(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 391 786**

(51) Int. CI.:
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07003042 .4**
(96) Fecha de presentación: **13.02.2007**
(97) Número de publicación de la solicitud: **1959606**
(97) Fecha de publicación de la solicitud: **20.08.2008**

(54) Título: **Unidad de seguridad**

(45) Fecha de publicación de la mención BOPI:
29.11.2012

(45) Fecha de la publicación del folleto de la patente:
29.11.2012

(73) Titular/es:
SECUNET SECURITY NETWORKS AKTIENGESELLSCHAFT (100.0%)
KRONPRINZENSTRASSE 30
45128 ESSEN, DE

(72) Inventor/es:
KNECHTEL, HARRY;
HOFMANN, MARCO;
HETTSTEDT, GUNNAR y
LINDLBAUER, MARC

(74) Agente/Representante:
LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Unidad de seguridad.

La invención concierne a una unidad de seguridad para un conjunto de comunicación de, por ejemplo, un vehículo, un avión, un barco o similar, en el que la unidad de seguridad presenta al menos un módulo de coordinación configurado como un módulo de hardware para coordinar módulos individuales dentro de la unidad de seguridad, en la que la unidad de seguridad presenta al menos un módulo de criptografía configurado como un módulo de hardware con el cual se generan, almacenan, administran y/o procesan claves criptográficas, en la que la unidad de seguridad presenta al menos un módulo de comunicación externo para comunicar la unidad de seguridad con uno o varios equipos externos no integrados en el conjunto de comunicación y en la que la unidad de seguridad presenta al menos un módulo de programación a través del cual la unidad de seguridad o uno o varios módulos de la unidad de seguridad pueden ser programados, por ejemplo, por un sistema externo. Un equipo de esta clase (por ejemplo un vehículo) presenta usualmente un gran número de componentes eléctricos o electrónicos, los cuales, o bien sus unidades de control, pueden estar unidos uno con otro a través de una red de comunicación y, por tanto, pueden formar un conjunto de comunicación. El término red de comunicación significa en el marco de la invención especialmente un sistema de BUS, por ejemplo un sistema de BUS en un automóvil, un avión, un barco o un sistema de BUS o una red para máquinas en cadenas de producción o bien para instalaciones administradas a distancia. Tales equipos (por ejemplo vehículos automóviles) disponen hoy en día de un gran número de unidades de control que pueden estar configuradas como aparatos de control programables y que están conectadas en red con su entorno en una medida cada vez mayor. Por este motivo, existen esfuerzos para asegurar la integridad y autenticidad de los datos de tales aparatos de control. A este respecto, es conocido en principio el recurso de utilizar procedimientos criptográficos para asegurar la integridad y autenticidad de los datos. En vehículos es ya conocido el recurso de utilizar protocolos criptográficamente protegidos para transportar datos a los vehículos en el taller y en el campo de una manera asegurada. Se conoce por el documento DE 101 28 305 A1 una unidad de control que dispone de una memoria programable. Asimismo, la unidad de control según el documento DE 101 28 305 A1 dispone de un equipo de control que comprueba la autenticidad de los datos que deberán introducirse en la unidad de control. Los procedimientos conocidos en este terreno se basan en software y se ejecutan en procesadores que no poseen en absoluto zonas de memoria criptográficamente aseguradas o bien solo las poseen en grado insuficiente. Asimismo, tales procesadores no poseen la potencia de cálculo necesaria para protocolos criptográficos complejos y las correspondientes operaciones de cálculo. Se conoce por el documento DE 199 55 545 A1 un sistema de control para vehículos automóviles con varios aparatos de control unidos uno con otro, estando asociado a cada aparato de control un controlador de criptografía. En el sistema de control se intercambian entonces los datos entre los distintos aparatos de control de una manera segura contra manipulaciones y cifrada.

