(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112567338 B
(45)授权公告日 2024.07.26

(21)申请号 201980053746.X
(22)申请日 2019.08.08
(65)同一申请的已公布的文献号
申请公布号 CN 112567338 A
(43)申请公布日 2021.03.26
(30)优先权数据
2018-151423 2018.08.10 JP
2019-129961 2019.07.12 JP
(85)PCT国际申请进入国家阶段日
2021.02.08
(86)PCT国际申请的申请数据
PCT/JP2019/031453 2019.08.08
(87)PCT国际申请的公布数据
WO2020/032192 JA 2020.02.13
(73)专利权人 株式会社电装
地址 日本爱知县
(72)发明人 原田雄三 上原一浩 夏目充启 河崎卓也
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 舒艳君 王海奇
(51)Int.Cl.
G06F 8/656(2006.01)
B60R 16/02(2006.01)
B60R 16/023(2006.01)
G06F 8/658(2006.01)
(56)对比文件
JP 2015079440 A,2015.04.23
JP 2018065410 A,2018.04.26
WO 2016098376 A1,2016.06.23
审查员 林方清

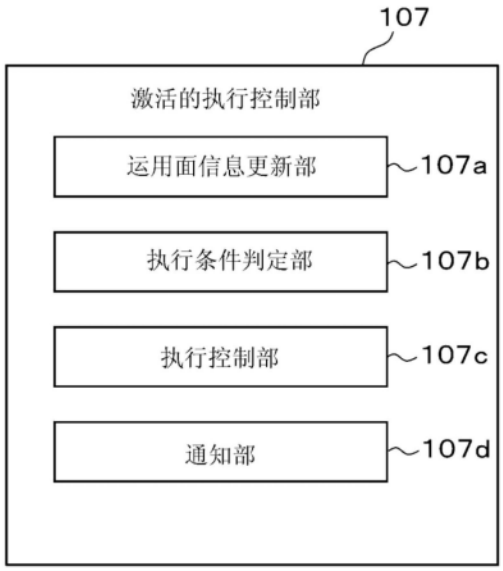
权利要求书2页 说明书138页 附图239页

(54)发明名称

电子控制装置及系统、激活的执行控制方法及记录介质

(57)摘要

电子控制装置(19)具备:运用面信息更新部(107a),在完成第二数据储存面的程序的改写,并且从车辆用主装置指示了激活请求的情况下,更新表示第一数据储存面以及第二数据储存面中哪一个为运用面的运用面信息;执行条件判定部(107b),判定激活的执行条件的成立;以及执行控制部(107c),在通过执行条件判定部判定为激活的执行条件成立的情况下,在重新启动后,基于运用面信息使第二数据储存面作为启动面启动。



CN 112567338 B

1.一种电子控制装置,具备包含第一数据储存面和第二数据储存面的非易失性存储器,从车辆用主装置接收更新数据,并将接收到的该更新数据写入至上述第二数据储存面,改写上述第二数据储存面的程序,上述电子控制装置具备:

运用面信息更新部,在完成上述第二数据储存面的程序的改写,并且从上述车辆用主装置指示了激活请求的情况下,更新表示上述第一数据储存面以及上述第二数据储存面中的哪一个为运用面的运用面信息;

执行条件判定部,判定激活的执行条件的成立;以及

执行控制部,在由上述执行条件判定部判定为激活的执行条件成立的情况下,在上述电子控制装置重新启动后,基于上述运用面信息使上述第二数据储存面作为启动面启动,

在完成上述第二数据储存面的程序的改写,并且未从上述车辆用主装置指示激活请求而上述电子控制装置重新启动的情况下,上述执行控制部基于上述运用面信息使上述第一数据储存面作为启动面启动。

2.根据权利请求1所述的电子控制装置,其中,

上述执行条件判定部将从上述车辆用主装置指示了软件的复位请求、从上述车辆用主装置指示了电源的复位请求、以及与上述车辆用主装置的通信中断持续了规定时间中的至少任意一个作为执行条件。

3.根据权利请求1或者2所述的电子控制装置,其中,

上述电子控制装置具备通知部,在未完成上述第二数据储存面的程序的改写时,在从上述车辆用主装置指示了激活请求的情况下,上述通知部向上述车辆用主装置通知否定响应作为通知信息。

4.根据权利请求3所述的电子控制装置,其中,

在虽然程序改写部完成了上述第二数据储存面的程序的改写但改写后的数据验证为否时,在从上述车辆用主装置指示了激活请求的情况下,上述通知部向上述车辆用主装置通知否定响应作为通知信息。

5.一种车辆用电子控制系统,具备:车辆用主装置,从外部获取更新数据,将获取到的该更新数据分发至改写对象的电子控制装置,对改写对象的电子控制装置指示程序的改写;以及电子控制装置,具备包含第一数据储存面和第二数据储存面的非易失性存储器,从车辆用主装置接收更新数据,将接收到的该更新数据写入至上述第二数据储存面,改写上述第二数据储存面的程序,其中,

上述电子控制装置具备:

运用面信息更新部,在完成上述第二数据储存面的程序的改写,并且从上述车辆用主装置指示了激活请求的情况下,更新表示上述第一数据储存面以及上述第二数据储存面中的哪一个为运用面的运用面信息;

执行条件判定部,判定激活的执行条件的成立;以及

执行控制部,在由上述执行条件判定部判定为激活的执行条件成立的情况下,在上述电子控制装置重新启动后,基于上述运用面信息使上述第二数据储存面作为启动面启动,

在完成上述第二数据储存面的程序的改写,并且未从上述车辆用主装置指示激活请求而上述电子控制装置重新启动的情况下,上述执行控制部基于上述运用面信息使上述第一数据储存面作为启动面启动。

6.一种激活的执行控制方法,其中,

电子控制装置具备包含第一数据储存面和第二数据储存面的非易失性存储器,从车辆用主装置接收更新数据,将接收到的该更新数据写入至上述第二数据储存面,改写上述第二数据储存面的程序,

上述激活的执行控制方法在电子控制装置中执行以下步骤:

运用面信息更新步骤,在完成上述第二数据储存面的程序的改写,并且从上述车辆用主装置指示了激活请求的情况下,更新表示上述第一数据储存面以及上述第二数据储存面中的哪一个为运用面的运用面信息;

执行条件判定步骤,判定激活的执行条件的成立;以及

启动控制步骤,在通过上述执行条件判定步骤判定为激活的执行条件成立的情况下,在上述电子控制装置重新启动后,基于上述运用面信息使上述第二数据储存面作为启动面启动;在完成上述第二数据储存面的程序的改写,并且未从上述车辆用主装置指示激活请求而上述电子控制装置重新启动的情况下,基于上述运用面信息使上述第一数据储存面作为启动面启动。

7.一种记录介质,记录有激活的执行控制程序,其中,

电子控制装置具备包含第一数据储存面和第二数据储存面的非易失性存储器,从车辆用主装置接收更新数据,将接收到的该更新数据写入至上述第二数据储存面,改写上述第二数据储存面的程序,

上述激活的执行控制程序使电子控制装置执行以下步骤:

运用面信息更新步骤,在完成上述第二数据储存面的程序的改写,并且从上述车辆用主装置指示了激活请求的情况下,更新表示上述第一数据储存面以及上述第二数据储存面中的哪一个为运用面的运用面信息;

执行条件判定步骤,判定激活的执行条件的成立;以及

启动控制步骤,在通过上述执行条件判定步骤判定为激活的执行条件成立的情况下,在上述电子控制装置重新启动后,基于上述运用面信息使上述第二数据储存面作为启动面启动;在完成上述第二数据储存面的程序的改写,并且未从上述车辆用主装置指示激活请求而上述电子控制装置重新启动的情况下,基于上述运用面信息使上述第一数据储存面作为启动面启动。

电子控制装置及系统、激活的执行控制方法及记录介质

[0001] 相关申请的交叉引用

[0002] 本申请基于2018年8月10日申请的日本申请编号2018－151423号以及2019年7月12日申请的日本申请编号2019－129961号,并在此引用其记载内容。

技术领域

[0003] 本公开涉及电子控制装置、车辆用电子控制系统、激活的执行控制方法以及激活的执行控制程序。

背景技术

[0004] 近年来,伴随着驾驶辅助功能、自动驾驶功能等车辆控制的多样化,搭载于车辆的电子控制装置(以下,称为ECU(Electronic Control Unit))的车辆控制、诊断等的程序的规模越来越大。另外,伴随着基于功能改善等的版本升级,改写(重编)ECU的程序的机会也越来越多。另一方面,伴随着通信网络的发展等,联网汽车的技术也日益普及。根据这样的情况,例如专利文献1中提出了如下技术:在车辆侧设置有作为中继装置的车辆用主装置,车辆用主装置将通过无线从中心装置接收到的更新数据分发至改写对象ECU,从而利用OTA(Over The Air:空中下载)对改写对象ECU的程序进行改写。

[0005] 专利文献1:日本特开2016－224898号公报

[0006] 在专利文献1中,在车辆用主装置中,对改写对象ECU指示将从中心装置3下载的更新数据写入到非易失性存储器(例如闪存)。作为搭载于ECU的非易失性存储器的种类,有在一个面具有储存控制程序等数据的数据储存面的单面单独方式存储器、在伪两面具有数据储存面的单面挂起方式存储器、在实际的两面具有数据储存面的双面存储器。由于搭载单面挂起方式存储器、双面存储器的ECU在双面具有数据储存面,所以将双面中的一方作为运用面并且将另一方作为非运用面,在改写程序的情况下,通过将非运用面作为改写面,并将新程序写入改写面,能够改写非运用面的程序。搭载单面挂起方式存储器、双面存储器的ECU若完成向非运用面的新程序的改写,则切换运用面和非运用面,并进行重新启动,从而激活新程序。

[0007] 若在改写对象ECU完成了程序的改写的时机进行激活,则有在与其它的ECU的协作处理中产生不良情况的担心。

发明内容

[0008] 本公开是鉴于上述的事情而完成的,其目的在于提供在将在多个面具有数据储存面的电子控制装置作为程序的改写对象的情况下,能够基于来自外部的指示适当地控制激活的电子控制装置、车辆用电子控制系统、激活的执行控制方法以及激活的执行控制程序。

[0009] 根据本公开的一方式,具备包含第一数据储存面和第二数据储存面的非易失性存储器,从车辆用主装置接收更新数据,将该接收的更新数据写入第二数据储存面,改写第二数据储存面的程序。运用面信息更新部若程序改写部完成第二数据储存面的程序的改写,

并且从车辆用主装置指示了激活请求,则更新表示第一数据储存面以及第二数据储存面中哪一个为运用面的运用面信息。执行条件判定部判定激活的执行条件的成立。执行控制部若通过执行条件判定部判定为激活的执行条件成立,则在重新启动后,基于运用面信息使第二数据储存面作为启动面启动。

[0010] 若判定为激活的执行条件成立,则在重新启动后,基于运用面信息使第二数据储存面作为启动面启动。在将在多个面具有数据储存面的电子控制装置作为程序的改写对象的情况下,能够基于来自外部的指示适当地控制激活。

附图说明

[0011] 参照附图并且通过下述的详细描述,本公开的上述目的以及其他的目的、特征、优点变得更加明确。其中,附图为:

[0012] 图1是表示一实施方式的整体构成的图。

[0013] 图2是表示CGW的电气结构的图。

[0014] 图3是表示DCM的电气结构的图。

[0015] 图4是表示ECU的电气结构的图。

[0016] 图5是表示电源线的连接方式的图。

[0017] 图6是表示将重编数据以及分发规格数据打包的方式的图。

[0018] 图7是表示DCM用的改写规格数据的图。

[0019] 图8是表示CGW用的改写规格数据的图。

[0020] 图9是表示分发规格数据的图。

[0021] 图10是表示将分发数据包解包的方式的图。

[0022] 图11是表示嵌入型单面单独存储器中的通常动作时的方式的图。

[0023] 图12是表示嵌入型单面单独存储器中的改写动作时的方式的图。

[0024] 图13是表示下载型单面单独存储器中的通常动作时的方式的图。

[0025] 图14是表示下载型单面单独存储器中的改写动作时的方式的图。

[0026] 图15是表示嵌入型单面挂起存储器中的通常动作时的方式的图。

[0027] 图16是表示嵌入型单面挂起存储器中的改写动作时的方式的图。

[0028] 图17是表示下载型单面挂起存储器中的通常动作时的方式的图。

[0029] 图18是表示下载型单面挂起存储器中的改写动作时的方式的图。

[0030] 图19是表示嵌入型双面存储器中的通常动作时的方式的图。

[0031] 图20是表示嵌入型双面存储器中的改写动作时的方式的图。

[0032] 图21是表示下载型双面存储器中的通常动作时的方式的图。

[0033] 图22是表示下载型双面存储器中的改写动作时的方式的图。

[0034] 图23是表示改写应用程序的方式的图。

[0035] 图24是表示改写应用程序的方式的图。

[0036] 图25是表示改写应用程序的方式的图。

[0037] 图26是表示通过电源控制改写应用程序的方式的时序图。

[0038] 图27是表示通过电源控制改写应用程序的方式的时序图。

[0039] 图28是表示通过电源自保持改写应用程序的方式的时序图。

[0040] 图29是表示通过电源自保持改写应用程序的方式的时序图。

[0041] 图30是表示阶段的图。

[0042] 图31是表示通常时的画面的图。

[0043] 图32是表示活动通知产生时的画面的图。

[0044] 图33是表示活动通知时的画面的图。

[0045] 图34是表示下载同意时的画面的图。

[0046] 图35是表示下载同意时的画面的图。

[0047] 图36是表示下载执行中的画面的图。

[0048] 图37是表示下载执行中的画面的图。

[0049] 图38是表示下载完成时的画面的图。

[0050] 图39是表示安装同意时的画面的图。

[0051] 图40是表示安装同意时的画面的图。

[0052] 图41是表示安装执行中的画面的图。

[0053] 图42是表示安装执行中的画面的图。

[0054] 图43是表示激活同意时的画面的图。

[0055] 图44是表示IG接通时的画面的图。

[0056] 图45是表示确认操作时的画面的图。

[0057] 图46是表示确认操作时的画面的图。

[0058] 图47是中心装置的功能框图。

[0059] 图48是DCM的功能框图。

[0060] 图49是CGW的功能框图。

[0061] 图50是CGW的功能框图。

[0062] 图51是ECU的功能框图。

[0063] 图52是车载显示器的功能框图。

[0064] 图53是分发数据包的发送判定部的功能框图。

[0065] 图54是表示分发数据包的发送判定处理的流程图。

[0066] 图55是分发数据包的下载判定部的功能框图。

[0067] 图56是表示分发数据包的下载判定处理的流程图。

[0068] 图57是写入数据的传输判定部的功能框图。

[0069] 图58是表示写入数据的传输判定处理的流程图。

[0070] 图59是写入数据的获取判定部的功能框图。

[0071] 图60是表示写入数据的获取判定处理的流程图。

[0072] 图61是安装的指示判定部的功能框图。

[0073] 图62是表示安装的指示判定处理的流程图。

[0074] 图63是表示指示安装的方式的图。

[0075] 图64是表示指示安装的方式的图。

[0076] 图65是表示生成随机值的方式的图。

[0077] 图66是安全访问密钥的管理部的功能框图。

[0078] 图67是表示安全访问密钥的生成处理的流程图。

[0079] 图68是表示生成安全访问密钥的方式的图。

[0080] 图69是表示安全访问密钥的消除处理的流程图。

[0081] 图70是表示写入数据的验证所涉及的处理的流程的图。

[0082] 图71是写入数据的验证部的功能框图。

[0083] 图72是表示写入数据的验证处理的流程图。

[0084] 图73是表示将写入数据的验证所涉及的处理分散后的方式的图。

[0085] 图74是表示将写入数据的验证所涉及的处理分散后的方式的图。

[0086] 图75是表示将写入数据的验证所涉及的处理分散后的方式的图。

[0087] 图76是表示将写入数据的验证所涉及的处理分散后的方式的图。

[0088] 图77是表示写入数据的验证以及应用程序的改写的流程的图。

[0089] 图78是表示写入数据的验证以及应用程序的改写的流程的图。

[0090] 图79是数据储存面信息的发送控制部的功能框图。

[0091] 图80是表示数据储存面信息的发送控制处理的流程图。

[0092] 图81是表示通知双面改写信息的方式的顺序图。

[0093] 图82是非改写对象的电源管理部的功能框图。

[0094] 图83是表示非改写对象的电源管理处理的流程图。

[0095] 图84是表示启动状态、停止状态、睡眠状态的迁移的图。

[0096] 图85是表示启动状态、停止状态、睡眠状态的迁移的图。

[0097] 图86是表示电源线的连接方式的图。

[0098] 图87是表示电池余量的监视处理的流程图。

[0099] 图88是文件的传输控制部的功能框图。

[0100] 图89是表示文件的传输控制处理的流程图。

[0101] 图90是表示授受文件的方式的图。

[0102] 图91是表示授受文件的方式的图。

[0103] 图92是表示分割文件以及写入文件的图。

[0104] 图93是表示CGW将传输请求发送至DCM的方式的图。

[0105] 图94是表示CGW将传输请求发送至DCM的方式的图。

[0106] 图95是表示CGW将写入数据分发至改写对象ECU的方式的图。

[0107] 图96是表示CGW将写入数据分发至改写对象ECU的方式的图。

[0108] 图97是表示CGW将写入数据分发至改写对象ECU的方式的图。

[0109] 图98是表示ECU的连接方式的图。

[0110] 图99是写入数据的分发控制部的功能框图。

[0111] 图100是表示总线负载表的图。

[0112] 图101是表示改写对象ECU所属表的图。

[0113] 图102是表示写入数据的分发控制处理的流程图。

[0114] 图103是表示分发写入数据的方式的图。

[0115] 图104是表示分发写入数据的方式的图。

[0116] 图105是表示车辆行驶中的分发写入数据的方式的图。

[0117] 图106是表示停车中的分发写入数据的方式的图。

[0118] 图107是表示写入数据的分发量的图。

[0119] 图108是表示写入数据的分发量的图。

[0120] 图109是激活请求的指示部的功能框图。

[0121] 图110是表示激活请求的指示处理的流程图。

[0122] 图111是表示指示激活请求的方式的图。

[0123] 图112是激活的执行控制部的功能框图。

[0124] 图113是表示改写处理的流程图。

[0125] 图114是表示激活的执行控制处理的流程图。

[0126] 图115是改写对象的分组部的功能框图。

[0127] 图116是表示改写对象的组管理处理的流程图。

[0128] 图117是表示改写对象的组管理处理的流程图。

[0129] 图118是表示将改写对象分组的方式的图。

[0130] 图119是回滚的执行控制部的功能框图。

[0131] 图120是表示回滚方法的确定处理的流程图。

[0132] 图121是表示取消请求的判定处理的流程图。

[0133] 图122是表示取消请求的判定处理的流程图。

[0134] 图123是表示取消请求的判定处理的流程图。

[0135] 图124是表示取消请求的判定处理的流程图。

[0136] 图125是表示取消请求的判定处理的流程图。

[0137] 图126是表示执行回滚的方式的图。

[0138] 图127是表示执行回滚的方式的图。

[0139] 图128是表示执行回滚的方式的图。

[0140] 图129是表示执行回滚的方式的图。

[0141] 图130是表示执行回滚的方式的图。

[0142] 图131是改写进展状况的显示控制部的功能框图。

[0143] 图132是表示改写进展状况的显示控制处理的流程图。

[0144] 图133是表示改写进展状况的显示控制处理的流程图。

[0145] 图134是表示改写进展状况的画面的图。

[0146] 图135是表示改写进展状况的画面的图。

[0147] 图136是表示改写进展状况的画面的图。

[0148] 图137是表示改写进展状况的画面的图。

[0149] 图138是表示改写进展状况的画面的图。

[0150] 图139是表示进展图显示的迁移的图。

[0151] 图140是表示进展图显示的迁移的图。

[0152] 图141是表示进展图显示的迁移的图。

[0153] 图142是表示进展图显示的迁移的图。

[0154] 图143是表示改写进展状况的画面的图。

[0155] 图144是差分数据的匹配性判定部的功能框。

[0156] 图145是表示差分数据的匹配性判定处理的流程图。

[0157] 图146是表示判定差分数据的匹配性的方式的图。

[0158] 图147是表示判定差分数据的匹配性的方式的图。

[0159] 图148是改写的执行控制部的功能框图。

[0160] 图149是表示通常动作处理的流程图。

[0161] 图150是表示改写动作处理的流程图。

[0162] 图151是表示信息通知处理的流程图。

[0163] 图152是表示改写程序的验证处理的流程图。

[0164] 图153是表示发送识别信息以及写入数据的方式的图。

[0165] 图154是表示发送识别信息以及写入数据的方式的图。

[0166] 图155是表示安装指示处理的流程图。

[0167] 图156是会话的确立部的功能框图。

[0168] 图157是表示程序的构成的图。

[0169] 图158是表示状态迁移的图。

[0170] 图159是表示状态迁移的图。

[0171] 图160是表示状态迁移的图。

[0172] 图161是表示会话的调停的图。

[0173] 图162是表示会话的调停的图。

[0174] 图163是表示第一状态的状态迁移管理处理的流程图。

[0175] 图164是表示第一状态的状态迁移管理处理的流程图。

[0176] 图165是表示第一状态的状态迁移管理处理的流程图。

[0177] 图166是表示第二状态的状态迁移管理处理的流程图。

[0178] 图167是表示第二状态的状态迁移管理处理的流程图。

[0179] 图168是表示程序的构成的图。

[0180] 图169是表示状态迁移的图。

[0181] 图170是重试点的确定部的功能框图。

[0182] 图171是表示闪存的构成的图。

[0183] 图172是表示处理标志的设定处理的流程图。

[0184] 图173是表示处理标志的判定处理的流程图。

[0185] 图174是表示处理标志的判定处理的流程图。

[0186] 图175是进展状态的同步控制部的功能框图。

[0187] 图176是进展状态的同步控制部的功能框图。

[0188] 图177是表示收发进展状态信号的方式的图。

[0189] 图178是表示进展状态的同步控制处理的流程图。

[0190] 图179是表示进展状态的同步控制处理的流程图。

[0191] 图180是表示进展状态的显示处理的流程图。

[0192] 图181是显示控制信息的发送控制部的功能框图。

[0193] 图182是表示显示控制信息的发送控制处理的流程图。

[0194] 图183是显示控制信息的接收控制部的功能框图。

[0195] 图184是表示显示控制信息的接收控制处理的流程图。

[0196] 图185是表示分发规格数据中包含的信息的图。

[0197] 图186是进展显示的画面显示控制部的功能框图。

[0198] 图187是表示改写规格数据的图。

[0199] 图188是表示菜单选择时的画面的图。

[0200] 图189是表示用户选择时的画面的图。

[0201] 图190是表示用户登记时的画面的图。

[0202] 图191是表示进展显示的画面显示控制处理的流程图。

[0203] 图192是表示进展显示的画面显示控制处理的流程图。

[0204] 图193是表示消息帧的图。

[0205] 图194是表示激活同意时的画面的图。

[0206] 图195是表示项目的显示有无的设定的图。

[0207] 图196是表示项目的显示有无的设定的图。

[0208] 图197是表示激活同意时的画面的图。

[0209] 图198是表示数据通信的方式的图。

[0210] 图199是表示活动通知时的消息帧的图。

[0211] 图200是表示下载同意时的消息帧的图。

[0212] 图201是表示安装同意时的消息帧的图。

[0213] 图202是表示激活同意时的消息帧的图。

[0214] 图203是表示画面的迁移的图。

[0215] 图204是表示活动通知产生时的画面的图。

[0216] 图205是表示下载同意时的画面的图。

[0217] 图206是表示下载同意时的画面的图。

[0218] 图207是表示下载执行中的画面的图。

[0219] 图208是表示下载完成时的画面的图。

[0220] 图209是表示安装同意时的画面的图。

[0221] 图210是表示激活同意时的画面的图。

[0222] 图211是程序更新的报告控制部的功能框图。

[0223] 图212是表示程序更新的报告控制处理的流程图。

[0224] 图213是表示指示器的报告方式的图。

[0225] 图214是表示改写对象为双面存储器的情况下的报告方式的迁移的图。

[0226] 图215是表示改写对象为单面挂起存储器的情况下的报告方式的迁移的图。

[0227] 图216是表示改写对象为单面单独存储器的情况下的报告方式的迁移的图。

[0228] 图217是表示连接方式的图。

[0229] 图218是CGW中的电源自保持的执行控制部的功能模块。

[0230] 图219是ECU中的电源自保持的执行控制部的功能模块。

[0231] 图220是表示CGW中的电源自保持的执行控制处理的流程图。

[0232] 图221是表示ECU中的电源自保持的执行控制处理的流程图。

[0233] 图222是表示需要电源自保持的期间的图。

[0234] 图223是表示改写应用程序的方式的整体顺序图。

[0235] 图224是表示改写应用程序的方式的整体顺序图。

[0236] 图225是表示改写应用程序的方式的整体顺序图。

[0237] 图226是表示改写应用程序的方式的整体顺序图。

[0238] 图227是表示改写应用程序的方式的整体顺序图。

[0239] 图228是表示改写应用程序的方式的整体顺序图。

[0240] 图229是表示改写应用程序的方式的整体顺序图。

[0241] 图230是表示改写应用程序的方式的整体顺序图。

[0242] 图231是表示改写应用程序的方式的整体顺序图。

[0243] 图232是表示改写应用程序的方式的整体顺序图。

[0244] 图233是表示改写应用程序的方式的整体顺序图。

[0245] 图234是表示第一实施方式中的车辆信息通信系统的整体构成的图。

[0246] 图235是表示CGW的电气结构的图。

[0247] 图236是表示ECU的电气结构的图。

[0248] 图237是表示电源线的连接方式的图。

[0249] 图238是表示将重编数据以及分发规格数据打包的方式的图。

[0250] 图239是表示将分发数据包解包的方式的图。

[0251] 图240是以框图的方式表示中心装置中的主要与服务器的各功能相关的部分的图。

[0252] 图241是表示中心装置中的处理的流程的图像图。

[0253] 图242是表示结构信息DB中登记的车辆的结构信息的一个例子的图。

[0254] 图243是表示ECU重编数据DB中登记的程序、数据的一个例子的图。

[0255] 图244是表示ECU元数据DB中登记的规格数据的一个例子的图。

[0256] 图245是表示个体车辆信息DB中登记的车辆的结构信息的一个例子的图。

[0257] 图246是表示数据包DB中登记的分发数据包数据的一个例子的图。

[0258] 图247是表示活动DB中登记的活动数据的一个例子的图。

[0259] 图248是表示生成ECU重编数据DB中登记的程序、数据的处理的流程图。

[0260] 图249是表示生成ECU元数据DB中登记的规格数据的一个例子的处理的流程图。

[0261] 图250是表示规格数据的一个例子的图。

[0262] 图251是表示总线负载表的一个例子的图。

[0263] 图252是表示生成数据包DB中登记的分发数据包的处理的流程图。

[0264] 图253是以图像方式表示数据包文件的内容的图。

[0265] 图254是表示在第二实施方式中,在中心装置与车辆侧系统之间执行的处理流程的顺序图。

[0266] 图255是表示中心装置进行的处理的流程图。

[0267] 图256是以图像方式表示在图248所示的流程图的步骤D6、D7中进行的处理内容的图。

[0268] 图257是表示从车辆侧系统向中心装置发送散列值的情况下的处理的流程图。

[0269] 图258是表示在第三实施方式中,在中心装置与车辆侧系统之间执行的处理流程的顺序图。

[0270] 图259是表示中心装置进行的处理的流程图。

[0271] 图260是表示中心装置通过SMS向EV车和组合车分别进行通知的状态的顺序图。

[0272] 图261是表示在第四实施方式中,在中心装置与车辆侧系统之间执行的处理流程的顺序图。

[0273] 图262是以图像方式表示在第五实施方式中在供应商、中心装置、车辆侧系统之间进行的处理的图。

[0274] 图263是表示在供应商、中心装置、车辆侧系统之间进行的处理流程的顺序图(其1)。

[0275] 图264是表示在供应商、中心装置、车辆侧系统之间进行的处理流程的顺序图(其2)。

[0276] 图265是表示在供应商、中心装置、车辆侧系统之间进行的处理流程的顺序图(其3)。

[0277] 图266是第一实施方式的变形(其1),是表示使多个数据包对应于一个活动的情况下的数据包DB的数据格式的图。

[0278] 图267是表示使多个数据包对应于一个活动的情况下的活动DB的数据格式的图。

[0279] 图268是按组生成规格数据的情况下的与图242相当图。

[0280] 图269是按组生成分发数据包的情况下的与图245相当图。

[0281] 图270是第一实施方式的变形(其2),是表示数据包生成工具的处理内容的图。

具体实施方式

[0282] 以下,参照附图对一实施方式进行说明。车辆用程序改写系统(相当于车辆用电子控制系统)是能够通过OTA(Over The Air:空中下载)改写搭载于电子控制装置(以下,称为ECU(Electronic Control Unit))的车辆控制、诊断等的应用程序的系统。在本实施方式中,对通过有线或者无线改写应用程序的情况进行了说明,但也能够例如应用于通过有线或者无线改写地图应用中所使用的地图数据、ECU中所使用的控制参数等、各种应用中所使用的数据的情况。

[0283] 通过有线的应用程序的改写除了从车辆外部经由有线获取应用程序并改写之外,也包括从车辆外部经由有线获取在执行应用程序时使用的各种数据并改写。通过无线的应用程序的改写除了从车辆外部经由无线获取应用程序并改写之外,也包括从车辆外部经由无线获取在执行应用程序时使用的各种数据并改写。

[0284] 如图1所示,车辆用程序改写系统1具有通信网络2侧的中心装置3、车辆侧的车辆侧系统4、以及显示终端5。通信网络2包括例如利用4G线路等的移动体通信网络、因特网、WiFi(Wireless Fidelity:无线保真)(注册商标)等而构成。此外,在本实施方式中,主要对车辆侧的构成进行说明,关于中心装置3的构成,在图234至图270中详细描述。

[0285] 显示终端5是具有受理来自用户的操作输入的功能、显示各种画面的功能的终端,例如是用户能够携带的智能手机、平板等移动终端6、配置于车厢内的车载显示器7。移动终端6若在移动体通信网络的通信范围内,则能够经由通信网络2与中心装置3进行数据通信。车载显示器7与车辆侧系统4连接且也可以是兼具导航功能的构成。另外,车载显示器7既可以是具有ECU的功能的车载显示器ECU,也可以具有控制向中心显示器、仪表显示器等的显

示的功能。

[0286] 若用户在车厢外且在移动体通信网络的通信范围内,则能够一边通过移动终端6确认应用程序的改写所涉及的各种画面一边进行操作输入,进行应用程序的改写所涉及的手续。用户在车厢内,能够一边通过车载显示器7确认应用程序的改写所涉及的各种画面一边进行操作输入,进行应用程序的改写所涉及的手续。即,用户能够在车厢外和车厢内分开使用移动终端6和车载显示器7,进行应用程序的改写所涉及的手续。

[0287] 中心装置3在车辆用程序改写系统1中总括通信网络2侧的程序更新功能,作为OTA中心发挥作用。中心装置3具有文件服务器8、网页服务器9以及管理服务器10,各服务器8~10构成为能够相互进行数据通信。即,中心装置3按各功能包括不同的多个服务器而构成。

[0288] 文件服务器8是管理从中心装置3分发至车辆侧系统4的应用程序的文件的服务器。文件服务器8管理从自中心装置3分发至车辆侧系统4的应用程序的提供企业亦即供应商等提供的更新数据(以下,也称为重编数据(Reprogram-Data)、写入数据)、从OEM(Original Equipment Manufacturer:原始设备制造商)提供的分发规格数据、从车辆侧系统4获取的车辆状态等。文件服务器8能够经由通信网络2与车辆侧系统4之间进行数据通信,若产生分发数据包的下载请求,则将使重编数据和分发规格数据打包成一个文件的分发数据包发送至车辆侧系统4。

[0289] 网页服务器9是管理网页信息的服务器。网页服务器9根据来自移动终端6等具有的网页浏览器的请求发送自身管理的网页数据。管理服务器10是管理登记到应用程序的改写服务的用户的个人信息、每个车辆的应用程序的改写历史等的服务器。

[0290] 车辆侧系统4具有主装置11(相当于车辆用主装置)。主装置11具有DCM(Data Communication Module:数据通信模块)12(相当于车载通信设备)和CGW(Central Gate Way:中央网关)13(相当于车辆用网关装置)。DCM12和CGW13经由第一总线14连接为能够进行数据通信。DCM12与中心装置3之间经由通信网络2进行数据通信。DCM12若从文件服务器8下载分发数据包,则从下载的该分发数据包提取写入数据,并将提取出的该写入数据传输至CGW13。

[0291] CGW13具有数据中继功能,若从DCM12获取写入数据,则对作为应用程序的改写对象的改写对象ECU指示获取到的该写入数据的写入,并将写入数据分发至改写对象ECU。另外,若在改写对象ECU中完成写入数据的写入,应用程序的改写完成,则CGW13对改写对象ECU指示使该改写完成后的应用程序有效的激活。

[0292] 主装置11在车辆用程序改写系统1中总括车辆侧的程序更新功能,作为OTA主机发挥作用。此外,在图1中,例示出DCM12和车载显示器7与相同的第一总线14连接的构成,但也可以是DCM12和车载显示器7与不同的总线连接的构成。另外,既可以是CGW13具有DCM12的功能的一部分或者整体的构成,也可以是DCM12具有CGW13的功能的一部分或者整体的构成。即,在主装置11中,DCM12和CGW13的功能分担可以任意构成。主装置11既可以由DCM12以及CGW13的2个ECU构成,也可以由具有DCM12的功能和CGW13的功能的一个综合ECU构成。

[0293] 除了第一总线14之外,在CGW13还连接有第二总线15、第三总线16、第四总线17、第五总线18作为车内侧的总线,经由总线15~17连接有各种ECU19,并且经由总线18连接有电源管理ECU20。

[0294] 第二总线15例如是车身系统网络的总线。与第二总线15连接的ECU19是进行车身

系统的控制的ECU。进行车身系统的控制的ECU例如是控制车门的上锁/解锁的车门ECU、控制向仪表显示器的显示的仪表ECU、控制空调的驱动的空调ECU、控制车窗的开闭的车窗ECU、为了车辆的防盗而驱动的安全ECU等。

[0295] 第三总线16例如是行驶系统网络的总线。与第三总线16连接的ECU19是进行行驶系统的控制的ECU。进行行驶系统的控制的ECU例如是控制引擎的驱动的引擎ECU、控制制动器的驱动的制动器ECU、控制自动变速器的驱动的ECT(Electronic Controlled Transmission:电子控制变速器)ECU、控制动力转向的驱动的动力转向ECU等。

[0296] 第四总线17例如是多媒体系统网络的总线。与第四总线17连接的ECU19是进行多媒体系统的控制的ECU。进行多媒体系统的控制的ECU例如是用于控制导航系统的导航ECU、控制电子收费系统(ETC(Electronic Toll Collection System,注册商标))的ETCECU等。总线15～17也可以是车身系统网络的总线、行驶系统网络的总线、多媒体系统网络的总线以外的系统的总线。另外,总线的根数、ECU19的个数不限于例示的构成。电源管理ECU20是管理供给至DCM12、CGW13、各种ECU19等的电源的ECU。

[0297] 在CGW13连接有第六总线21作为车外侧的总线。在第六总线21连接有能够装卸地连接工具23(相当于服务工具)的DLC(Data Link Coupler:数据链路耦合器)连接器22。车内侧的总线14～18以及车外侧的总线21例如由CAN(Controller Area Network:控制器局域网,注册商标)总线构成,CGW13根据CAN的数据通信标准、诊断通信标准(UDS(Unified Diagnosis Services):ISO14229)与DCM12、各种ECU19以及工具23之间进行数据通信。此外,也可以DCM12和CGW13通过以太网连接,也可以DLC连接器22和CGW13通过以太网连接。

[0298] 改写对象ECU19若从CGW13接收到写入数据,则将接收到的该写入数据写入闪存(相当于非易失性存储器)来改写应用程序。在上述的构成中,CGW13作为若从改写对象ECU19接收写入数据的获取请求则将写入数据分发至改写对象ECU19的重编主机发挥作用。改写对象ECU19作为若从CGW13接收写入数据则将接收到的该写入数据写入闪存来改写应用程序的重编从机发挥作用。

[0299] 作为改写应用程序的方式,有通过有线进行改写的方式和通过无线进行改写的方式。所谓通过有线改写应用程序的方式是指使用从车辆外部经由有线获取到的应用程序对改写对象ECU19进行改写的方式。具体而言,若工具23与DLC连接器22连接,则工具23将写入数据传输到CGW13。CGW13作为网关发挥作用,将有线改写请求发送至改写对象ECU19,对改写对象ECU19指示写入数据的写入(安装),将从工具23传输的写入数据分发至改写对象ECU19。将写入数据分发至改写对象ECU19是对写入数据进行中继。

[0300] 所谓通过无线改写应用程序的方式是指使用从车辆外部经由无线获取到的应用程序对改写对象ECU19进行改写的方式。具体而言,DCM12若从文件服务器8下载分发数据包,则从下载的该分发数据包提取写入数据,并将该写入数据传输到CGW13。CGW13作为改写工具发挥作用,对改写对象ECU19指示写入数据的写入(安装),将从DCM12传输的写入数据分发至改写对象ECU19。

[0301] 作为诊断ECU19的方式,有通过有线进行诊断的方式和通过无线进行诊断的方式。所谓通过有线进行诊断的方式是指从车辆外部经由有线对ECU19进行诊断的方式。具体而言,若工具23与DLC连接器22连接,则工具23将诊断请求传输到CGW13。CGW13作为网关发挥作用,将诊断请求发送至诊断对象ECU19,将从工具23传输的诊断指令分发至诊断对象

ECU19。诊断对象ECU19进行与从CGW13接收到的诊断指令对应的诊断处理。

[0302] 所谓通过无线进行诊断的方式是指从车辆外部经由无线对ECU19进行诊断的方式。具体而言,若诊断指令作为诊断请求被从中心装置3发送至DCM12,则DCM12将诊断指令传输至CGW13。CGW13作为网关发挥作用,将诊断指令作为诊断请求分发至诊断对象ECU19。诊断对象ECU进行与从CGW13接收到的诊断指令对应的诊断处理。

[0303] 如图2所示,CGW13具有微型计算机(以下,称为微机)24、数据传输电路25、电源电路26以及电源检测电路27作为电气功能模块。微机24具有CPU(Central Processing Unit:中央处理装置)24a、ROM(Read Only Memory:只读存储器)24b、RAM(Random Access Memory:随机存取存储器)24c、以及闪存24d。在闪存24d中包含有不能从CGW13的外部读出信息的安全区域。微机24执行储存于非过渡性实体存储介质的各种控制程序进行各种处理,控制CGW13的动作。

[0304] 数据传输电路25控制与总线14～18、21之间的依据CAN的数据通信标准、诊断通信标准的数据通信。电源电路26输入电池电源(以下,称为+B电源)、附件电源(以下,称为ACC电源)、点火电源(以下,称为IG电源)。电源检测电路27检测电源电路26输入的+B电源的电压值、ACC电源的电压值、IG电源的电压值,并将这些检测到的电压值与规定的电压阈值比较,将其比较结果输出到微机24。微机24根据从电源检测电路27输入的比较结果,判定从外部供给至CGW13的+B电源、ACC电源、IG电源是正常还是异常。

[0305] 如图3所示,DCM12具有微机28、无线电路29、数据传输电路30、电源电路31以及电源检测电路32作为电气功能模块。微机28具有CPU28a、ROM28b、RAM28c以及闪存28d。在闪存28d中包含有不能从DCM12的外部读出信息的安全区域。微机28执行储存于非过渡性实体存储介质的各种控制程序进行各种处理,控制DCM12的动作。用于保存从中心装置3下载的数据的闪存也可以配置于CGW13。

[0306] 无线电路29控制与中心装置3的经由通信网络2的数据通信。数据传输电路30控制与总线14之间的依据CAN的数据通信标准的数据通信。电源电路31输入+B电源、ACC电源、IG电源。电源检测电路32检测电源电路31输入的+B电源的电压值、ACC电源的电压值、IG电源的电压值,并将这些检测出的电压值与规定的电压阈值比较,将其比较结果输出到微机28。微机28根据从电源检测电路32输入的比较结果,判定从外部供给至DCM12的+B电源、ACC电源、IG电源是正常还是异常。

[0307] 另外,DCM12具有例如通过GPS(Global Positioning System:全球定位系统)检测车辆位置的车辆位置检测功能。DCM12的闪存28d具有能够存储从中心装置3下载的分发数据包的足够的存储器容量,具有比CGW13的闪存24d大的存储器容量。即,通过DCM12的闪存28d是具有足够的存储器容量的结构,从而即使CGW13的闪存24d不是具有足够的存储器容量的结构,在主装置11中,也能够从中心装置3下载分发数据包,并将下载的该分发数据包积蓄到DCM12。

[0308] 如图4所示,ECU19具有微机33、数据传输电路34、电源电路35以及电源检测电路36作为电气功能模块。微机33具有CPU28a、ROM28b、RAM33c以及闪存28d。在闪存28d中包含有不能从ECU19的外部读出信息的安全区域。微机33执行储存于非过渡性实体存储介质的各种控制程序进行各种处理,控制ECU19的动作。

[0309] 数据传输电路34控制与总线15～17之间的依据CAN的数据通信标准的数据通信。

电源电路35输入+B电源、ACC电源、IG电源。电源检测电路36检测电源电路35输入的+B电源的电压值、ACC电源的电压值、IG电源的电压值,并将这些检测出的电压值与规定的电压阈值比较,将其比较结果输出到微机33。微机33根据从电源检测电路27输入的比较结果,判定从外部供给至ECU19的+B电源、ACC电源、IG电源是正常还是异常。此外,ECU19除了自身连接的例如传感器、致动器等的负载不同,基本上是相同的构成。

[0310] 车载显示器7具有与图4所示的ECU19相同的构成。电源管理ECU20具有与图4所示的ECU19相同的构成。电源管理ECU20连接为能够与后述的电源控制电路43之间进行数据通信。

[0311] 如图5所示,电源管理ECU20、CGW13、ECU19与作为电源供给线的+B电源线37、ACC电源线38、IG电源线39连接。+B电源线37与车辆电池40的正极连接。ACC电源线38经由ACC开关41与车辆电池40的正极连接。若用户进行ACC操作,则ACC开关41从断开切换为接通,车辆电池40的输出电压施加于ACC电源线38。若是例如将钥匙插入到插入口的类型的车辆,则ACC操作是将钥匙插入到插入口并从“OFF”位置转动到“ACC”位置的操作,若是按下开始按钮的类型的车辆,则ACC操作是将开始按钮按下一次的操作。

[0312] IG电源线39经由IG开关42与车辆电池40的正极连接。若用户进行IG操作,则IG开关42从断开切换为接通,车辆电池40的输出电压被施加到IG电源线39。若是例如将钥匙插入到插入口的类型的车辆,则IG操作是将钥匙插入到插入口并从“OFF”位置转动到“ON”位置的操作,若是按下开始按钮的类型的车辆,则IG操作是将开始按钮按下两次的操作。车辆电池40的负极接地。

[0313] 当ACC开关41和IG开关42双方断开时,仅+B电源被供给到车辆侧系统4。将仅+B电源供给到车辆侧系统4的状态称为+B电源状态。当ACC开关41接通且IG开关42断开时,ACC电源和+B电源被供给至车辆侧系统4。将ACC电源和+B电源被供给至车辆侧系统4的状态称为ACC电源状态。当ACC开关41和IG开关42双方接通时,+B电源、ACC电源以及IG电源被供给至车辆侧系统4。将+B电源、ACC电源以及IG电源被供给至车辆侧系统4的状态称为IG电源状态。另外,除了上述的各电源状态以外,也考虑有给予适合通过无线的程序更新的电源的电源状态等。

[0314] 对于ECU19而言,启动条件根据电源状态而不同,被区分为在+B电源状态下启动的+B电源系统ECU、在ACC电源状态下启动的ACC系统ECU、在IG电源状态下启动的IG系统ECU。例如在车辆防盗等用途中驱动的ECU19被区分为+B电源系统ECU。例如在音频等非行驶系统的用途中驱动的ECU19被区分为ACC系统ECU。例如在引擎控制等行驶系统的用途中驱动的ECU19被区分为IG系统ECU。

[0315] +B电源系统ECU构成为与+B电源线37、ACC电源线38以及IG电源线39连接,在+B电源状态时选择+B电源线37,在ACC电源状态时选择ACC电源线38,在IG电源状态时选择IG电源线39。ACC系统ECU构成为与ACC电源线38以及IG电源线39连接,在ACC电源状态时选择ACC电源线38,在IG电源状态时选择IG电源线39。IG系统ECU与IG电源线39连接。

[0316] CGW13通过向处于睡眠状态的ECU19发送启动请求,来使该启动请求的发送目的地的ECU19从睡眠状态转移至启动状态。另外,CGW13通过向处于启动状态的ECU19发送睡眠请求,来使该睡眠请求的发送目的地的ECU19从启动状态转移至睡眠状态。CGW13通过例如使发送至总线15～17的发送信号的波形不同,能够使特定的ECU19转移至启动状态或者睡眠

状态。即,按各ECU19预先决定启动请求波形以及睡眠请求波形,ECU19若接收到适合自身的启动请求波形,则从睡眠状态转移至启动状态,若从CGW13接收到适合自身的睡眠请求波形,则从启动状态转移至睡眠状态。

[0317] CGW13例如在ECU(ID1)以及ECU(ID2)为启动状态的情况下发送第一波形,从而使ECU(ID1)从启动状态转移至睡眠状态,将ECU(ID2)保持为启动状态。另外,CGW13在ECU(ID1)以及ECU(ID2)为启动状态的情况下发送第二波形,从而将ECU(ID1)保持为启动状态,使ECU(ID2)从启动状态转移至睡眠状态。

[0318] 电源控制电路43与ACC开关41以及IG开关42并联连接。CGW13将电源控制请求发送至电源管理ECU20,使电源管理ECU20控制电源控制电路43。即,CGW13通过将电源启动请求作为电源控制请求发送至电源管理ECU20,来使ACC电源线38、IG电源线39和车辆电池40的正极在电源控制电路43的内部连接。在该状态下,即使ACC开关41、IG开关42断开,ACC电源、IG电源也被供给至车辆侧系统4。另外,CGW13通过将电源停止请求作为电源控制请求发送至电源管理ECU20,来使ACC电源线38、IG电源线39和车辆电池40的正极在电源控制电路43的内部断开。

[0319] DCM12、CGW13、ECU19、电源管理ECU20分别具有电源自保持电路,具有保持来自车辆电池40的电源供给的电源自保持功能。即,关于DCM12、CGW13、ECU19、电源管理ECU20,若在处于启动状态时车辆电源从ACC电源或者IG电源切换为+B电源,则不在该切换之后立即从启动状态转移至停止状态或者睡眠状态,而利用来自车辆电池40的电源供给将启动状态继续规定时间(例如几分钟)而自保持驱动电源。DCM12、CGW13、ECU19、电源管理ECU20在车辆电源从ACC电源或者IG电源切换至+B电源后经过规定时间之后从启动状态转移至停止状态或者睡眠状态。若例如是引擎控制系统的ECU19,则通过在车辆电源从ACC电源或者IG电源切换至+B电源之后电源自保持功能工作,从而将在车辆行驶中获取到的与引擎控制有关的各种数据存储为日志。

[0320] 接下来,对从中心装置3分发至主装置11的分发数据包进行说明。如图6所示,在车辆用程序改写系统1中,根据从作为应用程序的提供企业的供应商提供的写入数据和从OEM提供的改写规格数据(相当于规格数据)生成重编数据。改写规格数据也可以在中心装置3中生成。作为从供应商提供的写入数据,有相当于旧应用程序与新应用程序的差分的差分数据和相当于新应用程序整体的全部数据。差分数据、全部数据也可以通过公知的数据压缩技术压缩。在图6中,例示从供应商A～C提供差分数据作为写入数据,根据从供应商A提供的ECU(ID1)的已加密的差分数据和认证符、从供应商B提供的ECU(ID2)的已加密的差分数据和认证符、从供应商C提供的ECU(ID3)的已加密的差分数据和认证符、以及从OEM提供的改写规格数据生成重编数据的情况。

[0321] 认证符是为了验证差分数据的完整性而对每个写入数据赋予的数据,例如根据ECU(ID)、与该ECU(ID)相关联的密钥信息、以及差分数据生成。这里,在应用程序的改写在中途被取消的情况下,用于回写(回滚)到旧版本的写入数据也可以包含于重编数据。

[0322] 从OEM提供的改写规格数据包括能够确定改写对象ECU19的信息、能够确定改写对象ECU19为多个的情况下的改写顺序的信息、能够确定后述的回滚方法的信息等作为应用程序的改写所涉及的信息。改写规格数据是定义DCM12、CGW13、改写对象ECU19等中的改写所涉及的动作的数据。改写规格数据被区分为DCM12使用的DCM用的改写规格数据、和CGW13

使用的CGW用的改写规格数据。

[0323] 如图7所示,DCM用的改写规格数据包括规格数据信息和ECU信息。规格数据信息包括地址信息和文件名。ECU信息包括与改写对象ECU19的个数对应份的、将各改写对象ECU19的更新程序(写入数据)发送至CGW13时参照的地址信息等。具体而言,ECU信息至少包括识别ECU的ID(ECU(ID))、获取更新程序时的参照地址(更新程序获取地址)、更新程序大小、获取回滚程序时的参照地址(回滚程序获取地址)、以及回滚程序大小。回滚程序是用于在应用程序的改写在中途被取消时将应用程序返回至原来的版本的程序(写入数据)。

[0324] 如图8所示,CGW用的改写规格数据包括组信息、总线负载表、电池负载、改写时的车辆状态、以及ECU信息。CGW用的改写规格数据除了这些以外也可以包括改写步骤信息、显示的场景信息等。组信息是表示改写对象ECU19所属的组以及改写顺序的信息,例如作为第一组信息,规定了以ECU(ID1)、ECU(ID2)、ECU(ID3)的顺序改写应用程序的内容,作为第二组信息,规定了以ECU(ID4)、ECU(ID5)、ECU(ID6)的顺序改写应用程序的内容。总线负载表是后述的图100所示的表,将在后面描述详细。电池负载是表示在车辆中能够允许的车辆电池40的电池余量的下限值的信息。改写时的车辆状态是表示在车辆状态为何种状态的情况下进行改写的信息。

[0325] ECU信息是与改写对象ECU19有关的信息,至少包括ECU_ID(相当于装置识别信息)、连接总线(相当于总线识别信息)、连接电源、安全访问密钥信息、存储器种类、改写方法、电源自保持时间、改写面信息、更新程序版本、更新程序获取地址、更新程序大小、回滚程序版本、回滚程序获取地址、回滚程序大小、以及写入数据种类。

[0326] 连接总线表示ECU19所连接的总线。连接电源表示ECU19所连接的电源线。安全访问密钥信息表示用于CGW13访问改写对象ECU19的认证所使用的密钥信息,包括随机值或者唯一信息、密钥模式、解密运算模式。存储器种类表示搭载于改写对象ECU19的存储器是单面单独存储器、单面挂起存储器(也称为伪双面存储器)、双面存储器中的哪一种。改写方法表示是基于电源自保持的改写以及基于电源控制的改写中的哪一种。电源自保持时间表示在改写方法是基于电源自保持的改写的情况下继续电源自保持的时间。改写面信息表示哪个面是运用面、哪个面是非运用面。运用面也称为启动面,非运用面也称为改写面。

[0327] 更新程序版本表示更新程序的版本。更新程序获取地址表示更新程序的地址。更新程序大小表示更新程序的数据大小。回滚程序版本表示回滚程序的版本。回滚程序获取地址表示回滚程序的地址。回滚程序大小表示回滚程序的数据大小。写入数据种类表示写入数据是差分数据和全部数据中的哪个种类。此外,改写规格数据除了这些信息以外,还能够包括由系统独自定义的信息。

[0328] DCM12若获取到DCM用的改写规格数据,则对获取到的该DCM用的改写规格数据进行解析。DCM12若解析DCM用的改写规格数据,则控制从储存有改写对象ECU19的更新程序的地址获取写入数据,将获取到的该写入数据传输到CGW13等的改写所涉及的动作。

[0329] CGW13若获取到CGW用的改写规格数据,则对获取到的该CGW用的改写规格数据进行解析。CGW13若解析CGW用的改写规格数据,则根据解析结果控制向DCM12请求改写对象ECU19的更新程序的规定大小量的传输、或以所指定的顺序将写入数据分发至改写对象ECU19等的改写所涉及的动作。

[0330] 在文件服务器8登记有上述的重编数据,并且登记有从OEM提供的分发规格数据。

从OEM提供的分发规格数据是定义显示终端5中的各种画面的显示所涉及的动作的数据。如图9所示,分发规格数据包括语言信息、显示语句、数据包信息、图像数据、显示模式、显示控制程序等。

[0331] 显示终端5若从CGW13获取分发规格数据,则对获取到的该分发规格数据进行解析,根据该解析结果控制各种画面的显示。显示终端5例如对预先保持的显示用帧,重叠显示从分发规格数据获取到的显示语句,或执行从分发规格数据获取到的显示控制程序。此外,分发规格数据除了这些信息以外,还能够包括由系统独自定义的信息。

[0332] 文件服务器8若登记有重编数据和分发规格数据,则对该登记的重编数据进行加密,生成储存了用于认证数据包的数据包认证符、已加密的重编数据、以及分发规格数据的分发数据包。认证符是为了验证重编数据以及分发规格数据的完整性而赋予的数据,例如根据与CGW13相关联的密钥信息、重编数据以及分发规格数据生成。文件服务器8若从外部接收分发数据包的下载请求,则将该分发数据包发送至DCM12。此外,在图6中,例示出文件服务器8生成储存了重编数据和分发规格数据的分发数据包,将重编数据和分发规格数据作为一个文件同时发送至DCM12的情况,但也可以将重编数据和分发规格数据作为不同的文件发送至DCM12。即,文件服务器8也可以先将分发规格数据发送至DCM12,然后将重编数据发送至DCM12。该情况下,可以对分发规格数据、重编数据分别赋予认证符。

[0333] 如图10所示,DCM12若从文件服务器8下载分发数据包,则使用储存于下载的该分发数据包的数据包认证符,验证已加密的重编数据的完整性。若验证结果为正,则DCM12对已加密的重编数据进行解密。若DCM12将已加密的重编数据解密,则对该解密后的重编数据进行解包(Unpackaging),分割为已加密的差分数据和认证符、DCM用的改写规格数据、CGW用的改写规格数据来提取。在图10中,例示出分割为ECU(ID1)的已加密的差分数据和认证符、ECU(ID2)的已加密的差分数据和认证符、ECU(ID3)的已加密的差分数据和认证符、DCM用的改写规格数据、CGW用的改写规格数据来提取的情况。

[0334] 接下来,参照图11至图22对ECU19的闪存33d进行说明。ECU19的闪存33d根据存储器结构被区分为在1面具有闪存面的单面单独存储器、在伪2面具有闪存面的单面挂起存储器、在实质性的2面具有闪存面的双面存储器。在这之后,将搭载单面单独存储器的ECU19称为单面单独存储器ECU,将搭载单面挂起存储器的ECU19称为单面挂起存储器ECU,将搭载双面存储器的ECU19称为双面存储器ECU。

[0335] 单面单独存储器是在单面具有闪存面的构成,所以没有运用面以及非运用面这样的概念,不能在执行应用程序中改写应用程序。另一方面,单面挂起存储器、双面存储器是在2面具有闪存面的构成,所以有运用面以及非运用面这样的概念,能够在执行运用面的应用程序中改写非运用面的应用程序。双面存储器是在完全分离的2面具有闪存面的构成,所以能够在车辆行驶中等任意时机改写应用程序。单面挂起存储器是将单面单独存储器以伪方式用2面划分的构成,能正常地进行读出、写入的时机有限制,不能在车辆行驶中改写应用程序,能够在IG电源断开的停车中改写应用程序。

[0336] 另外,单面单独存储器、单面挂起存储器、双面存储器分别有嵌入了重编固件的重编固件嵌入型(以下,称为嵌入型)和从外部下载重编固件的重编固件下载型(以下,称为下载型)。重编固件是用于改写应用程序的固件。

[0337] 以下,对各闪存的构成依次进行说明。

[0338] (A)单面单独存储器

[0339] (A—1)嵌入型单面单独存储器

[0340] 参照图11以及图12对嵌入型单面单独存储器进行说明。嵌入型单面单独存储器具有差分引擎工作区域、应用程序区域、以及引导程序区域。在应用程序区域配置有版本信息、参数数据、应用程序、固件、以及通常时向量表。在引导区域配置有引导程序、进展状态点2、进展状态点1、启动判定信息、无线重编固件、有线重编固件、启动判定用程序、以及引导时向量表。

[0341] 如图11所示,微机33在执行车辆控制处理、诊断处理等应用处理的通常动作时,执行启动判定用程序,参照引导时向量表和通常时向量表搜索起始地址,执行应用程序的规定地址。

[0342] 微机33在执行应用程序的改写处理的改写动作时,不执行应用程序而执行无线或者有线重编固件。图12表示使用差分数据作为更新程序来改写应用程序的动作。如图12所示,微机33将应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过嵌入的重编固件中包括的差分引擎,根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则将该新数据写入至存储器的规定地址来改写应用程序。

[0343] (A—2)下载型单面单独存储器

[0344] 参照图13以及图14对下载型单面单独存储器进行说明。下载型与上述的嵌入型相比较,在从外部下载无线重编固件、有线重编固件,并在改写应用程序之后,删除该无线重编固件、有线重编固件的点上不同。在通过无线更新应用程序的情况下,预先例如在图6所示的重编数据中包括由各ECU19执行的无线重编固件。ECU19从CGW13接收自身ECU用的无线重编固件,将接收到的该自身ECU用的无线重编固件保存到RAM。

[0345] 如图13所示,微机33在执行车辆控制处理、诊断处理等应用处理的通常动作时,与嵌入型同样地执行启动判定用程序,参照引导时向量表和通常时向量表搜索起始地址,执行应用程序的规定地址。

[0346] 如图14所示,微机33在执行应用程序的改写处理的改写动作时,使应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过从外部下载的重编固件中包括的差分引擎,根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则写入该新数据来改写应用程序。

[0347] (B)单面挂起存储器

[0348] (B—1)嵌入型单面挂起存储器

[0349] 参照图15以及图16对嵌入型单面挂起存储器进行说明。嵌入型单面挂起存储器具有差分引擎工作区域、应用程序区域、以及引导程序区域。进行程序更新的重编固件与单面单独存储器同样地配置于引导程序区域,不是程序更新的对象。作为程序更新的对象的应用程序区域以伪方式具有A面和B面,在A面和B面分别配置有版本信息、应用程序、以及通常时向量表。在引导区域配置有引导程序、重编固件、重编时向量表、启动面判定功能、启动面判定信息、以及引导时向量表。

[0350] 如图15所示,微机33在执行车辆控制处理、诊断处理等应用处理的通常动作时,执

行引导程序,通过启动面判定功能根据A面和B面的各启动面判定信息判定A面以及B面中的哪个面是运用面。微机33若判定为将A面设为运用面,则参照A面的通常时向量表搜索起始地址,执行A面的应用程序。同样地,微机33若判定为将B面设为运用面,则参照B面的通常时向量表搜索起始地址,执行B面的应用程序。此外,在图15中,将重编固件配置于引导程序区域,但也可以构成为重编固件也为程序更新的对象,而配置于A面或者B面各自的区域。

[0351] 如图16所示,微机33在执行非运用面的应用程序的改写处理的改写动作时,使非运用面的应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过嵌入的重编固件内的差分引擎,根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则将该新数据写入非运用面来改写非运用面的应用程序。在图16中,例示出A面是运用面且B面是非运用面的情况。

[0352] (B—2)下载型单面挂起存储器

[0353] 参照图17以及图18对下载型单面挂起存储器进行说明。下载型与上述的嵌入型相比较,在从外部下载重编固件和重编时向量表,并在改写应用程序之后,删除该重编固件和重编时向量表的点上不同。

[0354] 如图17所示,微机33在执行车辆控制处理、诊断处理等应用处理的通常动作时,与嵌入型同样地,执行引导程序,通过启动面判定功能根据A面和B面的各启动面判定信息判定新旧并判定A面以及B面中的哪个面是运用面。微机33若判定为将A面设为运用面,则参照A面的通常时向量表搜索起始地址,执行A面的应用程序。同样地,微机33若判定为将B面设为运用面,则参照B面的通常时向量表搜索起始地址,执行B面的应用程序。

[0355] 如图18所示,微机33在执行应用程序的改写处理的改写动作时,使非运用面的应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过从外部下载的重编固件内的差分引擎,根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则写入该新数据来改写应用程序。在图18中,例示出A面是运用面且B面是非运用面的情况。像这样,在单面挂起存储器中,能够在执行A面的应用程序的同时在后台执行B面的应用程序的改写。

[0356] (C)双面存储器

[0357] (C—1)嵌入型双面存储器

[0358] 参照图19以及图20对嵌入型双面存储器进行说明。嵌入型单面单独存储器具有A面的应用程序区域以及改写程序区域、B面的应用程序区域以及改写程序区域、以及引导程序区域。在引导区域,引导程序被配置为不能改写。引导程序包括引导交换功能和引导时向量表。在各应用程序区域配置有版本信息、参数数据、应用程序、固件、以及通常时向量表。在各改写程序区域配置有控制改写的程序、重编进展管理信息2、重编进展管理信息1、启动面判定信息、无线重编固件、有线重编固件、以及引导时向量表。在引导区域配置有引导程序、引导交换功能、以及引导时向量表。

[0359] 如图19所示,微机33在执行车辆控制处理、诊断处理等应用处理的通常动作时以及执行非运用面的应用程序的改写处理的改写动作时,都执行引导程序,根据A面和B面的各启动面判定信息通过引导交换功能判定新旧并判定A面以及B面中的哪个面是运用面。微机33若判定为将A面设为运用面,则参照A面的引导时向量表和A面的通常时向量表搜索起

始地址,执行A面的应用程序。同样地,微机33若判定为将B面设为运用面,则参照B面的引导时向量表和B面的通常时向量表搜索起始地址,执行B面的应用程序。

[0360] 如图20所示,微机33在执行非运用面的应用程序的改写处理的改写动作时,使非运用面的应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过嵌入的重编固件内的差分引擎,根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则将该新数据写入非运用面来改写非运用面的应用程序。此外,暂时保存至差分引擎工作区域的旧数据既可以将运用面的应用程序作为对象,也可以将非运用面的应用程序作为对象。此时,在将运用面的应用程序作为对象的情况下,在新数据的写入之前消除非运用面的数据。这里,在从车辆外部获取到的重编数据不是差分数据而是全部数据(全数据)的情况下,将获取到的重编数据作为新数据写入至非运用面。在图20中,例示出A面是运用面且B面是非运用面的情况。此外,暂时保存至差分引擎工作区域的旧数据既可以将运用面的应用程序作为对象,也可以将非运用面的应用程序作为对象。在需要使应用程序的执行地址匹配的情况下,使非运用面的应用程序作为旧数据保存。

[0361] (C—2)下载型双面存储器

[0362] 参照图21以及图22对下载型双面存储器进行说明。下载型与上述的嵌入型相比较,在从外部下载无线重编固件、有线重编固件,并在改写应用程序之后,删除该无线重编固件、有线重编固件的点上不同。

[0363] 如图21所示,微机33在执行车辆控制处理等应用处理、诊断处理的通常动作时以及执行非运用面的应用程序的改写处理的改写动作时,都与嵌入型同样地,执行引导程序,根据A面和B面的各启动面判定信息通过引导交换功能判定新旧并判定A面以及B面中的哪个面是运用面,执行运用面的应用程序来执行应用处理。

[0364] 如图22所示,微机33在执行应用程序的改写处理的改写动作时,使非运用面的应用程序作为旧数据暂时保存至差分引擎工作区域。微机33读出暂时保存至差分引擎工作区域的旧数据,通过从外部下载的重编固件根据读出的该旧数据和存储于RAM33c的差分数据复原新数据。微机33若根据旧数据和差分数据生成新数据,则将该新数据写入至非运用面来改写非运用面的应用程序。此外,暂时保存至差分引擎工作区域的旧数据既可以将运用面的应用程序作为对象,也可以将非运用面的应用程序作为对象。此时,在将运用面的应用程序作为对象的情况下,在新数据的写入之前消除非运用面的数据。这里,在从车辆外部获取到的重编数据不是差分数据而是全部数据(全数据)的情况下,将获取到的重编数据作为新数据写入至非运用面。在图22中,例示出A面是运用面且B面是非运用面的情况。此外,暂时保存至差分引擎工作区域的旧数据既可以将运用面的应用程序作为对象,也可以将非运用面的应用程序作为对象。像这样,在双面存储器中,能够在执行A面的应用程序的同时在后台执行B面的应用程序的改写。

[0365] 如上所述,在嵌入型以及下载型的任意一种构成中,都在各应用区域配置有应用程序和用于改写应用程序的改写程序。此外,在图20以及图22中,示出了应用程序作为重编对象,但也可以改写程序作为重编对象。另外,在希望不能改写改写程序的情况下,也可以将改写程序配置于引导区域。也可以将用于有线改写的程序配置于引导区域以便例如在经销商等中能够可靠地实施经由工具23的通过有线的改写。

[0366] 接下来,参照图23至图25对改写应用程序的整体顺序进行说明。此外,这里,对用户操作作为显示终端5的移动终端6来在停车中改写应用程序的情况进行说明,但操作车载显示器7来在停车中改写应用程序的情况也相同。从中心装置3发送至DCM12的分发数据包储存有一个以上的改写对象ECU19的写入数据。即,在分发数据包中,若改写对象ECU19是一个,则储存有面向该一个改写对象ECU19的一个写入数据,若改写对象ECU19为多个,则储存有面向该多个改写对象ECU19中的每一个的多个写入数据。这里,改写对象ECU19有2个,将2个改写对象ECU19称为改写对象ECU(ID1)以及改写对象ECU(ID2)。另外,将改写对象ECU(ID1)以及改写对象ECU(ID2)以外的ECU19称为其他ECU。

[0367] 改写对象ECU(ID1)以及改写对象ECU(ID2)分别若判定为从主装置11接收到例如版本通知信号的发送请求,则判定为版本通知信号的发送条件成立。若版本通知信号的发送条件成立,则改写对象ECU(ID1)将包括自身存储的应用程序的版本信息和能够识别自身的ECU(ID)的版本通知信号发送至主装置11。主装置11若从改写对象ECU(ID1)接收到版本通知信号,则将接收到的该版本通知信号发送至中心装置3。同样地,若版本通知信号的发送条件成立,则改写对象ECU(ID2)将包括自身存储的应用程序的版本和能够识别自身的ECU(ID)的版本通知信号发送至主装置11。主装置11若从改写对象ECU(ID2)接收到版本通知信号,则将接收到的该版本通知信号发送至中心装置3。

[0368] 中心装置3若从改写对象ECU(ID1)以及改写对象ECU(ID2)接收到版本通知信号,则确定接收到的该版本通知信号所包括的应用程序的版本和ECU(ID),判定有无应该分发至该版本通知信号的发送源的改写对象ECU19的写入数据。中心装置3根据从改写对象接收到的版本通知信号确定出改写对象ECU19的当前的应用程序的版本,对照该当前的应用程序的版本和正在管理的最新的版本。

[0369] 若根据版本通知信号确定出的版本与正在管理的最新的版本是相同的值,则中心装置3判定为没有应该分发至该版本通知信号的发送源的改写对象ECU19的写入数据,不需要更新存储于改写对象ECU19的应用程序。另一方面,若根据版本通知信号确定出的版本是小于正在管理的最新的版本的值,则中心装置3判定为有应该分发至该版本通知信号的发送源的改写对象ECU19的写入数据,需要更新存储于改写对象ECU19的应用程序。

[0370] 中心装置3若判定为需要更新存储于改写对象ECU19的应用程序,则将需要进行更新的主旨通知给移动终端6。若被通知了需要更新的主旨,则移动终端6显示可否分发画面(A1)。可否分发画面与后述的活动通知画面同等。用户能够通过显示于移动终端6的可否分发画面确认需要进行更新的主旨,能够选择是否更新。

[0371] 若用户在移动终端6中选择进行更新的主旨(A2),则移动终端6将分发数据包的下载请求通知给中心装置3。若被从移动终端6通知了分发数据包的下载请求,则中心装置3将分发数据包发送至主装置11。

[0372] 主装置11若从中心装置3下载分发数据包,则对下载的该分发数据包开始数据包认证处理(B1)。主装置11对分发数据包进行认证,若完成数据包认证处理,则开始写入数据提取处理(B2)。主装置11从分发数据包提取出写入数据,若完成写入数据提取处理,则将下载完成通知信号发送至中心装置3。

[0373] 中心装置3若从主装置11接收到下载完成通知信号,则将下载完成通知给移动终端6。若被从中心装置3通知了下载完成,则移动终端6显示下载完成通知画面(A3)。用户能

够通过显示于移动终端6的下载完成通知画面确认下载完成的主旨,能够设定车辆侧的应用程序的改写开始时刻。

[0374] 若用户在移动终端6中设定车辆侧的应用程序的改写开始时刻(A4),则移动终端6将改写开始时刻通知给中心装置3。若被从移动终端6通知了改写开始时刻,则中心装置3将用户设定的该改写开始时刻存储为设定开始时刻。若当前时刻到达设定开始时刻(A5),则中心装置3将改写指示信号发送至主装置11。

[0375] 主装置11若从中心装置3接收改写指示信号,则将电源启动请求发送至电源管理ECU20,使改写对象ECU(ID1)、改写对象ECU(ID2)、其他ECU从停止状态或者睡眠状态转移至启动状态(X1)。

[0376] 主装置11开始向改写对象ECU(ID1)分发写入数据,对改写对象ECU(ID1)指示写入数据的写入。改写对象ECU(ID1)开始从主装置11接收写入数据,若被指示写入数据的写入,则开始写入数据的写入,开始程序改写处理(C1)。改写对象ECU(ID1)若完成从主装置11接收写入数据,完成写入数据的写入,完成程序改写处理,则将改写完成通知信号发送至主装置11。

[0377] 主装置11若从改写对象ECU(ID1)接收到改写完成通知信号,则开始向改写对象ECU(ID2)分发写入数据,对改写对象ECU(ID2)指示写入数据的写入。改写对象ECU(ID2)开始从主装置11接收写入数据,若被指示写入数据的写入,则开始写入数据的写入,开始程序改写处理(D1)。改写对象ECU(ID2)若完成从主装置11接收写入数据,完成写入数据的写入,完成程序改写处理,则将改写完成通知信号发送至主装置11。主装置11若从改写对象ECU(ID2)接收到改写完成通知信号,则将改写完成通知信号发送至中心装置3。

[0378] 中心装置3若从主装置11接收到改写完成通知信号,则将应用程序的改写完成通知给移动终端6。若被从中心装置3通知了应用程序的改写完成,则移动终端6显示改写完成通知画面(A6)。用户能够通过显示于移动终端6的改写完成通知画面确认完成了应用程序的改写的主旨,能够设定同步实施作为激活。

[0379] 若用户在移动终端6中设定同步实施(A7),即,用户设定针对新程序的激活的同意,则移动终端6将同步实施通知给中心装置3。若被从移动终端6通知了同步实施,则中心装置3将同步切换指示信号发送至主装置11。主装置11若从中心装置3接收到同步切换指示信号,则将接收到的该同步切换指示信号分发至改写对象ECU(ID1)以及改写对象ECU(ID2)。

[0380] 改写对象ECU(ID1)以及改写对象ECU(ID2)分别若从主装置11接收到同步切换指示信号,则开始将下次启动的应用程序从旧应用程序切换为新应用程序的程序切换处理(C2、D2)。改写对象ECU(ID1)以及改写对象ECU(ID2)分别若完成程序切换处理,则将切换完成通知信号发送至主装置11。

[0381] 主装置11若从改写对象ECU(ID1)以及改写对象ECU(ID2)接收到切换完成通知信号,则将版本读出信号分发至改写对象ECU(ID1)以及改写对象ECU(ID2)。改写对象ECU(ID1)以及改写对象ECU(ID2)分别若从主装置11接收到版本读出信号,则读出之后运用的应用程序的版本(C3、D3),将包括读出的该版本的最新版本通知信号发送至主装置11。主装置11通过从改写对象ECU(ID1)以及改写对象ECU(ID2)接收版本通知信号,来检查软件的版本,或根据需要进行回滚。

[0382] 主装置11若从改写对象ECU(ID1)以及改写对象ECU(ID2)接收到版本通知信号,则将电源停止请求发送至电源管理ECU20,使改写对象ECU(ID1)、改写对象ECU(ID2)、其他ECU从启动状态转移至停止状态或者睡眠状态(X2)。

