



(12) 发明专利申请

(10) 申请公布号 CN 105468385 A

(43) 申请公布日 2016. 04. 06

(21) 申请号 201410429601. 4

(22) 申请日 2014. 08. 27

(71) 申请人 比亚迪股份有限公司

地址 518118 广东省深圳市坪山新区比亚迪
路 3009 号

(72) 发明人 张爽 高爱莲

(74) 专利代理机构 北京清亦华知识产权代理事
务所(普通合伙) 11201

代理人 张大威

(51) Int. Cl.

G06F 9/445(2006. 01)

G06F 17/30(2006. 01)

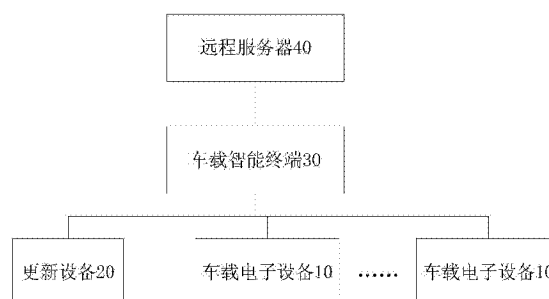
权利要求书2页 说明书6页 附图2页

(54) 发明名称

车载电子设备软件的更新系统和方法

(57) 摘要

本发明公开了一种车载电子设备软件的更新系统和方法。所述系统包括：车载智能终端，用于当更新设备连接至车辆的诊断接口时，获取更新设备的标识码，并将更新设备的标识码发送至远程服务器，接收远程服务器发送的判断结果，当判断结果为合法时，生成第一控制指令，并将第一控制指令发送至更新设备，当判断结果为不合法时，生成第二控制指令，并将第二控制指令发送至更新设备；远程服务器，用于判断更新设备的标识码是否合法，并将判断结果发送至车载智能终端；更新设备，用于根据第一控制指令对至少一个车载电子设备的软件进行更新，或根据第二控制指令停止工作。本发明实施例的系统，可防止用户私自使用不合法的更新设备，保障行车安全。



1. 一种车载电子设备软件的更新系统,其特征在于,包括:至少一个车载电子设备、更新设备、车载智能终端和远程服务器,其中,

所述车载智能终端,用于当所述更新设备连接至车辆的诊断接口时,获取所述更新设备的标识码,并将所述更新设备的标识码发送至所述远程服务器,以及接收所述远程服务器发送的判断结果,当所述判断结果为合法时,生成第一控制指令,并将所述第一控制指令发送至所述更新设备,当所述判断结果为不合法时,生成第二控制指令,并将所述第二控制指令发送至所述更新设备;

所述远程服务器,用于判断所述更新设备的标识码是否合法,并将所述判断结果发送至所述车载智能终端;

所述更新设备,用于根据所述第一控制指令对所述至少一个车载电子设备的软件进行更新,或根据所述第二控制指令停止工作。

2. 如权利要求1所述的车载电子设备软件的更新系统,其特征在于,还包括:

厂家输入终端,用于为所生产的每个更新设备分配标识码,并将所述每个更新设备的标识码发送至所述远程服务器,以使所述远程服务器将所述每个更新设备的标识码存储在标识码数据库中。

3. 如权利要求2所述的车载电子设备软件的更新系统,其特征在于,所述远程服务器,具体用于:

判断所述更新设备的标识码是否存在于所述标识码数据库中;

如果是,则判断所述更新设备的标识码合法;

如果否,则判断所述更新设备的标识码不合法。

4. 如权利要求1所述的车载电子设备软件的更新系统,其特征在于,所述车载智能终端,还用于:

当所述判断结果为不合法时,生成提示信息,以对用户进行提示。

5. 如权利要求1所述的车载电子设备软件的更新系统,其特征在于,其中,所述至少一个车载电子设备、所述更新设备和所述车载智能终端都与车辆的CAN总线相连,所述车载智能终端和所述远程服务器通过3G或4G网络建立通信连接。

