por ejemplo, imprimir en la pantalla del operador (si existe), y puede usarse para cualquier propósito, por ejemplo, inspección, envío de mensajes, control o depuración del sistema. **La figura 15** describe el flujo de mensajes en el gestor de mensajes **1801** de la interfaz, de acuerdo con algunas realizaciones. La unidad de recepción de mensajes recibe un mensaje en una de las interfaces del gestor de mensajes en la etapa **3200.** Los encabezados del mensaje se pueden determinar en la etapa **3301,** y la ruta apropiada del mensaje se decide en la etapa **3302.** El mensaje se envía a continuación a su interfaz de destino en la etapa **3303.** El clasificador y el analizador son parte del elemento de filtro/proxy **1304,** por lo que solo si el mensaje se dirige al elemento de filtro/proxy **1304**, lo gestionarán. Las otras opciones de enrutamiento de un mensaje son a la interfaz física **1602** o la interfaz de configuración **1605.** Dado que el clasificador y el analizador no son parte del gestor de mensajes, **1801** no se describen aquí. El gestor de mensajes de la interfaz **1801** puede recopilar y guardar cualquier información estadística sobre el sistema y los mensajes que se envían al mismo o desde el mismo (por ejemplo, el número de mensajes que se recibieron o se enviaron a cada interfaz).

En algunas realizaciones, cada elemento de filtro **1304** está acoplado con al menos 2 de dichos gestores de mensajes **1801** y cada elemento proxy **1304** está acoplado con al menos uno de dichos gestores de mensajes **1801,** uno para cada interfaz a la que están conectados.

MÓDULO DE CONFIGURACIÓN

El "módulo de configuración" **1807** indica el "módulo de configuración, estadística y control" **1807** (algunas realizaciones se ilustran en la **figura 11**).

En algunas realizaciones, el módulo de configuración **1807** está conectado al gestor de mensajes de la interfaz **1801** usando dos tipos de conexiones: una conexión de mensajes **1609** y una conexión de configuración **1810.** El módulo de configuración **1807** puede enviar o recibir mensajes hacia/desde el gestor de mensajes de la interfaz **1801** a través de la conexión de mensajes **1609.** El módulo de configuración **1807** está conectado al elemento de filtro/proxy **1304** usando una conexión de configuración **1810.** El módulo de configuración **1807** controla la configuración del elemento de filtro/proxy **1304** y los gestores de mensajes **1801** a través de la conexión de configuración **1810,** cambiando su comportamiento, registrando sus actividades y/o cualquier otro cambio configurable que admitan. Este módulo **1807** se controla externamente utilizando una interfaz OOB (interfaz externa de E/S) **1806,** que puede ser cualquier interfaz de datos (por ejemplo, interfaz de transmisor receptor asíncrono universal (UART)). El módulo de configuración **1807** también puede tener conectada una memoria no volátil **1805** (por ejemplo, memoria flash). Esta memoria **1805** almacena datos que utiliza el módulo de configuración **1807.** Dichos datos pueden incluir, pero no se limitan a, diferentes configuraciones del sistema que se cargarán en los componentes del sistema (por ejemplo, los elementos de filtro **1304** y los gestores de mensajes de las interfaces **1801**), e información estadística. También podría, pero no necesariamente, manipular esta memoria **1805,** a través de la interfaz OOB **1806** o directamente. Dicha manipulación puede incluir, pero no se limita a, borrar la memoria, copiarla, descargarla, copiar nueva información, etc.

En algunas realizaciones, el módulo de configuración **1807** puede conectarse en banda, es decir, a uno o más de los buses de comunicación **105,** dado que está protegido de alguna manera. En algunas realizaciones, esta configuración en banda es opcional y puede desactivarse después de que se complete la etapa de configuración inicial (por ejemplo, durante la fabricación o montaje del vehículo).

ELEMENTO DE FILTRO/PROXY

La figura 16 ilustra un ejemplo simple de un elemento de filtro/proxy (unidades combinadas de clasificación de mensajes y analizador de mensajes) **1304,** construido a partir de dos componentes de filtrado de interfaz **2001,** de acuerdo con algunas realizaciones de la presente invención. Cada componente de filtro de interfaz **2001** filtra los

mensajes que llegan desde su interfaz de entrada (unidad de recepción de mensajes) y los envía después de filtrarlos a su interfaz de salida (unidad de transmisión de mensajes). Un ejemplo más detallado de **2001** se ilustra en la **figura 17,** de acuerdo con algunas realizaciones. Un mensaje llega desde la entrada de interfaz de proxy **2000** del gestor de mensajes **1801,** y entra en el selector de reglas **2100** de la unidad de clasificación de mensajes (también denominado clasificador), que de acuerdo con las propiedades del mensaje (tal como encabezados, origen, destino, datos o cualquier otra propiedad) lo envía a la regla apropiada **2102** en la unidad de análisis de mensajes. Si no se encuentra una regla adecuada, el selector de reglas rechaza el mensaje de acuerdo con su política (las políticas posibles se describen a continuación). La regla apropiada **2102** (de la pluralidad de reglas **2102**) que recibe el mensaje lo verifica más a fondo y decide si el mensaje debe permitirse o no, o si debe modificarse. La acción sobre el resultado de una regla **2102** es parte de la unidad del analizador de mensajes. Si se debe permitir el mensaje, la regla **2102** pasa el mensaje a la salida de interfaz proxy **2002** conectada a la unidad de transmisión de mensajes del gestor de mensajes **1801.** Si se debe cambiar el mensaje, la regla **2102** (del analizador) puede hacer los cambios necesarios y pasar el mensaje a la salida de interfaz proxy **2002** conectada a la unidad de transmisión de mensajes. En algunas realizaciones, si no se debe permitir el mensaje, se notifica al selector de reglas **2100** y elige la siguiente regla apropiada **2102** para el mensaje o rechaza el mensaje de acuerdo con su política. Si no se encuentran más reglas apropiadas **2102**, el selector de reglas **2100** actúa de acuerdo con su política en tal caso. La política del selector de reglas **2100** puede incluir, entre otros, descartar el mensaje, notificar al remitente o realizar cualquier acción preconfigurada. Una regla **2102** puede ser de cualquier tipo y también puede ser una regla de temporización como se describirá a continuación. Una regla **2102** puede requerir que se firme un mensaje, que se verifique la firma de un mensaje o que se transmita condicionalmente un mensaje como se describe en la sección del módulo de autentificación a continuación. Debe quedar claro que el término regla **2102** abarca cualquier combinación de una pluralidad de reglas **2102,** por lo que se puede aplicar más de una regla **2102** a cualquier mensaje. El número de reglas **2102** no está limitado y puede variar. En algunas realizaciones, el módulo de configuración **1807** también puede controlar la adición o eliminación de reglas **2102** dinámicamente. Una regla **2102** puede contener cualquier lógica de filtrado para decidir si un mensaje es legal o no. Dicha lógica puede incluir, entre otros, propiedades del mensaje, encabezados del mensaje, contenido del mensaje, longitud del mensaje, estado del filtro, tiempos del mensaje o cualquier otro parámetro o propiedad o cualquier combinación de estas propiedades, de una manera de lista blanca o negra. Un ejemplo de lógica de filtrado puede ser verificar que el destino del mensaje sea 'y', que la ID del mensaje esté entre 'xx' y 'zz', la longitud de los datos del mensaje es 3 y los dos primeros bytes del mensaje son 'aa' y 'bb'.

La figura 18 ilustra un ejemplo de la lógica del filtro y el flujo de mensajes descritos, de acuerdo con algunas realizaciones. El mensaje se recibe en la entrada de la interfaz de proxy en la etapa **3000** y se entrega al selector de reglas de unidad de clasificación de mensajes **2100,** que selecciona la siguiente regla de filtro apropiada **2102** para filtrar el mensaje en la etapa **3001.** Si no se encuentra la regla apropiada **2102**, el mensaje puede descartarse en la etapa **3206.** Si se encontró una regla **2102**, mediante la regla **2102** (mediante la unidad de análisis de mensajes) se comprueba el mensaje para determinar su legalidad de acuerdo con la regla **2102** en la etapa **3003.** Si el mensaje no es legal de acuerdo con la regla **2102,** vuelve al selector de reglas **2100** para seleccionar la siguiente regla apropiada **2102** en la etapa **3001.** En algunas realizaciones, si el mensaje es legal de acuerdo con la regla **2102,** se envía a la salida de la interfaz proxy **2002** en la etapa **3207.**

REGLAS DE TEMPORIZACIÓN

La figura 19 describe una regla de temporización **2300,** que es un tipo de regla **2102** que se puede agregar a la lista de reglas **2102** (por ejemplo, como regla **2102**) en el elemento de filtro **1304** descrito anteriormente, de acuerdo con algunas realizaciones de la presente invención. La diferencia entre una regla de sincronización **2300** y una regla regular **2102** es que la regla de sincronización **2300** no solo filtra los mensajes entrantes, sino que también aplica el límite de velocidad de acuerdo con una política que también puede incluir la configuración del tráfico de la comunicación, por ejemplo, el envío mensajes a la interfaz proxy **1808** en tiempos predefinidos (depósito con fugas), evitando así ataques de denegación de servicio (DOS). Cuando el selector de reglas **2100** envía el mensaje recibido a una regla de temporización **2300,** la lógica de filtrado **2301** funciona como en una regla regular **2102.** En caso de que se permita el mensaje, se envía a través de la interfaz **2302** a la memoria intermedia de salida de la regla **2303,** en el que está almacenado en la memoria intermedia y esperando ser enviado a la salida de la interfaz proxy **2002.** Cuando llega el momento correcto, la función de tiempo **2305** verifica si hay mensajes esperando en la memoria intermedia de salida **2303,** y si es así, extrae un mensaje a través de la interfaz **2304** y lo envía a la salida de interfaz proxy **2002.** En caso de que el mensaje sea ilegal, la lógica de filtrado **2301** rechazará el mensaje. En cualquier caso, ya sea un mensaje legal o ilegal, el selector de reglas **2100** puede ser notificado del resultado de la operación.

La figura 20 ilustra un ejemplo de la lógica de la regla de temporización **2300** y el flujo de mensajes descrito, de acuerdo con algunas realizaciones. El mensaje se recibe en la entrada de la interfaz proxy **2002** en la etapa **3000** y se está filtrando como en una regla regular (no temporizada) **2102** en la etapa **3101**). Si el mensaje es ilegal, se descarta en la etapa **3102.** En caso de que el mensaje sea legal, se almacena en la memoria intermedia de salida de la regla de temporización **2300** y espera ser enviado en la etapa **3103.** Cuando llega el momento, la tarea de temporización de la regla **2300** transfiere el mensaje que espera en la memoria intermedia de salida a la unidad de transmisión para enviarlo a su destino en la etapa **3104.** La ventaja de usar una regla de temporización **2300** es la prevención de ataques de DOS. Los ejemplos de tales ataques de DOS incluyen, entre otros, el envío rápido de mensajes y el tiempo planificado de envío de mensajes. Además, este tipo de regla puede ayudar a manejar el mal funcionamiento enviando

muchos mensajes a través del bus de comunicación **105** que conduce a DOS. Otra ventaja es la capacidad de dicho filtro para tender un puente entre dos buses **105** con diferentes capacidades para gestionar el ritmo de los mensajes. Este tipo de filtro **703** es bastante simple de configurar en comparación con otros filtros con estado y puede gestionar muchas amenazas.

PROXY

La figura 21 ilustra el diseño del elemento proxy **2500**, de acuerdo con algunas realizaciones de la presente invención. El elemento proxy **2500** está conectado a uno o más gestores de mensajes **1801** a través de las interfaces **1808.** Cada elemento proxy **2500** está compuesto por emuladores de enlace (uno para cada interfaz) **2501** y un filtro de estado y actualizador **2502.** Un elemento proxy **2500** emula la operación de un segmento de bus **105** hacia el otro sin permitir la comunicación directa entre los segmentos. Todos los mensajes transferidos hacia cualquier segmento usando un elemento proxy **2500** son creados por el elemento proxy **2500** usando sus máquinas de estado y reglas (a diferencia de un filtro convencional que permite que pasen mensajes que no están bloqueados).

En algunas realizaciones, es posible usar un elemento proxy **2500** conectado solo a un gestor de mensajes **1801,** en caso de que sea necesario emular un lado desconectado como si estuviera conectado. Un ejemplo para tal caso puede ser ensamblar una radio que necesita una conexión al vehículo sin hacer la conexión, emulando dicha conexión usando un elemento proxy **2500.**

La figura 22 ilustra una realización de un emulador de enlace **2501** que emula un protocolo de comunicación entre dos o más participantes hacia los participantes que están conectados a su lado emulado (por ejemplo, si TCP es el protocolo, el emulador enviará mensajes Ack (reconocimiento) para cada mensaje recibido), de acuerdo con algunas realizaciones. El emulador de enlace **2501** gestiona y guarda un estado de la comunicación (por ejemplo, si TCP es el protocolo, el emulador guardará una ventana de los mensajes reconocidos). El estado que almacena el emulador de enlaces puede incluir datos y metadatos relacionados con los mensajes recibidos y enviados. El emulador de enlace **2501** puede actualizar el filtro de estado y el actualizador pasiva o activamente con su estado actual. La comunicación se verá afectada por el estado del emulador de enlace, los mensajes recibidos y la hora.

En algunas realizaciones, el emulador de enlace **2501** ilustrado en la **figura 22** consiste en una capa de abstracción de protocolo/controlador de alto nivel **2601,** una máquina de estado **2602** y un módulo de datos de estado/configuración **2603.** Una capa de abstracción de protocolo **2601** actúa como una capa de abstracción de los protocolos de comunicación que gestiona el elemento proxy **2500**. Se comunica de manera relativamente simple con la máquina de estado **2602,** mediante el envío de mensajes de metadatos, estado y comandos a través de la interfaz **2604.** La máquina de estado **2602** implementa la lógica que incluye el emulador de enlace **2501**. La lógica que implementa la máquina de estados **2602** incluye, pero no se limita a, actualizar el estado, responder inmediatamente a eventos, etc. (por ejemplo, al recibir un mensaje TCP actualiza la ventana almacenada en **2603,** cambia el estado y envía un mensaje Ack a través del capa de abstracción de protocolo **2601**). El módulo de datos de estado/configuración **2603** almacena el estado actual del emulador de enlace **2501** y se puede acceder tanto por la máquina de estado **2602** por el filtro de estado y el actualizador **2502.** La máquina de estados **2602** y los módulos de datos de estado/configuración **2603** se comunican enviándose estados entre sí a través de la interfaz de estado **2605.**

En algunas realizaciones, el filtro de estado y el actualizador **2502** lee el estado de cada emulador de enlace **2501** usando el enlace de estado de lectura **2504** de forma pasiva o activa y de acuerdo con la lógica del proxy, configura el estado en cada uno de los emuladores de enlace **2501** a través del enlace de configuración **2503.** En algunas realizaciones, los mensajes nunca se transfieren directamente entre los emuladores de enlace **2501;** la única comunicación entre los emuladores de enlace **2501** es mediante una actualización de estado. El filtro de estado **2502** permitirá que solo pasen estados legítimos entre los emuladores de enlace **2501.**

En algunas realizaciones, la lógica del elemento proxy **2500** es codificada o configurable.

Los filtros de estado convencionales existentes tienen una máquina de estado interna que intenta emular el estado de los mensajes transferidos y cuando la máquina de estado descubre una anomalía, los mensajes se descartan. Cuando la máquina de estado del filtro es diferente de la máquina de estado utilizada por las partes que se comunican, puede ocurrir un estado inconsistente entre el filtro y las partes que se comunican, lo que permite que pase la comunicación prohibida (por ejemplo, una configuración de tiempo de espera TCP diferente). En algunas realizaciones, permitir que solo pase un estado entre los emuladores de enlace y diseñar correctamente el proxy, puede resolver el problema mencionado anteriormente.

Ahora se describe un ejemplo de aplicación proxy de acuerdo con algunas realizaciones de la materia objeto actualmente divulgada:
Una radio **112** a menudo usa la pantalla integrada del vehículo para mostrar información (por ejemplo, la frecuencia de la estación de radio). El ejemplo asume que una comunicación normal de radio-vehículo es entre la radio y el sistema de visualización. El sistema de visualización envía su tipo de modelo y envía repetidamente un mensaje de mantenimiento de vida. La radio **112** se comunica con el sistema de visualización, consulta el tipo de modelo y envía datos de visualización de acuerdo con las capacidades de la pantalla.

Una aplicación de elemento proxy **2700,** como se ve en la **figura 23,** consiste en un emulador de enlace **2701** hacia el vehículo **2708,** un emulador de enlace **2703** hacia la radio **112** y un filtro de estado y actualizador **2502,** de acuerdo con algunas realizaciones. El elemento proxy es solo una parte del sistema de seguridad **703,** que se omitió de la figura por motivos de claridad.

