



# (12)发明专利

(10)授权公告号 CN 103796882 B

(45)授权公告日 2017.07.25

(21)申请号 201280044908.1

(22)申请日 2012.09.17

(65)同一申请的已公布的文献号  
申请公布号 CN 103796882 A

(43)申请公布日 2014.05.14

(30)优先权数据  
11306159.2 2011.09.16 EP

(85)PCT国际申请进入国家阶段日  
2014.03.14

(86)PCT国际申请的申请数据  
PCT/EP2012/068201 2012.09.17

(87)PCT国际申请的公布数据  
W02013/037996 EN 2013.03.21

(73)专利权人 金雅拓股份有限公司

地址 法国默东

(72)发明人 Y.格雷萨斯 P.勒罗伊

(74)专利代理机构 北京市柳沈律师事务所  
11105

代理人 李芳华

(51)Int.Cl.  
B60R 25/00(2013.01)

审查员 胡欣

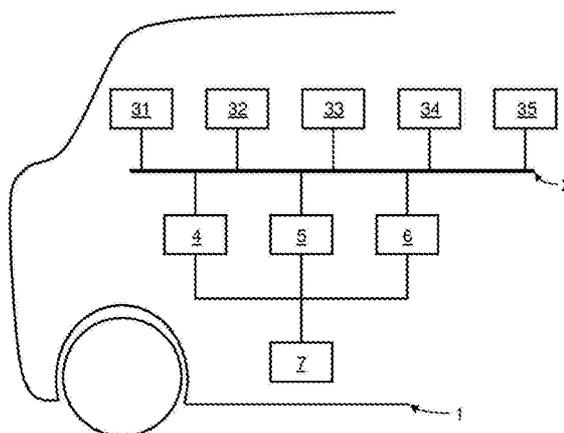
权利要求书1页 说明书4页 附图2页

## (54)发明名称

提供对安全性数据的防护访问的车辆

## (57)摘要

本发明涉及一种车辆(1),包括:多路复用的通信总线(2);与该通信总线(2)连接的引擎控制单元(4);防护元件(6),被放置在车辆中,并被配置为通过该通信总线进行通信,该防护元件安全地存储(64)与该车辆相关的安全性数据。



1. 一种车辆(1),其特征在于包括:
  - 多路复用的通信总线(2);
  - 与该通信总线(2)连接的引擎控制模块(4);
  - 智能卡(6),其是防篡改的并被放置在车辆中,并被配置为通过该通信总线进行通信,该智能卡安全地存储(64)与该车辆相关的安全性数据,所述智能卡(6)包括存储与所述车辆(1)相关的所述安全性数据的持久存储区域(64)、和被配置为验证请求对所述持久存储区域(64)的读或写访问的实体的安全性管理模块(63)。
2. 根据权利要求1的车辆(1),其中该智能卡被配置为与该引擎控制模块(4)通信,以恢复与该车辆相关的安全性数据,并被配置为存储所恢复的安全性数据。
3. 根据权利要求1的车辆,进一步包括与该通信总线连接的几个电子控制单元(33),该智能卡被配置为与这些电子控制单元通信,并安全地存储这些电子控制单元所提供的数据。
4. 根据权利要求1的车辆,其中该通信总线是控制器局域网兼容总线。
5. 根据权利要求1的车辆,进一步包括车辆装置供电电池(7),该智能卡(6)包括电力变压器(84),与所述装置供电电池连接,并对该智能卡的电子电路供电。
6. 根据权利要求1的车辆,其中该智能卡(6)包括无线通信接口(83)。
7. 根据权利要求1的车辆,其中该持久存储区域(64)和该安全性管理模块(63)嵌入在智能卡芯片(62)中。
8. 根据权利要求7的车辆,其中该智能卡(6)包括与所述通信总线连接的通信接口(81),并进一步包括通信管理模块(82),形成该通信接口和该智能卡芯片(62)之间的通信桥。