6. 一种车载电子设备软件的更新方法,其特征在于,包括以下步骤:

当更新设备连接至车辆的诊断接口时,车载智能终端获取所述更新设备的标识码,并将所述更新设备的标识码发送至远程服务器;

所述远程服务器判断所述更新设备的标识码是否合法,并将判断结果发送至所述车载智能终端;

当所述判断结果为合法时,所述车载智能终端生成第一控制指令,并将所述第一控制指令发送至所述更新设备,以使所述更新设备根据所述第一控制指令对车载电子设备的软件进行更新;以及

当所述判断结果为不合法时,所述车载智能终端生成第二控制指令,并将所述第二控制指令发送至所述更新设备,以使所述更新设备根据所述第二控制指令停止工作。

7. 如权利要求6所述的车载电子设备软件的更新方法,其特征在于,还包括:

生产厂家为所生产的每个更新设备分配标识码,并将所述每个更新设备的标识码发送至所述远程服务器;

所述远程服务器将所述每个更新设备的标识码存储在标识码数据库中。

8. 如权利要求 7 所述的车载电子设备软件的更新方法,其特征在于,所述远程服务器判断所述更新设备的标识码是否合法,具体包括:

判断所述更新设备的标识码是否存在于所述标识码数据库中;

如果是,则判断所述更新设备的标识码合法;

如果否,则判断所述更新设备的标识码不合法。

9. 如权利要求 6 所述的车载电子设备软件的更新方法,其特征在于,还包括:

当所述判断结果为不合法时,所述车载智能终端生成提示信息,以对用户进行提示。

10. 如权利要求 6 所述的车载电子设备软件的更新方法,其特征在于,其中,所述车载电子设备、所述更新设备和所述车载智能终端都与车辆的 CAN 总线相连,所述车载智能终端和所述远程服务器通过 3G 或 4G 网络建立通信连接。

车载电子设备软件的更新系统和方法

技术领域

[0001] 本发明涉及车辆技术领域,尤其涉及一种车载电子设备软件的更新系统和方法。

背景技术

[0002] 随着汽车电子的发展,人们越来越能感受到汽车电子智能化所带来的行车乐趣。由于电子产品都会面临更新换代的问题,所以,有的用户会私自对车载电子设备的软件进行更新。这种做法容易引起车身故障并且对用户本身的用车安全造成影响,可能还会引起用户和汽车生产厂家之间的纠纷。

发明内容

[0003] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。为此,本发明的一个目的在于提出一种车载电子设备软件的更新系统,该系统可以防止用户私自使用不合法的更新设备更新车载电子设备的软件,提高了车载电子设备软件更新的安全性,从而给用户的行车安全带来了保障。

[0004] 本发明的第二个目的在于提出一种车载电子设备软件的更新方法。

[0005] 为了实现上述目的,本发明第一方面实施例的车载电子设备软件的更新系统,包括:至少一个车载电子设备、更新设备、车载智能终端和远程服务器,其中,所述车载智能终端,用于当所述更新设备连接至车辆的诊断接口时,获取所述更新设备的标识码,并将所述更新设备的标识码发送至所述远程服务器,以及接收所述远程服务器发送的判断结果,当所述判断结果为合法时,生成第一控制指令,并将所述第一控制指令发送至所述更新设备,当所述判断结果为不合法时,生成第二控制指令,并将所述第二控制指令发送至所述更新设备;所述远程服务器,用于判断所述更新设备的标识码是否合法,并将所述判断结果发送至所述车载智能终端;所述更新设备,用于根据所述第一控制指令对所述至少一个车载电子设备的软件进行更新,或根据所述第二控制指令停止工作。