Por tanto, la invención se basa en el problema de crear una unidad de seguridad de la clase descrita al principio, por ejemplo para un vehículo automóvil o similar, que garantice una alta medida de seguridad junto con un funcionamiento impecable y rápido.

Para resolver este problema, la invención preconiza una unidad de seguridad (Secure Communication Unit – unidad de comunicación segura) para, por ejemplo, un vehículo, un avión, un barco o similar de la clase citada al principio, la cual se caracteriza porque el módulo de comunicación, en el caso de una situación comprometida de uno o varios módulos, encapsula el módulo o los módulos comprometidos frente a uno o varios de los módulos restantes, porque se pueden cifrar y/o firmar con el módulo de criptografía, a través de una interfaz, los datos recibidos de otro módulo y porque se pueden descifrar los datos recibidos de otro módulo y/o se pueden comprobar sus firmas con el módulo de criptografía a través de la interfaz,

en donde la unidad de seguridad está unida o puede unirse con varias unidades de control del conjunto de comunicación a través de al menos una red de comunicación y en donde la unidad de seguridad presenta al menos un modulo de comunicación interno para comunicar la unidad de seguridad con una o varias unidades de seguridad del conjunto de comunicación, y/o

en donde la unidad de seguridad presenta al menos un módulo de comunicación de procesador para comunicar la unidad de seguridad con al menos un procesador externo.

El módulo de criptografía integrado en la unidad de seguridad genera claves criptográficas, por ejemplo claves simétricas o asimétricas. Según la invención, se pueden cifrar y/o firmar los datos recibidos de otro módulo a través de una interfaz. Además, según la invención, con ayuda del módulo de criptografía se pueden descifrar datos recibidos de otro módulo y/o se pueden comprobar o valorar firmas a través de una interfaz. La unidad de seguridad presenta aquí al menos un módulo de coordinación para coordinar y comunicar los distintos módulos dentro de la unidad de seguridad. El módulo de coordinación administra los recursos de hardware, asigna aplicaciones a estos recursos y asegura la comunicación entre los módulos de la unidad de seguridad o bien controla los módulos. De esta forma, el módulo de coordinación asegura que puedan hacerse funcionar los distintos módulos dentro de la unidad de seguridad, sin que éstos se influyan entonces mutuamente, y que, según la invención, en el caso de una situación comprometida se encapsule también el módulo comprometido frente a los restantes módulos conectados. La autentificación se efectúa entonces a través del módulo de criptografía. El módulo de coordinación

garantiza la seguridad contra fallos de la unidad de seguridad según la invención. Conforme a la invención, la unidad de seguridad está equipada al menos con un módulo de programación a través del cual se pueden programar la unidad de seguridad o uno o varios módulos de la unidad de seguridad, por ejemplo por medio de un sistema externo. El módulo de criptografía está configurado según la invención como un módulo de hardware. Según la invención, el módulo de coordinación y/o el módulo de programación están configurados como módulos de hardware.

La unidad de seguridad según la invención puede estar destinada, por ejemplo, a un conjunto de comunicación de, por ejemplo, un vehículo, un avión, un barco o similar o bien puede integrarse en un conjunto de comunicación de esta clase. Este conjunto de comunicación puede componerse de varias unidades de control a base de componentes eléctricos o electrónicos individuales que están unidas una con otra a través de una red de comunicación, por ejemplo un bus. Según la invención, la unidad de seguridad está unidad con las unidades de control restantes a través de esta red de comunicación. Según la invención, la unidad de seguridad presenta un módulo de comunicación interno para comunicar la unidad de seguridad con una o varias unidades de control (Electronic Control Unit – unidad de control electrónica) del conjunto de comunicación. Este módulo de comunicación interno puede (como opción) cargarse posteriormente a través del módulo de programación.

