(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102393888 B
(45)授权公告日 2015.04.22

(21)申请号 201110204515.X
(22)申请日 2011.07.21
(73)专利权人 广州汽车集团股份有限公司
地址 510000 广东省广州市越秀区东风中路448-458号成悦大厦23楼
(72)发明人 黄丽芳 黄少堂 李济泰 黄向东 张斌
(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 郝传鑫 姚佳
(51)Int.Cl.
G06F 21/44(2013.01)

(56)对比文件
US 2006/0206899 A1,2006.09.14, 全文.
CN 101013406 A,2007.08.08, 全文.
CN 101276313 A,2008.10.01, 权利要求7、权利要求9.

审查员 王晓敏

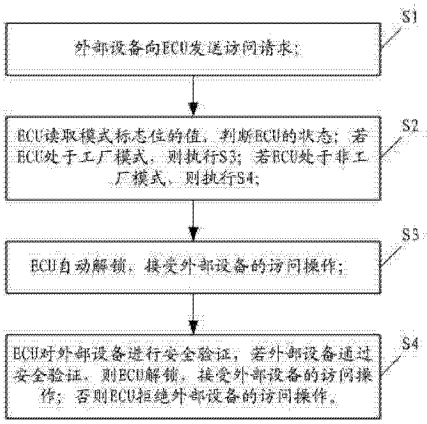
权利要求书1页 说明书3页 附图2页

(54)发明名称

ECU安全访问处理方法

(57)摘要

本发明公开了一种ECU安全访问处理方法，ECU在生产线上时被设置为工厂模式，ECU出厂时被设置为非工厂模式；在外部设备向ECU发送访问请求时，ECU读取模式标志位的值，判断ECU的状态；若ECU处于工厂模式，则ECU自动解锁，接受外部设备的访问操作；若ECU处于非工厂模式，则ECU对外部设备进行安全验证操作，当外部设备通过安全验证时，ECU解锁，接受外部设备的访问操作；否则ECU拒绝外部设备的访问操作。本发明实施例能够减少汽车在生产线上的检测步骤，提高生产效率，而且还能保证ECU的安全性。



CN 102393888 B

1. 一种 ECU 安全访问处理方法，其特征在于，包括：

S1、外部设备向 ECU 发送访问请求；

S2、ECU 读取模式标志位的值，判断 ECU 的状态；若 ECU 处于工厂模式，则执行 S3；若 ECU 处于非工厂模式，则执行 S4；

S3、ECU 自动解锁，接受外部设备的访问操作；

S4、ECU 对外部设备进行安全验证；若外部设备通过安全验证，则 ECU 解锁，接受外部设备的访问操作；否则 ECU 拒绝外部设备的访问操作；

所述 ECU 还配置有数据标识符，外部设备通过写数据流服务，设定所述数据标识符的参数值，使所述 ECU 在生产线上时被设置为工厂模式，使所述 ECU 出厂时被设置为非工厂模式。

2. 如权利要求 1 所述的 ECU 安全访问处理方法，其特征在于，在所述步骤 S2 中，ECU 读取模式标志位的值，若所述模式标志位的值为 1，则判定 ECU 处于工厂模式；若所述模式标志位的值为 0，则判定 ECU 处于非工厂模式。

3. 如权利要求 2 所述的 ECU 安全访问处理方法，其特征在于，

当所述数据标识符的参数值在 $00 ～ $0F 区段时，所述模式标志位的值为 1；

当所述数据标识符的参数值在 $10 ～ $FF 区段时，所述模式标志位的值为 0。

4. 如权利要求 3 所述的 ECU 安全访问处理方法，其特征在于，所述模式标志位、数据标识符均配置在所述 ECU 的内部存储器中。

5. 如权利要求 4 所述的 ECU 安全访问处理方法，其特征在于，外部设备通过写数据流服务设定所述数据标识符的参数值，使 ECU 处于工厂模式或非工厂模式。

6. 如权利要求 5 所述的 ECU 安全访问处理方法，其特征在于，外部设备通过写数据流服务将所述数据标识符的参数值写成 $00 后，所述数据标识符的参数值被锁定，不可修改。

7. 如权利要求 6 所述的 ECU 安全访问处理方法，其特征在于，外部设备通过写数据流服务，将生产线上的 ECU 设置为工厂模式，将出厂的 ECU 的数据标识符的参数值写成 $00。