[0383] 主装置11将最新版本通知信号发送至中心装置3。中心装置3若从主装置11接收到最新版本通知信号,则根据接收到的该最新版本通知信号确定改写对象ECU(ID1)以及改写对象ECU(ID2)的应用程序的最新的版本,将确定出的该最新的版本通知给移动终端6。若移动终端6被从中心装置3通知了最新的版本,则在移动终端6中显示表示通知的该最新的版本的最新版本通知画面(A8)。用户能够通过显示于移动终端6的最新版本通知画面确认最新的版本,能够确认完成了激活的主旨。

[0384] 接下来,参照图26至图29对改写应用程序的情况下的DCM12、CGW13、改写对象ECU19的动作的时序图进行说明。此外,这里,对在通过用户操作接通了IG开关42的期间中、即车辆能够行驶中改写双面存储器ECU的应用程序,在通过用户操作断开了IG开关42之后的停车中改写单面挂起存储器ECU以及单面单独存储器ECU的应用程序的情况进行说明。另外,对通过电源控制改写应用程序的情况和通过电源自保持改写应用程序的情况进行说明。

[0385] (一)通过电源控制改写应用程序的情况

[0386] 参照图26以及图27对通过电源控制改写应用程序的情况进行说明。通过电源控制进行的应用程序的改写是指不使用电源自保持电路而根据电源的切换来控制改写动作的构成。若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则DCM12、CGW13、双面存储器ECU、单面挂起存储器ECU、单面单独存储器ECU分别开始通常动作(t1)。

[0387] 若被从中心装置3通知了下载开始,则DCM12从通常动作转移至下载动作,开始从中心装置3下载分发数据包(t2)。DCM12可以在进行通常动作的同时在后台进行分发数据包的下载。DCM12若完成从中心装置3下载分发数据包,则从下载动作复原到通常动作(t3)。

[0388] 若被从中心装置3或者CGW13通知了改写指示信号(安装指示信号),则DCM12从通常动作转移至数据传输/中心通信动作,开始数据传输/中心通信动作(t4)。即,DCM12从分发数据包提取写入数据,开始向CGW13传输写入数据,并且从CGW13获取改写的进展状况,开始向中心装置3通知改写的进展状况。

[0389] CGW13若开始从DCM12获取写入数据,则从通常动作转移至重编主动作,开始重编主动作,开始向双面存储器ECU分发写入数据,指示写入数据的写入。双面存储器ECU若开始从CGW13接收写入数据,则在通常动作中开始编程阶段(以下,也称为安装阶段)。即,双面存储器ECU在进行通常动作的同时在后台进行应用程序的安装。双面存储器ECU开始向闪存写入接收到的写入数据,开始应用程序的改写。

[0390] 在双面存储器ECU中改写应用程序的期间,若通过用户将IG开关从接通切换为断开而车辆电源从IG电源切换为+B电源,则DCM12中断数据传输/中心通信动作,CGW13中断重编主动作,双面存储器ECU中断安装阶段,中断应用程序的改写(t5)。

[0391] 然后,若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则DCM12再次开始数据传输/中心通信动作,CGW13再次开始重编主动作,双面存储器ECU再次开始安装阶段,再次开始应用程序的改写(t6)。即,通过用户将IG开关从接通切换为断

开而车辆电源从IG电源切换为+B电源,然后,通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,每当产生断路(Trip),双面存储器ECU都重复应用程序的改写的中断和再次开始(t7,t8)。

[0392] 双面存储器ECU若完成写入数据的写入,完成应用程序的改写,则结束安装阶段,从通常动作转移至等待激活。即,双面存储器ECU在未进行激活阶段的时刻,不在改写了应用程序的新面(B面)启动,保持旧面(A面)启动(t9)。

[0393] 在通过用户将IG开关从接通切换为断开而车辆电源从IG电源切换为+B电源之后(t10),若在该时刻双面存储器ECU完成应用程序的改写,则CGW13将电源启动请求发送至电源管理ECU20。若通过CGW13将电源启动请求发送至电源管理ECU20而车辆电源从+B电源切换为IG电源,则DCM12再次开始数据传输/中心通信动作,CGW13再次开始重编主动作,开始向单面挂起存储器ECU以及单面单独存储器ECU分发写入数据。若单面挂起存储器ECU以及单面单独存储器ECU分别开始从CGW13接收写入数据,则从通常动作转移至引导处理,在引导处理中开始安装阶段(t11)。即,单面挂起存储器ECU以及单面单独存储器ECU不与通常动作并行地进行安装,而在应用程序不动作的引导处理中进行安装。

[0394] 单面挂起存储器ECU若开始应用程序的改写,则在完成应用程序的改写之前通过用户操作而IG开关42从断开切换为接通的情况下,中断应用程序的改写。单面挂起存储器ECU不将中断了应用程序的改写的非运用面(B面),而将运用面(A面)作为启动面来复原。单面单独存储器ECU若开始应用程序的改写,则即使在完成应用程序的改写之前通过用户操作而IG开关42从断开切换为接通,也继续应用程序的改写。这是因为关于单面单独存储器ECU,若在应用程序的改写中途中断,则不能复原为通常动作。优选在开始了单面单独存储器ECU的应用程序的改写之后,到完成应用程序的改写之前使由用户进行的IG开关42操作无效。

[0395] 单面挂起存储器ECU若完成写入数据的写入,完成应用程序的改写,则在引导处理中结束安装阶段,从引导处理转移至等待激活。即,单面挂起存储器ECU在未进行激活阶段的时刻,不在改写了应用程序的新面(B面)启动,保持旧面(A面)启动。单面单独存储器ECU若完成写入数据的写入,完成应用程序的改写,则在引导处理中结束安装阶段,成为等待激活(t12)。

[0396] 若根据来自CGW13的激活指示而电源管理ECU20将车辆电源从IG电源切换为+B电源,则双面存储器ECU以及单面挂起存储器ECU分别进行从旧面向新面的切换,在新面启动,在新面启动中开始后编程阶段(以下,也称为激活阶段)。单面单独存储器ECU开始重启,在安装完成后的重启中开始激活阶段(t13、t14)。在激活中,进行通过新程序正确地启动的确认、向CGW13的版本信息的通知等。

[0397] 若激活完成,根据来自CGW13的激活完成指示而电源管理ECU20将车辆电源从IG电源切换为+B电源,则DCM12从数据传输/中心通信动作转移至睡眠/停止动作,开始睡眠/停止动作。CGW13从重编主动作转移至睡眠/停止动作,开始睡眠/停止动作。双面存储器ECU、单面挂起存储器ECU、单面单独存储器ECU分别从新面启动转移至睡眠/停止动作(t15)。

[0398] 之后,若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则双面存储器ECU以及单面挂起存储器ECU分别将新面(B面)作为启动面并启动新应用程序,单面单独存储器ECU启动新应用程序(t16)。

[0399] (二)通过电源自保持改写应用程序的情况

[0400] 参照图28以及图29对通过电源自保持改写应用程序的情况进行说明。通过电源自保持进行的应用程序的改写是指使用电源自保持电路控制改写动作的构成。若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则DCM12、CGW13、双面存储器ECU、单面挂起存储器ECU、单面单独存储器ECU分别开始通常动作(t21)。

[0401] 若被从中心装置3通知了下载开始,即,被通知有基于新程序的更新,则DCM12从通常动作转移至下载动作,开始从中心装置3下载分发数据包(t22)。若DCM12完成从中心装置3下载分发数据包,则从下载动作复原到通常动作(t23)。

[0402] 若被从中心装置3或者CGW13通知了改写指示信号(安装指示信号),则DCM12从通常动作转移至数据传输/中心通信动作,开始数据传输/中心通信动作(t24)。即,DCM12从分发数据包提取写入数据,开始向CGW13传输写入数据,并且从CGW13获取改写的进展状况,开始向中心装置3通知改写的进展状况。

[0403] CGW13若开始从DCM12获取写入数据,则从通常动作转移至重编主动作,开始重编主动作,开始向双面存储器ECU分发写入数据,指示写入数据的写入。双面存储器ECU若开始从CGW13接收写入数据,则在通常动作中开始编程阶段(以下,也称为安装阶段)。即,双面存储器ECU在进行通常动作的同时在后台进行应用程序的安装。双面存储器ECU开始向闪存写入接收到的写入数据,开始应用程序的改写。

[0404] 在双面存储器ECU中改写应用程序的期间,若通过用户将IG开关从接通切换为断开而车辆电源从IG电源切换为+B电源(t25),则在紧接车辆电源从IG电源切换为+B电源之后,DCM12继续数据传输/中心通信动作,CGW13继续重编主动作,双面存储器ECU继续安装阶段,继续应用程序的改写。若从车辆电源从IG电源切换为+B电源后经过预先设定的时间亦即自保持期间,则DCM12中断数据传输/中心通信动作,CGW13中断重编主动作,双面存储器ECU中断安装阶段,中断应用程序的改写(t26)。即,在从IG开关42断开起经过规定时间之前,通过来自车辆电池40的电力供给继续安装。

[0405] 之后,若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则DCM12再次开始数据传输/中心通信动作,CGW13再次开始重编主动作,双面存储器ECU再次开始安装阶段,再次开始应用程序的改写(t27)。即,通过用户将IG开关从接通切换为断开而车辆电源从IG电源切换为+B电源,然后,用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,每当产生断路,双面存储器ECU都重复应用程序的改写的中断和再次开始(t28～t30)。但是,在从车辆电源从IG电源切换为+B电源起经过自保持期间之前,DCM12继续数据传输/中心通信动作,CGW13继续重编主动作,双面存储器ECU继续安装阶段,继续应用程序的改写。

[0406] 双面存储器ECU若完成写入数据的写入,完成应用程序的改写,则结束安装阶段,从通常动作转移至等待激活。即,双面存储器ECU在未进行激活阶段的时刻,不在改写了应用程序的新面(B面)启动,保持旧面(A面)启动(t31)。

[0407] 若通过用户将IG开关从接通切换为断开而车辆电源从IG电源切换为+B电源,在该时刻在双面存储器ECU中完成应用程序的改写,则单面挂起存储器ECU以及单面单独存储器ECU分别从通常动作转移至引导处理,开始引导处理,在引导处理中开始安装阶段(t32)。

[0408] 单面挂起存储器ECU以及单独存储器ECU若分别完成写入数据的写入,完成应用程

序的改写,则在引导处理中结束安装阶段(t33)。若通过CGW13将电源启动请求发送至电源管理ECU20而车辆电源从+B电源切换为IG电源,则DCM12再次开始数据传输/中心通信动作(t34)。

[0409] 单面挂起存储器ECU若完成写入数据的写入,完成应用程序的改写,则从引导处理转移至等待激活。即,单面挂起存储器ECU在未进行激活阶段的时刻,不在改写了应用程序的新面(B面)启动,保持旧面(A面)启动。单面单独存储器ECU若完成写入数据的写入,完成应用程序的改写,则在引导处理中结束安装阶段,成为等待激活(t35)。

[0410] 若根据来自CGW13的激活指示而电源管理ECU20将车辆电源从IG电源切换为+B电源,则双面存储器ECU以及单面挂起存储器ECU分别进行从旧面向新面的切换,在新面启动,在新面启动中开始激活阶段。单面单独存储器ECU开始重启,在安装完成后的重启中开始激活阶段(t36、t37)。

[0411] 若激活完成,根据来自CGW13的激活完成指示而电源管理ECU20将车辆电源从IG电源切换为+B电源,则DCM12从数据传输/中心通信动作转移至睡眠/停止动作,开始睡眠/停止动作。CGW13从重编主动作转移至睡眠/停止动作,开始睡眠/停止动作。双面存储器ECU、单面挂起存储器ECU以及单面单独存储器ECU分别从新面启动转移至睡眠/停止动作(t38)。

[0412] 在此之后,若通过用户将IG开关从断开切换为接通而车辆电源从+B电源切换为IG电源,则双面存储器ECU以及单面挂起存储器ECU分别将新面(B面)作为启动面并启动新应用程序,单面单独存储器ECU启动新应用程序(t39)。

[0413] CGW13在从中心装置3下载分发数据包之前、向写入数据的改写对象ECU19分发之前进行以下的检查。CGW13在从中心装置3下载分发数据包之前,进行电波环境、车辆电池40的电池余量、DCM12的存储器容量的检查,以便能正常地进行下载。CGW13在向写入数据的改写对象ECU19分发之前,作为用于以免使安装环境不稳定的有人环境的检查,进行侵入传感器的检测、车锁的检测、窗帘的检测、IG断开的检测,作为改写对象ECU19是否能够写入的检查,进行版本、异常产生的检查,以便能正常地进行写入数据的分发。另外,作为分发至改写对象ECU19的写入数据的检查,CGW13在开始安装之前,进行篡改检查、访问认证、版本检查等,在执行安装的期间,进行通信中断检查、异常产生的检查等,在完成安装之后,进行版本检查、完整性检查、DTC(Diagnostic Trouble Code,错误代码)检查等。

[0414] 接下来,参照图30至图46对显示终端5显示的画面进行说明。如图30所示,在通过OTA对改写对象ECU19的应用程序进行改写的构成中,有活动通知、下载、安装、激活的阶段。活动通知是指程序更新的通知。例如接受在中心装置3中判断为有应用程序的更新,主装置11下载分发规格数据等是活动通知。显示终端5随着应用程序的改写进展而在各阶段中显示画面。此外,这里,对车载显示器7显示的画面进行说明。

[0415] 如图31所示,CGW13在活动通知前的通常时,例如使作为导航功能之一的公知的路径引导画面等导航画面501显示于车载显示器7。若从该状态产生活动通知,则如图32所示,CGW13使表示产生活动通知的活动通知图标501a显示于导航画面501的右下。用户通过确认活动通知图标501a的显示,能够把握与应用程序的更新有关的活动通知的产生。

[0416] 若用户从该状态操作活动通知图标501a,则如图33所示,CGW13使活动通知画面502弹出显示在导航画面501上。此外,CGW13并不局限于使活动通知画面502弹出显示,也可以采用其他的显示方式。CGW13在活动通知画面502中,例如显示“有能利用的软件更新”的

引导来将活动通知的产生通知给用户,并且使“确认”按钮502a、“稍后”按钮502b显示,等待用户的操作。该情况下,用户通过操作“确认”按钮502a,能够进入用于使应用程序的改写开始的下一画面。此外,CGW13在用户操作了“稍后”按钮502b的情况下,使活动通知画面502的弹出显示消除,返回至图32所示的显示活动通知图标501a的画面。

[0417] 若用户从该状态操作“确认”按钮502a,则如图34所示,CGW13将显示从导航画面501切换为下载同意画面503,使下载同意画面503显示于车载显示器7。CGW13在下载同意画面503中,将活动ID、更新名称通知给用户,并且使“下载开始”按钮503a、“详细确认”按钮503b、“返回”按钮503c显示,等待用户的操作。该情况下,用户通过操作“下载开始”按钮503a,能够使下载开始,通过操作“详细确认”按钮503b,能够使下载的详细显示,通过使“返回”按钮503c显示,能够拒绝下载,返回至前一画面。在操作了“返回”按钮503c的情况下,并且用户通过操作活动通知图标501a,能够进入用于开始下载的画面。

[0418] 若用户从使该下载同意画面503显示的状态操作“详细确认”按钮503b,则如图35所示,CGW13切换下载同意画面503的显示内容,使下载的详细显示于车载显示器7。作为下载的详细,CGW13使用接收到的分发规格数据,使更新内容、更新所需时间、伴随更新的车辆功能的限制等显示。另外,若用户操作“下载开始”按钮503a,则CGW13经由DCM12开始分发数据包的下载。与开始分发数据包的下载并行地,如图36所示,CGW13将显示从下载同意画面503切换为导航画面501,使导航画面501再次显示于车载显示器7,使表示下载执行中的下载执行中图标501b显示于导航画面501的右下。用户通过确认下载执行中图标501b的显示,能够把握分发数据包的下载执行中。

[0419] 若用户从该状态操作下载执行中图标501b,则如图37所示,CGW13将显示从导航画面501切换为下载执行中画面504,使下载执行中画面504显示于车载显示器7。CGW13在下载执行中画面504中,将下载的执行中通知给用户,并且使“详细确认”按钮504a、“返回”按钮504b以及“取消”按钮504c显示,等待用户的操作。该情况下,用户通过操作“详细确认”按钮504a,能够使下载执行中的详细显示,通过操作“取消”按钮504c,能够使下载中断。

[0420] CGW13若完成下载,则如图38所示,使下载完成通知画面505弹出显示在导航画面501上。CGW13在下载完成通知画面505中,例如显示“下载已完成。能够进行软件更新”的引导来将下载的完成通知给用户,并且使“确认”按钮505a、“稍后”按钮505b显示,等待用户的操作。该情况下,用户通过操作“确认”按钮505a,能够进入用于开始安装的画面。

[0421] 若用户从该状态操作“确认”按钮505a,则如图39所示,CGW13将显示从导航画面501切换为安装同意画面506,使安装同意画面506显示于车载显示器7。CGW13在安装同意画面506中,将与安装有关的所需时间、限制事项以及时间表的设定通知给用户,并且使“立即更新”按钮506a、“予约更新”按钮506b、“返回”按钮506c显示,等待用户的操作。该情况下,用户能够通过操作“立即更新”按钮506a,来使安装立刻开始。另外,用户通过设定希望执行安装的时刻,并操作“予约更新”按钮506b,能够以预约的方式开始安装。另外,用户通过操作“返回”按钮506c,能够拒绝安装,返回至前一画面。在操作了“返回”按钮506c的情况下,并且用户通过操作下载执行中图标501b,能够进入至用于开始安装的画面。

[0422] 若用户从该状态操作“立即更新”按钮506a,则如图40所示,CGW13切换安装同意画面506的显示内容,使安装的详细显示于车载显示器7。CGW13在这里的安装同意画面506中,将受理安装的请求并开始安装的主旨通知给用户。

[0423] CGW13若开始安装,则如图41所示,将显示从安装同意画面506切换为导航画面501,使导航画面501再次显示于车载显示器7,使表示安装执行中的安装执行中图标501c显示于导航画面501的右下。用户通过确认安装执行中图标501c的显示,能够把握安装执行中。

[0424] 若用户从该状态操作安装执行中图标501c,则如图42所示,CGW13将显示从导航画面501切换为安装执行中画面507,使安装执行中画面507显示于车载显示器7。CGW13在安装执行中画面507中,将安装的执行中通知给用户。CGW13也可以例如使安装的所需剩余时间、进展百分比显示于安装执行中画面507。

[0425] CGW13若完成安装,则如图43所示,将显示从导航画面501切换为激活同意画面508,使激活同意画面508显示于车载显示器7。CGW13在激活同意画面508中,将激活的内容通知给用户,并且使“返回”按钮508a以及“OK”按钮508b显示,等待用户的操作。该情况下,用户通过操作“返回”按钮508a,能够拒绝激活,返回至前一画面。另外,用户通过操作“OK”按钮508b,能够同意激活。此外,在操作了“返回”按钮508a的情况下,并且用户通过操作安装执行中图标501c,能够进入至用于执行激活的画面。此外,关于这些显示、同意,也能够根据用户的设定、程序的场景不显示而省略。

[0426] 若用户在从用户操作了“OK”按钮508b后的状态接通IG电源,则如图44所示,CGW13使激活完成通知画面509弹出显示在导航画面501上。CGW13在激活完成通知画面509中,例如显示“软件更新完成”的引导来将激活的完成通知给用户,并且使“OK”按钮509a、“详细确认”按钮509b显示,等待用户的操作。该情况下,用户通过操作“OK”按钮509a,能够使激活完成通知画面509的弹出显示消除,通过操作“详细确认”按钮509b,能够使激活的完成的详细显示。

[0427] 若用户从该状态操作“OK”按钮509a,则如图45所示,CGW13将显示从导航画面501切换为确认操作画面510,使确认操作画面510显示于车载显示器7。CGW13在确认操作画面510中,将激活的完成通知给用户,并且使“详细确认”按钮510a、“OK”按钮510b显示,等待用户的操作。该情况下,用户通过操作“详细确认”按钮510a,能够使激活的完成的详细显示。

[0428] 若用户从该状态操作“详细确认”按钮510a,则如图46所示,CGW13切换确认操作画面510的显示内容,使激活完成的详细显示于车载显示器7。CGW13将通过更新而追加的功能、变更的功能等作为更新详细显示,并且显示“OK”按钮510b。CGW13根据用户操作了“OK”按钮509a、510b,判断为用户确认了软件更新完成。

[0429] 如以上说明那样,车辆侧系统4控制活动通知、下载、安装、激活、更新完成这样的各动作阶段,并且向用户提示与各动作阶段匹配的显示。此外,在上述的说明中,构成为CGW13进行显示的控制,但也可以构成为车载显示器7从CGW13接收动作阶段、分发规格数据并进行显示。

[0430] 接下来,参照图47至图233对车辆用程序改写系统1进行的特征性处理进行说明。车辆用程序改写系统1进行以下所示的特征性处理。

[0431] (1)分发数据包的发送判定处理

[0432] (2)分发数据包的下载判定处理

[0433] (3)写入数据的传输判定处理

[0434] (4)写入数据的获取判定处理

[0435] (5)安装的指示判定处理

[0436] (6)安全访问密钥的管理处理

[0437] (7)写入数据的验证处理

[0438] (8)数据储存面信息的发送控制处理

[0439] (9)非改写对象的电源管理处理

[0440] (10)文件的传输控制处理

[0441] (11)写入数据的分发控制处理

[0442] (12)激活请求的指示处理

[0443] (13)激活的执行控制处理

[0444] (14)改写对象的组管理处理

[0445] (15)回滚的执行控制处理

[0446] (16)改写进展状况的显示控制处理

[0447] (17)差分数据的匹配性判定处理

[0448] (18)改写的执行控制处理

[0449] (19)会话的确立处理

[0450] (20)重试点的确定处理

[0451] (21)进展状态的同步控制处理

[0452] (22)显示控制信息的发送控制处理

[0453] (23)显示控制信息的接收控制处理

[0454] (24)进展显示的画面显示控制处理

[0455] (25)程序更新的报告控制处理

[0456] (26)电源自保持的执行控制处理

[0457] 中心装置3、DCM12、CGW13、ECU19、车载显示器7分别具有以下的功能模块作为进行上述的(1)～(26)的特征性处理的构成。

[0458] 如图47所示,中心装置3具有分发数据包发送部51。分发数据包发送部51若从DCM12接收分发数据包的下载请求,则将分发数据包发送至DCM12。作为进行特征性处理的构成,除了上述的构成之外,中心装置3还具有分发数据包的发送判定部52、进展状态的同步控制部53、显示控制信息的发送控制部54、以及写入数据选定部55(相当于更新数据选定部)。写入数据选定部55(相当于更新数据选定部)若从主装置11接收到数据储存面信息,则基于根据接收到的该数据储存面信息确定出的软件版本以及运用面,选定适合非运用面的写入数据。即,分发数据包发送部51将包括由写入数据选定部55选定的写入数据的分发数据包发送至DCM12。将在后面描述进行特征性处理的功能模块。

[0459] 如图48所示,DCM12具有下载请求发送部61、分发数据包下载部62、写入数据提取部63、写入数据传输部64、改写规格数据提取部65、以及改写规格数据传输部66。下载请求发送部61将分发数据包的下载请求发送至中心装置3。分发数据包下载部62从中心装置3下载分发数据包。若通过分发数据包下载部62从中心装置3下载了分发数据包,则写入数据提取部63从下载的该分发数据包提取写入数据。

[0460] 若通过写入数据提取部63从从分发数据包提取出写入数据,则写入数据传输部64将提取的该写入数据传输至CGW13。若通过分发数据包下载部62从中心装置3下载了分发数

据包,则改写规格数据提取部65从下载的该分发数据包提取改写规格数据。若通过改写规格数据提取部56从分发数据包提取出改写规格数据,则改写规格数据传输部66将提取出的该改写规格数据传输至CGW13。作为进行特征性处理的构成,除了上述的构成之外,DCM12还具有分发数据包的下载判定部67和写入数据的传输判定部68。将在后面描述进行特征性处理的功能模块。

[0461] 如图49以及图50所示,CGW13具有获取请求发送部71、写入数据获取部72(相当于更新数据存储部)、写入数据分发部73(相当于更新数据分发部)、改写规格数据获取部74、以及改写规格数据解析部75。写入数据获取部72通过写入数据被从DCM12传输,来从DCM12获取写入数据。若写入数据由写入数据获取部72获取,则当成为该写入数据的分发时机时,写入数据分发部73将获取到的该写入数据分发至改写对象ECU19。改写规格数据获取部74通过改写规格数据被从DCM12传输,来从DCM12获取改写规格数据。若改写规格数据由改写规格数据获取部74获取,则改写规格数据解析部75解析获取到的该改写规格数据。

[0462] 作为进行特征性处理的构成,除了上述的构成之外,CGW13还具有写入数据的获取判定部76、安装的指示判定部77、安全访问密钥的管理部78、写入数据的验证部79、数据储存面信息的发送控制部80、非改写对象的电源管理部81、文件的传输控制部82、写入数据的分发控制部83、激活请求的指示部84、改写对象的组管理部85、回滚的执行控制部86、改写进展状况的显示控制部87、进展状态的同步控制部88、显示控制信息的接收控制部89、进展显示的画面显示控制部90、程序更新的报告控制部91、以及电源自保持的执行控制部92。将在后面描述进行特征性处理的功能模块。

[0463] 如图51所示,ECU19具有写入数据接收部101和程序改写部102。写入数据接收部101从CGW13接收写入数据。若通过写入数据接收部101从CGW13接收到写入数据,则程序改写部102将接收到的该写入数据写入闪存来改写应用程序。作为进行特征性处理的构成,除了上述的构成之外,ECU19还具有差分数据的匹配性判定部103、改写的执行控制部104、会话的确立部105、重试点的确定部106、激活的执行控制部107、以及电源自保持的执行控制部108。将在后面描述进行特征性处理的功能模块。

[0464] 如图52所示,车载显示器7具有分发规格数据的接收控制部111。分发规格数据的接收控制部111控制分发规格数据的接收。

[0465] 以下,对上述的(1)~(26)的各处理依次进行说明。

[0466] (1)分发数据包的发送判定处理、(2)分发数据包的下载判定处理

[0467] 参照图53以及图54对中心装置3中的分发数据包的发送判定处理参进行说明,参照图55以及图56对主装置11中的分发数据包的下载判定处理进行说明。

[0468] 如图53所示,中心装置3在分发数据包的发送判定部52中具有软件信息获取部52a、更新有无判定部52b、更新适合与否判定部52c、以及活动信息发送部52d。软件信息获取部52a从车辆侧获取各ECU19的软件信息。具体而言,软件信息获取部52a从车辆侧获取包括版本、写入面等软件信息和硬件信息的ECU结构信息。软件信息获取部52a也可以从车辆侧与这些ECU结构信息一并获取故障代码、防盗报警功能的设定、许可协议信息等车辆状态信息。

[0469] 若通过软件信息获取部52a获取软件信息,则更新有无判定部52b基于获取到的该软件信息判定有无针对车辆的更新数据。即,更新有无判定部52b比较获取到的该软件信息

的版本和自身管理的最新的软件信息的版本,判定两者是否一致,判定有无针对车辆的更新数据。更新有无判定部52b若判定为两者一致,则判定为没有针对车辆的更新数据,若判定为两者不一致,则判定为有针对车辆的更新数据。

[0470] 若由更新有无判定部52b判定为有针对车辆的更新数据,则更新适合与否判定部52c判定车辆状态是否是适合使用分发数据包的程序等的更新的状态。具体而言,更新适合与否判定部52c判定许可协议是否成立、车辆位置是否在由用户预先登记的规定范围内、车辆的报警功能的设定是否被有效化、ECU19的故障信息是否产生,判定车辆状态是否是适合分发数据包的下载的状态。即,更新适合与否判定部52c判定是否是有成为违反用户的意图的更新的可能性的车辆、有即使假设下载成功也在下载后的安装中失败的可能性的车辆。

[0471] 更新适合与否判定部52c若判定为是许可协议成立、车辆位置在由用户预先登记的规定范围内、车辆的报警功能的设定被有效化、未产生ECU19的故障信息的状态,则判定为车辆状态是适合使用分发数据包的程序等的更新的状态。更新适合与否判定部52c若判定为是许可协议不成立、车辆位置不在由用户预先登记的规定范围内、车辆的报警功能的设定未被有效化、产生ECU19的故障信息中的至少任一项,则判定为车辆状态不是适合使用分发数据包的程序等的更新的状态。

[0472] 若由更新适合与否判定部52c判定为车辆状态是适合使用分发数据包的程序等的更新的状态,则活动信息发送部52d将活动信息发送至主装置11。若由更新适合与否判定部52c判定为车辆状态不是适合使用分发数据包的程序等的更新的状态,则活动信息发送部52d不将活动信息发送至主装置11。活动信息发送部52d通过进行上述的判定,来预先存储与未将活动信息发送至主装置11的车辆有关的信息。此外,也可以在中心装置3中显示与未将活动信息发送至主装置11的车辆有关的信息。

[0473] 接下来,参照图54对中心装置3中的分发数据包的发送判定部52的作用进行说明。中心装置3执行分发数据包的发送判定程序,进行分发数据包的发送判定处理。

[0474] 中心装置3若开始分发数据包的发送判定处理,则从车辆侧获取软件信息(S101,相当于软件信息获取步骤)。即,中心装置3判定是否有针对车辆的软件更新。中心装置3基于获取到的该软件信息判定有无针对车辆的更新数据(S102,相当于更新有无判定步骤)。中心装置3若判定为有针对车辆的更新数据(S102:是),则判定车辆状态是否是适合使用分发数据包的程序等的更新的状态(S103,相当于更新适合与否判定步骤)。中心装置3若判定为车辆状态是适合使用分发数据包的程序等的更新的状态(S103:是),则将活动信息发送至主装置11(S104,相当于活动信息发送步骤),结束分发数据包的发送判定处理。

[0475] 中心装置3若判定为没有针对车辆的更新数据(S102:否),则将不是分发数据包的发送对象的主旨、即没有应用程序的更新的主旨发送至主装置11(S105),结束分发数据包的发送判定处理。中心装置3若判定为车辆状态不是适合使用分发数据包的程序等的更新的状态(S103:否),则将不适合程序等的更新的主旨及其理由发送至主装置11(S106),结束分发数据包的发送判定处理。该情况下,主装置11使不适合程序等的更新的主旨及其理由显示于车载显示器7。例如若许可协议不成立,则主装置11例如使“由于许可无效而不能更新程序。请咨询经销商。”等显示于车载显示器7。由此,能够将不适合程序等的更新的主旨的理由提示给用户,能够将适当的信息提示给用户。

[0476] 如以上说明那样,中心装置3通过在向主装置11发送分发数据包之前,在活动信息

的发送之前,进行分发数据包的发送判定处理,从而能够判定是否是适合使用分发数据包的程序等的更新的状态。而且,中心装置3能够仅在判定为是适合使用分发数据包的程序等的更新的状态的情况下为了将分发数据包发送至主装置11而将活动信息发送至主装置11。

[0477] 作为适合使用分发数据包的程序等的更新的情况,而在许可协议成立、车辆位置在由用户预先登记的规定范围内、车辆的报警功能的设定被有效化、ECU19的故障信息未产生的情况下,中心装置3能够将活动信息发送至主装置11。即,中心装置3能够避免在许可协议不成立、或车辆位置在远离自家的位置等的规定范围外、或车辆的报警功能的设定被无效化、或产生ECU19的故障信息的情况下,将活动信息发送至主装置11的事态。这样,对于有成为违反用户的意图的更新的可能性的车辆、有即使假设下载成功也在安装中失败的可能性的车辆,中心装置3能够不使活动信息发送至主装置11。

[0478] 此外,中心装置3也可以在分发数据包的发送中进行分发数据包的发送判定处理。该情况下,中心装置3若在分发数据包的发送中判定为车辆状态是适合使用分发数据包的程序等的更新的状态,则继续分发数据包的发送,但若在分发数据包的发送中判定为车辆状态不是适合使用分发数据包的程序等的更新的状态,则中断分发数据包的发送。即,若在分发数据包的发送中例如产生ECU19的故障信息,则中心装置3中断分发数据包的发送。

[0479] 接下来,对接收到从中心装置3发送的活动信息的主装置11的处理进行说明。参照图55以及图56对主装置11中的分发数据包的下载判定处理进行说明。车辆用程序改写系统1在主装置11中进行分发数据包的下载判定处理。上述的(1)分发数据包的发送判定处理是中心装置3在下载阶段之前的活动通知阶段进行的判定处理,但分发数据包的下载判定处理是主装置11在下载阶段进行的判定处理。此外,在本实施方式中,对在主装置11中DCM12进行分发数据包的下载判定处理的情况进行说明,但也可以CGW13具有DCM12的功能,从而CGW13进行分发数据包的下载判定处理。

[0480] 如图55所示,DCM12在分发数据包的下载判定部67中具有活动信息接收部67a、可下载判定部67b、以及下载执行部67c。活动信息接收部67a从中心装置3接收活动信息。此外,若从中心装置3接收到活动信息,则显示图32所示的活动通知图标501a。若由活动信息接收部67a接收到活动信息,则可下载判定部67b判定车辆状态是否是能够下载分发数据包的状态。即,可下载判定部67b判定用于与中心装置3进行通信的电波环境是否良好、车辆电池40的电池余量是否为规定容量以上、DCM12的存储器空闲容量是否为规定容量以上,判定车辆状态是否是能够下载分发数据包的状态。

[0481] 可下载判定部67b若判定为电波环境良好、车辆电池40的电池余量为规定容量以上、DCM12的存储器空闲容量为规定容量以上,则判定为车辆状态是能够下载分发数据包的状态。可下载判定部67b若判定为电波环境不良好、车辆电池40的电池余量不为规定容量以上、DCM12的存储器空闲容量不为规定容量以上中的至少任一项,则判定为车辆状态不是能够下载分发数据包的状态。

[0482] 这样,可下载判定部67b判定是否有不能正常地完成下载的可能性。此外,以在图34以及图35所示的下载同意画面503中由用户操作了“下载开始”按钮503a作为条件,来进行可下载判定部67b的判定。另外,可下载判定部67b也可以构成为也判定中心装置3中的判定项目。即,可下载判定部67b在例如车辆的报警功能的设定被有效化的情况、未产生ECU19的故障信息的情况下,判定为是能够下载的状态。

[0483] 若由可下载判定部67b判定为车辆状态是能够下载分发数据包的状态,则下载执行部67c从中心装置3下载分发数据包。即,下载执行部67c在确认了能够正常地完成下载之后,执行分发数据包的下载。

[0484] 若由可下载判定部67b判定为车辆状态不是能够下载分发数据包的状态,则下载执行部67c不从中心装置3下载分发数据包。即,下载执行部67c在有不能正常地完成下载的可能性的情况下,不执行分发数据包的下载。该情况下,下载执行部67c对车载显示器7指示在导航画面501显示表示不能开始下载的主旨及其理由的弹出画面。

[0485] 接下来,参照图56对主装置11中的分发数据包的下载判定部67的作用进行说明。主装置11执行分发数据包的下载判定程序,进行分发数据包的下载判定处理。

[0486] 主装置11若开始分发数据包的下载判定处理,则从中心装置3接收活动信息(S201,相当于活动信息接收步骤)。主装置11判定车辆状态是否是能够下载分发数据包的状态(S202,相当于可下载判定步骤)。主装置11若判定为车辆状态是能够下载分发数据包的状态(S202:是),则从中心装置3下载与该活动对应的分发数据包(S203,相当于下载执行步骤),结束分发数据包的下载判定处理。主装置11若判定为车辆状态不是能够下载分发数据包的状态(S202:否),则不从中心装置3下载分发数据包,结束分发数据包的下载判定处理。

[0487] 如以上说明那样,主装置11能够通过在从中心装置3下载分发数据包之前进行分发数据包的下载判定处理,来判定车辆状态是否是能够下载分发数据包的状态。而且,主装置11能够仅在车辆状态是能够下载分发数据包的状态的情况下下载分发数据包。

[0488] 作为适合分发数据包的下载的情况,而在电波环境良好、车辆电池40的电池余量为规定容量以上、DCM12的存储器空闲容量为规定容量以上的情况下,主装置11能够从中心装置3下载分发数据包。即,能够避免在电波环境不良好、或车辆电池40的电池余量小于规定容量、或DCM12的存储器空闲容量小于规定容量的情况下,从中心装置3下载分发数据包的事态。

[0489] 此外,主装置11也可以在分发数据包的下载中进行分发数据包的下载判定处理。该情况下,主装置11若在分发数据包的下载中判定为车辆状态是能够下载分发数据包的状态,则继续从中心装置3下载分发数据包,但若在分发数据包的下载中判定为车辆状态不是能够下载分发数据包的状态,则中断从中心装置3下载分发数据包。即,若在分发数据包的下载中例如电波环境不良好、或车辆电池40的电池余量小于规定容量、或DCM12的存储器空闲容量小于规定容量,则主装置11中断分发数据包的下载。

[0490] 这样,通过在中心装置3中判定是否是有成为违反用户的意图的更新的可能性的车辆、有安装失败的可能性的车辆,并且在主装置11中判定是否有下载失败的可能性,从而能够抑制从中心装置3向主装置11的无用的活动信息或分发数据包的发送。

[0491] 中心装置3具有以下的构成。具备:软件信息获取部52a,从车辆侧获取电子控制装置的软件信息;更新有无判定部52b,基于由上述软件信息获取部获取到的软件信息,判定有无针对车辆的更新数据;更新适合与否判定部52c,在由上述更新有无判定部判定为有更新数据的情况下,判定车辆状态是否是适合更新的状态;以及活动信息发送部52d,在由上述更新适合与否判定部判定为车辆状态是适合更新的状态的情况下,将与更新有关的活动信息发送至车辆用主装置。

[0492] 主装置11具有以下的构成。具备:活动信息接收部67a,从中心装置接收活动信息;可下载判定部67b,在由上述活动信息接收部接收到活动信息的情况下,判定车辆状态是否是能够下载分发数据包的状态;以及下载执行部67c,在由上述可下载判定部判定为车辆状态是能够下载分发数据包的状态的情况下,从中心装置下载分发数据包。

[0493] (3)写入数据的传输判定处理、(4)写入数据的获取判定处理、(5)安装的指示判定处理

[0494] 参照图57以及图58对写入数据的传输判定处理进行说明,参照图59以及图60对写入数据的获取判定处理进行说明,参照图61至图64对安装的指示判定处理进行说明。车辆用程序改写系统1在DCM12中进行写入数据的传输判定处理。这里,设为从中心装置3发送至DCM12的分发数据包被解包,从分发数据包提取出写入数据的状态。

[0495] 如图57所示,DCM12在写入数据的传输判定部68中具有获取请求接收部68a和通信状态判定部68b。获取请求接收部68a从CGW13接收写入数据的获取请求。若由获取请求接收部68a接收到写入数据的获取请求,则通信状态判定部68b例如在用户预先设定的传输可否判定标志为第一规定值的情况下,判定中心装置3与DCM12之间的数据通信的状态。传输可否判定标志例如在安装时检查规定条件的情况下为1(第一规定值),在省略检查的情况下为0(第二规定值)。写入数据传输部64将由通信状态判定部68b判定为中心装置3与DCM12之间的数据通信处于连接状态作为条件来将写入数据传输至CGW13。

[0496] 接下来,参照图58对DCM12中的写入数据的传输判定部68的作用进行说明。DCM12执行写入数据的传输判定程序,进行写入数据的传输判定处理。这里,对根据来自中心装置3的安装指示,CGW13对DCM12请求获取写入数据的情况的处理进行说明。

[0497] DCM12若判定为从CGW13接收到写入数据的获取请求,则开始写入数据的传输判定处理。DCM12若开始写入数据的传输判定处理,则判定传输可否判定标志(S301、S302)。DCM12若判定为传输可否判定标志是第一规定值(S301:是),则判定中心装置3与自身之间的数据通信的状态(S303)。DCM12若判定为中心装置3与自身之间的数据通信处于连接状态(S303:是),则将写入数据传输至CGW13(S304),结束写入数据的传输判定处理。DCM12若判定为中心装置3与自身之间的数据通信不处于连接状态而处于中断状态(S303:否),则不将写入数据传输至CGW13,结束写入数据的传输判定处理。

[0498] 另外,DCM12若判定为传输可否判定标志为第二规定值(S302:是),则不判定中心装置3与自身之间的数据通信的状态而将写入数据传输至CGW13,结束写入数据的传输判定处理。

[0499] 如以上说明那样,DCM12通过在向CGW13传输写入数据之前进行写入数据的传输判定处理,来在传输可否判定标志为第一规定值的情况下判定中心装置3与自身之间的数据通信的状态。DCM12若判定为数据通信处于连接状态,则开始写入数据的传输,若判定为数据通信处于中断状态,则不开始写入数据的传输而待机。在能够进行与中心装置3的数据通信的状况下,能够将写入数据传输至CGW13,能够在改写对象ECU19中执行安装。

[0500] 例如在改写对象ECU19为多个,安装需要时间的情况下,能够将安装的进展状况从车载侧系统4通知给中心装置3,能够在移动终端6逐一显示进展状况。此外,DCM12也可以在写入数据的传输中进行写入数据的传输判定处理。该情况下,DCM12若在写入数据的传输中判定为数据通信处于连接状态,则继续写入数据的传输,但若在写入数据的传输中判定为

数据通信处于中断状态,则中断写入数据的传输。

[0501] 接下来,对写入数据的获取判定处理进行说明。车辆用程序改写系统1在CGW13中进行写入数据的获取判定处理。上述的(3)写入数据的传输判定处理是在安装阶段由DCM12进行的判定处理,写入数据的获取判定处理是在相同的安装阶段由CGW13进行的判定处理。

[0502] 如图59所示,CGW13在写入数据的获取判定部76中具有事件产生判定部76a和通信状态判定部76b。事件产生判定部76a判定来自中心装置3的写入数据的获取请求(安装指示)的事件产生。若由事件产生判定部76a判定为写入数据的获取请求的事件产生,则通信状态判定部76b例如在用户预先设定的获取可否判定标志为第一规定值的情况下,判定中心装置3与DCM12之间的数据通信的状态。获取可否判定标志例如在安装时检查规定条件的情况下为1(第一规定值),在省略检查的情况下为0(第二规定值)。这里,事件产生判定部76a也可以基于用户指示了安装来判定事件产生,例如若接受用户通过车载显示器7进行了安装的指示操作(参照图39)的通知,则判定为产生写入数据的获取请求的事件。

[0503] 接下来,参照图60对CGW13中的写入数据的获取判定部76的作用进行说明。CGW13执行写入数据的获取判定程序,进行写入数据的获取判定处理。

[0504] CGW13若判定写入数据的获取请求的事件产生,则开始写入数据的获取判定处理。CGW13若开始写入数据的获取判定处理,则判定获取可否判定标志(S401、S402)。CGW13若判定为获取可否判定标志为第一规定值(S401:是),则判定中心装置3与DCM12之间的数据通信的状态(S403)。CGW13若判定为中心装置3与DCM12之间的数据通信是连接(S403:是),则将写入数据的获取请求发送至DCM12(S404),结束写入数据的获取判定处理。在此之后,CGW13若被从DCM12传输写入数据,则将传输的该写入数据分发至改写对象ECU19。CGW13若判定为中心装置3与DCM12之间的数据通信不是连接而是中断(S403:否),则不将写入数据的获取请求发送至DCM12,结束写入数据的获取判定处理。

[0505] 另外,CGW13若判定为获取可否判定标志为第二规定值(S402:是),则不判定中心装置3与DCM12之间的数据通信的状态而将写入数据的获取请求发送至DCM12,结束写入数据的获取判定处理。

[0506] 如以上说明那样,CGW13通过在从DCM12获取写入数据之前进行写入数据的获取判定处理,来在获取可否判定标志为第一规定值的情况下判定中心装置3与DCM12之间的数据通信的状态。CGW13若判定为数据通信处于连接状态,则开始写入数据的获取,若判定为数据通信处于中断状态,则不开始写入数据的获取而待机。在能够进行与中心装置3的通信的状况下,能够从DCM12获取写入数据,能够在改写对象ECU19中执行安装。

[0507] 例如在改写对象ECU19为多个,安装需要时间的情况下,能够将安装的进展状况从车载侧系统4通知给中心装置3,能够在移动终端6逐一显示进展状况。此外,CGW13也可以在写入数据的获取中进行写入数据的获取判定处理。该情况下,若在写入数据的获取中判定为数据通信处于连接状态,则CGW13继续写入数据的获取,但若在写入数据的获取中判定为数据通信处于中断状态,则CGW13中断写入数据的获取。

[0508] 接下来,更详细地对上述的写入数据的获取判定进行说明。写入数据的获取是与安装有关的处理之一,这里,参照图61至图64对安装的指示判定处理进行说明。车辆用程序改写系统1在CGW13中进行安装的指示判定处理。上述的(1)分发数据包的发送判定处理、(2)分发数据包的下载判定处理是在下载阶段进行的判定处理,(3)写入数据的传输判定处

理、(4)写入数据的获取判定处理是在下载完成后的安装阶段进行的处理,(5)安装的指示判定处理是在安装阶段以及激活阶段进行的处理。这里,设为分发数据包被下载到DCM12,并且如图10所示,向写入对象ECU19的写入数据(更新数据、差分数据)被解包的状态。

[0509] 如图61所示,CGW13在安装的指示判定部77中具有安装条件判定部77a、安装指示部77b、车辆状态信息获取部77c、激活条件判定部77d、以及激活指示部77e。安装条件判定部77a判定第一条件、第二条件、第三条件、第四条件、第五条件是否成立。第一条件是获得了与安装有关的用户同意这样的条件。与安装有关的用户同意表示例如在图39所示的画面中用户对安装的同意操作(例如按下“立即更新”按钮506a)。或者,也可以将从下载到激活视为一个更新,作为用户对更新的同意操作。

[0510] 第二条件是CGW13能够与中心装置3进行数据通信这样的条件。第三条件是车辆状态为能够安装这样的条件。第四条件是改写对象ECU19为能够安装这样的条件。这里,第四条件不仅包括安装对象的改写对象ECU19能够安装,也包括与该安装对象的改写对象ECU19协作的改写对象ECU19也能够安装。第五条件是写入数据为正常数据这样的条件。这里,正常数据包括适合改写对象ECU19的数据、未被篡改的数据等。

[0511] 若由安装条件判定部77a判定为第一条件、第二条件、第三条件、第四条件以及第五条件全部成立,则安装指示部77b对改写对象ECU19指示安装应用程序。即,若由安装条件判定部77a判定为获得了与安装有关的用户同意、CGW13能够与中心装置3进行数据通信、车辆状态为能够安装的状态、改写对象ECU19为能够安装的状态、写入数据为正常数据,则安装指示部77b对改写对象ECU19指示安装应用程序。具体而言,安装指示部77b从DCM12获取写入数据,将获取到的该写入数据传输至改写对象ECU19。若由安装条件判定部77a判定为第一条件、第二条件、第三条件、第四条件以及第五条件中的至少任一条件不成立,则安装指示部77b不对改写对象ECU19指示安装应用程序而待机,或者将不能开始安装的主旨及其理由提示给用户。

[0512] 车辆状态信息获取部77c从中心装置3获取车辆状态信息。激活条件判定部77d在全部改写对象ECU19中完成了应用程序的安装的情况下,判定第六条件、第七条件、第八条件是否成立。第六条件是获得了与激活有关的用户同意这样的条件。与激活有关的用户同意表示例如在如图43所示的画面中用户对激活的同意操作(例如按下“OK”按钮508b)。或者,也可以将从下载到激活视为一个更新,作为用户对更新的同意操作。第七条件是车辆状态为能够激活的状态这样的条件。第八条件是改写对象ECU19为能够激活的状态这样的条件。

[0513] 若由激活条件判定部77d判定为第六条件、第七条件以及第八条件全部成立,则激活指示部77e对改写对象ECU19指示激活应用程序。关于具体内容,在后述的(12)激活请求的指示处理中进行说明。即,若由激活条件判定部77d判定为获得了与激活有关的用户同意、车辆状态为能够激活的状态、改写对象ECU19为能够激活的状态,则激活指示部77e对改写对象ECU19指示激活应用程序。通过进行激活,写入至改写对象ECU19的更新程序被有效化。若由激活条件判定部77d判定为第六条件、第七条件以及第八条件中的至少任一条件不成立,则激活指示部77e不对改写对象ECU19指示激活应用程序而待机,或者将不能开始激活的主旨及其理由提示给用户。

[0514] 接下来,参照图62至图64对CGW13中的安装的指示判定部77的作用进行说明。

CGW13执行安装的指示判定程序,进行安装的指示判定处理。

[0515] CGW13若开始安装的指示判定处理,则判定第一条件是否成立,判定是否获得了与安装有关的用户同意(S501,相当于安装条件判定步骤的一部分)。CGW13若判定为获得了与安装有关的用户同意(S501:是),则判定第二条件是否成立,判定是否能够与中心装置3进行数据通信(S502,相当于安装条件判定步骤的一部分)。CGW13基于DCM12中的通信电波状况,判定是否能够与中心装置3进行数据通信。

[0516] CGW13若判定为能够与中心装置3进行数据通信(S502:是),则判定第三条件是否成立,判定车辆状态是否为能够安装(S503,相当于安装条件判定步骤的一部分)。作为车辆状态,CGW13例如判定车辆电池40的电池余量是否为规定容量以上、在改写对象ECU19的存储器结构为单面存储器的情况下车辆是否为停车状态(IG断开状态)等,判定车辆状态是否为能够安装。这些车辆状态的条件也可以构成为参照接收到的改写规格数据(参照图8)。CGW13例如在车辆电池40的电池余量为由改写规格数据指定的规定容量以上、与由改写规格数据指定的车辆状态(仅停车状态可、或者仅行驶状态可、或者停车状态和行驶状态都可)匹配等情况下,判定为车辆状态为能够安装。

[0517] CGW13若判定为车辆状态为能够安装(S503:是),则判定第四条件是否成立,判定改写对象ECU19是否为能够安装(S504,相当于安装条件判定步骤的一部分)。CGW13例如在改写对象ECU19未产生故障代码、向改写对象ECU19的安全访问成功等情况下,判定为改写对象ECU19为能够安装。这里,关于故障代码的产生有无,除了针对写入写入数据的改写对象ECU19进行确认之外,针对与该改写对象ECU19进行协作控制的ECU19也进行确认。即,CGW13不仅针对改写对象ECU19,还针对与该改写对象ECU19进行协作控制的ECU19,判定是否产生故障代码。

[0518] CGW13若判定为改写对象ECU19为能够安装(S504:是),则判定第五条件是否成立,判定写入数据是否是正常数据(S505,相当于安装条件判定步骤的一部分)。CGW13在是与改写对象ECU19的写入面(非运用面)匹配的写入数据且针对写入数据的完整性的验证结果为正常等的情况下,判定为写入数据是正常数据。CGW13若判定为写入数据是正常数据(S505:是),则对改写对象ECU19指示安装应用程序(S506,相当于安装指示步骤),这样,CGW13将满足第一条件作为条件,进行第二条件及其之后的判定。另外,CGW13最后进行第五条件的判定。CGW13若判定为第一条件至第五条件全部成立,则对改写对象ECU19指示安装应用程序。

[0519] 另一方面,CGW13若判定为未获得与安装有关的用户同意(S501:否),判定为不能与中心装置3进行数据通信(S502:否),判定为车辆状态不为能够安装(S503:否),判定为改写对象ECU19不为能够安装(S504:否),判定为写入数据不是正常数据(S505:否),则不对改写对象ECU19指示安装应用程序。此外,在上述的处理中,对与其他条件相比先判定获得了与安装有关的用户同意的条件的构成进行了说明,但也可以是比其他条件后判定的构成。

[0520] CGW13若对改写对象ECU19指示安装应用程序,则将写入数据分发至改写对象ECU19(S507),判定是否完成了安装(S508)。CGW13若判定为完成了安装(S508:是),则判定第六条件是否成立,判定是否获得了与激活有关的用户同意(S509)。CGW13若判定为获得了与激活有关的用户同意(S509:是),则判定第七条件是否成立,判定车辆状态是否是能够激活的状态(S510)。

[0521] CGW13若判定为车辆状态是能够激活的状态(S510:是),则判定第八条件是否成

立,判定改写对象ECU19是否是能够激活的状态(S511)。CGW13若判定为改写对象ECU19是能够激活的状态(S511:是),则对改写对象ECU19指示激活(S512),这样,CGW13若判定为第六条件至第八条件全部成立,则对改写对象ECU19指示激活。

[0522] 另外,CGW13在改写对象ECU19为多个的情况下,既可以分别独立地指示安装,也可以一起指示。在改写对象ECU19为ECU(ID1)、ECU(ID2)的情况下分别独立地指示安装的方式中,如图63所示,CGW13针对ECU(ID1)判定安装条件是否成立。CGW13若针对ECU(ID1)判定为安装条件成立,则对ECU(ID1)指示安装。接下来,CGW13针对ECU(ID2)判定安装条件是否成立。这里,作为安装条件,CGW13针对ECU(ID2)判定第四条件以及第五条件是否成立即可。CGW13若针对ECU(ID2)判定为安装条件成立,则对ECU(ID2)指示安装。

[0523] 在改写对象ECU19为ECU(ID1)、ECU(ID2)的情况下一起指示安装的方式中,如图64所示,CGW13针对ECU(ID1)判定安装条件是否成立。即,CGW13判定第一条件至第三条件、和关于ECU(ID1)的第四条件以及第五条件。CGW13若针对ECU(ID1)判定为安装条件成立,则针对ECU(ID2)判定安装条件是否成立。即,CGW13判定关于ECU(ID2)的第四条件以及第五条件。若关于ECU(ID2),安装条件成立,则CGW13对ECU(ID1)以及ECU(ID2)指示安装。CGW13例如同时并行进行向ECU(ID1)传输改写数据和向ECU(ID2)传输改写数据。这样,CGW13在一起指示安装的方式中,判定第一条件至第三条件、和关于全部改写对象ECU的第四条件以及第五条件。而且,CGW13在满足这些全部条件后指示安装。

[0524] 如以上说明那样,CGW13通过在对改写对象ECU19指示安装之前进行安装指示判定处理,从而若判定为获得了与安装有关的用户同意的第一条件、能够与中心装置3进行数据通信的第二条件、车辆状态为能够安装的状态的第三条件、改写对象ECU19为能够安装的状态的第四条件、写入数据是正常数据的第五条件全部成立,则对改写对象ECU19指示安装应用程序。能够对改写对象ECU19适当地指示应用程序的安装。

[0525] (6)安全访问密钥的管理处理

[0526] 参照图65至图69对安全访问密钥的管理处理进行说明。安全访问密钥是指CGW13在进行写入数据的安装之前进行访问改写对象ECU19时的设备认证的密钥。车辆用程序改写系统1在CGW13中进行安全访问密钥的管理处理。这里,以通过上述的(3)写入数据的传输判定处理、或者(4)写入数据的获取判定处理而处于CGW13能够从DCM12获取写入数据的状态为前提进行说明。使用安全访问密钥的设备认证相当于上述的(5)安装的指示判定处理中的第四条件(步骤S505)。

[0527] 在CGW13将写入数据分发至改写对象ECU19时,需要CGW13与改写对象ECU19之间使用安全访问密钥进行安全访问(设备认证)。该情况下,考虑有在CGW13中,对改写对象ECU19请求随机值的生成,从改写对象ECU19获取由改写对象ECU19生成的随机值,计算获取到的该随机值生成安全访问密钥的方法。然而,在这样的方法中,如果在不进行应用程序的改写时也从改写对象ECU19获取随机值,则也能够保持安全访问密钥,所以可能产生安全访问密钥的泄漏风险。

[0528] 另外,如果构成为在CGW13中将从改写对象ECU19获取到的随机值发送至中心装置3,中心装置3计算随机值并生成安全访问密钥,则也可以不保持安全访问密钥,所以能够减少安全访问密钥的泄漏风险。然而,在中心装置3计算随机值的构成中,到改写对象ECU19从中心装置3获取随机值为止的待机时间较长,较难满足诊断通信的时间规定。根据这样的情

况,在本实施方式中,采用以下的构成。

[0529] 如图65所示,供应商使用安全访问密钥的加密/解密密钥对每个改写对象ECU19的安全访问密钥进行加密来生成随机值。这里所说的随机值包括与过去使用的值不同的值、与过去使用的值相同的值的任意一方,是指随机的值。随机值是被加密的安全访问密钥。供应商将生成的随机值与重编数据一起提供。安全访问密钥、安全访问密钥的加密/解密密钥、随机值对每个ECU19是唯一的密钥。

[0530] 若随机值与重编数据一起被从供应商提供,则OEM将提供的该随机值与识别ECU19的ECU(ID)建立对应关系并储存于图8所示的CGW用的改写规格数据。另外,OEM也将对随机值进行解密所需要的密钥模式、解密运算模式储存于CGW用的改写规格数据。作为密钥模式,存储共享密钥/公开密钥等方式、密钥长度等,作为解密运算模式,储存解密运算所使用的算法的种类等。若将随机值、密钥模式以及解密运算模式储存于CGW用的改写规格数据,则OEM将储存有该随机值的CGW用的改写规格数据与重编数据一起提供给中心装置3。这些从供应商提供的信息被保存于后述的ECU重编数据DB以及ECU元数据DB。

[0531] 若改写规格数据(DCM用的改写规格数据以及CGW用的改写规格数据)与重编数据一起被从OEM提供,则中心装置3将包括提供的该改写规格数据和重编数据的分发数据包发送至主装置11。在主装置11中,DCM12若从中心装置3下载分发数据包,则将改写规格数据和写入数据传输至CGW13。

[0532] 如图66所示,CGW13在安全访问密钥的管理部78中具有安全区域78a(相当于解密密钥存储部)、随机值提取部78b(相当于密钥导出值提取部)、密钥模式提取部78c、解密运算模式提取部78d、密钥生成部78e、安全访问执行部78f、会话转移请求部78g、以及密钥消除部78h。关于安全区域78a,不能从ECU19的外部读出信息,并且配置有安全访问密钥的加密/解密密钥、解密运算算法。随机值提取部78b从CGW用的改写规格数据的解析结果提取出该改写规格数据所包含的随机值(密钥导出值)。随机值是与改写对象ECU19的ECU(ID)建立对应关系且被加密的值。

[0533] 密钥模式提取部78c从CGW用的改写规格数据的解析结果提取该改写规格数据所包含的密钥模式。解密运算模式提取部78d从CGW用的改写规格数据的解析结果提取该改写规格数据所包含的解密运算模式。

[0534] 若由随机值提取部78b提取出随机值,则密钥生成部78e检索安全区域78a,从配置于安全区域78a的安全访问密钥的解密密钥束中使用与ECU(ID)对应的解密密钥对提取出的该随机值进行解密,生成安全访问密钥。该情况下,密钥生成部78e使用通过由密钥模式提取部78c提取的密钥模式确定出的解密密钥,根据通过由解密运算模式提取部78d提取的解密运算模式确定出的解密运算方式,对密钥导出值进行解密。即,准备多个密钥模式以及多个解密运算模式,由CGW用的改写规格数据指定密钥模式以及解密运算模式,从而密钥生成部78e使用该密钥模式以及解密运算模式生成安全访问密钥。

[0535] 若由密钥生成部78e生成安全访问密钥,则安全访问执行部78f使用生成的该安全访问密钥执行对改写对象ECU19的安全访问。具体而言,安全访问执行部78f发送例如使用安全访问密钥对ECU(ID)进行加密后的加密数据,对改写对象ECU19请求访问。改写对象ECU19若接收加密数据,则使用自身保持的安全访问密钥对接收到的该加密数据进行解密。而且,改写对象ECU19对通过解密生成的解密数据和自身的ECU(ID)进行比较,在两者一致

的情况下许可对自身的访问,在两者不一致的情况下不许可对自身的访问。

[0536] 会话转移请求部78g请求向改写会话的转移。在从默认会话转移至改写会话后,安全访问执行部78f执行安全访问。此外,也可以在转移至默认会话以外的会话(例如诊断会话)之后进行安全访问,然后,转移至改写会话。密钥消除部78h在由安全访问执行部78f执行对改写对象ECU19的安全访问并且改写对象ECU19的应用程序的改写完成之后,消除由密钥生成部78e生成的安全访问密钥。

[0537] 接下来,参照图67至图69对CGW13中的安全访问密钥的管理部78的作用进行说明。CGW13执行安全访问密钥的管理程序,进行安全访问密钥的管理处理。作为安全访问密钥的管理处理,CGW13进行安全访问密钥的生成处理、安全访问密钥的消除处理。以下,对各个处理依次进行说明。

[0538] (6—1)安全访问密钥的生成处理

[0539] CGW13若开始安全访问密钥的生成处理,则解析从DCM12获取到的改写规格数据(S601,相当于改写规格数据解析步骤),从CGW用的改写规格数据提取随机值、密钥模式、解密运算模式(S602,相当于密钥导出值提取步骤)。

[0540] CGW13检索安全区域78a,从配置于安全区域78a的安全访问密钥的解密密钥束中使用与ECU(ID)对应的解密密钥对从CGW用的改写规格数据提取出的随机值进行解密,生成安全访问密钥(S603,相当于密钥生成步骤)。

[0541] 如图68所示,CGW13根据CGW用的改写规格数据生成安全访问密钥。CGW13进行向能够将写入数据写入的改写会话的会话转移请求(S604),使用安全访问密钥,执行针对改写对象ECU19的安全访问(S605),CGW13若完成安全访问的执行,则将写入数据分发至改写对象ECU19(S606),进行会话维持请求(S607)。CGW13若判定为完成了安装(S608:是),则结束安全访问密钥的生成处理。

[0542] (6—2)安全访问密钥的消除处理

[0543] CGW13若开始安全访问密钥的消除处理,则判定是否完成了改写对象ECU19的应用程序的改写(S611)。CGW13若判定为完成了改写对象ECU19的应用程序的改写(S611:是),则消除执行安全访问密钥的生成处理而生成的安全访问密钥(S612),结束安全访问密钥的消除处理。

[0544] 如以上说明那样,CGW13通过进行安全访问密钥的管理处理,从而从改写规格数据的解析结果提取与改写对象ECU19对应的随机值,使用存储于安全区域78a的与改写对象ECU19对应的解密密钥对该随机值进行解密,生成安全访问密钥。不从外部获取安全访问密钥,而在CGW13中生成安全访问密钥,从而能够减少安全访问密钥的泄漏风险,并且能够适当地执行对改写对象ECU19的安全访问。

[0545] 此外,优选CGW13在改写对象ECU19为多个的情况下,在进行各个写入数据的安装之前进行安全访问密钥的生成处理。即,优选:若是改写对象ECU19为ECU(ID1)、ECU(ID2)、ECU(ID3)的情况,则CGW13按ECU(ID1)的安全访问密钥的生成处理、向ECU(ID1)的写入数据的安装、ECU(ID2)的安全访问密钥的生成处理、向ECU(ID2)的写入数据的安装、ECU(ID3)的安全访问密钥的生成处理、向ECU(ID3)的写入数据的安装的顺序进行。例如如图63所示,CGW13进行安全访问处理作为针对ECU(ID1)的安装条件是否成立的一个处理,在访问被正常许可的情况下,对于ECU(ID1)指示安装。然后,CGW13进行安全访问处理作为针对ECU

(ID2)的安装条件是否成立的一个处理,在访问被正常许可的情况下,对于ECU(ID2)指示安装。

[0546] 另外,改写对象ECU19若通过CGW13进行对自身的安全访问而许可对自身的访问,则通过从CGW13接收会话转移请求而解除安全访问,成为写入数据能够写入至闪存的状态。会话转移请求例如是指如图155所示的第二状态中的“改写会话转移请求”。改写对象ECU19若在从许可对自身的访问起的规定时间(例如5秒)以内没有从CGW13接收会话转移请求,则成为超时,锁定安全访问,不受理会话转移请求的接收。CGW13在从确定对改写对象ECU19的访问的许可起的规定时间以内未将会话转移请求发送至改写对象ECU19的情况下,需要将会话维持请求发送至改写对象ECU19,保持改写对象ECU19不超时,将会话转移请求发送至改写对象ECU19。

[0547] 另外,例如在改写的中途通过取消操作而版本1.0的应用程序被写入运用面,版本2.0的应用程序被写入非运用面,若从该状态产生向版本2.0的活动通知,则可以不进行安装仅进行激活即可,所以也可以省略安全访问处理。

[0548] (7)写入数据的验证处理

[0549] 参照图70至图78对写入数据的验证处理进行说明。车辆用程序改写系统1在CGW13中进行写入数据的验证处理。CGW13既可以在获取上述的(6)安全访问密钥的管理处理中的访问许可之前,也可以在获取访问许可之后进行在本实施方式中说明的写入数据的验证处理。

[0550] 如图70所示,若供应商、OEM生成写入数据,则对生成的该写入数据应用数据验证值计算算法来生成数据验证值。这里,写入数据既可以是要更新的新程序,也可以是从旧程序向新程序的差分数据。供应商、OEM对该数据验证值应用使用规定的密钥(密钥值(key值))的加密来生成认证符,将写入数据和认证符建立对应关系地登记到中心装置3。具体而言,按各ECU19将这些数据存储于后述的重编数据DB。而且,中心装置3生成包括写入数据和认证符的分发数据包,存储于数据包DB。

[0551] 若产生来自主装置11的分发数据包的下载请求,则中心装置3根据该下载请求将包括写入数据和认证符的分发数据包发送至主装置11。该情况下,从中心装置3发送至主装置11的写入数据是暗文,从中心装置3发送至主装置11的认证符也是暗文。此外,从中心装置3发送至主装置11的认证符也可以是明文。在从中心装置3发送至主装置11的认证符是明文的情况下,不需要后述的解密处理。

[0552] 主装置11若从中心装置3下载分发数据包,则从下载的该分发数据包提取改写对象ECU19的写入数据,在将该写入数据分发至改写对象ECU19之前,验证该写入数据的妥当性。即,主装置11依次执行解密处理、第一验证值计算处理、第二验证值计算处理、比较处理、判定处理,验证写入数据。解密处理是解密以暗文发送的认证符的处理。第一验证值计算处理是根据解密后的认证符使用密钥(密钥值)计算作为期待值的第一数据验证值的处理。第二验证值计算处理是使用数据验证值计算算法根据写入数据计算第二数据验证值的处理。比较处理是比较第一数据验证值和第二数据验证值的处理。判定处理是根据比较处理的比较结果来判定写入数据的妥当性的处理。

[0553] 如图71所示,CGW13在写入数据的验证部79中具有可写入判定部79a、处理执行请求部79b、处理结果获取部79c、以及验证部79d。可写入判定部79a判定在改写对象ECU19中

是否能够进行写入数据的写入。若由可写入判定部69a判定为在改写对象ECU19中能够进行写入数据的写入,则处理执行请求部79b将处理执行请求通知给DCM12,对DCM12请求处理的执行。处理执行请求部68b将解密处理、第一验证值计算处理、第二验证值计算处理、比较处理、判定处理中的至少任一个的处理执行请求通知给DCM12。处理结果获取部68c通过被从DCM12通知处理结果,来从DCM12获取处理结果。若由处理结果获取部68c获取处理结果,则验证部79d使用该处理结果验证写入数据。即,在上述的构成中,CGW13相当于第一装置以及第一功能部,DCM12相当于第二装置以及第二功能部。

[0554] 接下来,参照图72至图77对CGW13中的写入数据的验证部79的作用进行说明。CGW13执行写入数据的验证程序,进行写入数据的验证处理。

[0555] CGW13若开始写入数据的验证处理,则将处理执行请求通知给DCM12,对DCM12请求处理的执行(S701,相当于处理执行请求步骤)。CGW13将上述的解密处理、第一验证值计算处理、第二验证值计算处理、比较处理、判定处理中的至少任一个的处理执行请求通知给DCM12。CGW13若从DCM12获取处理结果(S702,相当于处理结果获取步骤),则使用获取到的该处理结果验证写入数据(S703,相当于验证步骤)。

[0556] 以下,例示出CGW13将处理执行请求通知给DCM12的几个情况。在图73的例示中,CGW13将解密处理、第一验证值计算处理、第二验证值计算处理的处理执行请求通知给DCM12。DCM12若被从CGW13通知解密处理、第一验证值计算处理、第二验证值计算处理的处理执行请求,则依次执行解密处理、第一验证值计算处理、第二验证值计算处理。DCM12执行处理结果通知处理,将通过第一验证值计算处理计算出的第一数据验证值、通过第二验证值计算处理计算出的第二数据验证值作为处理结果通知给CGW13。CGW13若执行处理结果获取处理,从DCM12获取第一数据验证值、第二数据验证值,则使用该第一数据验证值、第二数据验证值,依次执行比较处理、判定处理。CGW13根据判定处理的判定结果的是否为正验证写入数据。在本例示中,DCM12保持用于计算第一数据验证值的密钥。

[0557] 在图74的例示中,CGW13将解密处理、第二验证值计算处理的处理执行请求通知给DCM12。DCM12若被从CGW13通知解密处理、第二验证值计算处理的处理执行请求,则依次执行解密处理、第二验证值计算处理,将通过第二验证值计算处理计算出的第二数据验证值通知给CGW13。CGW13若执行处理结果获取处理,从DCM12获取第二数据验证值,则执行第一验证值计算处理,使用通过第一验证值计算处理计算出的第一数据验证值、该第二数据验证值,依次执行比较处理、判定处理。CGW13根据判定处理的判定结果的是否为正验证写入数据。在本例示中,CGW13保持用于计算第一数据验证值的密钥。

[0558] 在图75的例示中,CGW13将解密处理、第一验证值计算处理、第二验证值计算处理、比较处理的处理执行请求通知给DCM12。DCM12若被从CGW13通知解密处理、第一验证值计算处理、第二验证值计算处理、比较处理的处理执行请求,则依次执行解密处理、第一验证值计算处理、第二验证值计算处理、比较处理。DCM12执行处理结果通知处理,将比较处理的比较结果作为处理结果通知给CGW13。CGW13若执行处理结果获取处理,从DCM12获取比较结果,则使用该比较结果执行判定处理。CGW13根据判定处理的判定结果的是否为正验证写入数据。在本例示中,DCM12保持用于计算第一数据验证值的密钥。

[0559] 在图76的例示中,CGW13将解密处理、第一验证值计算处理、第二验证值计算处理、比较处理、判定处理的处理执行请求通知给DCM12。DCM12若被从CGW13通知解密处理、第一

验证值计算处理、第二验证值计算处理、比较处理、判定处理的处理执行请求，则依次执行解密处理、第一验证值计算处理、第二验证值计算处理、比较处理、判定处理。DCM12执行处理结果通知处理，将判定处理的判定结果作为处理结果通知给CGW13。CGW13若执行处理结果获取处理，从DCM12获取处理结果，则根据由该处理结果表示的判定结果的是否为正验证写入数据。在本例示中，DCM12保持用于计算第一数据验证值的密钥。

[0560] CGW13在改写对象ECU19为多个的情况下，如以下那样进行针对多个改写对象ECU19的写入数据的验证处理。CGW13在改写对象ECU19为多个的情况下，有对于多个改写对象ECU19一起验证写入数据的方法和分别独立地验证写入数据的方法。

[0561] 在对于多个改写对象ECU19一起验证写入数据的方法中，例如如图77所示，CGW13一起验证ECU(ID1)的写入数据、ECU(ID2)的写入数据、ECU(ID3)的写入数据，分发至ECU(ID1)的写入数据的写入对象ECU(ID1)，分发至ECU(ID2)的写入数据的写入对象ECU(ID2)，分发至ECU(ID3)的写入数据的写入对象ECU(ID3)。该情况下，通过一起进行针对多个改写对象ECU19的写入数据的验证，能够缩短从针对多个改写对象ECU19的写入数据的验证开始到程序的改写完成为止所需的时间。即，与对于多个改写对象ECU19分别独立地验证写入数据的构成相比，能够缩短从针对多个改写对象ECU19的写入数据的验证开始到程序的改写完成为止所需的时间。

[0562] 在对于多个改写对象ECU19分别独立地验证写入数据的方法中，例如如图78所示，CGW13验证ECU(ID1)的写入数据，分发至ECU(ID1)的写入数据的写入对象ECU(ID1)，验证ECU(ID2)的写入数据，分发至ECU(ID2)的写入数据的写入对象ECU(ID2)，验证ECU(ID3)的写入数据，分发至ECU(ID3)的写入数据的写入对象ECU(ID2)。该情况下，通过在分发写入数据之前验证写入数据，能够避免非法访问，能够提高可靠性。即，在对于多个改写对象ECU19一起验证写入数据的构成中，从根据改写顺序完成验证到分发写入数据为止的时间根据改写顺序而不同，若从完成验证到分发写入数据的时间变长，则担心在其间产生由非法访问引起的篡改的危险性，但通过在紧接分发写入数据之前验证写入数据，能够避免这样的事态。

[0563] 如以上说明那样，CGW13通过进行写入数据的验证处理，使从中心装置3下载分发数据包的DCM12执行写入数据的验证所涉及的处理中的至少一部分。在CGW13、改写对象ECU19中，即使用于存储写入数据的区域不能确保，或不能搭载验证用的运算程序，也能够在将写入数据写入至改写对象ECU19之前，适当地进行写入数据的验证。