[0006] 根据本发明实施例的车载电子设备软件的更新系统,当更新设备连接至车辆的诊断接口时,车载智能终端读取更新设备的标识码,并将更新设备的标识码发送至远程服务器,远程服务器判断更新设备的标识码是否合法,如果合法,车载智能终端则允许更新设备对车载电子设备的软件进行更新,如果不合法,车载智能终端则会阻止更新设备的正常运行,该系统结构简单、操作简单,可以防止用户私自使用不合法的更新设备更新车载电子设备的软件,提高了车载电子设备软件更新的安全性,从而给用户的行车安全带来了保障。

[0007] 为了实现上述目的,本发明第二方面实施例的车载电子设备软件的更新方法,包括以下步骤:当更新设备连接至车辆的诊断接口时,车载智能终端获取所述更新设备的标识码,并将所述更新设备的标识码发送至远程服务器;所述远程服务器判断所述更新设备的标识码是否合法,并将判断结果发送至所述车载智能终端;当所述判断结果为合法时,所述车载智能终端生成第一控制指令,并将所述第一控制指令发送至所述更新设备,以使所述更新设备根据所述第一控制指令对车载电子设备的软件进行更新;以及当所述判断结果

为不合法时,所述车载智能终端生成第二控制指令,并将所述第二控制指令发送至所述更新设备,以使所述更新设备根据所述第二控制指令停止工作。

[0008] 根据本发明实施例的车载电子设备软件的更新方法,当更新设备连接至车辆的诊断接口时,车载智能终端读取更新设备的标识码,并将更新设备的标识码发送至远程服务器,远程服务器判断更新设备的标识码是否合法,如果合法,车载智能终端则允许更新设备对车载电子设备软件进行更新,如果不合法,车载智能终端则会阻止更新设备的正常运行,该方法可以防止用户私自使用不合法的更新设备更新车载电子设备软件,提高了车载电子设备软件更新的安全性,从而给用户的行车安全带来了保障。

附图说明

[0009] 图 1 是根据本发明一个实施例的车载电子设备软件的更新系统的结构示意图;

[0010] 图 2 是根据本发明一个实施例的车载电子设备软件的更新系统的结构示意图;

[0011] 图 3 是根据本发明另一个实施例的车载电子设备软件的更新系统的结构示意图;

[0012] 图 4 是根据本发明一个实施例的车载电子设备软件的更新方法的流程图。

具体实施方式

[0013] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0014] 图 1 是根据本发明一个实施例的车载电子设备软件的更新系统的结构示意图。如图 1 所示,本发明实施例的车载电子设备软件的更新系统,包括:至少一个车载电子设备 10、更新设备 20、车载智能终端 30 和远程服务器 40。

[0015] 其中,车载智能终端 30 用于当更新设备 20 连接至车辆的诊断接口时,获取更新设备 20 的标识码,并将更新设备 20 的标识码发送至远程服务器 40,以及接收远程服务器 40 发送的判断结果,当判断结果为合法时,生成第一控制指令,并将第一控制指令发送至更新设备 20,当判断结果为不合法时,生成第二控制指令,并将第二控制指令发送至更新设备 20。

[0016] 在本发明的一个实施例中,至少一个车载电子设备 10、更新设备 20 和车载智能终端 30 都与车辆的 CAN(Controller Area Network,控制器局域网)总线相连,车载智能终端 30 和远程服务器 40 通过 3G 或 4G 网络建立通信连接。

[0017] 具体地,当用户想要更新车载电子设备 10 的软件时,首先将更新设备 20 连接到车辆的诊断接口,此时,更新设备 20 便连接到了车辆的 CAN 总线上,如图 2 所示,由于更新设备 20 在出厂时被写入了标识码,所以,车载智能终端 30 可以通过 CAN 总线读取更新设备 20 的标识码,并将更新设备 20 的标识码发送至远程服务器 40。

[0018] 更具体地,车载智能终端 30 还用于接收远程服务器 40 发送的判断结果,当判断结果为合法时,生成第一控制指令,并将第一控制指令发送至更新设备 20,当判断结果为不合法时,生成第二控制指令,并将第二控制指令发送至更新设备 20。