ECU 安全访问处理方法

技术领域

[0001] 本发明涉及汽车电子技术领域，尤其涉及一种 ECU 安全访问处理方法。

背景技术

[0002] 随着汽车工业的发展，汽车诊断通讯系统的应用也越来越广泛：安全验证是诊断通讯系统应用中的一个典型例子。在常规车载诊断应用中，涉及安全的重要信息的写入、读取及其它一些特殊功能的实现，必须要经过安全验证服务进行解锁后才可操作。

[0003] 如图 1 所示，现有的安全验证流程如下：外部设备请求给车载 ECU（Electric Control Unit，电子控制单元）发送种子；ECU 将随机的种子返回给外部设备；外部设备收到种子后，按照一种安全验证算法，计算出一个密钥，并将该密钥发送给 ECU；ECU 将收到的密钥与内部计算出来的密钥进行对比，如果匹配，则安全验证通过，ECU 解锁，允许外部设备进行后续的相关操作；否则安全验证不通过，ECU 拒绝解锁。

[0004] 上述安全验证方法对 ECU 内部特殊功能起到一定的保护作用。但是，每次对 ECU 进行访问操作时，都需要通过繁琐的安全验证步骤进行解锁，工厂里的每套设备都需要集成 ECU 的安全算法。在汽车生产阶段，生产节拍要求很高。如果汽车在每个工位上进行下线检测前都要进行安全验证，重复地进行安全算法的计算，操作步骤繁琐，大大影响了生产效率。同时，主机厂需要将各个 ECU 的安全算法提供给各个生产设备供应商，使各个设备集成安全算法。由于多个厂家知悉这些安全算法，极其容易泄漏，保密性不高。

发明内容

[0005] 本发明提出一种 ECU 安全访问处理方法，能够减少汽车在生产线上的检测步骤，提高生产效率，而且还能保证 ECU 的安全性。

[0006] 本发明实施例提供的 ECU 安全访问处理方法，包括：

[0007] S1、外部设备向 ECU 发送访问请求；

[0008] S2、ECU 读取模式标志位的值，判断 ECU 的状态；若 ECU 处于工厂模式，则执行 S3；若 ECU 处于非工厂模式，则执行 S4；

[0009] S3、ECU 自动解锁，接受外部设备的访问操作；

[0010] S4、ECU 对外部设备进行安全验证；若外部设备通过安全验证，则 ECU 解锁，接受外部设备的访问操作；否则 ECU 拒绝外部设备的访问操作；

[0011] 所述 ECU 还配置有数据标识符，外部设备通过写数据流服务，设定所述数据标识符的参数值，使所述 ECU 在生产线上时被设置为工厂模式，使所述 ECU 出厂时被设置为非工厂模式。

[0012] 其中，在所述步骤 S2 中，ECU 读取模式标志位的值，若所述模式标志位的值为 1，则判定 ECU 处于工厂模式；若所述模式标志位的值为 0，则判定 ECU 处于非工厂模式。

[0013] 进一步的，所述 ECU 还配置有数据标识符；当所述数据标识符的参数值在 $00 ～ $0F 区段时，所述模式标志位的值为 1；当所述数据标识符的参数值在 $10 ～ $FF 区段时，所

述模式标志位的值为0。

[0014] 外部设备通过写数据流服务，将生产线上的ECU设置为工厂模式。

[0015] 外部设备通过写数据流服务，将出厂的ECU的数据标识符的参数值写成$00，该ECU被设置为非工厂模式，且所述数据标识符的参数值被锁定，不可修改。

[0016] 本发明实施例提供的ECU安全访问处理方法，将生产线上的ECU设置为工厂模式，外部设备与ECU之间不用安全验证即可进行所有访问操作，步骤简单，从而避免了安全算法的繁琐计算，缩短操作时间，大大提高生产效率。同时，各个ECU的安全算法不用释放给各个设备生产厂商，减少了安全算法泄密的可能性；生产线上的ECU的访问操作，都是由专业技术人员通过专用设备在固定的工位进行的，即使不用安全验证，直接进行操作也不会造成任何影响。整车出厂后，ECU被设定为非工厂模式，外部设备对ECU的所有访问操作都需要通过安全验证后才能进行，提高ECU的安全性。