El emulador de enlace **2701** hacia el vehículo **2708** está conectado entre el vehículo **2708** y el filtro de estado y el actualizador **2502.** Contiene el texto formateado (datos de pantalla) **2704** designado para la pantalla y el tipo de pantalla (estado) **2705.** Al inicio, este emulador de enlace hacia el vehículo **2701** consulta el sistema de visualización para su tipo, almacena la información en **2705** y la envía al filtro de estado y al actualizador **2502.** El emulador de enlace hacia el vehículo **2701** está en modo operativo si contiene datos de visualización válidos y un tipo de visualización válido. Cuando está en modo operativo, el emulador de enlace **2701** envía mensajes que contienen datos de visualización en cada cambio de datos de visualización según el tipo de visualización.

El emulador de enlace hacia la radio **2703** está conectado entre la radio **112** y el filtro de estado y el actualizador **2502.** Contiene el mismo tipo de registros que el emulador de enlace hacia el vehículo **2701.** Al inicio, el emulador de enlace **2703** espera recibir un tipo de visualización del filtro de estado y el actualizador. Una vez que el emulador de enlace **2703** tiene un tipo de visualización válido en **2707**, responde a las consultas sobre el tipo de visualización recibido desde la radio. El emulador de enlace **2703** envía mensajes repetidos de mantenimiento a la radio. El emulador de enlace **2703** almacena los datos de los mensajes de pantalla recibidos de la radio en el registro de datos de pantalla **2706.** Si se cambia el registro de datos de visualización **2706**, el emulador de enlace **2703** envía el nuevo estado al filtro de estado y al actualizador **2502.**

El filtro de estado y el actualizador **2502** reciben el tipo de visualización desde el emulador de enlace hacia el vehículo **2701.** Si el tipo de visualización es válido, el filtro de estado y el actualizador **2502** lo envían al emulador de enlace hacia la radio **2703.** El filtro de estado y el actualizador **2502** reciben los datos de visualización desde el emulador de enlace hacia la radio **2703.** Si los datos de la pantalla son válidos, envían los datos al emulador de enlace hacia el vehículo **2701.**

Debe entenderse que las reglas **2102** descritas anteriormente son simplemente un ejemplo de posibles tipos de reglas **2102,** y las reglas **2102** también pueden ser cualquier tipo de otras reglas **2102,** o cualquier combinación de las mismas. Existe la posibilidad de combinar las reglas **2102** en una fila, de modo que el mensaje de salida de una regla **2102** se enviará como entrada a la siguiente regla **2102.** Una regla **2102** también puede cambiar las propiedades del mensaje, el contenido o cualquier otro dato relacionado con el mensaje, antes de enviarlo a su interfaz de salida **2002.** Cualquier persona experta en la materia y que lea la memoria descriptiva actual podrá aconsejar inmediatamente diferentes tipos y combinaciones de reglas **2102,** y todas estas reglas **2102** están abarcadas por la presente invención.

ECU CRÍTICA CON COMUNICACIÓN EXTERNA

Algunas realizaciones descritas anteriormente se relacionan con la protección de las ECU críticas de seguridad **100** que no tienen ninguna interfaz de comunicación externa. Sin embargo, en las realizaciones en las que las ECU críticas para la seguridad **100** tienen interfaces de comunicación externas, el sistema de seguridad **703** también se puede usar para proteger las ECU **75** como se describe en esta sección.

En algunas realizaciones, las ECU críticas de seguridad **100** tienen una interfaz de comunicación externa (por ejemplo, algunas ECU de comunicación de vehículo a vehículo (V2V) pueden ordenar al vehículo que frene). Dicha ECU podría enviar mensajes críticos (es decir, tener efecto sobre el comportamiento del vehículo) y mensajes no críticos (por ejemplo, información de tráfico). Los mensajes no críticos se pueden filtrar de la misma manera que se describe en las secciones anteriores.

En algunas realizaciones, algunas ECU responsables de la seguridad **100** (por ejemplo, el control electrónico de estabilidad (ESC) **110** o Mobileye) tienen la capacidad de supervisar los mensajes que llegan del conductor (por ejemplo, una ECU de ESC controla el pedal del freno y evita el deslizamiento debido al frenado). Tal ECU **110** puede supervisar mensajes críticos específicos y prevenir el daño causado por estos mensajes. Estos mensajes se indican mediante ECM (mensajes críticos externos).

En algunas realizaciones, el sistema de seguridad **703** puede permitir que el ECM relevante (es decir, el ECM soportado por la ECU externa crítica) pase hacia el bus interno **105** del vehículo siempre que estos mensajes sean supervisados efectivamente por una ECU de seguridad. De esta manera, el sistema electrónico **101** del vehículo respalda de forma segura los mensajes críticos y que potencialmente pueden salvar vidas. Tal sistema de seguridad **703** también puede usarse en caso de que no haya una ECU de seguridad relevante, pero en tal caso será posible atacar el vehículo usando los mensajes críticos permitidos.

En algunas realizaciones donde una ECU con una comunicación externa tiene la capacidad de enviar mensajes críticos al bus de comunicación **105,** el controlador debe tener la capacidad de anular o deshabilitar manualmente los mensajes de esta ECU.

MODBUS Y OTROS PROTOCOLOS DE CONTROL

MODBUS es un protocolo ampliamente utilizado en sistemas de control industrial. De manera similar al bus CAN **105,** es un protocolo simple utilizado por controladores. Además, existen varios otros protocolos de control con características similares, tal como FlexRay, bus VAN, bus LIN, etc. Las realizaciones descritas anteriormente para el bus CAN pueden ser aplicables a otros protocolos de comunicación, tal como MODBUS, mutatis mutandis.

En algunas realizaciones, la principal diferencia entre la implementación de un filtro y/o proxy **703** para el bus CAN **105** y cualquier otro protocolo es la capa física y la lógica específica del filtro. Los diferentes protocolos tienen diferentes características de mensaje, por lo que requieren diferentes tipos de filtrado (por ejemplo, un filtro MODBUS toma un aviso especial en el campo del código de función). La lógica de proxy puede ser diferente, pero el concepto de proxy es el mismo: El emulador de enlace **2501** tiene que gestionar la comunicación con un protocolo de comunicación específico (por ejemplo, gestión de mensajes y máquina de estado específica **2602** para el protocolo). El filtro de estado y el actualizador **2502** filtran y actualizan el estado como filtro y actualizador de estado proxy del bus CAN **105**.

MODBUS está construido como arquitectura maestro-esclavo, lo que significa que hay un maestro y uno o más esclavos conectados al bus **105.** El maestro puede enviar una solicitud (por ejemplo, comando de lectura o escritura de datos) a uno o más esclavos, y los esclavos relevantes deben actuar de acuerdo con la solicitud y enviar su respuesta al maestro a través del bus **105.**

En algunas realizaciones, un proxy **703** que protege dicho bus de comunicación **105** puede guardar las propiedades de solicitud enviadas y permitir que solo la respuesta relevante pase hacia el maestro (por ejemplo, la solicitud y la respuesta pueden caracterizarse por su código de función).

En algunas realizaciones, dicho proxy **703** también puede generar la solicitud y/o respuesta recibidas por sí mismo de acuerdo con los mensajes que recibe, y enviar el mensaje generado en lugar del mensaje original.

En algunas realizaciones, un proxy **703** puede bloquear solicitudes que se originan desde cualquier componente que no debería funcionar como maestro en el bus.

UNIDAD DE AUTENTIFICACIÓN

En una realización de la presente invención, el sistema de seguridad **703** también funciona como una unidad de autentificación. La unidad de autentificación puede ser otro módulo del sistema de seguridad **703** de la invención.

La unidad de autentificación de la invención es responsable de verificar que la comunicación se realice con contrapartes auténticas dentro o fuera del sistema electrónico **101** del vehículo. Las unidades de autentificación se pueden integrar con las ECU **75** y, en particular, con las ECU **75** que no tienen una interfaz de comunicación externa. Para una mejor seguridad, se puede acoplar una unidad de autentificación a cada ECU crítica de seguridad **110,** cada ECU valiosa **75** y cada ECU con una interfaz de comunicación externa **109.**

La unidad de autentificación puede emplear uno o más mecanismos para la autentificación de una fuente o destino de comunicación. En algunas realizaciones, las unidades de autentificación pueden ser el origen o el destino de los mensajes. Estos mecanismos son, por ejemplo, la autentificación de un elemento de origen o destino (que envía o recibe mensajes); transmisión condicional de mensajes basada en una autentificación exitosa; y firma y/o verificación de firma de mensajes.

En algunas realizaciones, la unidad de autentificación también puede cifrar y/o descifrar mensajes. Este tipo de cifrado se puede usar para mantener el secreto, la integridad, la autenticidad, etc.

Autentificación: cualquier unidad de autentificación (autónoma o acoplada o integrada con una ECU **905**) puede realizar un procedimiento de autentificación con cualquier otra unidad de autentificación (autónoma o acoplada o integrada con una ECU **905**). En algunas realizaciones, una unidad de autentificación autónoma se puede acoplar con un bus **105.** En algunas realizaciones, una unidad de autentificación autónoma se puede acoplar con una o más ECU **75.** En algunas realizaciones, la unidad de autentificación está integrada con una ECU **905** (es decir, la unidad de autentificación está incluida dentro de la ECU **905** como parte del sistema de seguridad **703**). En algunas realizaciones, la unidad de autentificación es un sistema de seguridad autónomo **703** que no está acoplado con ninguna ECU **75** cuando se demuestra que su existencia es significativa, por ejemplo, para demostrar que un proveedor válido proporcionó un subsistema general. En algunas realizaciones, referirse a la autentificación de una ECU **75** significa autentificar la unidad de autentificación junto con la misma.

En algunas realizaciones, cada unidad de autentificación está configurada con una lista de todas las unidades de autentificación en el sistema **101** con las cuales se requiere autentificación. Cada unidad de autentificación puede iniciar periódicamente un proceso de autentificación con cualquier otra unidad de autentificación. El período después del cual se debe renovar la autentificación puede ser fijo o variable por unidad de autentificación. El proceso de

autentificación puede involucrar un mensaje de desafío desde una unidad de autentificación a otra. La unidad de autentificación receptora responde entonces al desafío con una respuesta (generalmente encriptada). La unidad de autentificación que ha enviado el mensaje de desafío verifica la respuesta y, si es correcta, marca esa unidad de autentificación en la lista como autentificada. Si la respuesta no es correcta, el desafío puede repetirse una o más veces, después de lo cual esa unidad de autentificación se marcará en la lista como no identificada (no autentificada).

Los mensajes de desafío y respuesta fluyen entre las unidades de autentificación como mensajes regulares en el sistema electrónico del vehículo. Estos mensajes son recibidos por una unidad de recepción. La unidad de clasificación los clasifica como mensajes de desafío/respuesta y los envía a la unidad de análisis de mensajes que los gestiona.

La unidad de análisis de mensajes es capaz de iniciar mensajes de desafío cuando es necesario autentificar una ECU **75** antes de entregarle un mensaje o considerar un mensaje desde la misma.

En algunas realizaciones, el proceso de autentificación también puede ser iniciado por una unidad de autentificación, cuando la unidad de autentificación o la ECU **75** a la que está acoplada, están programadas para autentificar periódicamente las ECU **75** en su lista de autentificación.

En algunas realizaciones, el proceso de autentificación puede ser unidireccional o bidireccional. En un proceso de autentificación unidireccional, cada unidad de autentificación envía un desafío a la otra. Es decir, la unidad de autentificación A desafía la unidad de autentificación B, y la unidad de autentificación B desafía la unidad de autentificación A. En un proceso de autentificación bidireccional, el mensaje de desafío enviado por la unidad de autentificación A a la unidad de autentificación B es suficiente para autentificar la unidad de autentificación A, y la autentificación la unidad B no necesita emitir su propio mensaje de desafío a la unidad de autentificación A.

En algunas realizaciones, el proceso de autentificación puede ser multidireccional, es decir, la unidad de autentificación A emite un mensaje de desafío y/o respuesta que llega a una pluralidad de unidades de autentificación a través de uno o más buses de comunicación **105.**

Transmisión condicional de mensajes basada en autentificación: la unidad de análisis de mensajes se puede configurar para transmitir un mensaje solo si un requisito de autentificación se cumple. Ejemplos de requisitos de autentificación incluyen, entre otros: que la unidad de autentificación de origen está autentificada; que la ECU de destino **75** está autentificada; que cualquier otra ECU **75** (no de origen o destino) está autentificada; que cualquier combinación de ECU **75** se autentifica, etc. El requisito de autentificación puede estar en contra del origen, el destino o cualquier otra ECU **75.**

Cuando un mensaje que requiere autentificación llega a la unidad de clasificación de mensajes, el mensaje se clasifica como que requiere autentificación contra ECU X **75,** y el mensaje se envía a la unidad de análisis de mensajes. La unidad de análisis de mensajes verifica si la ECU X **75** está autentificada. Si la ECU X **75** está autentificada, la unidad de análisis de mensajes continúa procesando el mensaje. Si la ECU X **75** no está autentificada, la unidad de análisis de mensajes puede decidir descartar el mensaje o emitir un mensaje de desafío a la ECU X **75** para ver si se autentifica.

Cabe destacar que el requisito de autentificación no tiene que implicar necesariamente la ECU de origen o de destino **75.** Por ejemplo, cuando la ECU 1 **75** envía un mensaje a la ECU 2 **75,** puede ser necesario que la ECU **1 75** se autentique con la ECU 7 **75** antes de que el mensaje pueda transmitirse a la ECU 2 **75.**

Firma y verificación: una de las acciones que puede realizar la unidad de análisis de mensajes se relaciona con la firma de mensajes. Cuando llega un mensaje con una firma, la unidad de análisis puede verificar que la firma sea válida. La unidad de análisis también puede agregar una firma a un mensaje antes de transferirlo a la unidad de transmisión.

La figura 24 ilustra un filtro de comunicación unidireccional básico/sistema de seguridad proxy **703.** Un mensaje recibido por la entrada del puerto físico **1800** se inserta en la unidad de recepción de mensajes en el gestor de mensajes **1801.** La unidad de recepción de mensajes transmite el mensaje a través de la entrada de interfaz de proxy **2000** a la unidad de clasificación de mensajes (clasificador) **2100** en el elemento unidireccional de filtro/proxy **1304.** El clasificador **2100** clasifica el mensaje y envía el mensaje y la clasificación del mensaje al selector de acciones **2801** en la unidad de análisis de mensajes **2800,** que elige la acción adecuada de acuerdo con la clasificación. La unidad de análisis de mensajes **2800** realiza una acción **2102** (sin pérdida de generalidad) sobre el mensaje de acuerdo con la clasificación y envía un mensaje (si es necesario) a través de la salida de interfaz proxy **2002** a la unidad de transmisión de mensajes **1801.** La unidad de transmisión de mensajes en el gestor de mensajes **1801** transmite el mensaje a la salida del puerto físico **1800.**

La figura 25 ilustra una realización del proceso de verificación/firma de mensajes entre el filtro/proxy de comunicación (sistemas de seguridad) A y **B 905.** Un ECU A lógico **900** envía un mensaje a un filtro/proxy de comunicación **A 905** (que contiene reglas para una unidad de autentificación **2900,** que ilustra el grupo de reglas **2102** a cargo de los procesos de autentificación y firma). La lógica **900** de la ECU es básicamente parte o la totalidad de los mecanismos de procesamiento de la ECU **905,** excepto el controlador/transceptor de capa física **904** que se encarga de enviar

físicamente las señales de comunicación al mundo exterior, que es un bus de comunicación **105.** El mensaje llega a la unidad de clasificación **2100** que clasifica el mensaje como "firma requerida contra el filtro de comunicación/proxy **B" 905.** La unidad de análisis **2800** recibe el mensaje y procede a firmarlo contra el filtro de comunicación/proxy **B 905.** El proceso de firma implica modificar el mensaje original al agregarle una firma (en un formato predeterminado). La unidad de análisis **2800** puede procesar adicionalmente el mensaje (además de la firma) de acuerdo con las instrucciones de clasificación recibidas y las reglas generales **2102** del analizador **2800.** La unidad de análisis **2800** enviará el mensaje a la unidad de transmisión de mensajes en el gestor de mensajes **1801** que enviará el mensaje a su destino **904,** que es un controlador de capa física (puerto) de **A.**

A continuación, el mensaje llegará a su puerto de destino **904** en la ECU **B 905,** y se transferirá a la unidad de recepción en el gestor de mensajes **1801** en el filtro de comunicación/proxy **B 703** y desde allí a la unidad de clasificación **2100.** La unidad de clasificación **2100** clasifica el mensaje como que requiere verificación de firma contra filtro de comunicación/proxy **A 703.** Cuando la unidad de análisis **2800** recibe el mensaje, verifica que la firma sea auténtica. Si se verifica la firma, el mensaje original se extrae del mensaje firmado y se transfiere a la unidad de transmisión de mensajes relevante en el gestor de mensajes **1801** que entrega el mensaje a la lógica **900** de **B.**

En algunas realizaciones, si la verificación de firma ha fallado, la unidad de análisis **2800** ignorará (descartará) el mensaje y no se tomarán medidas adicionales sobre el mensaje. En algunas realizaciones, se registrará el resultado de la verificación de firma.