La invención parte del conocimiento de que la seguridad dentro de un conjunto de comunicación que presenta un gran número de equipos eléctricos o electrónicos con unidades de control correspondientes, se incrementa considerablemente cuando, según la invención, está integrada en este conjunto de comunicación una unidad de seguridad que presenta un modulo de criptografía que está realizado en hardware, por ejemplo como ASIC o FPGA. La unidad de criptografía genera y almacena material de clave criptográfica de una manera segura. Asimismo, a través del módulo de criptografía se producen una ejecución segura y rápida de operaciones criptográficas, así como un almacenamiento de datos. El módulo de coordinación proporciona una administración segura contra fallos y eficiente de las funciones descritas y un encapsulado de los módulos conectados al módulo de comunicación en el caso de una situación comprometida de un módulo, efectuándose el encapsulado frente al módulo comprometido por medio de un bloqueo del acceso al módulo de comunicación. El módulo de programación garantiza una capacidad de carga posterior segura de módulos para adaptar una unidad de seguridad a los requisitos de diferentes entornos de uso y, por ejemplo, diferentes fabricantes de vehículos.

La posibilidad descrita de integración de una unidad de seguridad en un conjunto de comunicación representa una forma de realización posible de la invención. Sin embargo, la unidad de seguridad según la invención puede hacerse funcionar también en solitario o independientemente de un conjunto de comunicación de esta clase y, en consecuencia, en el “modo autónomo”. Con esto se quiere dar a entender en el marco de la invención que la unidad de seguridad no se comunica con un conjunto de comunicación (directamente) a través de, por ejemplo, un módulo de comunicación interno, sino que lo hace, por ejemplo, con un procesador que no es él mismo objeto de la unidad de seguridad. Esta comunicación puede efectuarse a través del módulo de comunicación del procesador descrito en lo que sigue, el cual puede estar integrado también en la unidad de seguridad.

En consecuencia, en una forma de realización preferida la unidad de seguridad está constituida al menos por la unidad de criptografía realizada en hardware, el módulo de coordinación realizado en hardware, el módulo de programación realizado en hardware y el módulo de comunicación interno, el cual puede ser programado opcionalmente a través de la unidad de criptografía después de recibir la autorización pertinente.

Según la invención, la unidad de seguridad presenta al menos un módulo de comunicación externo para comunicar la unidad de seguridad con uno o varios equipos externos. Equipo externo significa un equipo que no está integrado en el conjunto de comunicación. En consecuencia, para la comunicación con sistemas situados fuera del conjunto de comunicación, la unidad de seguridad proporciona el módulo de comunicación externo (adicional), el cual, después de la autorización pertinente, puede ser programado a través del módulo de criptografía.

Según la invención, la unidad de seguridad presenta al menos un módulo de comunicación de procesador para comunicar la unidad de seguridad con al menos un procesador externo. En consecuencia, a través de este módulo de comunicación de procesador que, después de recibir la autorización pertinente, puede ser programado a través de la unidad de criptografía, se puede efectuar una vinculación de la unidad de seguridad con otro procesador. Asimismo, la unidad de seguridad proporciona la posibilidad de cargar otros módulos, después de recibir la autorización pertinente, en la unidad de seguridad a través del módulo de criptografía y de notificar esto al módulo de coordinación.

El módulo de comunicación interno puede estar configurado como módulo de hardware o como módulo de software. Además, existe la posibilidad de que el módulo de comunicación externo esté configurado como módulo de hardware o como módulo de software. Por último, el modulo de comunicación de procesador puede estar configurado como módulo de hardware o como módulo de software.

El módulo de comunicación interno, el módulo de comunicación externo, el módulo de programación y/o el módulo de comunicación de procesador están unidos con la unidad de criptografía a través del módulo de coordinación o

bien acceden a la unidad de criptografía a través del módulo de coordinación.