[0564] 在图74所例示的CGW13进行第一验证值计算处理的构成中，CGW13保持密钥(密钥值)，不将该密钥发送至DCM12而进行验证处理，所以与DCM12进行第一验证值计算处理的构成相比，能够提高安全性。另外，在改写对象ECU19为多个的情况下，既可以使用由多个改写对象ECU19共享的共享密钥(密钥值)进行第一验证值计算处理，也可以使用按多个改写对象ECU19而不同的单独密钥(密钥值)进行第一验证值计算处理。

[0565] 此外，以上例示了CGW13将处理执行请求通知给DCM12的构成，但例如在DCM12中处理负载增大而妨碍本来的处理这样的情况下，也可以代替DCM12而使用导航装置、改写对象ECU19以外的ECU，将处理执行请求通知给导航装置、改写对象ECU19以外的ECU。另外，在DCM12和CGW13为一体型的情况下，在能够不妨碍本来的处理地进行应对的情况下，也可以对自身的处理执行部请求处理执行请求。例如也可以在同一ECU内在不同的软组件间进行。

另外,也可以对构成为具有DCM12以及CGW13的功能的一个综合ECU的主装置11应用上述的构成。例如在图73至图76中,将CGW13中的处理功能作为第一功能部,将DCM12中的处理功能作为第二功能部,从第一功能部向第二功能部通知处理执行请求,从第二功能部向第一功能部返回执行结果。在构成为综合ECU的主装置11中,在处理负载增大而妨碍通信处理、中继处理这样的情况下,也可以代替第二功能部,而将处理执行请求通知给导航装置、改写对象ECU19以外的ECU。

[0566] 另外,数据验证值既可以按应用程序整体计算一个值,也可以按应用程序的模块单位计算多个值。若写入数据是全部数据,则能够在完成写入数据后在完整性验证中使用。

[0567] 此外,相对于安全访问是验证CGW13和改写对象ECU19是否也可以连接的方法,写入数据的验证包括作为写入数据的分发目的地的中心装置3正规(基于TLS通信的连接、相互认证)、从中心装置3下载写入数据的通信路径正规(通信路径隐藏、加密)、从中心装置3下载的写入数据未被篡改(篡改检测)、以及从中心装置3下载的写入数据不能篡改(加密)这样的概念。

[0568] 另外,对新程序的改写时的写入数据进行了说明,但向旧程序回写时的回滚时的写入数据也相同。该情况下,CGW13也可以在从中心装置3下载回滚时的写入数据的时刻进行验证,但也可以在紧接通过产生写入的取消请求而将回滚用的写入数据分发至改写对象ECU19之前进行验证。

[0569] (8)数据储存面信息的发送控制处理

[0570] 参照图79至图81对数据储存面信息的发送控制处理进行说明。车辆用程序改写系统1在CGW13中进行数据储存面信息的发送控制处理。

[0571] 如图79所示,CGW13在数据储存面信息的发送控制部80中具有数据储存面信息获取部80a、数据储存面信息发送部80b、改写方法确定部80c、以及改写方法指示部80d。数据储存面信息获取部80a从各ECU19获取与硬件以及软件有关的信息作为ECU结构信息。详细而言,在多个面具有数据储存面的双面存储器ECU以及单面挂起存储器ECU的情况下,获取包括各个数据储存面的版本信息的软件ID以及能够确定运用面的信息作为双面改写信息(以下,称为面信息)。

[0572] 若由数据储存面信息获取部80a获取到包括面信息的ECU结构信息,则数据储存面信息发送部80b使获取到的该面信息作为ECU结构信息之一从DCM12发送至中心装置3。既可以每当切换IG开关42的接通断开,数据储存面信息发送部80b使ECU结构信息发送至中心装置3,也可以根据来自中心装置3的请求使ECU结构信息发送至中心装置3。另外,不仅双面存储器ECU以及单面挂起存储器ECU,对于单面单独存储器ECU,数据储存面信息发送部80b也可以一并发送包括面信息的ECU构成。

[0573] 改写方法确定部80c根据CGW13用的改写规格数据的解析结果确定出改写方法。改写方法表示改写对象ECU19中的安装时的电源切换方法。若由改写方法确定部80c确定出改写方法,则改写方法指示部80d对改写对象ECU19指示基于确定出的该改写方法改写应用程序。即,若由改写方法确定部80c确定出基于电源自保持的改写方法,则改写方法指示部80d对改写对象ECU19指示基于电源自保持改写应用程序。若由改写方法确定部80c确定出基于电源控制的改写方法,则改写方法指示部80d对改写对象ECU19指示不使用电源自保持而基于电源控制改写应用程序。

[0574] 接下来,参照图80以及图81对CGW13中的数据储存面信息的发送控制部80的作用进行说明。CGW13执行数据储存面信息的发送控制程序,进行数据储存面信息的发送控制处理。

[0575] CGW13若开始数据储存面信息的发送控制处理,则将包括面信息的ECU结构信息请求发送至全部ECU19(S801),从全部ECU19获取包括面信息的ECU结构信息(S802,相当于数据储存面信息获取步骤)。CGW13若从各改写对象ECU19获取ECU结构信息,则将获取到的该ECU结构信息发送至DCM12(S803,相当于数据储存面信息发送步骤),等待从DCM12获取写入数据和改写规格数据(S804)。这里,CGW13也可以在预先确定出改写对象ECU19的情况下,仅从确定出的该改写对象ECU19获取面信息等。

[0576] DCM12若从CGW13接收到ECU结构信息,则暂时积蓄接收到的该ECU结构信息,若成为将ECU结构信息发送(上载)至中心装置3的时机,则将该ECU结构信息发送至中心装置3。中心装置3若从DCM12接收到ECU结构信息,则保存并解析接收到的该ECU结构信息。

[0577] 中心装置3确定作为面信息的发送源的各ECU19的各面的应用程序的版本以及哪个面是运用面,确定适合确定出的2个面的应用程序的版本以及运用面的写入数据(相当于更新数据选定步骤)。中心装置3例如在A面是运用面,储存于该运用面的应用程序是版本2.0,B面是非运用面,储存于该非运用面的应用程序是版本1.0的情况下,确定B面用的版本3.0的写入数据作为写入数据。中心装置3在写入数据是差分数据的情况下,确定从版本1.0更新为版本3.0的差分数据。中心装置3若确定出写入数据,则将包括确定出的该写入数据和改写规格数据的分发数据包发送至DCM12(相当于分发数据包发送步骤)。

[0578] 中心装置3既可以静态地选择发送至DCM12的分发数据包,也可以动态地生成。中心装置3在静态地选择发送至DCM12的分发数据包的情况下,管理多个储存有写入数据的分发数据包,选定适合非运用面的写入数据,从多个分发数据包中选择储存有选定的该写入数据的分发数据包并发送至DCM12。中心装置3在动态地生成发送至DCM12的分发数据包的情况下,若确定出适合非运用面的写入数据,则生成储存了确定出的该写入数据的分发数据包并发送至DCM12。

[0579] DCM12若从中心装置3下载分发数据包,则从下载的该分发数据包提取写入数据和改写规格数据,将提取出的该写入数据和改写规格数据传输至CGW13。

[0580] CGW13若判定为从DCM12获取到写入数据和改写规格数据(S804:是),则解析获取到的该改写规格数据(S805),根据该改写规格数据的解析结果判定针对改写对象ECU19的改写方法(S806、S807)。

[0581] CGW13若判定为改写方法是基于电源自保持的改写(S806:是),则将是能够安装的车辆状态作为条件来将写入数据获取请求发送至DCM12,从DCM12获取写入数据,将获取到的该写入数据分发至改写对象ECU19,通过电源自保持改写应用程序(S808),结束数据储存面信息的发送控制处理。通过电源自保持改写应用程序的方法如使用上述的图28以及图29在(二)通过电源自保持改写应用程序的情况中所述。

[0582] CGW13若判定为改写方法是基于电源控制的改写(S807:是),则将处于停车中作为条件来将写入数据获取请求发送至DCM12,从DCM12获取写入数据,将获取到的该写入数据分发至改写对象ECU19,通过电源控制改写应用程序(S809),结束数据储存面信息的发送控制处理。通过电源控制改写应用程序的方法如使用上述的图26以及图27在(一)通过电源控

制改写应用程序的情况中所述。

[0583] 如以上说明那样,CGW13通过进行数据储存面信息的发送控制处理,从而将包括面信息的ECU结构信息通知给中心装置3,使包括适合ECU结构信息的写入数据的分发数据包从中心装置3下载到DCM12。CGW13从DCM12获取适合该面信息的写入数据,将该写入数据分发至改写对象ECU19。能够在将搭载有在2面具有数据储存面的闪存的ECU19作为改写对象的情况下,适当地改写应用程序。

[0584] 此外,作为中心装置3对分发数据包进行分发的方式,有以下所示的第一分发方式至第三分发方式。在第一分发方式中,中心装置3例如分发储存了A面用的版本2.0的写入数据和B面用的版本2.0的写入数据的一个分发数据包。DCM12从自中心装置3下载到的分发数据包提取A面用的版本2.0的写入数据和B面用的版本2.0的写入数据,并将提取出的该写入数据传输至CGW13。CGW13若被从DCM12传输A面用的版本2.0的写入数据和B面用的版本2.0的写入数据,则选择其中的某一个分发至改写对象ECU19。即,是与各数据储存面对应的写入数据包含于分发数据包,在主装置11中选择适合改写对象ECU19的改写数据的构成。

[0585] 在第二分发方式中,中心装置3例如选择储存了A面用的版本2.0的写入数据的分发数据包或者储存了B面用的版本2.0的写入数据的分发数据包中的某一个并分发。DCM12从自中心装置3下载的分发数据包提取写入数据,将提取出的该写入数据传输至CGW13。CGW13将从DCM12传输的写入数据分发至改写对象ECU19。即,是基于从DCM12上载的面信息,中心装置3选择包括非运用面用的写入数据的分发数据包的构成。

[0586] 在第三分发方式中,中心装置3例如分发储存了A面用以及B面用共享的版本2.0的写入数据的分发数据包。DCM12从自中心装置3下载的分发数据包提取A面用以及B面用共享的版本2.0的写入数据,将提取出的该写入数据传输至CGW13。CGW13将被从DCM12传输的A面用以及B面用共享的版本2.0的写入数据分发至改写对象ECU19。改写对象ECU19若从CGW13接收到A面用以及B面用共享的版本2.0的写入数据,则将接收到的该写入数据写入A面或者B面的某一面。该情况下,在改写对象ECU19中,执行应用程序时,微机的地址解决功能发挥作用,从而无论将写入数据写入A面或者B面的哪个面都适当地动作。即,通过写入对象ECU19的微机解决伴随着面的差异的执行地址的不同,从而中心装置3以及主装置11能够在不了解面的情况下动作。

[0587] 从CGW13经由DCM12发送至中心装置3的包括面信息的ECU结构信息也可以除了2个面的应用程序的版本以及能够确定运用面的信息之外,还包括车辆确定信息、系统确定信息、ECU确定信息、利用环境信息等。

[0588] 车辆确定信息是用于确定分发数据包的分发目的地的车辆的唯一的信息,例如是VIN(Vehicle Identification Number:车辆识别编号)。在符合OBD(On-board diagnostics:车载诊断)法规的车辆中,通过OBD法规的规定能够利用VIN,但若是例如EV车辆那样的不符合OBD法规的车辆,则不能利用VIN,所以代替VIN采用个体车辆识别信息即可。

[0589] 系统确定信息是用于确定是哪种重编系统的唯一的信息。CGW13能够对能够进行利用自身管理的诊断通信的有线改写的系统进行无线改写,但不能对除此以外的独自方式的系统进行无线改写。即,这是因为是利用经由有线获取到的程序更新的机制,进行经由无线获取到的程序更新的系统。因此,在中心装置3中,需要判定将哪个分发数据包分发至哪

个系统,通过使用系统确定信息能够管理在车辆搭载怎样的系统。中心装置3能够通过判定系统确定信息,来判定每个系统的改写方式、将多个系统作为改写对象的情况下的改写顺序等。

[0590] ECU确定信息是用于确定改写对象ECU19的唯一的信息,是包括用于唯一地确定改写ECU和写入该改写对象ECU19的应用程序的软件版本和硬件版本的信息。ECU确定信息也相当于ECU产品编号。在利用全部数据写入最新的软件的情况下,也可以仅是硬件版本。另外,也能够定义规格版本、配置版本等能够确定应用程序的信息,并且,也能够定义微机ID、子微机ID、闪存ID、软件子版本、软件孙版本等。

[0591] 利用环境信息是用于确定用户利用车辆的环境的唯一的信息。通过利用环境信息从CGW13经由DCM12发送至中心装置3,从而中心装置3能够分发适合用户利用车辆的环境的应用程序。例如对喜欢从停止时起的急加速驾驶的用户分发强化加速的应用程序,对喜欢环保驾驶的用户分发虽然加速性能差但强化了环保驾驶的应用程序等,能够分发适合用户利用车辆的环境的应用程序。

[0592] 另外,以上对在改写对象ECU19的微机搭载有闪存的情况进行了说明,但在改写对象ECU19的微机连接有外置存储器的情况下,对外置存储器与双面存储器同等地进行处理,将外置存储器的写入区域区分为2个来将写入数据写入。在改写对象ECU19的微机搭载有闪存,并且连接有外置存储器的情况下,也有进行将存储于外置存储器的程序暂时复制(复印)到微机的存储器的处理的情况。因为也有外置存储器一般被用作ECU的动作日志的存储区域的情况,所以优选在开始了写入数据向外置存储器的写入的情况下,中断动作日志的存储,在完成了写入数据向外置存储器的写入的情况下,再次开始动作日志的存储。

[0593] 并不局限于改写应用程序的情况,例如关于地图数据等具有被逐一更新的性质的数据,也有双面以及版本这样的概念,所以在改写地图数据的情况下也相同。

[0594] (9)非改写对象的电源管理处理

[0595] 参照图82至图87对非改写对象ECU19的电源管理处理进行说明。车辆用程序改写系统1在CGW13中进行非改写对象ECU19的电源管理处理。在本实施方式中,设为通过DCM12完成分发数据包的下载,CGW13获取改写规格数据,在车辆停车状态下CGW13将写入数据分发至改写对象ECU19的状况。CGW13在将写入数据分发至改写对象ECU19的情况下,对电源管理ECU20请求IG电源接通,使全部ECU19成为启动状态。

[0596] 如图82所示,CGW13在非改写对象ECU19的电源管理部81中具备改写对象确定部81a、可安装判定部81b、状态转移控制部81c、以及改写顺序确定部81d。改写对象确定部81a根据改写规格数据的解析结果确定改写对象ECU19以及非改写对象ECU19。可安装判定部81b判定是否能够对改写对象ECU19安装。

[0597] 状态转移控制部81c能够转移ECU19的状态,使停止状态或者睡眠状态的ECU19转移至启动状态(唤醒状态),或使启动状态的ECU19转移至停止状态或者睡眠状态。另外,状态转移控制部81c使通常动作状态的ECU19转移至省电力动作状态,或使省电力动作状态的ECU19转移至通常动作状态。若由可安装判定部81b判定为能够安装,则状态转移控制部81c将至少一个以上的非改写对象ECU19控制成停止状态、睡眠状态或者省电力动作状态。改写顺序确定部81d根据改写规格数据的解析结果确定改写对象ECU19的改写顺序。

[0598] 接下来,参照图83至图87对CGW13中的非改写对象ECU19的电源管理部81的作用进

行说明。CGW13执行非改写对象的电源管理程序,进行非改写对象的电源管理处理。这里,对CGW13使成为管理对象的全部ECU19成为启动状态的情况进行说明。

[0599] CGW13若开始非改写对象ECU19的电源管理处理,则根据CGW用的改写规格数据的解析结果确定改写对象ECU19和非改写对象ECU19(S901),根据改写规格数据的解析结果确定一个以上的改写对象ECU19的改写顺序(S902)。CGW13判定是否能够进行写入数据的写入(S903,相当于可写入判定步骤),若判定为能够进行写入数据的写入(S903:是),则将电源断开请求(停止请求)发送至ACC系统的非改写对象ECU19以及IG系统的非改写对象ECU19,使ACC系统的非改写对象ECU19以及IG系统的非改写对象ECU19从启动状态转移至停止状态(S904,相当于状态转移控制步骤)。

[0600] CGW13判定是否将电源断开请求向符合的全部ECU19发送完成(S905),若判定为将电源断开请求向符合的全部ECU19发送完成(S905:是),则将睡眠请求发送至+B电源系统的非改写对象ECU19,使+B电源系统的非改写对象ECU19从启动状态转移至睡眠状态(S906,相当于状态转移控制步骤)。

[0601] CGW13判定是否将睡眠请求向符合的全部ECU19发送完成(S907),若判定为将睡眠请求向符合的全部ECU19发送完成(S907:是),则判定是否对全部改写对象ECU19完成了应用程序的改写(S908)。CGW13若判定为对全部改写对象ECU19完成了应用程序的改写(S908:是),则结束非改写对象ECU19的电源管理处理。CGW13若判定为未对全部改写对象ECU19完成应用程序的改写(S908:否),则返回至步骤S904,重复步骤S904及其之后的步骤。

[0602] CGW13在改写对象ECU19为多个的情况下,既可以使多个改写对象ECU19的状态分别独立地转移,也可以使多个改写对象ECU19的状态一起转移。即,在图83中,示出CGW13对非改写对象ECU19发送电源断开请求或者睡眠请求的处理。在接下来所示的图84以及图85中,对除了针对非改写对象ECU19的电源管理处理之外,还进行针对改写对象ECU19的电源管理处理的情况进行说明。

[0603] 首先,使用图84对CGW13使多个改写对象ECU19的状态分别独立地转移的情况进行说明。如图84所示,对例如改写对象ECU19是ECU(ID1)、ECU(ID2)、ECU(ID3),并且在停车中改写按从早到晚的改写顺序依次由ECU(ID1)、ECU(ID2)、ECU(ID3)指定的改写对象ECU19的情况进行说明。

[0604] CGW13使ECU(ID1)、ECU(ID2)、ECU(ID3)全部从停止状态或者睡眠状态转移至启动状态。CGW13将第一个改写的ECU(ID1)保持启动状态不变,使ECU(ID2)、ECU(ID3)从启动状态转移至停止状态或者睡眠状态,将写入数据分发至ECU(ID1)。CGW13若完成写入数据向ECU(ID1)的分发,则使ECU(ID1)从启动状态转移至停止状态或者睡眠状态,使第二个改写的ECU(ID2)从停止状态或者睡眠状态转移至启动状态,将ECU(ID3)保持停止状态或者睡眠状态不变,将写入数据分发至ECU(ID2)。

[0605] CGW13若完成写入数据向ECU(ID2)的分发,则将ECU(ID1)保持停止状态或者睡眠状态不变,使ECU(ID2)从启动状态转移至停止状态或者睡眠状态,使第三个改写的ECU(ID3)从停止状态或者睡眠状态转移至启动状态,将写入数据分发至ECU(ID3)。CGW13若完成写入数据向ECU(ID3)的分发,则将ECU(ID1)、ECU(ID2)保持停止状态或者睡眠状态不变,使ECU(ID3)从启动状态转移至停止状态或者睡眠状态。这样,CGW13控制为仅使多个改写对象ECU19中的当前改写中的ECU19成为启动状态。

[0606] 接下来,使用图85对CGW13使多个改写对象ECU19的状态一起转移的情况进行说明。如图85所示,对例如改写对象ECU19是ECU(ID1)、ECU(ID2)、ECU(ID3),并且在停车中改写按从早到晚的改写顺序依次由ECU(ID1)、ECU(ID2)、ECU(ID3)指定的改写对象ECU19的情况进行说明。

[0607] CGW13使ECU(ID1)、ECU(ID2)、ECU(ID3)全部从停止状态或者睡眠状态转移至启动状态。CGW13将ECU(ID1)、ECU(ID2)、ECU(ID3)全部保持启动状态不变,将写入数据分发至ECU(ID1)。CGW13若完成写入数据向ECU(ID1)的分发,则将写入数据分发至ECU(ID2)。CGW13若完成写入数据向ECU(ID2)的分发,则将写入数据分发至ECU(ID3)。CGW13若完成写入数据向ECU(ID3)的分发,则使ECU(ID1)、ECU(ID2)、ECU(ID3)全部从启动状态转移至停止状态或者睡眠状态。这样,CGW13将多个改写对象ECU19全部控制为启动状态,直至安装全部完成为止。这里,CGW13也可以同时并行地进行写入数据向ECU(ID1)、ECU(ID2)、ECU(ID3)的分发。

[0608] 在停车中改写对象ECU19改写应用程序的情况下,不一定是对改写对象ECU19的供给电压稳定的环境,所以担心在应用程序的改写中车辆电池40电池电量耗尽的事态。特别是,若改写对象ECU19为多个,则应用程序的改写所需的时间变长,所以在应用程序的改写中车辆电池40电池电量耗尽的可能性提高。对于该点,通过如上述那样使非改写对象ECU19成为停止状态或者睡眠状态,能够将在程序的改写中车辆电池40的电池余量不足的事态防患于未然。并且,通过使改写对象ECU19中的不是当前改写中的ECU19成为停止状态或者睡眠状态,能够进一步抑制消耗电力。

[0609] 以上,对在停车中对改写对象ECU19的应用程序进行改写的情况进行了说明,但对在车辆行驶中对改写对象ECU19的应用程序进行改写的情况进行说明。在车辆行驶中改写对象ECU19改写应用程序的情况下,处于对改写对象ECU19的供给电压稳定的环境,所以不会担心在应用程序的改写中车辆电池40成为电池电量耗尽的事态,但也可能有车辆电池40的电池余量较少的情况。根据这样的情况,优选在车辆行驶中,使不需要动作的ECU19转移至停止状态或者睡眠状态。如图86所示,在是在车辆行驶中不需要动作的ECU44与+B电源线37连接,但不与ACC电源线38以及IG电源线39连接的构成的情况下,CGW13使在该车辆行驶中不需要动作的ECU44从启动状态转移至停止状态或者睡眠状态。ECU44例如是具有防盗等功能的ECU。即,CGW13在车辆行驶中全部ECU19处于启动状态的期间,使不需要动作并且不是改写对象的ECU44转移至停止状态或者睡眠状态。由此,能够抑制伴随着车辆行驶中的安装的消耗电力的增加。

[0610] 另外,CGW13监视车辆电池40的电池余量,进行上述的非改写对象的电源管理处理。这里,使用图87对电池余量的监视处理进行说明。CGW13若开始电池余量的监视处理,则在将写入数据向改写对象ECU19分发的期间监视电池余量(S911),判定电池余量为第一规定容量以上、还是电池余量小于第一规定容量并且为第二规定容量以上、还是电池余量小于第二规定容量(S912～S914)。

[0611] CGW13若判定为电池余量为第一规定容量以上(S912:是),则将非改写对象ECU19保持启动状态不变,继续写入数据向改写对象ECU19的分发(S915)。CGW13若判定为电池余量小于第一规定容量并且为第二规定容量以上(S913:是),则使非改写对象ECU19中的在行驶中不需要动作的ECU转移至停止状态或者睡眠状态,继续写入数据向改写对象ECU19的分发(S916)。CGW13若判定为电池余量小于第二规定容量(S914:是),则判定是否能够中断改

写(S917)。

[0612] CGW13若判定为能够中断改写(S917:是),则中断写入数据的分发(S918)。CGW13若判定为不能中断改写(S917:否),则使非改写对象ECU19中的能够转移至停止状态或者睡眠状态的全部ECU转移至停止状态或者睡眠状态(S919)。

[0613] CGW13判定是否完成改写(S920),若判定为未完成改写(S920:否),则返回至步骤S911,重复步骤S911及其之后的步骤。若判定为完成了改写(S920:是),则CGW13使停止状态或者睡眠状态的改写对象ECU19转移至启动状态(S921),结束电池余量的监视处理。这里,第一规定容量以及第二规定容量的值既可以由CGW13预先具有,也可以使用通过改写规格数据指定的值。

[0614] 另外,CGW13也可以在步骤S919中使例如具有报警功能等特定功能的ECU19从转移至停止状态或者睡眠状态的对象排除,使除了具有特定功能的ECU19之外的非改写对象ECU19从启动状态转移至停止状态或者睡眠状态。CGW13也可以在能够在改写对象ECU19改写应用程序中执行应用控制的情况下,将除了能够与该改写对象ECU19通信的ECU19之外的非改写对象ECU19设为停止状态或者睡眠状态。当全部ECU19处于停止状态或者睡眠状态时,并且若例如车辆位置成为规定位置或当前时刻成为规定时刻等而改写条件成立,则CGW13也可以使改写对象ECU19从停止状态或者睡眠状态转移至启动状态。

[0615] CGW13也可以将启动电源(+B电源系统ECU、ACC系统ECU、IG系统ECU)、域组(车身系统、行驶系统、多媒体系统)、同步时机中的任意一个作为基准对改写对象ECU19或者非改写对象ECU19进行分组,以组为单位使改写对象ECU19成为启动状态,或以组为单位使非改写对象ECU19成为停止状态或者睡眠状态。

[0616] 另外,CGW13也可以是以总线为单位进行电源控制的构成。即,若判定为与特定总线连接的全部ECU19是非改写对象ECU19,则CGW13也可以通过断开该特定总线的电源,来使与该特定总线连接的全部非改写对象ECU19转移至停止状态或者睡眠状态。

[0617] 如以上说明那样,CGW13通过进行非改写对象的电源管理处理,从而若判定为能够对改写对象ECU19安装,则使至少一个以上的非改写对象ECU19成为停止状态、睡眠状态或者省电力动作状态。能够将在应用程序的改写中车辆电池40的电池余量变得不足的事态防患于未然。另外,通过非改写对象ECU19成为停止状态、睡眠状态或者省电力动作状态,从而能够抑制通信负载的增大。

[0618] (10)文件的传输控制处理

[0619] 参照图88至图97对文件的传输控制处理进行说明。车辆用程序改写系统1在CGW13中进行文件的传输控制处理。本实施方式是将DCM12(相当于第一装置)保持的改写数据经由CGW13(相当于第二装置)发送至改写对象ECU19(相当于第三装置)时的处理。

[0620] 如图88所示,CGW13在文件的传输控制部82中具有传输对象文件确定部82a、第一数据大小确定部82b、获取信息确定部82c、第二数据大小确定部82d、以及分割文件传输请求部82e。传输对象文件确定部82a使用改写规格数据的解析结果将包括写入改写对象ECU19的写入数据的文件确定为传输对象文件。在例如改写对象ECU19是ECU(ID1)、ECU(ID2)以及ECU(ID3)的情况下,传输对象文件确定部82a从图8所示的CGW用的改写规格数据获取ECU(ID1)、ECU(ID2)以及ECU(ID3)的ECU信息,根据获取到的该ECU信息将包括写入数据的文件确定为传输对象文件。作为传输对象文件,既可以确定获取该文件时的地址、索

引,也可以确定该文件的文件名。

[0621] 若由传输对象文件确定部82a确定出传输对象文件,则第一数据大小确定部82b确定用于获取该传输对象文件的第一数据大小。若由传输对象文件确定部82a确定出传输对象文件,则获取信息确定部82c将地址确定为用于获取该传输对象文件的获取信息。此外,在本实施方式中,将地址确定为用于获取传输对象文件的获取信息,但如果是用于获取传输对象文件的获取信息,则并不局限于地址,也可以是文件名、ECU(ID)等。第二数据大小确定部82d确定用于向改写对象ECU19分发写入数据的第二数据大小。即,第一数据大小是从DCM12向CGW13的数据传输大小,第二数据大小是从CGW13向改写对象ECU19的数据传输大小。

[0622] 若由获取信息确定部82c确定出地址,由第一数据大小确定部82b确定出第一数据大小,则分割文件传输请求部82e对DCM12指定该地址和第一数据大小,向DCM12请求分割文件的传输。例如在应该向ECU(ID1)分发的写入文件的数据量为1M字节的情况下,分割文件传输请求部82e请求从地址0x10000000将写入数据按1k字节传输。

[0623] 接下来,参照图89至图97对CGW13中的文件的传输控制部82的作用进行说明。CGW13执行文件的传输控制程序,进行文件的传输控制处理。

[0624] CGW13若判定为从DCM12接收到解包完成通知信号,则开始文件的传输控制处理。所谓解包是指如图10所示将分发数据包文件分成每个ECU的数据以及各改写规格数据的处理。CGW13若开始文件的传输控制处理,则将规定地址发送至DCM12(S1001)。DCM12从CGW13接收到规定地址,则将该规定地址的接收作为契机将CGW用的改写规格数据传输至CGW13。CGW13通过被从DCM12传输CGW用的改写规格数据,而获取CGW用的改写规格数据(S1002)。

[0625] CGW13若从DCM12获取CGW用的改写规格数据,则解析获取到的该CGW用的改写规格数据(S1003),根据改写规格数据的解析结果确定出传输对象文件(S1004,相当于传输对象文件确定步骤)。CGW13确定出与该传输对象文件对应的地址(S1005,相当于获取信息确定步骤),确定出与该传输对象文件对应的第一数据大小(S1006,相当于第一数据大小确定步骤)。CGW13将确定出的该地址和数据大小根据SID(Service Identifier)35的规定发送至DCM12,对存储器区域指定该地址和数据大小,向DCM12请求传输分割文件(S1007)。

[0626] DCM12若从CGW13接收到地址和数据大小,则解析DCM用的改写规格数据,将与该地址和数据大小对应的文件作为分割文件传输至CGW13。CGW13通过被从DCM12传输分割文件来获取分割文件(S1008)。该情况下,CGW13也可以在将获取到的该文件存储到RAM之后,存储至闪存。

[0627] CGW13判定是否完成了应该获取的全部分割文件的获取(S1009)。例如在应该向ECU(ID1)分发的写入文件的数据量为1M字节的情况下,CGW13获取每1k字节的分割文件,重复每1k字节的分割文件的获取并判定是否完成了获取1M字节的数据量。CGW13若判定为未完成应该获取的全部分割文件的获取(S1009:“否”),则返回步骤S1004,重复步骤S1004之后的步骤。CGW13若判定为完成了应该获取的全部文件的获取(S1009:“是”),则结束文件的传输控制处理。另外,在改写对象ECU19为多个的情况下,CGW13针对各改写对象ECU19重复上述的文件的传输控制处理。

[0628] 即,例如在改写对象ECU19为ECU(ID1)、ECU(ID2)以及ECU(ID3)的情况下,CGW13若完成向ECU(ID1)分发写入数据,则对于ECU(ID2)进行文件的传输控制处理,若完成向ECU

(ID2)分发写入数据,则对于ECU(ID3)进行文件的传输控制处理。另外,CGW13也可以依次进行针对多个改写对象ECU19的传输控制处理,也可以并行进行。

[0629] 在图90中,表示在DCM12的存储器内,例如ECU(ID1)的写入数据文件存储于地址“1000”～“3999”、ECU(ID2)的写入数据文件存储于地址“4000”～“6999”、ECU(ID3)的写入数据文件存储于地址“7000”～的情况。

[0630] 在该情况下,如图91所示,CGW13若从DCM12接收解包完成通知信号,则向DCM12发送地址“0000”,从DCM12获取改写规格数据。即,DCM12若将地址“0000”的接收判定为是CGW用的改写数据的获取请求,则向CGW13发送CGW用的改写规格数据。CGW13指定ECU(ID1)作为写入数据的传输对象,指定地址“1000”和数据大小“1k字节”,从DCM12获取包含存储于地址“1000”～“1999”的ECU(ID1)的写入数据的分割文件。CGW13若从DCM12获取分割文件,则向ECU(ID1)分发在该分割文件中包含的写入数据。

[0631] CGW13接下来同样地指定ECU(ID1)作为写入数据的传输对象,指定地址“2000”和数据大小“1k字节”,从DCM12获取包含存储于地址“2000”～“2999”的ECU(ID1)的写入数据的分割文件。CGW13若从DCM12获取分割文件,则向ECU(ID1)分发在该分割文件中包含的写入数据。直到写入数据向ECU(ID1)的写入全部完成为止,CGW13重复从DCM12按1k字节获取分割文件,重复向ECU(ID1)分发在该分割文件中包含的写入数据。即,CGW13若从DCM12获取1k字节的写入数据,则向改写对象ECU19发送该1k字节的写入数据,若完成向改写对象ECU19的发送,则从DCM12获取下一1k字节的写入数据。CGW13重复这些处理直到写入全部完成为止。

[0632] CGW13若在ECU(ID1)中正常地完成写入数据的写入,则指定ECU(ID2)作为写入数据的传输对象,指定地址“4000”和数据大小“1k字节”,从DCM12获取包含存储于地址“4000”～“4999”的ECU(ID2)的写入数据的分割文件。CGW13若从DCM12获取分割文件,则向ECU(ID2)分发在该分割文件中包含的写入数据。

[0633] CGW13若在ECU(ID2)中正常地完成写入数据的写入,则指定ECU(ID3)作为写入数据的传输对象,指定地址“7000”和数据大小“1k字节”,从DCM12获取包含存储于地址“7000”～“7999”的ECU(ID2)的写入数据的分割文件。CGW13若从DCM12获取分割文件,则向ECU(ID2)分发在该分割文件中包含的写入数据。

[0634] 如以上说明那样,CGW13通过进行文件的传输控制处理,而根据改写规格数据的解析结果确定出传输对象文件,确定与该传输对象文件对应的地址和数据大小。CGW13向DCM12指定该地址和数据大小,对DCM12请求对传输对象文件进行了分割的分割文件的传输,从DCM12获取分割文件。由此,在利用DCM12的存储器保存容量较大的写入数据的状态下,能够向ECU19分发写入数据。即,在CGW13中不需要准备用于存储容量较大的文件的存储器,能够削减CGW13的存储器容量。

[0635] 这里,对于从DCM12向CGW13传输的分割文件的数据量与从CGW13向改写对象ECU19分发的写入文件的数据量的关系进行说明。在上述的例示中,如图92所示,对从DCM12向CGW13传输的分割文件的数据量为1k字节的情况进行了说明,但从DCM12向CGW13传输的分割文件的数据量与从CGW13向改写对象ECU19分发的写入文件的数据量的关系也可以是任意的。

[0636] 即,例如如果由于CAN通信上的理由,改写对象ECU19采用以4k字节接收写入数据

的规格,则CGW13以4k字节为单位向改写对象ECU19分发写入文件的数据量。在该情况下,如果从DCM12向CGW13传输的分割文件的数据量为1k字节,则CGW13在从DCM12获取四个分割文件之后,向改写对象ECU19分发4k字节。即,从DCM12向CGW13传输的分割文件的数据量比从CGW13向改写对象ECU19分发的写入文件的数据量小。在这样的关系中,在CGW13中,能够抑制存储器容量的增大,并且并行地从DCM12获取分割文件、向改写对象ECU19分发写入数据。

[0637] 即,若从DCM12向CGW13传输的分割文件的数据量为4k字节,则要想并行地从DCM12获取分割文件、向改写对象ECU19分发写入数据,需要使CGW13的存储器容量为8k字节。通过使从DCM12向CGW13传输的分割文件的数据量为1k字节,不用使CGW13的存储器容量为8k字节,就能够并行地从DCM12获取分割文件、向改写对象ECU19分发写入数据。例如预先确保CGW13的存储器容量为5k字节,CGW13向改写对象ECU19分发从DCM12完成获取到的4k字节,并且从DCM12获取下一1k字节。而且,CGW13在完成了向改写对象ECU19分发4k字节之后,从DCM12进一步获取下一1k字节。

[0638] 另一方面,例如如果由于CAN通信上的理由,改写对象ECU19采用以128字节接收写入数据的规格,则CGW13以128字节向改写对象ECU19分发写入数据。在该情况下,如果从DCM12向CGW13传输的分割文件的数据量为1k字节,则CGW13在从DCM12获取一个分割文件之后,向改写对象ECU19按128字节进行分发。即,从DCM12向CGW13传输的分割文件的数据量比从CGW13向改写对象ECU19分发的写入文件的数据量大。例如预先确保CGW13的存储器容量为2k字节,CGW13以128字节为单位向改写对象ECU19分发从DCM12完成获取到的1k字节,并且从DCM12获取下一1k字节。而且,CGW13在完成了向改写对象ECU19分发128字节×8次之后,从DCM12进一步获取下一1k字节。

[0639] 这样,只要使从DCM12向CGW13传输的分割文件的数据量为固定值(例如1k字节),根据改写对象ECU19的规格使从CGW13向改写对象ECU19分发的写入文件的数据量为可变值即可。CGW13例如也可以使用由改写规格数据指定的各ECU的数据传输大小,决定向改写对象ECU19分发的数据量。

[0640] CGW13向DCM12发送传输请求,向DCM12请求分割文件的传输,但作为向DCM12请求分割文件的传输的方式,存在第一请求方式和第二请求方式。改写对象ECU19若完成写入数据的接收,则向CGW13发送表示完成了写入数据的接收的接收完成通知,若完成写入数据的写入,则向CGW13发送表示完成了写入数据的写入的写入完成通知。

[0641] 使用图93对第一分发方式进行说明。CGW13若从DCM12获取分割文件,则将获取到的该分割文件作为写入数据分发至改写对象ECU19。改写对象ECU19若完成写入数据的接收,则向CGW13发送接收完成通知,开始写入数据的写入处理。CGW13若从改写对象ECU19接收写入数据的接收完成通知,则向DCM12发送传输请求,向DCM12请求下一分割文件的传输。CGW13若从DCM12获取下一分割文件,则将获取到的该下一分割文件作为写入数据分发至改写对象ECU19。

[0642] 这样,CGW13在第一分发方式中,不用等待改写对象ECU19的写入数据的写入完成,而从DCM12获取下一写入数据,向改写对象ECU19分发。因此,在第一分发方式中,在CGW13中,若改写对象ECU19未完成写入数据的写入,则即使从DCM12获取下一分割文件而向改写对象ECU19分发下一写入数据,改写对象ECU19也有可能不能接收下一写入数据。然而,如果改写对象ECU19完成写入数据的写入,则能够从DCM12迅速地获取下一分割文件而迅速地向

改写对象ECU19分发下一写入数据。

[0643] 使用图94对第二分发方式进行说明。CGW13若从DCM12获取分割文件,则将获取到的该分割文件作为写入数据分发至改写对象ECU19。改写对象ECU19若完成写入数据的接收,则向CGW13发送接收完成通知,开始写入数据的写入处理。改写对象ECU19若完成写入,则向CGW13发送写入完成通知。CGW13若从改写对象ECU19接收写入完成通知,则向DCM12发送传输请求,向DCM12请求下一分割文件的传输。CGW13若从DCM12获取下一分割文件,则将获取到的该下一分割文件作为写入数据分发至改写对象ECU19。

[0644] 这样,在第二分发方式中,CGW13在等待改写对象ECU19的写入数据的写入完成之后,从DCM12获取下一写入数据,向改写对象ECU19分发。因此,在第二分发方式中,在CGW13中,直到从DCM12获取下一分割文件为止需要时间,能够在改写对象ECU19完成了写入数据的写入的状态下向DCM12请求分割文件的传输。因此,若从DCM12获取下一分割文件而向改写对象ECU19分发下一写入数据,则能够向改写对象ECU19可靠地分发下一写入数据。

[0645] 另外,CGW13通过SID34、36、37向改写对象ECU19分发写入数据,作为向改写对象ECU19分发写入数据的方式,存在第一分发方式和第二分发方式。在第一分发方式中,如图95所示,CGW13按规定的数据量(例如1k字节)对应该分发的写入数据进行分割而分发。在第二分发方式中,如图96所示,CGW13不对应该分发的写入数据进行分割而统一地分发。CGW13通过最初向改写对象ECU19分发的SID34,选择第一分发方式或者第二分发方式中的任一方。如图97所示,CGW13通过接收针对最后向改写对象ECU19分发的SID37的ACK(SID74),而确定改写对象ECU19的写入数据的接收。针对该SID37的ACK相当于通过图93和图94上述的写入数据的接收完成通知。即,在第一分发方式中,CGW13若接收针对最后向改写对象ECU19分发SID37的ACK,则通过使下一写入数据的地址自加1,而与向改写对象ECU19分发下一写入数据同时地,进一步从DCM12获取下一写入数据。

[0646] 另外,在DCM用的改写规格数据中将地址与文件对应起来,但作为将地址与文件对应起来的方法,例如也可以设计文件夹结构,在文件夹1储存规格数据,在文件夹2储存文件1,在文件夹3储存文件2而进行管理,也可以按文件名的顺序进行管理。在例如图10所示的解包中,在文件夹1储存DCM用的改写规格数据和CGW用的改写规格数据,在文件夹2储存ECU(ID1)的认证符和差分数据,在文件夹3储存ECU(ID2)的认证符和差分数据而进行管理。

[0647] 另外,CGW13例如在由于通信中断等某种理由而中断了向改写对象ECU19分发写入数据的情况下,从改写对象ECU19获取能够确定完成了写入数据的写入的地址的信息,向DCM12请求从未完成该写入的时刻起传输包含写入数据的分割文件。或者,CGW13也可以向DCM12请求包含来自起始的写入数据的分割文件的传输。

[0648] 如以上说明那样,CGW13若通过进行文件的传输控制处理,将包含写入到改写对象ECU19的写入数据的文件确定为传输对象文件,确定用于获取传输对象文件的地址和第一数据大小,向DCM12请求分割文件的传输,从DCM12传输分割文件,则向改写对ECU分发写入数据。能够高效地进行从DCM12向CGW13的写入数据的传输、从CGW13向改写对象ECU19的写入数据的分发。

[0649] (11)写入数据的分发控制处理

[0650] 参照图98至图108对写入数据的分发控制处理进行说明。车辆用程序改写系统1在CGW13中进行写入数据的分发控制处理。CGW13经由车辆内的总线向ECU19发送写入数据,因

此进行写入数据的分发控制处理,以使分发写入数据的过程中的总线负载不会变得过高。

[0651] 如图98所示,假定+B电源系统ECU、ACC系统ECU、IG系统ECU与同一总线连接的情况。在该情况下,在+B电源状态下,仅+B电源系统ECU启动,ACC系统ECU和IG系统ECU停止,因此向该总线传送仅+B电源系统ECU的车辆控制数据。在处于ACC电源状态时,+B电源系统ECU和ACC系统ECU启动,IG系统ECU停止,因此向该总线传送+B电源系统ECU和ACC系统ECU的车辆控制数据。在处于IG电源状态时,+B电源系统ECU、ACC系统ECU和IG系统ECU启动,因此向该总线传送+B电源系统ECU、ACC系统ECU和IG系统ECU的车辆控制数据。即,车辆控制数据的传送量按较多的顺序为IG电源状态、ACC电源状态、+B电源状态。

[0652] 如图99所示,CGW13在写入数据的分发控制部83中具有第一对应关系确定部83a、第二对应关系确定部83b、传送允许量确定部83c、分发频度确定部83d、总线负载测量部83e和分发控制部83f。

[0653] 第一对应关系确定部83a根据改写规格数据的解析结果确定出表示电源状态与总线的传送允许量的关系的第一对应关系,确定图100所示的总线负载表。传送允许量是指在未产生数据的冲突、延迟的状况下能够发送接收数据的传送负载的值。总线负载表是表示电源状态与总线的传送允许量的对应关系的表,按每个总线来规定。传送允许量是相对于最大传送允许量能够传送的车辆控制数据与写入数据的传送量的合计。

[0654] 在图100的例示中,第一总线的传送允许量相对于最大传送允许量为“80%”,因此CGW13在IG电源状态下,允许相对于最大传送允许量的“50%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“30%”作为写入数据的传送允许量。另外,对于第一总线,CGW13在ACC电源状态下,允许相对于最大传送允许量的“30%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“50%”作为写入数据的传送允许量。另外,对于第一总线,CGW13在+B电源状态下,允许相对于最大传送允许量的“20%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“60%”作为写入数据的传送允许量。如图100所示,第二总线和第三总线也被同样地规定。

[0655] 第二对应关系确定部83b根据改写规格数据的解析结果确定出表示改写对象ECU19所属的总线与电源系统的关系的第二对应关系,确定图101所示的改写对象ECU所属表。改写对象ECU所属表是表示改写对象ECU19所属的总线和电源系统的表。

[0656] 在图101的例示中,CGW13对于第一改写对象ECU19,将其与第一总线连接,在+B电源状态、ACC电源状态、IG电源状态中的任一状态下都启动,因此将第一改写对象ECU19确定为+B电源系统ECU。另外,CGW13对于第二改写对象ECU19,将其与第二总线连接,在+B电源状态下停止,但在ACC电源状态、IG电源状态下启动,因此将第二改写对象ECU19确定为ACC系统ECU。另外,CGW13对于第三改写对象ECU19,将其与第三总线连接,在+B电源状态、ACC电源状态下停止,但在IG电源状态下启动,因此将第三改写对象ECU19确定为IG系ECU。

[0657] CGW13使用图8所示的改写规格数据中的“连接总线”和“连接电源”的数据,而确定将改写对象ECU19与哪个总线连接,是哪个电源系统。另外,如果能够确定这些信息,则不一定需要以表的形式保存。

[0658] 传送允许量确定部83c根据第一对应关系的确定结果和第二对应关系的确定结果确定出改写对象ECU19所属的总线的传送允许量、即与进行程序的更新时的车辆的电源状态对应的传送允许量。若具体地说明,传送允许量确定部83c使用第二对应关系即改写对象

ECU所属表,而确定改写对象ECU19所属的总线,使用第一对应关系即总线负载表,对于确定出的该总线,确定每个电源状态的传送允许量。

[0659] 分发频度确定部83d使用预先决定的电源状态与写入数据的分发频度的对应关系,确定与安装时的电源状态对应的写入数据的分发频度。若具体地说明,分发频度确定部83d使用总线负载表,确定由传送允许量确定部83c确定出的传送允许量中的、为了分发写入数据而分配的传送允许量,确定写入数据的分发频度。分发频度确定部83d例如确定改写对象ECU19所属的总线为第一总线,确定安装时的电源状态为IG电源状态,将传送允许量确定为“80%”,将其中为了分发写入数据而分配的传送允许量确定为“30%”,由此确定写入数据的分发频度。为了分发写入数据而分配的传送允许量相当于传送限制信息。

[0660] 总线负载测量部83e对改写对象ECU19所属的总线的总线负载进行测量。总线负载测量部83e例如通过对以单位时间接收到的帧数或者比特数进行计数而测量总线负载。分发控制部83f根据由分发频度确定部83d确定出的分发频度来控制写入数据的分发。

[0661] 接下来,参照图102至图108对CGW13中的写入数据的分发控制部83的作用进行说明。CGW13执行写入数据的分发控制程序,进行写入数据的分发控制处理。

[0662] CGW13若从DCM12接收解包完成通知信号,则开始写入数据的分发控制处理。CGW13从DCM12获取CGW用的改写规格数据(S1101),根据该CGW用的改写规格数据确定出总线负载表和改写对象ECU所属表(S1102)。CGW13根据改写对象ECU所属表确定出改写对象ECU19所属的总线(S1103)。CGW13根据总线负载表确定出与该改写对象ECU19所属的总线、即进行更新时的车辆的电源状态对应的传送允许量。而且,CGW13考虑所确定出的传送允许量,确定写入数据的分发频度(S1104、相当于分发频度确定步骤)。例如在对于第一改写对象ECU19即ECU(ID1),在车辆行驶中分发写入数据的情况下,CGW13参照IG电源状态下的第一总线的传送允许量。在图100的例示中,IG电源状态下的第一总线的传送允许量为“80%”,其中在车辆控制数据中允许“50%”的传送,在写入数据中允许“30%”的传送。另外,传送允许量终究是用于表示事例的值,关于数值,设定在按适用的通信的规格的允许范围内。

[0663] 由于在CAN的500[kbps]上的规格中为1帧250[μs]左右,因此若在1秒内产生4次间断,则产生四个帧,总线负载为100%。CGW13通过判定在总线产生的间断,而确定写入数据的分发频度。CGW13开始以单位时间接收到的帧数的测量,开始总线负载的测量(S1105),判定该测量出的总线负载是否超过传送允许量(S1106),设定分发间隔。分发间隔是指在CGW13中向改写对象ECU19分发写入数据,从改写对象ECU19接收写入完成通知(ACK),直到将下一写入数据向改写对象ECU19发送为止的时间间隔。

[0664] CGW13若判定为该测量出的总线负载未超过传送允许量(S1106:“否”),则将写入数据的分发间隔设定为预先设定的最短间隔,如图103所示,开始向改写对象ECU19分发写入数据的(S1107、相当于分发控制步骤)。即,CGW13将CAN上的1帧的分发间隔设定为预先设定的最短间隔,开始向改写对象ECU19分发写入数据。另外,CAN上的1帧包含数据量为8字节的写入数据。另外,CAN FD(CAN with Flexible Data-Rate:具有灵活的数据速率的CAN)上的1帧包含数据量为64字节的写入数据。

[0665] 另一方面,CGW13若判定为该测量出的总线负载超过传送允许量(S1106:“是”),则对总线负载不超过传送允许量的间隔进行计算(S1108),将写入数据的分发间隔设定为该计算出的间隔,如图104所示,开始向改写对象ECU19分发写入数据(S1109,相当于分发控制

步骤)。

[0666] CGW13例如在IG电源状态下针对第一总线判定总线负载是否超过传送允许量即“80％”,若判定为总线负载不超过传送允许量,则设定成写入数据的传送允许量为“30％”的分发间隔T1。即,如图100的总线负载表所示,CGW13在IG电源状态下使用第一总线中的写入数据的传送允许量即“30％”,来设定分发间隔T1。CGW13设定分发间隔T1,以成为所允许的最大传送量。另外,CGW13也可以使测量对象收敛于写入数据的帧而测量总线负载,判定基于写入数据的总线负载是否超过写入数据的传送允许量“30％”。CGW13若判定为总线负载超过传送允许量,则根据该总线负载超过传送允许量的量,变更为总线负载不超过传送允许量的分发间隔T2(＞T1)。这样,CGW13在从DCM12获取写入数据之后,待机到达到所设定的分发间隔为止,然后向改写对象ECU19分发写入数据。

[0667] CGW13若开始向改写对象ECU19分发写入数据,则判定是否完成了向改写对象ECU19分发写入数据,并且持续地判定该测量出的总线负载是否超过传送允许量(S1110、S1011)。CGW13若判定为该测量出的总线负载不超过传送允许量(S1111:“否”),则将写入数据的分发间隔设定为预先设定的最短间隔,变更向改写对象ECU19分发写入数据的分发间隔(S1112)。另一方面,CGW13若判定为该测量出的总线负载超过传送允许量(S1111:“是”),则对总线负载不超过传送允许量的间隔进行计算(S1113),将写入数据的分发间隔设定为该计算出的间隔,变更向改写对象ECU19分发写入数据的分发间隔(S1114)。

[0668] CGW13若判定为完成了向改写对象ECU19分发写入数据(S1110:“是”),停止以单位时间接收到的帧数的测量,停止总线负载的测量(S1115),结束写入数据的分发控制处理。这里,在改写对象ECU19为多个的情况下,CGW13针对向全部的改写对象ECU19的安装,进行写入数据的分发控制处理。

[0669] 如以上说明那样,CGW13通过进行写入数据的分发控制处理,使用预先决定的电源状态与写入数据的分发频度的对应关系,确定向改写对象ECU19分发写入数据的分发频度,根据该分发频度来控制写入数据的分发。能够抑制进行安装时的、数据的冲突、延迟等。另外,不用妨碍同一总线中的车辆控制数据的分发,就能够使写入数据的分发共存。

[0670] 另外,以上,在CGW13中,例示了根据改写规格数据的解析结果确定出总线负载表的构成,也可以是预先保存总线负载表的构成。另外,在CGW13中,例示了根据改写规格数据的解析结果确定出改写对象ECU所属表的构成,但也可以采用预先保存改写对象ECU所属表的构成。

[0671] 也可以在车辆处于行驶中的电源状态下使写入数据的分发量相对地少,在停车中的电源状态下使写入数据的分发量相对地多。即,如图105所示,在车辆处于行驶中的IG电源接通时,CGW13通过IG系ECU、ACC系统ECU、+B电源系统ECU发送CAN帧,而使车辆控制、诊断等应用数据的传送量相对地多,因此使写入数据的分发量相对地少。另外,如图106所示,在停车中的IG电源断开时,CGW13通过仅+B电源系统ECU发送CAN帧,而使车辆控制、诊断等应用数据的传送量相对地少,使写入数据的分发量相对地多。即,CGW13在不妨碍车辆控制、诊断等应用数据的传送的空闲容量内调整写入数据的分发量。

[0672] 另外,也可以如图107所示,在CGW13中,在从改写对象ECU19发送事件帧的情况下,通过接收事件帧而使间断的频度变高,总线负载变高,因此使写入数据的分发量相对地少,在未从改写对象ECU19发送事件帧的情况下,使写入数据的分发量相对地多。

[0673] 另外,也可以如图108所示,在车辆系统中,在确定了CGW13处于写入数据的分发中的情况下,通过使车辆控制、诊断等应用数据的发送间隔延长到所允许的最大间隔,而降低总线负载。在CGW13中,也可以通过由车辆系统延长应用数据的发送间隔而降低总线负载,由此使写入数据的分发量相对地多。

[0674] 嵌入到改写规格数据中的总线负载表例如被一律地共用设定,而与车辆制造商的车型、等级等无关。这是因为,若ECU的装备由于例如车型、等级等而大幅不同,则总线负载大幅不同,若根据车型、等级等独立地设定最佳的总线负载表,则在该验证中需要工时等需要繁琐的麻烦,因此避免这样的繁琐的麻烦。

[0675] 与像上述那样车辆在行驶中进行安装的情况同样,在车辆在停车中进行安装的情况下,也进行写入数据的分发控制处理。在该情况下,如果改写对象ECU19为+B电源系统ECU,则也可以在+B电源状态下进行更新,因此参照总线负载表中的+B电源状态的传送允许量。另一方面,在改写对象ECU19为IG系统ECU的情况下,在IG电源状态下进行安装,因此参照总线负载表中的IG电源状态的传送允许量。这里,例如在改写对象ECU19为ACC系统ECU的情况下,也可以在IG电源状态下进行安装。在该情况下,参照总线负载表中的IG电源状态的传送允许量。另外,对保存总线负载表和改写对象ECU所属表的构成进行了说明,但只要能够确定每个电源状态的写入数据的分发频度,则也可以是保存任意的表的形式。

[0676] (12)激活请求的指示处理

[0677] 参照图109至图111对激活请求的指示处理进行说明。车辆用程序改写系统1在CGW13中进行激活请求的指示处理。CGW13针对完成了应用程序的改写的多个改写对象ECU19,进行激活请求以使该改写后的程序有效。在本实施方式中,CGW13通过对CGW用的改写规格数据进行解析,而成为掌握改写对象ECU19的组的状态。另外,CGW13仅在停车中进行激活请求,在车辆行驶中不进行激活请求。

[0678] 如图109所示,CGW13在激活请求的指示部84中具有改写对象确定部84a、改写完成判定部84b、激活可执行判定部84c、以及激活请求指示部84d。改写对象确定部84a将协作控制的多个改写对象ECU19作为对象,确定多个改写对象ECU19。改写完成判定部84b若通过改写对象确定部84a确定多个改写对象ECU19,则判定在确定出的该多个改写对象ECU19的全部中是否完成了程序的改写。

[0679] 若由改写完成判定部84b判定为在多个改写对象ECU19的全部中完成了程序的改写,则激活可执行判定部84c判定是否能够执行激活。在进行基于用户的激活同意的情况下、并且在车辆处于停车状态的情况下,激活可执行判定部84c判定为能够执行激活。

[0680] 若由激活可执行判定部84c判定为能够执行激活,则激活请求指示部84d指示激活请求。具体而言,激活请求指示部84d在对新面指示了切换请求之后,指示复位请求,监视会话转移超时、或者监视改写对象ECU19的内部复位,由此指示激活请求。在双面存储器ECU或者单面挂起存储器ECU中,通过在写入了应用程序的新面(非运用面)启动,而激活应用程序。另一方面,在单面单独存储器ECU中,通过重新启动来激活应用程序。另外,改写对象ECU19也可以构成为在对新面指示了切换请求之后,不取决于激活请求,而由自身进行复位。

[0681] 接下来,参照图110和图111对CGW13中的激活请求的指示部的作用进行说明。CGW13执行激活请求的指示程序,进行激活请求的指示处理。

[0682] CGW13若开始激活请求的指示处理,则确定多个改写对象ECU19(S1201、相当于改写对象确定步骤)。具体而言,CGW13通过参照在改写规格数据中记载的ECU(ID),而确定改写对象ECU19。CGW13判定在确定出的该多个改写对象ECU19的全部中是否完成了应用程序的改写(S1202、相当于改写完成判定步骤)。CGW13例如按在改写规格数据中记载的ECU(ID)的顺序,而依次进行针对改写对象ECU19的安装,若针对最后记载的ECU(ID)的安装完成则判定为在全部的改写对象ECU19中完成了写入。

[0683] CGW13若判定为在确定出的该多个改写对象ECU19的全部中完成了应用程序的改写(S1202:“是”),则判定是否能够执行激活(S1203、相当于激活可执行判定步骤)。具体而言,CGW13判定在此之前是否得到了针对更新的用户同意、车辆是否处于停车状态等,若满足这些条件,则判定为能够执行激活。用户同意也可以是针对更新处理整体的同意,也可以是针对激活的同意。CGW13若判定为能够执行激活(S1203:“是”),则此后,同时向多个改写对象ECU19指示激活请求(相当于激活请求指示步骤)。这里,假设ECU(ID1)、ECU(ID2)和ECU(ID3)是同一组的改写对象ECU19而进行说明。

[0684] CGW13若判定为针对ECU(ID1)、ECU(ID2)和ECU(ID3),能够执行激活,则开始激活请求的指示处理。CGW13若开始激活请求的指示处理,则对改写对象ECU19指示向新面的切换请求(S1204)。CGW13对电源管理ECU20请求使IG电源从断开切换为接通(S1205)。虽然车辆处于停车状态,IG开关42处于断开的状态,但CGW13为了进行激活而使IG电源从断开切换为接通。另外,CGW13在安装之后接着进行激活的情况下,由于IG电源处于接通状态,因此不进行S1205,对睡眠状态的改写对象ECU19进行启动请求(唤醒请求)。

[0685] CGW13向改写对象ECU19发送软件的复位请求,向改写对象ECU19指示软件的复位请求(S1206)。改写对象ECU19如果采用与软件的复位请求对应的规格,则在从CGW13接收软件的复位请求时,将软件复位而重新启动,激活应用程序。在改写对象ECU19为单面单独存储器ECU的情况下,改写对象ECU19通过利用新应用程序进行重新启动,而从旧应用程序切换为新应用程序。在改写对象ECU19为单面挂起存储器ECU或者双面存储器ECU的情况下,改写对象ECU19对存储于闪存的运用面信息(A面或者B面)进行更新,将写入了新应用程序的面切换为运用面,由此从旧应用程序切换为新应用程序。

[0686] CGW13对电源管理ECU20请求将IG电源从接通切换为断开、将IG电源从断开切换为接通,向改写对象ECU19指示电源的复位请求,向改写对象ECU19指示重新启动(S1207)。改写对象ECU19即使采用不与软件的复位请求对应的规格也是,若将IG电源从接通切换为断开、将IG电源从断开切换为接通,则将自身复位而重新启动,激活应用程序。在该情况下也是,在改写对象ECU19为单面单独存储器ECU的情况下,改写对象ECU19通过利用新应用程序进行重新启动,而从旧应用程序切换为新应用程序。在改写对象ECU19为单面挂起存储器ECU或者双面存储器ECU的情况下,改写对象ECU19对存储于闪存的运用面信息(A面或者B面)进行更新,将写入了新应用程序的面切换为运用面,由此从旧应用程序切换为新应用程序。另外,CGW13监视会话转移超时(S1208),监视改写对象ECU19的内部复位(S1209)。

[0687] 即,如果改写对象ECU19采用不与软件的复位请求对应的规格,则CGW13即使向改写对象ECU19发送软件的复位请求也无法指示激活,因此通过向改写对象ECU19指示电源的复位请求,而进行不与软件的复位请求对应的规格的改写对象ECU19的激活。例如在引擎ECU等IG系统ECU中,由于是因电源接通断开而一定复位的构成,因此多数情况下是不与软

件的复位请求对应的情况。在改写对象ECU19的观点中,根据从CGW13指示了软件的复位请求、从CGW13指示了电源的复位请求、会话转移超时、内部复位中的任一方,而进行激活(新程序中的启动)。

[0688] 与软件的复位请求对应的改写对象ECU19若被从CGW13指示软件的复位请求,则自身强制地进行复位,进行激活。ACC系统、IG系统ECU的改写对象ECU19若被从CGW13指示电源的复位请求,则不强制地供给电源,因此在下次的电源的供给时进行复位,进行激活。+B电源系统ECU的改写对象ECU19与ACC系统、IG系统ECU的改写对象ECU19不同,由于始终供给电源,因此通过会话转移超时、内部复位而进行激活。另外,针对各改写对象ECU19的激活的方法由改写规格数据指定。

[0689] CGW13若被从全部的改写对象ECU19通知利用新应用程序正常启动,向DCM12发送切换完成通知(S1210)。DCM12向中心装置3通知完成了更新程序的激活。CGW13对电源管理ECU20请求使IG电源从接通切换为断开,完成的激活同步指示处理。CGW13若通过用户操作而将IG电源从断开切换为接通,则向DCM12发送各ECU的程序版本、启动面等。DCM12向中心装置3通知从CGW13接收到的各ECU19的信息。这里,也可以在DCM12向中心装置3通知激活完成时,向中心装置3发送包含各ECU的程序版本和面信息的ECU结构信息。图111表示改写对象ECU19为双面存储器ECU或者单面挂起存储器ECU的情况。

[0690] 如以上说明那样,CGW13通过进行激活请求的指示处理,而将完成了应用程序的改写的多个改写对象ECU19在独自的时机进行从旧程序向新程序的切换的情况防患于未然,适当地使在该多个改写对象ECU19中从旧程序向新程序的切换时机一致。即,相互协作的多个改写对象ECU19的程序版本成为不匹配的状态,避免在协作的处理中产生不良情况。

[0691] (13)激活的执行控制处理

[0692] 参照图112至图114对激活的执行控制处理进行说明。激活的执行控制处理是伴随着CGW13进行上述的(12)激活请求的指示处理,而被从CGW13指示了激活请求的改写对象ECU19进行的处理。车辆用程序改写系统1在改写对象ECU19中进行激活的执行控制处理。这里,改写对象ECU19具有单面暂停方式存储器、双面存储器那样的多个数据储存面。改写对象ECU19具有第一数据储存面和第二数据储存面,成为在非运用面(新面)完成了改写数据的安装的状态。

[0693] 如图112所示,ECU19在激活的执行控制部107中,具有运用面信息更新部107a、执行条件判定部107b、执行控制部107c、以及通知部107d。运用面信息更新部107a若被从CGW13指示激活请求,则面向下次的重新启动,更新闪存的启动面判定信息(运用面信息)。运用面信息更新部107a例如在当前A面启动,在B面写入了新程序的情况下,将运用面信息从A面更新为B面。

[0694] 作为激活的执行条件,执行条件判定部107b判定是否从CGW13指示了软件的复位请求、是否从CGW13向电源管理ECU20指示了电源的复位请求、与CGW13的通信中断是否持续了规定时间。在满足任意一个条件的情况下,执行条件判定部107b判定为激活的执行条件成立。也可以不是来自CGW13的指示,而由电源检测电路36检测是否指示了电源的复位请求。若由执行条件判定部107b判定为激活的执行条件成立,则执行控制部107c根据运用面信息而进行将启动面从旧面(当前运用的面)向新面(当前未运用的面)切换的新面切换(激活)。通知部107d向CGW13通知运用面信息、版本信息等通知信息。

[0695] 接下来,参照图113和图114对改写对象ECU19的激活的执行控制部107的作用进行说明。改写对象ECU19执行激活的执行控制程序,进行激活的执行控制处理。

[0696] (13-1)改写处理

[0697] 改写对象ECU19若开始改写处理,则作为改写前处理,进行产品号读出、认证等存储器消除之前的处理(S1301)。改写对象ECU19判定是否从中心装置3接收到改写面信息(S1302)。改写对象ECU19例如根据是否从CGW13获取在包含于分发数据包的改写规格数据中记载的改写面信息,而判定是否接收到改写面信息。改写对象ECU19若判定为从中心装置3接收到改写面信息(S1302:“是”),则对该改写面信息与自身管理的改写面信息(运用面信息)进行对照,判定两者是否一致(S1303)。这里,改写面信息例如记载于从中心装置3发送的改写规格数据。例如在自身管理的改写面信息是运用面为A面且非运用面为B面的情况下,在记载于改写规格数据的改写面信息表示非运用面(B面)的情况下判定为两者一致,在记载于规格数据的改写面信息表示运用面(A面)的情况下,判定为两者不一致。

[0698] 改写对象ECU19若判定为两者一致(S1303:“是”),则作为改写处理,进行存储器消除、写入数据的写入、检验(S1304),结束改写处理。检验例如是写入到闪存的数据的完整性验证。改写对象ECU19若判定为两者不一致(S1303:“否”),则向CGW13发送否定响应(S1305),结束改写处理。

[0699] (13-2)激活的执行控制处理

[0700] 改写对象ECU19若开始激活的执行控制处理,则将非运用面作为改写面,判定是否完成了向改写面改写应用程序(S1311)。改写对象ECU19若判定为完成了向改写面改写应用程序(S1311:“是”),则对写入到闪存的应用程序的完整性进行验证,判定改写后的数据验证的是否为正(S1312)。改写对象ECU19若判定为改写后的数据验证为正(S1312:“是”),则将新面的改写完成标志设定为“OK”并存储(S1313)。

[0701] 然后,改写对象ECU19判定是否从CGW13指示了激活请求(S1314)。改写对象ECU19若判定为指示了激活请求(S1314:“是”),则判定新面的改写完成标志是否为“OK”(S1315),若判定为新面的改写完成标志为“OK”(S1315:“是”),则更新运用面信息(S1316、相当于运用面信息更新步骤)。即,例如在运用面为A面且非运用面为B面的情况下将B面作为改写面而完成了向改写面改写应用程序的情况下,改写对象ECU19将表示运用面为A面且非运用面为B面的运用面信息更新为表示运用面为B面且非运用面为A面的运用面信息。

[0702] 改写对象ECU19若更新为运用面信息,则判定是否从CGW13受理了软件的复位请求,是否从CGW13向电源管理ECU20指示了电源的复位请求、判定是否在指示了软件的复位请求之后与CGW13的通信中断持续了规定时间,判定激活的执行条件是否成立(S1317、相当于执行条件判定步骤)。这里,若这些激活的执行条件中的任一方成立则改写对象ECU19重新启动、或由ECU分别确定重新启动条件。

[0703] 改写对象ECU19若判定出从CGW13指示了软件的复位请求、从CGW13向电源管理ECU20指示电源的复位请求、在指示软件的复位请求之后经过了规定时间中的任一方,判定为激活的执行条件成立(S1317:“是”),则执行重新启动(复位)。改写对象ECU19通过执行重新启动,而根据更新后的运用面信息,将新面(B面)作为启动面而启动(S1318、相当于启动控制步骤),结束激活的执行控制处理。即,改写对象ECU19在重新启动后,在安装了应用程序的B面启动。

[0704] 改写对象ECU19若判定为未完成向新面改写应用程序的(S1311:“否”)、或者判定为改写后的数据验证为否(S1312:“否”),则判定是否指示了激活请求(S1319),若判定为指示了激活请求(S1319:“是”),则向CGW13发送否定响应(S1320),返回步骤S1311。另外,改写对象ECU19也可以在判定为改写后的数据验证为否的情况下,结束激活的执行控制处理,进行回滚等处理。另外,改写对象ECU19若判定为新面的改写完成标志不是“OK”(S1315:“否”),则向CGW13发送否定响应(S1321),返回步骤S1311。

[0705] 如以上说明那样,改写对象ECU19通过进行激活的执行控制处理,若被从CGW13指示激活请求,则面向下次的重新启动,更新运用面信息,若激活的执行条件成立,则在重新启动后,根据运用面信息而进行将启动面从旧面切换为新面的新面切换。即,即使更新程序的安装完成,只要不从CGW13指示激活,改写对象ECU19也不通过更新程序启动。例如,即使伴随着用户将IG开关42从断开操作到接通,改写对象ECU19重新启动,如果没有从CGW13指示激活,则在相同的运用面启动。CGW13向多个改写对象ECU19同时指示激活,然后,通过软件复位、电源复位或者会话超时来执行重新启动,由此能够使多个改写对象ECU19的更新程序同时有效化。另外,在上述的说明中,说明了数据储存面为2面的情况,但关于数据储存面为3面以上的情况也同样。

[0706] 另外,在上述的(12)CGW13的激活请求的指示处理中,CGW13对完成了应用程序的改写的多个改写对象ECU19进行激活请求的指示处理,由此将完成了应用程序的改写的多个改写对象ECU19在独自的时机进行从旧程序向新程序的切换的情况防患于未然,能够适当地使在该多个改写对象ECU19中从旧程序向新程序的切换时机一致。

[0707] (14)改写对象的组管理处理

[0708] 参照图115至图118对改写对象的组管理处理进行说明。车辆用程序改写系统1在CGW13中进行改写对象的组管理处理。CGW13对属于同一组的一个以上的改写对象ECU19同时指示应用程序的激活。另外,CGW13按组单位进行从安装到激活为止的控制。这里,假设ECU(ID1)和ECU(ID2)为第一组的改写对象ECU19,ECU(ID11)、ECU(ID12)和ECU(ID13)为第二组的改写对象ECU19而进行说明。

[0709] 如图115所示,CGW13在改写对象的组管理部85中,具有组生成部85a、指示执行部85b。组生成部85a根据CGW用的改写规格数据的解析结果,对应该同时进行版本升级的改写对象ECU19进行分组而生成组。若通过组生成部85a生成组,则指示执行部85b以该组为单位按规定的顺序进行安装的指示,若安装完成,则以该组为单位进行激活的指示。

[0710] 接下来,参照图116至图118对CGW13的改写对象的组管理部85的作用进行说明。CGW13执行改写对象的分组程序,进行改写对象的组管理处理。CGW13若开始改写对象的组管理处理,则从DCM12获取CGW用的改写规格数据(S1401、相当于改写规格数据获取步骤),对获取到的该改写规格数据进行解析(S1402、相当于改写规格数据解析步骤),判定本次的改写对象ECU19的所属组。CGW13例如也可以参照与改写规格数据的ECU相关的信息,确定所属于哪个组,也可以参照与改写规格数据的组相关的信息,确定哪个ECU所属于该组。CGW13针对一个组,判定是否为最初的改写对象ECU19的改写(S1403),判定是否是属于与上次的改写对象ECU19相同的组的改写对象ECU19的改写(S1404),判定是否是属于与上次的改写对象ECU19不同的组的改写对象ECU19的改写(S1405、相当于组生成步骤)。

[0711] CGW13若判定为是最初的改写对象ECU19的改写(S1403:“是”)、或者判定为是属于

与上次的改写对象ECU19相同的组的改写对象ECU19的改写(S1404:“是”),则向改写对象ECU19指示应用程序的改写,进行改写对象ECU19的应用程序的改写(S1406)。而且,CGW13判定是否存在下一改写对象ECU19(S1407)。CGW13若判定为存在同一组内的下一改写对象ECU19(S1407:“是”),则返回上述的步骤S1403～S1405,重复S1403～S1405。

[0712] CGW13若判定为是属于与上次的改写对象ECU19不同的组的改写对象ECU19的改写(S1405:“是”),则转移至激活请求的指示处理(S1408、相当于指示执行步骤)。

[0713] CGW13若开始激活请求的指示处理,则判定是否存在下一改写对象ECU19(S1411)。即,CGW13判定是否存在未完成安装的组。CGW13若判定为存在下一改写对象ECU19(S1411:“是”),则向属于完成了改写的组的改写对象ECU19指示激活请求(S1412)。即,在未对属于第二组的改写对象ECU19进行安装的情况下,CGW13对已经完成了改写的第一组的改写对象ECU(ID1)和ECU(ID2)指示激活。

[0714] CGW13向改写对象ECU19指示软件的复位请求,向改写对象ECU19指示基于经由电源管理ECU20将电源从接通切换为断开、从断开切换为接通的重新启动,而使改写对象ECU(ID1)和ECU(ID2)的应用程序同时启动。

[0715] CGW13判定下一改写对象ECU19的改写时机(S1413、S1314)。即,CGW13判定属于第二组的改写对象ECU19的改写时机。CGW13若判定为下一改写对象ECU19的改写时机是下次的从用户乘车向下车的切换时(S1413:“是”),则将IG电源从接通切换为断开(S1415),结束激活请求的指示处理,返回改写对象的组管理处理。例如由用户预先设定允许应用程序的更新的执行的时间段,CGW13在预测为在该时间段朝向属于第二组的改写对象ECU19的安装未完成时,在下次的停车状态下进行安装。在该情况下,返回原来的停车状态,CGW13指示电源管理ECU20将IG电源断开。