## 提供对安全性数据的防护访问的车辆

### 技术领域

[0001] 本发明一般涉及机动车,并更具体地,涉及与车辆相关的安全性(security)数据的存储,必须对所述安全性数据提供保护访问以防止伪造(forgery)。

### 背景技术

[0002] 交通工具按照数字或模拟形式来在存储与其关联的各种数据。存储的数据例如是里程(mileage)、到下一次大修(overhaul)的距离、车辆序列号、车牌数据、车辆故障的日期和类型等。存储的数据可以根据其存储介质被可视地访问或电子地访问。例如,里程被存储在引擎控制模块(ECM)中并显示在仪表板上。车辆故障的日期和类型也被存储在引擎控制模块中。这样的数据可使用通过专用连接器与引擎控制模块连接的特定电子仪器来读取并有时修改。

[0003] 引擎控制模块一般从汽车中的各个装置收集数据。车辆现在包括遍布车辆的大量电子控制单元,用于执行安全(safety)、控制或舒适功能。这样的控制单元特别用来管理变速箱(transmission)、安全气囊、防抱死制动系统/ABS、巡航控制、电动助力转向/EPS、音频系统、窗、门、镜子调整等。这些电子控制单元中的一些形成独立子系统,但是其间的通信或者与ECM的通信是必要的。ECM可基于其他电子控制单元提供的信息来特别编辑如同里程的要保护的数据。子系统可能也需要控制致动器或接收来自传感器的反馈。

[0004] CAN(控制器局域网)是在道路车辆中使用的支持分布式实时控制和多路复用的串行通信技术。CAN是基于消息的协议。如今,生产的大部分车辆都集成CAN总线。CAN标准在ISO 11898规范中特别定义。

[0005] 对安全性数据的访问既没有安全到足以防止伪造,也不可能用于没有专用诊断工具的最终用户。

### 发明内容

[0006] 由此,存在对于克服这些缺陷中的一个或多个的车辆的需求。本发明由此涉及一种车辆,包括:

[0007] 一多路复用的通信总线;

[0008] 一与该通信总线连接的引擎控制单元;

[0009] 一防护元件,被放置在车辆中,并被配置为通过该通信总线进行通信,该防护元件安全地存储与该车辆相关的安全性数据。

[0010] 根据另一实施例,该防护元件被配置为与该引擎控制单元通信,以恢复与该车辆相关的安全性数据,并被配置为存储所恢复的安全性数据。

[0011] 根据另一实施例,该车辆进一步包括与该通信总线连接的几个电子控制单元,该防护元件被配置为与这些电子控制单元通信,并安全地存储这些电子控制单元所提供的数据。

[0012] 根据实施例,该通信总线是控制器局域网兼容总线。

[0013] 根据另一实施例,该车辆进一步包括装置供电的电池,该防护设备包括电力变压器,与所述装置供电的电池连接,并对该防护设备的电子电路供电。

[0014] 根据另一实施例,该防护元件包括无线通信接口。

[0015] 根据另一实施例,该防护元件包括持久存储区域,存储与该车辆相关的所述安全性数据。

[0016] 根据实施例,该防护元件包括安全性管理模块,被配置为验证请求对所述持久存储区域的读或写访问的实体。

[0017] 根据另一实施例,该持久存储区域和该安全性管理模块被嵌入在智能卡芯片中。

[0018] 根据另一实施例,该防护元件包括与所述通信总线连接的转换器,并进一步包括通信管理模块,形成该转换器和该智能卡芯片之间的通信桥。

### 附图说明

[0019] 通过参考附图对于几个实施例的以下描述,本发明的优点将变得清楚,其中:

[0020] 一图1是根据本发明的车辆的示例的示意图;

[0021] 一图2是固定在图1的车辆上的防护元件的示意图;

[0022] 一图3是防护元件的另一实施例的示意图;