En consecuencia, en el marco de la invención se puede generar en el vehículo un anclaje de confianza criptográfica seguro con un solo control de, por ejemplo, un fabricante de automóviles, que confiera la plena eficacia al procedimiento criptográfico y a sus aplicaciones y que pueda ejecutar las operaciones criptográficas con suficiente rapidez para garantizar la seguridad en base a funciones criptográficas. Se garantiza entonces la seguridad especialmente también en estados temporalmente críticos del vehículo. Se puede tratar aquí de procesos en cadena rápidos para una producción barata de vehículos, procesos de servicio rápidos para minimizar los costes de mantenimiento, comunicación de vehículo a vehículo y accesos en línea al vehículo. Asimismo, la invención parte del conocimiento de que, por ejemplo, en el sector de vehículos, aviones y barcos han de tenerse en cuenta requisitos especiales referentes al entorno de utilización. En lo que sigue se explica en particular la invención con más detalle ayudándose de unos dibujos que representan solamente un ejemplo de realización. Muestran:

La figura 1, un diagrama de bloques simplificado de un conjunto de comunicación con una unidad de seguridad según la invención y

La figura 2, un fragmento del objeto según la figura 1 en representación esquemática.

En las figuras se representa un conjunto de comunicación KV para un equipo que presenta un gran número de componentes eléctricos o electrónicos. Este equipo puede consistir, por ejemplo, en un vehículo automóvil. Los distintos componentes eléctricos o electrónicos presentan sendas unidades de control ECU. Estas distintas unidades de control ECU están unidas una con otra a través de una red de comunicación BUS que en el ejemplo de realización está configurada como un sistema de BUS. Un bus de vehículo de esta clase puede consistir, por ejemplo, en un bus CAN. En el ejemplo de realización representado se ha integrado en este conjunto de comunicación KV una unidad de seguridad SCU que, al igual que ocurre también con las unidades de control, está conectada al sistema de BUS. Éste se encuentra representado esquemáticamente en la figura 1. Sin embargo, la unidad de seguridad SCU puede hacerse funcionar también en solitario o sin el conjunto de comunicación representado, es decir, en un “modo autónomo”.

La constitución y el funcionamiento de esta unidad de seguridad SCU según la invención se desprenden especialmente de la figura 2.

Esta unidad de seguridad SCU conectada al bus del vehículo presenta de momento un modulo de criptografía KU, un módulo de coordinación KM, un módulo de programación PM y un módulo de comunicación interno IKOM. En cualquier caso, el módulo de criptografía KU, el módulo de coordinación KM y el módulo de programación PM están realizados en hardware. El módulo de comunicación interno IKOM está opcionalmente previsto y puede ser cargado posteriormente, por ejemplo, a través del módulo de programación PM.

Asimismo, en el ejemplo de realización se han integrado en la unidad de seguridad SCU un modulo de comunicación externo EKOM y un módulo de comunicación de procesador IPCM.

El núcleo funcional de esta unidad de seguridad SCU es la unidad de criptografía configurada como módulo de hardware o el módulo de criptografía KU con el cual se generan, almacenan, administran y/o procesan claves criptográficas. La unidad de criptografía KU proporciona un entorno seguro para la generación y administración de material de clave criptográfica. Asimismo, se proporcionan zonas de memoria seguras. Estas zonas de memorias seguras están protegidas contra lectura y escritura no autorizadas de datos de cualquier clase, pero especialmente de claves criptográficas. Estas zonas de memoria pueden ser configuradas también respecto del acceso y la administración de los datos allí depositados. Así, se puede ajustar si estos datos son nuevamente exportables o deberán emplearse tan solo dentro de la unidad de seguridad.