Puede haber muchas implementaciones de agregar y verificar una firma y todas están abarcadas por la presente invención. Un ejemplo de esto puede ser: calcular un valor hash en el contenido de los datos del mensaje y a continuación cifrar el resultado utilizando una clave compartida entre las partes. La firma se realiza agregando el resultado cifrado al mensaje, y la verificación se realiza haciendo ese proceso y comparando el resultado con la firma enviada incorporada. Si ambos resultados son iguales, la firma del mensaje es válida.

En algunas realizaciones, uno o más sistemas de seguridad de proxy/filtro de comunicación **703** de la invención pueden implementarse fuera del sistema informático **101** del vehículo.

En algunas realizaciones, por consideraciones de eficiencia, la adición y/o verificación de firma no necesita ocurrir con todos los mensajes, sino solo con mensajes que fueron clasificados como tales por la unidad de clasificación.

La unidad de clasificación **2100** tiene en cuenta los requisitos de formato de cada mensaje, incluyendo la longitud máxima permitida, de modo que al agregar una firma el mensaje sigue siendo válido y puede transmitirse y leerse correctamente. El sistema debe ser consistente con el protocolo incluso al modificar mensajes. Eso significa que no todos los mensajes se firmarán, por ejemplo, si la firma hará que el tamaño del mensaje exceda el límite del protocolo.

Si, por ejemplo, las ECU **A** y **B 75** intercambian mensajes de diferentes tipos y tamaños, incluso si solo un tipo de mensajes funciona mal, todo el sistema puede funcionar mal, una situación que debe evitarse. En consecuencia, la unidad de clasificación **2100** está configurada para que los mensajes firmados cumplan con todos los requisitos de formato de los mensajes regulares (sin firmar) y, por lo tanto, puedan transmitirse y leerse correctamente.

REIVINDICACIONES

1. Un dispositivo (703) para gestionar mensajes entre una unidad de control electrónico (ECU) de vehículo en una carcasa de la ECU y un bus de comunicación del vehículo (105) bajo el control de una unidad de datos (1408), estando cada uno de los mensajes compuesto de múltiples partes, comprendiendo el dispositivo:

un primer puerto físico (1800) para conectarse a la ECU;
un primer transceptor (1801) acoplado al primer puerto físico para transmitir mensajes a, y recibir mensajes desde la ECU;
un segundo puerto físico (1800) para conectarse al bus de comunicación; y
un segundo transceptor (1801) acoplado al segundo puerto físico para transmitir mensajes a, y recibir mensajes desde el bus de comunicación;
una unidad de filtrado de mensajes que recibe mensajes desde dichos primer o segundo transceptor y los filtra de acuerdo con al menos una propiedad de mensaje;
el dispositivo gestiona los mensajes bajo el control de una unidad de datos (1408) y además comprende:

un tercer puerto físico (1806), que es una interfaz fuera de banda, para conectarse a la unidad de datos;
un tercer transceptor (1608) acoplado al tercer puerto físico para recibir desde la unidad de datos una regla asociada a una parte del mensaje;
un software y un procesador (1807) para ejecutar el software, estando el procesador acoplado para controlar el primer, el segundo y el tercer transceptores; y
una carcasa única para alojar el primer, el segundo y el tercer puertos físicos, el primer, el segundo y el tercer transceptores, y el procesador, en donde la carcasa única es distinta de, y externoa a la carcasa de la ECU,
en donde el dispositivo es operativo para recibir un mensaje de la ECU a través del primer puerto físico, y en respuesta a la regla recibida desde la unidad de datos a través del tercer puerto físico, para pasar, bloquear o cambiar y a continuación pasar el mensaje recibido al bus de comunicación a través del segundo puerto físico, o en donde el dispositivo está operativo para recibir un mensaje del bus de comunicación a través del segundo puerto físico, y en respuesta a la regla recibida de la unidad de datos a través del tercer puerto físico, para pasar, bloquear o cambiar y a continuación pasar el mensaje recibido a la ECU a través del primer puerto físico.

2. El dispositivo de acuerdo con la reivindicación 1, en donde el dispositivo es adicionalmente operativo para recibir múltiples mensajes desde la ECU a través del primer puerto físico, y en respuesta a la regla recibida desde la unidad de datos a través del tercer puerto físico, para pasar, bloquear o cambiar y a continuación pasar cada uno de los mensajes recibidos al bus de comunicación a través del segundo puerto físico, y en donde el dispositivo está operativo para recibir múltiples mensajes del bus de comunicación a través del segundo puerto físico, y en respuesta a la regla recibida de la unidad de datos a través del tercer puerto físico, para pasar, bloquear o cambiar y a continuación pasar cada uno de los mensajes recibidos a la ECU a través del primer puerto físico.

3. El dispositivo de acuerdo con la reivindicación 1, en el que todos los mensajes recibidos desde la ECU y desde el bus de comunicación están asociados a una propiedad, y en el que cada uno de los mensajes incluye un valor de la propiedad, y en donde la regla identifica la propiedad y uno o más valores, y un mensaje recibido específico se pasa, se bloquea o se cambia y a continuación se pasa, en respuesta a la comparación del valor del mensaje específico con uno o más valores de regla.

4. El dispositivo de acuerdo con la reivindicación 1, en el que todos los mensajes recibidos desde la ECU y desde el bus de comunicación están asociados a una información de temporización, y en donde la regla incluye uno o más valores de temporización, y un mensaje recibido específico se pasa, se bloquea o se cambia y a continuación se pasa, en respuesta a la comparación de la información específica de sincronización de mensajes con uno o más valores de sincronización de reglas.

5. El dispositivo de acuerdo con la reivindicación 1, además operativo para limitar la velocidad de transmisión de mensajes a la ECU a través del primer puerto físico, y en donde el dispositivo comprende además una memoria intermedia acoplada entre el primer y el segundo transceptor, para adaptarse entre la velocidad de entrada de mensajes desde el bus de comunicación a través del segundo puerto físico y la velocidad de salida de mensajes a la ECU a través del primer puerto físico.

6. El dispositivo de acuerdo con la reivindicación 1, adicionalmente operativo para detectar o prevenir un ataque de denegación de servicio (DoS), en donde un mensaje se transmite a la ECU a través del primer puerto físico solo durante un intervalo de tiempo predeterminado después de que haya sido transmitido el mensaje anterior.

7. El dispositivo de acuerdo con la reivindicación 1, además operativo para limitar la velocidad de transmisión de mensajes al bus de comunicación a través del segundo puerto físico, comprendiendo además el dispositivo una memoria intermedia acoplada entre el primer y el segundo transceptor, para adaptarse entre la velocidad de entrada de mensajes desde la ECU a través del primer puerto físico y la velocidad de salida de mensajes al bus de comunicación a través del segundo puerto físico.

8. El dispositivo de acuerdo con la reivindicación 1, en el que un mensaje se transmite al bus de comunicación a través del segundo puerto físico solo durante un intervalo de tiempo predeterminado después de que haya sido transmitido el mensaje anterior.

9. El dispositivo de acuerdo con la reivindicación 1, que comprende además un emulador de bus de comunicación acoplado al primer transceptor para emular el bus de comunicación a la ECU, y en donde el dispositivo es operativo para emular el bus de comunicación a la ECU.

10. El dispositivo de acuerdo con la reivindicación 1, que comprende, además, en la única carcasa:

un cuarto puerto físico para conectarse a un bus de comunicación adicional o a una ECU adicional; y
un cuarto transceptor acoplado al cuarto puerto físico para transmitir mensajes a, y para recibir mensajes desde el bus de comunicación adicional respectivo o la ECU adicional, en donde el cuarto transceptor está acoplado para ser controlado por el procesador, y
en donde el dispositivo está operativo para recibir mensajes del cuarto puerto físico y en respuesta a la regla recibida desde la unidad de datos a través del tercer puerto físico, para pasar, bloquear o cambiar y a continuación pasar los mensajes recibidos al bus de comunicación a través del segundo puerto físico, o hacia la ECU a través del primer puerto físico.

11. El dispositivo de acuerdo con la reivindicación 1, además operativo para agregar una firma a parte de, o a todos los mensajes recibidos desde la ECU a través del primer puerto físico, y para transmitir los mensajes firmados al bus de comunicación a través del segundo puerto físico, o es operativo para agregar una firma a parte o a la totalidad de los mensajes recibidos desde el bus de comunicación a través del segundo puerto físico, y para transmitir los mensajes firmados a la ECU a través del primer puerto físico.

12. El dispositivo de acuerdo con la reivindicación 1, en el que el bus de comunicación está de acuerdo con un primer protocolo o está usando una primera velocidad de datos, y en el que la ECU se puede conectar a un bus de comunicación de acuerdo con un segundo protocolo o está usando una segunda velocidad de datos, y en donde el dispositivo está operativo para convertir respectivamente entre el primer y el segundo protocolo o entre la primera y la segunda velocidades de datos.

13. El dispositivo de acuerdo con la reivindicación 1, para usarse con un esquema de autentificación que usa un par de mensajes que consiste en un mensaje de desafío y un mensaje de respuesta de desafío, en donde la ECU se determina como autentificada en función del uso del esquema de autentificación, y en donde el dispositivo está operativo para transmitir a la ECU a través del primer puerto físico el mensaje de desafío, y recibir una respuesta desde la ECU a través del primer puerto físico.

14. El dispositivo de acuerdo con la reivindicación 1, en el que el bus de comunicación del vehículo consiste, emplea, usa, se basa o es compatible con una red de área de controlador (CAN), una red de interconexión local (LIN), un protocolo FlexRay o un bus de red de área de vehículo (VAN).

15. Un vehículo que comprende la unidad de control electrónico (ECU), el bus de comunicación del vehículo y el dispositivo de acuerdo con la reivindicación 1 conectado entre los mismos, y en donde el vehículo comprende además una unidad de control electrónico (ECU) adicional conectada al bus de comunicación del vehículo, y un dispositivo adicional de acuerdo con la reivindicación 1 conectado entre los mismos.

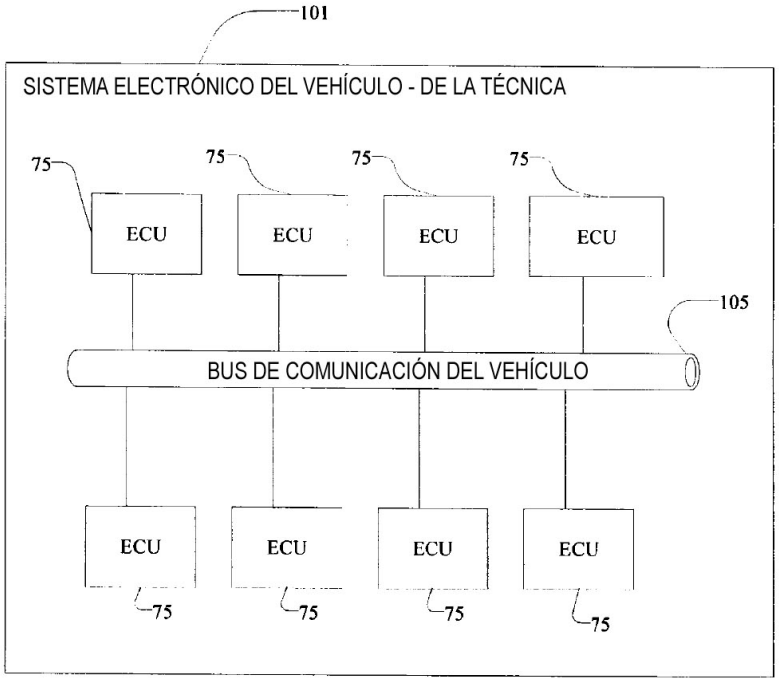

101
SISTEMA ELECTRÓNICO DEL VEHÍCULO - DE LA TÉCNICA
75
75
75
75
ECU
ECU
ECU
ECU
105
BUS DE COMUNICACIÓN DEL VEHÍCULO
ECU
ECU
ECU
ECU
75
75
75
75

Fig. 1

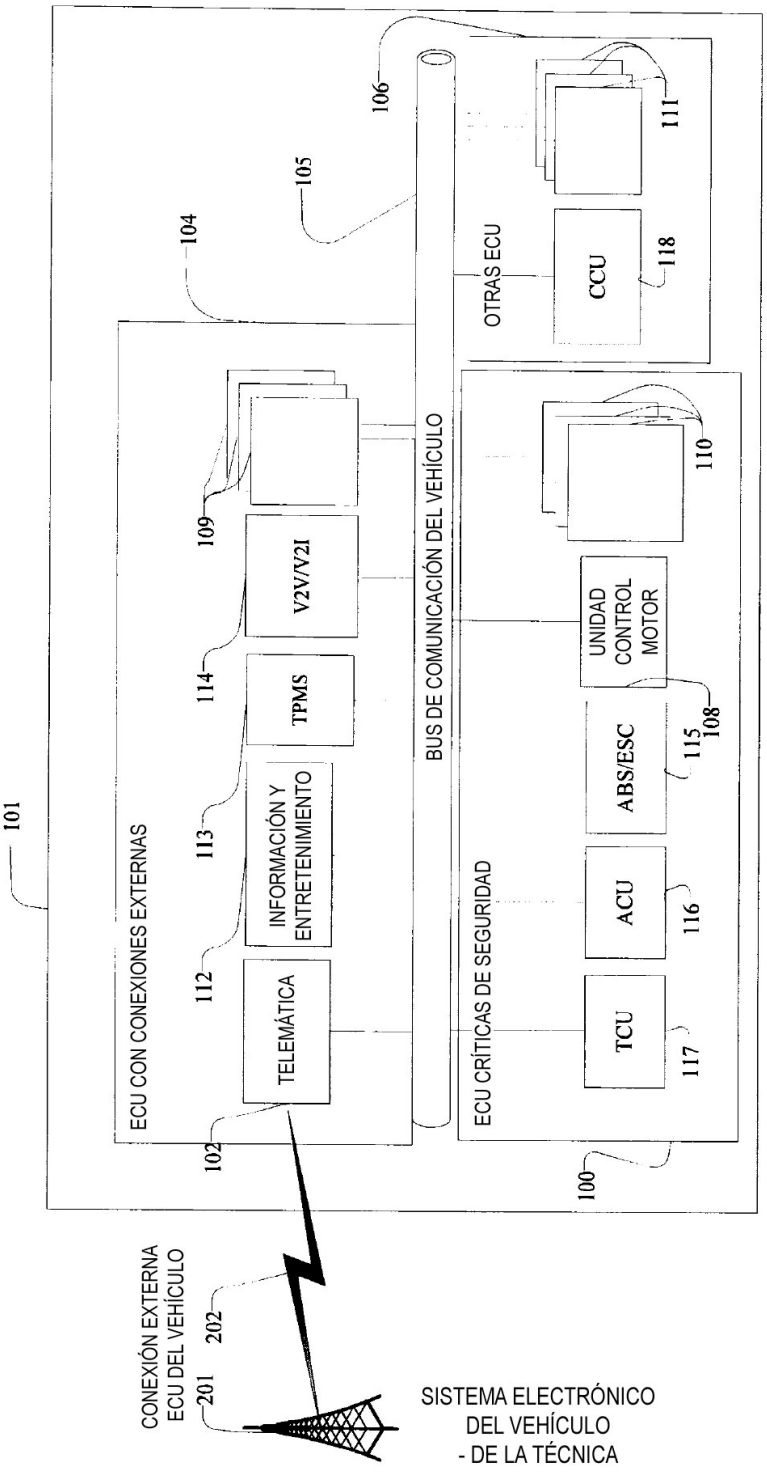

101
ECU CON CONEXIONES EXTERNAS
TELEMÁTICA
INFORMACIÓN Y ENTRETENIMIENTO
TPMS
V2V/V2I
102
112
113
114
109
104
105
106
BUS DE COMUNICACIÓN DEL VEHÍCULO
OTRAS ECU
CCU
118
111
ECU CRÍTICAS DE SEGURIDAD
TCU
ACU
ABS/ESC
UNIDAD CONTROL MOTOR
117
116
115
108
110
100
CONEXIÓN EXTERNA ECU DEL VEHÍCULO
201
202
SISTEMA ELECTRÓNICO DEL VEHÍCULO - DE LA TÉCNICA