[0023] 一图4是防护元件的另一实施例的示意图。

### 具体实施方式

[0024] 图1是根据本发明实施例的车辆1的示例的示意图。车辆1包括通信总线2,例如CAN总线。管理车辆安全特征的各种装置连接到总线2并遍布在车辆1中。车辆1特别包括引擎31、变速箱32、仪表板33、锁系统34和防抱死制动系统35。这些装置中的每一个执行与车辆安全性相关的功能性。例如,当车辆1正在移动时保持引擎31开启是避免不必要的主要安全事项。还不得不按照规则间隔来维护引擎。变速箱32的控制也可与提供有自动变速箱的车辆的安全相关,用于当用户换挡时避免不必要的引擎超速。仪表板33具有安全性特征:它应特别显示精确里程。锁系统34与安全相关,因为当汽车正在移动时,它可将汽车自动落锁,或者当驾驶员激励对应遥控器时,它能使得所有车门解锁。防抱死制动系统35显然与安全特征相关,因为当检测到抱死的车轮时,它不得不释放制动力。诸如驾驶员识别等进一步的安全性或安全特征也能通过与CAN总线2连接的附加装置来执行。关于这些装置执行的管理的主要问题正避免欺诈或正保证可靠的安全数据。

[0025] 引擎控制模块4、机身控制模块5和防护模块6也连接到CAN总线2。这些装置4、5和6由装置供电的电池7(典型地,施加车辆电网上的12V电压)供电。引擎控制模块ECM 4负责通过CAN总线2管理各个装置电子控制单元或传感器,诸如引擎31、变速箱32或仪表板33。机身控制模块5负责通过CAN总线2管理各个其他装置电子控制单元或传感器,诸如车辆1的锁系统34或各种灯。

[0026] 防护元件通常利用需要的安全性级别来定义包括能够嵌入智能卡级应用的防篡改智能卡芯片的装置。防护元件能集成在各种形式因素:SIM卡或SD卡、M2M形式因素中,或嵌入在较大电路中。

[0027] 防护模块6包括诸如智能卡的防护元件。防护元件意欲存储各种安全性数据,并且

如果满足验证需求,则提供对这些数据的访问。防护模块6可验证一个或多个授权的实体。存储的安全性数据例如是里程、到下一次大修的距離、車輛序列号、車輛类型、汽車制造商数据、車牌数据、主驾驶员身份、最后技术控制的里程或日期、車輛故障的日期和类型等。存储的安全性数据可以是車輛1中的其他地方中存储的数据的副本。例如,里程可以从ECM4拷贝的备用信息。車牌数据可以被存储在車牌中所嵌入的RFID标签中。車輛序列号可以被存储在位于引擎舱中的雕板(carved plate)中所嵌入的RFID标签中。

[0028] 防护元件还可以存储与安全相关的数据。例如,与引擎管理相关的参数可被存储在防护元件中(例如,喷射定时、涡轮增压机压力……),以检查用户是否还没有欺诈性地修改这些参数。这些参数的欺诈性修改可例如对引擎行为具有影响,并能导致意想不到的机能障碍。

[0029] 防护元件是机器对机器(M2M)兼容的。取决于目标安全性级别,防护元件应是可移除的或不可移除的(例如,焊接的)。M2M表示这样的技术,该技术允许装置与其他装置通信并得到特定属性作为支持从-40℃直到125℃的大温度范围。M2M使用装置(诸如传感器或测量仪表)来捕获通过网络向另一装置中的应用中继的事件(诸如温度、压力等)。应用将捕获的事件翻译为有意义的信息。根据这样的功能性,各种装置能充当该防护元件的主装置。

[0030] 图2示意性图示了防护模块6的第一实施例。防护模块6包括用作防护元件的智能卡65和智能卡接口翻译器8。智能卡65被插入到智能卡接口翻译器8的连接槽85中。