[0019] 远程服务器 40 用于判断更新设备 20 的标识码是否合法,并将判断结果发送至车载智能终端 30。

[0020] 具体地,远程服务器 40 接收到更新设备 20 的标识码之后,判断更新设备 20 是否为合法设备,例如,远程服务器 40 在标识码数据库中查找更新设备 20 的标识码是否存在,如果存在,则说明更新设备 20 是合法设备,如果不存在,则说明更新设备 20 为非法设备。其中,在更新设备出厂时,更新设备的生产厂家会将每个更新设备对应的标识码存储在远程服务器 40 中的标识码数据库中,具体的存储过程将在后面的实施例中进行详细说明。

[0021] 更新设备 20 用于根据第一控制指令对至少一个车载电子设备 10 的软件进行更新,或根据第二控制指令停止工作。

[0022] 具体地,当判断结果为合法时,车载智能终端 30 允许更新设备 20 对至少一个车载电子设备 10 的软件进行更新;当判断结果为不合法时,车载智能终端 30 会阻止更新设备 20 的正常运行,更新设备 20 则不能对车载电子设备 10 的软件进行更新。所以,当用户私自使用不合法的更新设备时,无法实现对车载电子设备 10 的软件的更新,必须去正规的汽车服务店,使用合法的更新设备去更新车载电子设备的软件,从而使车载电子设备的软件升级得到了安全保障。

[0023] 本发明实施例的车载电子设备软件的更新系统,当更新设备连接至车辆的诊断接口时,车载智能终端读取更新设备的标识码,并将更新设备的标识码发送至远程服务器,远程服务器判断更新设备的标识码是否合法,如果合法,车载智能终端则允许更新设备对车载电子设备的软件进行更新,如果不合法,车载智能终端则会阻止更新设备的正常运行,该系统结构简单、操作简单,可以防止用户私自使用不合法的更新设备更新车载电子设备的软件,提高了车载电子设备软件更新的安全性,从而给用户的行车安全带来了保障。

[0024] 在本发明的一个实施例中,车载智能终端 30 还用于:当判断结果为不合法时,生成提示信息,以对用户进行提示。

[0025] 具体地,当判断结果为不合法时,车载智能终端 30 生成提示信息以对用户进行提示。例如,可以通过车辆中的多媒体屏幕显示“当前更新设备为非法设备,为了行车安全,请不要随意更新车载电子设备”。

[0026] 在本发明的一个实施例中,如图 3 所示,车载电子设备软件的更新系统,还包括:厂家输入终端 50。

[0027] 厂家输入终端 50 用于为所生产的每个更新设备分配标识码,并将每个更新设备的标识码发送至远程服务器 40,以使远程服务器 40 将每个更新设备的标识码存储在标识码数据库中。

[0028] 具体地,在更新设备出厂时,厂家输入终端 50 会为每个更新设备分配标识码,并把标识码写入到对应的更新设备中,厂家输入终端 50 还将每个更新设备的标识码发送至远程服务器 40,以使远程服务器 40 将每个更新设备的标识码存储在标识码数据库中。例如,厂家输入终端 50 可以为电脑或者其他终端设备,厂家输入终端 50 中安装有更新设备标识码输入系统,用于将每个更新设备的标识码发送至远程服务器 40 中。

[0029] 在本发明的一个实施例中,远程服务器 40 具体用于:判断更新设备 20 的标识码是否存在于标识码数据库中;如果是,则判断更新设备 20 的标识码合法;如果否,则判断更新设备 20 的标识码不合法。

[0030] 具体地,远程服务器 40 判断更新设备 20 的标识码是否合法,具体为:远程服务器 40 接收到更新设备 20 的标识码后,查找更新设备 20 的标识码是否存在于标识码数据库中,