Fig. 2

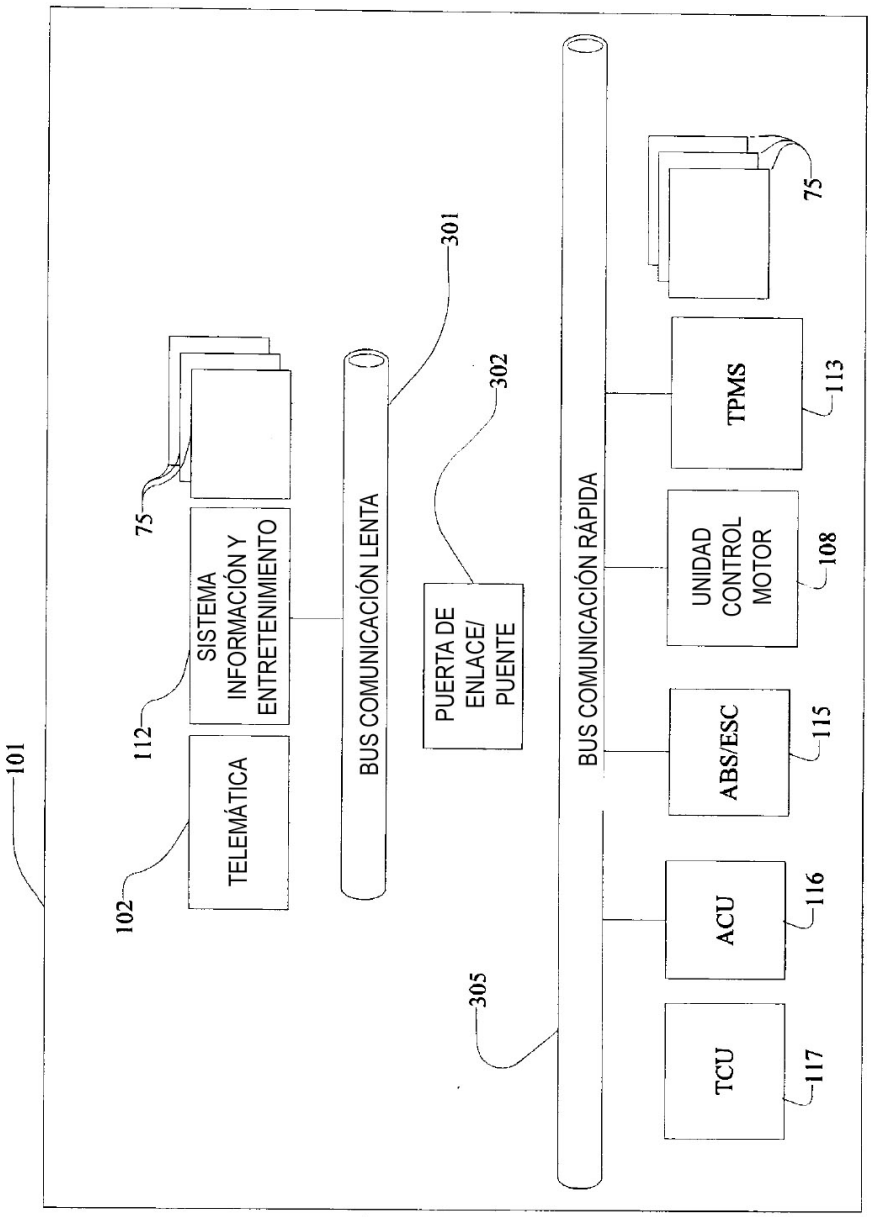

101
102
TELEMÁTICA
112
SISTEMA INFORMACIÓN Y ENTRETENIMIENTO
75
BUS COMUNICACIÓN LENTA
301
PUERTA DE ENLACE/ PUENTE
302
BUS COMUNICACIÓN RÁPIDA
305
TCU
117
ACU
116
ABS/ESC
115
UNIDAD CONTROL MOTOR
108
TPMS
113
75
SISTEMA ELECTRÓNICO
DEL VEHÍCULO - DE LA TÉCNICA

Fig. 3

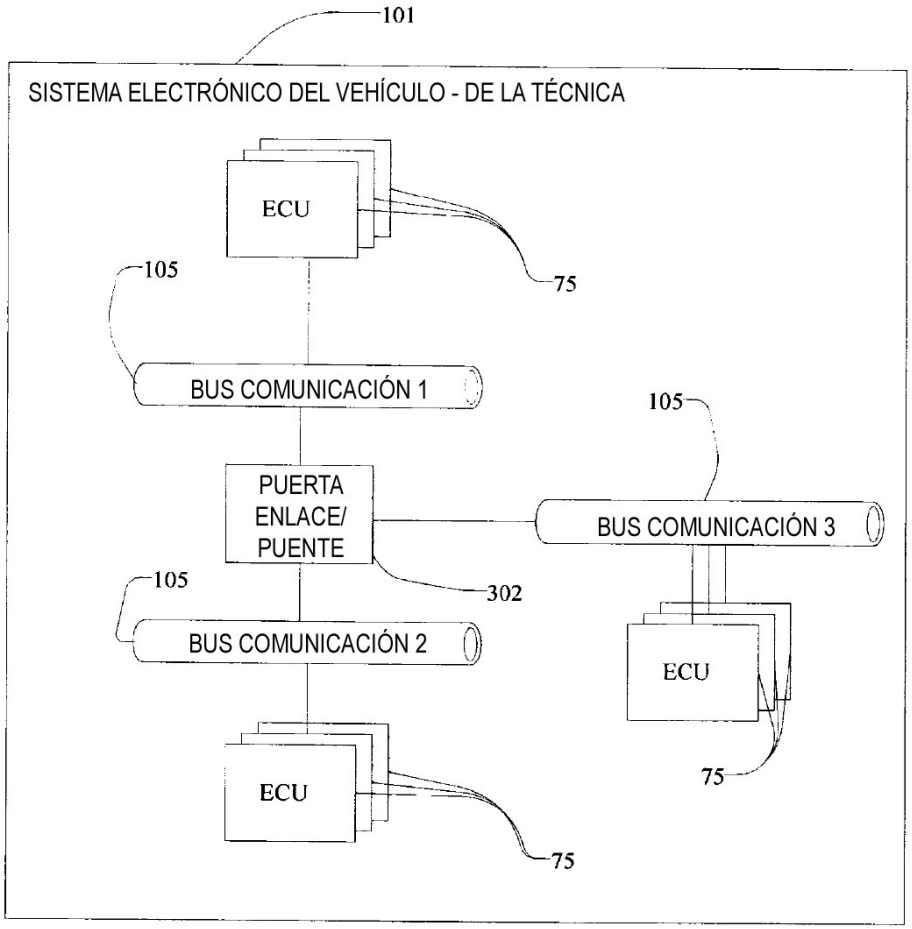
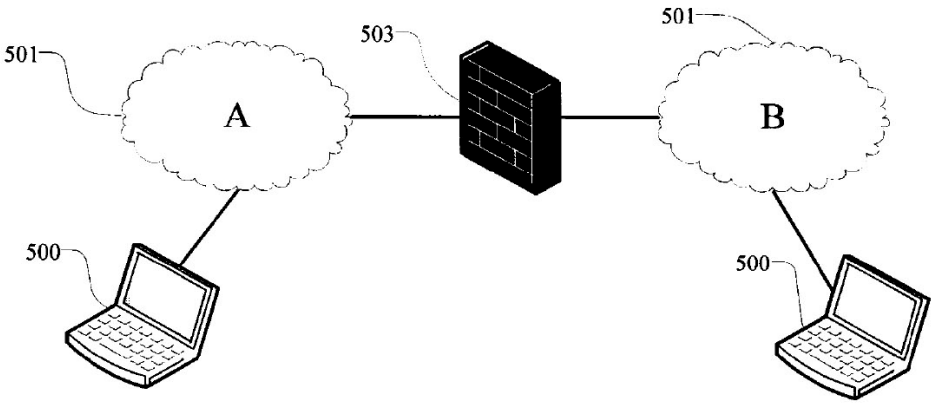

101
SISTEMA ELECTRÓNICO DEL VEHÍCULO - DE LA TÉCNICA
ECU
75
105
BUS COMUNICACIÓN 1
105
PUERTA ENLACE/ PUENTE
BUS COMUNICACIÓN 3
302
105
BUS COMUNICACIÓN 2
ECU
75
ECU
75

Fig. 4



CORTAFUEGOS - DE LA TÉCNICA

Fig. 5

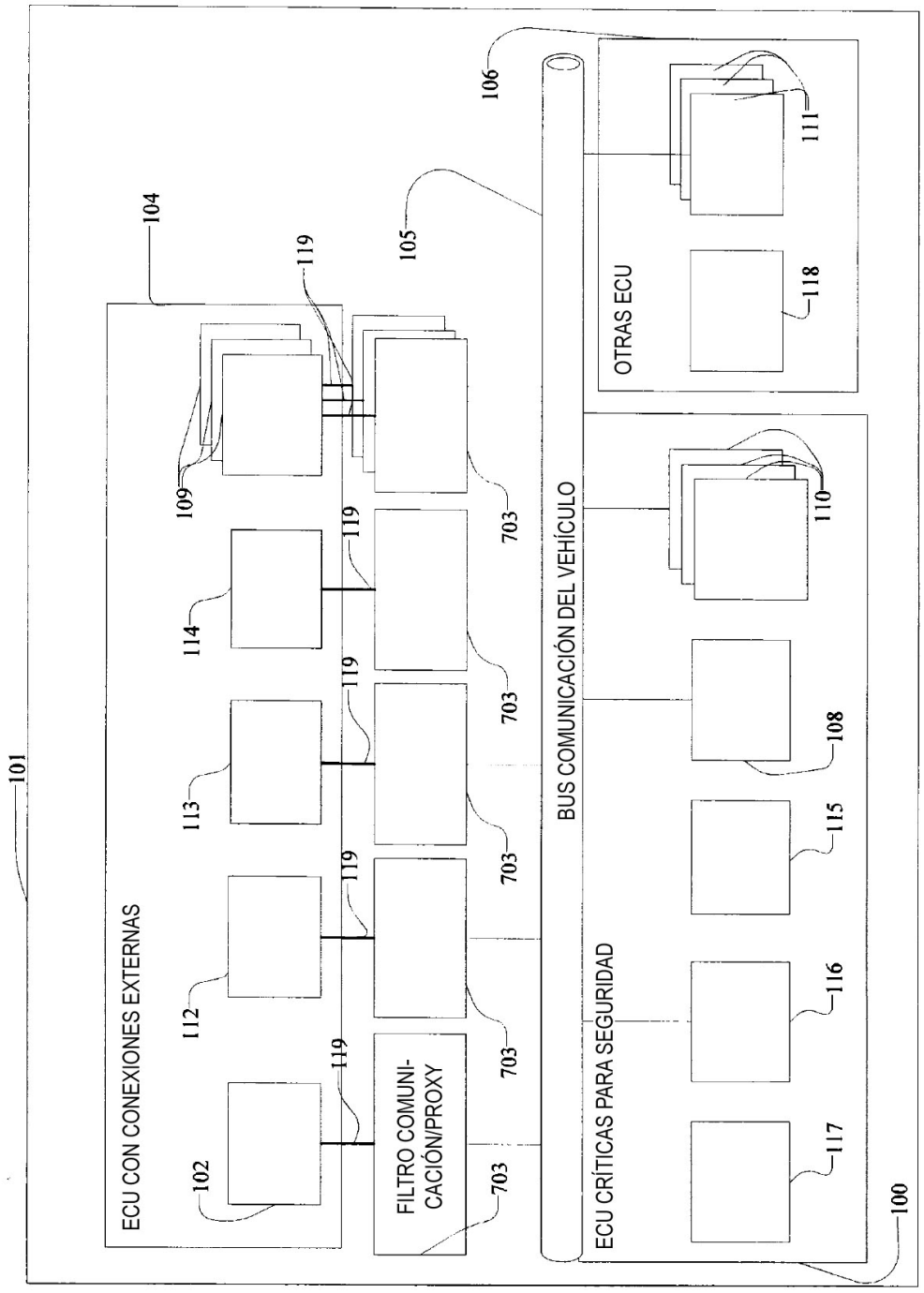

SISTEMA ELECTRÓNICO DEL VEHÍCULO
ECU CON CONEXIONES EXTERNAS
FILTRO COMUNI-CACIÓN/PROXY
BUS COMUNICACIÓN DEL VEHÍCULO
OTRAS ECU
ECU CRÍTICAS PARA SEGURIDAD
100
101
102
104
105
106
108
109
110
111
112
113
114
115
116
117
118
119
703

Fig. 6

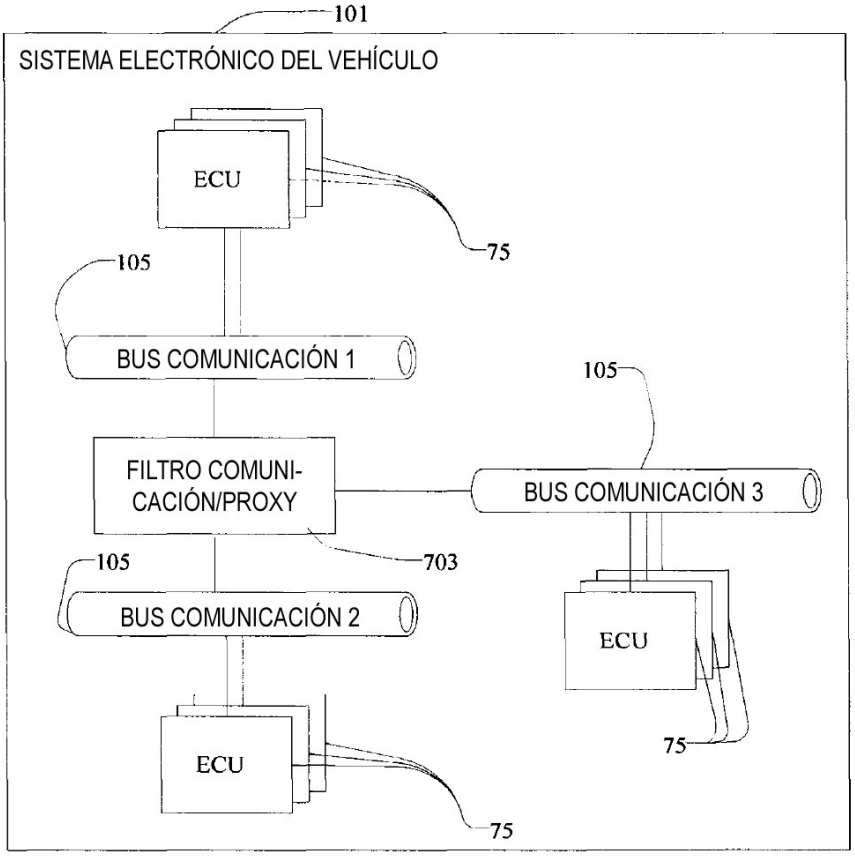

101
SISTEMA ELECTRÓNICO DEL VEHÍCULO
ECU
75
105
BUS COMUNICACIÓN 1
105
FILTRO COMUNI-
CACIÓN/PROXY
BUS COMUNICACIÓN 3
703
105
BUS COMUNICACIÓN 2
ECU
75
ECU
75

Fig. 7

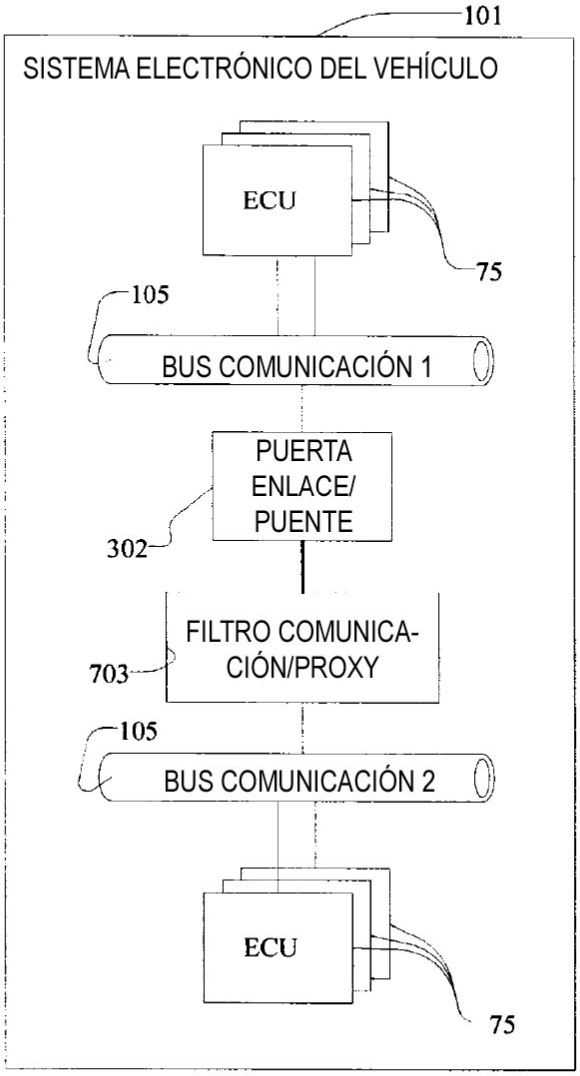

101
SISTEMA ELECTRÓNICO DEL VEHÍCULO
ECU
75
105
BUS COMUNICACIÓN 1
PUERTA ENLACE/ PUENTE
302
FILTRO COMUNICA-CIÓN/PROXY
703
105
BUS COMUNICACIÓN 2
ECU
75