[0031] 智能卡65包括按照本身已知的方式嵌入到卡基板中的芯片62。芯片62包括安全性管理模块63和持久数据存储区域64。安全性管理模块63执行防护应用。持久数据存储区域64存储所述安全性数据。这样的智能卡65一般被用来执行用户或装置验证。安全性管理模块63所以被配置为在其提供对区域64中存储的数据的写/读访问之前执行验证。这样的智能卡65能具有任何适当格式,诸如标准UICC格式或用于M2M应用的QFN(方形平面无引脚,其是标准不可移除格式)封装之中。

[0032] 智能卡接口翻译器8包括与CAN总线2连接的通信接口81。智能卡接口翻译器8有利地包括无线通信接口83。智能卡接口翻译器8包括通信管理模块82。通信管理模块82通过连接槽85与智能卡65通信。通信管理模块82管理通信接口81和智能卡65之间的通信、以及无线接口83和智能卡65之间的通信。通信管理模块82可形成智能卡65与通信接口81和83之间的协议桥。智能卡接口翻译器8进一步包括电力变压器84。电力变压器84通过車輛1的电网连接到电池7。电力变压器84将电池电压转换为较低电压,以对智能卡接口翻译器8和智能卡65的各个电路供电。

[0033] 由于通信管理模块82的存在,所以可使用标准智能卡65以获得非常成本有效的方案。智能卡65可使用适当协议和适当接口(例如,根据SWP标准)与通信管理模块82通信。

[0034] 无线通信接口83可与各个标准兼容,以例如通过移动电话通信网络进行通信,或根据NFC协议或根据诸如蓝牙或IEEE 802.15兼容协议的进一步协议来进行通信。

[0035] 可使用无线通信接口83,以使得防护模块6与不具有对于CAN总线2的访问权的其他装置通信。这样的装置可以特别是全球定位系统、智能移动电话、提供有RFID标签的車牌、或提供有RFID标签并显示車輛序列号的雕板。防护模块6由此能从这样的装置恢复数据,并将这些数据存储在存储区域64中。不同种类用户也能在不具有任何CAN特定通信装置的情况下,通过无线通信接口83访问防护模块6。最终用户能由此访问防护模块6,以咨询大

修或技术控制的下一次发生。专家能由此通过比较它们的数据和存储区域64中存储的数据,来检查车牌或雕板是否已被伪造。防护模块6还可以检测和验证提供有RFID标签的驾驶证。验证的驾驶证可与例如专用限速的车辆驾驶许可相关。ECM 4可访问防护模块6,以确定当控制引擎31时,它可能不得不应用哪个限速。

[0036] 当另一装置意欲访问防护模块6的内容时,防护模块6可充当从装置,或者当防护模块6从另一装置恢复数据时,防护模块6可充当主装置。

[0037] 接口翻译器8可固定到车辆框架(frame)上的非常隐蔽的地点处,以使得欺诈用户难以访问它。接口翻译器8可例如密封(seal)到车辆框架上。接口翻译器可放置(host)在车辆前座之间,并可通过专用阀门(trap)访问。该接口翻译器的欺诈性改变或去除尝试应该是困难的、漫长的并且可容易检测到的(如果可能的话),如果使用不兼容的工具用于这样的尝试的话。该防护模块6被设计为匹配机动车约束,例如在扬尘或潮湿环境下的工作温度、生活周期或工作能力。

[0038] 图3示意性图示了防护模块6的第二实施例。该实施例与第一实施例的不同之处在于,从智能卡接口翻译器8中剥夺通信管理模块82,并且智能卡65被配置为自己管理通信接口81和83。

[0039] 在该实施例中,使用特定芯片62。特定芯片62通过连接器85连接到通信接口81。特定芯片62提供与所述通信接口81连接的两个输入/输出接口。

[0040] 图4示意性图示了防护模块6的第三实施例。防护模块6包括用作防护元件的微控制器9(例如QNF格式)和接口翻译器8。微控制器9被焊接在接口翻译器8的连接槽85中。微控制器9包括例如属于第一通信接口95的衬垫和属于第二通信接口85的衬垫。这些衬垫被焊接到连接槽85。