[0716] CGW13若判定为下一改写对象ECU19的改写时机为本次的下车中(停车状态)(S1414:“是”),则判定车辆电池40的电池余量是否为阈值以上(S1417)。这里,阈值也可以是预先设定的值,也可以是从CGW用的改写规格数据中获取到的值。CGW13若判定为车辆电池40的电池余量不是阈值以上(S1416:“否”),则向电源管理ECU20指示将IG电源从接通切换为断开(S1415),结束激活请求的指示处理,返回改写对象的组管理处理。CGW13若判定为车辆电池40的电池余量为阈值以上(S1416:“是”),则持续IG电源的接通(S1417),结束激活请求的指示处理,返回改写对象的组管理处理。CGW13如图116所示那样,进行属于第二组的改写对象ECU19的应用程序改写。

[0717] CGW13若判定为不存在下一改写对象ECU19(S1411:“否”),则向属于完成了改写的组的改写对象ECU19指示激活请求(S1418),将IG电源从接通切换为断开(S1419),结束激活请求的指示处理,返回改写对象的组管理处理。例如若完成属于第二组的改写对象ECU(ID11)、ECU(ID12)和ECU(ID13)的改写,则不存在下一改写对象ECU19、即下一组。在该情况下,CGW13对ECU(ID11)、ECU(ID12)和ECU(ID12)指示更新程序的激活,在激活完成后,向电源管理ECU20指示IG电源断开。

[0718] 如图154所示,在改写ECU(ID1)至ECU(ID2)以及ECU(ID11)至ECU(ID13)的应用程序的情况下,如果ECU(ID1)、ECU(ID2)处于协作控制的关系,ECU(ID11)、ECU(ID12)、ECU(ID13)处于协作控制的关系,则在分发数据包中,作为第一组,ECU(ID1)和ECU(ID2)属于改写对象ECU19,作为第二组,ECU(ID11)、ECU(ID12)和ECU(ID13)属于改写对象ECU19。CGW13

若在属于第一组的ECU(ID1)、ECU(ID2)中完成应用程序的改写,则对ECU(ID1),ECU(ID2)同时指示激活请求。然后,CGW13若在属于第二组的ECU(ID11)、ECU(ID12)和ECU(ID13)中执行应用程序的改写,全部完成,则对ECU(ID11)、ECU(ID12)、ECU(ID13)指示激活请求。另外,通过对单面单独存储器即改写对象ECU19指示重新启动,而成为激活指示。

[0719] 如以上说明那样,CGW13通过进行激活请求的改写对象ECU19的组管理处理,而以该组为单位指示激活请求。能够同时进行处于协作控制的关系的多个ECU的版本升级。即,能够避免处于协作控制的关系的多个改写对象ECU19的应用程序的版本成为不匹配的状态而在协作控制的处理中产生不良情况。另外,CGW13以该组为单位,按规定的顺序进行安装。即,CGW13控制为,按组单位进行从安装到激活。

[0720] 另外,在本实施方式中,构成为在完成了属于第一组的改写对象ECU19的安装之后,进行属于第一组的改写对象ECU19的激活,接着在完成了属于第二组的改写对象ECU19的安装之后,进行属于第二组的改写对象ECU19的激活。然而,也可以持续进行针对属于第一组的改写对象ECU19的激活和针对属于第二组的改写对象ECU19的激活。即,也可以的,完成属于第一组的改写对象ECU19的安装,完成属于第二组的改写对象ECU19的安装,然后进行属于第一组的改写对象ECU19的激活,进行属于第二组的改写对象ECU19的激活。在该情况下,也可以同时进行针对属于第一组和第二组的改写对象ECU19的激活。

[0721] 另外,在改写对象ECU19中包含单面单独存储器ECU的情况下,也可以将对该一面单独存储器ECU的安装的指示作为组内的最后。在向处于协作动作的关系的改写对象ECU19指示安装的情况下,也可以先对作为数据的发送侧进行动作的改写对象ECU19指示安装,然后对作为数据的接收侧进行动作的改写对象ECU指示安装。

[0722] CGW13参照改写规格数据的存储器种类,根据改写对象ECU19的存储器种类而决定安装顺序。例如为双面存储器、单面挂起存储器、单面单独存储器的顺序。另外,作为处于协作动作的关系的ECU19的信息,CGW13预先保存数据发送侧和数据接收侧中的任一方,基于该信息而决定改写对象ECU19的安装顺序。

[0723] 另外,在存在多个组的情况下,安装的顺序例如也可以基于紧急度、安全度、功能、时间等来决定。紧急度是指是否需要立即安装的指标,在若放置而不安装则导致人灾、事故等的可能性比较高的情况下紧急度较高,在即使放置而不安装,与人灾、事故等相关连的可能性也比较低的情况下紧急度较低,优先安装紧急度高的组。安全度是指基于安装时的微机的种类的限制的指标,按限制少的顺序、即双面存储器、单面挂起存储器、单面单独存储器的顺序进行安装。功能是指对于用户来说的便利性的指标,优先安装对于用户来说的便利性较高的组。时间是指安装所需要的时间的指标,优先对安装所需要的时间较短的组进行安装。

[0724] 另外,CGW13在向属于同一组的第一改写对象ECU19和第二改写对象ECU19指示安装的情况下,在第一改写对象ECU19中安装成功、在第二改写对象ECU19中安装失败的情况下,向第二改写对象ECU19指示回滚,向第一改写对象ECU19指示回滚。

[0725] 另外,CGW13在向属于第一组的改写对象ECU19和属于第二组的改写对象ECU19指示安装的情况下,在属于第一组的改写对象ECU19中安装失败的情况下,向属于第二组的改写对象ECU19指示安装。CGW13例如在图116中,在属于第一组的改写对象ECU19中安装失败的状态下成为第二组的改写的情况下(S1405;“是”),跳过针对第一组的激活请求的指示处

理(S1408),进入步骤S1407。而且,CGW13返回步骤S1403,开始第二组的安装,在完成了安装的情况下,对第二组进行激活请求的指示处理(S1408)。即,即使针对第一组的更新失败,CGW13也执行针对第二组的更新。

[0726] 另外,在一个活动(一个分发数据包内)存在2组的情况下,将针对活动的用户的同意操作和针对下载的用户的同意操作设为一次,使每个组进行二次针对安装的用户的同意操作和针对激活的用户的同意操作。即,在通过更新而变更的功能按每个组而不同的情况下,优选按每个该功能进行针对安装的用户的同意操作和针对激活的用户的同意操作。另外,还假定用户对于按每个组进行针对安装的用户的同意操作和针对激活的用户的同意操作感到繁琐,因此也可以将针对安装的用户的同意操作和针对激活的用户的同意操作在组整体中设为一次。

[0727] 例示了利用改写规格数据来判定改写对象ECU19的所属组的结构,但也可以是在CGW13中预先存储改写对象ECU19的所属组的结构。

[0728] (15)回滚的执行控制处理

[0729] 参照图119至图130对回滚的执行控制处理进行说明。车辆用程序改写系统1在CGW13中进行回滚的执行控制处理。回滚是指在中断应用程序的改写的情况下,用于将应用程序返回到原来的版本等、使改写对象ECU19的存储器复原到规定状态的写入或者回写,从用户来看,将改写对象ECU19的状态返回到开始写入数据的写入之前的状态。

[0730] 如图155所示,CGW13在回滚的执行控制部86中,具有取消请求判定部86a、回滚方法确定部86b、回滚执行部86c。取消请求判定部86a判定在应用程序的改写中是否产生了改写的取消请求。例如若用户操作移动终端6,选择程序改写的取消,则从获取了该取消的信息的中心装置3经由DCM12向CGW13通知程序的改写的取消请求。

[0731] 另外,在系统产生了异常的情况下,若向中心装置3通知系统的异常,则从中心装置3经由DCM12向CGW13通知程序的改写的取消请求。系统的异常是指例如向一个改写对象ECU19的写入成功,但向与该一个改写对象ECU19进行协作控制的其他的改写对象ECU19的写入失败的情况等。若像这样协作控制的多个改写对象ECU19中的一个写入失败,则判定为系统的异常,针对写入成功的改写对象ECU19,从中心装置3经由DCM12向CGW13通知程序的改写的取消请求。即,在产生取消请求的重要因素中包含基于用户的操作和系统的异常产生。

[0732] 回滚方法确定部86b根据搭载于改写对象ECU19的闪存的存储器种类、新程序或者旧程序的写入数据的数据种类,确定用于将改写对象ECU19的状态返回到开始写入数据的写入之前的状态的回滚方法。即,作为改写对象ECU19的存储器种类,回滚方法确定部86b确定闪存是单面单独存储器、单面挂起存储器或者双面存储器中的哪个,作为写入数据的数据种类,回滚方法确定部86b确定写入数据是全部数据或者差分数据中的哪个。

[0733] 而且,回滚方法确定部86b根据这些存储器种类和数据种类,确定第一回滚处理、第二回滚处理或者第三回滚处理。若通过回滚方法确定部86b确定回滚方法,则回滚执行部86c向改写对象ECU19指示与该回滚方法对应的回滚,使改写对象ECU19以旧程序进行动作。即,回滚执行部86c进行使改写对象ECU19的动作状态复原到开始该应用程序的改写之前的状态的回滚。

[0734] 接下来,参照图120至图130对CGW13的回滚执行控制部86的作用进行说明。CGW13

执行回滚执行控制程序,进行回滚执行控制处理。作为回滚的执行控制处理,CGW13进行回滚方法的确定处理、取消请求的判定处理。以下,对各个处理进行说明。

[0735] (15-1)回滚方法的确定处理

[0736] CGW13若开始回滚方法的确定处理,则对从DCM12获取到的CGW用的改写规格数据进行解析(S1501),根据该解析结果确定出回滚方法(S1502),结束回滚方法的确定处理。CGW13从图8所示的改写规格数据中获取存储器种类和回滚程序的数据种类,确定回滚方法。如果不论数据种类是新程序还是旧程序(回滚程序)都相同的运用,则也可以使用新程序的数据种类确定出回滚方法。

[0737] 即,如果改写对象ECU19的闪存为单面单独存储器且写入数据为全部数据,则作为产生了取消请求时的回滚方法,CGW13确定如下的方法(第一回滚处理),立即中断全部数据的分发,在改写对象ECU19中将旧应用程序的数据写入改写区域而改写为旧应用程序。用于单面单独存储器的旧应用程序(回滚用改写数据)与更新程序一同包含于分发数据包,CGW13利用与新应用程序相同的方法向改写对象ECU19分发旧应用程序。

[0738] 如果改写对象ECU19的闪存为单面单独存储器且写入数据为差分数据,则作为产生取消请求时的回滚方法,CGW13确定如下的方法(第二回滚处理),持续该差分数据的分发,在改写对象ECU19中将差分数据写入改写区域而改写为新应用程序之后,分发旧应用程序的差分数据,在改写对象ECU19中将旧数据写入改写区域而改写为旧应用程序。

[0739] 在写入数据为差分数据的情况下,改写对象ECU19使用写入到闪存的当前应用程序和从CGW13获取到的差分数据来复原新应用程序,进行新应用程序的写入。在向闪存写入不同的应用程序的状态下,写入对象ECU19无法根据差分数据复原新应用程序。因此,在单面单独存储器中,需要暂时改写为新应用程序的处理。这里,例如若当前应用程序为版本1.0,新应用程序为版本2.0,则改写程序(改写数据)是用于将版本1.0更新为版本2.0的差分数据,回滚用改写数据是用于将版本2.0更新为版本1.0的差分数据。

[0740] 如果改写对象ECU19的闪存为单面挂起存储器或者双面存储器,则CGW13确定如下的方法(第三回滚处理),持续写入数据的分发,如果在改写对象ECU19中运用面为A面,非运用面为B面,则CGW13将写入数据写入非运用面即B面而安装新应用程序,但抑制从A面向B面的运用面的切换。

[0741] (15-2)取消请求的判定处理

[0742] CGW13若确定为在改写对象ECU19中开始了应用程序的改写,则开始取消请求的判定处理,判定是否完成了应用程序的改写(S1511),判定是否产生了取消请求(S1512)。即,CGW13像上述那样,判定是否由于基于用户的操作、系统的异常产生等而产生了取消请求。

[0743] CGW13若判定为在完成应用程序的改写之前产生了取消请求、即在安装中产生了取消请求(S1512:“是”),则确定回滚对象的改写对象ECU19(S1513)。假设属于同一组的改写对象ECU19为ECU(ID1)、ECU(ID2)和ECU(ID3),ECU(ID1)为单面单独存储器,ECU(ID2)和ECU(ID3)为双面存储器,完成向ECU(ID1)的安装,在向ECU(ID2)的安装中途产生了取消请求。在该情况下,CGW13在S1413中,判定属于第一组的改写对象ECU19全部是否需要回滚。

[0744] CGW13确定为进行了应用程序的全部改写的ECU(ID1)和进行了应用程序的一部分改写的ECU(ID2)为回滚对象。CGW13判定确定出的该回滚对象的改写对象ECU19的闪存的存储器种类,判定闪存是单面单独存储器、单面挂起存储器和双面存储器中的哪个(S1514、

S1515)。CGW13若判定为闪存为单面单独存储器(S1514:“是”),则判定回滚程序的数据种类,判定回滚用写入数据是全部数据和差分数据中的哪个(S1516、S1517)。

[0745] CGW13若判定为回滚用写入数据是全部数据(S1516:“是”),则转移至第一回滚处理(S1518、相当于回滚执行步骤)。CGW13若开始第一回滚处理,则立即中断新程序即写入数据的分发(S1531)。而且,CGW13从DCM12获取全部数据即回滚用写入数据(旧程序),向改写对象ECU19分发。改写对象ECU19将从CGW13获取到的旧应用程序的数据写入闪存而改写为旧应用程序(S1532),结束第一回滚处理,返回取消请求的判定处理。

[0746] CGW13若判定为回滚用写入数据是差分数据(S1517:“是”),则转移至第二回滚处理(S1519、相当于回滚执行步骤)。CGW13若开始第二回滚处理,则持续新程序即写入数据的分发(S1541),在改写对象ECU19中复原差分数据而写入闪存,改写为新应用程序(S1542)。CGW13在向新应用程序的改写完成后,向改写对象ECU19分发从DCM12获取到的旧应用程序的写入数据(S1543)。在改写对象ECU19中复原旧应用程序的写入数据即差分数据,写入闪存而改写为旧应用程序(S1544),结束第二回滚处理,返回取消请求的判定处理。

[0747] CGW13若判定为改写对象ECU19为单面挂起存储器ECU或者双面存储器ECU(S1515:“是”),则转移至第三回滚处理(S1520、相当于回滚执行步骤)。在该情况下,CGW13不取决于改写数据种类,转移至第三回滚处理。CGW13若开始第三回滚处理,则持续该写入数据的分发(S1551),在改写对象ECU19中将写入数据写入非运用面(B面)而改写为新应用程序(S1552)。CGW13抑制从旧面(运用面:A面)向新面(非运用面:B面)的运用面的切换(S1553),结束第三回滚处理,返回取消请求的判定处理。另外,CGW13除了运用面的切换抑制之外,如图126所示,也可以将写入版本2.0的非运用面回写到改写为新应用程序之前的状态(例如版本1.0)。

[0748] CGW13若返回取消请求的判定处理,则判定对于全部的回滚对象的改写对象ECU19是否进行了回滚处理(S1521)。例如在上述的改写对象ECU19为ECU(ID1)、ECU(ID2)和ECU(ID3)的情况下的例示中,首先,CGW13根据回滚用数据种类,对于安装中途的单面单独存储器的ECU(ID1),进行第一回滚处理或者第二回滚处理。然后,CGW13对于完成了安装的双面存储器的ECU(ID2),进行第三回滚处理。

[0749] 此外,CGW13根据改写数据种类,对于单面单独存储器即ECU(ID1),进行第一回滚处理或者第二回滚处理。CGW13若判定为对于全部的回滚对象的改写对象ECU19未进行回滚处理(S1521:“否”),则返回步骤S1513,重复步骤S1513之后的步骤。CGW13若判定为对于全部的回滚对象的改写对象ECU19进行回滚处理(S1521:“是”),则结束取消请求的判定处理。CGW13对进行了回滚处理的属于第一组的ECU(ID1)、ECU(ID2)和ECU(ID3),同时指示旧应用程序的激活。单面单独存储器即ECU(ID1)重新启动,由此切换为旧应用程序。双面存储器即ECU(ID2)和ECU(ID3)不是在写入了更新程序的非运用面(B面)启动,而是在与此前相同的运用面(A面)启动。另外,在用户的意图发生变化,仍然执行程序更新时,在ECU(ID1)和ECU(ID3)中写入新应用程序,但由于在ECU(ID2)中,已经在非运用面安装完了新应用程序,因此省略写入。

[0750] CGW13若判定为未产生取消请求而完成了应用程序的改写(S1511:“是”),则判定是否完成了激活(S1522),判定是否产生了取消请求(S1523)。

[0751] CGW13若判定为在完成激活前产生了取消请求、即在激活中产生了取消请求

(S1523:“是”),则判定激活的指示是否到达改写对象ECU19,判定是否完成了运用面的切换(S1524)。

[0752] CGW13若判定为激活的指示未到达改写对象ECU19,判定为未完成运用面的切换(S1524:“否”),则进行第四回滚处理(S1525)。作为第四回滚处理,CGW13不切换运用面。或者,CGW13也可以不切换运用面而将非运用面返回到改写为新应用程序之前的状态。CGW13在不切换运用面的情况下,如图127所示,将写入版本1.0的面保存为运用面,将写入版本2.0的面保存为非运用面。在不切换运用面而将非运用面返回到改写为新应用程序之前的状态的情况下,如图128所示,CGW13将写入版本1.0的面保存为运用面,将写入版本2.0的面即非运用面回写到改写为新应用程序之前的状态(版本1.0)。

[0753] CGW13若判定为激活的指示到达改写对象ECU19,判定为完成了运用面的切换(S1524:“是”),则进行第五回滚处理。如图129所示,运用面的切换完成表示写入了版本2.0的面从非运用面切换为运用面,版本1.0的面从运用面切换为非运用面的状态。作为第五回滚处理,CGW13切换运用面、或者在将非运用面返回到改写为新应用程序之前的状态之后切换运用面。CGW13在切换运用面的情况下,如图129所示,将写入版本2.0的面从运用面切换为非运用面,将写入版本1.0的面从非运用面切换为运用面。在将非运用面返回到改写为新应用程序之前的状态之后切换运用面的情况下,如图130所示,CGW13将写入版本2.0的面即运用面回写到改写为新应用程序之前的状态(例如版本1.0),将返回到改写为该新应用程序之前的状态的面从运用面切换为非运用面,将写入版本1.0的面从非运用面切换为运用面。

[0754] 如以上说明那样,CGW13通过进行回滚的执行控制处理,若在应用程序的改写中产生改写的取消请求,则使改写对象ECU19的动作状态复原为从用户来看是开始该应用程序的改写之前的状态。由此,能够使属于同一组的改写对象ECU19全部同时地返回到原来的程序版本。另外,即使在下一程序更新中使用差分数据的情况下,也能够正确地复原写入数据。

[0755] (16)改写进展状况的显示控制处理

[0756] 参照图131至图143对改写进展状况的显示控制处理进行说明。车辆用程序改写系统1在CGW13中进行改写进展状况的显示控制处理。为了向用户传达应用程序的改写的进展状况,显示终端5即移动终端6、车载显示器7显示进展状况。作为显示的进展状况,不仅包含更新程序的情况,还包含例如由于用户的取消操作、更新失败等而回滚的情况。

[0757] 如图131所示,CGW13在改写进展状况的显示控制部87中,具有取消检测部87a、写入指示部87b、报告指示部87c。关于将存储于改写对象ECU19的第一写入数据改写为从中心装置3获取到的第二写入数据的程序的改写,取消检测部87a检测取消。取消检测部87a例如检测基于用户的取消操作、向改写对象ECU19的写入失败等异常。在是不适合于改写对象ECU19的写入数据的情况下、在对于写入数据检测出篡改的情况下、在产生了对改写对象ECU19的写入错误的情况下等、取消检测部87a检测出规定的异常的情况下,都回滚处理,因此这些异常的检测也视为取消的检测。

[0758] 写入指示部87b向改写对象ECU19分发第二写入数据,指示第二写入数据的写入。报告指示部87c指示与应用程序的改写相关的进展状况的报告。在通过写入指示部87b分发第二写入数据的过程中,报告指示部87c指示通过第一方式来报告与应用程序的改写相关

的进展状况,若通过取消检测部87a检测出取消,则指示通过第二方式来报告与应用程序的改写相关的进展状况。写入指示部87b若在分发第二写入数据的过程中,通过取消检测部87a检测出取消,则持续第二写入数据的分发。

[0759] CGW13根据确定改写对象ECU19的内部状态、确定来自中心装置3的指示、确定用户操作中任一方,而确定改写对象ECU19中的应用程序的改写。CGW13若确定应用程序的改写,则判定是通常时的改写(安装)还是回滚时的改写(卸载)。CGW13若根据确定改写对象ECU19的内部状态、确定来自中心装置3的指示、确定用户操作中的任一方,判定是通常时的改写还是回滚时的改写,则根据该判定结果对通常时或者回滚时的改写的进展状况进行运算,向显示终端5指示该运算出的进展状况的显示。

[0760] CGW13根据表示是通常时的改写还是回滚时的改写的改写判定结果,对显示终端5指示通常时的进展状况或者回滚时的进展状况的显示。CGW13指示显示,以区别表示通常时的改写的进展状况的进展显示和表示回滚时的改写的进展状况的进展显示。即,CGW13在通常时的改写的情况下以第一方式显示进展状况,在回滚时的改写的情况下,以与第一方式不同的第二方式显示进展状况。作为与显示进展状况时的显示相关的方式,CGW13在通常时和回滚时区别显示画面中的文字、项目、颜色、数值、闪烁等,而区别通常时的进展显示和回滚时的进展显示。另外,作为与显示进展显示时的显示以外的显示相关的方式,CGW13通过在通常时和回滚时区别声音、振动等,而区别通常时的进展显示和回滚时的进展显示。

[0761] 接下来,参照图132至图143对CGW13的作用进行说明。CGW13执行改写进展状况的显示控制程序,进行改写进展状况的显示控制处理。

[0762] CGW13若接收到表示在改写对象ECU19中开始了程序的改写的改写开始信号(如开始向改写对象ECU19的安装),则开始改写进展状况的显示控制处理。CGW13若开始改写进展状况的显示控制处理,则对CGW用的改写规格数据进行解析,确定改写对象ECU19的闪存的存储器种类和写入数据种类,确定通常时的改写对象ECU19(S1601)。CGW13若确定改写对象ECU19的闪存的存储器种类、写入数据种类和更新程序的大小(S1602),则根据该确定结果对通常时的改写进展状况进行运算,指示该运算出的通常时的改写进展状况的显示(S1603)。显示终端5根据来自CGW13的指示,以通常时的改写显示方式进行显示。

[0763] CGW13判定是否完成了应用程序的改写(S1604),判定是否产生了取消请求(S1605、相当于取消检测步骤)。CGW13例如在向改写对象ECU(ID1)的安装中,重复S1604和S1605,随时更新进展状况而进行显示。

[0764] CGW13若接收到表示在改写对象ECU19中完成了应用程序的改写的改写完成信号,判定为未产生取消请求而完成了应用程序的改写(S1604:“是”),则结束通常时的改写进展状况的显示(S1606),判定对于全部的改写对象ECU19是否完成了改写(S1607)。例如在完成了改写对象ECU(ID1)的安装的情况下,CGW13将ECU(ID1)的进展状况显示为100%。CGW13若判定为对于全部的改写对象ECU19未完成改写(S1607:“否”),则返回步骤S1601,重复步骤S1601之后的步骤。CGW13例如在S1601之后的步骤中,进行关于接下来安装的改写对象ECU(ID2)的进展显示。

[0765] CGW13若判定为在完成应用程序的改写之前产生了取消请求(S1605:“是”),则结束通常时的改写进展状况的显示(S1608),转移至回滚时的显示控制处理(S1609、相当于报告指示步骤)。这里,取消请求包含基于用户的取消请求、以及基于向改写对象ECU19的写入

失败等的系统的取消请求。

[0766] CGW13若开始回滚时的显示控制处理,则确定回滚时的改写对象ECU19(S1611),确定该回滚时的改写对象ECU19的闪存的存储器种类、回滚程序的数据种类和大小(S1612)。假设CGW13例如使属于同一组的改写对象ECU19为ECU(ID1)、ECU(ID2)和ECU(ID3),ECU(ID1)和ECU(ID2)的安装完成,在ECU(ID3)的安装中途产生了取消请求。在该情况下,CGW13根据各改写对象ECU19的存储器种类和写入数据种类,而确定回滚的需要与否和回滚方法。

[0767] CGW13确定成为回滚对象的改写对象ECU19的闪存的存储器种类和写入数据种类,确定回滚的需要与否和回滚方法(上述的S1518的第一回滚处理、S1519的第二回滚处理、S1520的第三回滚处理)。CGW13根据该确定结果对进展状况进行运算,显示进展状况,并且指示回滚时的改写进展状况的显示(S1613)。CGW13根据第一~第三回滚处理中的各个处理,写入的数据量不同。因此,CGW13根据第一~第三回滚处理来决定写入数据总量,根据与所写入的数据量的比例对进展(写入了几%)进行运算。CGW13判定作为回滚处理的应用程序的改写是否完成(S1614)。

[0768] CGW13向改写对象ECU19分发写入数据直到作为回滚处理的改写完成为止,并且重复上述的进展的运算和显示指示。CGW13在S1613中,以回滚时的显示方式显示运算出的进展状况。CGW13在S1614中,例如判定改写中途的ECU(ID3)的回滚是否正常完成。

[0769] CGW13若判定为针对回滚对象的改写对象ECU19的回滚完成(S1614:“是”),则结束回滚时的改写进展状况的显示(S1615)。CGW13例如持续对于ECU(ID3)回滚完成了100%的显示。

[0770] CGW13对于全部的回滚对象ECU19,判定是否完成了回滚时的改写(S1616)。CGW13若对于全部的回滚对象ECU19判定为未完成回滚时的改写(S1616:“否”),则返回步骤S1611,重复步骤S1611之后的步骤。

[0771] 例如在完成了安装的ECU(ID1)为单面单独存储器的情况下,CGW13进行回滚时的改写进展状况的显示(S1613)。另一方面,例如在完成了安装的ECU(ID2)为双面存储器且不需要回滚的情况下,从回滚时的改写对象除去ECU(ID2)。若ECU(ID3)和ECU(ID1)的回滚完成,则CGW13对于全部的回滚对象的改写对象ECU19,改写完成(S1616:“是”),结束回滚时的显示控制处理。

[0772] 另外,在上述的说明中,CGW13进行回滚时的显示控制处理,但也可以构成为,从CGW13获取需要的信息,并且车载显示器ECU7、中心装置3进行回滚时的显示控制处理。另外,也可以构成为,利用CGW13进行回滚时的改写、进展运算等,利用车载显示器ECU7、中心装置3进行回滚时的显示控制。即,并不局限于仅CGW13具有显示控制装置的功能的构成,也可以是利用CGW13和车载显示器ECU7分散地具有显示控制装置的功能的构成,也可以是利用CGW13和中心装置3分散地具有显示控制装置的功能的构成。

[0773] 以下,参照图134至图142对改写进展状况的显示进行说明。显示终端5在通常时的改写进展状况的显示中,如图134所示,将整体进展状况显示为“通常改写”,使用户掌握是通常时的改写进展状况的显示。也可以将“通常改写”显示为“安装”。作为第一方式,显示终端5进行通常时的改写进展状况的显示。

[0774] 显示终端5对于完成应用程序的改写、处于等待激活更新程序的同步指示的状态的改写对象ECU19,将进展状态显示为“等待同步指示”,对于处于改写中的状态的改写对象

ECU19,将进展状态显示为“通常改写中”。也可以将“等待同步指示”显示为“等待激活”。也可以将“通常改写中”显示为“安装中”。图134例示了ECU(ID0001)和ECU(ID0002)完成应用程序的改写而处于等待同步指示的状态,ECU(ID0003)处于通常改写中的状态的情况。

[0775] 显示终端5若从该状态产生取消请求,则如图135所示,例如弹出显示“受理了取消。复原到改写前的状态。请稍等。”这样的消息,使用户掌握受理了取消。作为第二方式,显示终端5进行受理了取消的显示。

[0776] 显示终端5若通过CGW13完成回滚时的改写的准备,则如图136所示,将整体进展状况显示为“回滚改写”,使用户掌握回滚时的改写进展状况的显示。也可以将“回滚改写”显示为“卸载”。显示终端5对于全部的改写对象ECU19将进展状态显示为“等待回滚”,将表示改写状况的进展的进展图的数值显示为“0%”。也可以将“等待回滚”显示为“等待卸载”。这里,采用ECU(ID0001)和ECU(ID0002)是单面单独存储器ECU,ECU(ID0003)是双面存储器ECU的例子,除了改写中途的ECU(ID0003)之外,完成了安装的ECU(ID0001)和ECU(ID0002)也需要回滚。在图136中,采用表示一个整体进展状况、并且分别显示各改写对象ECU19的进展状况的方式。

[0777] CGW13若开始回滚时的改写,则如图137所示,对于处于改写中的状态的改写对象ECU19,将进展状态显示为“回滚改写中(或卸载中)”。作为第三方式,显示终端5进行回滚时的改写进展状况的显示。图137例示了ECU(ID0003)处于回滚改写中的状态的情况。显示终端5若完成改写对象ECU19中的回滚,则如图138所示,对于完成了改写的改写对象ECU19,将进展状态作为“回滚完成”,以100%显示进展状况。

[0778] 在回滚对象ECU19是单面单独存储器ECU,是全部数据的改写的情况下,如图139所示,显示终端5使进展图的显示迁移。即,在回滚对象ECU19是单面单独存储器ECU,是全部数据的改写的情况下,立即中断全部数据的分发,在改写对象ECU19中将旧应用程序的数据写入闪存而改写为旧应用程序(第一回滚处理)。

[0779] 例如若在通常改写完成到“50%”的阶段产生取消请求(图139(a)),则显示终端5将进展图的数值显示为“0%”(图139(b)),根据写入旧应用程序的数据的进展而使进展图的数值增加,改写为旧应用程序(图139(c)、(d)、(e))。若对旧应用程序的改写100%完成,则显示终端5显示该改写对象ECU19为“回滚完成”。此外,图139和之后说明的图140～142表示各个ECU的进展显示。

[0780] 在回滚对象ECU19是单面单独存储器ECU、是差分数据的改写的情况下,如图140或者图141所示,显示终端5使进展图的显示迁移。即,在回滚对象ECU19是单面单独存储器、是差分数据的改写的情况下,CGW13持续差分数据的分发,在改写对象ECU19中将差分数据写入闪存而改写为新应用程序。CGW13向改写对象ECU19分发旧应用程序的数据,在改写对象ECU19中将旧数据写入闪存而改写为旧应用程序(第二回滚处理)。

[0781] 例如若在通常改写(安装)完成到“50%”的阶段产生取消请求(图140(a)、图141(a)),则显示终端5将进展图的数值显示为“0%”(图140(b)、图141(b))。改写对象ECU19使在此前写入的差分数据有效,连续进行从CGW13分发的差分数据的写入。即,从“0%”的显示切换为相当于有效的“50%”的比例的安装完成这样的进展显示(图140(c),图141(c))。显示终端5根据改写对象ECU19写入从CGW13分发的新程序的差分数据的进展而增加进展图的数值(图140(d)、(e)、图141(d)、(e))。显示终端5在改写对象ECU19完成了新应用程序的改

写之后,接着根据改写对象ECU19写入从CGW13分发的旧应用程序的差分数据的进展,而增加进展图的数值(图140(f)、(g)、图141(f)、(g))。即,作为回滚处理,与产生新程序的持续安装和旧程序的安装相配合地,显示终端5进行显示,以使得可知新程序写入的进展状况和旧程序写入的进展状况。

[0782] 在该情况下,也可以如图140所示,在显示终端5中,作为新应用程序的改写量,将左侧的进展图显示为“100%”,作为旧应用程序的改写量,将右侧的进展图显示为“100%”,由此使进展图的宽度整体为“200%”。在该情况下,显示终端5根据新应用程序的文件大小和所写入的新应用程序的累积数据大小,对新应用程序的进展百分比进行运算,根据旧应用程序的文件大小和所写入的旧应用程序的累积数据大小对旧应用程序的进展百分比进行运算,显示进展状况。

[0783] 另外,也可以如图141所示,在显示终端5中,通过使新应用程序的改写量为“50%”,使旧应用程序的改写量为“50%”,而使进展图的宽度整体为“100%”。在该情况下,显示终端5根据新应用程序的文件大小与旧应用程序的文件大小的合计值、所写入的新应用程序的累积数据大小与旧应用程序的累积数据大小的合计值,而对进展百分比进行运算并进行显示。

[0784] 在回滚对象ECU19为单面挂起存储器ECU或者双面存储器ECU的改写的情况下,如图142所示,显示终端5使进展图的显示迁移。即,在回滚对象ECU19为单面挂起存储器ECU或者双面存储器ECU的改写的情况下,CGW13持续向改写对象ECU19分发写入数据的,在改写对象ECU19中将写入数据写入非运用面而改写为新应用程序(第三回滚处理)。

[0785] 例如若在通常改写(安装)完成到“50%”的阶段产生取消请求(图142(a)),则显示终端5将进展图的数值显示为“0%”(图142(b))。改写对象ECU19使在此前写入的差分数据有效,持续进行从CGW13分发的差分数据的写入。即,从“0%”的显示切换为有效的相当于“50%”的比例的安装完成这样的进展显示(图142(c))。显示终端5根据改写对象ECU19写入从CGW13分发的写入数据的进展而增加进展图的数值(图142(d)、(e))。另外,在本实施方式中,对CGW13进行改写进展状况的显示控制处理进行了说明,但也可以是显示终端5进行改写进展状况的显示控制处理的构成。

[0786] 如以上说明那样,显示终端5通过进行改写进展状况的显示控制处理,在回滚处理的基础上,以区别应用程序的改写是通常时的改写(安装)还是回滚时的改写(卸载)的显示方式显示进展状况。用户受理更新程序的取消,能够掌握回滚推进。另外,以上,对针对每个改写对象ECU19显示进展状态的构成进行了说明,但如图143所示,也可以是一起显示改写对象ECU19的进展状态的构成。在该情况下,显示终端5将针对三个改写对象ECU19的进展显示作为一个进展状态进行显示而不是个别地显示。作为回滚处理,CGW13根据在三个改写对象ECU19中产生的写入完毕数据量相对于写入数据总量的比例,对进展进行运算。

[0787] (17)差分数据的匹配性判定处理

[0788] 参照图144至图147对差分数据的匹配性判定处理进行说明。车辆用程序改写系统1在改写对象ECU19中开始安装之前进行差分数据的匹配性判定处理。

[0789] 如图144所示,ECU19在差分数据的匹配性判定部103中,具有差分数据获取部103a、匹配性判定部103b、写入数据复原部103c、数据写入部103d、数据验证值计算部103e、改写规格数据获取部103f、数据识别信息获取部103g、以及改写面信息获取部103h。

[0790] 差分数据获取部103a获取用于对改写对象ECU19的电子控制装置的数据储存区域进行改写的数据、即表示旧数据与新数据的差分的差分数据。匹配性判定部103b基于与在闪存的数据储存区域中存储的储存数据相关的第一判定信息、以与差分数据相关联的方式获取到的第二判定信息,而判定差分数据是否与数据储存区域或者储存数据匹配。例如第一判定信息是针对储存数据的数据验证值,第二判定信息是针对旧数据的数据验证值或者针对新数据的数据验证值。若由匹配性判定部103b判定为差分数据的匹配性为正,则写入数据复原部103c使用差分数据和储存数据来复原写入数据,若由匹配性判定部103b判定为差分数据的匹配性为否,则写入数据复原部103c不复原写入数据。若通过写入数据复原部103c复原写入数据,则数据写入部103d将该复原后的写入数据储存于数据储存区域。数据验证值计算部103e计算针对将储存数据分割为一个以上而得到的各块的数据验证值。另外,数据验证值计算部103e获取与差分数据一同接收到的针对各块的数据验证值。

[0791] 改写规格数据获取部103f从CGW13获取CGW用的改写规格数据中的对应于自身的改写规格数据。数据识别信息获取部103g获取储存于差分数据的数据识别信息、以及旧数据即旧应用程序的数据识别信息。数据识别信息是能够识别差分数据是否为用于自身的数据的信息,例如是将规定的算法应用于旧数据而计算出的数据。

[0792] 改写面信息获取部103h获取在从CGW13获取到的改写规格数据中储存的改写面信息、以及旧数据即旧应用程序的改写面信息。改写面信息是表示写入数据即差分数据是用于写入闪存的哪个面的数据的信息,在改写对象ECU19为双面存储器或者单面挂起存储器的情况下,指定A面或者B面。在改写对象ECU19为单面单独存储器的情况下,不使用改写面信息。匹配性判定部103b若通过写入数据接收部101接收从CGW13分发的差分数据,则使用数据识别信息、数据验证值、改写面信息中的至少任意一个来判定该差分数据的匹配性。

[0793] 接下来,参照图145至图147对改写对象ECU19的差分数据的匹配性判定部103的作用进行说明。改写对象ECU19执行差分数据的匹配性判定程序,进行差分数据的匹配性判定处理。改写对象ECU19若开始差分数据的匹配性判定处理,则作为用于判定差分数据的匹配性的第一判定信息,获取与差分数据相关的数据识别信息、数据验证值和改写面信息(S1701)。作为第二判定信息,改写对象ECU19获取数据识别信息、旧数据的数据验证值、新数据的数据验证值和改写面信息(S1702)。

[0794] 改写对象ECU19判定第一判定信息的数据识别信息与第二判定信息的数据识别信息是否一致,并且第一判定信息的改写面信息与第二判定信息的改写面信息是否一致(S1703)。改写对象ECU19若判定为第一判定信息的数据识别信息与第二判定信息的数据识别信息不一致、或者第一判定信息的改写面信息与第二判定信息的改写面信息不一致(S1703:“否”),则判定为是不适当的写入数据,向CGW13通知错误信息,结束差分数据的匹配性判定处理。

[0795] 改写对象ECU19若判定为第一判定信息的数据识别信息与第二判定信息的数据识别信息一致,并且第一判定信息的改写面信息与第二判定信息的改写面信息一致(S1703:“是”),则对第一判定信息的数据验证值与第二判定信息的新数据的数据验证值进行对照,判定两者是否一致(S1704、相当于匹配性判定步骤)。改写对象ECU19若判定为两者不一致(S1704:“否”),则对第一判定信息的数据验证值与第二判定信息的旧数据的数据验证值进行对照,判定两者是否一致(S1705、相当于匹配性判定步骤)。

[0796] 改写对象ECU19若判定为两者一致(S1705:“是”),则复原写入数据(S1706、相当于复原写入数据的步骤),将该复原后的写入数据写入闪存(S1707、相当于数据写入步骤),判定是否完成了全部的写入(S1708)。改写对象ECU19若判定为未完成全部的写入(S1708:“否”),则返回步骤S1703,重复步骤S1703之后的步骤。改写对象ECU19若判定为完成了全部的写入(S1708:“是”),则结束差分数据的匹配性判定处理。

[0797] 改写对象ECU19若判定为第一判定信息的数据验证值与第二判定信息的新数据的数据验证值不一致(S1704:“否”),并且第一判定信息的数据验证值与第二判定信息的旧数据的数据验证值不一致(S1705:“否”),则判定是否是针对第一块的写入(S1709)。

[0798] 改写对象ECU19若判定为是针对第一块的写入(S1709:“是”),则由于是没有完成针对第一块的写入的状态,因此判定是否完成了全部的写入(S1708)。改写对象ECU19若判定为不是针对第一块的写入、即是针对第二块之后的块的写入(S1709:“否”),则重试写入(S1710),判定是否完成了全部的写入(S1708)。

[0799] 参照图146对改写对象ECU19是单面单独存储器ECU的情况进行说明。在从CGW13分发的差分数据中添加数据识别信息(旧)、针对每个旧数据的块而计算出的CRC值(数据验证值)。数据识别信息(旧)是指对旧数据(旧应用程序)应用规定的算法而计算出的数据。在将数据识别信息作为判定信息的情况下,改写对象ECU19对添加于差分数据的数据识别信息(旧)与存储于闪存的程序(旧数据)的数据识别信息(旧)进行对照,判定差分数据的匹配性。存储于闪存的数据识别信息(旧)是在将程序写入改写对象ECU19的闪存时,一并地存储的信息。或者,也可以将从写入到闪存的程序的起始地址起规定比特数视为数据识别信息(旧)。

[0800] 在将数据验证值作为判定信息的情况下,改写对象ECU19对存储于闪存的程序的每个块的CRC值进行计算,对在接收到的差分数据中添加的针对旧数据的CRC值(CRC(B1～Bn))和针对新数据的CRC值(CRC(B1’～Bn’)与该计算出的CRC值进行对照,判定差分数据的匹配性。在未将新程序写入闪存的状态下,在全部的块中接收到的CRC值与计算出的CRC值一致。改写对象ECU19在直到闪存的m(＜n)块为止写入了新程序的状态下写入中断、并再次开始的情况下,直到块1～m为止与针对新数据的CRC值(CRC(B1’～Bn’)一致,因此跳过写入处理(S1706、S1707)。而且,改写对象ECU19从块m+1观察与针对旧数据的CRC值(CRC(B1～Bn))的一致来进行写入处理(S1706、S1707)。

[0801] 另外,也可以在差分数据中添加新程序(新数据)的数据识别信息(新)和每个块的CRC值(CRC(B1‘～Bn’))。改写对象ECU19在将差分数据写入闪存,并完成了新程序的安装时,也一并地存储数据识别信息(新),用于下次的程序更新中的匹配性判定。另外,改写对象ECU19在完成了新程序的安装时,针对每个块读出写入到闪存的新程序而计算CRC值,与添加于差分数据的CRC值进行比较,验证是否正确地写入。

[0802] 参照图147对改写对象ECU19为双面存储器ECU的情况进行说明。在该情况下也是,在将数据验证值作为判定信息的情况下,改写对象ECU19对存储于闪存的程序的每个块的CRC值进行计算,对添加于接收到的差分数据的针对旧数据的CRC值(CRC(B1～Bn))、针对新数据的CRC值(CRC(B1’～Bn’)与该计算出的CRC值进行对照,判定差分数据的匹配性。在未将新程序写入于闪存的状态下,在全部的块中接收到的CRC值与计算出的CRC值一致。改写对象ECU19在直到闪存的m(＜n)块为止写入了新程序的状态下写入中断、并再次开始的情

况下,直到块1～m为止与针对新数据的CRC值(CRC(B1'～Bn'))一致,因此跳过写入处理(S1706、S1707)。而且,改写对象ECU19从块m+1观察与针对旧数据的CRC值(CRC(B1～Bn))的一致来进行写入处理(S1706,S1707)。

[0803] 假设闪存的A面为运用面并且是版本2.0,B面为非运用面并且是版本1.0,差分数据是用于将B面更新为版本3.0的差分数据(版本1.0与版本3.0的差分数据)。在从CGW13分发的差分数据中,添加数据识别信息(表示旧(版本1.0)的信息)、针对旧数据(旧程序(版本1.0))的每个块而计算出的CRC值、以及针对新数据(新程序(版本3.0))的每个块而计算出的CRC值。

[0804] 另外,在改写规格数据中包含表示针对改写对象ECU19的差分数据是写入闪存的哪个面的数据的改写面信息。在将改写面信息作为判定信息的情况下,改写对象ECU19对从改写规格数据中获取到的改写面信息和改写对象ECU19的非运用面信息(B面)进行对照,判定差分数据的匹配性。在将数据识别信息作为判定信息的情况下,改写对象ECU19对添加于差分数据的数据识别信息(旧(版本1.0))和存储于闪存的非运用面(B面)的旧程序(版本1.0)的数据识别信息(旧)进行对照,判定差分数据的匹配性。在将数据验证值作为判定信息的情况下,改写对象ECU19对存储于闪存的非运用面(B面)的旧程序(版本1.0)的每个块的CRC值进行计算,对添加于差分数据的CRC值(CRC(B1～Bn))与该计算出的CRC值进行对照,判定差分数据的匹配性。

[0805] 在上述的图143和图144的例子中,说明了数据识别信息和数据验证值被添加于差分数据,与差分数据一同从CGW13分发。然而,也可以将这些数据识别信息和数据验证值作为差分数据的头信息而添加,CGW13在向改写对象ECU19分发差分数据之前,向改写对象ECU19分发头信息。改写对象ECU19在从CGW13接收到头信息时,使用数据识别信息和数据验证值来判定差分数据的匹配性。

[0806] 另外,在图179和图180中,以改写数据为差分数据的情况为例进行了说明,但在改写数据为全部数据的情况下也同样。另外,在改写对象ECU19为单面单独存储器的情况下,在使用回滚用的差分数据而返回到原来的版本时也进行相同的匹配性判定。

[0807] 如以上说明那样,改写对象ECU19通过进行差分数据的匹配性判定处理,仅在差分数据的匹配性为正的情况下,执行基于差分数据而生成的写入数据的写入,将在差分数据的匹配性为否的情况下写入了基于差分数据而生成的写入数据的情况防患于未然。例如对于闪存的B面为非运用面的改写对象ECU19,在用于写入A面的差分数据包含于分发数据包的情况下,能够在将差分数据写入闪存之前检测不匹配。另外,在将其他ECU用的差分数据、版本不匹配的差分数据作为自身用的差分数据而包含于分发数据包的情况下,能够在将差分数据写入闪存之前检测不匹配。

[0808] 另外,改写对象ECU19在中断了写入数据的写入之后再次开始的情况下,基于针对闪存的储存数据的数据验证值、附带于接收到的差分数据的旧数据的数据验证值和新数据的数据验证值而判定差分数据的匹配性。改写对象ECU19也可以基于针对储存数据的数据验证值和接收到的新数据的验证值而判定差分数据的匹配性,从判定为该判定结果为否的最终块起,基于针对储存数据的数据验证值和接收到的旧数据的数据验证值而判定差分数据的匹配性。

[0809] 另外,改写对象ECU19直到判定为差分数据的匹配性为否的最终块的至少前段块

为止跳过写入数据的写入,从最终块或者该终块的后段块再次开始写入数据的写入。在块大小与写入数据的写入区域的数据大小相等的情况下,由于直到最终块为止完成写入数据的写入,因此只要跳过直到最终块为止的写入,从最终块的后段块再次开始写入即可。另一方面,在块大小与写入数据的写入区域的数据大小不相等的情况下,有可能在最终块中断写入数据的写入,因此需要从最终块再次开始写入。

[0810] (18)改写的执行控制处理

[0811] 参照图148至图155对改写的执行控制处理进行说明。车辆用程序改写系统1在ECU19中进行改写的执行控制处理。

[0812] 如图148所示,ECU19在改写的执行控制部104中,具有程序执行部104a、切换请求接收部104b、数据获取部104c、面信息通知部104d、固件获取部104e、安装执行部104f、以及激活执行部104g。程序执行部104a在执行运用面的应用程序、参数数据的过程中,执行运用面的改写程序而改写非运用面。切换请求接收部104b从CGW13接收激活请求。数据获取部104c从外部获取非运用面中的需要改写的区域的写入数据。面信息通知部104d向外部通知双面改写信息(以下,称为面信息)。固件获取部104e从外部获取改写程序的固件。安装执行部104f若被从CGW13指示安装,则将写入数据写入闪存,执行安装。激活执行部104g若被从CGW13指示激活,则在重新启动时执行切换运用面的激活。

[0813] 接下来,参照图149至图155对ECU19的改写的执行控制部104的作用进行说明。改写对象ECU19执行改写的执行控制程序,进行改写的执行控制处理。作为改写的执行控制处理,改写对象ECU19进行通常动作处理、改写动作处理、信息通知处理、以及应用程序的验证处理。以下,对各个处理进行说明。在本实施方式中,对改写对象ECU19为双面存储器ECU或者单面挂起存储器ECU的情况进行说明。

[0814] (18-1)通常动作处理

[0815] 改写对象ECU19若伴随着IG电源接通等,从停止状态或者睡眠状态转移至启动状态,则开始通常动作处理。改写对象ECU19若开始通常动作处理,则基于A面和B面的启动面判定信息确定出启动面(S1801),在该启动面启动(S1802)。改写对象ECU19对存储于启动面(运用面)的程序的完整性进行验证,判定启动面是否为正(S1803)。

[0816] 改写对象ECU19若判定为启动面的完整性的验证结果为否,判定为启动面为否(S1803:“否”),则向CGW13发送表示启动面的完整性的验证结果为否的错误信息(S1804),结束通常动作处理。CGW13若从改写对象ECU19接收错误信息,则向DCM12发送该错误信息。DCM12若从CGW13接收错误信息,则将接收到的该错误信息上传到中心装置3。即,若在改写对象ECU19中判定为启动面的完整性的验证结果为否,则向CGW13、DCM12、中心装置3通知该内容。

[0817] 改写对象ECU19若判定为启动面的完整性的验证结果为正,判定为启动面为正(S1803:“是”),则对存储于改写面(非运用面)的程序的完整性进行验证,判定改写面是否为正(S1805)。

[0818] 改写对象ECU19若判定为改写面的完整性的验证结果为否,判定为改写面为否(S1805:“否”),则向CGW13发送表示改写面的完整性的验证结果为否的错误信息(S1806)。CGW13若从改写对象ECU19接收错误信息,则向DCM12发送该错误信息。DCM12若从CGW13接收错误信息,则将接收到的该错误信息上传到中心装置3。即,若在改写对象ECU19中判定为改

写面的完整性的验证结果为否,则向CGW13、DCM12、中心装置3通知该内容。

[0819] 在执行应用程序之前由引导程序执行上述的完整性验证的处理。改写对象ECU19若结束完整性验证,则确定引导向量表的配置地址(S1807),确定通常时向量表的配置地址(S1808),确定应用程序的起始地址(S1809),执行应用程序,结束通常动作处理。

[0820] (18-2)改写动作处理

[0821] 改写对象ECU19若从CGW13接收改写请求,则开始改写动作处理。改写对象ECU19若开始改写动作处理,则与CGW13之间使用安全访问密钥来进行认证(S1811)。改写对象ECU19若判定为认证结果为正(S1812:“是”),则等待写入数据的接收(S1813)。改写对象ECU19若判定为从CGW13接收到写入数据(S1813:“是”),则在执行配置于启动面(运用面)的应用程序的状态下,对配置于改写面(非运用面)的应用程序进行改写(S1814)。

[0822] 改写对象ECU19判定是否完成了应用程序的改写(S1815),若判定为完成了应用程序的改写(S1815:“是”),则判定检验是否为正(S1816)。改写对象ECU19若判定为检验为正(S1816:“是”),则将改写完成标志设定为“OK”(S1817)。检验是指写入到非运用面的应用程序的完整性验证。

[0823] 改写对象ECU19判定是否从CGW13接收到激活请求(S1818)。改写对象ECU19若判定为从CGW13接收到激活请求(S1818:“是”),则例如将改写面的启动面信息的数值自加1,更新改写面的启动面信息(S1819)。即,此后,更新为表示在该改写面启动的信息。改写对象ECU19判定是否从CGW13接收到版本读出信号(S1820),若判定为接收到版本读出信号(S1820:“是”),则向CGW13发送运用面的版本信息、非运用面的版本信息、能够确定哪个面是运用面的识别信息(S1821),结束改写动作处理。这里,在改写对象ECU19中,也可以由切换前的运用面(旧面)的应用程序执行从S1811到S1821为止的全部的处理。另外,在改写对象ECU19中,由切换前的运用面(旧面)的应用程序执行从S1811到S1819为止的处理,在进行了S1819之后重新启动,由此也可以由切换后的运用面(新面)的应用程序执行从S1820到S1821为止的处理。

[0824] (18-3)信息通知处理

[0825] 改写对象ECU19若从停止状态或者睡眠状态转移至启动状态、或者例如IG电源接通或者从CGW13接收通知请求,则开始信息通知处理。改写对象ECU19若开始信息通知处理,则向CGW13通知能够唯一地确定与运用面、非运用面相关的应用程序、参数数据的识别信息和能够唯一地确定运用面、非运用面的存储器上的配置场所的识别信息。即,改写对象ECU19获取与启动面相关的启动面信息(S1831),向CGW13发送该启动面信息(S1832)。改写对象ECU19向CGW13发送A面和B面中的哪个面是启动面的信息和启动面的版本信息等来作为启动面信息。

[0826] 改写对象ECU19若完成向CGW13发送启动面信息,则获取与改写面相关的改写面信息(以下,也称为面信息)(S1833),向CGW13发送获取到的该改写面信息(S1834)。改写对象ECU19向CGW13发送A面和B面中的哪个面是改写面的信息和改写面的版本信息等来作为改写面信息。改写对象ECU19若完成向CGW13发送改写面信息,则向CGW13发送能够确定存储器上的启动面和改写面的配置地址的识别信息(S1835),结束信息通知处理。改写对象ECU19例如向CGW13发送闪存中的A面的开始地址和结束地址以及B面的开始地址和结束地址,来作为能够确定地址的识别信息。

[0827] (18-4)改写程序的验证处理

[0828] 改写对象ECU19若开始改写程序的验证处理,则判定是否获取了能够确定用于执行改写程序的地址的识别信息(S1841)。改写对象ECU19若判定为获取了能够确定用于执行改写程序的地址的识别信息(S1841:“是”),判定该识别信息与改写对象ECU19的启动面信息是否一致(S1842)。具体而言,改写对象ECU19判定启动面信息中的表示启动面的面信息与该识别信息是否一致。

[0829] 改写对象ECU19若判定为识别信息与改写对象ECU19的启动面信息一致(S1842:“是”),则获取改写程序(S1843),判定是否获取了能够确定用于进行应用程序的改写的地址的识别信息(S1844)。这里,改写对象ECU19如果是将改写程序预先嵌入于闪存的嵌入型结构,则在S1843中,从闪存获取启动面的写入程序而在RAM上执行。改写对象ECU19如果是未将改写程序预先嵌入闪存,从外部下载改写程序的下载型结构,则在S1843中,将改写程序下载到RAM而执行。

[0830] 改写对象ECU19若判定为获取了能够确定用于进行应用程序的改写的地址的识别信息(S1844:“是”),则判定该识别信息与改写对象ECU19的启动面信息是否一致(S1845)。具体而言,改写对象ECU19判定启动面信息中的表示非启动面的面信息与该识别信息是否一致。改写对象ECU19若判定为识别信息与ECU19的启动面信息一致(S1845:“是”),则进行应用程序的改写(S1846),结束改写程序的验证处理。

[0831] 改写对象ECU19若判定为识别信息与ECU19的启动面信息不一致(S1842:“否”)、或者判定为识别信息与改写对象ECU19的启动面信息不一致(S1845:“否”),则判定为不是在运用面、非运用面能够执行的应用程序、参数数据,向CGW13发送否定响应(S1847),结束改写程序的验证处理。例如在采用闪存的A面为运用面且B面为非运用面的双面存储器ECU的情况下,用于执行改写程序的地址是运用面即A面的地址,用于进行应用程序的改写的地址是非运用面即B面的地址。

[0832] 另外,如图150所示,改写对象ECU19也可以在从CGW13获取写入数据之前,从CGW13获取能够确定地址的识别信息。另外,如图151所示,改写对象ECU19也可以在从CGW13获取写入数据时获取能够确定地址的识别信息。改写对象ECU19例如在获取写入数据之前从CGW13接收改写规格数据,获取改写面信息。在改写面信息中包含能够识别哪个面是启动面、哪个面是改写面的数据,因此将该能够识别的数据作为能够确定地址的识别信息而使用。

[0833] 另外,与CGW13进行安装指示处理对应地,改写对象ECU19进行上述的(18-2)改写动作处理。这里,对由CGW13进行的安装指示处理进行说明。

[0834] CGW13若开始安装指示处理,则识别改写规格数据(S1851),对于全部的改写对象ECU19指定停车中的安装,但判定对于全部的改写对象ECU19是否指定车辆行驶中的安装,对于改写对象ECU19的每个存储器种类是否指定安装(S1852～S1854)。

[0835] CGW13若判定为对于全部的改写对象ECU19指定停车中的安装(S1852:“是”),则以得到安装的同意并且处于停车中为条件,向改写对象ECU19指示安装(S1855)。CGW13若判定为对于全部的改写对象ECU19指定车辆行驶中的安装(S1853:“是”),则以得到安装的同意且处于车辆行驶中为条件,向改写对象ECU19指示安装(S1856)。

[0836] CGW13若判定为对于改写对象ECU19的每个存储器种类指定安装(S1854:“是”),则

根据改写规格数据来判定存储器种类是双面存储器、还是单面挂起存储器或者单面单独存储器(S1857、S1858)。

[0837] CGW13若判定为改写对象ECU19的存储器种类为双面存储器,满足第一规定条件(S1857:“是”),则以得到安装的同意且处于车辆行驶中为条件,向改写对象ECU19指示安装(S1859)。CGW13若判定为改写对象ECU19的存储器种类是单面挂起存储器或者单面单独存储器,满足第二规定条件(S1858:“是”),则以得到安装的同意且处于停车中为条件,向改写对象ECU19指示安装(S1860)。

[0838] CGW13判定在全部的改写对象ECU19中是否完成了安装(S1861),若判定为在全部的改写对象ECU19中未完成安装(S1861:“否”),则返回步骤S1851,重复步骤S1851之后。

[0839] 即,如果改写对象ECU19为双面存储器ECU,则CGW13在车辆能够行驶的过程中指示安装。双面存储器ECU通过在车辆能够行驶的过程中被从CGW13指示安装,而在车辆能够行驶的过程中进行安装(相当于安装执行步骤)。如果改写对象ECU19为单面挂起存储器ECU、单面单独存储器ECU,则CGW13在停车中指示安装。单面挂起存储器ECU、单面单独存储器ECU通过在停车中被从CGW13指示安装,而在停车中进行安装(相当于安装执行步骤)。

[0840] CGW13若判定为在全部的改写对象ECU19中完成了安装(S1861:“是”),则判定是否处于停车中(S1862),若判定为处于停车中(S1862:“是”),则在停车中向改写对象ECU19指示激活(S1863),结束安装指示处理。改写对象ECU19通过在停车中被从CGW13指示激活,而进行激活(相当于激活执行步骤)。

[0841] 如以上说明那样,改写对象ECU19通过进行改写的执行控制处理,而在多个面具有数据储存面的构成中,在执行运用面的应用程序的过程中,执行运用面的改写程序而改写非运用面。能够改写应用程序的期间不限于停车状态,在车辆行驶中也能够改写应用程序。改写对象ECU19如果是双面存储器ECU,则通过在车辆能够行驶的过程中被从CGW13指示安装,能够在车辆能够行驶的过程中进行安装。改写对象ECU19如果是单面挂起存储器ECU、单面单独存储器ECU,则通过在停车中被从CGW13指示安装,能够在停车中进行安装。

[0842] (19)会话的确立处理

[0843] 参照图156至图169对会话的确立处理进行说明。车辆用程序改写系统1在改写对象ECU19中进行会话的确立处理。

[0844] 如图156所示,ECU19在会话的确立部105中,具有应用执行部105a、无线改写请求确定部105b、以及有线改写请求确定部105c。应用执行部105a具有对各程序的执行进行调停的功能。无线改写请求确定部105b具有确定经由无线的程序改写请求的功能。有线改写请求确定部105c具有确定经由有线的程序改写请求的功能。

[0845] 图157表示存储于闪存的各程序的构成。车辆控制程序是用于实现搭载于ECU19自身的车辆控制功能(例如转向控制功能)的程序。有线诊断程序是用于从车辆外部经由有线进行ECU19自身的诊断的程序。无线诊断程序是用于从车辆外部经由无线进行ECU19自身的诊断的程序。无线改写程序是用于进行从车辆外部经由无线获取到的程序的改写的程序。有线改写程序是用于进行从车辆外部经由有线获取到的程序的改写的程序。车辆控制程序作为第一程序配置于应用区域。有线诊断程序和有线改写程序作为第二程序配置于应用区域。无线诊断程序和无线改写程序作为第三程序配置于应用区域。换言之,第二程序是进行车辆控制以外的经由有线的特殊处理的程序,第三程序是进行车辆控制以外的经由无线的

特殊处理的程序。另外,有线改写程序也可以不配置于应用区域,而作为第四程序配置于引导区域。

[0846] 应用执行部105a控制为,能够同时执行第一程序、第二程序、以及第三程序(进行非排他控制)。应用执行部105a例如能够同时执行车辆控制程序、有线诊断程序、以及无线诊断程序。即,应用执行部105a能够同时执行车辆控制、利用有线的ECU19的诊断、以及利用无线的ECU19的诊断。同样,应用执行部105a控制为,能够同时执行车辆控制程序、有线诊断程序、以及无线改写程序,能够同时执行车辆控制程序、有线改写程序、以及无线诊断程序,能够同时执行车辆控制程序、有线改写程序、以及无线改写程序。

[0847] 另一方面,应用执行部105a进行排他控制,使得不能同时执行第二程序内的各程序。同样,进行排他控制,使得不能同时执行第三程序内的各程序。应用执行部105a例如对有线诊断程序和有线改写程序进行排他控制,对无线诊断程序和无线改写程序进行排他控制。即,应用执行部105a仅执行经由有线的特殊处理中的一个程序。同样,应用执行部105a仅执行经由无线的特殊处理中的一个程序。

[0848] 换言之,也可以说,无线改写程序配置在无线诊断程序的内部,作为无线诊断程序的一部分而嵌入。即,若通过将无线改写程序配置在无线诊断程序的内部的结构,在执行车辆控制程序和有线诊断程序的过程中像后述那样从默认会话或者无线诊断会话向无线改写会话迁移状态,则应用执行部105a控制为在持续车辆控制程序和有线诊断程序的执行的状态下,执行无线改写程序。应用执行部105a在持续车辆控制程序和有线诊断程序的执行的状态下,开始无线改写程序的执行,由此能够同时执行车辆控制程序、有线诊断程序、以及无线改写程序。即,应用执行部105a控制为,能够同时执行车辆控制、利用有线的ECU19的诊断、以及利用无线的应用程序的改写。

[0849] 这里,根据诊断处理、改写处理的具体的内容,产生无法同时执行利用有线的诊断和利用无线的诊断以及利用有线的改写和利用无线的改写的状况。例如在利用有线的改写和利用无线的改写对相同的区域进行改写的情况下,两者的处理冲突。因此,应用执行部105a根据处理、请求的具体内容,对有线诊断程序和无线诊断程序进行排他控制,另外,对有线改写程序和无线改写程序进行排他控制。另外,根据诊断处理的内容,还产生无法持续通常的车辆控制的情况。例如在进行使ECU进行动作而读出该结果的诊断处理的情况下,与通常的车辆控制不能同时执行。在该情况下,应用执行部105a进行如下的调停控制,使车辆控制程序待机,执行有线或者无线诊断程序。

[0850] 另一方面,在有线改写程序不配置于应用区域,而作为第四程序配置于引导区域的情况下,应用执行部105a进行与上述局部不同的调停控制。如图157中虚线所示,有线改写程序作为第四程序配置于有线诊断程序的外部,作为有线诊断程序的一部分而未嵌入。在该情况下,应用执行部105a在执行第四程序时,进行排他控制以结束第一~第三程序。即,应用执行部105a从执行第一~第三程序的模式切换为执行第四程序的专用模式。换言之,若通过将有线改写程序配置于有线诊断程序的外部的构成,在执行车辆控制程序和无线诊断程序的过程中像后述那样从有线诊断会话向有线改写会话迁移状态,则有线改写程序控制为停止车辆控制程序和无线诊断程序的执行,开始有线改写程序的执行。应用执行部105a通过停止车辆控制程序和无线诊断程序的执行,开始有线改写程序的执行,而不能同时执行车辆控制程序、无线诊断程序、以及有线改写程序,能够仅执行有线改写程序。即,

应用执行部105a控制为不能同时执行车辆控制、利用无线的ECU19的诊断、以及利用有线的应用程序的改写，能够仅执行利用有线的应用程序的改写。

[0851] 如图158所示，作为与利用有线的特殊处理相关的第一状态，应用执行部105a管理默认的状态(默认会话)、有线诊断的状态(有线诊断会话)、以及有线改写的状态(有线改写会话)。另外，作为与利用无线的特殊处理相关的第二状态，管理默认的状态(默认会话)和无线改写的状态(无线改写会话)，管理动作的内部状态。

[0852] 作为第一状态的状态迁移，应用执行部105a使能够依据诊断通信标准进行车辆控制的默认会话、能够从车辆外部经由有线进行ECU19的诊断的有线诊断会话、能够进行从车辆外部经由有线获取到的应用程序的改写的有线改写会话排他地进行状态迁移。使会话排他地状态迁移是指不能同时确立会话，使会话非排他地状态迁移是指能够同时确立会话。

[0853] 第一状态下的默认会话是表示没有进行利用有线的特殊处理的状态的模式，是能够执行车辆控制的状态。默认会话也可以说是对车辆控制完全没有带来影响的处理、例如也可以执行与车辆控制无关的诊断程序的模式。与车辆控制无关的诊断程序是用于进行故障代码等信息的读出等的程序。有线诊断会话是执行与ECU19的诊断相关的诊断程序的模式。至少在通过执行诊断程序而成为能够对车辆控制带来影响的状态的情况下，从默认会话转移至有线诊断会话。与ECU19的诊断相关的诊断程序是用于进行通信停止、诊查屏蔽、致动器驱动等的程序。有线改写会话是执行从车辆外部经由有线获取到的应用程序的改写的模式。

[0854] 应用执行部105a在第一状态下像以下那样进行会话的状态迁移。若在第一默认会话的状态下产生利用有线的诊断请求，则应用执行部105a根据诊断会话转移请求从第一默认会话转移至有线诊断会话，执行利用有线的诊断处理。若在有线诊断会话的状态下产生会话复原请求、产生超时、电源断开或者接收法规服务，则应用执行部105a从有线诊断会话转移至第一默认会话。若在第一默认会话的状态下产生有线改写请求，则应用执行部105a在根据诊断会话转移请求从第一默认会话转移至有线诊断会话之后，根据改写会话转移请求从有线诊断会话转移至有线改写会话，执行有线改写处理。若在有线改写会话的状态下产生会话复原请求、产生超时、电源断开或者接收法规服务，则应用执行部105a从有线改写会话转移至第一默认会话。另外，应用执行部105a根据会话维持请求维持当前的会话而不转移。

[0855] 作为第二状态的状态迁移，应用执行部105a使能够依据诊断通信标准而进行车辆控制的默认会话、与从车辆外部经由无线获取到的应用程序的改写相关的无线改写会话排他地状态迁移。无线改写会话是执行从车辆外部经由无线获取到的应用程序的改写的模式。

[0856] 应用执行部105a在第二状态下像以下那样进行会话的状态迁移。若在第二默认会话的状态下产生无线改写请求，则应用执行部105a根据改写会话转移请求从第二默认会话转移至无线改写会话，执行无线改写处理。若在无线改写会话的状态下产生会话复原请求、产生超时或者电源断开，则应用执行部105a从无线改写会话转移至第二默认会话。另外，应用执行部105a根据会话维持请求维持当前的会话而不转移。

[0857] 应用执行部105a执行作为第一程序的车辆控制程序，并且管理与利用有线的特殊处理相关的第一状态以及与利用无线的特殊处理相关的第二状态。例如若第一状态和第二

状态都在默认会话中产生有线诊断请求,则应用执行部105a在持续车辆控制程序的状态下,使第一状态转移至有线诊断会话,开始有线诊断程序的执行。在该状态下,若产生无线改写请求,则应用执行部105a在持续车辆控制程序和有线诊断程序的执行的状态下,使第二状态转移至无线改写会话,开始无线改写程序的执行。在该状态下,若产生有线改写请求,则应用执行部105a例如结束无线改写程序的执行,使第二状态转移至默认会话,并且结束有线诊断程序的执行,使第一状态转移至有线改写会话,开始有线改写程序的执行。应用执行部105a为了防止对相同的存储器区域的写入处理冲突,而进行排他地状态迁移(进行排他地控制),使得不同时确立第一状态的有线改写会话和第二状态的无线改写会话。

[0858] 无线改写请求确定部105b判定从外部接收到的改写请求的识别信息,确定无线改写请求。即,若从中心装置3向DCM12下载重编数据,CGW13向改写对象ECU19分发从DCM12传输来的重编数据,则无线改写请求确定部105b通过从CGW13与重编数据一同接收表示无线改写请求的识别信息,而确定无线改写请求。

[0859] 有线改写请求确定部105c判定从外部接收到的改写请求的识别信息,确定有线改写请求。即,若工具23与DLC连接器22连接,CGW13向改写对象ECU19分发从工具23传输来的重编数据,则有线改写请求确定部105c通过从CGW13与重编数据一同接收表示有线改写请求的识别信息,而确定有线改写请求。

[0860] 识别信息例如也可以是对应于在有线改写请求和无线改写请求中不同的识别ID的信息,也可以是,虽然是在有线改写请求和无线改写请求中相同的识别ID但对应于不同的数据的信息。即,只要能够识别有线改写请求和无线改写请求,则也可以是任意的信息。

[0861] 在应用执行部105a中,在图158中,对作为与利用无线的特殊处理相关的第二状态,管理默认会话和无线改写会话这两个状态的构成进行了说明,也可以如图159和图160所示,采用作为第二状态,管理默认会话、无线诊断会话和无线改写会话这三个状态的构成。无线诊断会话是执行用于从车辆外部经由无线进行ECU19的诊断的无线诊断程序的模式。至少在执行对车辆控制带来影响的无线诊断程序的情况下,转移至无线诊断会话。

[0862] 在图159所示的构成的情况下,应用执行部105a如以下那样进行第二状态的状态迁移。若在第二默认会话的状态下产生利用无线的诊断请求,则应用执行部105a根据诊断会话转移请求从第二默认会话转移至无线诊断会话,执行无线诊断处理。若在无线诊断会话的状态下产生会话复原请求、产生超时、电源断开,则应用执行部105a从无线诊断会话转移至第二默认会话。若在第二默认会话的状态下产生无线改写请求,则应用执行部105a在根据诊断会话转移请求从第二默认会话转移至无线诊断会话之后,根据改写会话转移请求从无线诊断会话转移至无线改写会话,执行无线改写处理。若在无线改写会话的状态下产生会话复原请求、产生超时、电源断开,则应用执行部105a从无线改写会话转移至第二默认会话。

[0863] 在图160所示的构成的情况下,应用执行部105a如以下那样进行第二状态的状态迁移。若在第二默认会话的状态下产生利用无线的诊断请求,则应用执行部105a根据诊断会话转移请求从第二默认会话转移至无线诊断会话,执行无线诊断处理。若在无线诊断会话的状态下产生会话复原请求、产生超时、电源断开,则应用执行部105a从无线诊断会话转移至第二默认会话。若在第二默认会话的状态下产生无线改写请求,则应用执行部105a在根据诊断会话转移请求从第二默认会话转移至无线诊断会话之后,根据改写会话转移请求

从无线诊断会话转移至无线改写会话、或者根据改写会话转移请求从第二默认会话转移至无线改写会话，执行无线改写处理。若在无线改写会话的状态下产生会话复原请求、产生超时、电源断开，则应用执行部105a从无线改写会话转移至第二默认会话。

[0864] 另外，第一状态的有线诊断会话与第二状态的无线诊断会话也可以执行相同的诊断程序，也可以执行不同的诊断程序。第一状态的有线改写会话与第二状态的无线改写会话也可以执行相同的改写程序，也可以执行不同的改写程序。例如也可以执行存储器的消除、写入等共用的改写程序。

[0865] 在图159和图160所示的构成中，对第一状态的各会话和第二状态的各会话的调停进行说明。如图157中说明的那样，说明如下的情况，有线诊断程序作为第二程序配置于应用区域，无线诊断程序和无线改写程序作为配置于第三程序应用区域，有线诊断程序作为第四程序配置于引导区域。换言之，是关于如下的构成的说明，无线改写程序作为无线诊断程序的一部分而嵌入，另一方面有线改写程序作为有线诊断程序的一部分而未嵌入。在该情况下，第一状态和第二状态的各会话中的程序执行的调停如图161所示那样。

[0866] 在第二状态为无线改写会话、并且第一状态为默认会话的情况下，应用执行部105a执行车辆控制程序，并且执行无线改写程序。在第二状态为无线改写会话、并且第一状态为有线诊断会话的情况下，应用执行部105a执行车辆控制程序，并且同时执行无线改写程序和有线诊断程序。