Fig. 8

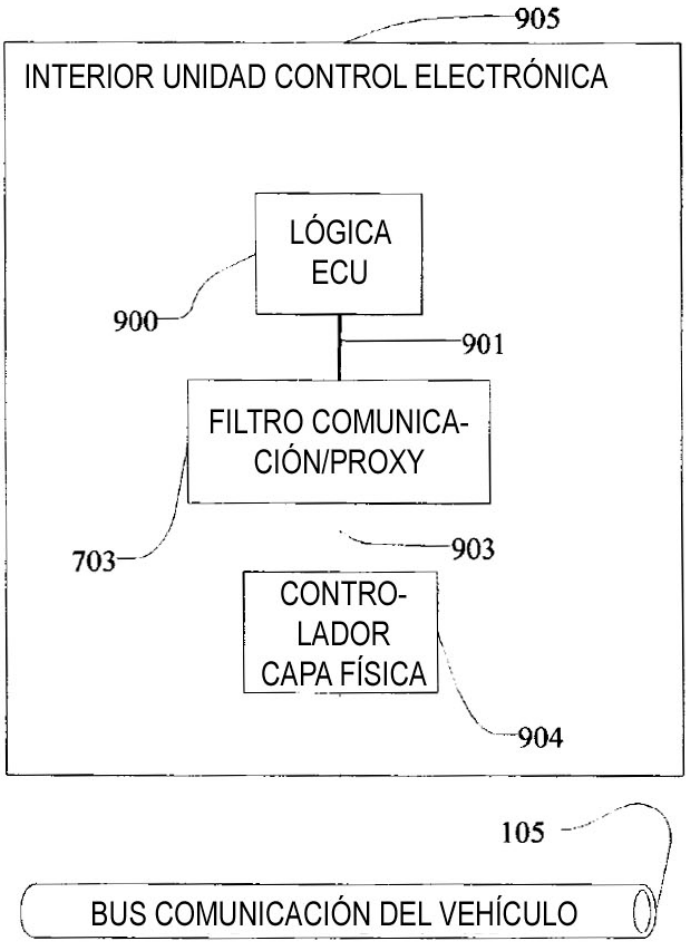

905
INTERIOR UNIDAD CONTROL ELECTRÓNICA
LÓGICA ECU
900
901
FILTRO COMUNICA-CIÓN/PROXY
703
903
CONTRO-LADOR CAPA FÍSICA
904
105
BUS COMUNICACIÓN DEL VEHÍCULO

Fig. 9

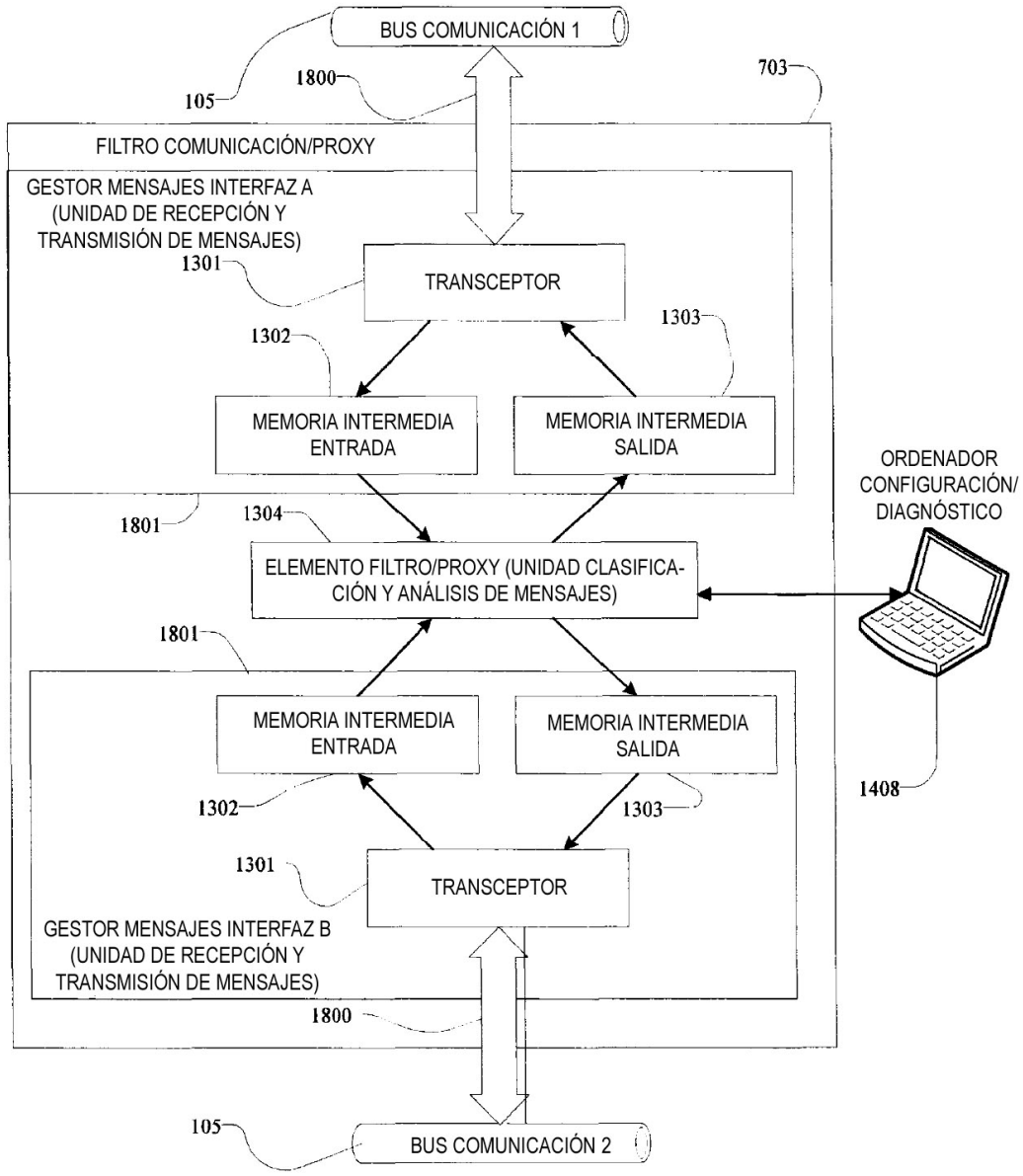

BUS COMUNICACIÓN 1
105
1800
703
FILTRO COMUNICACIÓN/PROXY
GESTOR MENSAJES INTERFAZ A (UNIDAD DE RECEPCIÓN Y TRANSMISIÓN DE MENSAJES)
1301
TRANSCEPTOR
1303
1302
MEMORIA INTERMEDIA ENTRADA
MEMORIA INTERMEDIA SALIDA
ORDENADOR CONFIGURACIÓN/ DIAGNÓSTICO
1801
1304
ELEMENTO FILTRO/PROXY (UNIDAD CLASIFICACIÓN Y ANÁLISIS DE MENSAJES)
1801
MEMORIA INTERMEDIA ENTRADA
MEMORIA INTERMEDIA SALIDA
1408
1302
1303
1301
TRANSCEPTOR
GESTOR MENSAJES INTERFAZ B (UNIDAD DE RECEPCIÓN Y TRANSMISIÓN DE MENSAJES)
1800
105
BUS COMUNICACIÓN 2

Fig. 10

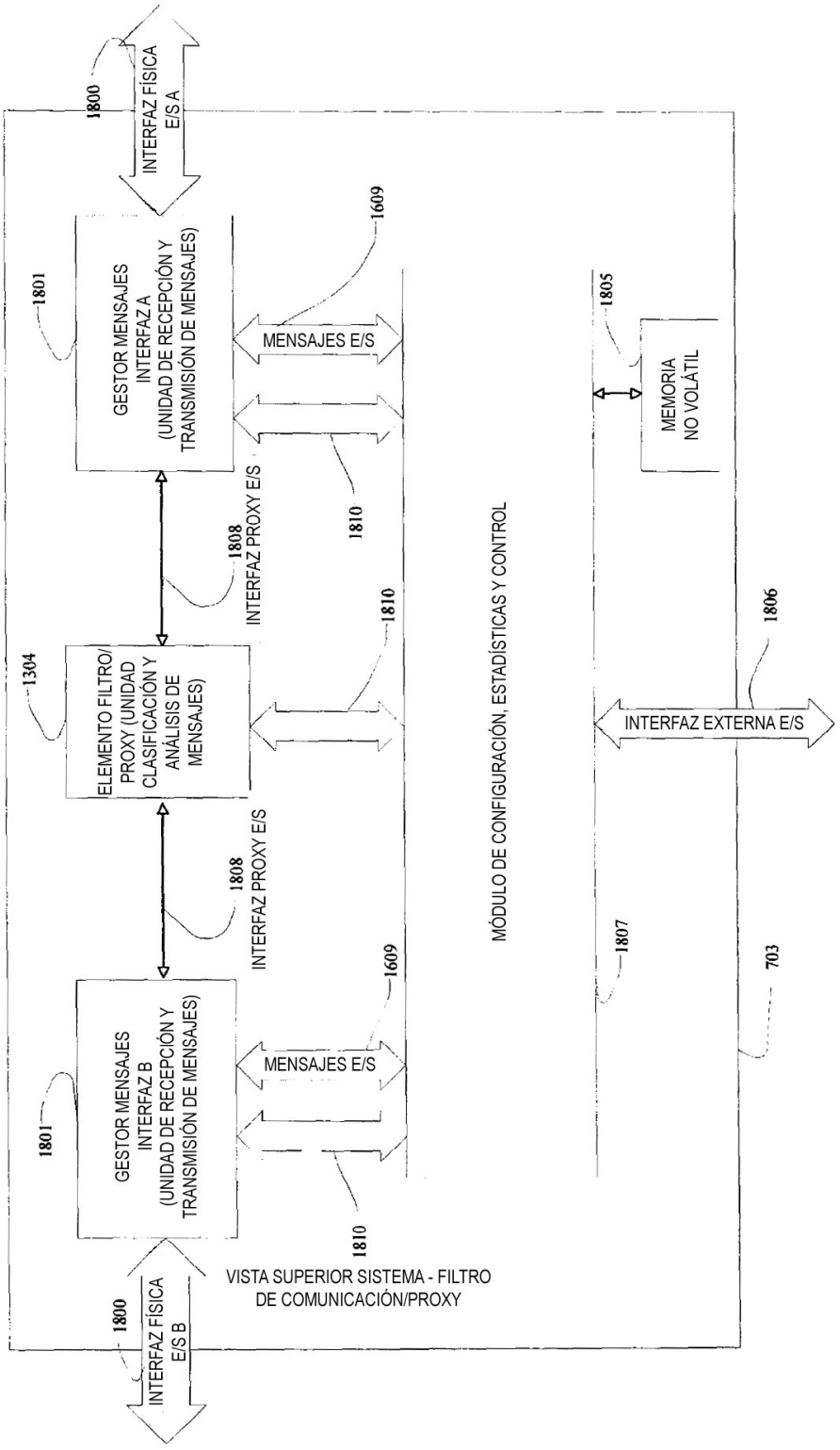

1800
INTERFAZ FÍSICA E/S A
1801
GESTOR MENSAJES INTERFAZ A (UNIDAD DE RECEPCIÓN Y TRANSMISIÓN DE MENSAJES)
1609
MENSAJES E/S
1810
1808
INTERFAZ PROXY E/S
1304
ELEMENTO FILTRO/ PROXY (UNIDAD CLASIFICACIÓN Y ANÁLISIS DE MENSAJES)
1810
1808
INTERFAZ PROXY E/S
1609
MENSAJES E/S
1801
GESTOR MENSAJES INTERFAZ B (UNIDAD DE RECEPCIÓN Y TRANSMISIÓN DE MENSAJES)
1810
1800
INTERFAZ FÍSICA E/S B
MÓDULO DE CONFIGURACIÓN, ESTADÍSTICAS Y CONTROL
1805
MEMORIA NO VOLÁTIL
1806
INTERFAZ EXTERNA E/S
1807
703
VISTA SUPERIOR SISTEMA - FILTRO DE COMUNICACIÓN/PROXY