附图说明

[0017] 图1是现有技术的EUC安全验证流程示意图；

[0018] 图2是本发明实施一提供的ECU安全访问处理方法的流程示意图；

[0019] 图3是本发明实施二提供的生产线上的ECU的检测流程图。

具体实施方式

[0020] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。

[0021] 参见图2，是本发明实施一提供的ECU安全访问处理方法的流程示意图。

[0022] 本发明实施例将ECU样件划分为工厂模式和非工厂模式：ECU在生产线上时被设置为工厂模式，ECU出厂时被设置为非工厂模式。工厂模式下的ECU不需要安全验证即可接受外部设备的访问操作；非工厂模式下的ECU必须通过安全验证后才接受外部设备的访问操作。

[0023] 需要说明的是，“ECU在生产线上”既包括单个ECU部件在生产线上的情况，也包括ECU被安装在汽车上，汽车在主机厂生产线上的情况。“ECU出厂”既包括单个ECU部件出厂的情况，也包括ECU被安装在汽车上，汽车出厂的情况。

[0024] 如图2所示，本实施例提供的ECU安全访问处理方法，包括以下步骤：

[0025] S1、外部设备向ECU发送访问请求；

[0026] S2、ECU读取模式标志位的值，判断ECU的状态；若ECU处于工厂模式，则执行S3；若ECU处于非工厂模式，则执行S4；

[0027] S3、ECU自动解锁，接受外部设备的访问操作；

[0028] S4、ECU对外部设备进行安全验证，若外部设备通过安全验证，则ECU解锁，接受外部设备的访问操作；否则ECU拒绝外部设备的访问操作。

[0029] 具体的，外部设备对ECU的访问操作包括在线配置、防盗匹配、遥控钥匙学习、零位标定、排气加注等操作。

[0030] 其中，在步骤S2中，ECU读取模式标志位的值，若模式标志位的值为1，则判定ECU处于工厂模式；若模式标志位的值为0，则判定ECU处于非工厂模式。

[0031] 进一步的，ECU 还配置有数据标识符；当数据标识符的参数值在 $00 ～ $0F 区段时(即数据标识符取 $00 ～ $0F 区段中的任一个值)，模式标志位的值为 1，ECU 处于工厂模式；当数据标识符的参数值在 $10 ～ $FF 区段时(即数据标识符取 $10 ～ $FF 区段中的任一个值)，模式标志位的值为 0，ECU 处于非工厂模式。

[0032] 优选的，所述模式标志位、数据标识符均配置在 ECU 的内部存储器(例如 EEPROM)中。外部设备通过写数据流服务，设定所述数据标识符的参数值，使 ECU 处于工厂模式或非工厂模式。而且，当外部设备通过写数据流服务将数据标识符的参数值写成 $00 后，数据标识符的参数值被锁定，不可修改。

[0033] 需要说明的是，本发明实施例仅为数据标识符的参数值取 16 位的 $00 ～ $FF 为例进行说明，数据标识符的参数值还可以使用其他数值。同理，数据标识符被锁定时的参数值除了 $00 外，还可以使用其他的数值。而且模式标志位除了取 0、1 外，也可以取其他的数值。

[0034] 在具体实施当中，外部设备通过写数据流服务，将生产线上的 ECU 设置为工厂模式。在工厂生产阶段，外部设备对 ECU 的所有的访问操作都省去安全验证步骤，从而避免了安全算法的繁琐计算，提高生产效率。同时，由于生产线上的对 ECU 进行访问操作的外部设备不需要集成安全算法，因此主机厂不用将安全算法发给各个设备生产厂商，大大减少了安全算法泄密的可能性。

[0035] ECU 出厂时，外部设备通过写数据流服务，将出厂的 ECU 的数据标识符的参数值写成 $00，该 ECU 被设置为非工厂模式，且该参数值被锁定，不可以再修改。ECU 出厂之后，外部设备对 ECU 的所有访问操作都要通过安全验证后才能进行，从而保证了 ECU 的安全性。例如，汽车整车出厂后，车载 ECU 被设定为非工厂模式，所有的对车载 ECU 的特殊诊断操作都需要 4S 店的专用诊断仪通过安全验证后才可进行。