[0867] 另一方面，在第一状态为有线改写会话、并且第二状态为默认会话的情况下，应用执行部105a结束车辆控制程序，仅执行有线改写程序。在第一状态为有线改写会话、并且第二状态为无线诊断会话的情况下，应用执行部105a结束无线诊断程序和车辆控制程序，仅执行有线改写程序。即，作为仅执行第四程序即有线改写程序的专用模式，应用执行部105a对第一～第三程序进行排他控制。

[0868] 另外，在有线诊断程序和有线改写程序作为第二程序配置于应用区域的构成中，各程序的调停与图161局部不同。即，在无线改写程序作为无线诊断程序的一部分被嵌并且有线改写程序作为有线诊断程序的一部分被嵌入的构成中，第一状态和第二状态的各会话中的程序执行的调停如图162所示那样。在这种情况下，在第一状态为有线改写会话、并且第二状态为默认会话的情况下，应用执行部105a执行车辆控制程序，并且执行有线改写程序。在第一状态为有线改写会话、并且第二状态为无线诊断会话的情况下，应用执行部105a执行车辆控制程序，并且同时执行有线改写程序和无线诊断程序。

[0869] 接下来，参照图163至图167对上述的构成的作用进行说明。在ECU19中，微机33执行会话的确立程序，进行会话的确立处理。

[0870] 微机33若检测出电源接通而启动，则执行会话确立程序而进行状态迁移管理处理，进行管理第一状态的状态迁移的状态迁移管理处理和管理第二状态的状态迁移的状态迁移管理处理。以下，对各个状态迁移管理处理进行说明。另外，这里，对应用执行部105a通过图158所示的构成、即不具有无线诊断会话的构成来管理第二状态的情况进行说明。

[0871] (19-1)第一状态的状态迁移管理处理

[0872] 微机33若检测出电源接通而启动，开始第一状态的状态迁移管理处理，则判定改写完成标志，判定是否正常地完成上次的应用程序的改写(S1901)。微机33若判定为改写完成标志为正，判定为正常地完成了上次的应用程序的改写(S1901:“是”)，则使第一状态转

移至默认会话(S1902)。即,微机33通过使第一状态转移至默认会话,而开始车辆控制处理。

[0873] 微机33若执行车辆控制程序而开始车辆控制处理,则判定在执行车辆控制处理的过程中,是否产生了有线诊断请求(S1903),判定是否产生了有线改写请求(S1904),判定状态迁移管理的完成条件的成立(S1905)。微机33若判定为在执行车辆控制处理的过程中,产生了有线诊断请求(S1903:“是”),则使第一状态从默认会话转移至有线诊断会话(S1906),执行有线诊断程序而开始有线诊断处理(S1907)。微机33判定有线诊断处理的完成条件的成立(S1908),若判定为有线诊断处理的完成条件成立(S1908:“是”),则结束有线诊断程序而结束有线诊断处理(S1909),使第一状态从有线诊断会话转移至默认会话(S1910)。

[0874] 微机33若判定为在执行车辆控制处理的过程中,产生了有线改写请求(S1904:“是”),则开始有线改写请求产生时的改写排他处理(S1911)。即,是用于进行排他控制的处理,以使有线改写处理与无线改写处理不冲突。微机33若开始有线改写请求产生时的改写排他处理,则判定在第二状态下是否处于转移至无线改写会话的过程中、即第二状态是否为无线改写会话(S1921)。微机33若判定为在第二状态下不处于转移至无线改写会话的过程中(S1921:“否”),则将第一状态确定为能够转移至有线改写会话(S1922)。微机33结束有线改写请求产生时的改写排他处理,复原到第一状态的状态迁移管理处理。

[0875] 微机33若判定为在第二状态下处于转移至无线改写会话的过程中(S1921:“是”),则判定使有线改写会话和无线改写会话中的哪个优先来进行排他控制。具体而言,微机33判定有线改写会话优先条件、无线改写会话优先条件、转移中改写会话优先条件中的任一方是否成立(S1923~S1925)。有线改写会话优先条件是使有线改写会话比无线改写会话优先的条件。无线改写会话优先条件是使无线改写会话比有线改写会话优先的条件。转移中改写会话优先条件是使转移中的改写会话优先、即使先转移的会话优先的条件。预先设定采用这些优先条件中的哪个条件,例如也可以针对车辆设定优先条件标志,也可以针对每个改写ECU设定优先条件标志。

[0876] 微机33若判定为有线改写会话优先条件成立(S1923:“是”),则在第二状态下根据会话复原请求使无线改写会话转移至默认会话而中断无线改写(S1926),将第一状态确定为能够转移至有线改写会话(S1922)。伴随着默认会话转移,微机33结束无线改写程序。微机33结束有线改写请求产生时的改写排他处理,复原到第一状态的状态迁移管理处理。

[0877] 微机33若判定为无线改写会话优先条件成立(S1924:“是”),则废弃有线改写请求而持续无线改写(S1927)。即,微机33将第二状态维持在无线改写会话,持续无线改写程序的执行,将第一状态确定为不能转移至有线改写会话(S1928)。微机33结束有线改写请求产生时的改写排他处理,复原到第一状态的状态迁移管理处理。

[0878] 微机33若判定为转移中改写会话优先条件成立(S1925:“是”),则在该情况下,也废弃有线改写请求而持续无线改写(S1927)。即,微机33将第二状态维持在无线改写会话,持续无线改写程序的执行,将第一状态确定为不能转移至有线改写会话(S1928)。微机33结束有线改写请求产生时的改写排他处理,复原到第一状态的状态迁移管理处理。微机33通过如这样执行有线改写请求产生时的改写排他处理,而排他地控制有线改写会话和无线改写会话,使得不同时确立会话。

[0879] 微机33若复原到第一状态的状态迁移管理处理,则作为有线改写请求产生时的改写排他处理的结果,判定是否能够转移至有线改写会话(S1912)。微机33若通过确定为利用

有线改写请求产生时的改写排他处理能够转移至有线改写会话,而判定为能够转移(S1912:“是”),则使第一状态从默认会话经由有线诊断会话而转移至有线改写会话(S1913),中断车辆控制处理而开始有线改写处理(S1914)。伴随着有线改写会话转移,微机33结束车辆控制程序。

[0880] 微机33判定有线改写处理的完成条件的成立(S1915),若判定为有线改写处理的完成条件成立(S1915:“是”),则完成有线改写处理(S1916),使第一状态从有线改写会话转移至默认会话(S1917)。这里,有线改写处理的完成条件例如是指应用程序的写入全部完成,执行了完整性验证的情况等。

[0881] 微机33若通过确定为利用有线改写请求产生时的改写排他处理不能转移至有线改写会话,而判定为不能转移(S1912:“否”),则不使第一状态从默认会话经由有线诊断会话而转移至有线改写会话。即,微机33将第一状态维持在默认会话。微机33若判定为状态迁移管理的完成条件成立(S1905:“是”),则完成第一状态的状态迁移管理处理。

[0882] 另外,以上,说明了如下的情况,微机33若在有线改写请求产生时的改写排他处理中,判定为在第二状态下处于转移至无线改写会话的过程中,判定为有线改写会话优先条件成立,则在第二状态下中断无线改写,但也可以根据无线改写的未改写余量而判定是否中断无线改写会话。

[0883] 微机33若判定为在第二状态下处于转移至无线改写会话的过程中(S1921:“是”),判定为有线改写会话优先条件成立(S1923:“是”),则在该转移中的无线改写会话中判定无线改写的未改写余量是否为规定量以上(例如20%以上)(S1931)。微机33若判定为无线改写的未改写余量为规定量以上(S1931:“是”),则使第二状态从无线改写会话转移至默认会话而中断无线改写(S1926)。微机33伴随着转移至默认会话,而结束无线改写程序。微机33若判定为无线改写的未改写余量不是规定量以上(S1931:“否”),则废弃该有线改写请求而持续无线改写(S1927)。即,如果直到完成无线改写为止的剩余时间比较长,则微机33中断无线改写会话,但如果直到完成无线改写为止的剩余时间比较短,则微机33持续无线改写会话而不中断。

[0884] (19-2)第二状态的状态迁移管理处理

[0885] 微机33若检测出电源接通而启动,开始第二状态的状态迁移管理处理,则判定改写完成标志,判定是否正常地完成了上次的应用程序的改写(S1941)。微机33若判定为改写完成标志为正,判定为正常地完成了上次的应用程序的改写(S1941:“是”),则使第二状态转移至默认会话(S1942)。即,微机33通过使第二状态转移至默认会话,而执行车辆控制程序,开始车辆控制处理。

[0886] 微机33若开始车辆控制处理,则判定是否产生了无线改写请求(S1943),判定状态迁移管理的完成条件的成立(S1944)。微机33若判定为在执行车辆控制处理的过程中,产生了无线改写请求(S1943:“是”),则开始无线改写请求产生时的改写排他处理(S1944)。微机33若开始无线改写请求产生时的改写排他处理,则判定在第一状态下是否处于转移至有线改写会话的过程中、即第一状态是否为有线改写会话(S1961)。微机33若判定为在第一状态下不处于转移至有线改写会话的过程中(S1961:“否”),则确定为能够转移至无线改写会话(S1962)。微机33结束无线改写请求产生时的改写排他处理,复原到第二状态的状态迁移管理处理。

[0887] 微机33若判定为在第一状态下处于转移至有线改写会话的过程中(S1961:“是”),则判定使有线改写会话和无线改写会话中的哪个优先来进行排他控制。具体而言,微机33判定无线改写会话优先条件、有线改写会话优先条件、以及转移中改写会话优先条件中的任意条件是否成立(S1963～S1965)。

[0888] 微机33若判定为无线改写会话优先条件成立(S1963:“是”),则在第一状态下根据会话复原请求使有线改写会话转移至默认会话而中断有线改写(S1966),将第二状态确定为能够转移至无线改写会话(S1962)。微机33伴随着转移至默认会话,而结束有线改写程序。微机33结束无线改写请求产生时的改写排他处理,复原到第二状态的状态迁移管理处理。

[0889] 微机33若判定为有线改写会话优先条件成立(S1964:“是”),则废弃无线改写请求而持续有线改写(S1967)。即,微机33将第一状态维持在有线改写会话,持续有线改写程序的执行,将第二状态确定为不能转移至无线改写会话(S1968)。微机33结束无线改写请求产生时的改写排他处理,复原到第二状态的状态迁移管理处理。

[0890] 微机33若判定为转移中改写会话优先条件成立(S1965:“是”),则在该情况下也是,废弃无线改写请求而持续有线改写(S1967)。即,微机33将第一状态维持在有线改写会话,持续有线改写程序的执行,将第二状态确定为不能转移至无线改写会话(S1968)。微机33结束无线改写请求产生时的改写排他处理,复原到第二状态的状态迁移管理处理。微机33通过如这样执行无线改写请求产生时的改写排他处理,而排他地控制有线改写会话和无线改写会话,不会同时确立会话。

[0891] 微机33若复原到第二状态的状态迁移管理处理,则作为无线改写请求产生时的改写排他处理的结果,判定是否能够转移至无线改写会话(S1945)。微机33若通过确定为利用无线改写请求产生时的改写排他处理能够转移至无线改写会话,而判定为能够转移(S1945:“是”),则使第二状态从默认会话转移至无线改写会话(S1946),执行无线改写程序而开始无线改写处理(S1847)。微机33判定无线改写处理的完成条件的成立(S1948),若判定为无线改写处理的完成条件成立(S1948:“是”),则结束无线改写处理(S1949),使第二状态从无线改写会话转移至默认会话(S1950)。伴随着转移至默认会话,微机33结束无线改写程序。这里,无线改写处理的完成条件例如是指应用程序的写入全部完成,执行了完整性验证的情况等。

[0892] 微机33若通过确定为利用无线改写请求产生时的改写排他处理不能转移至无线改写会话,而判定为不能转移(S1945:“否”),则不使第二状态从默认会话转移至无线改写会话。即,微机33将第二状态维持在默认会话。微机33若判定为状态迁移管理的完成条件成立(S1951:“是”),则结束第二状态的状态迁移管理处理。

[0893] 以上,说明了在应用执行部105a中,能够独立(同时)执行与利用有线的特殊处理相关的程序以及与利用无线的特殊处理相关的程序的情况,也可以如图165所示,采用将有线诊断程序和无线诊断程序共用化的构成。采用将车辆控制程序作为第一程序配置于应用区域、将诊断程序(有线诊断程序和无线诊断程序)和无线改写程序作为第二程序配置于应用区域的构成。有线改写程序也可以作为第二程序配置于应用区域,也可以作为第三程序配置于引导区域。应用执行部105a同时执行第一程序和第二程序。即,应用执行部105a控制为,能够同时执行车辆控制程序和共用化的诊断程序。另一方面,应用执行部105a对构成第

二程序的各程序的执行进行排他控制。即,控制为有线诊断程序、无线诊断程序、无线改写程序和有线改写程序中的仅任意一个进行动作。

[0894] 如图166所示,作为状态,应用执行部105a管理默认的状态(默认会话)、诊断的状态(诊断会话)、有线改写的状态(有线改写会话)、以及无线改写的状态(无线改写会话),管理动作的内部状态。这里管理的状态并不是利用有线和无线独立地管理的状态,而是混合地作为一个状态进行管理。

[0895] 在该构成中,也是应用执行部105a执行车辆控制程序,并且开始诊断程序的执行。另外,应用执行部105a执行车辆控制程序,并且开始无线改写程序、有线改写程序的执行。另一方面,应用执行部105a排他地控制无线诊断程序和有线诊断程序的执行。另外,应用执行部105a也排他地控制有线诊断程序和无线诊断程序、有线改写程序和无线改写程序的执行。即,应用执行部105a排他地控制构成第二程序的各程序的执行。

[0896] 这里,在将有线改写程序作为第三程序配置于引导区域的情况下,应用执行部105a排他地执行控制第三程序以及第一和第二程序。即,在执行有线改写程序的情况下,结束第一程序和第二程序,作为专用模式进行动作。

[0897] 如图166所示,应用执行部105a若产生诊断请求,则持续车辆控制程序的执行,并且转移至诊断会话,开始诊断程序的执行。在该状态下,若产生无线改写请求,则应用执行部105a结束诊断程序,转移至无线改写会话,并且开始无线改写程序的执行。持续车辆控制程序的执行。另一方面,在产生了有线改写请求的情况下,应用执行部105a结束诊断程序和车辆控制程序,转移至有线改写会话,并且开始有线改写程序的执行。

[0898] 即使无线改写程序配置在诊断程序的内部,若在执行车辆控制程序和诊断程序的过程中从诊断会话向无线改写会话迁移状态,则应用执行部105a在中断车辆控制程序和诊断程序的执行之后开始无线改写程序的执行。另外,在不伴随会话的情况下能够持续处理。

[0899] 如果有线改写程序配置于诊断程序的外部,则当在执行车辆控制程序和诊断程序的过程中从诊断会话向有线改写会话迁移状态时,应用执行部105a停止车辆控制程序和无线诊断程序的执行,有线改写程序开始执行。即,应用执行部105a不能同时执行车辆控制、利用有线或者无线的ECU19的诊断、以及利用有线的应用程序的改写,能够仅执行利用有线的应用程序的改写。

[0900] 如以上说明那样,ECU19通过进行会话的确立处理,而执行第一状态的状态迁移管理处理和第二状态的状态迁移管理处理,管理第一状态和第二状态中的各会话的状态迁移,非排他地确立第一状态的默认会话或者有线诊断会话和第二状态的无线改写会话。对于车辆控制或者ECU19的诊断和利用无线的程序的改写的请求,控制为非排他地执行车辆控制程序或者ECU19的诊断程序和无线改写程序,能够对于来自外部的各种请求,适当地调停。

[0901] 另外,在ECU19中,排他地确立有线改写会话和无线改写会话。能够控制为排他地执行有线改写程序和无线改写程序,适当地调停利用有线的程序的改写和利用无线的程序的改写。

[0902] 另外,在ECU19中,若有线改写会话优先条件成立,则使有线改写会话比无线改写会话优先。通过预先设定有线改写会话优先条件,与利用无线的程序的改写相比,能够优先地执行利用有线的程序的改写。例如与由车辆的用户指示的利用无线的程序的改写相比,

能够优先地执行由经销商等设置者指示的利用有线的程序的改写。

[0903] 另外,在ECU19中,若无线改写会话优先条件成立,则使无线改写会话比有线改写会话优先。通过预先设定无线改写会话优先条件,与利用有线的程序的改写相比,能够优先地执行利用无线的程序的改写。例如与经销商等设置者指示的利用有线的程序的改写相比,能够优先地执行由车辆的用户指示的利用无线的程序的改写。

[0904] 另外,在ECU19中,若转移中改写会话优先条件成立,则使转移中的改写会话优先。通过预先设定转移中改写会话优先条件,能够优先地执行转移中的改写。即,能够使有线改写和无线改写中的先开始的一方持续而不中断。

[0905] 在2面具有应用区域的构成中,采用在各应用区域配置有车辆控制程序、诊断程序、以及无线改写程序的构成,并行(同时)地执行车辆控制程序或者诊断程序、以及无线改写程序。通过设计闪存30d的存储器结构,能够并行地执行车辆控制程序或者诊断程序、以及无线改写程序。

[0906] 若在执行车辆控制程序或者有线诊断程序的过程中确定无线改写请求,则持续车辆控制程序或者有线诊断程序的执行,执行无线改写程序。在执行车辆控制程序或者有线诊断程序的过程中产生了无线改写请求时,能够并行(同时)地执行车辆控制程序或者有线诊断程序、以及无线改写程序。

[0907] 若在执行无线改写程序的过程中确定车辆控制请求或者有线诊断请求,则持续无线改写程序的执行,执行车辆控制程序或者有线诊断程序。在执行无线改写程序的过程中产生了车辆控制请求或者有线诊断请求时,能够并行(同时)地执行无线改写程序、以及车辆控制程序或者有线诊断程序。

[0908] 若在执行车辆控制程序或者无线诊断程序的过程中确定有线改写请求,则停止车辆控制程序或者无线诊断程序的执行,执行有线改写程序。在执行车辆控制程序或者无线诊断程序的过程中产生了有线改写请求时,能够仅排他地执行有线改写程序。

[0909] 在供重编固件嵌入的重编固件嵌入型的情况下,使用配置于应用区域的固件,执行改写程序。不用从外部下载重编固件,就能够执行非运用面的应用程序的改写处理。

[0910] 在从外部下载重编固件的重编固件下载型的情况下,使用从外部下载的固件,执行改写程序。在减少了应用区域中的改写程序的容量的基础上,能够执行非运用面的应用程序的改写处理。

[0911] 对在实质性的2面具有应用区域的双面存储器进行了说明,但关于在伪2面具有应用区域的单面暂停方式存储器、外置存储器,也能够应用。

[0912] 对根据旧数据和差分重编数据生成新数据的差分改写的情况进行了说明,但在删除旧数据而写入新数据的全改写的情况下也能够应用。

[0913] 对改写ECU19的应用程序的情况进行了说明,但在改写CGW13的应用程序的情况下也能够应用。即,也可以使CGW13的闪存26d为双面构成而成为与ECU19的闪存30d同等的构成,使微机26具有与ECU19的微机33同等的功能。

[0914] (20)重试点的确定处理

[0915] 参照图170至图174对重试点的确定处理进行说明。车辆用程序改写系统1在改写对象ECU19中进行重试点的确定处理。重试点是指在将写入数据分多次写入的情况下,在中断写入数据的写入的情况下,为了从中途再次开始该中断的写入数据的写入,表示处理完

成到何处的信息。作为中断写入数据的写入的情况,例如存在产生了基于用户操作的取消的情况、存在产生了通信中断等异常的情况、在停车状态下点火从断开切换为接通的情况等。

[0916] 在ECU19中,程序改写部102利用多个改写程序分担与应用程序的改写相关联的一系列的处理。程序改写部102具有进行第一处理的第一改写程序、进行第二处理的第二改写程序,依次执行各个改写程序。由第一改写程序进行的第一处理例如是消除闪存的数据的存储器消除处理、对写入数据进行写入的数据写入处理等。由第二改写程序进行的第二处理例如是检验处理、篡改检查处理等。

[0917] 如图170所示,ECU19在重试点的确定部106中,具有第一处理标志设定部106a、第二处理标志设定部106b、以及重试点确定部106c。若程序改写部102执行第一改写程序,则第一处理标志设定部106a判定该程序改写部102是否通过第一改写程序完成了第一处理,设定表示该判定结果的第一处理标志。第一处理标志设定部106a若判定为程序改写部102完成了第一处理,则将第一处理标志设定为“OK”。

[0918] 若程序改写部102执行第二改写程序,则第二处理标志设定部106b判定该程序改写部102是否通过第二改写程序完成了第二处理,设定表示该判定结果的第二处理标志。第二处理标志设定部106b若判定为程序改写部102完成了第二处理,则将第二处理标志设定为“OK”。

[0919] 在中断了与程序的改写相关联的处理的一部分的情况下,重试点确定部106c根据第一处理标志和第二处理标志确定由程序改写部102重试应用程序的改写时的重试点。另外,重试点确定部106c预先存储直到中断时为止的更新数据的写入量,在再次开始与程序的改写相关联的处理的情况下,向CGW13请求发送基于该存储的更新数据的写入量的更新数据。如图207所示,第一处理标志和第二处理标志存储于改写对象ECU19的闪存的同一块内。

[0920] 接下来,参照图172至图174对改写对象ECU19的重试点的确定部106的作用进行说明。改写对象ECU19执行重试点的确定程序,进行重试点的确定处理。作为重试点的确定处理,改写对象ECU19进行处理标志的设定处理、处理标志的判定处理。以下,对各个处理进行说明。

[0921] (20-1)处理标志的设定处理

[0922] 改写对象ECU19若开始处理标志的设定处理,判定是否完成应用程序的改写前的预先处理(S2001)。改写对象ECU19若判定为完成应用程序的改写前的预先处理(S2001:“是”),则将第一处理标志设定为“NG”,将第二处理标志设定为“NG”,并进行存储(S2002、相当于第一处理标志设定步骤、第二处理标志设定步骤)。

[0923] 改写对象ECU19若从CGW13接收写入数据,则开始第一处理(S2003),判定是否完成了第一处理(S2004)。改写对象ECU19若判定为完成了第一处理(S2004:“是”),则在将第二处理标志维持为“NG”的状态下,将第一处理标志设定为“OK”,并进行存储(S2005、相当于第一处理标志设定步骤、第二处理标志设定步骤)。一并地,改写对象ECU19存储有表示写入完成到闪存的哪处的写入完成地址。

[0924] 改写对象ECU19若开始朝向CGW13的写入完成通知等第二处理(S2006),则判定是否完成了第二处理(S2007)。改写对象ECU19若判定为完成了第二处理(S2007:“是”),则在

将第一处理标志维持为“OK”的状态下,将第二处理标志设定为“OK”并进行存储(S2008、相当于第一处理标志设定步骤、第二处理标志设定步骤),结束处理标志的设定处理。

[0925] (20-2)处理标志的判定处理

[0926] 改写对象ECU19若在从睡眠或者停止状态启动时,开始处理标志的判定处理,则由引导程序启动(S2011),从闪存读出第一处理标志和第二处理标志而进行判定(S2012～S2015)。

[0927] 改写对象ECU19若判定为第一处理标志为“NG”且第二处理标志为“NG”(S2012:“是”),则将重试点确定为第一处理的起始,向CGW13通知从第一处理的起始开始的重试请求(S2016、相当于重试点确定步骤),结束重试点的确定处理。即,改写对象ECU19向CGW13请求写入数据的分发。此时,改写对象ECU19还向CGW13通知从闪存读出的写入完成地址,由此CGW13确定可以对分割地分发的写入数据中的哪个进行分发。改写对象ECU19若判定为第一处理标志为“NG”且第二处理标志为“OK”(S2013:“是”),则在该情况下也是,将重试点确定为第一处理的起始(S2016、相当于重试点确定步骤),向CGW13通知从第一处理的起始开始的重试请求(S2017),结束处理标志的判定处理。

[0928] 改写对象ECU19若判定为第一处理标志为“OK”且第二处理标志为“NG”(S2014:“是”),则将重试点确定为第二处理的起始(S2018、相当于重试点确定步骤),向CGW13通知从第二处理的起始开始的重试请求(S2019),结束处理标志的判定处理。作为第二处理,ECU19例如向CGW13通知写入完成到哪个地址。

[0929] 改写对象ECU19若判定为第一处理标志为“OK”且第二处理标志为“OK”(S2015:“是”),则向CGW13通知与应用程序的改写相关联的处理的完成(S2020),结束处理标志的判定处理。另外,在CGW13分割地分发写入数据的情况下,改写对象ECU19按分割后的写入数据单位进行上述的重试点的设定。

[0930] 如以上说明那样,改写对象ECU19通过进行重试点的确定处理,而设定表示第一处理是否完成的第一处理标志,设定表示第二处理是否完成的第二处理标志,根据第一处理标志和第二处理标志确定出重试点。例如在第一处理完成且第二处理未完成的状态下改写对象ECU19被重新启动的情况下,能够抑制再次写入相同的写入数据。

[0931] 另外,改写对象ECU19在预先存储有完成了写入的写入数据的数据量、即将写入数据的写入完成到哪个字节,再次开始写入数据的写入的情况下,对CGW13请求从第几字节的写入数据起发送。改写对象ECU19在预先存储有写入数据的写入完成到哪个字节,并再次开始的情况下,对CGW13请求从第几字节的写入数据起发送,由此在再次开始时,CGW13能够避免再次发送已发送的写入数据,改写对象ECU19能够从完成了写入数据的写入的下一写入区域对写入数据进行写入。另外,不具有这样的存储有写入数据的写入完成到哪个字节的功能的改写对象ECU19在再次开始写入数据的写入的情况下,对CGW13请求从起始的写入数据起发送。

[0932] (21)进展状态的同步控制处理

[0933] 参照图175至图180对进展状态的同步控制处理进行说明。车辆用程序改写系统1在CGW13和中心装置3中进行进展状态的同步控制处理。作为能够进行用户的输入操作的显示终端5,车辆用程序改写系统1具有移动终端6和车载显示器7。车载显示器7通过与CGW13的协作而显示表示改写的进展的进展画面。移动终端6通过与中心装置3连接,显示表示由

中心装置3提供的改写的进展的进展画面。CGW13和中心装置3为了使在这些移动终端6和车载显示器7中显示的信息同步,而进行进展状态的同步控制处理。

[0934] 如上述的图30所示,例如如果改写对象ECU19为搭载了双面存储器的ECU19,则根据告知应用程序的改写而得到用户的同意的活动通知阶段、执行从中心装置3向DCM12下载写入数据的下载阶段、执行从CGW13向改写对象ECU19分发写入数据的安装阶段、将下次启动时的启动面从旧面切换为新面的激活阶段,进行与应用程序的改写相关联的步骤。即,用户对移动终端6、车载显示器7进行操作,推进同意各阶段的执行等与应用程序的改写相关联的一系列步骤。

[0935] 如图175所示,CGW13在进展状态的同步控制部88中,具有第一进展状态判定部88a、第一进展状态发送部88b、第二进展状态获取部88c、以及第一显示指示部88d。第一进展状态判定部88a判定程序的改写所涉及的第一进展状态,例如判定活动通知阶段、下载阶段、安装阶段、激活阶段这样的进展状态。活动通知阶段是直到接收活动、显示图32～图33所示的画面、得到用户同意为止的阶段。下载阶段是显示图34～图37所示的画面,得到用户同意而执行下载的阶段。安装阶段是下载完成,显示图38～图42所示的画面,得到用户同意而执行安装的阶段。激活阶段是显示图43所示的画面,得到用户的同意而执行激活的阶段。

[0936] 第一进展状态判定部88a若在用户乘车中,用户在车载显示器7中选择“同意程序更新的执行”,进行使阶段向下一步推进的操作,则通过将用户操作信号从车载显示器7向CGW13发送,而确定用户在车载显示器7中进行的操作,判定第一进展状态。在该情况下,选择“同意程序更新的执行”对应于对图70所示的“下载开始”按钮503a、图75所示的“立即更新”按钮506a、“预约更新”按钮506b、图79所示的“OK”按钮508b中的任意按钮进行操作。第一进展状态判定部88a若判定第一进展状态,则将该判定出的第一进展状态作为当前进展状态进行管理。

[0937] 第一进展状态发送部88b若通过第一进展状态判定部88a判定第一进展状态,则向中心装置3发送该判定出的第一进展状态,并且向车载显示器7等各车载显示设备发送。第二进展状态获取部88c从中心装置3获取程序的改写所涉及的第二进展状态。第一显示指示部88d若通过第一进展状态判定部88a判定第一进展状态,通过第二进展状态获取部获取第二进展状态,则基于该判定出的第一进展状态和获取到的该第二进展状态而指示在车载显示器7中能够显示的内容的制作。

[0938] 这里,在第二进展状态获取部88c从中心装置3获取第二进展状态的情况下,如果第二进展状态是比当前进展状态靠前的阶段,则第一进展状态判定部88a将第二进展状态作为当前进展状态进行管理。即,利用第二进展状态的值更新第一进展状态。而且,第一进展状态发送部88b向中心装置3发送当前进展状态即第一进展状态。例如在第一进展状态为“等待下载阶段”,进行了移动终端6中的用户同意操作的情况下,第二进展状态获取部88c从中心装置3获取“下载执行中阶段”来作为第二进展状态。由于从中心装置3获取到的“下载执行中阶段”是比当前进展状态靠前的阶段,因此第一进展状态判定部88a利用第二进展状态的值更新当前进展状态即第一进展状态,并且向中心装置3发送该更新后的第一进展状态,并且向车载显示器7等各种车载显示设备发送。作为第一进展状态,除了“下载执行中阶段”之外,也可以发送表示下载的进展程度的“下载完成X%”。

[0939] 在车载显示器7中产生了用户操作信号的情况下,第一显示指示部88d基于由第一

进展状态判定部88a判定出的第一进展状态,而指示内容的制作。另外,在移动终端6中产生了用户操作信号的情况下,第一显示指示部88d基于由第二进展状态获取部88c获取到的第二进展状态,而指示内容的制作。另外,如果采用管理为由第一进展状态判定部88a判定的第一进展状态始终为当前进展状态的构成、即采用主装置11管理当前进展状态的构成,则第一显示指示部88d只要基于第一进展状态来指示内容的制作即可。

[0940] 如图176所示,中心装置3在进展状态的同步控制部53中,具有第二进展状态判定部53a、第二进展状态发送部53b、第一进展状态获取部53c、以及第二显示指示部53d。第二进展状态判定部53a判定程序的改写所涉及的第二进展状态,例如判定活动通知阶段、下载阶段、安装阶段、激活阶段这样的进展状态。若在用户下车中(停车中),用户在移动终端6中选择“同意程序更新的执行”,进行使阶段向下一步推进的操作,如果是移动终端6与中心装置3能够进行数据通信的环境,则第二进展状态判定部53a接收从移动终端6发送的用户操作信号。

[0941] 第二进展状态判定部53a基于在此前由第一进展状态获取部53c从主装置11接收到的第一进展状态即当前进展状态和户操作信号,而判定第二进展状态。第二进展状态判定部53a例如若在当前进展状态为“等待安装阶段”时,接收表示“同意”的用户操作信号,则作为第二进展状态,判定为“安装执行中阶段”。另外,第二进展状态判定部53a也可以是“在等待安装阶段中存在用户同意”这样的判定。如果是中心装置3与DCM12能够进行数据通信的环境,则从中心装置3向DCM12发送移动终端6的用户操作信号。而且,通过从DCM12向CGW13传输用户操作信号,CGW13能够判定用户在移动终端6中进行的操作,判定进展状态。

[0942] 第二进展状态发送部53b若通过第二进展状态判定部53a判定第二进展状态,则向主装置11发送该判定出的第二进展状态。第一进展状态获取部53c从主装置11获取程序的改写所涉及的第一进展状态,作为当前进展状态进行管理。作为当前进展状态,也可以利用第一进展状态的值更新第二进展状态。第二显示指示部53d若通过第二进展状态判定部53a判定第二进展状态,通过第一进展状态获取部53d获取第一进展状态,则基于该判定出的第二进展状态和获取到的该第一进展状态,而指示在移动终端6中能够显示的内容的制作。

[0943] 例如如果仅是移动终端6的用户操作信号,则由第二进展状态判定部53a判定的第二进展状态与由第一进展状态获取部53d获取到的第一进展状态表示相同的进展状态。因此,第二显示指示部53d也可以基于第二进展状态而指示内容的制作。然后,在产生了车载显示器7的用户操作信号的情况下,第二显示指示部53d基于所获取到的第一进展状态而指示内容的制作。

[0944] 移动终端6例如若从中心装置3接收SMS来作为进展状态信号,则由用户选择记载于SMS的URL而与中心装置3连接,显示由中心装置3提供的规定阶段的画面。

[0945] 接下来,参照图177至图180对CGW13中的进展状态的同步控制部88和中心装置3中的进展状态的同步控制部53的作用进行说明。

[0946] 如图177所示,主装置11和中心装置3通过发送接收第一进展状态信号和第二进展状态信号,而使移动终端6和车载显示器7中的阶段的进展状态的显示同步。即,主装置11若更新当前进展状态即第一进展状态,则向中心装置3发送第一进展状态信号,并且向车载显示器7等各种车载显示设备发送第一进展状态信号。中心装置3将第一进展状态信号作为当前进展状态发送至移动终端6。由此,如果移动终端6能够访问中心装置3,则使移动终端6和

车载显示器7中的阶段的进展状态的显示同步。中心装置3基于移动终端6的用户同意操作向主装置11发送第二进展状态信号,由此如果移动终端6能够访问中心装置3,则使移动终端6和车载显示器7中的阶段的进展状态的显示同步。

[0947] 获取了第二进展状态信号的主装置11也可以在更新了当前进展状态即第一进展状态之后,向中心装置3和车载显示器7等各车载显示设备发送第一进展状态。即,通过由主装置11向中心装置3和车载显示器7等各车载显示设备发送当前进展状态,而实现作为阶段的管理装置的功能。这里,从移动终端6、车载显示器7和中心装置3发送的第二进展状态信号也可以是表示某个阶段的通知,但也可以是表示存在用户同意操作的通知、表示被操作的按钮的主旨的通知。

[0948] CGW13若开始进展状态的同步控制处理,则向车载显示器7发送分发规格数据(S2101)。分发规格数据中包含车载显示器7朝向用户显示的文本、内容。CGW13基于来自车载显示器7或者中心装置3的通知而判定用户在车载显示器7或者移动终端6中是否进行了操作(S2102)。CGW13若判定为用户在车载显示器7或者移动终端6中进行了操作(S2102:“是”),则基于第一进展状态,判定该操作是哪个阶段的操作(S2103～S2106、相当于第一进展状态判定步骤)。

[0949] CGW13若判定为是活动通知阶段(S2103:“是”),则实施活动通知阶段的处理(S2107),向车载显示器7和中心装置3发送表示该活动通知阶段的处理的进展状态的第一进展状态信号(S2111)。活动通知阶段的处理是指获取针对车载显示器7或者移动终端6的用户的输入操作等。

[0950] CGW13例如从车载显示器7、或者移动终端6经由中心装置3,除了获取同意或者不同意程序的更新之外,还获取允许执行的日期时间、场所等条件等。CGW13若从中心装置3经由DCM12获取了在移动终端6中存在同意的内容的用户的输入操作的情况,则向车载显示器7通知完成了同意的内容的进展。另一方面,CGW13若从车载显示器7获取了在车载显示器7中存在同意的内容的用户的输入操作的情况,则向中心装置3通知完成了同意的内容的进展。

[0951] CGW13若判定为是下载阶段(S2104:“是”),则实施下载阶段的处理(S2108),向车载显示器7和中心装置发送表示该下载阶段的处理的进展状态的第一进展状态信号(S2111)。下载阶段的处理例如是指计算分发数据包的下载完成了几%。

[0952] CGW13基于来自中心装置3的通知而决定下载完成了几%。CGW13向车载显示器7和中心装置3通知表示下载完成了几%的进展。CGW13重复这些处理直到分发数据包的下载完成为止。CGW13若下载完成,则向车载显示器7和中心装置3通知下载阶段完成的内容的进展。

[0953] CGW13若判定为是安装阶段(S2104:“是”),则实施安装阶段的处理(S2108),向车载显示器7和DCM12发送表示该安装阶段的处理的进展状态的进展状态信号(S2111)。安装阶段的处理例如是指计算向改写对象ECU19的安装完成了几%。

[0954] CGW13基于来自改写对象ECU19的通知而决定安装完成了几%。CGW13向车载显示器7和中心装置3通知表示安装完成了几%的进展。CGW13重复这些处理直到针对全部的改写对象ECU19的安装完成为止。CGW13若安装全部完成,则向车载显示器7和中心装置3通知安装阶段完成的内容的进展。

[0955] CGW13若判定为是激活阶段(S2104:“是”),则实施激活阶段的处理(S2108),向车载显示器7和DCM12发送表示该激活阶段的处理的进展状态的进展状态信号(S2111、相当于第一进展状态发送步骤)。激活阶段的处理例如是指计算属于同一组的一个以上的改写对象ECU19的激活完成了几%。CGW13基于来自改写对象ECU19的通知而决定激活完成了几%。CGW13向车载显示器7和中心装置通知表示激活完成了几%的进展。

[0956] CGW13判定是否完成了激活阶段(S2112),若判定为完成了激活阶段(S2112:“是”),则结束进展状态的同步控制处理。CGW13若判定为未完成激活阶段(S2112:“否”),则返回S2102。而且,CGW13推进各阶段的处理,并且计算处理完成了几%(S2107～S2110)。CGW13定期地向中心装置3发送阶段和完成了X%的内容来作为第一进展状态(S2111)。

[0957] 中心装置3若发送分发规格数据,开始进展状态的同步控制处理,则监视从DCM12发送的第一进展状态信号的接收(S2121)。中心装置3若判定为从DCM12接收到第一进展状态信号(S2121:“是”),则允许来自移动终端6的访问(S2122),判定根据第一进展状态信号确定出的阶段是哪个阶段(S2123～S2126)。

[0958] 中心装置3若判定为是活动通知阶段(S2123:“是”),则实施活动通知阶段的处理(S2127)。即,中心装置3制作活动通知阶段的画面,并且向移动终端6发送指示该活动通知阶段的画面的显示的显示指示信号,在移动终端6中通过与中心装置3的连接来显示活动通知阶段的画面。

[0959] 中心装置3若判定为是下载阶段(S2124:“是”),则实施下载阶段的处理(S2128)。即,中心装置3制作下载阶段的画面,并且向移动终端6发送指示下载阶段的画面的显示的显示指示信号,在移动终端6中通过与中心装置3的连接来显示下载阶段的画面。中心装置3若被从DCM12通知表示下载完成了几%的进展,则更新下载阶段的画面。

[0960] 中心装置3若判定为是安装阶段(S2125:“是”),则实施安装阶段的处理(S2129)。即,中心装置3制作安装阶段的画面,并且向移动终端6发送指示安装阶段的画面的显示的显示指示信号,在移动终端6中通过与中心装置3的连接来显示安装阶段的画面。中心装置3若被从DCM12通知表示安装完成了几%的进展,则更新安装阶段的画面。

[0961] 中心装置3若判定为是激活阶段(S2126:“是”),则实施激活阶段的处理(S2130)。即,中心装置3制作激活阶段的画面,并且向移动终端6发送指示激活阶段的画面的显示的显示指示信号,在移动终端6中通过与中心装置3的连接来显示激活阶段的画面。中心装置3若被从DCM12通知表示激活完成了几%的进展,则更新激活阶段的画面。中心装置3在对S2127～S2130中显示的画面进行用户同意等操作的情况下,向主装置11发送第二进展状态信号(S2131),结束进展状态的同步控制处理。

[0962] 车载显示器7若从CGW13接收分发规格数据,则开始进展显示处理,监视从CGW13发送的进展状态信号的接收(S2141)。车载显示器7若判定为从CGW13接收到进展状态信号(S2141:“是”),则允许车载显示器7的用户操作(S2142),判定根据进展状态信号确定出的阶段是哪个阶段(S2143～S2146)。

[0963] 车载显示器7若判定为是活动通知阶段(S2143:“是”),则使用在分发规格数据中包含的文本、内容等而显示活动通知阶段的画面(S2147)。车载显示器7若判定为是下载阶段(S2144:“是”),则显示下载阶段的画面(S2148)。车载显示器7若被从CGW13通知表示下载完成了几%的进展,则更新下载阶段的画面。

[0964] 车载显示器7若判定为是安装阶段(S2145:“是”),则显示安装阶段的画面(S2149)。车载显示器7若被从CGW13通知表示安装完成了几%的进展,则更新安装阶段的画面。车载显示器7若判定为是激活阶段(S2146:“是”),则显示激活阶段的画面(S2150)。车载显示器7若被从CGW13通知表示激活完成了几%的进展,则更新激活阶段的画面。

[0965] 如以上说明那样,在主装置11与中心装置3之间发送接收第一进展状态和第二进展状态。例如即使是移动终端6能够访问中心装置3,车载显示器7不能访问中心装置3的构成,通过在主装置11与中心装置3之间发送接收第一进展状态和第二进展状态,能够使应用程序的改写的进展状态等在多个显示终端适当地同步。

[0966] (22)显示控制信息的发送控制处理、(23)显示控制信息的接收控制处理

[0967] 参照图181和图182对中心装置3中的显示控制信息的发送控制处理进行说明,参照图183至图185对主装置11中的显示控制信息的接收控制处理进行说明。

[0968] 如图181所示,中心装置3在显示控制信息的发送控制部54中,具有写入数据存储部54a(相当于更新数据存储部)、显示控制信息存储部54b、以及信息发送部54c。写入数据存储部54a将针对多个改写对象ECU19的应用程序的改写作为一个活动,存储针对多个改写对象ECU19的写入数据。显示控制信息存储部54b存储包含显示控制信息的分发起始数据。显示控制信息是在车载显示器7中显示与改写对象ECU19中的应用程序的改写相关联的显示信息所需要的信息,是显示控制程序、属性信息。

[0969] 显示信息是指构成与应用程序的改写相关联的各种画面(活动通知画面、安装画面等)的数据。显示控制程序是实现与网页浏览器同等的功能的程序。属性信息是规定显示文字、显示位置、颜色等的信息。信息发送部54c向主装置11发送存储于写入数据存储部54a的写入数据和存储于显示控制信息存储部54b的显示控制信息。信息发送部54c将针对多个改写对象ECU19的写入数据作为一个数据包发送至主装置11。这里,作为显示控制信息,也可以包含表示是在哪个阶段显示的信息的阶段识别信息。例如是表示是在活动通知阶段、下载阶段、安装阶段和激活阶段中的哪个阶段显示的信息的阶段识别信息。

[0970] 接下来,参照图182对中心装置3中的显示控制信息的发送控制部54的作用进行说明。中心装置3执行显示控制信息的发送控制程序,进行显示控制信息的发送控制处理。

[0971] 中心装置3若开始显示控制信息的发送控制处理,则经由DCM12向CGW13发送分发起始数据(S2201、相当于控制信息发送步骤),经由DCM12向CGW13发送写入数据(S2202)。中心装置3经由DCM12向CGW13发送显示信息(S2203、相当于显示信息发送步骤),结束显示控制信息的发送控制处理。另外,中心装置3在发送与活动通知阶段、下载阶段、安装阶段、激活阶段的各阶段对应的显示控制信息的情况下,也可以将与各阶段对应的显示控制信息统一为一个文件发送至车载显示器7,也可以在每次结束阶段时向车载显示器7发送与下一阶段对应的显示控制信息。这里,中心装置3发送分发起始数据的时机可以构成为根据来自主装置11的请求来发送。

[0972] 如图183所示,CGW13在显示控制信息的接收控制部89中,具有信息接收部89a、改写指示部89b、以及显示指示部89c。信息接收部89a从中心装置3接收写入数据和显示控制信息。改写指示部89b若通过信息接收部89a从中心装置3接收写入数据,则向改写对象ECU19指示接收到的该写入数据的写入。在改写指示部89b向改写对象ECU19指示写入数据的写入之前,显示指示部89c向车载显示器7指示使用显示控制信息而显示与活动相关的信

息。另外,显示指示部89c也可以在写入数据的写入全部完成之后,指示作为历史信息,显示与活动相关的信息。

[0973] 接下来,参照图184对CGW13中的显示控制信息的接收控制部89的作用进行说明。CGW13执行显示控制信息的接收控制程序,进行显示控制信息的接收控制处理。由此,在作为显示终端,具有移动终端6和车载显示器7的情况下,能够使这些显示方式接近,能够提高用户的便利性。

[0974] CGW13若开始显示控制信息的接收控制处理,则从中心装置3经由DCM12接收分发规格数据(S2301、相当于控制信息接收步骤)。从中心装置3经由DCM12接收写入数据(S2302)。CGW13从中心装置3经由DCM12接收显示信息(S2303、相当于显示信息接收步骤)。CGW13判定是否使用来自中心装置3的分发规格数据中包含的显示控制信息(S2304)。CGW13若判定为使用显示控制信息(S2304:“是”),则向车载显示器7指示使用显示控制信息对显示信息进行显示(S2305)。即,CGW13向车载显示器7指示使用显示控制信息而显示与应用程序的改写相关联的画面。车载显示器7根据来自CGW13的指示,使用显示控制信息对显示信息进行显示。

[0975] CGW13若判定为不使用显示控制信息(S2304:“否”),则向车载显示器7指示使用预先保存的内容对显示信息进行显示(S2306)。即,CGW13向车载显示器7指示使用预先保存的内容而显示与应用程序的改写相关联的画面。车载显示器7根据来自CGW13的指示,使用预先保存的内容对显示信息进行显示。另外,车载显示器7在显示与活动通知阶段、下载阶段、安装阶段、激活阶段的各阶段对应的显示信息的情况下,也可以将与各阶段对应的显示控制信息统一而从中心装置3接收,也可以每次结束阶段时从中心装置3接收与下一阶段对应的显示控制信息。

[0976] 如图185所示,如果车载显示器7不具有网页浏览器的功能,在从中心装置3经由DCM12和CGW13向车载显示器7发送的发规格数据中包含属性信息但不包含显示控制程序,则车载显示器7使用预先保存的内容、帧,作为显示信息,在简易的画面显示属性信息。属性信息是指文本等数据及其显示位置、大小等,与在中心装置3制作的画面中使用的属性信息相同。即,车载显示器7显示的画面影像与中心装置3制作的画面影像存在背景、位图等不同点,但显示内容与中心装置3同等。

[0977] 如果车载显示器7不具有网页浏览器的功能,在从中心装置3经由DCM12和CGW13向车载显示器7发送的分发规格数据中包含显示控制程序和属性信息,则车载显示器7利用与中心装置3同等的画面对显示信息进行显示。这里,在分发规格数据中包含的显示控制程序和属性信息与在中心装置3制作的画面中使用的内容相同。

[0978] 如果车载显示器7不具有网页浏览器的功能但保存显示控制程序,在从中心装置3向车载显示器7发送的分发规格数据中包含属性信息,则车载显示器7利用与中心装置3同等的画面对显示信息进行显示。这里,车载显示器7保存的显示控制程序例如与在中心装置3制作的画面中使用的显示控制程序在版本方面不同。

[0979] 如果车载显示器7具有网页浏览器的功能,则车载显示器7通过与中心装置连接而利用与中心装置3相同的画面对显示信息进行显示。

[0980] 如以上说明那样,中心装置3通过进行显示控制信息的发送控制处理向车载显示器7发送显示控制信息,根据显示控制信息而在车载显示器7中对显示信息进行显示。由此,

在作为显示终端,具有移动终端6和车载显示器7的情况下,能够使这些显示方式接近,能够提高用户的便利性。CGW13通过进行显示控制信息的接收控制处理,而从中心装置3接收显示控制信息,从中心装置3接收显示信息,根据显示控制信息对显示信息进行显示。

[0981] (24)进展显示的画面显示控制处理

[0982] 参照图186至图210对进展显示的画面显示控制处理进行说明。车辆用程序改写系统1在CGW13中进行进展显示的画面显示控制处理。

[0983] 如图186所示,CGW13在进展显示的画面显示控制部90中,具有模式判定部90a和画面显示指示部90b。

[0984] 模式判定部90a判定是否通过用户的定制操作而设定定制模式。另外,模式判定部90a根据在改写规格数据中包含的场景信息来判定是否设定来自外部的外部模式。即,模式判定部90a参照图8所示的改写规格数据中包含的场景信息。如图8和图187所示,在改写规格数据中储存场景信息、有效期限信息、位置信息。场景信息表示本更新的场景(种类、场面等),同时指定本更新的画面显示。具体而言,存在调用标志、经销商标志、工厂用标志、功能更新通知标志、强制执行标志。

[0985] 调用标志是指定根据调用进行应用程序的改写的情况下的画面显示的标志。调用是指在判明由于设计、制造上的过错等而在制品中存在缺陷的情况下,根据法令的规定或者制造者、销售者的判断进行无偿修理、更换、回收等措施。

[0986] 经销商标志是指定在经销商进行应用程序的改写的情况下的画面显示的标志。工厂用标志是指定在工厂进行应用程序的改写的情况下的画面显示的标志。功能更新通知标志是指定在根据功能更新通知进行应用程序的改写的情况下的画面显示的标志。功能更新通知是指更新确定出的功能。例如功能更新通知标志是指定用于有偿(或者无偿)追加新的功能的程序更新中的画面显示的标志。

[0987] 强制执行标志是指定在根据强制执行进行应用程序的改写的情况下的画面显示的标志。强制执行是指虽然重复规定次数的活动通知,但不进行该应用程序的改写因而强制地进行应用程序的改写。例如强制执行标志是指定在强制地进行程序更新的情况下的画面显示的标志。

[0988] 表示这些场景信息的标志被设定为,在不相应的情况下全部为0(标志不成立),在相应的情况下任一个为1(标志成立)。模式判定部90a例如在调用标志成立时,判定为设定调用模式,在经销商标志成立时,判定为设定经销商模式,在工厂标志成立时,判定为设定工厂模式,在功能更新通知标志成立时,判定为设定功能更新模式,在强制执行标志成立时,判定为设定强制执行模式。

[0989] 有效期限信息是表示有效期限的信息,是成为是否执行应用程序的改写的判定基准的信息。如果当前时刻在有效期限信息所示的有效期限内,则CGW13执行应用程序的改写,如果当前时刻在有效期限信息所示的有效期限外,则CGW13不执行应用程序的改写。即,CGW13在下载了分发数据包之后,在进行程序的安装时参照有效期限信息,如果当前时刻在有效期限外,则不执行程序的安装,而放弃分发数据包。

[0990] 位置信息是表示位置的信息,是成为是否执行应用程序的改写的判定基准的信息,存在允许区域和禁止区域。在指定允许区域作为位置信息的情况下,如果车辆的当前位置在位置信息所示的允许区域内,则CGW13执行应用程序的改写,如果车辆的当前位置在位

置信息所示的允许区域外,则CGW13不执行应用程序的改写。在指定禁止区域作为位置信息的情况下,如果车辆的当前位置在位置信息所示的禁止区域外,则CGW13执行应用程序的改写,如果车辆的当前位置在位置信息所示的禁止区域内,则CGW13不执行应用程序的改写。即,CGW13在下载分发数据包之后,在进行程序的安装时参照位置信息,如果当前位置在允许区域外,则不执行程序的安装,等待安装直到处于允许区域内为止。

[0991] 画面显示指示部90b向显示终端5指示与应用程序的改写对应的画面显示。画面显示指示部90b通过指示与应用程序的改写的阶段对应的画面的显示有无,指示画面的项目的显示有无,指示画面的项目的显示内容的变更,向显示终端5指示画面显示。

[0992] 对用户的定制操作进行说明。另外,这里,对车载显示器7显示的画面进行说明,但移动终端6显示的画面也同样。另外,在后述的画面中,按钮的个数、配置等布局也可以是例示以外的布局。若用户在车载显示器7中进行菜单画面的显示操作,则如图188所示,CGW13使车载显示器7显示菜单选择画面511。CGW13在菜单选择画面511中,显示“软件更新”按钮511a、“更新结果确认”按钮511b、“软件版本一览”按钮511c、“更新历史”按钮511d、以及“用户信息登记”按钮511e,等待用户的操作。

[0993] 若用户从该状态操作“用户信息登记”按钮511e,则如图189所示,CGW13使车载显示器7显示用户选择画面512。CGW13在用户选择画面512中显示“用户”按钮512a～512c,等待用户的操作。

[0994] 若用户从该状态操作“用户”按钮512a,则如图190所示,CGW13使车载显示器7显示用户登记画面513。CGW13在用户登记画面513中,作为个人信息登记,显示邮件地址和VIN信息(单车识别信息)的输入栏,作为收费信息登记,显示信用卡号和有效期限的输入栏,作为应用程序的改写设定,显示活动通知、下载、安装、激活的“接通断开”按钮513a～513d,显示“详细信息”按钮513e,等待用户的操作。

[0995] 活动通知、下载、安装、激活的“接通断开”按钮513a～513d是选择对于活动通知、下载、安装、激活是否进行画面显示的按钮。具体而言,是在接收到活动通知时、开始下载时、开始安装时、开始激活时,使用户预先选择是否进行请求用户同意的内容显示的按钮。“详细信息”按钮513e是登记上述的有效期限信息和位置信息的按钮。这些用户设定的信息经由DCM12向中心装置3发送。另外,在用户利用移动终端6设定了这些信息的情况下,CGW13经由DCM12从中心装置3获取这些信息。

[0996] 如果用户对于活动通知、下载、安装、激活的画面感到烦躁的情况下,只要将该“接通断开”按钮513a～513d设定为断开即可。通过设定为断开,而省略请求用户同意的内容的显示。用户例如如果对于活动通知、激活的画面显示未感到烦躁,但对于下载、安装的画面显示感到烦躁的情况下,只要通过“接通断开”按钮513a将活动通知设定为接通,通过“接通断开”按钮513b将下载设定为断开,通过“接通断开”按钮513c将安装设定为断开,通过“接通断开”按钮513d将激活设定为接通即可。

[0997] 在该情况下,例如如果将活动通知设定为接通,将下载设定为断开,将安装设定为断开,将激活设定为接通,则显示终端5根据应用程序的改写阶段,显示活动通知画面,不显示下载同意画面和下载执行中画面,不显示安装同意画面和安装执行中画面,显示激活画面。即,如果用户在活动通知、下载、安装、激活的阶段中,设定为接通,则进行设定为该接通的阶段的画面显示,如果设定为断开,则不进行设定为该断开的阶段的画面显示,能够定制

画面显示。关于这样的画面显示的接通断开的设定,可以是,能够按每个阶段独立地设定,也可以是,能够将全部的阶段一并地一次性设定。

[0998] 另外,如果在用户希望登记有效期限、允许区域、禁止区域的情况下,只要操作“详细信息”按钮513e,设定有效期限、允许区域、禁止区域即可。用户能够定制允许应用程序的改写的有效期限作为有效期限信息,能够定制允许应用程序的改写的允许区域、禁止应用程序的改写的禁止区域作为位置信息。

[0999] 接下来,参照图191至图214对上述的构成的作用进行说明。CGW13执行进展显示的画面显示控制程序,进行进展显示的画面显示控制处理。

[1000] CGW13若开始进展显示的画面显示控制处理,则判定在改写规格数据中是否储存有效期限信息,以及在定制信息中是否设定有效期限信息(S2401)。CGW13若判定为在改写规格数据中储存有效期限信息(S2401:“是”),则判定当前时刻是否满足有效期限信息(S2402)。在存在储存于改写规格数据的有效期限信息和设定为定制信息的有效期限信息的情况下,CGW13判定是否满足双方。CGW13若判定为当前时刻在有效期限信息所示的有效期限外,当前时刻不满足有效期限信息(S2402:“否”),则结束进展显示的画面显示控制处理。

[1001] CGW13若判定为当前时刻在有效期限信息所示的有效期限内,当前时刻满足有效期限信息(S2402:“是”),则判定在改写规格数据中是否储存场景信息(S2403)。CGW13若判定为在改写规格数据中储存场景信息(S2403:“是”),则判定为设定外部模式,转移至按照该场景信息的设定内容的显示指示处理(S2404),向车载显示器7指示根据该成立的标志的模式进行与应用程序的改写对应的画面显示。例如如果调用标志成立,则CGW13向车载显示器7指示根据调用模式进行与应用程序的改写中对应的画面显示。例如如果经销商标志成立,则CGW13向车载显示器7指示根据经销商模式进行与应用程序的改写中对应的画面显示。

[1002] CGW13若判定为在改写规格数据中未储存场景信息(S2403:“否”),则判定是否通过用户的定制操作设定定制模式(S2405、相当于定制模式判定步骤)。CGW13若判定为设定定制模式(S2405:“是”),则转移至按照定制操作的设定内容的显示指示处理(S2406、相当于画面显示指示步骤),向车载显示器7指示根据定制模式进行与应用程序的改写对应的画面显示。

[1003] CGW13若判定为未设定定制模式(S2405:“否”),则转移至按照初始设定的设定内容的显示指示处理(S2407、相当于画面显示指示步骤),向车载显示器7指示根据定制模式进行与应用程序的改写对应的画面显示。即,CGW13优先应用储存于改写规格数据的场景信息,在未储存场景信息时,应用定制模式。在场景信息和定制模式都不存在的情况下,应用初始设定。这里,初始设定是指预先设定的值,例如活动通知、下载、安装和激活的任一方的设定都将设为接通的设定作为初始设定。

[1004] 接着,使用图192对S2404、S2406和S2407的画面显示指示处理进行说明。这里,例示了安装阶段中的画面显示指示处理,但其他的阶段也同样。CGW13若转移至显示指示处理,则设定画面的显示有无(S2411),设定画面的项目的显示有无(S2412),指示画面的项目的显示内容的变更(S2413)。CGW13向DCM12发送画面显示请求通知,从DCM12向车载显示器7发送画面显示请求(S2414),等待从DCM12接收操作结果信息(S2415)。操作结果信息是指表

示用户操作了哪个按钮的信息。另外,CGW13也可以向车载显示器7直接发送画面显示请求通知,接收操作结果信息。

[1005] CGW13若通过从车载显示器7向DCM12发送操作结果,而判定出从DCM12接收操作结果信息(S2415:“是”),则基于该操作结果信息来进行同意确认,判定用户是否同意了应用程序的改写(S2416)。

[1006] CGW13若判定为用户同意了应用程序的改写(S2416:“是”),则判定在改写规格数据中是否储存位置信息(S2417)。CGW13若判定为在改写规格数据中储存位置信息(S2417:“是”),则判定车辆的当前位置是否满足位置信息(S2418)。另外,在安装阶段以外的阶段,也可以省略S2417和S2418。在位置信息为允许区域的情况下,如果车辆的当前位置在允许区域内,则CGW13判定为车辆的当前位置满足位置信息(S2418:“是”),持续应用程序的改写(S2419)。

[1007] 另一方面,如果车辆的当前位置在允许区域外,则CGW13判定为车辆的当前位置不满足位置信息,中止应用程序的改写而不持续,结束画面显示指示处理。在位置信息为禁止区域的情况下,如果车辆的当前位置在禁止区域外,则CGW13判定为车辆的当前位置满足位置信息(S2418:“是”),持续应用程序的改写(S2419),结束画面显示指示处理。如果车辆的当前位置在禁止区域内,则CGW13判定为车辆的当前位置不满足位置信息,中止应用程序的改写而不持续,结束显示指示处理。

[1008] 对从CGW13向DCM12发送的画面显示请求通知、从DCM12向CGW13发送的操作结果信息进行说明。如图193所示,从CGW13向DCM12发送的画面显示请求通知中包含阶段ID、场景ID、画面结构信息。阶段ID是指对活动通知、下载、安装、激活这样的各阶段进行识别的ID。场景ID是指对图187所示的场景信息进行识别的ID。从DCM12向CGW13发送的操作结果信息中包含发送源信息、阶段ID、场景ID、操作结果、追加信息。CGW13对储存于画面显示请求通知的阶段ID和场景ID与储存于操作结果信息的阶段ID和场景ID进行对照,进行背离、调停的确认。

[1009] 即,如果在发送到DCM12的画面显示请求通知中储存的阶段ID和场景ID与在从DCM12接收到的操作结果信息中储存的阶段ID和场景ID一致,则CGW13判定为画面显示请求通知与操作结果信息匹配,画面显示请求通知与操作结果信息不背离,不需要进行调停。另一方面,如果在发送到DCM12的画面显示请求通知中储存的阶段ID和场景ID与在从DCM12接收到的操作结果信息中储存的阶段ID和场景ID不一致,则CGW13判定为画面显示请求通知与操作结果信息不匹配,画面显示请求通知与操作结果信息背离,需要进行调停。CGW13进行根据从DCM12接收到的操作结果信息是否进行处理这样的调停。

[1010] 画面结构信息是表示画面的结构要素的信息,如图194所示,例如在激活同意画面514中,存在“活动ID…”按钮514a、“更新名称A…”按钮514b、“更新名称B…”按钮514c、“详情确认”按钮514d、“返回”按钮514e、以及“OK”按钮514f这6个项目。在该情况下,如图195所示,如果画面结构信息的6个项目的全部被设定为“显示”,则如图194所示,在激活同意画面514显示6个项目的全部。即,用户能够操作“活动ID…”按钮514a、“更新名称A…”按钮514b、“更新名称B…”按钮514c、“详情确认”按钮514d、“返回”按钮514e、“OK”按钮514f中的任意一个。

[1011] 另一方面,如图196所示,如果画面结构信息的6个项目中的“活动ID…”按钮514a、

“更新名称A…”按钮514b、“更新名称B…”按钮514c、“详细信息”按钮514d、“OK”按钮514f被设定为“显示”,“返回”按钮514e被设定为不显示,则如图197所示,在激活同意画面514显示“活动ID…”按钮514a、“更新名称A…”按钮514b、“更新名称B…”按钮514c、“详细信息”按钮514d、“OK”按钮514f,另一方面,不显示“返回”按钮514e。即,用户能够操作“活动ID…”按钮514a、“更新名称A…”按钮514b、“更新名称B…”按钮514c、“详情确认”按钮514d、“OK”按钮514f中的任意一个,不显示“返回”按钮514e,因此不能操作“返回”按钮514e。例如对于基于调用等的重要度、紧急度比较高的应用程序的改写,不期望拒绝该激活,因此通过如上述那样使“返回”按钮514e不能操作,能够设定为不拒绝该激活。在该情况下,通过由用户操作“OK”按钮514f,而同意激活。

[1012] 对与CGW13、DCM12、车载显示器7、中心装置3、仪表装置45之间发送接收的画面显示、与用户操作相关的消息帧工作进行说明。如图198所示,CGW13与DCM12利用CAN、以太网连接,DCM12与车载显示器7利用USB连接。

[1013] CGW13经由DCM12与中心装置3之间进行数据通信。从CGW13通过诊查通信发送来的数据由DCM12进行协议变换,从DCM12通过HTTP通信而由中心装置3接收。例如CGW13经由DCM12向中心装置3发送表示当前的阶段、进展比例等当前进展状态的数据。从中心装置3通过HTTP通信发送来的数据由DCM12进行协议变换,从DCM12通过诊查通信而由CGW13接收。

[1014] CGW13经由DCM12与车载显示器7之间进行数据通信。从CGW13通过诊查通信发送来的数据由DCM12进行协议变换,从DCM12通过USB通信而由车载显示器7接收。从车载显示器7通过USB通信发送来的数据由DCM12进行协议变换,从DCM12通过诊查通信而由CGW13接收。例如CGW13经由DCM12获取与车载显示器7中的用户操作相关的信息。这样,在车辆用程序改写系统1中,构成为使DCM12具有协议变换功能,CGW13同样地处理移动终端6和车载显示器7。另外,通过将与用户操作相关的信息向CGW13汇总,从而CGW13对多个操作终端中的用户操作结果进行调停,能够管理当前进展状态。

[1015] 对与CGW13、DCM12、车载显示器7之间发送接收的消息帧的顺序进行说明。如图199至图206所示,在从CGW13向DCM12发送的画面显示请求通知、从DCM12向CGW13发送的操作结果信息中,在活动通知中将阶段ID设为“03”,在下载中将阶段ID设为“04”,在安装中将阶段ID设为“05”,在激活中将阶段ID设为“06”。在活动通知、下载、安装和激活的各阶段中,使消息帧的发送接收的顺序相同,通过使阶段ID不同来区分阶段。

[1016] 在图199中例示了活动通知阶段。CGW13管理当前进展状态,指定阶段ID、场景ID和画面结构信息,向DCM12发送画面显示请求通知。DCM12若从CGW13接收画面显示请求通知,则向车载显示器7发送画面显示请求。车载显示器7若从DCM12接收画面显示请求,则显示活动通知时的画面,若用户进行活动通知的确认操作,则向DCM12发送该操作结果。DCM12若从车载显示器7接收操作结果,则向CGW13发送操作结果信息。在由CGW13接收的操作结果信息中指定发送源信息、阶段ID、场景ID、操作结果和追加信息。CGW13基于从DCM12接收到的操作结果信息而更新当前进展状态。这里,在活动通知阶段中存在同意操作的情况下,CGW13将当前进展状态更新为下载阶段。

[1017] 在图200中,例示了下载阶段。CGW13管理当前进展状态,指定阶段ID、场景ID和画面结构信息,向DCM12发送画面显示请求通知。DCM12若从CGW13接收画面显示请求通知,则向车载显示器7发送画面显示请求。车载显示器7若从DCM12接收画面显示请求,则显示下载

同意时的画面,若用户进行下载的同意操作,则向DCM12发送该操作结果。DCM12若从车载显示器7接收操作结果,则向CGW13发送操作结果信息。在由CGW13接收的操作结果信息中,指定了发送源信息、阶段ID、场景ID、操作结果和追加信息。CGW13基于从DCM12接收到的操作结果信息而更新当前进展状态。这里,在下载阶段中存在同意操作的情况下,CGW13将当前进展状态更新为安装阶段。

[1018] 在图201中,例示了安装阶段。CGW13管理当前进展状态,指定阶段ID、场景ID和画面结构信息,向DCM12发送画面显示请求通知。DCM12若从CGW13接收画面显示请求通知,则向车载显示器7发送画面显示请求。车载显示器7若从DCM12接收画面显示请求,则显示安装同意时的画面,若用户进行安装的同意操作,则向DCM12发送该操作结果。DCM12若从车载显示器7接收操作结果,则向CGW13发送操作结果信息。在由CGW13接收的操作结果信息中,指定了发送源信息、阶段ID、场景ID、操作结果和追加信息。CGW13基于从DCM12接收到的操作结果信息而更新当前进展状态。这里,在安装阶段中存在同意操作的情况下,CGW13将当前进展状态更新为激活阶段。

[1019] 在图202中,例示了激活阶段。CGW13管理当前进展状态,指定阶段ID、场景ID和画面结构信息,向DCM12发送画面显示请求通知。DCM12若从CGW13接收画面显示请求通知,则向车载显示器7发送画面显示请求。车载显示器7若从DCM12接收画面显示请求,则显示激活同意时的画面,若用户进行激活的同意操作,则向DCM12发送该操作结果。DCM12若从车载显示器7接收操作结果,则向CGW13发送操作结果信息。在由CGW13接收的操作结果信息中,指定了发送源信息、阶段ID、场景ID、操作结果和追加信息。CGW13基于从DCM12接收到的操作结果信息而更新当前进展状态。

[1020] 参照图203至图210对画面显示进行说明。在没有设定定制模式,在改写规格数据的场景信息中没有设定任何标志的情况下,CGW13根据初始设定的内容而对显示终端5指示与应用程序的改写对应的画面显示(S2407)。如果初始设定是将活动通知、下载、安装、激活全部接通的设定,则如上述的图31至图46所示,CGW13对显示终端5指示画面显示,以依次显示导航画面501、活动通知画面502、下载同意画面503、下载执行中画面504、下载完成通知画面505、安装同意画面506、安装执行中画面507、激活同意画面508、激活完成通知画面509、确认操作画面510。此时,在活动通知画面502、下载同意画面503、安装同意画面506、激活同意画面508、确认操作画面510中,显示用于得到用户的同意(OK)的内容。

[1021] 在设定用户的定制模式的情况下,CGW13根据定制模式的内容向显示终端5指示与应用程序的改写对应的画面显示(S2406)。但是,限于未指定场景信息的情况。例如如果在定制模式中将活动通知设定为接通,将下载设定为断开,将安装设定为断开,将激活设定为接通,则CGW13向显示终端5指示画面显示,以使得在显示了活动通知画面502之后,不显示下载同意画面503、下载执行中画面504、下载完成通知画面505、安装同意画面506和安装执行中画面507,显示激活同意画面508。

[1022] 在改写规格数据的场景信息中设定了调用标志的情况下,CGW13根据调用模式的内容向显示终端5指示与应用程序的改写对应的画面显示(S2404)。在该情况下,如图204所示,CGW13在活动通知画面502中,使“之后”按钮502a不显示。另外,如图205和图206所示,CGW13在下载同意画面503中,使“返回”按钮503c不显示。另外,如图207所示,CGW13在下载执行中画面504中,使“返回”按钮504b不显示。另外,如图208和图209所示,CGW13在安装同

意画面505中,使“返回”按钮505b不显示。另外,如图210所示,CGW13在激活同意画面518中,使“返回”按钮不显示。

[1023] 即,在改写规格数据的场景信息中设定了调用标志的情况下,通过如上述那样将“之后”按钮、“返回”按钮设定为不显示,只要使“之后”按钮、“返回”按钮不显示即可。或者,在显示活动通知画面502,在下载同意画面503中得到了用户的同意之后,也可以省略安装同意画面505、激活同意画面518的显示。以上,对在改写规格数据的场景信息中设定了调用标志的情况进行了说明,但在改写规格数据的场景信息中设定经销商标志、工厂用标志、功能更新通知标志、强制执行标志的情况下也同样,只要根据进行应用程序的改写的状况,指示与阶段对应的画面的显示有无、画面的项目的显示有无、画面的项目的显示内容的变更即可。

[1024] 若具体地说明,在改写规格数据的场景信息中设定了经销商标志的情况下,在经销商环境中需要修理工序中的专用的画面显示,只要显示经销商用的专用的画面而不显示用户用的画面即可。即,经销商的作业者进行与应用程序的改写相关的操作,而不是由用户进行与应用程序的改写相关的操作,因此只要为了经销商的作业,将“之后”按钮、“返回”按钮设定为显示,而使“之后”按钮、“返回”按钮显示即可。另外,例如也可以显示“请实施经销商的改写”等提示,催促向经销商入库车辆。

[1025] 在改写规格数据的场景信息中设定了工厂用标志的情况下,在工厂环境下的制造工序中不需要画面显示,因此只要不显示画面即可。

[1026] 在改写规格数据的场景信息中设定了功能更新通知标志的情况下,即使用户利用定制进行不需要显示的设定,也需要用于向用户可靠地通知变更内容的画面显示,因此只要与定制的设定无关地显示用户用的画面即可。即,在判断为用户不需要同意的情况下,也强制地实施同意,只要强制地显示同意画面即可,因此只要通过如上述那样将“之后”按钮、“返回”按钮设定为显示,而显示“之后”按钮、“返回”按钮即可。

[1027] 在改写规格数据的场景信息中设定了强制执行标志的情况下,用户利用定制进行需要显示的设定,即使在用户不进行同意的情况下,也需要用于可靠地实施车辆的软件更新的强制执行,因此只要与定制的设定无关地,显示用户用的画面即可。即,一边判断为用户需要同意一边即使不需要同意也实施应用程序的改写,因此只要通过如上述那样将“之后”按钮、“返回”按钮设定为不显示,而不显示“之后”按钮、“返回”按钮即可。另外,由于是以进行同意为前提的功能,因此也可以不显示画面本身而作为得到同意的画面来执行改写。

[1028] 如以上说明那样,CGW13通过进行进展显示的画面显示控制处理,在设定了定制模式的情况下,向显示终端5指示与定制模式的设定内容对应的画面显示。用户能够定制与改写的进展对应的画面显示。

[1029] (25)程序更新的报告控制处理

[1030] 参照图211至图217对程序更新的报告控制处理进行说明。车辆用程序改写系统1在CGW13中进行程序更新的报告控制处理。

[1031] 如图211所示,CGW13在程序更新的报告控制部91中,具备阶段确定部91a、显示指示部91b、指示器显示控制部91c、图标显示控制部91d、详细信息显示控制部91e、以及无效化指示部91f。阶段确定部91a确定作为程序更新的进展状况的阶段。作为程序更新的阶段,

阶段确定部91a确定活动通知、下载同意、下载执行中、安装同意、安装执行中、激活同意、激活执行中和更新完成。

[1032] 显示指示部91b若通过阶段确定部91a确定程序更新的阶段,则指示以与确定出的该程序更新的阶段对应的方式显示指示器。指示器显示控制部91c若被从显示指示部91指示为显示指示器,则根据该指示而对指示器进行显示控制。具体而言,指示器显示控制部91c在仪表装置45中对指示器46进行点亮控制。