Fig. 11

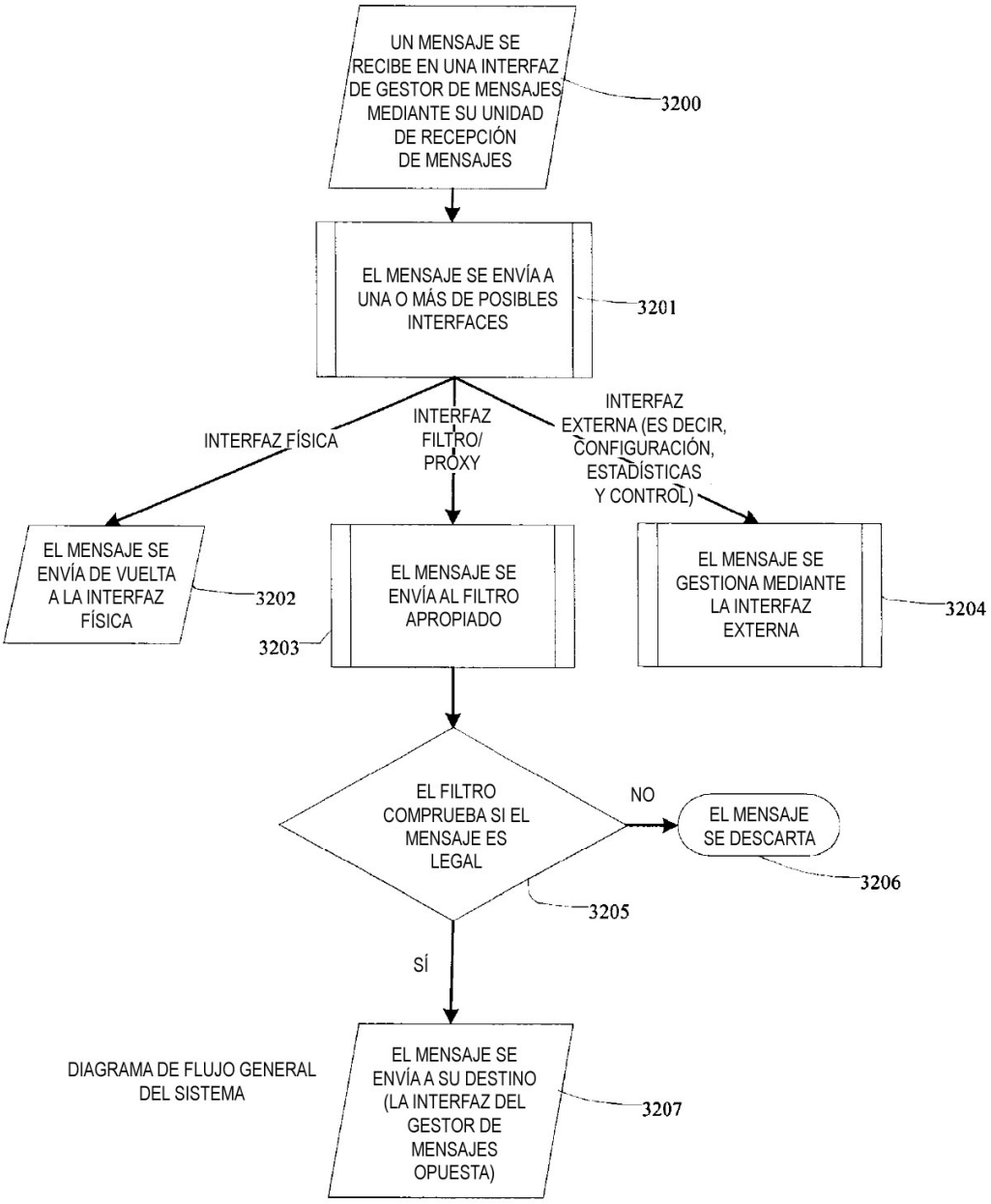


DIAGRAMA DE FLUJO GENERAL DEL SISTEMA

Fig. 12

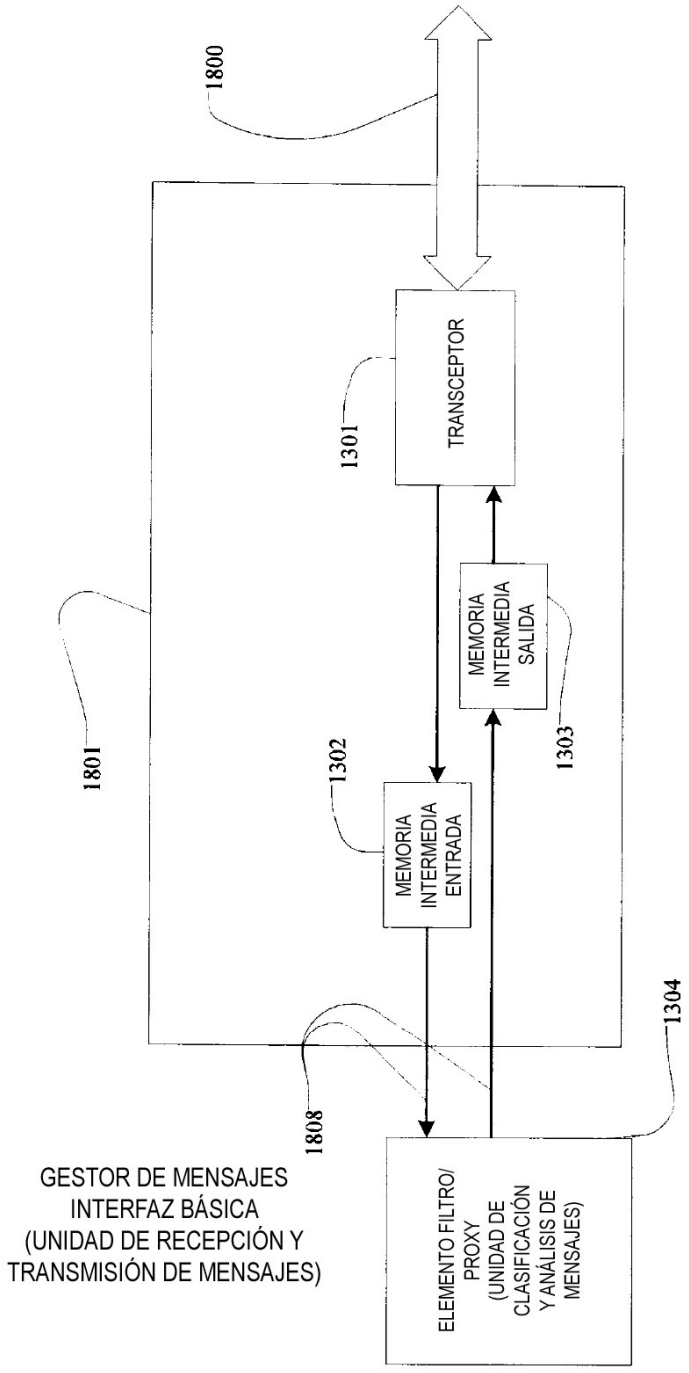

1800
TRANSCEPTOR
1301
MEMORIA INTERMEDIA SALIDA
1303
1801
1302
MEMORIA INTERMEDIA ENTRADA
1304
1808
GESTOR DE MENSAJES
INTERFAZ BÁSICA
(UNIDAD DE RECEPCIÓN Y
TRANSMISIÓN DE MENSAJES)
ELEMENTO FILTRO/
PROXY
(UNIDAD DE
CLASIFICACIÓN
Y ANÁLISIS DE
MENSAJES)

Fig. 13

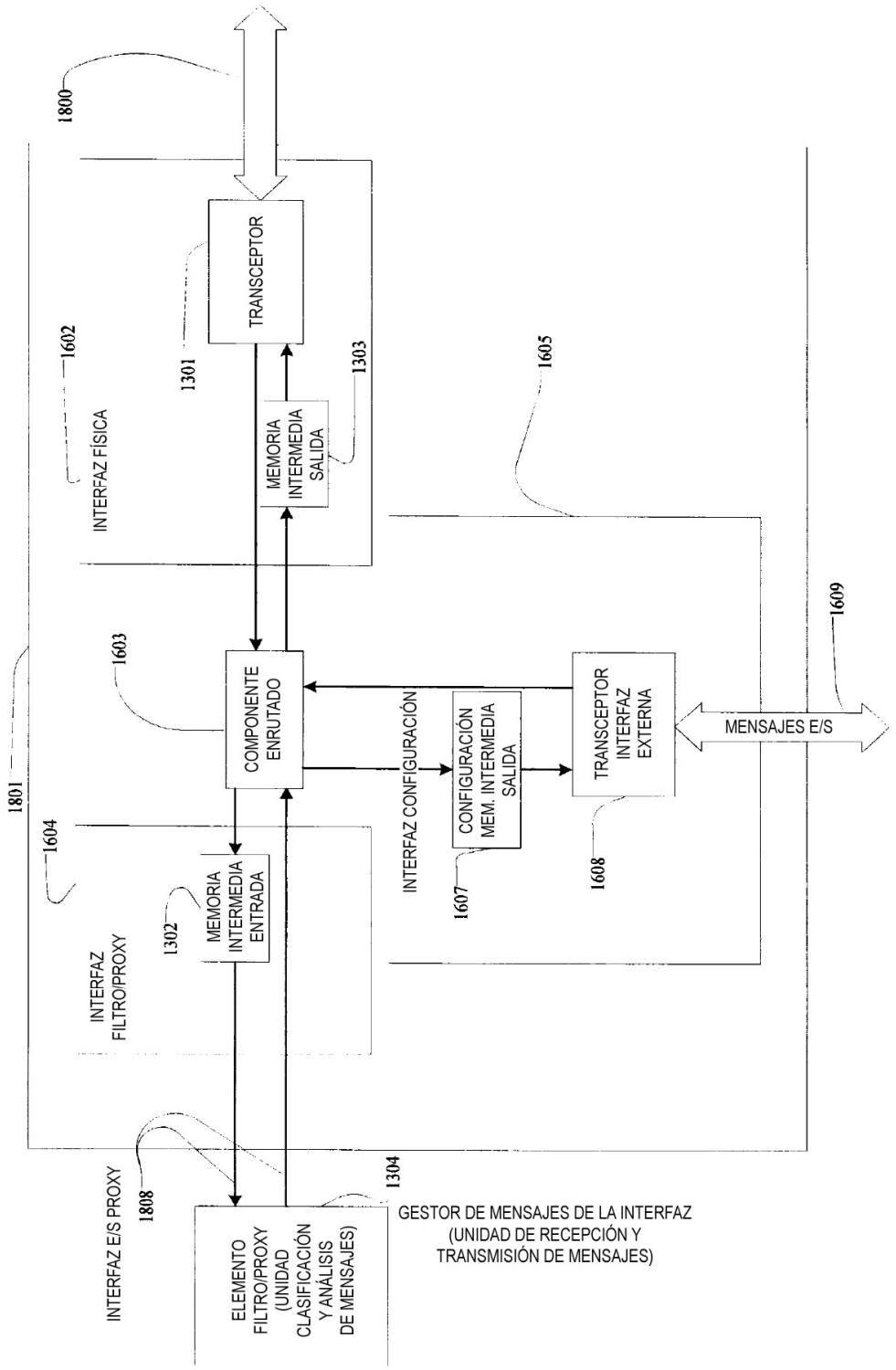

1800
TRANSCEPTOR
1301
1602
INTERFAZ FÍSICA
1303
MEMORIA INTERMEDIA SALIDA
1605
1609
1603
COMPONENTE ENRUTADO
INTERFAZ CONFIGURACIÓN
CONFIGURACIÓN MEM. INTERMEDIA SALIDA
TRANSCEPTOR INTERFAZ EXTERNA
MENSAJES E/S
1801
1604
1607
1608
1302
MEMORIA INTERMEDIA ENTRADA
INTERFAZ FILTRO/PROXY
INTERFAZ E/S PROXY
1808
1304
GESTOR DE MENSAJES DE LA INTERFAZ (UNIDAD DE RECEPCIÓN Y TRANSMISIÓN DE MENSAJES)
ELEMENTO FILTRO/PROXY (UNIDAD CLASIFICACIÓN Y ANÁLISIS DE MENSAJES)

Fig. 14

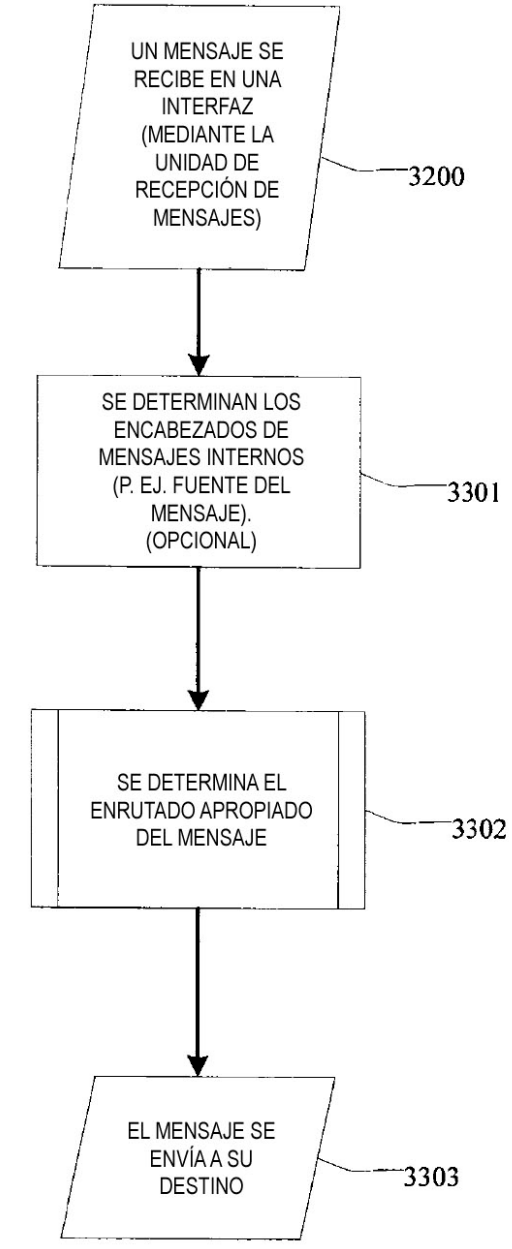


DIAGRAMA DE FLUJO DEL GESTOR DE MENSAJES DE LA INTERFAZ

Fig. 15

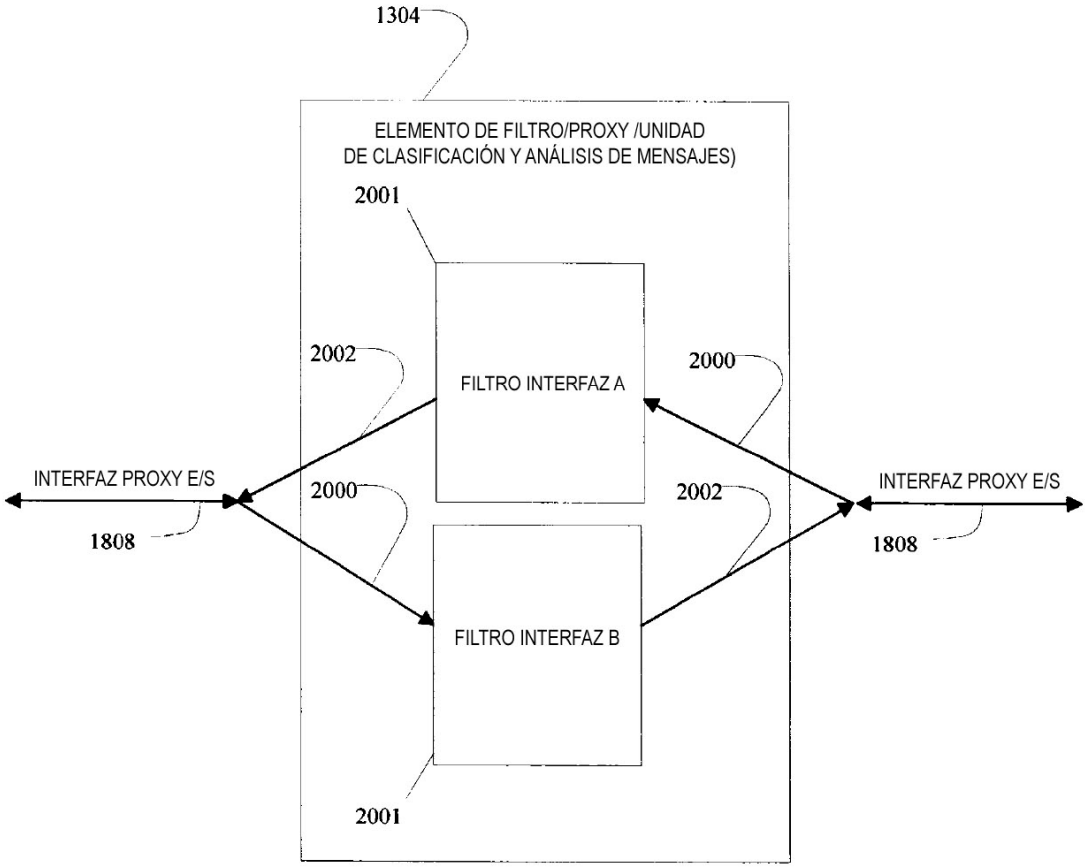

1304
ELEMENTO DE FILTRO/PROXY /UNIDAD
DE CLASIFICACIÓN Y ANÁLISIS DE MENSAJES)
2001
2002
FILTRO INTERFAZ A
2000
INTERFAZ PROXY E/S
1808
2000
2002
INTERFAZ PROXY E/S
1808
FILTRO INTERFAZ B
2001

Fig. 16

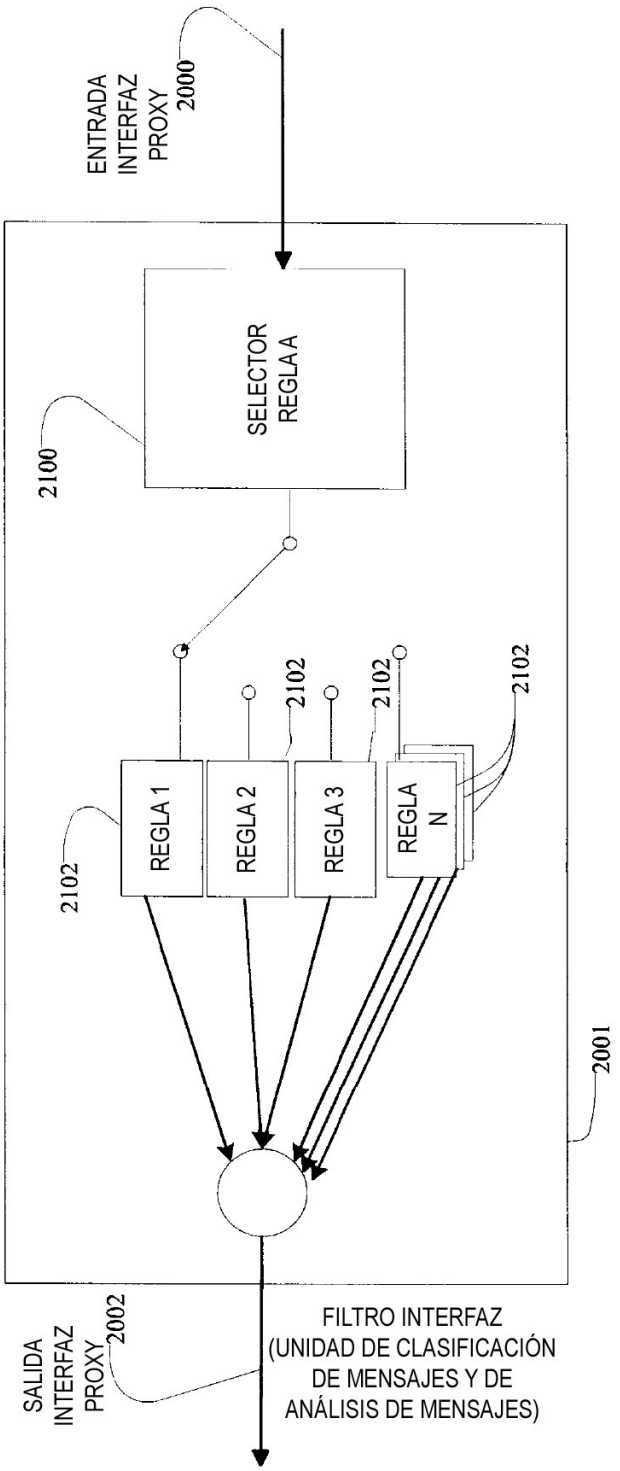

ENTRADA INTERFAZ PROXY
2000
SELECTOR REGLA A
2100
2102
2102
2102
REGLA 1
REGLA 2
REGLA 3
REGLA N
2102
2001
SALIDA INTERFAZ PROXY
2002
FILTRO INTERFAZ (UNIDAD DE CLASIFICACIÓN DE MENSAJES Y DE ANÁLISIS DE MENSAJES)