如果存在,则说明更新设备 20 是正规厂家生产的合法设备,如果不存在,则说明更新设备 20 是非法设备。

[0031] 为了实现上述实施例,本发明还提出了一种车载电子设备软件的更新方法。

[0032] 图 4 是根据本发明一个实施例的车载电子设备软件的更新方法的流程图。如图 4 所示,本发明实施例的车载电子设备软件的更新方法,包括以下步骤:

[0033] S101,当更新设备连接至车辆的诊断接口时,车载智能终端获取更新设备的标识码,并将更新设备的标识码发送至远程服务器。

[0034] 在本发明的一个实施例中,车载电子设备、更新设备和车载智能终端都与车辆的 CAN 总线相连,车载智能终端和远程服务器通过 3G 或 4G 网络建立通信连接。

[0035] 具体地,当用户想要更新车载电子设备的软件时,首先将更新设备连接到车辆的诊断接口,此时,更新设备便连接到了车辆的 CAN 总线上,由于更新设备在出厂时被写入了标识码,所以,车载智能终端可以通过 CAN 总线读取更新设备的标识码,并将更新设备的标识码发送至远程服务器。

[0036] S102,远程服务器判断更新设备的标识码是否合法,并将判断结果发送至车载智能终端。

[0037] 具体地,远程服务器接收到更新设备的标识码之后,判断更新设备是否为合法设备,例如,远程服务器在标识码数据库中查找更新设备的标识码是否存在,如果存在,则说明更新设备是合法设备,如果不存在,则说明更新设备为非法设备。其中,在更新设备出厂时,更新设备的生产厂家会将每个更新设备对应的标识码存储在远程服务器中的标识码数据库中,具体的存储过程将在后面的实施例中进行详细说明。

[0038] S103,当判断结果为合法时,车载智能终端生成第一控制指令,并将第一控制指令发送至更新设备,以使更新设备根据第一控制指令对车载电子设备的软件进行更新。

[0039] 具体地,车载智能终端接收远程服务器发送的判断结果,当判断结果为合法时,车载智能终端生成第一控制指令,并将第一控制指令发送至更新设备,即车载智能终端允许更新设备对车载电子设备的软件进行更新。

[0040] S104,当判断结果为不合法时,车载智能终端生成第二控制指令,并将第二控制指令发送至更新设备,以使更新设备根据第二控制指令停止工作。

[0041] 具体地,当判断结果为不合法时,车载智能终端生成第二控制指令,并将第二控制指令发送至更新设备,即车载智能终端会阻止更新设备的正常运行,更新设备则不能对车载电子设备的软件进行更新。

[0042] 所以,当用户私自使用不合法的更新设备时,无法实现对车载电子设备的软件的更新,必须去正规的汽车服务店,使用合法的更新设备去更新车载电子设备的软件,从而使车载电子设备的软件升级得到了安全保障。

[0043] 本发明实施例的车载电子设备软件的更新方法,当更新设备连接至车辆的诊断接口时,车载智能终端读取更新设备的标识码,并将更新设备的标识码发送至远程服务器,远程服务器判断更新设备的标识码是否合法,如果合法,车载智能终端则允许更新设备对车载电子设备的软件进行更新,如果不合法,车载智能终端则会阻止更新设备的正常运行,该方法可以防止用户私自使用不合法的更新设备更新车载电子设备的软件,提高了车载电子设备软件更新的安全性,从而给用户的行车安全带来了保障。

[0044] 在本发明的一个实施例中,车载电子设备软件的更新方法,还包括:当判断结果为不合法时,车载智能终端生成提示信息,以对用户进行提示。

[0045] 具体地,当判断结果为不合法时,车载智能终端生成提示信息以对用户进行提示。例如,可以通过车辆中的多媒体屏幕显示“当前更新设备为非法设备,为了行车安全,请不要随意更新车载电子设备”。

[0046] 在本发明的一个实施例中,车载电子设备软件的更新方法,还包括:生产厂家为所生产的每个更新设备分配标识码,并将每个更新设备的标识码发送至远程服务器;远程服务器将每个更新设备的标识码存储在标识码数据库中。