[0036] 参见图 3，是本发明实施二提供的生产线上的 ECU 的检测流程图。

[0037] ECU 零部件供应商向主机厂供货时，将 ECU 设置为工厂模式。在主机厂生产线上，ECU 被安装在汽车上。在汽车下线检测过程中，从检测线起始点到终检点，ECU 一直处于工厂模式，专用的下线检测设备可以跳过安全验证步骤直接对 ECU 进行钥匙学习、零位标定等操作，减少了操作步骤，提高了生产效率。在整车出厂时，ECU 被锁定为非工厂模式。

[0038] 本发明实施例提供的 ECU 安全访问处理方法，将生产线上的 ECU 设置为工厂模式，外部设备与 ECU 之间不用安全验证即可进行所有访问操作，步骤简单，从而避免了安全算法的繁琐计算，缩短操作时间，大大提高生产效率。同时，各个 ECU 的安全算法不用释放给各个设备生产厂商，减少了安全算法泄密的可能性；生产线上的 ECU 的访问操作，都是由专业技术人员通过专用设备在固定的工位进行的，即使不用安全验证，直接进行操作也不会造成任何影响。整车出厂后，ECU 被设定为非工厂模式，外部设备对 ECU 的所有访问操作都需要通过安全验证后才能进行，提高 ECU 的安全性。