La unidad de criptografía KU está aquí en condiciones de generar por medio de órdenes internas de la unidad de seguridad números aleatorios en longitud configurable y/o claves simétricas en longitud configurable y/o claves asimétricas en longitud configurable. La unidad de criptografía KU presenta aquí una interfaz genérica. Además, se han implementado algoritmos configurables, es decir que el módulo de criptografía KU puede ser configurado por medio del fechado con respecto a los algoritmos, manteniéndose igual la interfaz genérica hacia fuera. De esta manera, se pueden cifrar datos de cualquier clase o bien se pueden firmar éstos electrónicamente en forma simétrica o asimétrica o bien se calcula una huella dactilar de los datos. Asimismo, la unidad de criptografía posee una interfaz a través de la cual se la vincula a una PKI (Public Key Infrastruktur – infraestructura de clave pública). En consecuencia, como se ha explicado, se puede generar y almacenar con seguridad un par de claves asimétricas y se puede exportar una petición de certificación para ésta PKI. El módulo de criptografía KU está aquí en condiciones de exportar peticiones de certificación e importar certificados. Asimismo, la unidad de criptografía KU está en condiciones de proteger zonas de memoria situadas fuera de la unidad de seguridad SCU contra accesos de lectura y escritura desde fuera de la unidad de seguridad. Con ayuda del módulo de criptografía KU se comprueba firmas electrónicas (simétrica y asimétricamente), incluida la cadena de certificados eventualmente correspondiente. Además, la unidad de criptografía KU puede proporcionar un tiempo asegurado. Dado que la unidad de criptografía KU está realizada como un módulo de hardware, se garantiza que ésta no pueda ser programada desde fuera sin

autorización. Opcionalmente, es también resistente frente a ataques de hardware.

El módulo de coordinación KM representado también en la figura 2 forma, junto con el módulo de criptografía KU, el núcleo relevante para la seguridad y asegura que se hagan funcionar fiablemente los distintos módulos dentro de la unidad de seguridad, sin que se produzca una influenciación mutua. En el caso de una situación comprometida, el módulo de coordinación KM encapsula el módulo comprometido frente a los restantes módulos conectados. De esta manera, el módulo de coordinación, en su función como interfaz de comunicación SCU central, está en condiciones de suprimir la comunicación desde/hacia el módulo comprometido. El módulo de coordinación KM administra los recursos de hardware de la unidad de seguridad SCU y los adjudica a los respectivos módulos o aplicaciones. Siempre que sea necesario, el módulo de coordinación KM asegura la comunicación entre los distintos módulos de la unidad de seguridad.

Es de importancia también en el marco de la invención el módulo de comunicación interno (opcional) IKMO. Interno significa en este contexto la comunicación dentro del conjunto de comunicación KV, es decir, la comunicación de la unidad de seguridad SCU con distintas unidades de control ECU de un conjunto de comunicación. Estas unidades de control ECU pueden ser partes integrantes de, por ejemplo, componentes de vehículo correspondientes o bien pueden estar asociadas a tales componentes de vehículo. El módulo de comunicación interno IKOM realiza preferiblemente la comunicación bidireccional de la unidad de seguridad SCU con otros aparatos de control ECU del conjunto de comunicación KV. Si una unidad de control ECU dispone ella misma de una unidad de seguridad correspondiente y, en consecuencia, están integradas varias unidades de seguridad en un conjunto de comunicación, es posible entonces entre estas unidades de seguridad un intercambio de datos auténtico y protegido contra manipulaciones a través de un protocolo. Opcionalmente, el intercambio de datos es también confidencial. A este respecto, la figura 2 insinúa que, para la aplicación de métodos criptográficos, el módulo de comunicación interno IKOM accede a la unidad de criptografía KU a través del módulo de coordinación KM. Opcionalmente, existe la posibilidad de que el módulo de comunicación interno IKOM “escuche” de manera configurable a ciertos datos que se transmitan dentro del conjunto de comunicación, pudiendo estar previsto entonces que estos datos sean almacenados en la zona segura del módulo de criptografía KU.