[1033] 追随着指示器显示控制部91c对指示器进行显示控制,图标显示控制部91d在车载显示器7中对图标进行显示控制。追随着指示器显示控制部91c对指示器进行显示控制,详细信息显示控制部91e在车载显示器7或者移动终端6中对程序更新所涉及的图标和详细信息进行显示控制。图标是指图32所示的活动通知图标501a,详细信息例如是指图33所示的弹出显示的活动通知画面502、图34和图35所示的下载同意画面等。详细信息显示控制部91e指示以与通过阶段确定部91a确定出的程序更新的阶段对应的方式显示图标、或者指示显示与阶段和用户操作对应的详细信息画面。

[1034] 即使在通过在停车中进行程序更新而由电源管理ECU20进行电源控制的情况下,无效化指示部91f也向与电源管理ECU20、用户操作相关的各ECU19指示用户操作的受理的无效化。例如通过向引擎ECU47(参照图217)指示用户操作的受理的无效化,在改写对象ECU19的存储器构造为单面存储器、在停车中进行安装的情况下,即使用户进行了启动引擎的操作,也进行抑制以使受理无效化,使引擎不启动。另外,通过向电源管理ECU20指示用户操作的无效化,在改写对象ECU19的存储器构造为单面存储器、在停车中IG电源接通而进行安装的情况下,即使用户进行了断开IG电源的操作,也进行抑制以使受理无效化,使IG电源不断开。此时,无效化指示部91f也可以指示车载显示器7进行用户操作的受理被无效化的内容的报告。

[1035] 接下来,参照图212至图217对上述的构成的作用进行说明。CGW13执行程序更新的报告控制程序,执行程序更新的报告控制处理。

[1036] CGW13若开始程序更新的报告控制处理,则判定是否产生程序更新的活动(S2501)。CGW13若判定为产生程序更新的活动(S2501:“是”),则确定程序更新的阶段和存储器结构(S2502、相当于阶段确定步骤)。CGW13向仪表装置45指示以与确定出的该程序更新的阶段对应的方式显示指示器46(S2503、相当于显示指示步骤)。向车载显示器7指示显示与确定出的该程序更新的阶段对应的图标(S2504)。

[1037] CGW13判定详情显示请求的有无(S2505),若判定出存在详情显示请求(S2505:“是”),则判定是否能够与车载显示器7进行数据通信(S2506)。例如在用户按下了图32所示的活动通知图标501a、图33所示的“确认”按钮502a、图34所示的“详情确认”按钮503b等的情况下,CGW13判定为存在详情显示请求。CGW13若判定为能够与车载显示器7进行数据通信(S2506:“是”),则获取详细信息(S2507),向车载显示器7指示显示详细信息(S2508),向中心装置3指示显示详细信息(S2509)。

[1038] CGW13获取与活动通知一同接收到的报告内容、分发规格数据的报告内容,向车载显示器7通知而指示详细信息显示。另外,CGW13向中心装置3通知阶段和用户的操作内容来作为详细信息的显示指示,以在移动终端6中也显示与车载显示器7相同的内容。

[1039] CGW13判定是否结束了程序更新的事件(S2510)。

[1040] 例如若用户确认了激活完成,程序更新完成,则CGW13判定为事件结束。CGW13若判定为程序更新的事件未结束(S2510:“否”),则返回步骤S2502,重复步骤S2502之后的步骤。CGW13在活动通知、下载同意、下载执行中、安装同意、安装执行中、激活同意、激活执行中和更新完成的各阶段中,重复步骤S2502之后的步骤。

[1041] CGW13若判定为程序更新的事件结束(S2510:“是”),则结束程序更新的报告控制处理。

[1042] 仪表装置45在用户能够确认的规定位置配置有指示器46,若从CGW13接收报告请求通知,则作为应用程序的改写中的报告,使指示器46点亮或者闪烁。这里,也可以取代闪烁,是改变指示器46的颜色或者列举亮度等与通常的点亮显示相比进一步强调的点亮显示。即,只要是与通常的显示相比进一步强调的显示即可。另外,与程序更新相关的指示器46是一个,并且由一个设计构成。

[1043] 如图213所示,在应用程序的改写对象为双面存储器的情况下、为单面挂起存储器的情况下,为单面单独存储器的情况下,仪表装置45使各阶段中的指示器的报告方式不同。具体而言,仪表装置45根据从CGW13指定的阶段和存储器结构,而确定指示器46的报告方式,根据确定出的该报告方式进行报告。另外,也可以取代仪表装置45,由指示器显示控制部91c控制指示器46的报告方式,也可以由指示器显示控制部91c确定指示器46的报告方式,以该报告方式向仪表装置45指示对指示器46进行点亮控制。

[1044] 如图213所示,指示器显示控制部91c在安装、激活等对车辆的行驶会产生限制的阶段中,使指示器46例如以绿色闪烁显示。在改写对象ECU19为双面存储器的情况下,指示器显示控制部91c仅在激活执行中的阶段进行闪烁显示。在改写对象ECU19为单面挂起存储器的情况下,指示器显示控制部91c在IG断开中的安装执行中的阶段、激活同意的阶段和激活执行中的阶段进行闪烁显示。在改写对象ECU19为单面存储器的情况下,指示器显示控制部91c在安装执行中的阶段、激活同意的阶段和激活执行中的阶段进行闪烁显示。即,活动通知阶段、下载阶段和激活完成后的阶段(IG断开时、IG接通时、确认操作时)中的指示器46的显示不取决于存储器结构而是共用的,但安装阶段和激活阶段中的指示器46的显示取决于存储器结构而为不同的显示方式。这里,图213所示的IG断开时是指在停车中执行激活,伴随着激活完成而将IG电源断开时的显示方式,伴随着IG电源断开而使指示器46熄灭。然后,在通过用户操作将IG电源接通时,使指示器46点亮。这是为了向用户报告程序更新全部完成。而且,在图45所示的确认操作画面510中,若用户按下“OK”按钮510b,则判断为进行了确认操作,使指示器46熄灭。

[1045] 以下,对仪表装置45控制指示器46的报告方式的情况进行说明,但也可以如上述那样指示器显示控制部91c控制指示器46的报告方式。在图214中表示改写对象ECU19的存储器种类为双面存储器的情况下的指示器的报告方式。基于来自CGW13的指示,仪表装置45在从活动通知到激活同意为止的阶段中使指示器46点亮,在激活执行中的阶段中使指示器46闪烁。然后,仪表装置45在IG断开时使指示器46熄灭,在IG接通时使指示器46点亮,若用户进行针对更新完成的确认操作,则使指示器46熄灭。即,在为双面存储器的情况下,有可能在车辆的行驶中产生限制,仅处于激活执行中。仅激活的执行在车辆处于停车状态下进行,因此成为无法使车辆行驶的期间。因此,仪表装置45在激活执行中的阶段中使指示器46闪烁。另外,这里的指示器是规定的设计,在正常进展的情况下以绿色显示。

[1046] 在图215中表示改写对象ECU19的存储器种类为单面挂起存储器的情况下的指示器的报告方式。在应用程序的改写对象为单面挂起存储器的情况下,基于来自CGW13的指示,仪表装置45在从活动通知到安装同意为止的阶段中使指示器46点亮,在安装执行中在IG接通时使指示器46点亮,在IG断开时使指示器46闪烁。即,仪表装置45在IG接通状态下不执行向单面挂起存储器ECU的闪存的写入,因此使指示器46点亮,但在IG断开状态下执行向闪存的写入,因此使指示器46闪烁。仪表装置45在从激活同意到激活执行中为止的阶段中使指示器46闪烁。然后,在IG断开时使指示器46熄灭,在IG接通时使指示器46点亮,若用户进行针对更新完成的确认操作,则使指示器46熄灭。即,在为单面挂起存储器的情况下,从IG断开时的安装执行中到激活执行中为止,有可能在车辆的行驶中产生限制。因此,仪表装置45在这些阶段中使指示器46闪烁。这里,在为单面挂起存储器的情况下,即使在向非运用面的安装执行中,也能够通过中断该安装,而启动运用面对车辆进行行驶控制。因此,也可以与为双面存储器的情况同样,仅在无法使车辆行驶的激活执行中采用闪烁显示。

[1047] 在图216中表示改写对象ECU19的存储器种类为单面存储器的情况下的指示器的报告方式。在应用程序的改写对象为单面单独存储器的情况下,基于来自CGW13的指示,仪表装置45在从活动通知到安装同意为止的阶段中使指示器46点亮,在从安装执行中到激活执行中为止的阶段中使指示器46闪烁。然后,在IG断开时使指示器46熄灭,在IG接通时使指示器46点亮,若用户进行针对更新完成的确认操作,则使指示器46熄灭。即,在为单面存储器的情况下,从安装执行中到激活执行中为止,有可能在车辆的行驶中产生限制。因此,仪表装置45在这些阶段中使指示器46闪烁。

[1048] 另外,在一次的活动通知中作为程序的改写对象ECU19,包含双面存储器、单面挂起存储器、单面单独存储器的ECU19的情况下,仪表装置45按双面存储器、单面挂起存储器、单面单独存储器的顺序进行ECU19的应用程序的改写。CGW13在活动通知后,从针对双面存储器的ECU19的下载同意到安装执行中为止进行,仪表装置45在该期间使指示器46点亮。CGW13若结束针对双面存储器的ECU19的安装执行中的阶段,则从针对单面挂起存储器的ECU19的下载同意到安装执行中为止进行,仪表装置45在该期间使指示器46点亮。CGW13若结束针对单面挂起存储器的ECU19的安装执行中的阶段,则从针对单面单独存储器的ECU19的下载同意到安装同意为止进行,仪表装置45在该期间使指示器46点亮。

[1049] 从单面单独存储器的安装执行中到针对这些存储器种类不同的3种ECU19的激活执行中为止,仪表装置45使指示器46闪烁。仪表装置45在之后的IG断开时使指示器46熄灭,在IG接通时使指示器46点亮,若用户进行针对更新完成的确认操作,则使指示器46熄灭。

[1050] 另外,在一次的活动通知中作为程序的改写对象ECU19,包含双面存储器、单面挂起存储器、单面单独存储器的ECU19的情况下,仪表装置45也可以如以下那样进行控制。仪表装置45按照双面存储器、单面挂起存储器、单面单独存储器的顺序进行ECU19的应用程序的改写。CGW13在活动通知后,作为包含这些改写对象ECU19的更新数据的分发数据包的下载同意和下载执行中的指示器46,指示使绿色的规定设计点亮。然后,作为安装同意的指示器46,CGW13指示使绿色的规定设计点亮。另外,在包含单面单独存储器的ECU19的情况下,这里的安装同意兼用作激活同意。若得到针对安装的用户的同意,则CGW13第一步执行将作为双面存储器向ECU19的安装。在执行将双面存储器向ECU19的安装的期间,仪表装置45使指示器46点亮。CGW13若结束针对双面存储器的ECU19的安装执行中的阶段,则执行将单面

挂起存储器向ECU19的安装。在执行将单面挂起存储器向ECU19的安装的期间,仪表装置45使指示器46点亮。CGW13若结束单面挂起存储器相对于ECU19的安装执行中的阶段,则执行单面单独存储器相对于ECU19的安装。在执行将单面挂起存储器向ECU19的安装的期间,仪表装置45使指示器46闪烁。CGW13若这些改写对象ECU19的安装全部完成,则在持续指示器46的闪烁的状态下,执行激活。CGW13在之后的IG断开时向仪表装置45指示使指示器46熄灭,在IG接通时向仪表装置45指示使指示器46点亮,若用户进行针对更新完成的确认操作,则向仪表装置46指示使指示器46熄灭。

[1051] 在图214～图216所示的各阶段中,CGW13还向车载显示器7指示图标显示。CGW13在活动通知阶段中,指示显示图32所示的活动通知图标501a。CGW13在下载同意阶段中也持续该活动通知图标501a的显示。CGW13在下载执行中阶段中,指示显示图36所示的下载执行中图标501b。CGW13在安装同意阶段中,也可以持续该下载执行中图标501b的显示,也可以指示再次显示活动通知图标501a。CGW13在安装执行中阶段中,指示显示图41所示的安装执行中图标501c。CGW13在激活同意阶段中,也可以持续该安装执行中图标501c的显示,也可以指示再次显示活动通知图标501a。CGW13在激活执行中阶段和之后的IG断开时,不进行图标显示。CGW13在IG接通时,也可以指示再次显示活动通知图标501a,也可以使图44所示激活完成通知画面509弹出显示。若用户进行针对更新完成的确认操作,则CGW13不进行图标显示。另外,与程序更新相关的图标显示是一个,通过与各阶段对应的设计构成。

[1052] CGW13在如上述那样向指示器46指示应用程序的改写中的报告时,在应用程序的改写中产生了异常时,成为与正常时不同的报告方式。也可以是,在正常进行应用程序的改写时,CGW13例如指示以绿色进行点亮显示、闪烁显示,在产生了异常时,CGW13例如指示以黄色、红色进行点亮显示、闪烁显示。CGW13也可以根据异常的程度而使颜色不同,例如在异常的程度比较大时指示以红色进行点亮显示、闪烁显示,在异常的程度比较小时指示以黄色进行点亮显示、闪烁显示。这里所说的异常包含不能下载分发数据包的状态、不能安装写入数据的状态、在改写对象ECU19中不能对写入数据进行写入的状态、写入数据不正当的状态等。

[1053] 作为详情显示,车载显示器7基于用户的操作而依次显示上述的活动通知画面502、下载同意画面503、下载执行中画面504、下载完成通知画面505、安装同意506、安装执行中画面507、激活同意画面508、IG接通时画面509、以及针对更新完成的确认操作时画面510。与车载显示器7相同的详情显示在连接成能够与中心装置3进行通信的移动终端6中也能够显示。例如在未搭载车载显示器7的车辆中,在用户通过手柄开关的操作等请求了详情显示的情况下,CGW13经由DCM12向中心装置3请求详情显示。中心装置3通过制作详情显示的内容,并由移动终端6显示该内容,用户能够在移动终端6中确认详细信息。

[1054] 如图217所示,CGW13在停车中改写IG系统ECU、ACC系统ECU的单面挂起存储器、单面单独存储器的应用程序的情况下,强制地启动电源管理ECU20,使车辆电源成为接通的状态。在该情况下,若电源管理ECU20强制地启动,则通过电源管理ECU20的动作使仪表装置45、车载显示器7启动。因此,CGW13向仪表装置45、车载显示器7指示与程序更新相关的报告的抑制。仪表装置45若被从CGW13指示程序更新的报告的抑制,则不进行上述的指示器46的点亮、闪烁。车载显示器7若被从CGW13指示程序更新的报告的抑制,则不进行上述的详情显示。即,在停车中进行的安装、激活中,在用户不乘车的状况的情况下,由于不需要与程序更

新相关的报告,因此控制为不进行报告。

[1055] 另外,若电源管理ECU20强制地启动,使车辆电源成为接通的状态,则能够受理来自用户的按钮开关的操作而进行引擎控制,但CGW13向电源管理ECU20指示用户操作的受理的无效化,向仪表装置45、车载显示器7以及与用户操作相关的ECU19指示用户操作的受理的无效化的报告。仪表装置45若被从CGW13指示用户操作的受理的无效化,则即使用户在仪表装置45中进行操作,也使该操作的受理无效化。同样,车载显示器7若被从CGW13指示用户操作的受理的无效化,则即使用户在车载显示器7中进行操作,也是该操作的受理无效化。另外,引擎ECU47若被从CGW13指示用户操作的受理的无效化,则即使用户通过按钮开关进行使引擎启动的操作,也进行抑制以使该操作的受理无效化,使引擎不启动。

[1056] 如以上说明那样,CGW13通过进行程序更新的报告控制处理向仪表装置45指示应用程序的改写中的报告。即使在应用程序的改写中无法通过移动终端6、车载显示器7向用户通知的状况中也是,通过仪表装置45向用户通知处于应用程序的改写中,能够适当地向用户通知处于应用程序的改写中。另外,CGW13也可以根据应用程序的改写的进展状况而使报告方式发生变化。

[1057] (26)电源自保持的执行控制处理

[1058] 参照图218至图222对电源自保持的执行控制处理进行说明。车辆用程序改写系统1在CGW13、ECU19、车载显示器7、电源管理ECU20中进行电源自保持的执行控制处理。在该情况下,CGW13对ECU19、车载显示器7、电源管理ECU20指示电源自保持。即,CGW13与车辆用主装置对应,ECU19、车载显示器7、电源管理ECU20与车辆用从装置对应。CGW13具有第二电源自保持电路,车辆用从装置具有第一电源自保持电路。

[1059] 如图218所示,CGW13在电源自保持的执行控制部92中,具有车辆电源判定部92a、改写中判定部92b、第一电源自保持判定部92c、电源自保持指示部92d、第二电源自保持判定部92e、第二电源自保持有效化部92f、第二停止条件成立判定部92g、以及第二电源自保持停止部92h。

[1060] 车辆电源判定部92a判定车辆电源的接通断开。改写中判定部92b判定是否处于应用程序的改写中。改写中判定部95b判定哪个改写对象ECU19处于改写中。若由车辆电源判定部92a判定为车辆电源断开,由改写中判定部92b判定为处于程序的改写中,则第一电源自保持有效化部92c判定在车辆用从装置中自保持电源的必要性。即,第一电源自保持有效化部92c参照图8所示的改写规格数据,如果改写对象ECU19的ECU信息的改写方法被指定为电源自保持,则判定为存在自保持电源的必要性,如果被指定为电源控制,则判定为不存在自保持电源的必要性。

[1061] 电源自保持指示部92d若由第一电源自保持判定部92c判定为在车辆用从装置中需要自保持电源,则向车辆用从装置指示第一电源自保持电路的有效化。作为指示第一电源自保持电路的有效化的方式,电源自保持指示部92d存在指定电源自保持的完成时刻的方式、指示电源自保持的延长时间的方式、向车辆用从装置定期地持续输出自保持请求的方式。电源自保持指示部92d参照图8所示的改写规格数据,根据由改写对象ECU19的ECU信息的电源自保持时间指定的时间,对车辆用从装置指示第一电源自保持电路的有效化。

[1062] 即,如果采用指定电源自保持的完成时刻的方式,则电源自保持指示部92d将从当前时刻加上由改写规格数据指定的时间而得的时刻指定为完成时刻。如果采用指定电源自

保持的延长时间的方式,则电源自保持指示部92d将由改写规格数据指定的时间指定为延长时间。如果采用定期地向车辆用从装置持续输出自保持请求的方式,则直到由改写规格数据指定的时间经过为止,电源自保持指示部92d定期地向车辆用从装置持续输出自保持请求。

[1063] 若由车辆电源判定部92a判定为车辆电源断开,由改写中判定部92b判定为处于程序的改写中,则第二电源自保持判定部92e判定自身自保持电源的必要性。即,考虑CGW13是IG电源系统或者ACC电源系统的构成,判定自保持电源的必要性。若由第二电源自保持判定部92e判定为自身需要自保持电源,则第二电源自保持有效化部92f进行第二电源自保持电路的有效化。

[1064] 在该情况下,在第二电源自保持电路处于停止中的情况下,第二电源自保持有效化部92f通过使第二电源自保持电路启动,而使第二电源自保持电路有效化。在第二电源自保持电路处于启动中的情况下,第二电源自保持有效化部92f通过延长第二电源自保持电路的动作期间,来使电源自保持电路有效化。

[1065] 第二停止条件成立判定部92g判定第二电源自保持电路的电源自保持的停止条件是否成立。具体而言,第二停止条件成立判定部92g监视车辆电池40的电池余量、超时的产生、改写对象ECU19的改写完成,若判定为车辆电池40的电池余量小于规定容量、或者产生超时、或者改写对象ECU19完成了改写,则判定为第二电源自保持电路的电源自保持的停止条件成立。若由第二停止条件成立判定部92g判定为第二电源自保持电路的电源自保持的停止条件成立,则第二电源自保持停止部92h停止第二电源自保持电路。

[1066] 如图219所示,ECU19在电源自保持的执行控制部108中,具有指示判定部108a、第一电源自保持有效化部108b、第一停止条件成立判定部108c、以及第一电源自保持停止部108d。指示判定部108a判定是否被从CGW13指示了第一电源自保持电路的有效化。

[1067] 若由指示判定部108a判定为指示了第一电源自保持电路的有效化,则第一电源自保持有效化部108b使第一电源自保持电路有效化。在指定了电源自保持的完成时刻的情况下,第一电源自保持有效化部108b直到该指定的完成时刻为止使第一电源自保持电路有效化。在指定了电源自保持的延长时间的情况下,第一电源自保持有效化部108b直到从当前时刻起经过了该指定的延长时间为止使第一电源自保持电路有效化。在从CGW13输入自保持请求的情况下,第一电源自保持有效化部108b只要持续输入自保持请求,就使第一电源自保持电路有效化。

[1068] 在该情况下,在第一电源自保持电路处于停止中的情况下,第一电源自保持有效化部108b通过使第一电源自保持电路启动,而使第一电源自保持电路有效化。在第一电源自保持电路处于启动中的情况下,第一电源自保持有效化部108b通过延长第一电源自保持电路的动作期间,来使第一电源自保持电路有效化。另外,第一电源自保持有效化部108b保存默认的电源自保持时间,即使不指示第一电源自保持电路的有效化,也在该默认的电源自保持时间内使第一电源自保持电路有效化。即,第一电源自保持有效化部108b若被指示第一电源自保持电路的有效化,则使默认的电源自保持时间与基于来自CGW13的指示的电源自保持时间中的较长的一方优先而使第一电源自保持电路有效化。

[1069] 第一停止条件成立判定部108c判定第一电源自保持电路的电源自保持的停止条件是否成立。具体而言,如果电源自保持的对象是改写对象ECU19,则第一停止条件成立判

定部108c监视超时的产生、来自CGW13的停止指示,若判定为产生超时、或者接收来自CGW13的停止指示,则判定为第一电源自保持电路的电源自保持的停止条件成立。如果电源自保持的对象是车载显示器7,则第一停止条件成立判定部108c监视超时的产生、用户的下车、来自CGW13的停止指示,若判定为产生超时、或者用户的下车、或者接收来自CGW13的停止指示,则判定为第一电源自保持电路的电源自保持的停止条件成立。如果电源自保持的对象是电源管理ECU20,则第一停止条件成立判定部108c监视来自CGW13的停止指示,若判定为接收来自CGW13的停止指示,则判定为第一电源自保持电路的电源自保持的停止条件成立。若由第二停止条件成立判定部108c判定为第一电源自保持电路的电源自保持的停止条件成立,则第一电源自保持停止部108d停止第一电源自保持电路。

[1070] 接下来,参照图220至图222对上述的构成的作用进行说明。这里,对车辆用从装置为改写对象ECU19的情况进行说明。CGW13和改写对象ECU19分别执行电源自保持的执行控制程序,进行电源自保持的执行控制处理。

[1071] CGW13若开始电源自保持的执行控制处理,则判定车辆电源是否断开(S2601、相当于车辆电源判定步骤)。CGW13若判定为车辆电源断开(S2601:“是”),则判定是否处于应用程序的改写中(S2602、相当于改写中判定步骤)。CGW13若判定为处于应用程序的改写中(S2602:“是”),则将第二电源自保持电路启动(S2603、相当于第二电源自保持有效化步骤),判定在改写对象ECU19中自保持电源的必要性(S2604、相当于电源自保持判定步骤)。

[1072] CGW13若判定为在改写对象ECU19中需要保持电源自身(S2604:“是”),则向改写对象ECU19指示第一电源自保持电路的有效化(S2605、相当于电源自保持指示步骤)。CGW13判定电源自保持的停止条件是否成立(S2606),若判定为电源自保持的停止条件成立(S2606:“是”),则停止第二电源自保持电路(S2607),结束电源自保持的执行控制处理。

[1073] 以上,CGW13采用在判定为处于应用程序的改写中的情况下将电源自保持电路启动的构成,但也可以采用如下的构成,若判定为车辆电源断开,则将电源自保持电路启动,若判定为处于应用程序的改写中,将该启动中的电源自保持电路的动作时间延长。

[1074] 改写对象ECU19若开始电源自保持的执行控制处理,则判定车辆电源是否断开(S2611)。改写对象ECU19若判定为车辆电源断开(S2611:“是”),则将自保持电路启动(S2612),判定电源自保持的停止条件是否成立(S2613),判定是否从CGW13指示了电源自保持电路的有效化(S2614)。改写对象ECU19若判定为从CGW13指示了电源自保持电路的有效化(S2614:“是”),则将该启动中的电源自保持电路的动作期间延长(S2615)。改写对象ECU19若判定为电源自保持的停止条件成立(S2613:“是”),则停止电源自保持电路(S2616),结束电源自保持的执行控制处理。

[1075] 以上,改写对象ECU19采用在判定为车辆电源断开的情况下将电源自保持电路启动的构成,但也可以采用如下的构成,在判定为车辆电源断开的情况下使电源自保持电路不启动,若判定为车辆电源断开,并且判定为从CGW13指示了电源自保持电路的有效化,则使停止中的电源自保持电路启动。

[1076] 以上,对车辆用从装置为改写对象ECU19的情况进行了说明,但车辆用从装置为车载显示器7、电源管理ECU20的情况也同样。如图222所示,在改写对象ECU19中,在从安装准备到改写后处理为止的期间中需要电源自保持电路的动作,在车载显示器7中,在等待更新同意、等待下载同意、等待安装同意、等待激活同意的期间需要电源自保持电路的动作。

[1077] 如以上说明那样,CGW13通过进行电源自保持的执行控制处理,若判定为车辆电源断开,处于应用程序的改写中,则判定在改写对象ECU19中自保持电源的必要性,若判定为需要自保持电源,则向改写对象ECU19指示电源自保持电路的有效化。在改写对象ECU19中,若判定为从CGW13指示了电源自保持电路的有效化,则使电源自保持电路有效化。通过使电源自保持电路有效化,能够确保用于进行应用程序的改写的动作电源,能够适当地完成应用程序的改写。

[1078] 参照图223至图233对包含上述的特征性的处理(1)~(26)在内的程序更新的整体顺序进行说明。这里,说明如下的例子,对与第一总线连接的ECU(ID1)、ECU(ID2)和ECU(ID3)的应用程序进行改写,不对与第二总线连接的ECU(ID4)、ECU(ID5)和ECU(ID6)的应用程序进行改写。ECU(ID1)和ECU(ID4)为单面单独存储器,ECU(ID5)为单面挂起存储器,ECU(ID2)、ECU(ID3)和ECU(ID6)为双面存储器。另外,ECU(ID1)、ECU(ID4)、ECU(ID5)和ECU(ID6)为IG电源系统ECU,ECU(ID2)为ACC电源系统ECU,ECU(ID3)为+B电源系统ECU。

[1079] 首先,作为事前准备,用户操作移动终端6等,输入车辆编号(车辆的识别编号)、移动电话号码等个人信息,对中心装置3登记帐户(S5001)。另外,用户操作移动终端6等,输入执行条件,作为允许程序更新的执行的条件,指定车辆位置、时间段等。中心装置3在数据库中存储经由移动终端6接收到的个人信息等(S5002)。

[1080] 另外,车辆侧系统4的CGW13收集与车辆相关的信息(S5011),经由DCM12向中心装置3上传(S5012)。具体而言,是程序版本、各ECU19的存储器结构、运用面信息、搭载于车辆的电装部件、车辆位置、车辆的电源状态等信息。中心装置3在数据库中存储从车辆侧系统4接收到的信息(S5013)。

[1081] 若产生程序更新的必要性,则中心装置3根据从应用程序的提供企业即供应商提供的写入数据和存储于数据库的信息,生成图7和图8所示的改写规格数据。而且,中心装置3根据这些写入数据及其认证符、改写规格数据而生成重编数据。中心装置3将所生成的重编数据、另外生成的分发规格数据(图45)、数据包认证符打包成一个文件,生成分发数据包,并进行登记(S5021)。

[1082] 中心装置3在完成了分发数据包的准备之后,对用户进行程序更新的告知。中心装置3参照存储于数据库的个人信息,对移动终端6发送短消息服务(SMS)(S5031)。通过用户操作,移动终端6与记载于SMS的URL(Uniform Resource Locator:统一资源定位符)连接,显示告知内容(S5032)。移动终端6向中心装置3通知同意基于用户操作的程序更新的内容、或者不同意的内容(S5033)。中心装置3将用户的意思信息(同意或者不同意)登记于数据库(S5034)。这里,也可以取代移动终端6,使用车载显示器7向用户告知。

[1083] CGW13经由DCM12接收从中心装置3发送来的分发规格数据,并向车载显示器7传输(S5035)。车载显示器7对分发规格数据进行解析,显示作为告知内容的显示语句等(S5036)。另外,车载显示器7显示图标等图像数据,受理用户是否同意程序更新的输入。CGW13从车载显示器7接收用户的意思信息,经由DCM12向中心装置3通知(S5037)。

[1084] 在从用户得到了程序更新的同意的情况下,车辆侧系统4从中心装置3下载分发数据包。首先,中心装置3检查是否满足预先由用户指定的执行条件(S5041)。中心装置3在执行条件中的一个都不满足的情况下,不向DCM12发送分发数据包。在满足全部的执行条件的情况下,中心装置3向DCM12发送分发数据包(S5042)。DCM12若从中心装置3下载分发数据

包,则将下载的该分发数据包保存于闪存。而且,DCM12从分发数据包提取分发数据包认证符,验证重编数据和分发规格数据的完整性(S5043)。

[1085] DCM12例如使用由CGW13存储的密钥信息,对重编数据和分发规格数据的认证符进行运算。DCM12对运算出的认证符与从分发数据包提取的分发数据包认证符进行比较,在一致的情况下判定为验证成功,在不一致情况下判定为验证失败。DCM12若判定为验证失败,则删除分发数据包,并且向CGW13和中心装置3通知验证失败。

[1086] DCM12在判定为针对分发数据包的验证成功的情况下,如图10所示那样将分发数据包中包含的重编数据解包,分割为针对各改写对象ECU19的写入数据和改写规格数据(S5044)。改写规格数据预先分割为DCM用的改写规格数据和CGW用的改写规格数据。

[1087] DCM12向CGW13发送CGW用的改写规格数据(S5045)。CGW13对从DCM12接收到的CGW用的改写规格数据进行解析,在提取了所需要的信息之后,与DCM12之间进行针对各ECU19的写入数据的认证(S5046)。CGW13例如使用自身存储ECU(ID1)的密钥信息,而对ECU(ID1)的写入数据(差分数据)的认证符进行运算。CGW13对运算出的认证符与从重编数据提取的认证符进行比较,在一致的情况下判定为验证成功,在不一致的情况下判定为验证失败。CGW13若判定为验证失败,则删除分发数据包,并且向DCM12和中心装置3通知验证失败的内容。这里,在针对任意一个写入数据判定为验证失败的情况下,CGW13不对全部的ECU19进行程序更新。

[1088] CGW13若针对全部的写入数据判定为验证成功,则从DCM12接收分发规格数据,向车载显示器7传输接收到的该分发起始数据(S5047)。车载显示器7存储从CGW13传输来的分发规格数据。若以上的下载处理完成,则CGW13经由DCM12向中心装置3通知下载完成的内容(S5048)。

[1089] 中心装置3若被从车辆侧系统4通知下载完成,则对移动终端6发送SMS(S5049)。移动终端6通过用户操作与记载于SMS的URL连接,显示安装预约画面(S5050)。移动终端6向中心装置3通知通过用户操作而输入的安装日期时间(S5051)。中心装置3将安装日期时间与个人信息相关联地存储于数据库(S5052)。这里,也可以取代移动终端6,使用车载显示器7而使用户预约安装日期时间。车载显示器7若被从CGW13通知下载完成(S5053),则显示安装预约画面(S5054)。CGW13经由DCM12向中心装置3通知从车载显示器7接收到的安装日期时间(S5055)。

[1090] 在当前日期时间为登记于数据库的安装日期时间的情况下,中心装置3向车辆侧系统4指示安装开始(S5071)。DCM12若被从中心装置3指示安装,则检查安装执行条件(S5072)。DCM12例如检查车辆位置、与中心装置3的通信状况等。DCM12在满足全部的执行条件的情况下,使用数据包认证符来认证分发数据包(S5073)。若认证成功,则DCM12对分发数据包进行解包(S5074),提取DCM用的改写规格数据和CGW用的改写规格数据,在分割为每个ECU19的写入数据的基础上,向CGW13通知安装开始(S5075)。

[1091] CGW13若被从DCM12通知安装开始,则对从DCM12获取到的CGW用的改写规格数据进行解析,判定以哪个顺序改写哪个ECU19(S5076)。这里,设为第一个改写ECU(ID1),第二个改写ECU(ID2),第三个改写ECU(ID3)的顺序。CGW13使用各认证符而对DCM12保存的每个改写对象ECU19的写入数据全部进行验证(S5077)。这里,不仅可以验证用于版本升级的写入数据,而且还可以验证用于回滚的写入数据。

[1092] 若写入数据的验证成功,则CGW13对电源管理ECU20请求IG电源接通(S5078)。在停车中(IG开关42断开且ACC开关41断开)安装时,在改写对象ECU19为IG系统ECU或者ACC系统ECU的情况下,需要供给电力而使改写对象ECU19启动。电源管理ECU20向电源控制电路43请求进行与IG电源接通相同的电力供给(S5079)。若通过电源控制电路43向IG电源线39进行电力供给,则IG系统ECU和ACC系统ECU启动(唤醒)。

[1093] 然后,CGW13对非改写对象ECU19即ECU(ID5)、ECU(ID5)和ECU(ID6)、第二个之后改写的ECU(ID2)和ECU(ID3)请求睡眠(S5080)。另外,这里,在改写了第一个改写对象ECU19之后改写第二个改写对象ECU19,但也可以同时并行地改写多个改写对象ECU19。在该情况下,仅非改写对象ECU19请求睡眠。

[1094] CGW13与对各改写对象ECU19的安装并行地,进行电池余量的监视(S5081)和总线的通信负载的监视(S5082)。CGW13参照从CGW用的改写规格数据中提取出的电池负载的值、总线负载的值(总线负载表),在不超过允许值的范围内控制安装。CGW13例如在停车状态下,若电池负载达到允许值,则在该时刻中断安装。

[1095] 另外,例如若连接有改写对象ECU(ID1)的第一总线的总线负载达到允许值,则CGW14延迟向ECU(ID1)发送写入数据的频度。若完成了向全部的改写对象ECU19的安装,则这些监视结束。另外,在为单面单独存储器的情况下,无法在安装的中途结束,因此需要在安装开始前确认存在足够的电池余量。

[1096] CGW13向第一个改写的ECU(ID1)通知安装开始(S5101)。ECU(ID1)若被从CGW13通知安装开始,则使状态迁移为基于无线的程序更新模式(S5102)。由于ECU(ID1)为单面单独存储器ECU,因此无法并行地进行应用程序的执行、使用工具的诊断处理,成为基于无线的程序更新专用模式。

[1097] 在进行向第一个改写的ECU(ID1)的安装时,CGW13使用安全访问密钥进行访问认证(S5103)。若向ECU(ID1)的访问认证成功,则CGW13向ECU(ID1)发送写入数据即全部数据的信息。ECU(ID1)使用接收到的全部数据的信息,而判定写入数据是否与本ECU匹配(S5104)。ECU(ID1)在判定为匹配的情况下,进行写入处理。

[1098] CGW13从DCM12获取向ECU(ID1)的写入数据中的规定大小(例如1k字节)的分割文件,向ECU(ID1)分发(S5105)。ECU(ID1)将从CGW13接收到的分割文件写入闪存33d(S5106)。ECU(ID1)若写入完成,则存储重试点,该重试点表示写入到哪里的闪存地址,以使得能够从中途再次开始写入(S5107)。作为重试点,也可以存储表示执行到闪存的消除、写入以及这之后的处理中的哪里的标志。ECU(ID1)若存储重试点,则向CGW13通知写入完成(S5108)。

[1099] CGW13若从ECU(ID1)接受写入完成的通知,则经由DCM12向中心装置3通知改写状况的进展信息(S5109)。进展信息是指例如处于安装阶段以及ECU(ID1)的写入数据累积完成了多少字节写入等数据。中心装置3基于从DCM12发送来的进展信息,而对能够从移动终端6连接的网页画面进行更新(S5110)。移动终端6与中心装置3连接,作为更新后的进展状况,例如显示当前安装推进到几%等(S5111)。由此,即使在车辆处于停车状态,用户位于车外的情况下,也能够通过移动终端6掌握安装的进展状况。这里,也可以取代移动终端6,利用车载显示器7显示进展。CGW13若从ECU(ID1)接受改写完成的通知,则向车载显示器7通知改写状况的进展信息(S5112)。车载显示器7更新并显示进展状况的画面(S5113)。在如ECU(ID2)、ECU(ID3)那样为双面存储器结构的情况下,即使车辆处于行驶状态也能够安装。因

此,例如在车辆处于IG开关接通的情况下,车载显示器7可以显示进展状况。

[1100] CGW13若从ECU(ID1)接受写入完成的通知,则获取第二个分割文件作为下一写入数据,并向ECU(ID1)分发。此后,直到作为最后的写入数据的第N个分割文件为止,重复S5105～S5113的处理。ECU(ID1)若直到第N个分割文件为止完成写入,则对闪存的更新程序进行完整性验证,确认是否正确地写入(S5114)。CGW13若从ECU(ID1)接受完成全部的分割文件的写入、完整性验证成功的内容的通知,则对ECU(ID1)请求睡眠(S5115)。ECU(ID1)不通过安装后的更新程序启动,而暂时睡眠。

[1101] CGW13对第二个改写的ECU(ID2)请求唤醒(S5201)。CGW13向ECU(ID2)通知基于无线的程序更新、即开始安装的内容(S5202)。作为内部状态,ECU(ID2)使状态迁移为基于无线的程序更新模式(S5203)。双面存储器即ECU(ID2)在基于无线的程序更新模式的期间,能够进行应用程序的执行、基于工具的诊断的执行。CGW13对ECU(ID2)进行访问认证(S5204)。ECU(ID2)判定写入数据即差分数据是否与本ECU匹配(S5205)。由于ECU(ID2)为双面存储器,因此判定是否包含与闪存的非运用面匹配的写入数据。例如若ECU(ID2)的A面为运用面,B面为非运用面,则在写入数据是与B面不一致的地址的情况下,不进入之后的处理,CGW13经由DCM12向中心装置3通知写入数据错误的内容。而且,CGW13进行后述的回滚的处理。在判定为写入数据与本ECU匹配的情况下,进行对ECU(ID2)的写入处理。此后,与ECU(ID2)相关的S5206～S5216的处理与S5105～S5115相同。在S5207中,在向双面存储器即ECU(ID2)写入差分数据时,如图18所示,根据旧数据和差分数据对差分进行复原而生成新数据,并写入闪存33d。

[1102] 若相对于ECU(ID2)的安装全部完成,使ECU(ID2)睡眠,则CGW13对第三个改写的ECU(ID3)请求唤醒(S5301)。CGW13向ECU(ID3)通知基于无线的程序更新、即开始安装的内容(S5302)。作为内部状态,ECU(ID3)使状态迁移为基于无线的程序更新模式(S5303)。CGW13对ECU(ID3)进行访问认证(S5304)。ECU(ID3)判定写入数据即差分数据是否与本ECU匹配(S5305)。在判定为写入数据与本ECU匹配的情况下,进行对ECU(ID3)的写入处理。此后,与ECU(ID3)相关的S5306～S5315的处理与S5105～S5114相同。

[1103] 若对ECU(ID3)的安装全部完成,则CGW13结束电池余量的监视和总线的通信负载的监视(S5316,S5317)。而且,CGW13对ECU(ID1)和ECU(ID2)请求唤醒(S5401)。

[1104] 为了使ECU(ID1)、ECU(ID2)和ECU(ID3)以更新后的程序同时启动,CGW13对各个ECU请求将更新后的程序激活(S5402)。另外,在是不与激活的请求对应的ECU的情况下,可以取代激活请求,通知电源断开和电源接通,进行重新启动。

[1105] ECU(ID1)若接受来自CGW13的激活请求,则使自身重新启动(S5403)。由于ECU(ID1)是单面单独存储器,因此通过重新启动,以更新后的程序使ECU(ID1)启动。若安装后的重新启动完成,则ECU(ID1)将更新后的程序版本与激活完成一同向CGW13通知(S5404)。

[1106] ECU(ID2)若接受来自CGW13的激活请求,则将所存储的运用面信息从A面更新为B面(S5405),使自身重新启动(S5406)。而且,ECU(ID2)若在B面正常启动,则将激活完成与更新后的程序版本和运用面信息一同向CGW13通知(S5407)。

[1107] ECU(ID3)若接受来自CGW13的激活请求,则将所存储的运用面信息从A面更新为B面(S5408),使自身重新启动(S5409)。而且,ECU(ID3)若在B面正常启动,则将激活完成与更新后的程序版本和运用面信息一同向CGW13通知(S5410)。

[1108] CGW13若接受来自ECU(ID1)、ECU(ID2)和ECU(ID3)的激活完成通知,则经由DCM12将程序的更新完成与改写对象ECU(ID1)、ECU(ID2)和ECU(ID3)相关的更新后的程序版本和运用面信息一同向中心装置3通知(S5411)。中心装置3将从DCM12通知的信息登记于数据库(S5412),并且,将网页画面更新成作为进展状况的表示完成的显示(S5413)。移动终端6与中心装置3连接,显示完成了程序更新的内容的网页画面(S5414)。另外,CGW13若接受来自ECU(ID1)、ECU(ID2)和ECU(ID3)的激活完成通知,则向车载显示器7通知作为进展状况的完成了程序更新的内容(S5415)。车载显示器7显示完成了程序更新的内容(S5416)。另外,在车辆处于停车状态等不需要进展显示的情况下,CGW13不向车载显示器7通知进展。

[1109] 最后,CGW13对电源管理ECU20请求IG电源断开(S5418)。电源管理ECU20对电源控制电路43请求切断电力供给,以返回到安装开始前的IG开关断开的电源状态。若通过电源控制电路43,切断对IG电源线39和ACC电源线38的电力供给,则ECU(ID1)、ECU(ID2)、ECU(ID4)、ECU(ID5)和ECU(ID6)成为停止状态。

[1110] 在上述的例子中,说明了如下,由于包含单面单独存储器即ECU(ID1)的程序更新,因此在车辆处于停车状态时,从安装到激活为止连续进行。然而,例如在改写对象ECU19全部为双面存储器的情况下,也可以在行驶中在后台进行安装。另外,也可以构成为,在改写对象ECU19的安装完成的时刻,通过移动终端6从用户得到激活的同意。

[1111] 接下来,参照图230至图233,对在应用程序的安装中,由用户选择了程序更新的取消的情况下的回滚顺序进行说明。具体而言,关于针对ECU(ID1)安装完成,针对ECU(ID2)在安装中途的时刻由用户选择了取消的情况,进行说明。

[1112] 在由移动终端6通知了程序更新的取消的情况下,中心装置3向车辆侧系统4指示取消程序更新(S6001)。而且,中心装置3将网页画面变更为作为进展状况的回滚中的显示方式(S6002)。移动终端6显示表示回滚中的进展状况的网页画面(S6003)。

[1113] 若经由DCM12从中心装置3指示程序更新的取消,则CGW13基于改写对象ECU(ID1)、ECU(ID2)和ECU(ID3)的存储器结构以及安装状况,判定需要对哪个ECU进行怎样的回滚处理(S6004)。在该例中,判定完成向ECU(ID2)的安装,并且需要将ECU(ID1)返回到原来的版本这样的回滚处理的内容。

[1114] 而且,CGW13向车载显示器7通知回滚用的进展(S6005)。车载显示器7若被从CGW13通知回滚用的进展,则变更为回滚用的显示方式而显示进展(S6006)。车载显示器7例如显示为“回滚中”,并且将需要回滚的ECU(ID1)的进展显示为0%,将ECU(ID2)的进展显示为0%。

[1115] 作为针对ECU(ID2)的回滚处理,CGW13持续写入数据的安装。由于ECU(ID2)是双面存储器,因此也可以在中途中断向非运用面即B面的安装,持续将A面作为运用面进行动作。然而,在B面处于安装到中途的不完整的状态的情况下,在使用下次的差分数据的安装时,无法正确地复原差分。因此,针对ECU(ID2)将安装持续最后。

[1116] 具体而言,CGW13从DCM12获取针对ECU(ID2)的写入数据的分割文件(例如1k字节量),并向ECU(ID2)分发(S6007)。ECU(ID2)将从CGW13接收到的分割文件写入闪存33d(S6008)。若写入完成,则ECU(ID2)存储重试点,以使得能够从中途再次开始写入(S6009),向CGW13通知写入完成(S6010)。

[1117] CGW13若从ECU(ID2)接受写入完成的通知,则经由DCM12向中心装置3通知回滚状

况的进展信息(S6011)。回滚状况的进展信息例如是指作为ECU(ID2)的回滚,需要多少字节的写入,其中累积完成了多少字节写入等数据。中心装置3基于从DCM12发送来的进展信息,而能够更新从移动终端6连接的网页画面(S6012)。作为更新后的进展状况,移动终端6例如显示回滚当前进行到几%等的网页画面(S6013)。这里,也可以取代移动终端6,利用车载显示器7显示进展。CGW13若从ECU(ID2)接受改写完成的通知,则向车载显示器7通知回滚状况的进展信息(S6014)。车载显示器7更新并显示进展状况的画面(S6015)。此后,直到作为最后的写入数据的第N个分割文件为止,重复S6007～S6015的处理。

[1118] ECU(ID2)若直到第N个分割文件为止进行写入,则验证闪存33d的更新程序的完整性(S6016)。CGW13若从ECU(ID2)接受安装完成的通知,则对ECU(ID2)请求睡眠(S6017)。ECU(ID2)睡眠,而不会利用安装于非运用面即B面的更新程序启动。

[1119] 接着,CGW13为了进行对ECU(ID1)的回滚处理而对ECU(ID1)请求唤醒(S6101)。CGW13向ECU(ID1)通知开始用于回滚的安装的内容(S6102)。ECU(ID1)若被从CGW13通知安装开始,则使状态迁移为基于无线的程序更新模式(S6103)。CGW13与ECU(ID1)进行访问认证(S6104)。ECU(ID1)若访问认证成功,则判定回滚用的写入数据是否与本ECU匹配(S6105)。在判定为回滚用的写入数据与本ECU匹配的情况下,进行对ECU(ID1)的写入处理。

[1120] CGW13从DCM12获取向ECU(ID1)的回滚用的写入数据中的规定大小(例如1k字节)的分割文件,并向ECU(ID1)分发(S6016)。ECU(ID1)将从CGW13接收到的分割文件写入闪存33d(S6107)。ECU(ID1)若写入完成,则存储重试点,该重试点表示写入到哪里的闪存地址,以使得能够从中途再次开始写入(S6108)。ECU(ID1)若存储重试点,则向CGW13通知写入完成(S6109)。

[1121] CGW13若从ECU(ID1)接受写入完成的通知,则经由DCM12向中心装置3通知改写状况的进展信息(S6110)。中心装置3基于从DCM12发送来的进展信息,对能够从移动终端6连接的网页画面进行更新(S6111)。移动终端6与中心装置3连接,作为更新后的进展状况,例如显示回滚当前进行到几%等(S6112)。这里,也可以取代移动终端6,利用车载显示器7显示进展。CGW13若从ECU(ID1)接受写入完成的通知,则向车载显示器7通知改写状况的进展信息(S6113)。车载显示器7更新并显示回滚的进展状况的画面(S6114)。CGW13若从ECU(ID1)接受写入完成的通知,则作为下一写入数据,获取第二个分割文件,并向ECU(ID1)分发。此后,直到作为最后的写入数据的第N个分割文件为止,重复S6106～S6114的处理。

[1122] ECU(ID1)若直到第N个分割文件为止完成写入,则对闪存的回滚用程序进行完整性验证,确认是否正确地写入(S6115)。CGW13若从ECU(ID1)接受完成全部的分割文件的写入、完整性验证成功的内容的通知,则结束电池余量的监视和总线的通信负载的监视(S6116、S6117)。

[1123] 接着,CGW13对ECU(ID2)和ECU(ID3)请求唤醒(S6201)。为了以进行安装前的旧版本启动,CGW13对ECU(ID1)、ECU(ID2)和ECU(ID3)请求回滚用的激活(S6202)。单面单独存储器即ECU(ID1)与通常时的改写同样,通过重新启动将旧版本的程序启动。双面存储器即ECU(ID2)和ECU(ID3)与通常时的改写不同,不切换运用面,而将当前运用面即A面的程序启动。

[1124] ECU(ID1)若从CGW13接受回滚用的激活请求,则使自身重新启动(S6203)。ECU(ID1)若重新启动完成,则将程序版本与回滚用的激活完成一同向CGW13通知(S6204)。

[1125] ECU(ID2)若从CGW13接受回滚用的激活请求,则不对所存储的运用面信息进行更

新,而使自身重新启动(S6205)。ECU(ID2)若在持续运用面即A面正常启动,则将程序版本和运用面信息与回滚用的激活完成一同向CGW13通知(S6206)。

[1126] ECU(ID3)若从CGW13接受回滚用的激活请求,则不对所存储的运用面信息进行更新,而使自身重新启动(S6207)。ECU(ID3)若在持续运用面即A面正常启动,则将程序版本和运用面信息与回滚用的激活完成一同向CGW13通知(S6208)。

[1127] CGW13若从ECU(ID1)、ECU(ID2)和ECU(ID3)接受回滚用的激活完成通知,则经由DCM12向中心装置3通知回滚完成(S6209)。这里,CGW13还一并地通知与ECU(ID1)、ECU(ID2)和ECU(ID3)相关的程序版本和运用面信息。中心装置3将从DCM12通知的信息登记于数据库(S6210),并且将网页画面更新为作为进展状况的表示取消完成的显示(S6211)。移动终端6与中心装置3连接,显示完成了取消的内容的网页画面(S6212)。

[1128] 另外,CGW13若从ECU(ID1),ECU(ID2)以及ECU(ID3)接受回滚用的激活完成通知,则向车载显示器7通知完成了回滚作为进展状况(S6213)。车载显示器7显示完成了回滚(S6214)。

[1129] 最后,CGW13对于电源管理ECU20请求IG电源断开(S6215)。电源管理ECU20对电源控制电路43请求切断电力供给以便返回安装开始前的IG开关断开的状态。若通过电源控制电路43而切断向IG电源线39以及ACC电源线38的电力供给,则ECU(ID1)、ECU(ID2)、ECU(ID4)、ECU(ID5)以及ECU(ID6)成为停止状态。

[1130] 如以上所述,能够将CGW13作为重编主机来进行对多个改写对象ECU19的程序的更新。在本实施方式中,对将ECU(ID1)、ECU(ID2)以及ECU(ID3)作为一个组改写应用程序进行了说明,但对作为第二组的ECU(ID4)、ECU(ID5)以及ECU(ID6)改写应用程序时也相同。该情况下,对于第一组的ECU19进行了安装以及激活之后,对第二组的ECU19进行安装以及激活。

[1131] 另外,DCM12、CGW13、车载显示器装置7以及电源管理ECU20等的应用程序也同样能够改写。但是,这些ECU需要应用程序能够在程序更新中动作,所以优选由双面存储器构成。

[1132] 接下来,参照图234至图270对中心装置3的构成进行说明。此外,对第一实施方式至第五实施方式进行说明。

[1133] (第一实施方式)

[1134] 以下,参照图234至图253对第一实施方式进行说明。车辆用程序改写系统是能够通过OTA对搭载于车辆的ECU的车辆控制、诊断等应用程序进行改写的系统。如图234所示,车辆用程序改写系统1具有通信网络2侧的中心装置3、车辆侧的车辆侧系统4、以及显示终端5。通信网络2包括例如基于4G线路等的移动体通信网络、因特网、WiFi(Wireless Fidelity)(注册商标)等而构成。

[1135] 显示终端5是具有受理来自用户的操作输入的功能、显示各种画面的功能的终端,例如是用户能够携带的智能手机、平板等移动终端6、配置于车厢内的兼具导航功能的显示器、仪表显示器等车载显示器7。若移动终端6在移动体通信网络的通信范围内,则能够与通信网络2连接。车载显示器7与车辆侧系统4连接。

[1136] 若用户在车厢外且移动体通信网络的通信范围内,则能够一边在移动终端6确认应用程序的改写所涉及的各种画面一边进行操作输入,实现应用程序的改写所涉及的手续。用户能够在车厢内一边在车载显示器7确认应用程序的改写所涉及的各种画面一边进行操作输入,实现应用程序的改写所涉及的手续。即,用户能够在车厢外和车厢内分开使用

移动终端6和车载显示器7,实现应用程序的改写所涉及的手续。

[1137] 中心装置3在车辆用程序改写系统1中合并通信网络2侧的OTA的功能,作为OTA中心发挥作用。中心装置3具有文件服务器8、网页服务器9、以及管理服务器10,构成为各服务器8～10能够相互进行数据通信。

[1138] 文件服务器8是具备从中心装置3发送至车辆侧系统4的应用程序的管理功能,管理由作为应用程序的提供企业的供应商等提供的ECU程序以及其附带的信息、由OEM(Original Equipment Manufacturer)提供的分发规格数据、从车辆侧系统4获取的车辆状态等的服务器。文件服务器8能够经由通信网络2与车辆侧系统4之间进行数据通信,若产生分发数据包的下载请求,则将对重编数据和分发规格数据进行了打包的分发数据包发送至车辆侧系统4。网页服务器9是管理网页信息的服务器,对于移动终端6提供应用程序的改写所涉及的各种画面。管理服务器10管理登记到应用程序的改写的服务的用户的个人信息等,管理每个车辆的应用程序的改写历史等。

[1139] 车辆侧系统4具有主装置11。主装置11具有DCM12和CGW13,DCM12和CGW13连接为能够经由第一总线14进行数据通信。DCM12是与中心装置3之间经由通信网络2进行数据通信的车载通信设备,若从文件服务器8下载分发数据包,则从该分发数据包提取写入数据传输至CGW13。

[1140] CGW13是具有数据中继功能的车辆用网关装置,若从DCM12获取写入数据,则将该写入数据分发至改写应用程序的改写对象ECU。主装置11在车辆用程序改写系统1中合并车辆侧的OTA的功能,作为OTA主机发挥作用。此外,在图234中,例示出DCM12和车载显示器7与同一第一总线14连接的构成,但也可以是DCM12和车载显示器7与分立的总线连接的构成。

[1141] 除了第一总线14之外,在CGW13还连接有第二总线15、第三总线16、第四总线17、第五总线18作为车内侧的总线,经由总线15～17连接有各种ECU19,并且经由总线18连接有电源管理ECU20。

[1142] 第二总线15例如是车身系统网络的总线。与第二总线15连接的ECU19例如是控制车门的上锁/解锁的车门ECU、控制仪表显示的仪表ECU、控制空调的驱动的空调ECU、控制车窗的开闭的车窗ECU等进行车身系统的控制的ECU。第三总线16例如是行驶系统网络的总线。与第三总线16连接的ECU19例如是控制引擎的驱动的引擎ECU、控制制动器的驱动的制动器ECU、控制自动变速器的驱动的ECT(ETC(Electronic Toll Collection System,注册商标))ECU、控制动力转向的驱动的动力转向ECU等进行行驶系统的控制的ECU。

[1143] 第四总线17例如是多媒体系统网络的总线。与第四总线17连接的ECU19例如是用于控制导航系统的导航ECU、控制电子收费系统,即ECT系统的ETCECU等进行多媒体系统的控制的ECU。总线15～17也可以是车身系统网络的总线、行驶系统网络的总线、多媒体系统网络的总线以外的系统的总线。另外,总线的根数、ECU19的个数不限于例示的构成。

[1144] 电源管理ECU20是具有进行DCM12、CGW13、各种ECU19等的电源管理的功能的ECU。

[1145] 在CGW13连接有第六总线21作为车外侧的总线。在第六总线21连接有能够装卸地连接有工具23的DLC(Data Link Coupler)连接器22。车内侧的总线14～18以及车外侧的总线21例如由CAN(Controller Area Network,注册商标)总线构成,CGW13根据CAN的数据通信标准、诊断通信标准(UDS:ISO14229)与DCM12、各种ECU19、工具23之间进行数据通信。此外,既可以DCM12和CGW13通过以太网连接,也可以DLC连接器22和CGW13通过以太网连接。

[1146] 若改写对象ECU19从CGW13接收写入数据,则将该写入数据写入闪存改写应用程序。在上述的构成中,CGW13作为若从改写对象ECU19接收写入数据的获取请求,则作为将写入数据分发至改写对象ECU19的重编主机发挥作用。改写对象ECU19作为若从CGW13接收写入数据,则将该写入数据写入闪存改写应用程序的重编从机发挥作用。

[1147] 作为改写应用程序的方式,有通过有线改写的方式和通过无线改写的方式。在通过有线改写应用程序的方式中,若工具23与DLC连接器22连接,则工具23将写入数据传输至CGW13。CGW13将被从工具23传输的写入数据中继或者分发至改写对象ECU19。在通过无线改写应用程序的方式中,如上所述,DCM12若从文件服务器8下载分发数据包,则从该分发数据包提取写入数据,将该写入数据传输至CGW13。

[1148] 如图235所示,作为电气功能模块,CGW13具有微型计算机(以下,称为微机)24、数据传输电路25、电源电路26、以及电源检测电路27。微机24具有CPU(Central Processing Unit)24a、ROM(Read Only Memory)24b、RAM(Random Access Memory)24c、以及闪存24d。微机24执行储存于非过渡性实体存储介质的各种控制程序进行各种处理,控制CGW13的动作。

[1149] 数据传输电路25控制与总线14～18、21之间的依据CAN的数据通信标准、诊断通信标准的数据通信。电源电路26输入电池电源(以下,称为+B电源)、附件电源(以下,称为ACC电源)、点火电源(以下,称为IG电源)。电源检测电路27检测电源电路26输入的+B电源的电压值、ACC电源的电压值、IG电源的电压值,将这些检测出的电压值与规定的电压阈值相比较,将其比较结果输出至微机24。微机24根据从电源检测电路27输入的比较结果,判定从供给外部供给至CGW13的+B电源、ACC电源、IG电源是正常还是异常。

[1150] 如图236所示,作为电气功能模块,ECU19具有微机28、数据传输电路29、电源电路30、以及电源检测电路31。微机28具有CPU28a、ROM28b、RAM28c、以及闪存28d。微机28执行储存于非过渡性实体存储介质的各种控制程序进行各种处理,控制ECU19的动作。

[1151] 数据传输电路29控制与总线15～17之间的依据CAN的数据通信标准的数据通信。电源电路30输入+B电源、ACC电源、IG电源。电源检测电路31检测电源电路30输入的+B电源的电压值、ACC电源的电压值、IG电源的电压值,将这些检测出的电压值与规定的电压阈值相比较,并将其比较结果输出至微机28。微机28根据从电源检测电路27输入的比较结果,判定从外部供给至ECU19的+B电源、ACC电源、IG电源是正常还是异常。此外,ECU19除了连接的例如传感器、致动器等负载不同,基本上是相同的构成。另外,DCM12、车载显示器7、以及电源管理ECU的基本构成也与图236所示的ECU19相同。

[1152] 如图237所示,电源管理ECU20、CGW13、ECU19与+B电源线32、ACC电源线33、IG电源线34连接。+B电源线32与车辆电池35的正极连接。ACC电源线33经由ACC开关36与车辆电池35的正极连接。若用户进行ACC操作,则ACC开关36从断开切换为接通,车辆电池35的输出电压施加于ACC电源线33。例如若是将钥匙插入到插入口的类型的车辆,则ACC操作是将钥匙插入到插入口并从“OFF”位置转动到“ACC”位置的操作,若是按下开始按钮的类型的车辆,则ACC操作是按下一次开始按钮的操作。

[1153] IG电源线34经由IG开关37与车辆电池35的正极连接。若用户进行IG操作,则IG开关37从断开切换为接通,车辆电池35的输出电压施加于IG电源线34。例如若是将钥匙插入到插入口的类型的车辆,则IG操作是将钥匙插入到插入口并从“OFF”位置转动到“ON”位置的操作,若是按下开始按钮的类型的车辆,则IG操作是按下2次开始按钮的操作。车辆电池

35的负极接地。

[1154] 当ACC开关36和IG开关37双方断开时,仅+B电源被供给至车辆侧系统4。将仅+B电源被供给至车辆侧系统4状态称为+B电源状态。当ACC开关36接通且IG开关37断开时,ACC电源和+B电源被供给至车辆侧系统4。将ACC电源和+B电源被供给至车辆侧系统4的状态称为ACC电源状态。当ACC开关36和IG开关37双方接通时,+B电源、ACC电源、以及IG电源被供给至车辆侧系统4。将+B电源、ACC电源、以及IG电源被供给至车辆侧系统4的状态称为IG电源状态。

[1155] 对于ECU19而言,启动状态根据电源状态不同,被区分为在+B电源状态下启动的+B系统ECU、在ACC电源状态下启动的ACC系统ECU、在IG电源状态下启动的IG系统ECU。例如在车辆防盗等用途中驱动的ECU19是+B系统ECU。例如音频等非行驶系统的用途中驱动的ECU19是ACC系统ECU。例如引擎控制等行驶系统的用途中驱动的ECU19是IG系统ECU。

[1156] CGW13通过对于处于睡眠状态的ECU19发送启动请求,而使该启动请求的发送目的地的ECU19从睡眠状态转移至启动状态。另外,CGW13通过对于处于启动状态的ECU19发送睡眠请求,而使该睡眠请求的发送目的地的ECU19从启动状态转移至睡眠状态。CGW13通过使例如发送至总线15～17的发送信号的波形不同,来从多个ECU中选择启动请求、睡眠请求的发送目的地的ECU19。

[1157] 电源控制电路38与ACC开关36以及IG开关37并联连接。CGW13将电源控制请求发送至电源管理ECU20,使电源管理ECU20控制电源控制电路38。即,CGW13将电源启动请求作为电源控制请求发送至电源管理ECU20,使ACC电源线33、IG电源线34与车辆电池35的正极在电源控制电路38的内部连接。在该状态下,即使ACC开关36、IG开关37断开,ACC电源、IG电源也被供给至车辆侧系统4。CGW13将电源停止请求作为电源控制请求发送至电源管理ECU20,使ACC电源线33、IG电源线34与车辆电池35的正极在电源控制电路38的内部中断。

[1158] DCM12、CGW13、ECU19具有电源自保持功能。即,若DCM12、CGW13、ECU19处于启动状态时车辆电源从ACC电源或者IG电源切换为+B电源,则不在该切换之后立即从启动状态转移至睡眠状态或者停止状态,而即使在该切换之后也将启动状态继续规定时间将驱动电源自保持。DCM12、CGW13、ECU19在车辆电源从ACC电源或者IG电源切换为+B电源之后经过规定时间(例如几秒)后从启动状态转移至睡眠状态或者停止状态。

[1159] 接下来,参照图238至图239对从中心装置3分发至主装置11的分发数据包进行说明。在车辆用程序改写系统1中,根据由作为应用程序的提供企业的供应商提供的写入数据和主要由OEM提供的改写规格数据生成重编数据。作为由供应商提供的写入数据,有相当于旧应用程序与新应用程序的差分的差分数据、和相当于新应用程序整体的全部数据。差分数据、全部数据也可以通过公知的数据压缩技术被压缩。在图238中,例示出差分数据作为写入数据被从供应商A～C提供,根据从供应商A提供的ECU(ID1)的已加密的差分数据和认证符、从供应商B提供的ECU(ID2)的已加密的差分数据和认证符、从供应商C提供的ECU(ID3)的已加密的差分数据和认证符、以及从OEM提供的改写规格数据生成重编数据的情况。认证符对每个写入数据赋予。

[1160] 此外,在图238中,示出从旧应用程序更新到新应用程序时的差分数据,但也可以为将用于从新应用程序回写到旧应用程序的回滚用差分数据一并包含于重编数据的构成。例如,在改写对象ECU19为单面存储器的情况下,使重编数据包含回滚用差分数据。

[1161] 从OEM提供的改写规格数据是如下的数据:包括能够确定改写对象ECU19的信息、能够确定改写对象ECU19为多个时的改写顺序的信息、能够确定后述的回滚方法的信息等作为应用程序的改写所涉及的信息,并定义DCM12、CGW13、改写对象ECU19中的改写所涉及的动作。改写规格数据被区分为DCM12使用的DCM用的改写规格数据和CGW13使用的CGW用的改写规格数据。DCM用的改写规格数据中记载了与改写对象ECU19对应的文件的读出所需要的信息。如上述那样,CGW用改写规格数据记载有控制改写对象ECU19中的改写所需要的信息。

[1162] DCM12若获取DCM用的改写规格数据,则解析该DCM用的改写规格数据,根据该解析结果控制向CGW13的写入数据的传输等改写所涉及的动作。CGW13若获取CGW用的改写规格数据,则解析该CGW用的改写规格数据,根据该解析结果控制从DCM12获取写入数据、向改写对象ECU19的写入数据的分发等改写所涉及的动作。

[1163] 文件服务器8中登记有上述的重编数据,并且登记有从OEM提供的分发规格数据。从OEM提供的分发规格数据是定义显示终端5中的各种画面的显示所涉及的动作的数据。

[1164] 文件服务器8若登记有重编数据和分发规格数据,则对重编数据进行加密,生成将用于认证数据包的数据包认证符、已加密的重编数据、以及分发规格数据打包成一个文件的分发数据包。文件服务器8若从外部接收分发数据包的下载请求,则将该分发数据包发送至DCM12。此外,在图238中,例示出文件服务器8生成储存了重编数据和分发规格数据的分发数据包,将重编数据和分发规格数据同时发送至DCM12的情况,但也可以将重编数据和分发规格数据分别发送至DCM12。即,文件服务器8也可以先将分发规格数据发送至DCM12,然后将重编数据发送至DCM12。另外,文件服务器8将重编数据和分发规格数据作为一个文件亦即分发数据包,向DCM12发送分发数据包和数据包认证符。

[1165] DCM12若从文件服务器8下载分发数据包,则验证储存于该分发数据包的数据包认证符和已加密的重编数据,若验证结果是正,则对已加密的重编数据进行解密。DCM12若对已加密的重编数据进行解密,则将该解密得到的重编数据解包,生成每个ECU的已加密的差分数据和认证符,DCM用的改写规格数据、CGW用的改写规格数据。在图239中,例示出生成ECU(ID1)的已加密的差分数据和认证符、ECU(ID2)的已加密的差分数据和认证符、ECU(ID3)的已加密的差分数据和认证符、改写规格数据的情况。

[1166] 图240将中心装置3中的主要的服务器8～10的各功能的部分以框图方式表示。另外,图241表示中心装置3对于ECU的程序更新进行的处理的概要。此外,以下,有时将“数据库”记载为“DB”。如图240所示,中心装置3具备数据包管理部3A、结构信息管理部3B、个体车辆信息管理部3C以及活动管理部3D。数据包管理部3A具有规格数据生成部201、数据包生成部202以及数据包分发部203、和ECU重编数据DB204、ECU元数据DB205以及数据包DB206。结构信息管理部3B具有结构信息登记部207以及结构信息DB208。

[1167] 供应商使用作为管理服务器10的用户界面(UI)功能的输入部218以及显示部219,登记各个ECU的数据。作为各个ECU的数据,有新程序、差分数据等程序文件、程序文件的验证数据、大小、加密方式等程序文件相关信息、以及ECU19的存储器构造等ECU属性信息相关的数据。程序文件存储于ECU重编数据DB204。ECU属性信息存储于ECU元数据DB205。程序文件相关信息既可以存储于ECU重编数据DB204,也可以存储于ECU元数据DB205。ECU重编数据DB204是更新数据存储部的一个例子。另外,ECU元数据DB205是装置相关信息存储部的一个

例子。

[1168] OEM经由结构信息登记部207按车辆型号将正规的结构信息登记到结构信息DB208。正规的结构信息是指由公共机构认可的车辆的结构信息。构成是与搭载于车辆的ECU19的硬件以及软件有关的识别信息,是车辆相关信息的一个例子。结构信息也包含有由多个ECU19构成的系统构成的识别信息、由多个系统构成的车辆构成的识别信息。另外,作为结构信息,也可以登记与程序的更新有关的车辆的限制信息。例如,也可以登记记载于改写规格数据的ECU的组信息、总线负载表、与电池负载有关的信息等。ECU元数据DB205是装置相关信息存储部的一个例子。另外,结构信息DB208是车辆信息存储部的一个例子。

[1169] 规格数据生成部201参照各DB生成改写规格数据。数据包生成部202生成包括改写规格数据和重编数据的分发数据包,登记到数据包DB206。数据包生成部202也可以包括分发规格数据来生成分发数据包。数据包分发部203将被登记的分发数据包分发至车辆侧系统4。分发数据包相当于文件。

[1170] 个体车辆信息管理部3C具有个体车辆信息登记部209、结构信息确认部210、更新有无确认部211以及SMS发送控制部212、以及个体车辆信息DB213。个体车辆信息登记部209将由各个车辆上载的个体车辆信息登记到个体车辆信息DB213。个体车辆信息登记部209也可以将车辆生产或者销售时刻中的个体车辆信息作为初始值登记到个体车辆信息DB213。结构信息确认部210在进行被上载的个体车辆信息的登记时,将个体车辆信息与结构信息DB208中登记的同一型号车辆的结构信息进行对照。更新有无确认部211确认对个体车辆信息有无基于新的程序的更新,即有无活动。SMS发送控制部212在个体车辆信息被更新的情况下,将与更新有关的消息通过SMS(Short Message Service:短信服务)发送至对应的车辆。

[1171] 活动管理部3D具备活动生成部214、活动分发部215以及指示通知部216、活动DB217。OEM通过活动生成部214生成与程序更新有关的信息亦即活动信息,并登记到活动DB217。此外,这里的活动信息相当于上述的“分发规格数据”,主要是与在车辆侧系统4显示的更新内容有关的信息。活动分发部215将活动信息分发至车辆。指示通知部216将与程序更新相关的必要的指示通知给车辆。在车辆侧系统4中,例如用户基于由中心装置3发送的活动信息,判断是否进行更新程序的下载,若需要则进行下载。此外,各管理部3A～3D的除了各数据库之外的部分是由计算机的硬件以及软件实现的功能。车辆通信部222是用于在中心装置3与车辆侧系统4之间通过无线相互地进行数据通信的功能模块。

[1172] 以下,更详细地对上述的处理进行说明,首先,对登记到各数据库的数据的内容进行说明。如图242所示,作为一个例子,在结构信息DB208登记有以下的数据。“车辆型号”表示车辆类型。“Vehicle SW ID”是针对车辆整体的软件ID,相当于车辆软件ID。“Vehicle SW ID”对各车辆仅赋予一个,随着任意一个以上的ECU的应用程序的版本被更新而被更新。若将搭载于各车辆的多个ECU19的组设为“系统”,则“Sys ID”是该系统的ID。

[1173] 例如,在图234中,车身系统ECU19的组是车身系统系统,行驶系统ECU19的组是行驶系统。“Sys ID”随着构成系统的任意一个以上的ECU的应用程序的版本被更新而被更新。“ECU ID”是表示各ECU的种类的装置识别用的ID。“ECU SW ID”是针对各ECU的软件ID,相当于ECU软件ID。这里,为了方便,由对“ECU ID”标注了软件的版本的信息表示。“ECU SW ID”随着该ECU的应用程序的版本被更新而被更新。另外,即使是相同的“ECU ID”且是相同的程

序版本,在硬件构成不同的情况下,也使用不同的“ECU SW ID”。即,“ECU SW ID”是表示ECU的产品编号的信息。

[1174] 在图242中,示出与“车辆型号”=“aaa”的车辆有关的结构信息。示出搭载于车辆的ECU19中的自动驾驶ECU(ADS)、引擎ECU(ENG)、制动器ECU(BRK)、以及电动动力转向ECU(EPS)。例如,相对于“Vehicle SW ID”=“0001”的“ECU SW ID”是“ads_001”、“eng_010”、“brk_001”、“eps_010”,“Vehicle SW ID”=“0002”的“ECU SW ID”是“ads_002”、“eng_010”、“brk_005”、“eps_011”,3个软件版本被更新。伴随于此,“Sys ID”=“SA01”被更新为“SA02”,“Sys ID”=“SA02”被更新为“SA03”。这样,在结构信息DB208中,在车辆的生产或者销售时刻登记有初始值,然后,随着任意一个以上的ECU的应用程序的版本被更新而被更新。即,结构信息DB208表示各车辆型号、市场上正规存在的结构信息。

[1175] 如图243所示,作为一个例子,在ECU重编数据DB204登记有以下的程序、数据。在图243中,作为搭载于某车辆型号的ECU19中的应用程序被更新的ECU19,例示出自动驾驶ECU(ADS)、制动器ECU(BRK)、以及电动动力转向ECU(EPS)。对于这些更新对象ECU19的最新的“ECU SW ID”,登记有ECU的旧程序以及新程序文件、新程序的完整性验证数据、作为新程序与旧程序的差分数据的更新数据文件、更新数据的完整性验证数据、同样地作为差分数据的回滚数据文件、回滚数据的完整性验证数据等。完整性验证数据是将散列函数应用于数据值而得到的散列值。此外,在代替差分数据将更新数据作为新程序的全部数据时,更新数据的完整性验证数据与新程序的该数据相等。