[0047] 具体地,在更新设备出厂时,生产厂家通过厂家输入终端为每个更新设备分配标识码,并把标识码写入到对应的更新设备中,以及通过厂家输入终端将每个更新设备的标识码发送至远程服务器,以使远程服务器将每个更新设备的标识码存储在标识码数据库中。其中,厂家输入终端可以为电脑或者其他终端设备,厂家输入终端中安装有更新设备标识码输入系统,用于将每个更新设备的标识码发送至远程服务器中。

[0048] 在本发明的一个实施例中,远程服务器判断更新设备的标识码是否合法,具体包括:判断更新设备的标识码是否存在于标识码数据库中;如果是,则判断更新设备的标识码合法;如果否,则判断更新设备的标识码不合法。

[0049] 具体地,远程服务器接收到更新设备的标识码后,查找更新设备的标识码是否存在于标识码数据库中,如果存在,则说明更新设备是正规厂家生产的合法设备,如果不存在,则说明更新设备是非法设备。

[0050] 在本发明的描述中,需要理解的是,术语“中心”、“纵向”、“横向”、“长度”、“宽度”、“厚度”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”“内”、“外”、“顺时针”、“逆时针”、“轴向”、“径向”、“周向”等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。

[0051] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0052] 在本发明中,除非另有明确的规定和限定,术语“安装”、“相连”、“连接”、“固定”等术语应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或成一体;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通或两个元件的相互作用关系,除非另有明确的限定。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本发明中的具体含义。

[0053] 在本发明中,除非另有明确的规定和限定,第一特征在第二特征“上”或“下”可以是第一和第二特征直接接触,或第一和第二特征通过中间媒介间接接触。而且,第一特征在第二特征“之上”、“上方”和“上面”可是第一特征在第二特征正上方或斜上方,或仅仅表示第一特征水平高度高于第二特征。第一特征在第二特征“之下”、“下方”和“下面”可以是第一特征在第二特征正下方或斜下方,或仅仅表示第一特征水平高度小于第二特征。

[0054] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示

例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0055] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