[0041] 微控制器9按照本身已知的方式包括芯片92。芯片92包括安全性管理模块93和持久数据存储区域94。安全性管理模块93和持久数据存储区域94可与安全性管理模块63和持久数据存储区域64相同。

[0042] 接口翻译器8包括与CAN总线2连接的通信接口81。接口翻译器8有利地包括无线通信接口83。微控制器9被配置为自己管理通信接口81和83。接口翻译器8进一步包括电力变压器84。电力变压器84通过车辆1的电网连接到电池7。

[0043] 当另一装置意欲访问防护模块6的内容时,防护模块6可充当从装置,或者当防护模块6从另一装置恢复数据时,防护模块6可充当主装置。接口翻译器8可固定到车辆框架上的非常隐蔽的地点处,以使得欺诈用户难以访问它。

[0044] 尽管公开的两个实施例都包括可移除地插入到连接槽中的智能卡,但是本发明也应用到以下的防护元件,其中将安全性管理电路焊接到防护元件电路的剩余部分。

[0045] 尽管参考CAN总线公开了实施例,但是可使用其他类型多路复用的通信总线来执行本发明,诸如在名称Flexray下已知的总线。

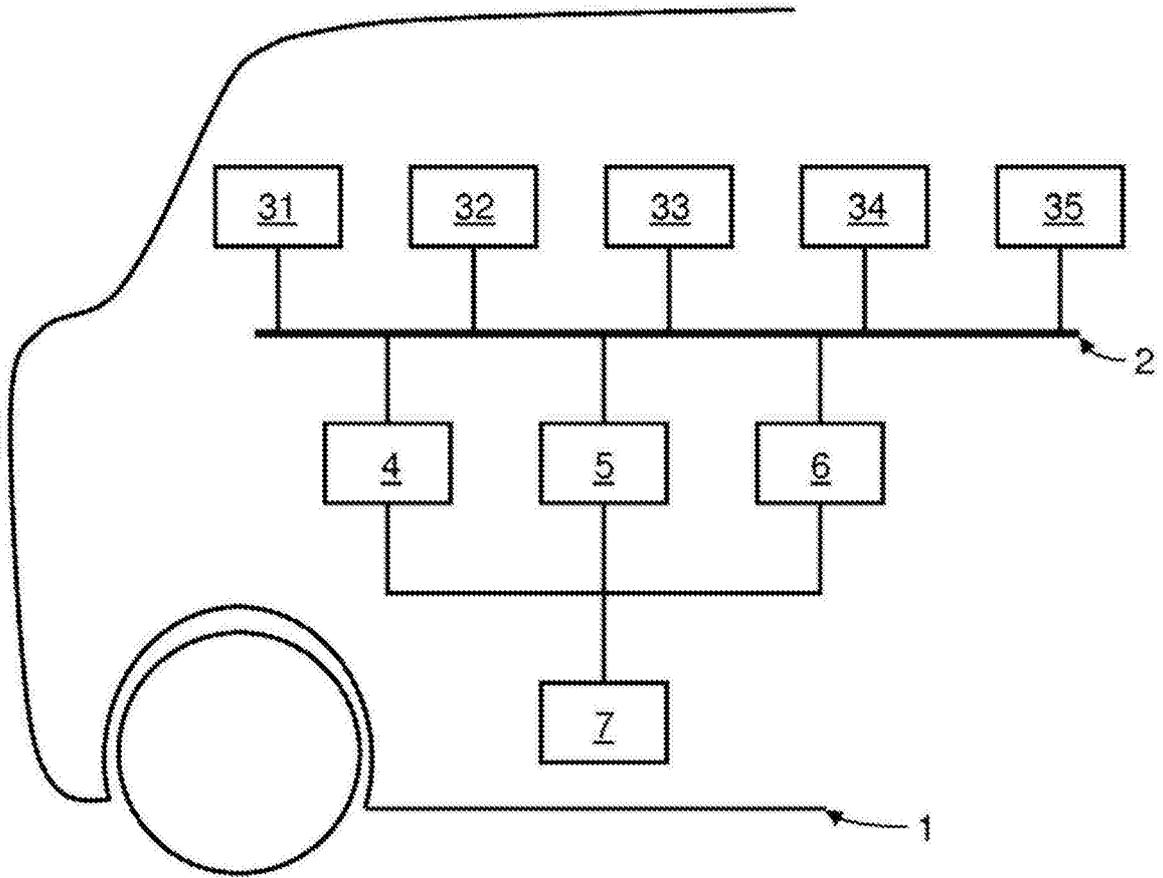


图1

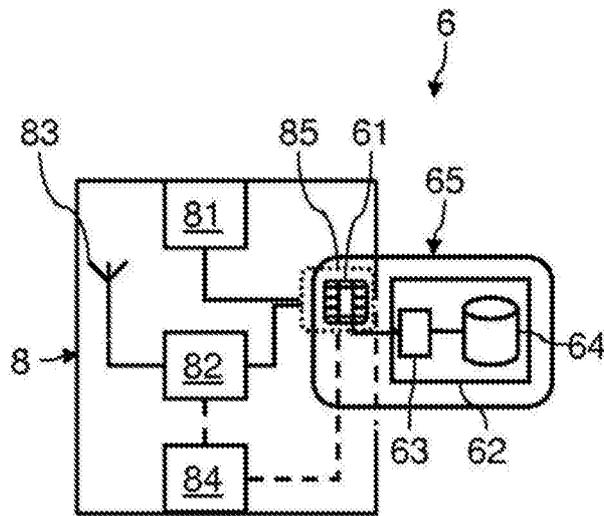


图2

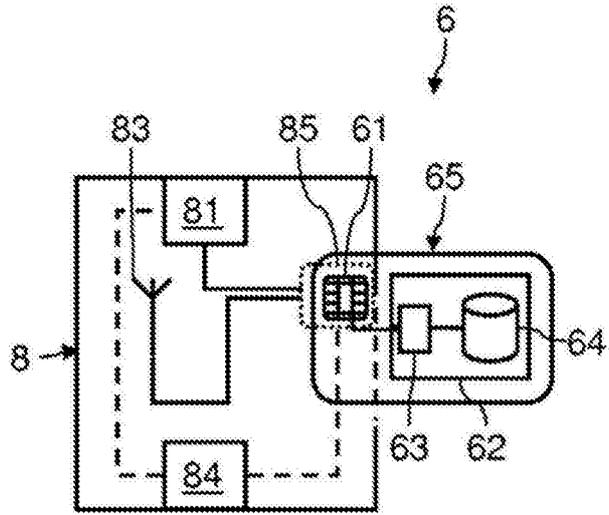


图3

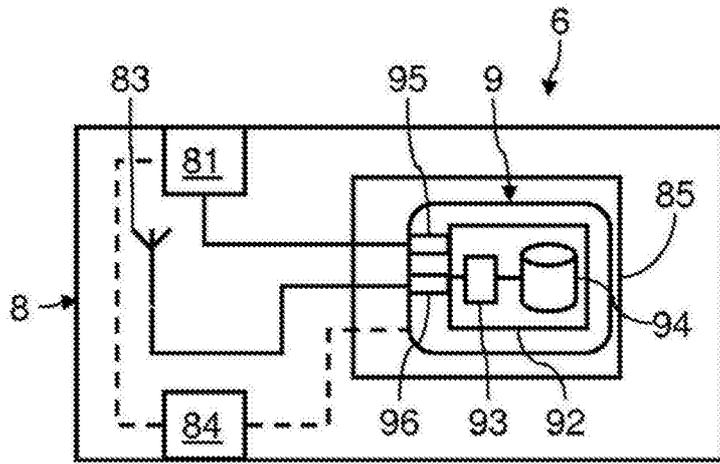


图4