[0039] 以上所述是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明的保护范围。

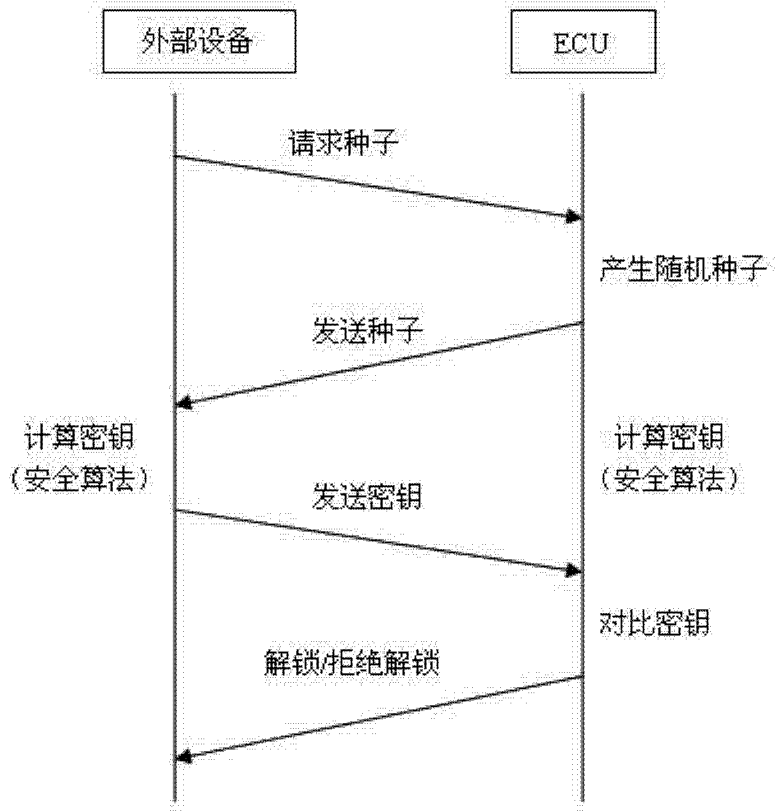

外部设备
ECU
请求种子
产生随机种子
发送种子
计算密钥
（安全算法）
计算密钥
（安全算法）
发送密钥
对比密钥
解锁/拒绝解锁

图 1

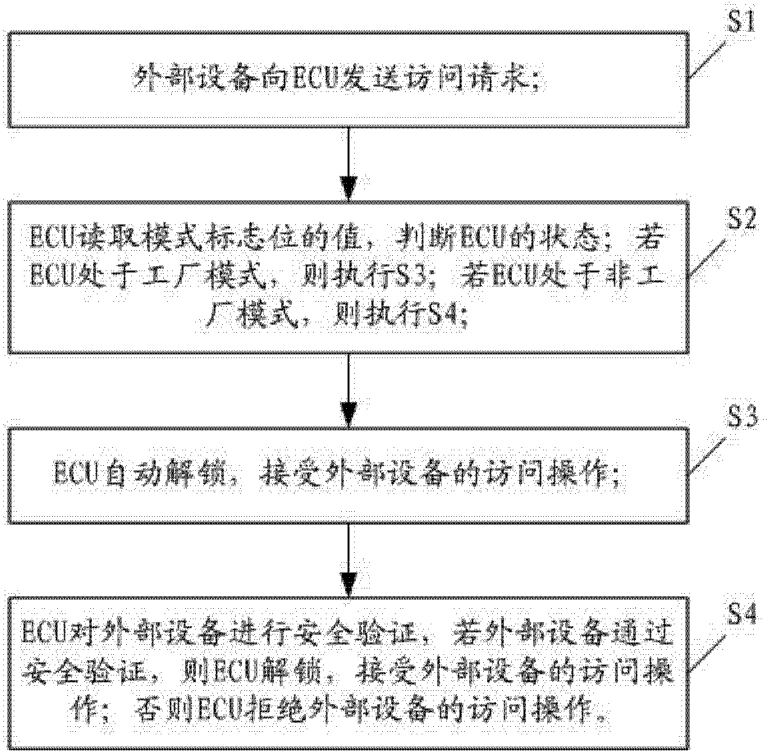

S1
外部设备向ECU发送访问请求；
S2
ECU读取模式标志位的值，判断ECU的状态；若ECU处于工厂模式，则执行S3；若ECU处于非工厂模式，则执行S4；
S3
ECU自动解锁，接受外部设备的访问操作；
S4
ECU对外部设备进行安全验证，若外部设备通过安全验证，则ECU解锁，接受外部设备的访问操作；否则ECU拒绝外部设备的访问操作。

图 2

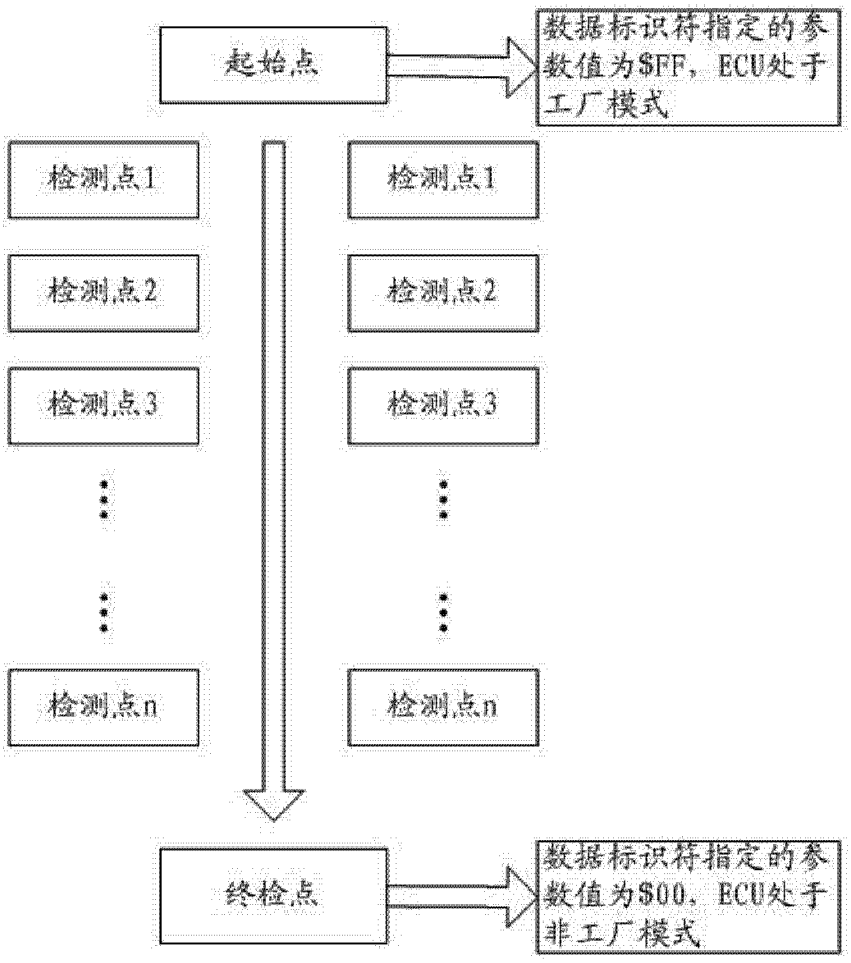

起始点
数据标识符指定的参数值为$FF，ECU处于工厂模式
检测点1
检测点2
检测点3
检测点n
检测点1
检测点2
检测点3
检测点n
终检点
数据标识符指定的参数值为$00，ECU处于非工厂模式

图 3