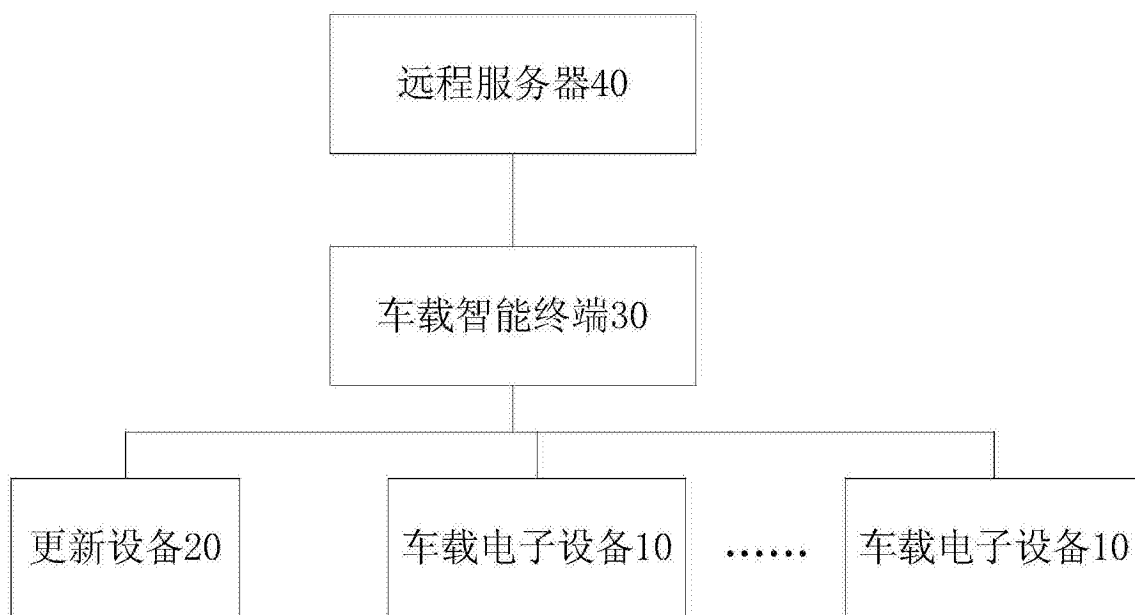


图 1

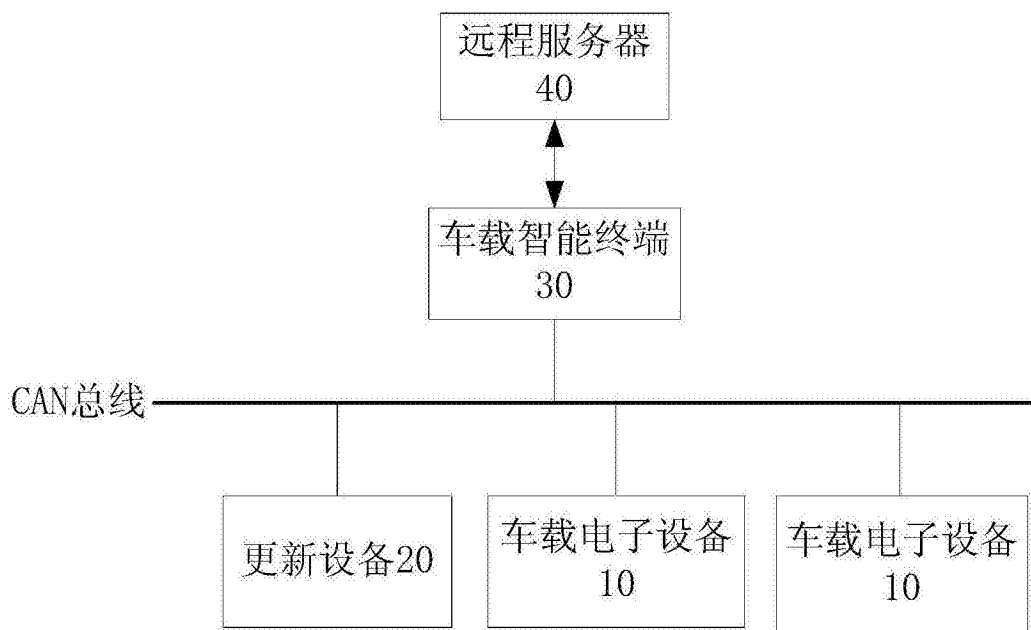


图 2