Mientras que el módulo de comunicación interno IKOM en funcionamiento realiza la comunicación dentro del conjunto de comunicación, el módulo de comunicación externo adicionalmente previsto EKOM realiza una comunicación de datos entre la unidad de seguridad del conjunto de comunicación y un sistema externo, por ejemplo un sistema conectado fuera del vehículo o no conectado al BUS. Tal sistema externo ES puede consistir, por ejemplo, en un equipo de ensayo o bien un servidor temporalmente conectado. El establecimiento de la conexión se efectúa aquí en forma auténtica, es decir que se produce una conexión únicamente cuando el módulo de comunicación externo EKOM ha autentificado el sistema externo ES con ayuda del módulo de criptografía KU. Opcionalmente, se autentifica también la unidad de seguridad SCU con ayuda del módulo de comunicación externo EKOM frente al sistema externo ES. Asimismo, existe opcionalmente la posibilidad de que los datos transmitidos sean transmitidos también en forma auténtica y, en caso necesario, en forma cifrada. La autentificación de los datos puede estar acoplada aquí también a la autentificación del establecimiento de la conexión. Además, existe la posibilidad de que el módulo de comunicación externo EKOM disponga de uno o varios filtros que decidan sobre la retransmisión de datos. Un módulo de comunicación externo EKOM almacena los datos de autentificación de una conexión.

Una parte integrante esencial de la unidad de seguridad según la invención es también el módulo de programación PM representado en la figura 2. A través de éste es posible el acceso configurable a zonas de memoria de la unidad de seguridad, con lo que se pueden cargar posteriormente módulos y datos. El acceso de programación se efectúa en forma autentificada a través de un sistema externo ES. Éste está insinuado en la figura 2 por medio de la conexión entre el sistema externo ES y el módulo de programación PM, mientras que el módulo de programación PM está conectado entonces a su vez con el módulo de coordinación KM y, en consecuencia, a través de este módulo de coordinación KM, con los restantes módulos de la unidad de seguridad. El módulo de programación comprueba entonces la autenticidad e integridad de los módulos y datos cargados posteriormente.

Por último, se ha insinuado en la figura 2 que la unidad de seguridad puede disponer de un módulo de comunicación de procesador (opcional) IPC que haga posible una comunicación IPC bidireccional de la unidad de seguridad SCU con otro procesador. De esta manera, la unidad de seguridad SCU proporciona los servicios criptográficos de la unidad de criptografía KU a otro procesador µC a través de un protocolo. El procesador representado en la figura 2 puede ser en el ejemplo de realización un microcontrolador µC.

En una forma de realización modificada (no representada) la unidad de seguridad no se comunica (directamente) con un conjunto de comunicación, sino que se comunica, a través de, por ejemplo, el módulo de comunicación de procesador IPCM, con un procesador que puede retransmitir eventualmente después informaciones/datos. En este caso, que se denomina “modo autónomo” en el marco de la invención, se puede prescindir eventualmente del módulo de comunicación interno IKOM.

REIVINDICACIONES

1. Unidad de seguridad (SCU) para un conjunto de comunicación de, por ejemplo, un vehículo, un avión, un barco o similar,

en la que la unidad de seguridad (SCU) presenta al menos un módulo de coordinación (KM) configurado como un módulo de hardware para coordinar módulos individuales dentro de la unidad de seguridad (SCU),

en la que la unidad de seguridad (SCU) presenta al menos un módulo de criptografía (KU) configurado como un módulo de hardware con el que se pueden generar, almacenar, administrar y/o procesar claves criptográficas,

en la que la unidad de seguridad (SCU) presenta al menos un módulo de comunicación externo (EKOM) para comunicar la unidad de seguridad (SCU) con uno o varios equipos externos (ES) no integrados en el conjunto de comunicación (KV), y

en la que la unidad de seguridad (SCU) presenta al menos un módulo de programación (PM) a través del cual la unidad de seguridad (SCU) o uno o varios módulos de la unidad de seguridad (SCU) pueden ser programados, por ejemplo por un sistema externo (ES)

caracterizada porque

el módulo de coordinación (KM), en el caso de una situación comprometida de uno o varios módulos, encapsula el módulo o los módulos comprometidos frente a uno o más de los módulos restantes,