Fig. 17

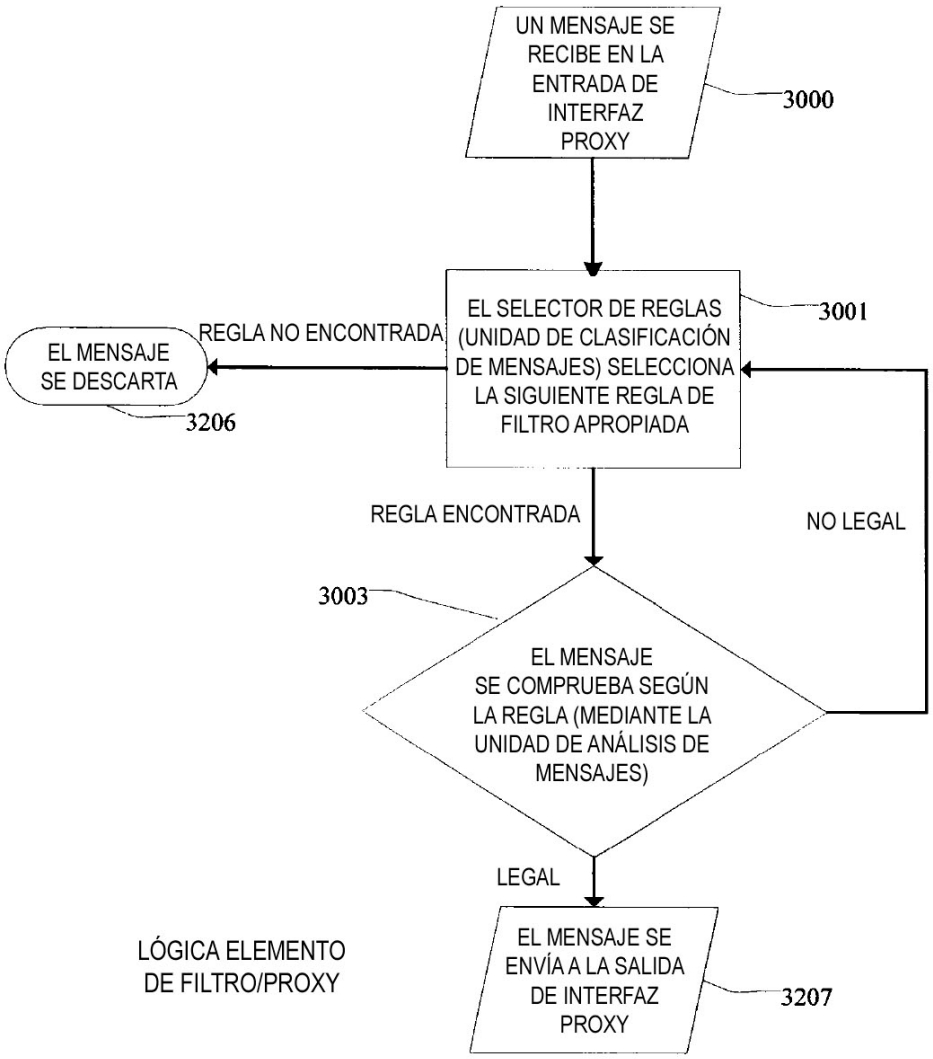

UN MENSAJE SE RECIBE EN LA ENTRADA DE INTERFAZ PROXY
3000
EL SELECTOR DE REGLAS (UNIDAD DE CLASIFICACIÓN DE MENSAJES) SELECCIONA LA SIGUIENTE REGLA DE FILTRO APROPIADA
3001
REGLA NO ENCONTRADA
EL MENSAJE SE DESCARTA
3206
REGLA ENCONTRADA
NO LEGAL
3003
EL MENSAJE SE COMPRUEBA SEGÚN LA REGLA (MEDIANTE LA UNIDAD DE ANÁLISIS DE MENSAJES)
LEGAL
EL MENSAJE SE ENVÍA A LA SALIDA DE INTERFAZ PROXY
3207
LÓGICA ELEMENTO DE FILTRO/PROXY

Fig. 18

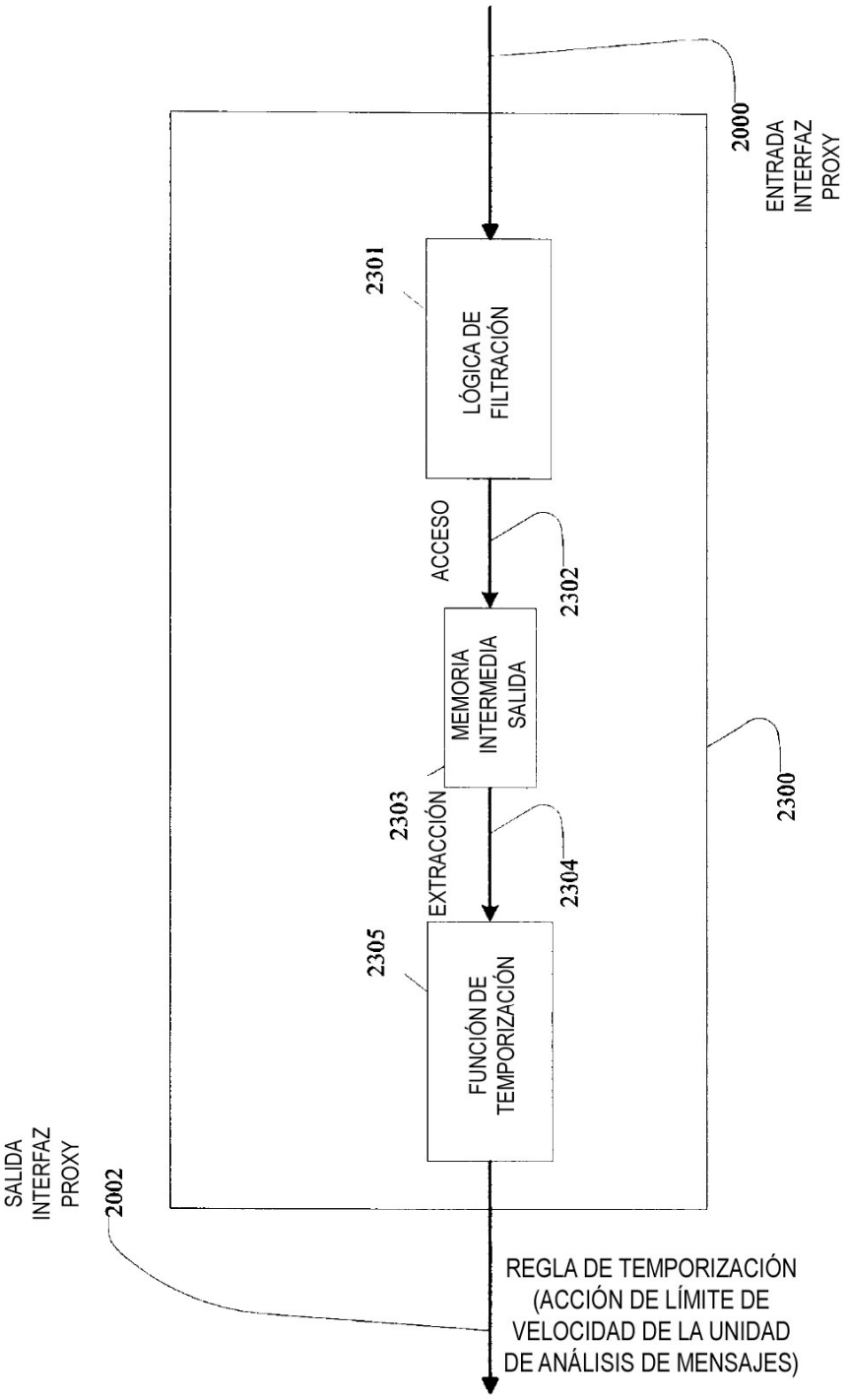

2000
ENTRADA INTERFAZ PROXY
2301
LÓGICA DE FILTRACIÓN
ACCESO
2302
MEMORIA INTERMEDIA SALIDA
2303
EXTRACCIÓN
2304
2305
FUNCIÓN DE TEMPORIZACIÓN
2300
SALIDA INTERFAZ PROXY
2002
REGLA DE TEMPORIZACIÓN (ACCIÓN DE LÍMITE DE VELOCIDAD DE LA UNIDAD DE ANÁLISIS DE MENSAJES)

Fig. 19

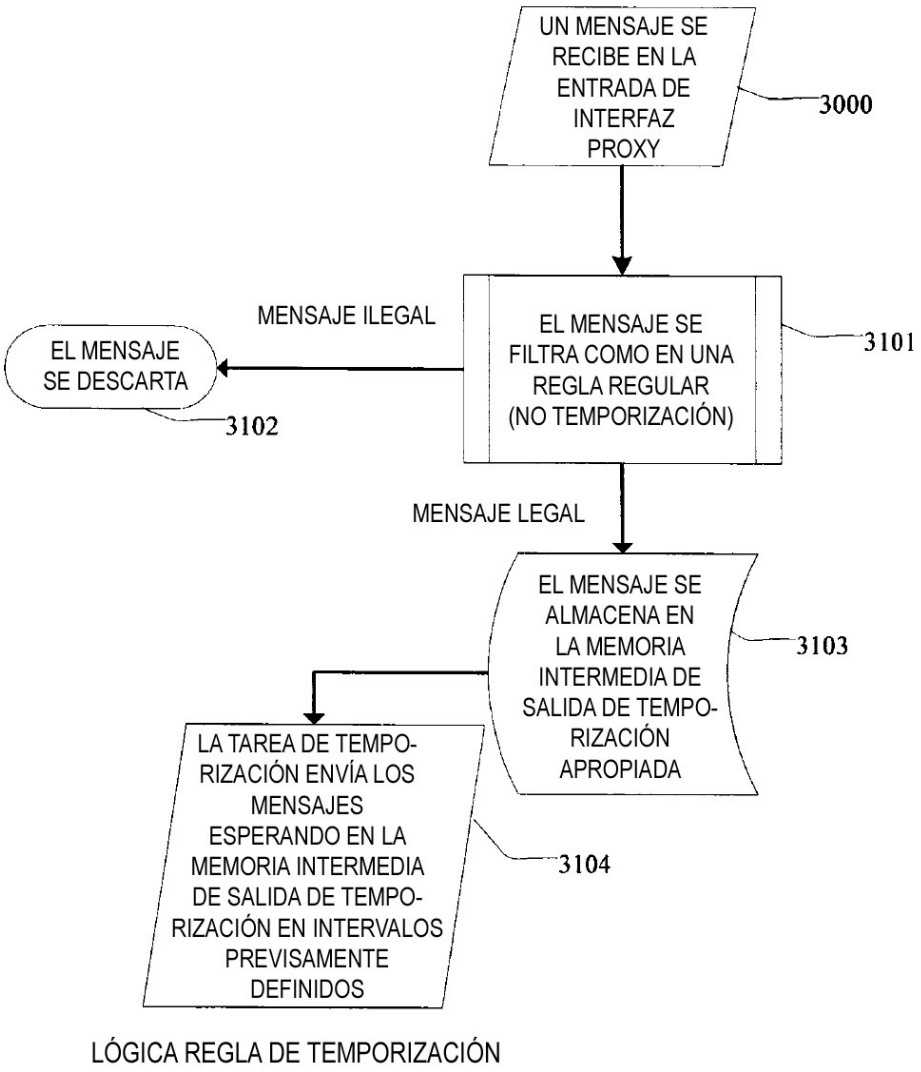

UN MENSAJE SE RECIBE EN LA ENTRADA DE INTERFAZ PROXY
3000
EL MENSAJE SE FILTRA COMO EN UNA REGLA REGULAR (NO TEMPORIZACIÓN)
3101
MENSAJE ILEGAL
EL MENSAJE SE DESCARTA
3102
MENSAJE LEGAL
EL MENSAJE SE ALMACENA EN LA MEMORIA INTERMEDIA DE SALIDA DE TEMPO-RIZACIÓN APROPIADA
3103
LA TAREA DE TEMPO-RIZACIÓN ENVÍA LOS MENSAJES ESPERANDO EN LA MEMORIA INTERMEDIA DE SALIDA DE TEMPO-RIZACIÓN EN INTERVALOS PREVISAMENTE DEFINIDOS
3104
LÓGICA REGLA DE TEMPORIZACIÓN

Fig. 20

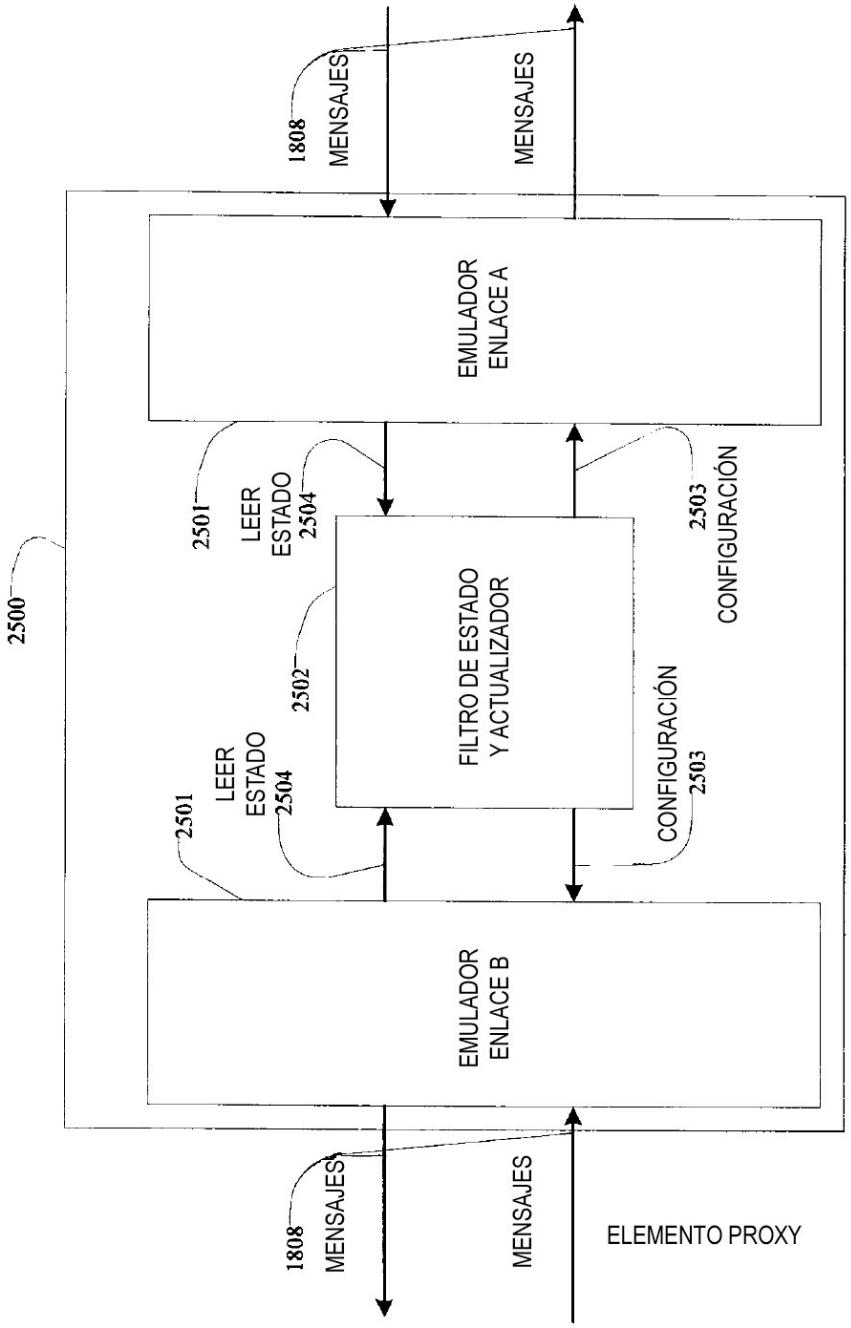

1808
MENSAJES
MENSAJES
EMULADOR ENLACE A
2501
LEER ESTADO 2504
2503
CONFIGURACIÓN
2500
2502
FILTRO DE ESTADO Y ACTUALIZADOR
2501
LEER ESTADO 2504
CONFIGURACIÓN 2503
EMULADOR ENLACE B
1808
MENSAJES
MENSAJES
ELEMENTO PROXY