[1176] 此外,在图243中,示出了最新的“ECU SW ID”的数据结构,但在保存有旧的“ECU SW ID”的数据的情况下,旧程序文件也可以是参照一个旧的“ECU SW ID”的新程序文件的构成。另外,各完整性验证数据既可以为登记由供应商运算出的值的形式,也可以为中心装置3运算并登记的形式。

[1177] 如图244所示,作为一个例子,在ECU元数据DB205登记有以下所示的各个ECU的规格数据。对于最新的“ECU SW ID”而言,是更新数据文件的大小、回滚数据文件的大小、ECU19具备的闪存28d是2面以上的构成的情况下表示是A面、B面、C面等哪个面用的程序的面信息、传输大小、程序文件的读出用地址等。这些是更新数据相关信息的一个例子。

[1178] 另外,在ECU元数据DB205也登记有表示ECU19的属性的属性信息。属性信息是指表示与ECU有关的硬件属性、以及软件属性的信息。“传输大小”是从CGW13向ECU19分割传输改写数据时的传输大小,“密钥”是CGW13安全地访问ECU19时使用的密钥。这些是软件属性信息的一个例子。另外,对于“车辆型号”以及“ECU ID”而言,也包括ECU19具备的闪存28d的存储器结构、连接ECU19的总线种类、与ECU19连接的电源的种类等。这些是硬件属性信息的一个例子。

[1179] 这里,存储器结构“单面”是在1面具有闪存面的单面单独方式存储器,“双面”是在2面具有闪存面的双面存储器,“挂起”是在伪2面具有闪存面的单面挂起方式存储器。硬件属性信息以及软件属性信息是在车辆侧系统4中各个ECU19的改写控制所使用的信息。硬件属性信息也能够预先由CGW13存储,在本实施例中,为了减少车辆侧系统4中的管理负载,而由中心装置3管理。另外,软件属性信息是直接指定各个ECU19的改写动作的数据。由中心装置3管理以便能够实现车辆侧系统4中的灵活控制。

[1180] 如图245所示,作为一个例子,在个体车辆信息DB213中登记有以下所示的每个个

体车辆的数据。主要登记有每个个体车辆的结构信息、针对程序更新的个体车辆的状态信息。具体而言,是作为各车辆的ID的“VIN”、作为结构信息的“Vehicle SW ID”、“Sys ID”、“ECU ID”、“ECU SW ID”等。作为这些结构信息的散列值的“Digest”值也由中心装置3运算、存储。在存储器结构是双面的情况下,“运用面”是写入了ECU19当前运用的程序的面,登记有与结构信息一起上载的值。

[1181] “访问日志”是车辆将个体车辆信息上载到中心装置3的年月日以及时刻。“重编状态”表示车辆中的重编的状态,例如有“活动发行完毕”、“激活完成”、“下载完成”等。换句话说,根据该进展状态可知车辆中的重编进行到哪个阶段,在哪个阶段停滞。此外,在由车辆侧系统4对于中心装置3上载结构信息等时,对该信息等赋予各车辆的“VIN”。

[1182] 如图246所示,在数据包DB206登记有分发数据包的ID、分发数据包文件以及分发数据包的完整性验证用的数据。如图247所示,在活动DB217登记有以下的数据。活动信息的ID、分发数据包ID、表示具体的更新内容作为活动内容的文本文等消息信息、作为成为活动的对象的车辆的ID的“VIN”的列表、更新前后的“Vehicle SW ID”、更新前后的“ECU SW ID”的列表等。“对象VIN”列表能够对个体车辆信息DB213和活动DB217进行对照并登记。此外,这些活动信息也可以一并登记到数据包DB206。

[1183] 接下来,对本实施方式的作用进行说明。在图248中,对针对数据包管理部3A中的ECU重编数据DB204的登记处理进行说明。如图248所示,显示部219以及输入部218启动管理服务器10的重编数据登记用的画面,从供应商的工作人员受理ECU19的新旧程序文件的输入(A1)。例如,也可以使用使由CSV形式等标记了结构信息的文件登记为文件的UI等。接着,数据包管理部3A生成新程序的完整性验证数据(A2),生成将旧程序作为基础向新程序更新时的差分数据文件以及更新用差分数据的完整性验证数据作为更新用的差分数据(A3、A4)。

[1184] 接下来,生成将新程序作为基础向旧程序更新时的差分数据文件以及该数据的完整性验证数据作为回滚用的差分数据(A5、A6)。将这些程序文件以及验证数据登记到ECU重编数据DB204,并且基于一个旧的“ECU SW ID”生成新的“ECU SW ID”并登记(A7)。这里,在不分发差分而分发全部数据的情况下,能够省略与差分数据有关的步骤。

[1185] 完整性验证数据是例如应用散列函数而生成的散列值。例如使用SHA－256(Secure Hash Algorithm 256-bit)作为散列函数的情况下,将数据值按64字节划分为消息块。而且,若对于初始散列值应用最初的消息块的数据值,获得32字节长度的散列值,则对该散列值应用下一消息块的数据值,依次反复同样地获得32字节长度的散列值。

[1186] 在图249中,对规格数据生成部201中的改写规格数据的生成处理进行说明。这里,对针对“车辆型号”＝“aaa”的车辆的改写规格数据的生成处理进行说明,其他的车辆也相同。

[1187] 中心装置3启动规格数据生成部201的规格数据生成程序,经由显示部219以及输入部218受理来自OEM的工作人员的输入。首先,规格数据生成部201决定成为更新对象的ECU19。如图249所示,规格数据生成部201访问ECU重编数据DB204,将能够选择被登记的“ECU SW ID”中的成为更新对象的“ECU SW ID”的显示画面输出到显示部219。规格数据生成部201以特定的ECU顺序保持经由输入部218由OEM的工作人员选择的1个以上的“ECU SW ID”(B1)。这里,ECU顺序是指表示车辆侧系统4中的ECU19的改写顺序。规格数据生成部201

将由OEM的工作人员指定的顺序作为特定的ECU顺序。

[1188] 另外,规格数据生成部201也可以不访问结构信息DB208接受来自OEM的工作人员的输入,决定成为更新对象的ECU19。规格数据生成部201参照针对最新的“Vehicle SW ID”的“ECU SW ID”和针对一个旧的“Vehicle SW ID”的“ECU SW ID”,提取有更新的ECU19。例如,在图242中,“ADS”“BRK”“EPS”是更新对象ECU19。规格数据生成部201将登记到结构信息DB208的顺序作为特定的ECU顺序。

[1189] 而且,规格数据生成部201生成具有成为更新对象的多个“ECU SW ID”的ECU组信息(B2)。这里,参照结构信息DB208,使用“Sys ID”,例如由“Sys ID”为“SA01_02”的“ECU ID”构成组1,由“Sys ID”为“SA02_02”的“ECU ID”构成组2。例如,在图242中,将组1作为“ADS”,将组2作为第一个是“BRK”、第二个是“EPS”。这样,规格数据生成部201决定成为更新对象的ECU、ECU所属的组、以及组内的ECU顺序。

[1190] 接下来,规格数据生成部201访问ECU元数据DB205获取更新数据相关信息、硬件属性信息、以及软件属性信息作为与成为更新对象的ECU19有关的规格数据(B3)。例如图250所示,更新数据相关信息是“更新程序版本”“更新程序获取地址”“更新程序大小”“回滚程序版本”“回滚程序获取地址”“回滚程序大小”“写入数据种类”“写入面”。硬件属性信息是“连接总线”“连接电源”“存储器种类”。软件属性信息是“改写面信息”“安全访问密钥信息”“改写方法”“传输大小”。“改写方法”是表示在从IG接通切换为断开时使电源自保持电路有效来进行改写(电源自保持)还是根据IG接通以及IG断开进行改写(电源控制)的数据。作为“安全访问密钥信息”,也可以包含密钥以外的信息。

[1191] 以下,对各信息进行说明。

[1192] • “写入数据种类”是表示程序是差分数据还是全部数据的种类。也可以分别记载针对更新程序的写入数据种类和针对回滚程序的写入数据种类。

[1193] • “写入面”是表示对于双面存储器的ECU19用于写入哪个面的程序的信息。

[1194] • “连接总线”是识别连接有ECU19的总线的信息。

[1195] • “连接电源”是表示连接有ECU19的电源状态的信息,记载有表示电池电源(+B电源)、附件电源(ACC电源)、以及点火电源(IG电源)的任一个的值。

[1196] • “存储器种类”是识别ECU19的存储器结构的信息,记载有表示双面存储器、单面挂起方式存储器(伪双面存储器)、以及单面存储器等的值。

[1197] • “改写面信息”是表示ECU19的哪个面是启动面(运用面)哪个面是改写面(非运用面)的信息。

[1198] • “安全访问密钥信息”是用于使用密钥进行向ECU19的访问认证的信息,包括密钥导出密钥、密钥模式、以及解密运算模式的信息。

[1199] • “传输大小”是向ECU19分割传输程序时的数据大小。

[1200] 例如图250所示,这些信息将“ECU ID”作为关键字,作为上述的特定的ECU顺序保持。若规格数据生成部201对全部ECU获取信息(B4;是),则对成为更新对象的车辆指定“改写环境信息”(B5)。“改写环境信息”是指将ECU的组或者车辆整体作为对象的车辆侧系统4中的改写控制所使用的信息,是直接指定改写动作的数据。例如,作为将车辆整体作为对象的改写环境信息,是表示在车辆的行驶中(IG开关的接通中)还是在停车中(IG开关的断开中)进行车辆侧系统4中的程序更新的“车辆状态”、表示能够在车辆侧系统4中执行程序更

新的电池余量的限制的“电池负载(电池的余量)”、表示在车辆侧系统4中能够传输写入数据的总线负载的限制的总线负载表信息等。

[1201] 另外,作为将组作为对象的改写环境信息,是属于该组的ECU19以及组内的ECU顺序等。在车辆侧系统4中,控制为程序更新以组为单位同步,以所指定的ECU顺序执行对ECU19的写入。规格数据生成部201启动改写环境信息登记用的画面,受理来自OEM的工作人员的输入。或者,也可以为导入输入有改写环境信息的Excel(注册商标)的形式。或者,也可以为提取登记到结构信息DB208的限制信息的形式。此外,规格数据生成部201使用上述的步骤B2的生成结果作为将组作为对象的改写环境信息。

[1202] 总线负载表是表示电源状态与总线的传送允许量的对应关系的表格。如图251所示,传送允许量是相对于最大传送允许量能够传送的车辆控制数据与写入数据的传送量的合计。在该例示中,第一总线的传送允许量相对于最大传送允许量为“80%”,所以CGW13在IG电源状态下,允许相对于最大传送允许量的“50%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“30%”作为写入数据的传送允许量。另外,CGW13在ACC电源状态下,允许相对于最大传送允许量的“30%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“50%”作为写入数据的传送允许量。另外,CGW13在+B电源状态下,允许相对于最大传送允许量的“20%”作为车辆控制数据的传送允许量,允许相对于最大传送允许量的“60%”作为写入数据的传送允许量。第二总线以及第三总线也相同。

[1203] 最后,规格数据生成部201根据预先决定的规定的数据结构配置生成或者获取到的各数据,生成图250所示那样的改写规格数据(B6)。即,规格数据生成部201以能够在车辆侧系统4解释的数据结构生成改写规格数据。此外,对于各ECU信息而言,可以根据组的从小到大的顺序并且组内ECU顺序记载到改写规格数据。例如,在图242中,将组1设为“ADS”,将组2的第一个为“BRK”、第二个为“EPS”的情况下,规格数据的ECU信息栏中最初排列“ADS”的ECU信息,接下来排列“BRK”的ECU信息,最后排列“EPS”的ECU信息。

[1204] 在图250所示的规格数据中,ECU信息的“ECU ID”～“传输大小”是包括对象ECU19的种类的对象装置相关信息的一个例子,与上述的硬件属性信息以及软件属性信息对应。另外,“更新程序版本”～“写入面”是更新数据相关信息的一个例子。另外,将ECU的组或者车辆整体作为对象的“改写环境”是指定车辆中的更新处理的更新处理信息的一个例子。

[1205] 在图252中,对数据包生成部202中的数据包生成处理进行说明。与上述相同,这里,对针对“车辆型号”=「aaa」的车辆的数据包生成处理进行说明。如图252所示,以工作人员的指示为契机,中心装置3启动数据包管理部3A的数据包生成部202。数据包生成部202与步骤B1同样地决定成为更新对象的“ECU SW ID”(C1)。数据包生成部202通过ECU重编数据DB204获取与成为更新对象的“ECU SW ID”对应的各数据生成一个重编数据(C2)。例如,在图243中,数据包生成部201获取新程序的完整性验证数据、作为差分数据的更新数据、更新数据的完整性验证数据、旧程序的完整性验证数据、作为差分数据的回滚数据、以及回滚数据的完整性验证数据,生成重编数据。而且,将生成的重编数据和通过步骤B1～B6说明的对应的改写规格数据合并而生成一个分发数据包文件(C3)。接下来,生成已生成的数据包文件的完整性验证数据(C4),与数据包文件一起登记到数据包DB206(C5)。

[1206] 图253以图像方式表示如上述那样生成的数据包文件的内容。示出根据ECU顺序将与成为更新对象的“ADS”、“BRK”以及“EPS”对应的更新数据、完整性验证数据合并成一个重

编数据,进一步与改写规格数据合并而生成一个分发数据包文件的图像。这里,回滚数据也可以仅在成为更新对象的ECU19的存储器结构为单面的情况下,包含到重编数据。在存储器结构为双面或者挂起的情况下,不进行针对运用面的改写,所以能够省略作为旧程序的回滚数据。

[1207] 如以上那样,根据本实施方式,在中心装置3的ECU重编数据DB204中存储有搭载于车辆的多个ECU19中的成为更新应用程序的对象的ECU19的更新程序的数据。在结构信息DB208中,与车辆的种类一起存储有针对搭载于车辆的多个ECU19的每一个的“ECU ID”以及存储于ECU19的应用程序的“ECU SW ID”等车辆相关信息。在ECU元数据DB205中存储有改写对象ECU19的属性以及与更新数据相关的更新数据相关信息。

[1208] 而且,规格数据生成部201基于存储于结构信息DB208以及ECU元数据DB205的信息将与写入对象ECU19的更新数据一起向车辆发送的规格数据生成为包括对象ECU19的种类、属性、更新数据相关信息、以及表示与数据更新有关的改写环境的信息。并且,数据包生成部202生成包括规格数据和重编数据的分发数据包,并登记到数据包DB206。而且,数据包分发部203将所登记的分发数据包分发至车辆侧系统4。由此,车辆侧系统4能够通过接收与更新数据一起发送的规格数据,来基于该规格数据适当地选择对象ECU19,适当地控制使用更新数据的写入处理。

[1209] 而且,规格数据生成部201生成针对多个ECU19的规格数据作为一个文件,进一步,与针对多个ECU19的重编数据一起由数据包生成部202打包为一个文件,所以车辆侧系统4若接收到一个分发数据包则能够将更新数据写入多个ECU19。

[1210] 另外,作为规格数据的车辆相关信息包括将多个ECU19的一部分分组的组信息,所以车辆侧系统4能够根据由组信息规定的顺序选择成为对象的ECU19,写入更新数据。例如,在有许多成为某功能改善的对象的ECU19的情况下,将组1作为车身系统ECU19,将组2作为行驶系统ECU19,将组3作为MM系统ECU19,从而能够使车辆侧系统4中的程序更新分3次执行。因此,与全部ECU一起执行程序更新的情况相比,能够缩短每次的用户的等待时间。

[1211] 另外,改写环境信息中包括与车辆有关的“车辆状态(IG接通状态)”以及“电池负载”和与ECU19有关的“总线负载表”,所以车辆侧系统4能够基于这些信息决定写入更新数据的时机等。换句话说,使用OEM或者中心装置3的服务企业能够通过指定针对车辆的执行限制条件作为改写环境信息,来运用灵活的程序更新。

[1212] 另外,规格数据生成部201从与预先设定的改写顺序较早的ECU19有关的信息按顺序根据预先决定的数据结构生成规格数据,所以车辆侧系统4能够根据规格数据中的ECU ID的配置顺序写入更新数据。换句话说,将具有相互协作的处理的ECU19分组为一个组,考虑该相互协作的处理的内容,规定ECU顺序,从而在车辆侧系统4中,即使在向新程序的更新时机完全不同步的情况下,也能够没有不方便地完成程序更新。例如,在ECU(ID1)的新程序具有向ECU(ID2)发送规定消息的处理,ECU(ID2)的新程序具有在不能接收从ECU(ID1)发送的规定消息的情况下成为超时错误的处理的情况下,可以将ECU顺序规定为先更新ECU(ID1)然后更新ECU(ID2)。

[1213] (第二实施方式)

[1214] 如图254所示,第二实施方式涉及在图241中车辆侧系统4最初向中心装置3进行发送的“车辆结构信息同步”。若在车辆侧IG开关37被接通,则以此为契机,CGW13对于DCM12发

送“同步开始请求”。DCM12接受该请求将“结构信息收集请求”返回给CGW13。于是,CGW13对于各ECU19进行程序版本的咨询。各ECU19将“ECU SW ID”返回给CGW13。另外,存储器结构为双面或者挂起的ECU19将表示多个面中的哪个面是运用面且哪个面是非运用面的面信息也一起返回给CGW13。进一步,各ECU19也可以将成为控制对象的致动器等的校准信息、用于接受程序更新服务的许可信息、在ECU19产生的故障代码一并向CGW13发送。

[1215] CGW13若完成从各ECU19接收“ECU SW ID”,则将这些全部与“VIN”一起发送至DCM12。此时,也可以将由CGW13管理的“Vehicle SW ID”以及“Sys ID”也一并向DCM12发送。DCM12接受该信息,将全部“ECU SW ID”作为对象,例如使用散列函数生成一个作为摘要值的散列值。如上所述,在使用SHA－256作为散列函数的情况下,将连续地连结全部“ECU SW ID”的值而得到的数据值每64字节划分为消息块,对于初始散列值应用最初的消息块的数据值得到32字节长度的散列值,对该散列值依次应用后续的消息块的数据值,最终获得32字节长度的散列值。这里,DCM12也可以将不仅包括全部“ECU SW ID”还包括“Vehicle SW ID”、“Sys ID”、面信息以及校准信息的值作为对象,生成一个散列值。

[1216] DCM12将如上述那样得到的“ECU SW ID”的摘要值与“VIN”一起发送至中心装置3。另外,DCM12也可以将故障代码、许可信息与摘要值一并发送。以下,有将上述摘要值称为“结构信息摘要”,将作为其来源的“ECU SW ID”的全部数据值称为“全部结构信息”的情况。“全部结构信息”也可以包括“Vehicle SW ID”、“Sys ID”、面信息、以及校准信息。

[1217] 如后述那样,中心装置3进行摘要值的比较、个体车辆信息DB213的更新。使结构信息同步的中心装置3确认有无程序更新,在有更新的情况下将活动信息通知给车辆侧系统4。然后,车辆侧系统4下载分发数据包,进行向成为对象的ECU19的安装,进行新程序的激活。以完成这些更新处理为契机,CGW13对于DCM12发送“同步开始请求”,以下,在同步完成通知之前进行与上述相同的处理。另外,也可以在更新程序后进行以IG开关37被接通为契机进行的上述的处理。

[1218] 如图255所示,若中心装置3的个体车辆信息管理部3C通过车辆侧系统4接收“结构信息摘要”(D1),则在该时刻与登记到个体车辆信息DB213的对应的车辆的“结构信息摘要”进行对照,判断两者是否一致(D2)。“个体车辆信息摘要”既可以将预先运算出的值登记到个体车辆信息DB213,也可以在从车辆侧系统4接收到的时刻,使用登记到个体车辆信息DB213的结构信息运算摘要值。若两者一致(是),则判断车辆的个体车辆信息是否适合登记到结构信息DB208的正规的组合(D6)。此外,由于也有结构信息DB208在规定的时机被更新的可能性,所以在步骤D2中两者一致的情况(是)和两者不一致的情况下(否)都进行步骤D6的判断。

[1219] 这里,例如图256所示,上述的是否适合的判断检查从车辆侧系统4上载的结构信息的“Vehicle SW ID”与“ECU SW ID”的组合是否正规。在该图所示的列表中,与登记到结构信息DB208的“Vehicle SW ID＝0001”对应的“ECU ID＝ADS”的“ECU SW ID”是“ads_001”,“ECU ID＝BRK”的“ECU SW ID”是“brk_001”,“ECU ID＝EPS”的“ECU SW ID”是“eps_010”。

[1220] 与此相对,VIN＝300的车辆C同样地是“Vehicle SW ID＝0001”,但“ECU ID＝ADS”的“ECU SW ID”是“ads_002”,“ECU ID＝BRK”的“ECU SW ID”是“brk_003”,这2个ECU19与登记到结构信息DB208的结构信息不同。因此,在步骤D6中为“否”,换句话说是非正规,判断为

“NG”,结构信息确认部210向作为管理车辆侧系统4以及OEM等生产的车辆的信息的装置的图241所示的管理装置220通知异常(D12)。异常的通知例如通过SMS发送控制部212使用SMS进行。SMS发送控制部212是通信部的一个例子。即使这2个ECU19不是基于新程序的更新对象ECU,中心装置3也将该车辆判断为非正规,不进行步骤D7之后的处理。

[1221] 另一方面,VIN＝100的车辆A是“Vehicle SW ID＝0001”,“ECU ID＝ADS”的“ECU SW ID”是“ads_001”,“ECU ID＝BRK”的“ECU SW ID”是“brk_001”,与登记到结构信息DB208的结构信息全部一致。因此,在步骤D6中为“是”,换句话说是正规,判断为“OK”,进入步骤D7。这里,结构信息确认部210也可以通过车辆C的“ECU SW ID”的组合是否存在于结构信息DB208,来判断是正规还是非正规。另外,除了“Vehicle SW ID”之外,也可以将“Sys ID”加入判断材料。

[1222] 接下来,更新有无确认部211经由活动管理部3D访问活动DB217,确认有无基于新程序的更新(D7)。更新的有无通过比较从车辆侧系统4上载的“Vehicle SW ID”和活动DB217的“更新前Vehicle SW ID”来判断。例如图23所示,VIN＝100的车辆A是更新前的“Vehicle SW ID＝0001”,所以判断为有更新(是)。该情况下,更新有无确认部211将对应的活动ID“Cpn_001”通知给上述车辆A的车辆侧系统4(D8)。活动信息相当于更新通知信息,活动DB217是更新通知信息存储部的一个例子。

[1223] 此外,若使活动DB217具有更新前后的“Sys ID”,则也能够通过“Sys ID”确认有无更新。另外,也可以代替“Vehicle SW ID”,而比较上载的“ECU SW ID”列表和活动DB217的“更新前ECU SW ID列表”,来判断有无更新。

[1224] 车辆侧系统4将被通知的活动ID作为关键字从中心装置3获取与上述ID对应的活动文件(D9)。活动文件包含有说明活动内容的文本文、执行程序更新时的限制事项等。限制事项是指执行下载、安装时的条件,例如电池余量、分发数据包的下载所需要的RAM的空闲容量、车辆的当前位置等。车辆侧系统4解析活动文件,使用车载显示器7显示活动内容等。用户参照根据活动内容显示于车载显示器7的消息,决定是否更新ECU19的应用程序。若经由车载显示器7受理用户的同意操作,则CGW13经由DCM12向中心装置3通知同意更新。于是,中心装置3将与上述活动ID对应的数据包ID的分发数据包文件以及完整性验证数据发送至车辆侧系统4(D10)。

[1225] 另外,若在步骤D7中没有更新(否),则向车辆侧系统4通知“无更新”(D11)。例如图256所示,VIN＝200的车辆A是更新后的“Vehicle SW ID＝0002”,由于与活动DB217的“更新前Vehicle SW ID”的任一个都不一致,所以判断为无更新。

[1226] 另一方面,若在步骤D2中“结构信息摘要”的对照结果不一致(否),则中心装置3向车辆侧系统4请求“全部结构信息”的发送(D3)。该发送对应于“全部数据发送请求的通知”。若与此对应,车辆侧系统4发送“全部结构信息”,则中心装置3接收该信息(D4)。而且,中心装置3的个体车辆信息管理部3C更新登记到个体车辆信息DB213的该车辆的信息(D4)。此后,转移至步骤D6。个体车辆信息DB213是车辆侧结构信息存储部的一个例子。此外,由CGW13进行的“同步开始请求”的发送也可以在IG开关37被断开的时机等进行。

[1227] 如以上所述,根据第二实施方式,若车辆侧系统4从多个ECU19接收与各ECU19的构成有关的结构信息,则生成基于多个结构信息的数据值的散列值,并将该散列值发送至中心装置3。中心装置3具有个体车辆信息DB213,比较由车辆侧系统4发送的散列值和存储于

个体车辆信息DB213的车辆的结构信息的散列值。而且,若两者不一致,则向车辆侧系统4请求“全部结构信息”的发送。于是,车辆侧系统4接受该发送,将“全部结构信息”发送至中心装置3,若中心装置3接收“全部结构信息”,则基于该数据值更新存储于个体车辆信息DB213的结构信息。

[1228] 若这样构成,则车辆侧系统4首先向中心装置3发送结构信息的散列值,仅在中心装置3中的散列值的比较结果不一致时,将结构信息的全部的数据值发送至中心装置3。由此,能够减少车辆侧系统4发送的数据的大小,所以即使车辆侧系统4搭载于多个车辆,也能够在总体上减少通信量。特别是,在车辆侧系统4中,在IG接通时等预先决定的时机上载结构信息的情况下,可能产生该通信集中的时间段。因此,能够通过使用散列值减少发送数据量,来减少通信负载。

[1229] 另外,CGW13从成为更新数据的改写对象的全部的ECU19接收结构信息,生成基于这些全部数据值的散列值,DCM12在车辆的点火开关37被接通或者断开的时机发送散列值,所以能够在车辆的行驶被开始或者结束的时机将散列值发送至中心装置3。因此,中心装置3能够使个体车辆信息DB213的结构信息适当地与车辆同步。

[1230] 另外,若车辆侧系统4从多个ECU19接收各ECU19的“ECU SW ID”,则将对这些信息组合了“Vehicle SW ID”的结构信息列表发送至中心装置3。中心装置3比较由车辆侧系统4发送的“ECU SW ID”列表和存储于结构信息DB208的对应的车辆的正规的“ECU SW ID”列表,若判断为被发送的列表的组合非正规,则将异常检测发送至车辆侧系统4以及管理装置220。

[1231] 若这样构成,则中心装置3能够将车辆的结构信息的组合处于多个ECU19不能配合妨碍车辆的行驶这样的状态作为异常来检测,并通知给车辆侧系统4。由此,车辆侧系统4能够进行禁止车辆的行驶等的对应。

[1232] 中心装置3对于车辆的结构信息的组合非正规的车辆不实施更新有无的确认处理(D7)。因此,能够防止在不正规的车辆中执行程序更新。即使不正规的ECU19不是基于新程序的更新对象ECU,中心装置3也不实施更新有无的确认处理(D7)。在车辆侧系统4中执行程序更新时,也产生针对不是更新对象的ECU19的控制。因此,在具有不正规的ECU19的车辆中,有可能程序更新不能正常地完成,所以中心装置3不对该车辆执行程序更新。

[1233] 另外,中心装置3具备存储有将产生了基于新程序的更新通知给车辆侧所使用的活动信息的活动DB217,对于判断为正规的车辆,确认有无对应的车辆的活动信息。若有更新,则将该活动信息发送至车辆侧系统4。由此,能够对于用户提示活动信息,促使更新应用程序。能够以从车辆的结构信息上载为契机,中心装置3执行这些结构信息的同步、是否是正规的结构信息的判断、以及更新有无的确认作为一系列的处理,来对于适当的车辆迅速地通知程序的更新。

[1234] 此外,也可以如将第二实施方式如以下那样变形来实施。

[1235] • “同步开始请求”的发送由中心装置3对于车辆侧系统4进行,也可以若接收到“同步开始请求”则DCM12对于CGW13发送“结构信息收集请求”。例如,在“车辆型号=aaa”的结构信息DB208被更新时,中心装置3对于该车辆型号的车辆发送“同步开始请求”。

[1236] • 另外,也可以在成为更新数据的改写对象的ECU19中,在完成改写的时机将散列值发送至中心装置3。即,在成为改写对象的ECU19全部的程序更新完成的时机,也执行图

255所示的步骤D1～D12的流程图。

[1237] • 中心装置3在双方的散列值的比较结果是一致时,对于车辆侧系统4请求各ECU16的结构信息的组合列表的发送。而且,也可以若接收到上述组合列表,则进行步骤D6～D12的处理。

[1238] • 也可以中心装置3在双方的散列值的比较结果是一致时也参照活动DB217,确认对应的车辆的活动信息的有无。

[1239] 也可以如图256所示进行从车辆侧系统4向中心装置3的散列值的发送。图256是表示CGW13的处理的流程图。例如,在IG开关37被接通时,CGW13从各ECU19收集结构信息(D21),对于收集到的结构信息的数据值生成散列值(D22)。而且,将生成的散列值与存储于闪存24d的散列值(上次生成值)相比较,判断是否有差异(D23)。若有差异(是),则将本次生成的散列值存储于闪存24d(D24),将上述散列值发送至中心装置3。在步骤D23中,若双方的散列值没有差异(否)则结束处理。此外,在闪存24d预先存储有针对结构信息的初始值的散列值。由此,能够减少车辆侧系统4向中心装置3上载结构信息的次数。

[1240] (第三实施方式)

[1241] 第三实施方式涉及为了使车辆侧系统4中的应用程序的更新率提高而中心装置3的活动管理部3D执行的功能。如图258所示,例如在车辆侧系统4中,用户通过Config文件将HTTP轮询的间隔设定为3天程度,从而车辆侧系统4对于中心装置3周期性地确认应用程序的更新有无。由此,在对于与活动DB217对应的车辆设定了VIN的活动信息后进行更新确认的时刻,由中心装置3向车辆侧系统4通知“有更新”。即,如第二实施方式中说明那样,以从车辆侧系统4使用HTTP上载结构信息为契机,中心装置3进行更新确认这样的处理在经过3天后的IG接通的时机执行。

[1242] 若构成为这样以来自车辆的通知为契机进行更新有无,则中心装置3不需要在设定了活动信息的时刻从中心装置3向成为该活动的对象的全部车辆发送活动信息。然而,在用户长期不使用车辆的情况下,其间一直未进行使用HTTP的更新有无的确认。因此,也假定用户不知道新的活动被发行,产生未进行应用程序的更新的车辆。

[1243] 因此,如图259所示,中心装置3的SMS发送控制部212定期地或者在规定的时机参照个体车辆信息DB213检查各车辆的访问日志(E1)。而且,判断是否由在规定期间未进行向中心装置3的访问,换句话说用于应用程序的更新确认的结构信息的发送的车辆(E2)。规定期间为以在活动DB217设定了新的活动的日期为起算日的例如7天程度。换句话说,SMS发送控制部212将个体车辆信息DB213的“Vehicle SW ID”符合活动DB217的“更新前Vehicle SW ID”的车辆作为对象,确定出在7天间未进行更新确认的车辆。此外,SMS发送控制部212也可以将全部车辆作为对象,确定出在规定期间未进行更新确认的车辆。

[1244] 此外,在个体车辆信息DB213中,在由工厂生产出车辆时通过OEM登记有初始数据,然后,例如通过伴随车辆被销售的来自OEM的通知输入最初的访问日志。该访问日志实质上相当于用于使以下的程序的更新有效化的通知。访问日志未被输入的车辆成为步骤E2的判断对象外。

[1245] 若有在规定期间未进行更新确认的车辆(是),则SMS发送控制部212通过个体车辆信息DB213的型号、装备信息等判断该车辆的特性(E3)。作为这里的特性,SMS发送控制部212判断是电动汽车;能够进行SMS(Short Message Service)接收的EV、还是能够进行SMS

接收的现有的汽油引擎车,换句话说常规引擎车;组合车、还是难以接收SMS的车辆。例如,搭载于车辆的DCM12在不具有接收SMS的功能的情况、不进行接收SMS的契约的情况下,判断为是难以接收SMS的车辆。

[1246] 若是EV,则发送使该车辆的ECU19启动使结构信息发送序列开始的SMS(E5,参照图260)。若DCM12接收SMS,还行SMS中记载的指令,则成为IG接通电源状态,启动的CGW13经由DCM12向中心装置3发送结构信息。然后,如图255所示的步骤D1～D12那样,进行更新确认,执行分发数据包的下载等。在EV的情况下,电池的容量较大,所以认为能够足够保持停车状态作为IG接通电源状态进行程序的下载。因此,使用SMS使ECU19启动自动地开始更新确认以及下载之后的序列。

[1247] 假设在EV车的电池的余量较少的情况下,在车辆侧系统4中参照图250所示的改写规格数据,在低于被指定的电池余量的状态的情况下,被控制为不开始安装。或者,参照作为限制事项被记载于中心装置3通过步骤D9发送的活动文件的电池余量,在低于被指定的电池余量的状态的情况下,控制为在车辆侧系统4中不开始分发数据包的下载。

[1248] 在组合车中,在DCM12间歇地启动的期间,对于处于能够接收SMS的状态的车辆,SMS发送控制部212发送能够在车载显示器7显示的SMS(E4,参照图260)。例如,CGW13将接收到的SMS中记载的文本文在下次IG接通的时机向车载显示器7显示指示。另外,也可以在个体车辆信息DB213登记有用户的移动终端6的信息的情况下,向该移动终端6发送SMS。例如,使“有活动信息。请接通IG。”这样的文字消息显示。个体车辆信息DB213是用户信息存储部的一个例子。另一方面,针对处于难以接收SMS的状态的车辆不进行任何处理,向另外的用户进行邮寄等来应对(E6)。

[1249] 如以上所述,根据第三实施方式,车辆侧系统4将多个ECU19的结构信息发送至中心装置3,在个体车辆信息DB213中,由各车辆发送的结构信息与发送日一起存储。另外,在活动DB217中存储有活动ID以及能够识别数据更新的对象车辆的对象VIN列表作为活动信息。而且,中心装置3参照个体车辆构成DB213,若在从与对象车辆相关联的发送日起的规定期间内没有结构信息的发送,则通过SMS向对象车辆的车辆侧系统4发送用于促使数据更新的消息。

[1250] 若这样构成,则用户没有搭乘车辆的机会,所以在继续结构信息未被发送至中心装置3的状况的情况下,若经过存储于个体车辆信息DB213的发送日起的规定期间,则中心装置3也向对象车辆的车辆侧系统4发送用于促使数据更新的消息。因此,用户能够通过参照该消息来识别需要数据更新。

[1251] 而且,中心装置3通过参照个体车辆信息DB213和活动DB217来决定程序更新的对象车辆。即,在个体车辆信息DB213存储有结构信息被从各车辆发送的日期,在活动DB217存储有对象VIN列表。因此,中心装置3能够通过来自各车辆的结构信息的发送日和对象VIN列表决定程序更新的对象车辆。

[1252] 另外,若车辆侧系统4以车辆的点火开关37被接通为契机,从各ECU19接收各个结构信息,则将结构信息发送至中心装置3。因此,在用户搭乘车辆时,能够将结构信息可靠地发送至中心装置3。

[1253] 而且,若对象车辆是电动汽车,则中心装置3使该对象车辆的ECU启动的指令包含于消息来发送,接收到该消息的车辆侧系统4使ECU19启动,使与数据更新有关的处理执行。

即,电动汽车的电池的容量比较充裕,所以能够不等待用户的操作使ECU19执行与数据更新有关的处理。因此,能够使数据更新高效地执行。

[1254] 另外,若对象车辆是组合车,则中心装置3至少将能够在对象车辆的车载显示器7显示的文字信息作为消息发送。因此,组合车的用户能够通过参照显示于车载显示器7的文字信息来识别需要数据更新。

[1255] 另外,中心装置3在个体车辆信息DB213存储有用户的移动终端6的发送目的地时,将能够显示于移动终端6的文字信息作为消息发送。由此,即使用户没有搭乘车辆的机会,也能够通过参照显示于移动终端6的文字信息,来识别需要数据更新。

[1256] 进一步,若用户经由移动终端6预先将活动的发送日和发送目的地发送至中心装置3,则中心装置3将该发送日以及发送目的地存储到个体车辆信息DB213。例如,用户指定活动发行的翌日作为发送日,不将车载显示器7而将移动终端6指定为发送目的地。另外,用户指定未乘车的规定时刻作为发送日,指定车辆作为发送目的地,进行向自动地程序更新的同意操作。由此,不管有无结构信息的发送,中心装置3都将活动信息在上述发送日对于上述发送目的地发送。因此,在预先把握暂时没有用户搭乘车辆的机会时,能够设定为在用户设定的发送日接收活动信息。

[1257] 此外,也可以将第三实施方式如以下方式那样变形来实施。

[1258] • 也可以将用户信息存储部与个体车辆信息DB213分开设置。

[1259] • 活动信息的发送也可以使用SMS以外。

[1260] • 也可以代替将发送日存储于个体车辆信息DB213,中心装置3例如存储没有从车辆侧的发送的日期,在该日期连续7天时发送促使数据更新的消息。

[1261] (第四实施方式)

[1262] 第四实施方式表示用户指定活动信息、消息的通知方法的情况。例如,假定用户预先确定在1个月期间左右不乘车,没有接通IG开关37的机会的情况。如图261所示,用户通过移动终端6向中心装置3发送活动产生时的通知目的地以及通知的日期时间的设定。例如,进行在1个月后向移动终端6通知活动信息这样的设定。由此,个体车辆信息管理部3C使上述通知目的地以及通知日期时间的信息存储于个体车辆信息DB213,根据设定向用户进行通知。例如,若在该1个月的期间设定活动(1、2)这2个,则SMS发送控制部212在1个月后向用户的移动终端6通知活动(1、2)的信息,促使程序更新。

[1263] 如以上那样,根据第四实施方式,若用户经由移动终端6将活动信息的发送日和发送目的地发送至中心装置3,则中心装置3将上述发送日以及发送目的地存储于个体车辆信息DB213。而且,中心装置3在存储的发送日对于发送目的地发送活动信息。由此,在确认用户在恒定期间不搭乘车辆的情况下,能够停止从中心装置3发送不必要的活动信息。

[1264] (第五实施方式)

[1265] 第五实施方式表示在中心装置3向车辆侧系统4发送更新程序的数据时,车辆侧系统4赋予验证数据的完整性所使用的验证数据的功能。如图262以及图263所示,供应商使用数据包管理部3A制作登记到ECU重编数据DB204的数据。具体而言,数据包管理部3A制作用于将旧程序改写为新程序的新差分数据作为更新数据(Y1),制作作为针对ECU19的新程序的完整性验证数据的散列值,以及针对新差分数据的散列值(Y2)。这里,也可以在ECU为单面存储器的情况下,制作用于将新程序改写为旧程序的旧差分数据作为回滚数据,制作针

对ECU19的旧程序的散列值、以及针对旧差分数据的散列值。

[1266] 数据包管理部3A对于各散列值应用使用了作为规定的密钥的密钥值的加密生成认证符(Y3)。而且,数据包管理部3A发送更新数据以及各带认证符的完整性验证数据,存储于ECU重编数据DB204(Y4)。数据包管理部3A如上述那样生成数据包,生成针对数据包的完整性验证数据,向车辆侧系统4发送(Y5)。

[1267] 主装置(OTA主机)11运算针对数据包的完整性验证数据,比较该运算值和接收到的数据包的完整性验证数据,进行数据包的完整性验证(Y6)。若数据包的完整性验证成功,则主装置11将ECU的更新数据以及完整性验证数据向改写对象ECU(目标ECU)19发送(Y7)。

[1268] 改写对象ECU19运算针对更新数据的完整性验证数据,比较该运算值和接收到的更新数据的完整性验证数据,进行更新数据的完整性验证(Y8)。若更新数据的完整性验证成功,则改写对象ECU19复原作为更新数据的差分数据,进行向闪存28d的写入(Y9)。若写入完成,则改写对象ECU19运算针对写入闪存28d的数据的完整性验证数据,比较该运算值和接收到的新程序的完整性验证数据,进行闪存28d的完整性验证(Y10)。改写对象ECU19将该验证结果向主装置11发送(Y11),主装置11将接收到的该验证结果作为安装结果通知向中心装置3发送(Y12)。

[1269] 例如图243所示,数据包管理部3A对于最新的“ECU SW ID”生成以下的完整性验证数据。在ECU的存储器结构为双面存储器或者挂起的情况下,能够省略以下(3)(4)。

[1270] (1)生成作为针对ECU的新程序的完整性验证数据的散列值。进行该处理的功能部分是第一验证值生成部(步骤A1)的一个例子。

[1271] (2)生成作为用于以ECU的旧程序为基础向新程序更新的差分数据的更新数据、作为该更新数据的完整性验证数据的散列值。进行该处理的功能部分是第二验证值生成部(步骤A4)的一个例子。

[1272] (3)生成作为针对ECU的旧程序的完整性验证数据的散列值。进行该处理的功能部分是第四验证值生成部(步骤A5)的一个例子。

[1273] (4)生成作为用于以ECU的新程序为基础向旧程序更新的差分数据的更新数据、作为该更新数据的完整性验证数据的散列值。进行该处理的功能部分是第五验证值生成部(步骤A7)的一个例子。

[1274] 此外,“程序”也包括在程序中使用的常量数据等。若是“ECU SW ID=ads_002”,则对于更新数据“Adsfile001-002”生成该散列值x1。如上所述,散列函数例如使用SHA-256。散列值相当于验证值。这里,数据包管理部3A也可以构成为对于散列值应用使用了作为规定的密钥的密钥值的加密生成认证符而生成带认证符的完整性验证数据。

[1275] 接下来,供应商通过对于完整性验证数据应用使用作为规定的密钥的密钥值的加密生成认证符而生成带认证符的完整性验证数据,将更新数据和带认证符的完整性验证数据建立对应关系地提供给OEM。换句话说,通过数据包管理部3A,各程序和针对此的带认证符的完整性验证数据以被登记到ECU重编数据DB204而提供给OEM。通过OEM的指示,数据包管理部3A使用ECU重编数据DB204等如上述那样生成改写规格数据,生成分发数据包,登记到数据包DB206。若从车辆侧系统4产生更新数据的下载请求,则中心装置3根据该下载请求将包括更新数据和带认证符的完整性验证数据的分发数据包分发至车辆侧系统4。此外,权利要求书中的“完整性验证数据”包括仅包括散列值的数据、和包括基于密钥的加密的带认

证符的完整性验证数据的任一方。

[1276] 若车辆侧系统4的主装置11接收分发数据包,则使用对分发数据包赋予的完整性验证数据(第三验证值),验证分发数据包的妥当性。具体而言,比较使用分发数据包运算出的完整性验证数据和接收到的完整性验证数据,若一致则判断为正常。在作为验证的结果确认为正常的情况下,主装置11将分发数据包解包为每个ECU的数据(参照图239)。而且,主装置11将更新数据以及带认证符的完整性验证数据传输到写入目的地的ECU19。

[1277] ECU19使用带认证符的完整性验证数据(第二验证值)验证更新数据的妥当性。具体而言,比较使用接收到的更新数据运算出的完整性验证数据和接收到的完整性验证数据,若一致则判断为正常。在作为验证的结果确认为正常的情况下,ECU19的CPU28a进行向闪存28d的写入处理。若写入处理完成,则ECU19使用带认证符的完整性验证数据(第一验证值)读出写入闪存28d的数据,验证其妥当性。具体而言,比较使用读出的数据运算出的完整性验证数据和接收到的完整性验证数据,若一致则判断为正常。此外,这里的完整性验证数据也在ECU19的启动时使用,所以预先向闪存28d的规定区域存储。若这些处理完成,则ECU19包括验证结果,将写入响应发送至主装置11。主装置11向中心装置3通知安装结果。此外,图中的“目标ECU”与“对象ECU”是相同意思,“OTA主机”与“DCM”是相同意思。CPU28a是写入处理部的一个例子。

[1278] 这里,在安装的中途产生程序更新的取消的情况下,ECU19进行回滚处理。ECU19写入更新数据,并且使用带认证符的完整性验证数据(第五验证值)验证回滚用差分数据的妥当性。具体而言,比较使用回滚用差分数据运算出的完整性验证数据和接收到的完整性验证数据,若一致则判断为正常。在作为验证的结果确认为正常的情况下,ECU19在完成了更新数据的写入之后,开始使用回滚用差分数据的写入。而且,在完成写入之后,ECU19使用带认证符的完整性验证数据(第四验证值),读出写入闪存28d的数据,验证其妥当性。此外,接收到的差分数据(更新数据、回滚用差分数据)的完整性验证也可以是不由ECU19进行,而由主装置11进行的构成。

[1279] 如图264所示,然后,若上述车辆的IG开关37被接通,则以此为契机,ECU19进行启动时的数据验证。ECU19使用带认证符的完整性验证数据(第一验证值或者第四验证值)验证启动的程序等的完整性。首先,在闪存28d中,对于写入了被更新的程序、常量数据的评价对象区域的数据值应用散列函数,获取散列值。接下来,对带认证符的完整性验证数据进行解密,对解密结果所包含的散列值(期待值)和获取到的散列值(运算值)进行对照,判断写入闪存28d的程序等是否被篡改。若双方的散列值一致为“OK”,则ECU19如通常那样进行启动处理。对于各ECU19进行同样的处理,若全部的评价对象ECU19的结果是“OK”,结束处理。

[1280] 另一方面,若任意一个ECU19的验证结果异常,为“NG”,则ECU19保存处理的日志向主装置11通知错误。主装置11同样地保存日志向中心装置3通知错误。中心装置3同样地保存日志向OEM等的管理装置220通知错误。向管理装置220的通知例如通过SMS发送控制部212使用SMS进行,或通过经由因特网线路的电子邮件的发送等进行。

[1281] 在上述的实施例中,构成为在车辆侧系统4中,进行完整性的验证。在图265中,对由中心装置3进行完整性的验证(与期待值的比较)的情况进行说明。在图265中,例如在IG接通等时机中,ECU19在向主装置11发送更新后的应用程序的版本信息时,与版本信息一起与上述同样地生成带认证符的完整性验证数据并发送(X1)。ECU19运算针对闪存28d的数据

的完整性验证数据,将该运算值向主装置11发送。主装置11包含带认证符的完整性验证数据作为结构信息并发送至中心装置3(X2)。

[1282] 中心装置3访问ECU重编数据DB204,获取与目标ECU19的“ECU SW ID”一致的带认证符的完整性验证数据(X3、X4),并与从车辆侧上载的完整性验证数据进行对照(X5)。具体而言,从ECU重编数据DB获取与“ECU SW ID”对应的新程序的完整性验证数据并进行对照。若对照的结果不一致,是NG(X6;NG),则对于OEM的管理装置220通知异常(X7)。该处理部分的功能相当于异常报告部。

[1283] 中心装置3将对照结果向主装置11发送(X8),主装置11将接收到的对照结果向改写对象ECU19发送(X9)。改写对象ECU19在对照结果为OK的情况下,按照通常那样使应用程序动作,在对照结果为NG的情况下,不使应用程序动作。此外,在本实施例中,数据包管理部3A能够省略新程序的完整性验证数据生成(步骤A1)、旧ECU程序的完整性验证数据生成(步骤A5)。

[1284] 此外,在上述中,ECU19在进行了更新数据的写入之后,在车辆的IG开关37被接通的时机验证更新数据的完整性,但也可以代替于此,在进行了更新数据的写入之后验证完整性。

[1285] 另外,在上述的实施方式中,仅对更新数据赋予带认证符的完整性验证数据,也可以如以下那样实施。

[1286] • 从ECU重编数据DB204获取新程序以及对应的更新数据(数据获取步骤;步骤A1)。

[1287] • 第一验证值生成部对新程序生成第一散列值(第一验证值生成步骤;步骤A2)。

[1288] • 第二验证值生成部对更新数据生成第二散列值(第二验证值生成步骤;步骤A4)。数据包生成部202使分发数据包包括更新数据、规格数据和第一以及第二散列值(分发数据包生成步骤)。更新数据与新差分数据对应。

[1289] • 第三验证值生成部对分发数据包生成第三散列值(第三验证值生成步骤;步骤C4)。

[1290] • 数据包分发部203将分发数据包以及第三散列值发送至车辆侧系统4(发送步骤)。

[1291] 此外,对于认证符而言,既可以仅对分发数据包以及第三散列值赋予,也可以在生成各散列值的每个阶段赋予。数据包分发部203相当于发送部。

[1292] 该情况下,在车辆侧系统4中,

[1293] • 作为接收处理部的DCM12接收分发数据包以及第三散列值。

[1294] • 第三验证处理部比较根据分发数据包数据生成的散列值和接收到的第三散列值,验证分发数据包数据的完整性。

[1295] • 第二验证处理部比较根据更新数据生成的散列值和接收到的第二散列值,验证更新数据的完整性。

[1296] • 作为写入处理部的一个例子的CPU28a将更新数据写入闪存28d。

[1297] • 第一验证处理部通过写入更新数据来对成为新程序的闪存28d内的数据值生成散列值,与接收到的第一散列值相比较,验证新程序的完整性。

[1298] 若更新数据的验证结果是NG,则中止向闪存28d的写入。另外,若写入闪存28d的新

程序的验证结果是NG,则使新程序无效,根据需要进行回滚处理。此外,第一～第三验证处理部也可以由CPU28a实现。另外,若第一～第三验证处理部的任意一个验证结果是NG,则作为发送处理部的DCM12向中心装置3通知异常。

[1299] 进一步,除了上述之外,如图243所示,在存在用于返回改写更新数据前的旧程序的状态的回滚数据时,也可以如以下那样实施。

[1300] • 第四验证值生成部对于旧程序生成第四散列值(第四验证值生成步骤;步骤A5)。

[1301] • 第五验证值生成部对于用于将新程序返回旧程序的回滚数据生成第五散列值(第五验证值生成步骤;步骤A7)。回滚数据表示回滚用差分数据,与旧差分数据对应。

[1302] • 数据包生成部202使分发数据包包括更新数据、回滚用差分数据、改写规格数据和第一、第二、第三以及第四散列值(分发数据包生成步骤)。

[1303] 该情况下,在车辆侧系统4中,将更新数据改写到闪存28d的期间,若例如由用户指示改写中止则取消改写,进行向旧程序的还原,换句话说回滚。这仅是ECU19的存储器结构为单面存储器的情况。

[1304] • 第二验证处理部计算针对分发数据包所包含的回滚数据的散列值,比较计算出的散列值和第五散列值验证回滚数据的完整性。

[1305] • CPU28a使用回滚数据进行向闪存28d的写入。

[1306] • 第一验证处理部对于通过向闪存28d的写入而还原的旧程序计算散列值,比较计算出的散列值和第四散列值验证旧程序的完整性。

[1307] 如以上那样,根据第五实施方式,在ECU重编数据DB204存储有作为改写对象的目标ECU19的新程序、旧程序、以及作为用于从旧程序更新为新程序的新差分数据的更新数据。第一验证值生成部使用新程序生成第一散列值,第二验证值生成部使用更新数据生成第二散列值。数据包生成部202生成包括针对多个目标ECU19的更新数据和第一以及第二验证值及规格数据的数据包。第三验证值生成部使用分发数据包生成第三散列值,数据包分发部203将分发数据包与第三散列值一起发送至车辆侧系统4。

[1308] 若车辆侧系统4接收分发数据包以及第三散列值,则第三验证处理部计算针对分发数据包的散列值,与第三散列值相比较验证分发数据包的完整性。第二验证处理部计算分发数据包所包含的与目标ECU19对应的更新数据散列值,并与分发数据包所包含的第二散列值相比较来验证更新数据的完整性。

[1309] CPU28a将更新数据写入闪存28d,第一验证处理部计算针对闪存28d的被更新的新程序的数据的散列值,与第一散列值相比较,验证新程序的数据的完整性。这样,能够使用各散列值在多个阶段验证各数据值的完整性。而且,能够对于新程序3重地验证完整性,能够避免车辆侧系统4写入不完整的新程序、以不正确的新程序动作。

[1310] 另外,在ECU重编数据DB204存在回滚数据时,第四验证值生成部对于旧程序生成第四散列值,第五验证值生成部对于回滚数据生成第五散列值。数据包生成部202使分发数据包包括更新数据、第一以及第二散列值、回滚数据、第四以及第五散列值。

[1311] 而且,在车辆侧系统4中进行回滚时,第二验证处理部计算针对分发数据包所包含的回滚数据的散列值,与第五散列值相比较验证回滚数据的完整性。CPU28a使用回滚数据进行向闪存28d的写入。第一验证处理部对于通过向闪存28d的写入而还原的旧程序计算散

列值,与第四散列值相比较来验证旧程序的完整性。由此,也能够对于回写的旧程序验证完整性。在上述中,第一～第五验证值生成部是中心装置3的数据包管理部3A内的功能模块。第一、第二、第四以及第五验证处理部是车辆侧系统4的目标ECU19内的功能模块。另外,第三验证处理部是车辆侧系统4的主装置11(OTA主机11)内的功能模块。

[1312] (第一实施方式的变形其1)

[1313] 如图266以及图267所示,也可以使一个活动「cpn_001」对应多个数据包“pkg_001_1”以及“pkg_001_2”。另外,也可以将多个数据包作为多个组。在上述的实施例中,构成为在一个数据包中包括多个组。在本变形例中,以一个组生成一个数据包,对于一个活动分发多个数据包。例如,数据包“pkg_001_1”包含有属于组1的ECU亦即“ADS”以及“BRK”,数据包“pkg_001_2”包含有属于组2的ECU亦即“EPS”。

[1314] 该情况下,如图268以及图269所示,按组分别独立地生成规格数据以及分发数据包。在图268中,规格数据生成部201生成例如记载了“ADS”以及“BRK”的ECU信息的第一规格数据作为组1的规格数据。规格数据生成部201生成例如记载了“EPS”的ECU信息的第二规格数据作为组2的规格数据。而且,在图269中,数据包生成部202生成例如根据ECU顺序合并了属于组1的“ADS”以及“BRK”的更新数据等的重编数据,与第一规格数据合并而生成数据包文件“pkg001_1.dat”。数据包生成部202使用属于组2的“EPS”的更新数据等生成重编数据,与第二规格数据合并而生成数据包文件“pkg001_2.dat”。

[1315] (第一实施方式的变形其2)

[1316] 图270表示合并了规格数据生成部201以及数据包生成部202的功能构成一个数据包生成工具221的情况下的处理内容。以下,重新对各处理进行说明。

[1317] 在规格数据生成处理中,将由工作人员输入的值作为规格数据信息以预先规定了比特数、排列顺序的数据结构输出,生成规格数据。作为规格数据信息,除了例如图250所例示的值即ECU(ID1)、ECU(ID2)、ECU(ID3)这样的ECU单位的信息以外,还输入车辆单位或者系统(组)单位的信息。所谓车辆单位的信息是指例如图250所示的改写环境信息,所谓系统单位的信息是指例如图250所示的组信息、ECU顺序的信息。车辆单位、系统单位的输入信息也可以分别作为单独的文件。也可以使规格数据生成处理具有自动地计算更新数据的文件大小等一部分的值并使规格数据反映的功能。

[1318] 在数据包生成处理中,将所生成的规格数据、各ECU的更新数据、作为各ECU的完整性验证数据输入的值、文件以预先规定了比特数、排列顺序的数据结构输出,生成分发数据包的文件。各ECU的更新数据以及完整性验证数据按组的从小到大的顺序、ECU顺序的从小到大的顺序排列。这里,除了更新数据(新差分数据)以外,也可以将回滚用数据(旧差分数据)添加到输入。作为完整性验证数据,输入了“ECU程序(新)的完整性验证数据”“更新数据的完整性验证数据”。在也添加回滚数据的情况下,也将“ECU旧程序的完整性验证数据”“旧差分数据的完整性验证数据”添加到输入。

[1319] 在完整性验证数据生成处理中,如对图252的步骤C4描述那样,对被生成的数据包文件生成完整性验证数据。

[1320] 被生成的数据包文件、对数据包文件生成的完整性验证数据由工作人员登记到数据包DB206。

[1321] 中心装置3执行的功能既可以由硬件实现,也可以由软件实现。另外,也可以通过

硬件与软件的配合实现。

[1322] 改写的数据不仅是应用程序,也可以是地图等数据、控制参数等数据。

[1323] 结构信息的内容不限于例示的内容,可以根据各自的设计适当地选择。

[1324] 规格数据的内容也不限于例示的内容。

[1325] 活动信息、分发规格数据也可以包含于分发数据包发送至车辆侧,也可以与分发数据包分别地发送至车辆侧。

[1326] 在第五实施方式中,也可以预先将分发数据包以及第三验证值存储于数据包存储部,数据包发送部213根据来自车载侧系统4的请求,将与该请求相关联的分发数据包以及第三验证值发送至车载侧系统4。

[1327] 根据本实施方式,通过进行上述的(13)激活的执行控制处理能够得到以下所示的作用效果。在改写对象ECU19中,若判定为激活的执行条件成立,则在重新启动后,基于运用面信息使第二数据储存面作为启动面启动。在将在双面具有数据储存面的ECU19作为应用程序的改写对象的情况下,能够基于来自外部的指示适当地控制激活。

[1328] 在改写对象ECU19中,将从CGW13指示了软件的复位请求、从CGW13指示了电源的复位请求、以及与CGW13的通信中断持续了规定时间作为执行条件。能够将从CGW13指示了软件的复位请求、从CGW13指示了电源的复位请求、以及与CGW13的通信中断持续了规定时间作为执行条件,在重新启动后,基于运用面信息使第二数据储存面作为启动面启动。

[1329] 在改写对象ECU19中,若在未完成第二数据储存面的程序的改写时,从CGW13指示了激活请求,则向CGW13通知否定响应。能够向CGW13通知虽然指示了激活请求但未完成第二数据储存面的程序的改写的主旨。

[1330] 在改写对象ECU19中,若在虽然完成第二数据储存面的程序的改写但改写后的数据验证为否时,从CGW13指示了激活请求,则向CGW13通知否定响应。能够向CGW13通知虽然完成第二数据储存面的程序的改写但改写后的数据验证为否的主旨。

[1331] 本公开根据实施例进行了描述,但可理解为不限于该实施例、构造。本公开也包含各种变形例、均等范围内的变形。另外,也将各种组合、方式,甚至其中仅包含一个要素、更多或者更少要素的其他的组合、方式纳入本公开的范畴、思想范围。

[1332] 本公开中记载的控制部及其方法也可以由通过构成编程为执行由计算机程序具体化的一个或多个功能的处理器以及存储器而提供的专用计算机实现。或者,本公开中记载的控制部及其方法也可以由通过利用一个以上的专用硬件逻辑电路构成处理器而提供的专用计算机实现。或者,本公开中记载的控制部及其方法也可以由通过编程为执行一个或多个功能的处理器以及存储器与由一个以上的硬件逻辑电路构成的处理器的组合构成的一个以上的专用计算机实现。另外,计算机程序也可以作为由计算机执行的指令存储于计算机可读非过渡有形记录介质。

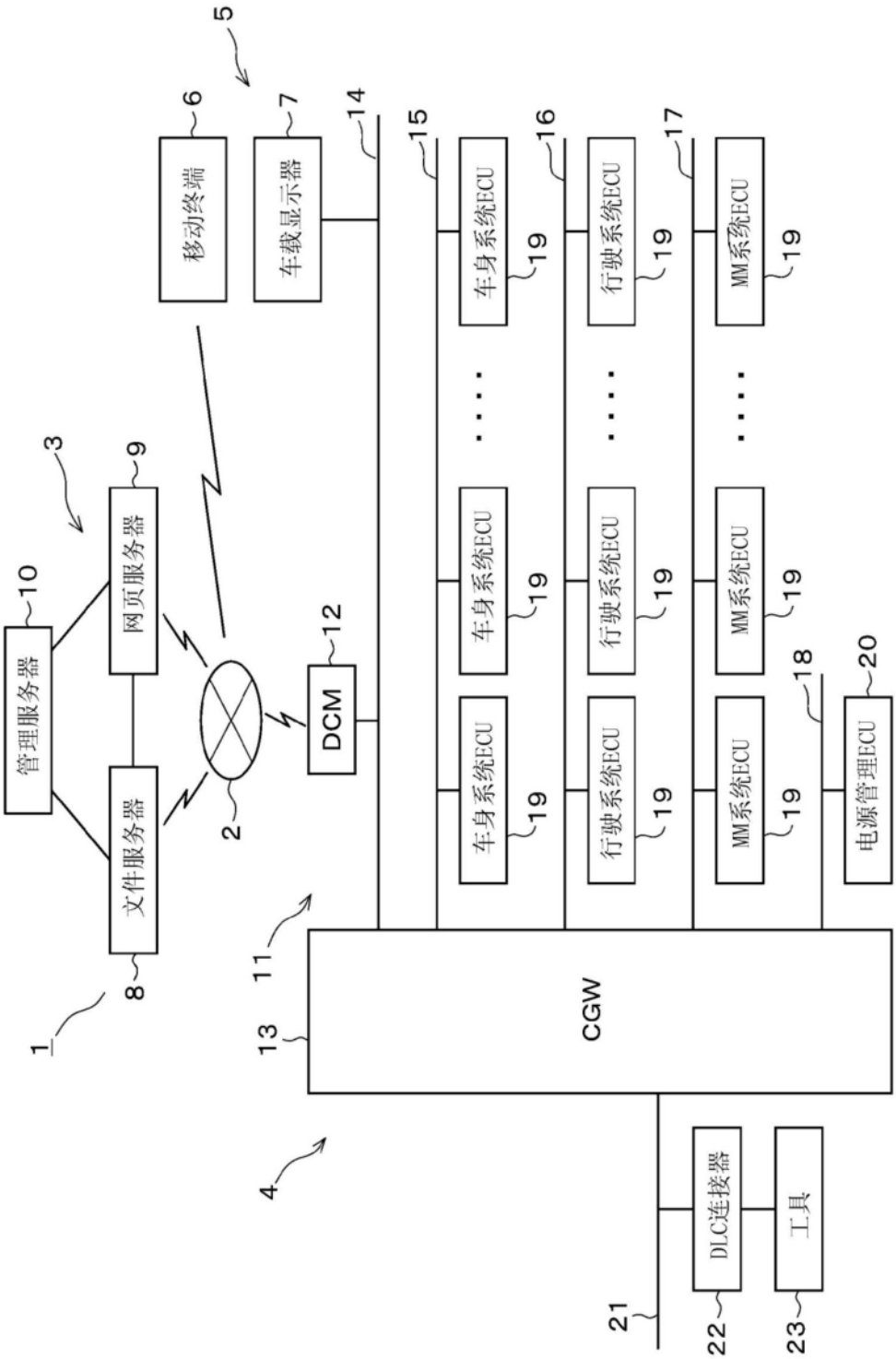

1
2
3
4
5
6
移动终端
7
车载显示器
8
文件服务器
9
网页服务器
10
管理服务器
11
12
DCM
13
CGW
14
15
16
17
18
19
车身系统ECU
行驶系统ECU
MM系统ECU
20
电源管理ECU
21
22
DLC连接器
23
工具

图1

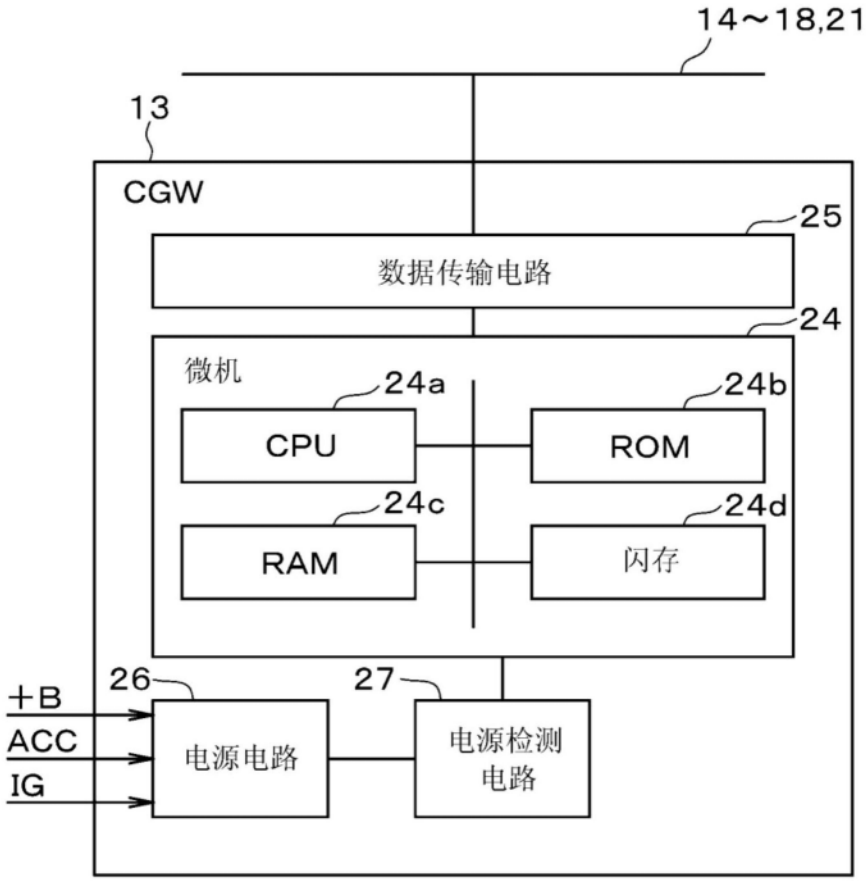

14～18,21
13
CGW
25
数据传输电路
24
微机
24a
CPU
24b
ROM
24c
RAM
24d
闪存
26
27
+B
ACC
IG
电源电路
电源检测
电路

图2

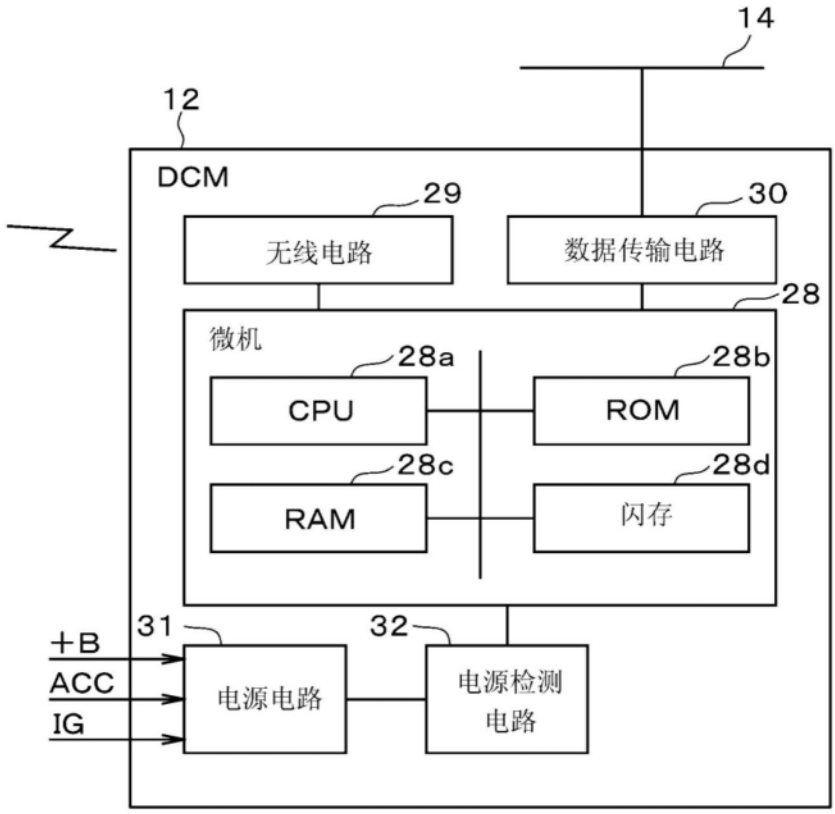

14
12
DCM
29
无线电路
30
数据传输电路
28
微机
28a
CPU
28b
ROM
28c
RAM
28d
闪存
31
32
+B
ACC
IG
电源电路
电源检测
电路

图3

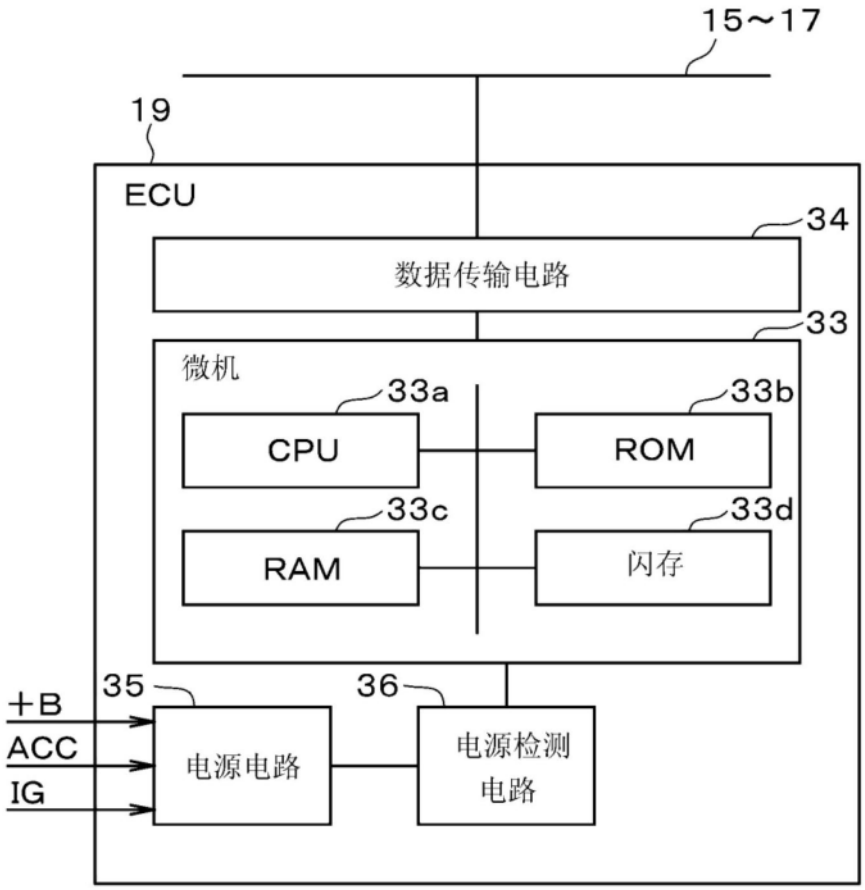

15～17
19
ECU
34
数据传输电路
33
微机
33a
CPU
33b
ROM
33c
RAM
33d
闪存
35
36
+B
ACC
IG
电源电路
电源检测
电路

图4

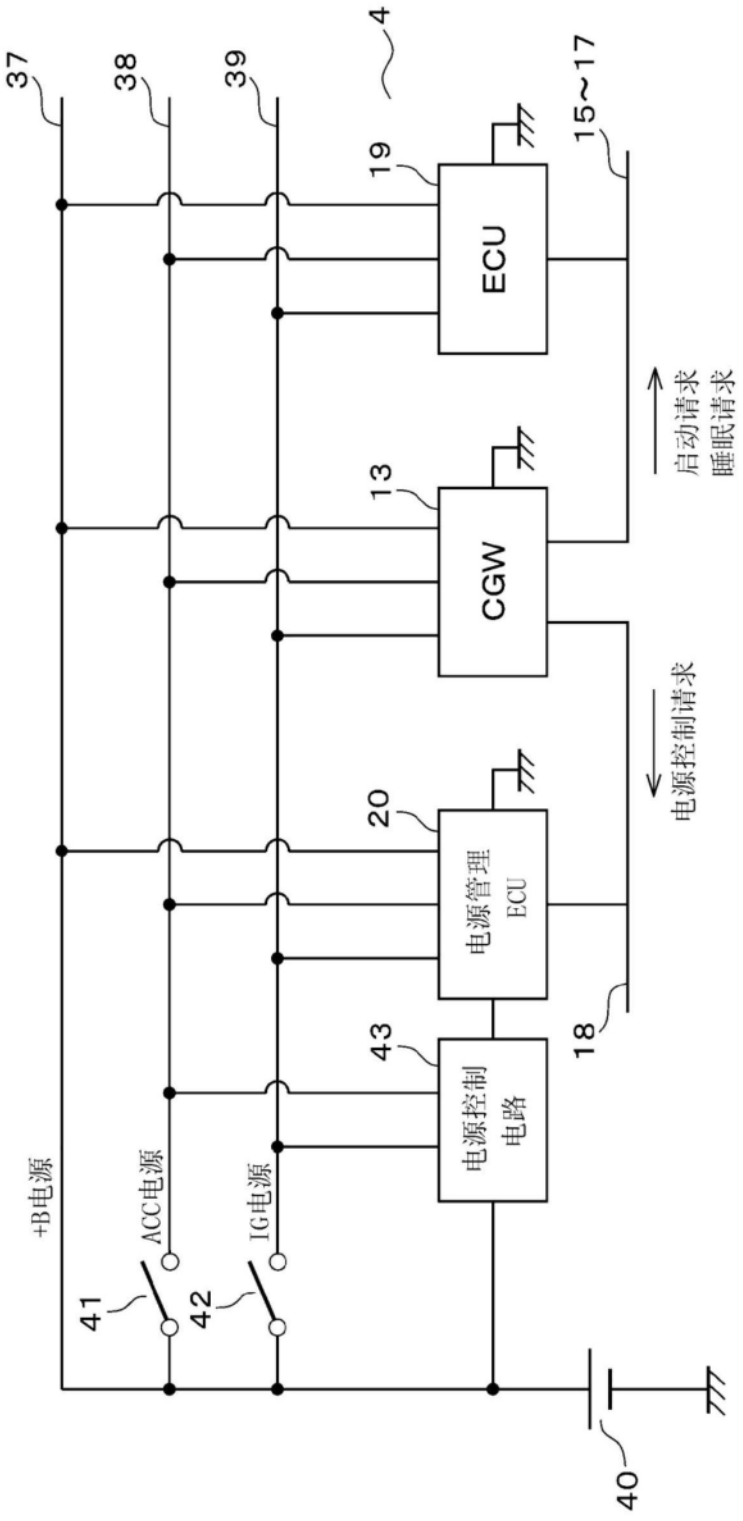

37
38
39
4
15~17
19
ECU
13
CGW
20
电源管理
ECU
43
电源控制
电路
18
40
41
42
+B电源
ACC电源
IG电源
启动请求
睡眠请求
电源控制请求