los datos recibidos de otro módulo pueden ser cifrados y/o firmados, a través de una interfaz, con el módulo de criptografía (KU), y

los datos recibidos de otro módulo pueden ser descifrados y/o las firmas pueden ser comprobadas o evaluadas, a través de la interfaz, con el módulo de criptografía (KU),

en donde la unidad de seguridad (SCU) está conectada o puede conectarse con varias unidades de control (ECU) del conjunto de comunicación (KV) a través de al menos una red de comunicación (BUS) y en donde la unidad de seguridad (SCU) presenta al menos un módulo de comunicación interno (IKOM) para comunicar la unidad de seguridad (SCU) con una o varias unidades de control (ECU) del conjunto de comunicación (KV), y/o

en donde la unidad de seguridad (SCU) presenta al menos un módulo de comunicación de procesador (IPCM) para comunicar la unidad de seguridad (SCU) con al menos un procesador externo (µC).

2. Unidad de seguridad según la reivindicación 1, **caracterizada** porque la red de comunicación está configurada como un sistema de BUS (BUS).

3. Unidad de seguridad según cualquiera de las reivindicaciones 1 ó 2, **caracterizada** porque el módulo de programación (PM) está configurado como un módulo de hardware.

4. Unidad de seguridad según cualquiera de las reivindicaciones 1 a 3, **caracterizada** porque el módulo de comunicación interno (IKOM), el módulo de comunicación externo (EKOM) y/o el módulo de comunicación de procesador (IPCM) están configurados como módulos de hardware y/o como módulos de software.

5. Unidad de seguridad según cualquiera de las reivindicaciones 1 a 4, **caracterizada** porque el módulo de comunicación interno (IKOM), el módulo de comunicación externo (EKOM), el módulo de programación (PM) y/o el módulo de programación de procesador (IPCM) se comunican con el módulo de criptografía (KU) o acceden al módulo de criptografía (KU) a través del módulo de coordinación (KM).

6. Conjunto de comunicación (KV) para un equipo que presenta uno o varios componentes eléctricos o electrónicos, por ejemplo un vehículo, un avión, un barco o similar con varias unidades de control (ECU) conectadas una con otra a través de al menos una red de comunicación (BUS), estando conectada a la red de comunicación (BUS) al menos una unidad de seguridad (SCU) según cualquiera de las reivindicaciones 1 a 5.

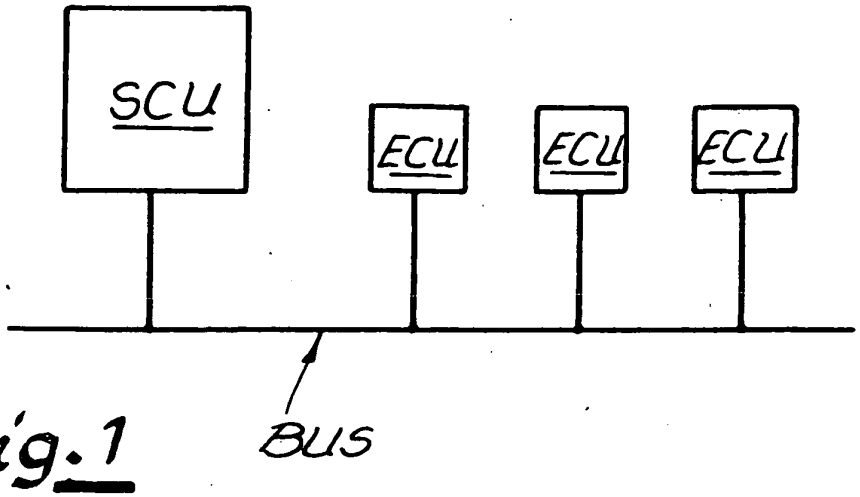

Fig.1

Fig.2