Fig. 21

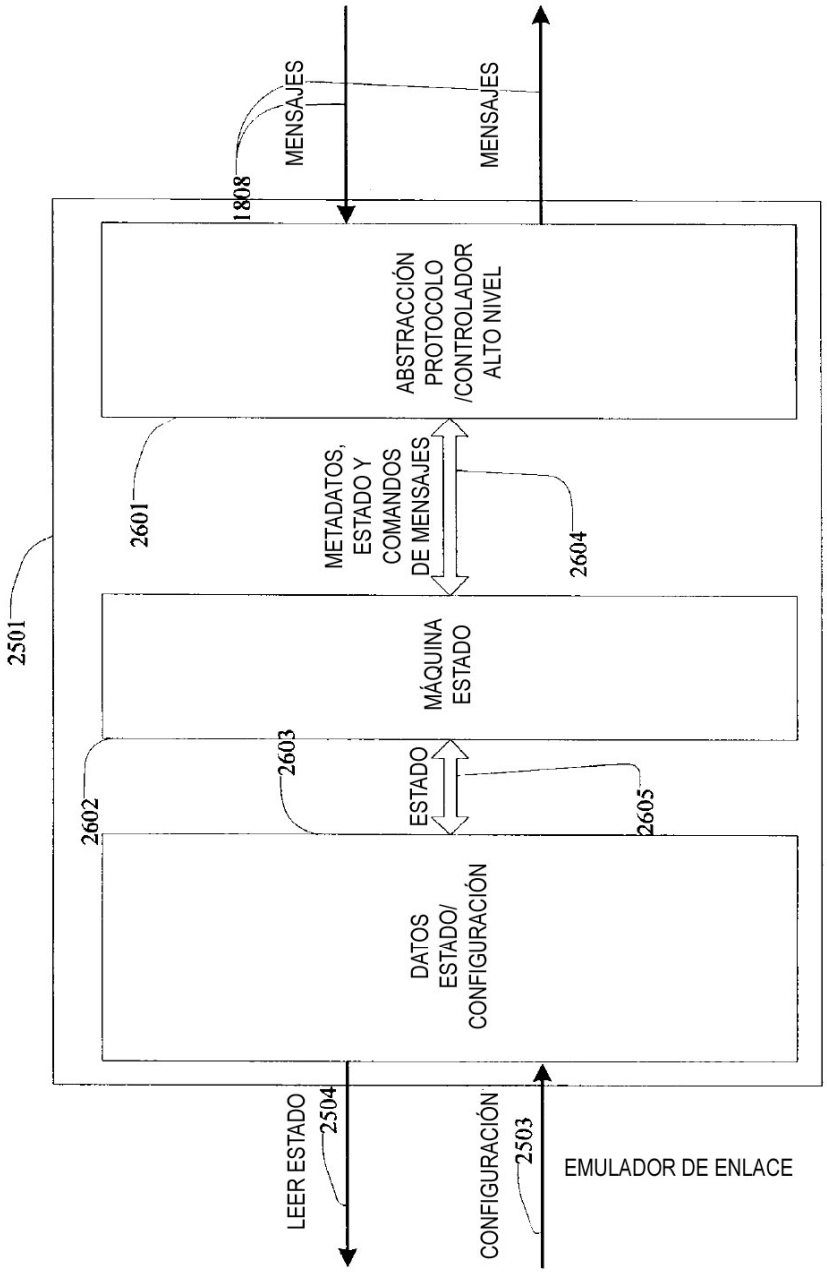

MENSAJES
MENSAJES
1808
ABSTRACCIÓN PROTOCOLO /CONTROLADOR ALTO NIVEL
2601
METADATOS, ESTADO Y COMANDOS DE MENSAJES
2604
2501
MÁQUINA ESTADO
2603
ESTADO
2605
2602
DATOS ESTADO/ CONFIGURACIÓN
LEER ESTADO
2504
CONFIGURACIÓN
2503
EMULADOR DE ENLACE

Fig. 22

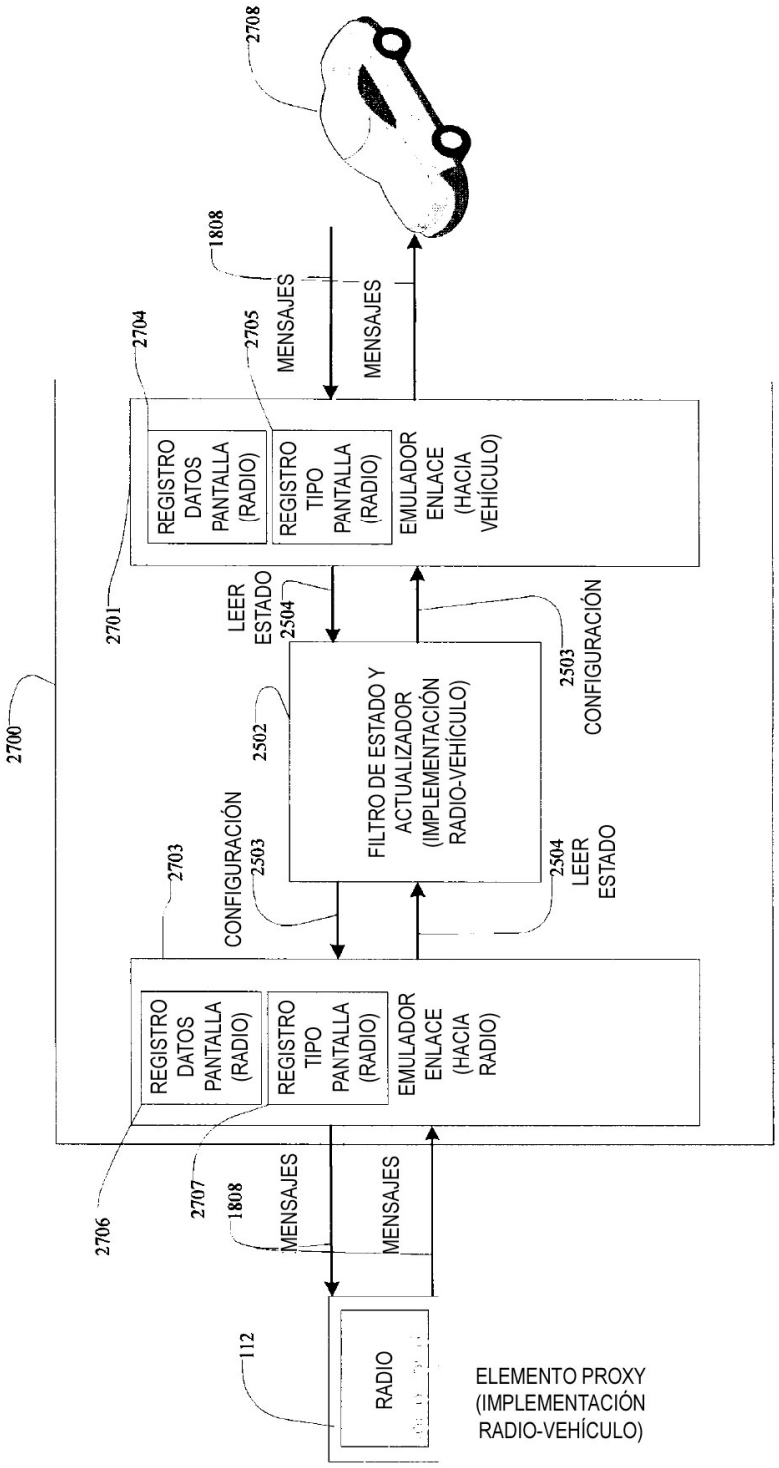

2708
1808
MENSAJES
MENSAJES
2704
2705
REGISTRO DATOS PANTALLA (RADIO)
REGISTRO TIPO PANTALLA (RADIO)
EMULADOR ENLACE (HACIA VEHÍCULO)
2701
LEER ESTADO
2504
2503
CONFIGURACIÓN
2700
2502
FILTRO DE ESTADO Y ACTUALIZADOR (IMPLEMENTACIÓN RADIO-VEHÍCULO)
CONFIGURACIÓN
2503
2703
2504
LEER ESTADO
REGISTRO DATOS PANTALLA (RADIO)
REGISTRO TIPO PANTALLA (RADIO)
EMULADOR ENLACE (HACIA RADIO)
2706
2707
1808
MENSAJES
MENSAJES
112
RADIO
ELEMENTO PROXY (IMPLEMENTACIÓN RADIO-VEHÍCULO)

Fig. 23

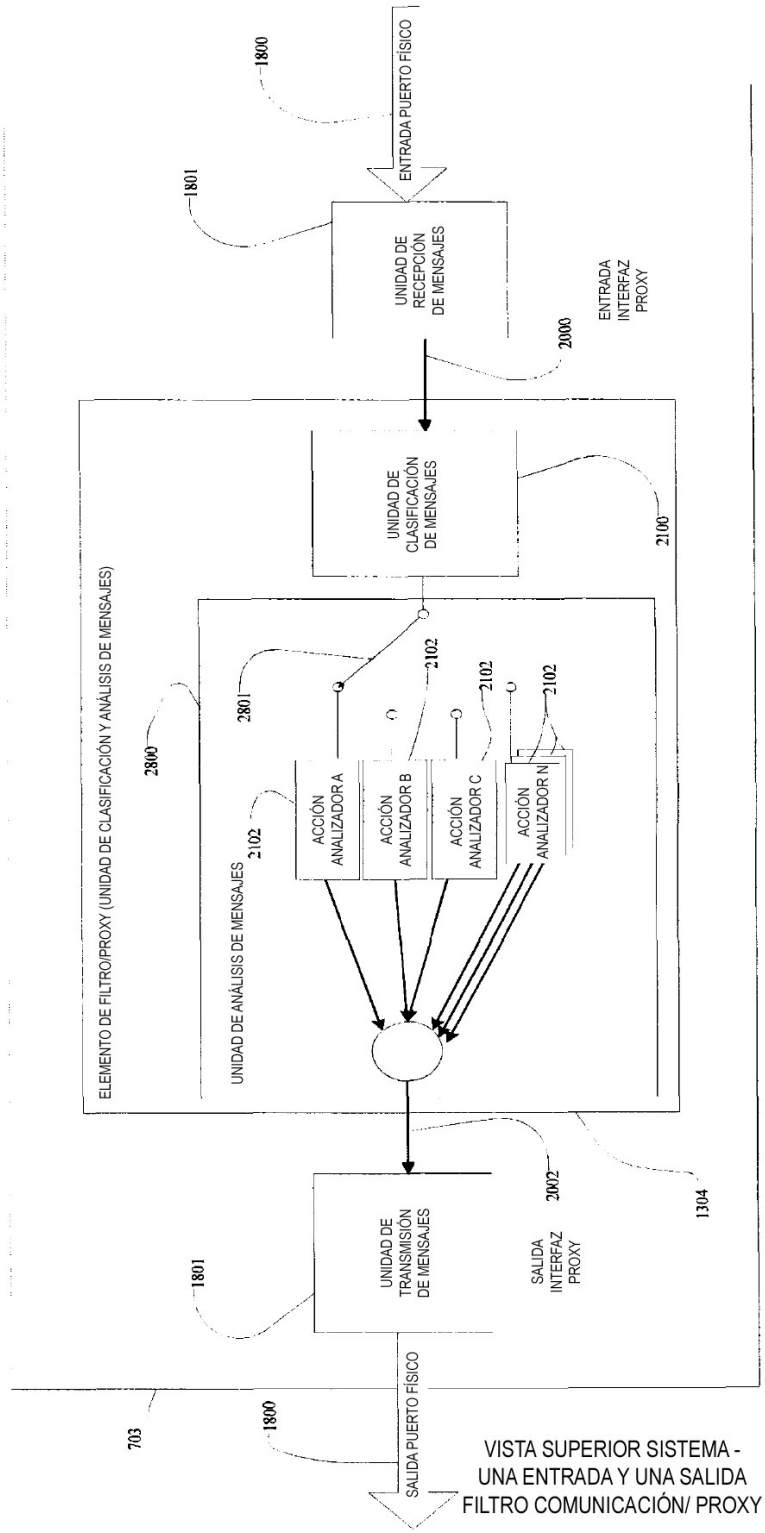

1800
ENTRADA PUERTO FÍSICO
1801
UNIDAD DE RECEPCIÓN DE MENSAJES
ENTRADA INTERFAZ PROXY
2000
UNIDAD DE CLASIFICACIÓN DE MENSAJES
2100
ELEMENTO DE FILTRO/PROXY (UNIDAD DE CLASIFICACIÓN Y ANÁLISIS DE MENSAJES)
2800
UNIDAD DE ANÁLISIS DE MENSAJES
2801
2102
ACCIÓN ANALIZADOR A
ACCIÓN ANALIZADOR B
ACCIÓN ANALIZADOR C
ACCIÓN ANALIZADOR N
UNIDAD DE TRANSMISIÓN DE MENSAJES
SALIDA INTERFAZ PROXY
2002
1304
SALIDA PUERTO FÍSICO
703
VISTA SUPERIOR SISTEMA - UNA ENTRADA Y UNA SALIDA FILTRO COMUNICACIÓN/ PROXY

Fig. 24

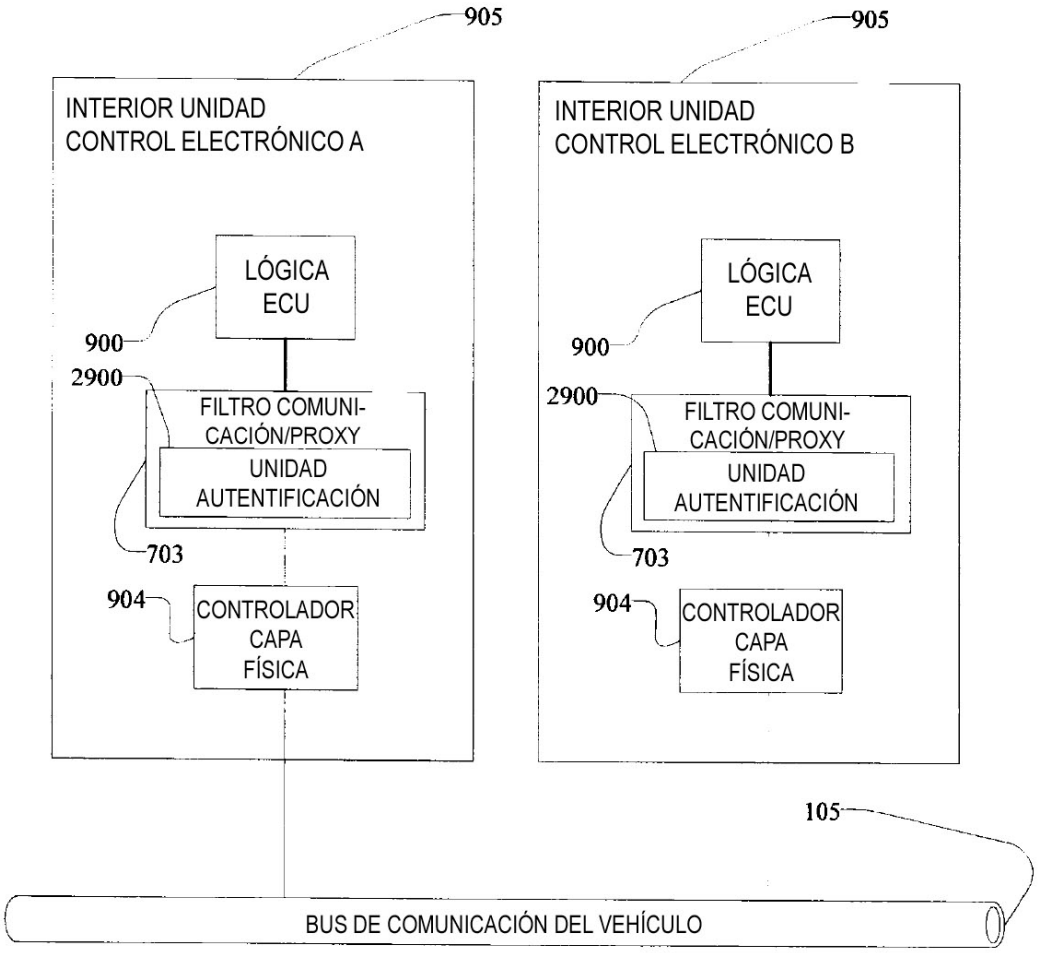

905
905
INTERIOR UNIDAD CONTROL ELECTRÓNICO A
INTERIOR UNIDAD CONTROL ELECTRÓNICO B
LÓGICA ECU
LÓGICA ECU
900
900
2900
2900
FILTRO COMUNI-CACIÓN/PROXY
FILTRO COMUNI-CACIÓN/PROXY
UNIDAD AUTENTIFICACIÓN
UNIDAD AUTENTIFICACIÓN
703
703
904
904
CONTROLADOR CAPA FÍSICA
CONTROLADOR CAPA FÍSICA
105
BUS DE COMUNICACIÓN DEL VEHÍCULO

Fig. 25