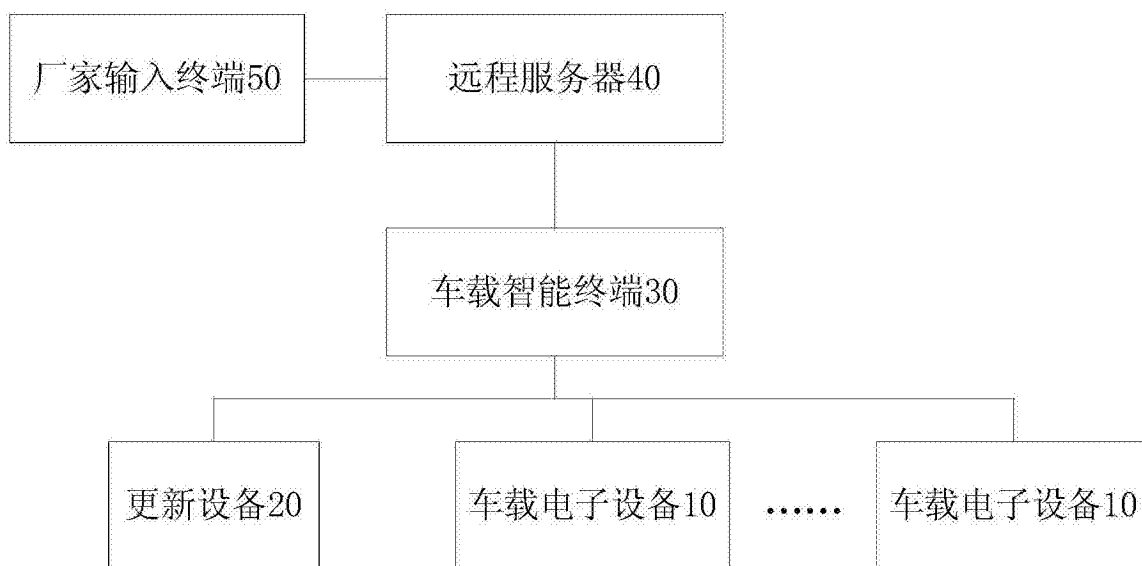


图 3

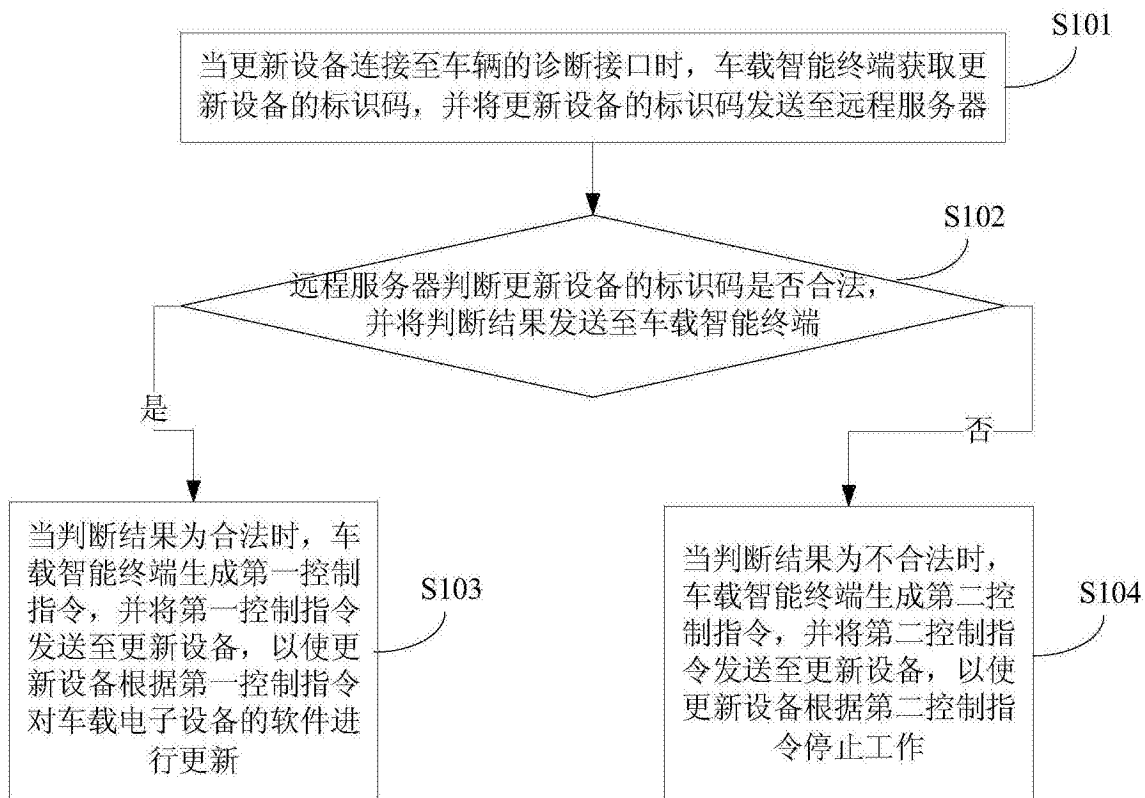


图 4