图5

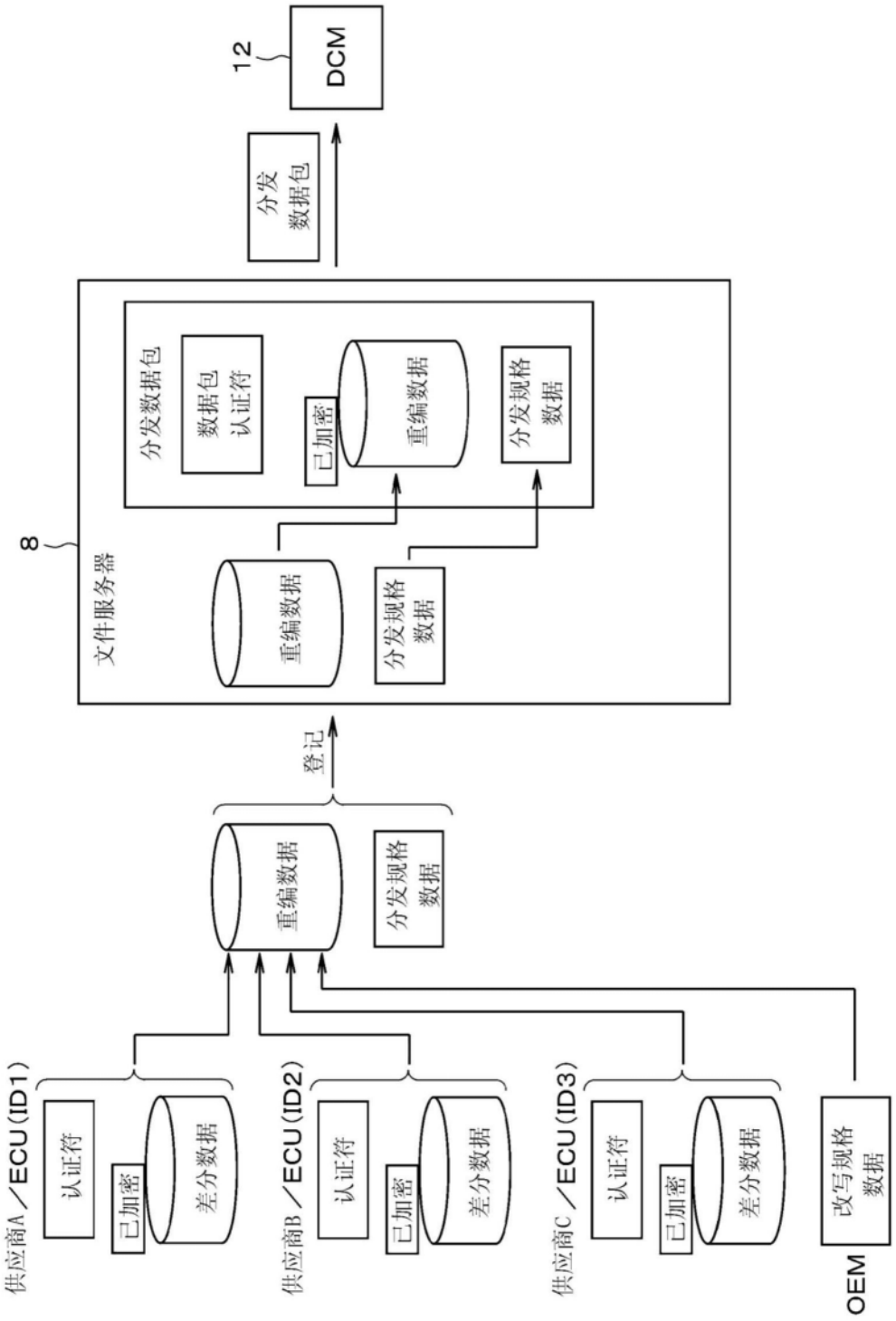

12
DCM
分发
数据包
8
文件服务器
分发数据包
数据包
认证符
已加密
重编数据
分发规格
数据
重编数据
分发规格
数据
登记
重编数据
分发规格
数据
供应商A／ECU(ID1)
认证符
已加密
差分数据
供应商B／ECU(ID2)
认证符
已加密
差分数据
供应商C／ECU(ID3)
认证符
已加密
差分数据
改写规格
数据
OEM

图6

DCM用的改写规格数据

项目		值（例示）
规格数据信息	地址信息	0x10000000
	文件名	规格. bin
ECU（ID1）信息	ECU ID	1
	更新程序获取地址	0x10000000
	更新程序大小	1M字节
	回滚程序获取地址	0x20000000
	回滚程序大小	1M字节
ECU（ID2）信息	ECU ID	2
	更新程序获取地址	0x30000000
	更新程序大小	1M字节
	回滚程序获取地址	0x40000000
	回滚程序大小	1M字节
ECU（ID3）信息	ECU ID	3
	更新程序获取地址	0x50000000
	更新程序大小	1M字节
	回滚程序获取地址	0x60000000
	回滚程序大小	1M字节
ECU（ID4）信息	ECU ID	4
	更新程序获取地址	0x70000000
	更新程序大小	1M字节
	回滚程序获取地址	0x80000000
	回滚程序大小	1M字节
ECU（ID5）信息	ECU ID	5
	更新程序获取地址	0x90000000
	更新程序大小	1M字节
	回滚程序获取地址	0xA0000000
	回滚程序大小	1M字节
ECU（ID6）信息	ECU ID	6
	更新程序获取地址	0xB0000000
	更新程序大小	1M字节
	回滚程序获取地址	0xC0000000
	回滚程序大小	1M字节

图7

CGW用的改写规格数据

项目		值（例示）
组信息	第一组信息	ECU(ID1)→ECU(ID2)→ECU(ID3)
	第二组信息	ECU(ID4)→ECU(ID5)→ECU(ID6)
总线负载表		参照图100
电池负载		40%
改写时的车辆状态		全部停车中 / 全部行驶中 / 最优
场景信息		召回 / 经销商 / 工厂用 / 功能更新通知 / 强制执行
ECU（IDn）信息 n=1~6	ECU_ID	ECU_ID
	连接总线	第一总线
	连接电源	+B电源、ACC电源、IG电源
	安全访问密钥信息	随机值 密钥模式 解密运算模式
	存储器种类	单面单独存储器 / 伪双面存储器 / 双面存储器
	改写方法	电源自保持 / 电源控制
	电源自保持时间	5分钟
	改写面信息	A面是启动面，B面是改写面
	更新程序版本	2.0
	更新程序获取地址	1
	更新程序大小	10M字节
	回滚程序版本	1.0
	回滚程序获取地址	0x8000
	回滚程序大小	10M字节
	更新程序数据种类	差分数据 / 全部数据
	回滚程序数据种类	差分数据 / 全部数据

图8

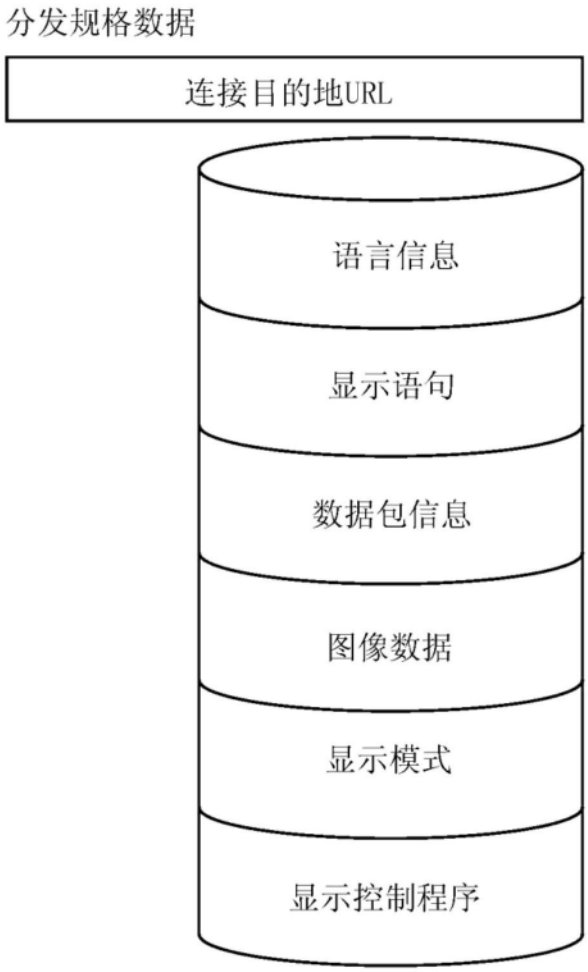


图9

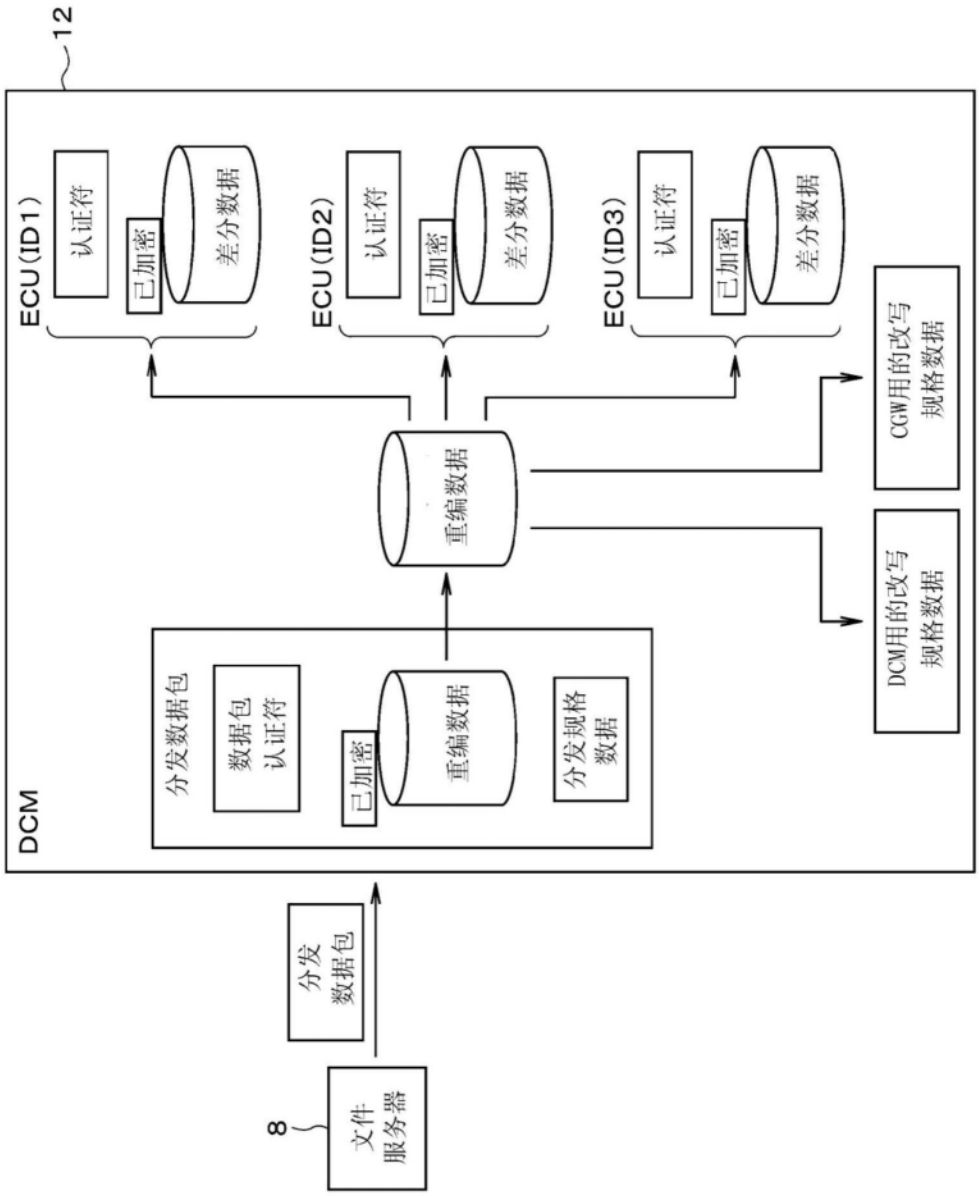

12
ECU(ID1)
认证符
已加密
差分数据
ECU(ID2)
认证符
已加密
差分数据
ECU(ID3)
认证符
已加密
差分数据
重编数据
CGW用的改写规格数据
DCM用的改写规格数据
DCM
分发数据包
数据包认证符
已加密
重编数据
分发规格数据
分发数据包
8
文件服务器

图10

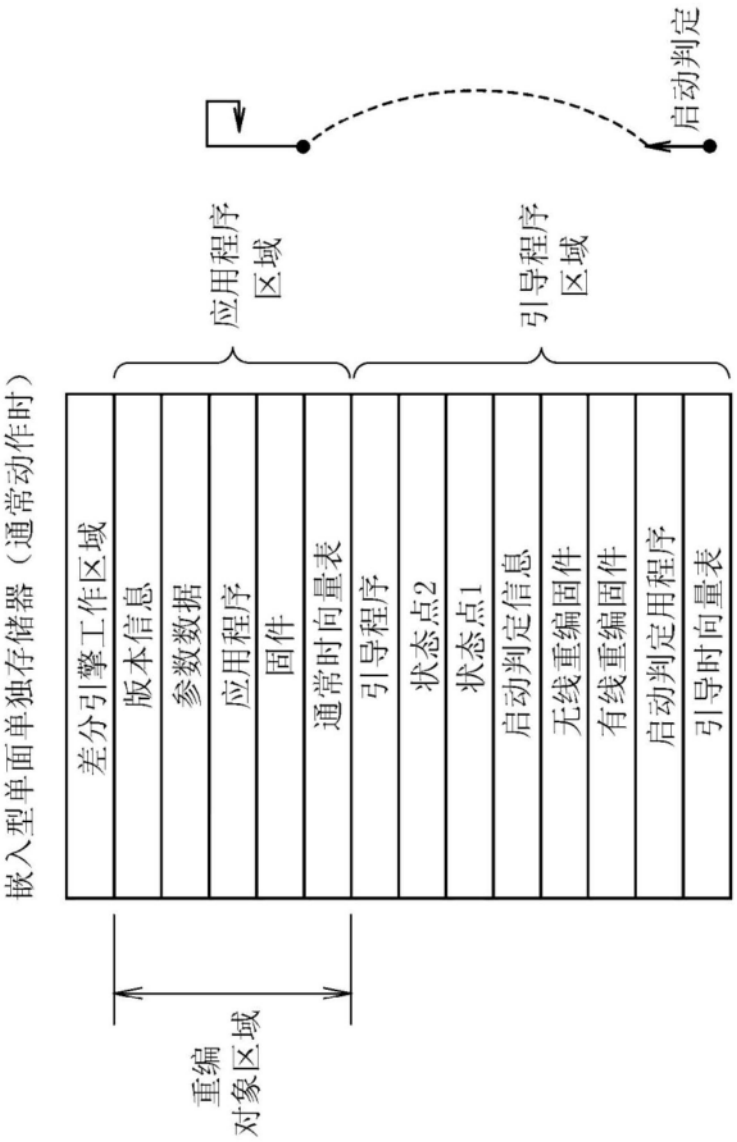

嵌入型单面单独存储器（通常动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表
引导程序
状态点2
状态点1
启动判定信息
无线重编固件
有线重编固件
启动判定用程序
引导时向量表
应用程序区域
引导程序区域
启动判定
重编对象区域

图11

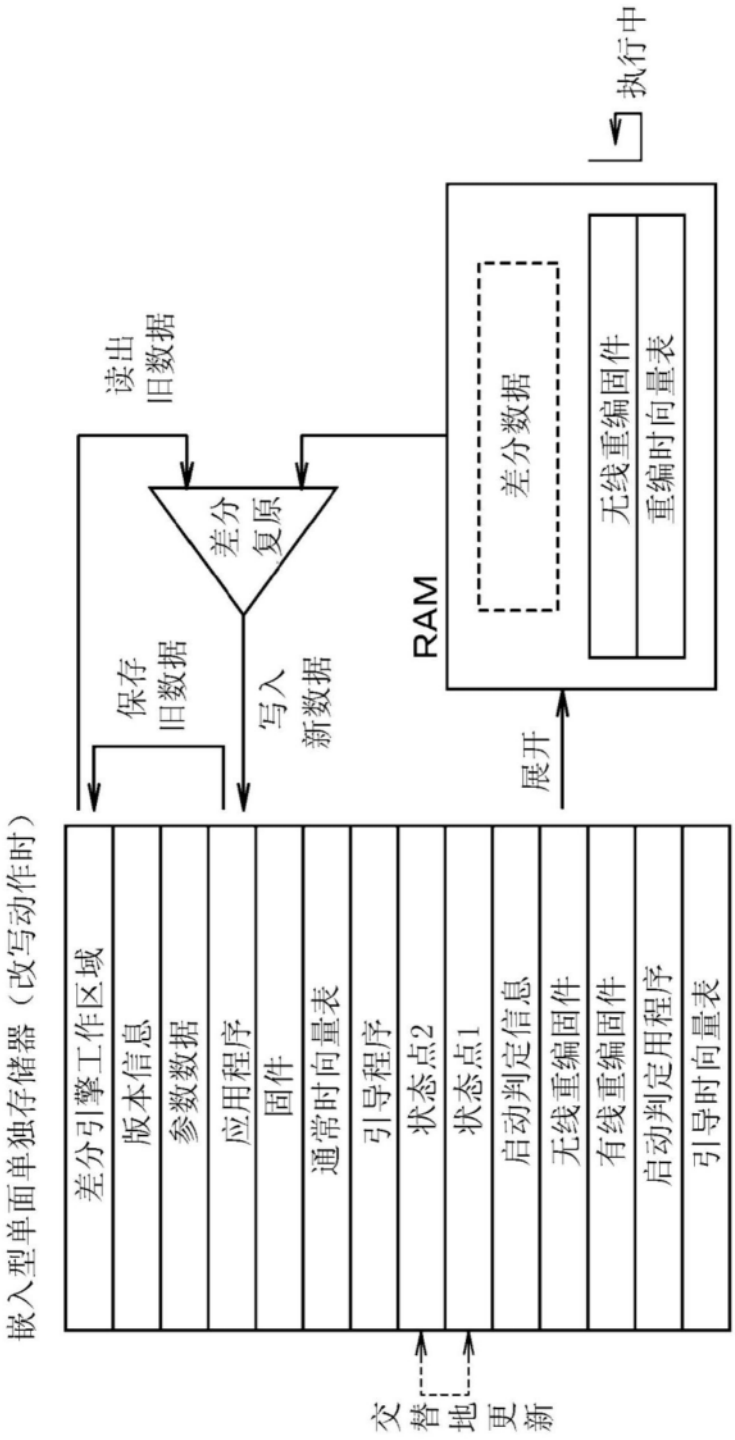

嵌入型单面单独存储器（改写动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表
引导程序
状态点2
状态点1
启动判定信息
无线重编固件
有线重编固件
启动判定用程序
引导时向量表
交替地更新
保存旧数据
读出旧数据
差分复原
写入新数据
展开
RAM
差分数据
无线重编固件
重编时向量表
执行中

图12

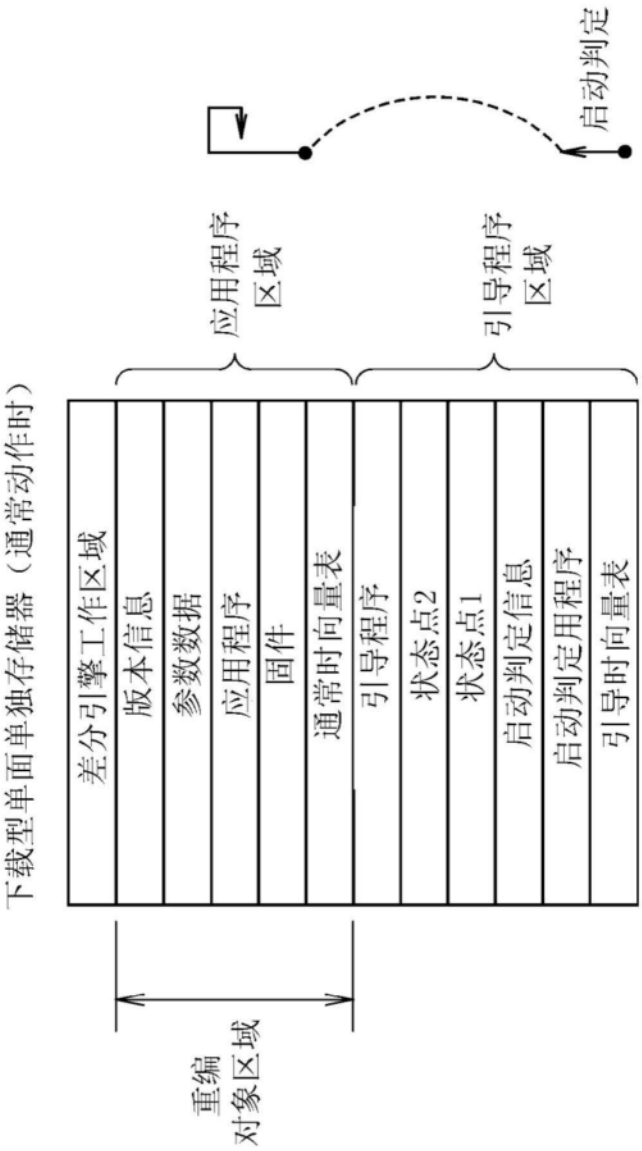

下载型单面单独存储器（通常动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表
引导程序
状态点2
状态点1
启动判定信息
启动判定用程序
引导时向量表
应用程序区域
引导程序区域
启动判定
重编对象区域

图13

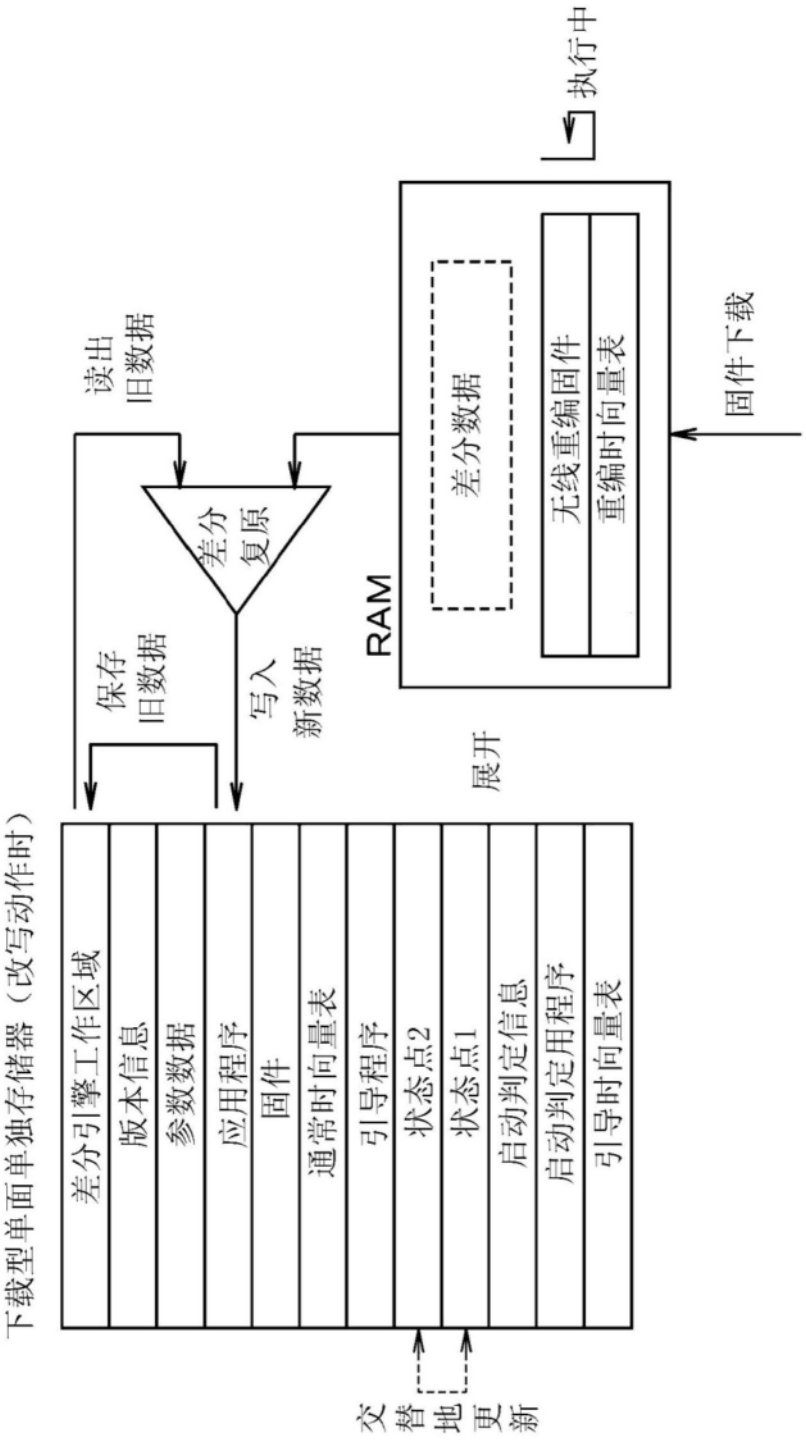

执行中
读出
旧数据
差分
复原
保存
旧数据
写入
新数据
RAM
差分数据
无线重编固件
重编时向量表
固件下载
展开
下载型单面单独存储器（改写动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表
引导程序
状态点2
状态点1
启动判定信息
启动判定用程序
引导时向量表
交替地更新

图14

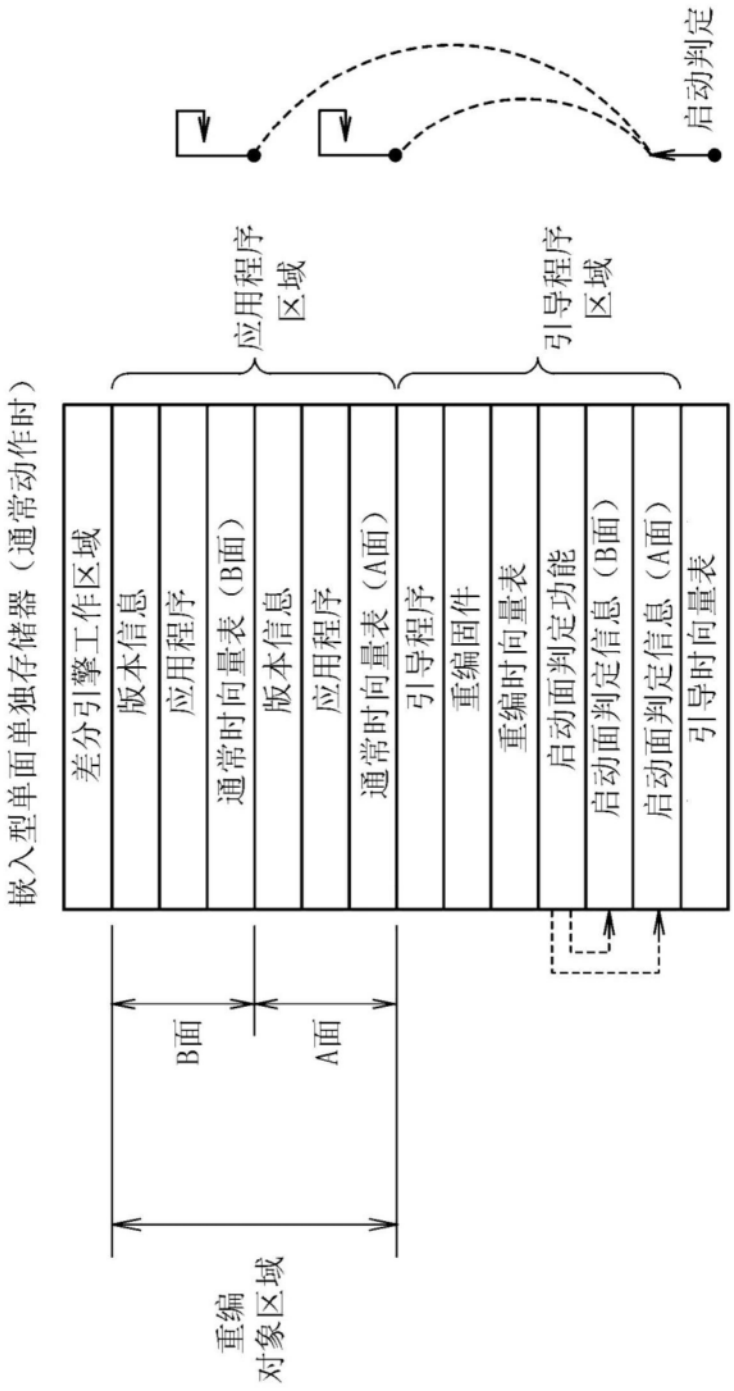

启动判定
应用程序区域
引导程序区域
嵌入型单面单独存储器（通常动作时）
差分引擎工作区域
版本信息
应用程序
通常时向量表（B面）
版本信息
应用程序
通常时向量表（A面）
引导程序
重编固件
重编时向量表
启动面判定功能
启动面判定信息（B面）
启动面判定信息（A面）
引导时向量表
B面
A面
重编对象区域

图15

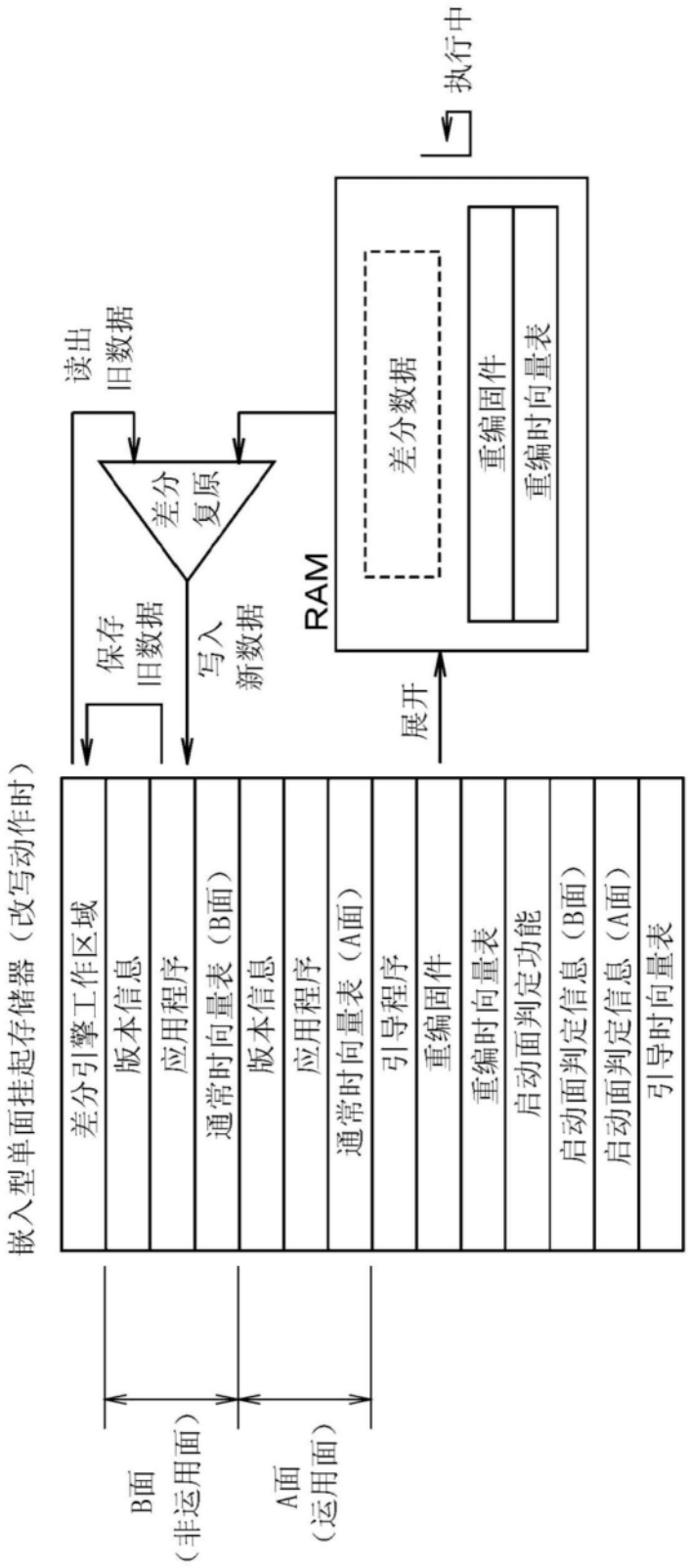

嵌入型单面挂起存储器（改写动作时）
差分引擎工作区域
版本信息
应用程序
通常时向量表（B面）
版本信息
应用程序
通常时向量表（A面）
引导程序
重编固件
重编时向量表
启动面判定功能
启动面判定信息（B面）
启动面判定信息（A面）
引导时向量表
B面
（非运用面）
A面
（运用面）
保存
旧数据
写入
新数据
读出
旧数据
差分
复原
展开
RAM
差分数据
重编固件
重编时向量表
执行中

图16

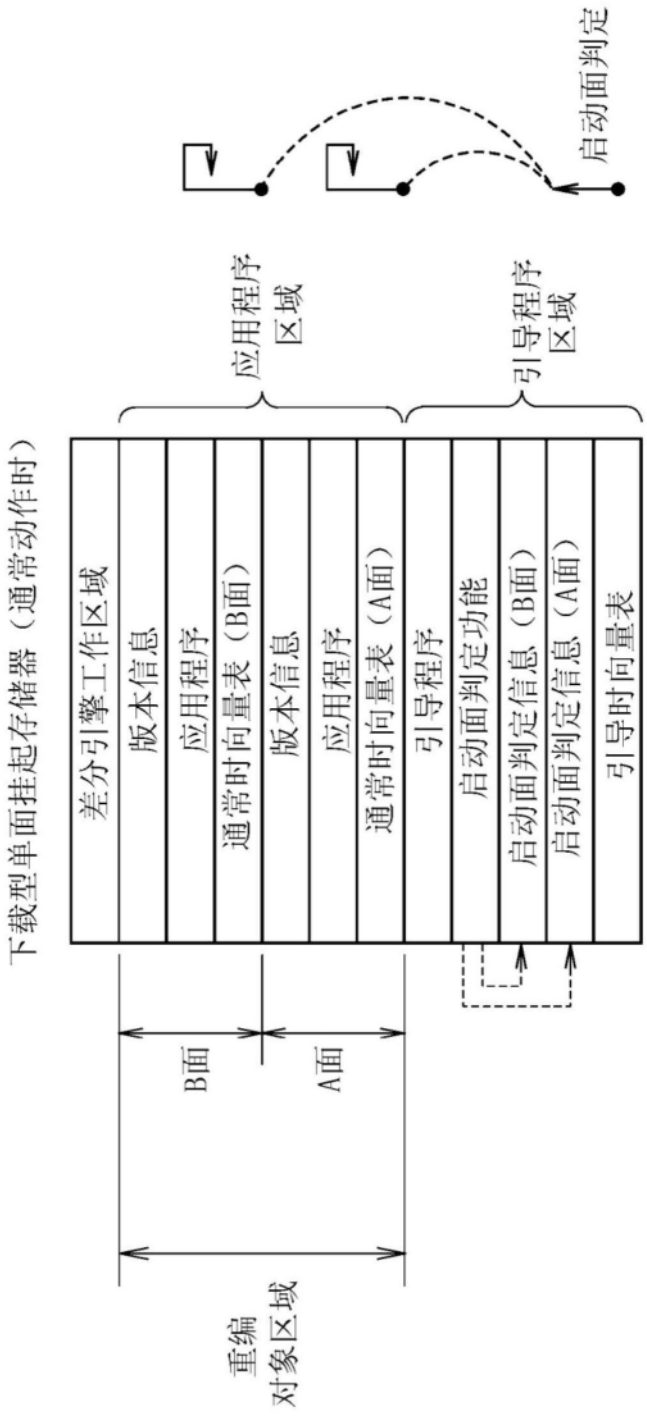

启动面判定
应用程序区域
引导程序区域
下载型单面挂起存储器（通常动作时）
差分引擎工作区域
版本信息
应用程序
通常时向量表（B面）
版本信息
应用程序
通常时向量表（A面）
引导程序
启动面判定功能
启动面判定信息（B面）
启动面判定信息（A面）
引导时向量表
B面
A面
重编对象区域

图17

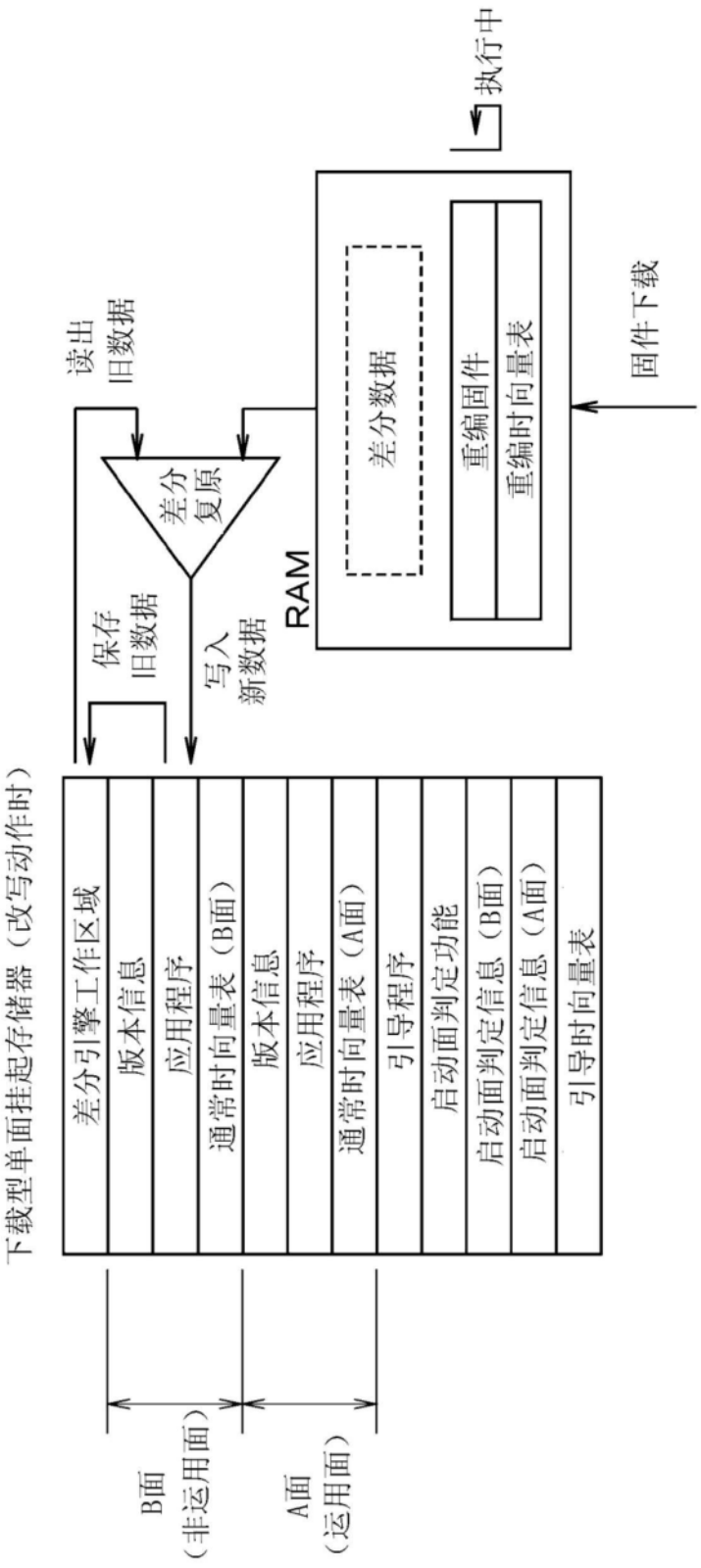

执行中
读出
旧数据
差分
复原
保存
旧数据
写入
新数据
RAM
差分数据
重编固件
重编时向量表
固件下载
下载型单面挂起存储器（改写动作时）
差分引擎工作区域
版本信息
应用程序
通常时向量表（B面）
版本信息
应用程序
通常时向量表（A面）
引导程序
启动面判定功能
启动面判定信息（B面）
启动面判定信息（A面）
引导时向量表
B面
（非运用面）
A面
（运用面）

图18

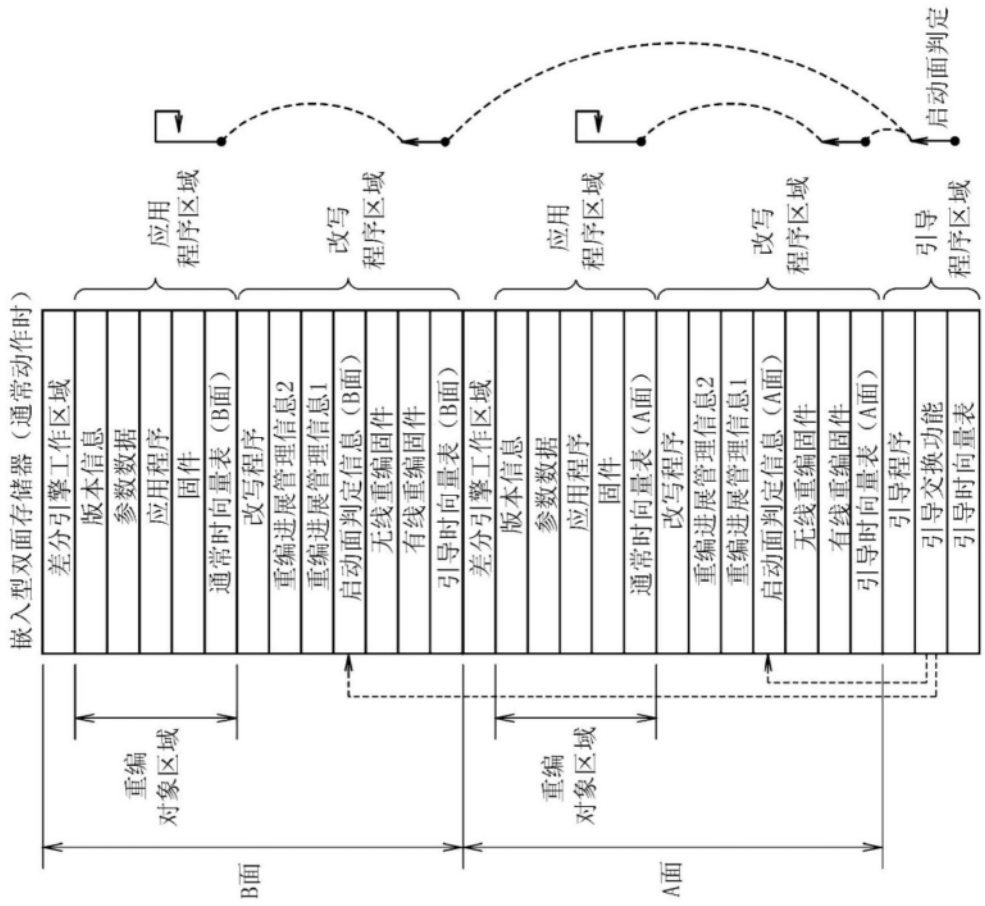

嵌入型双面存储器（通常动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（B面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（B面）
无线重编固件
有线重编固件
引导时向量表（B面）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（A面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（A面）
无线重编固件
有线重编固件
引导时向量表（A面）
引导程序
引导交换功能
引导时向量表
应用程序区域
改写程序区域
应用程序区域
改写程序区域
引导程序区域
启动面判定
重编对象区域
重编对象区域
B面
A面

图19

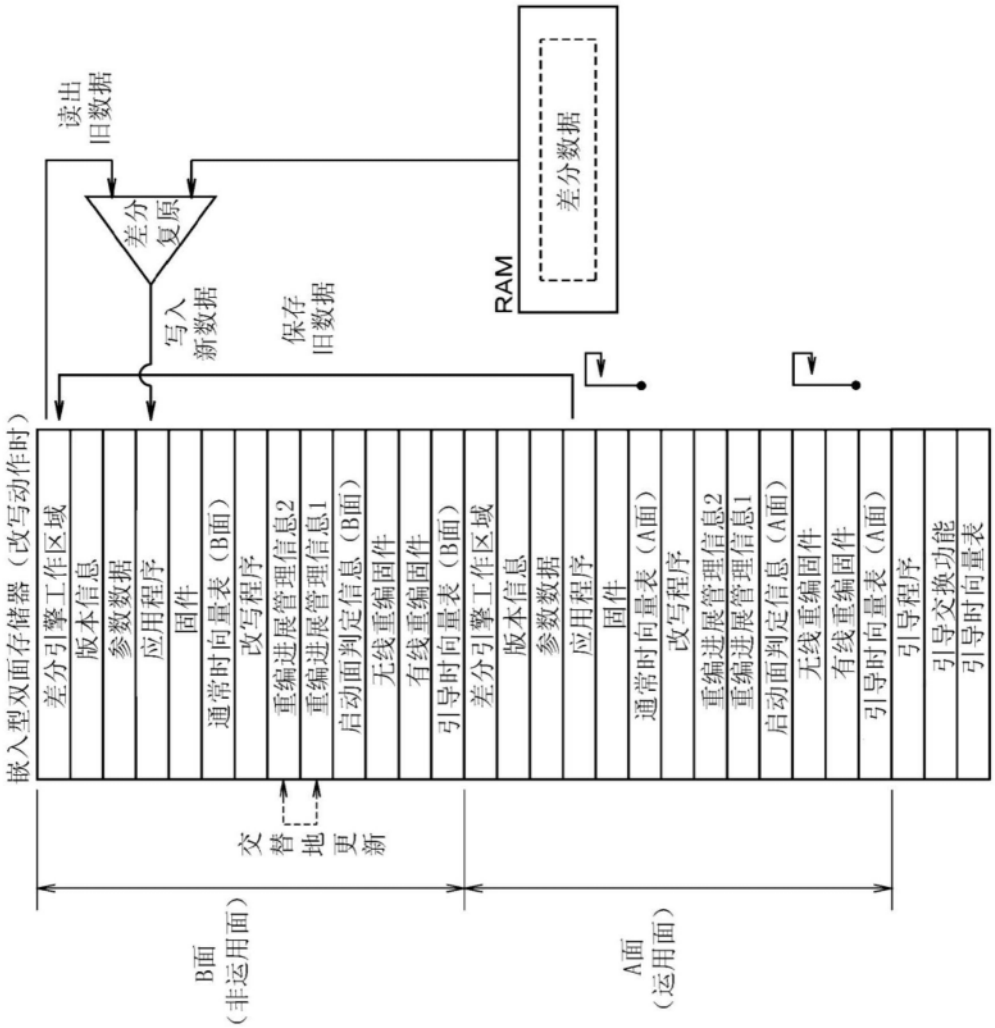

读出
旧数据
差分
复原
写入
新数据
保存
旧数据
RAM
差分数据
嵌入型双面存储器（改写动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（B面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（B面）
无线重编固件
有线重编固件
引导时向量表（B面）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（A面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（A面）
无线重编固件
有线重编固件
引导时向量表（A面）
引导程序
引导交换功能
引导时向量表
交替地更新
B面
（非运用面）
A面
（运用面）

图20

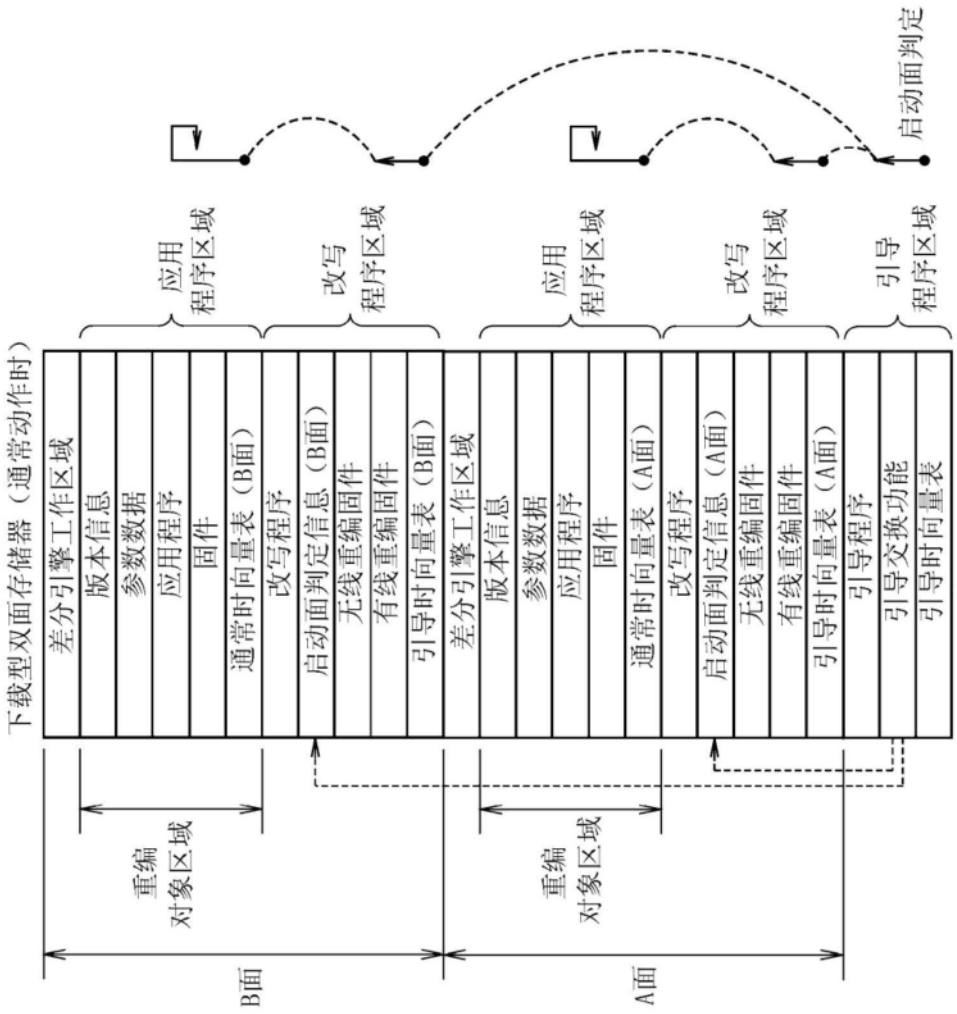

下载型双面存储器（通常动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（B面）
改写程序
启动面判定信息（B面）
无线重编固件
有线重编固件
引导时向量表（B面）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（A面）
改写程序
启动面判定信息（A面）
无线重编固件
有线重编固件
引导时向量表（A面）
引导程序
引导交换功能
引导时向量表
应用程序区域
改写程序区域
应用程序区域
改写程序区域
引导程序区域
启动面判定
重编对象区域
重编对象区域
B面
A面

图21

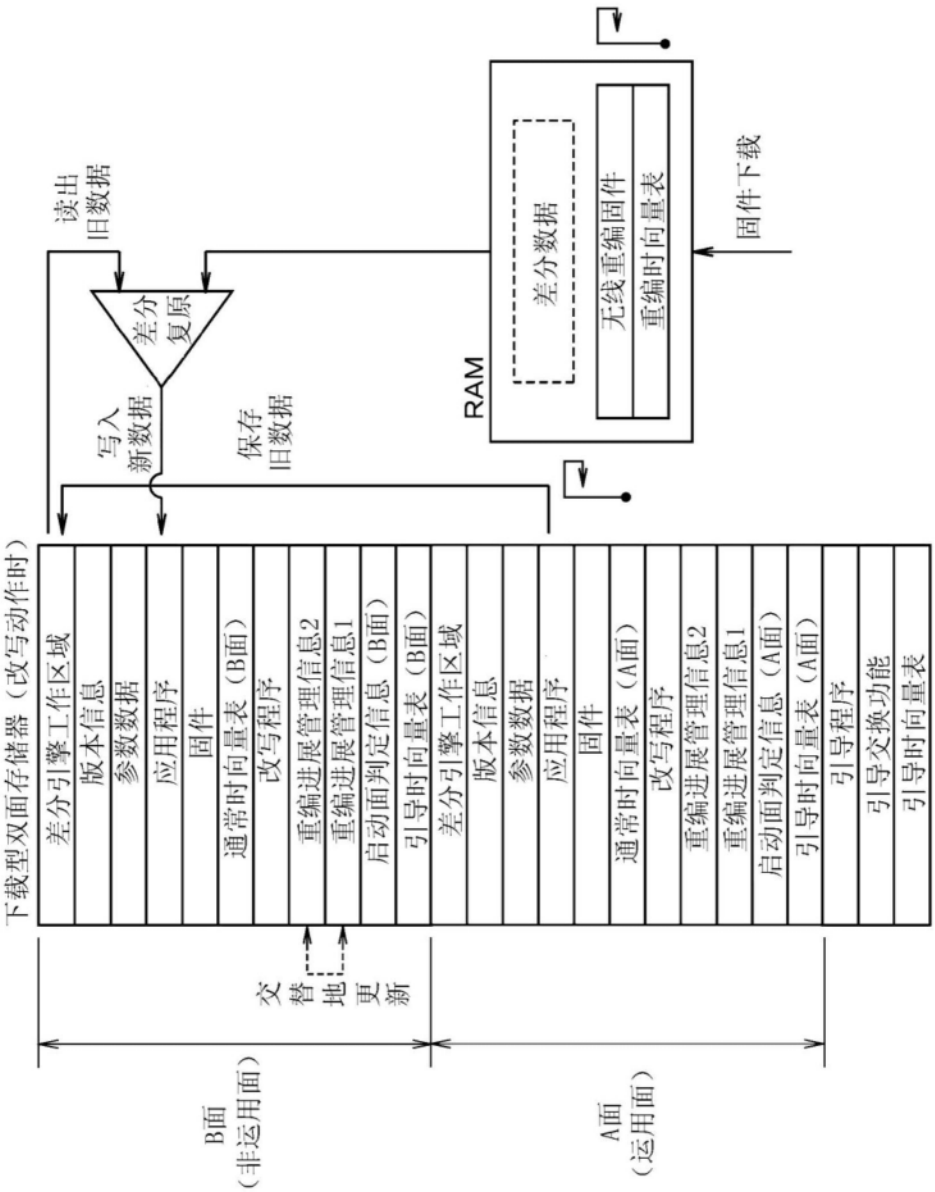

下载型双面存储器（改写动作时）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（B面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（B面）
引导时向量表（B面）
差分引擎工作区域
版本信息
参数数据
应用程序
固件
通常时向量表（A面）
改写程序
重编进展管理信息2
重编进展管理信息1
启动面判定信息（A面）
引导时向量表（A面）
引导程序
引导交换功能
引导时向量表
交替地更新
B面（非运用面）
A面（运用面）
读出旧数据
差分复原
写入新数据
保存旧数据
RAM
差分数据
无线重编固件
重编时向量表
固件下载

图22

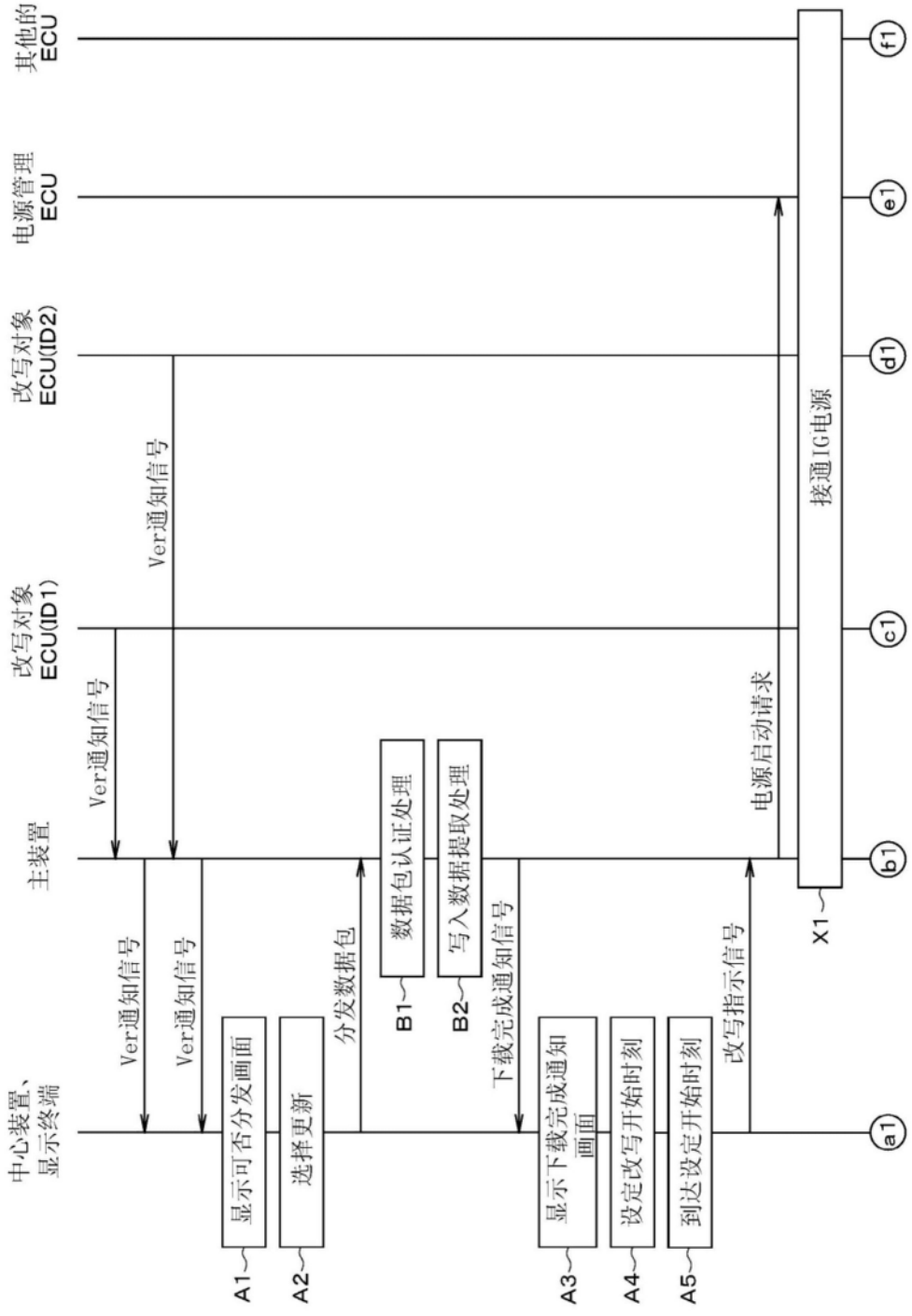

中心装置、显示终端
主装置
改写对象ECU(ID1)
改写对象ECU(ID2)
电源管理ECU
其他的ECU
Ver通知信号
Ver通知信号
Ver通知信号
显示可否分发画面
选择更新
分发数据包
数据包认证处理
写入数据提取处理
下载完成通知信号
显示下载完成通知画面
设定改写开始时刻
到达设定开始时刻
改写指示信号
电源启动请求
接通IG电源
A1
A2
B1
B2
A3
A4
A5
X1
a1
b1
c1
d1
e1
f1

图23

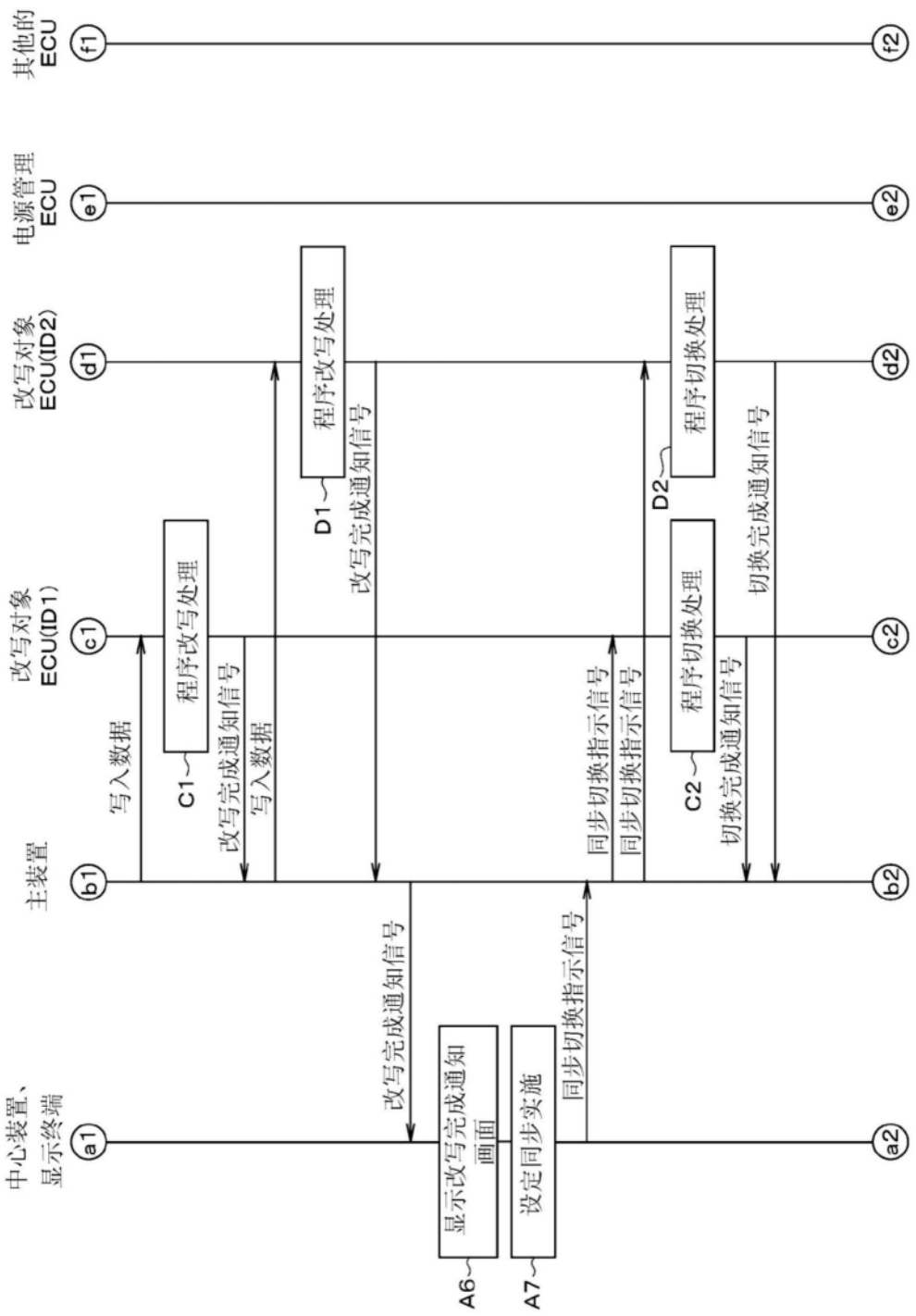

其他的ECU
电源管理ECU
改写对象ECU(ID2)
改写对象ECU(ID1)
主装置
中心装置、显示终端
f1
f2
e1
e2
d1
d2
c1
c2
b1
b2
a1
a2
写入数据
C1
程序改写处理
改写完成通知信号
写入数据
D1
程序改写处理
改写完成通知信号
同步切换指示信号
同步切换指示信号
D2
程序切换处理
C2
程序切换处理
切换完成通知信号
切换完成通知信号
改写完成通知信号
显示改写完成通知画面
A6
设定同步实施
A7
同步切换指示信号

图24

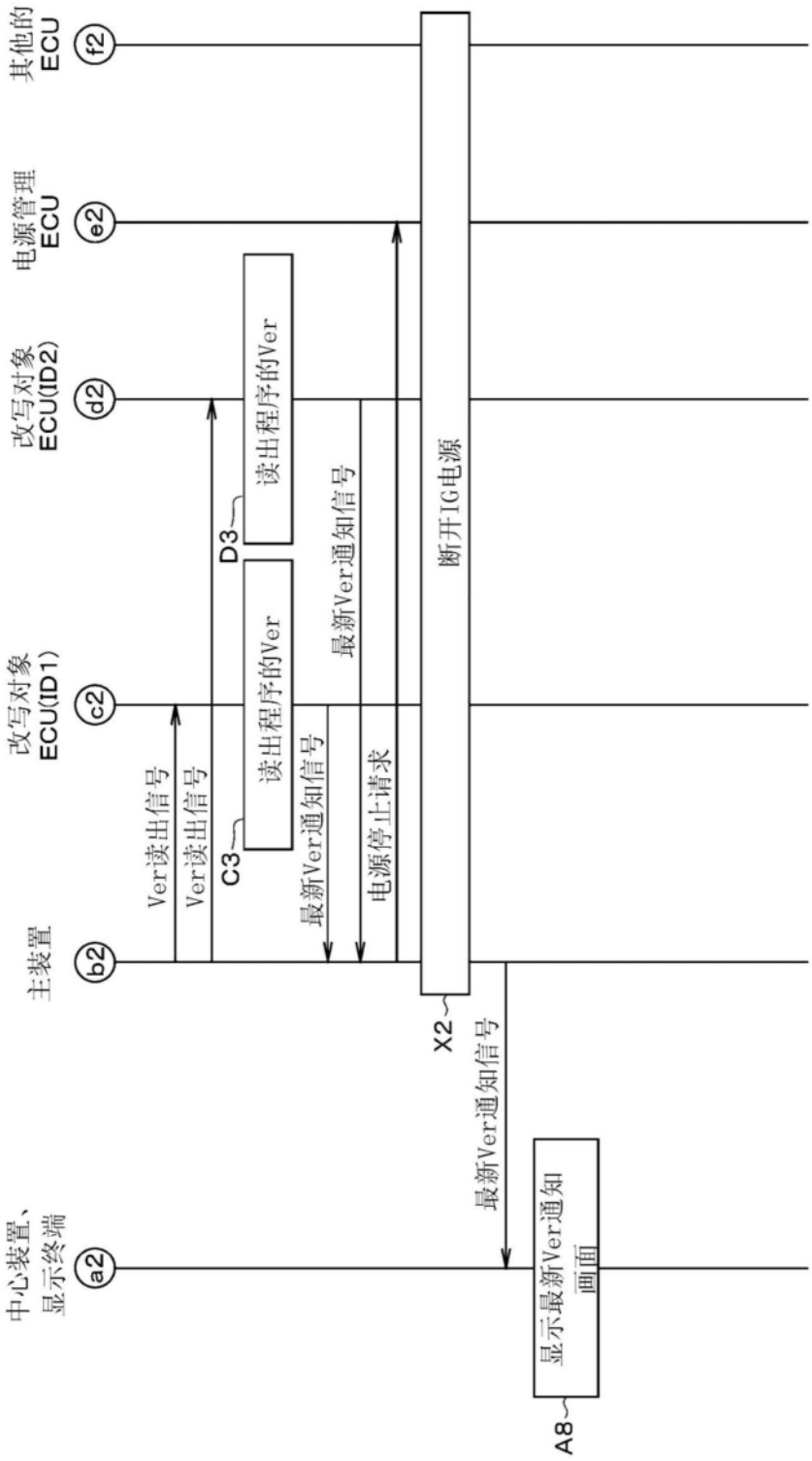

中心装置、显示终端
a2
主装置
b2
改写对象ECU(ID1)
c2
改写对象ECU(ID2)
d2
电源管理ECU
e2
其他的ECU
f2
Ver读出信号
Ver读出信号
C3
读出程序的Ver
最新Ver通知信号
电源停止请求
D3
读出程序的Ver
最新Ver通知信号
断开IG电源
X2
最新Ver通知信号
显示最新Ver通知画面
A8

图25

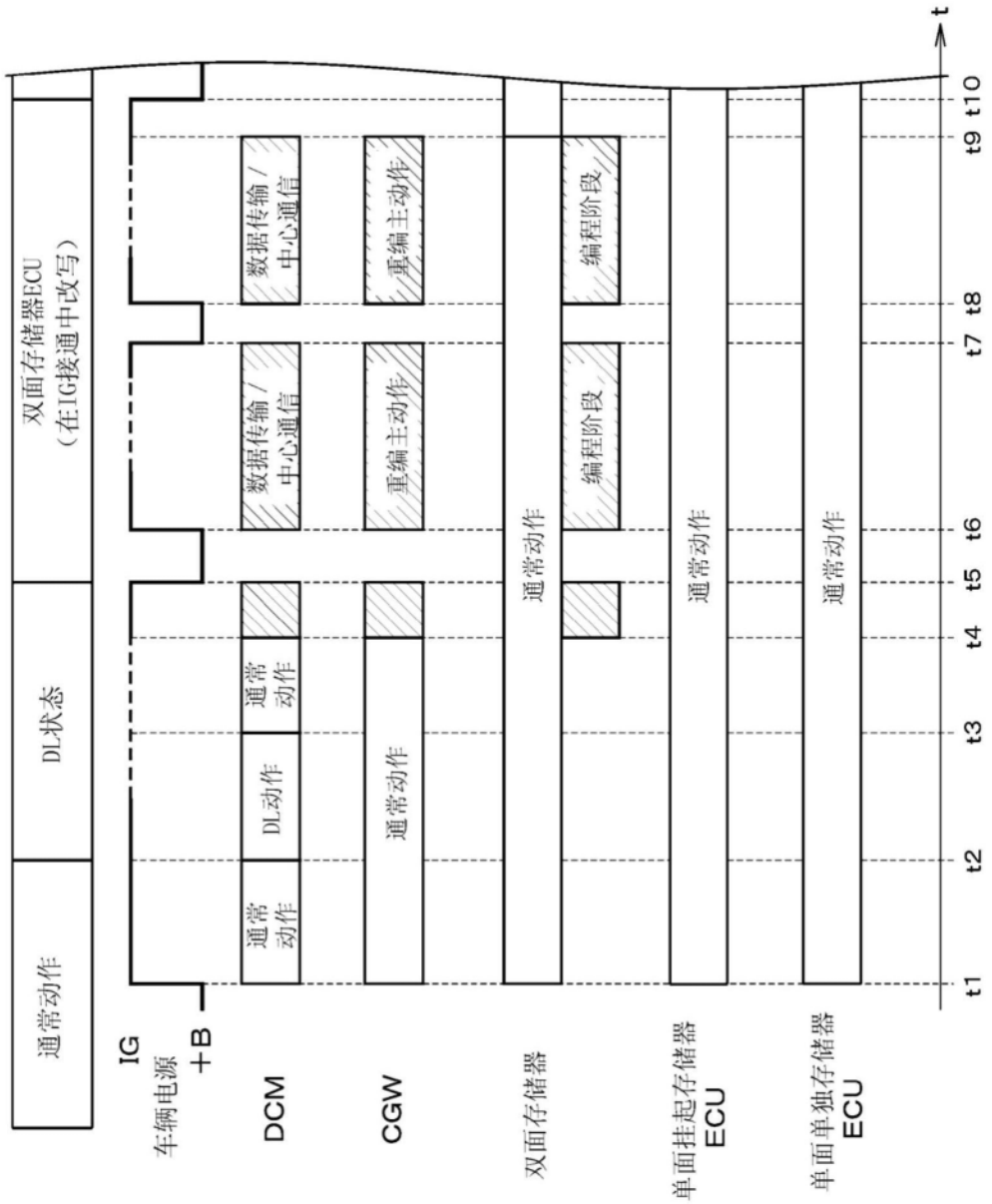

双面存储器ECU
（在IG接通中改写）
DL状态
通常动作
IG
车辆电源
+B
DCM
通常动作
DL动作
通常动作
数据传输/中心通信
CGW
通常动作
重编主动作
双面存储器
通常动作
编程阶段
单面挂起存储器ECU
通常动作
单面单独存储器ECU
通常动作
t
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10

图26

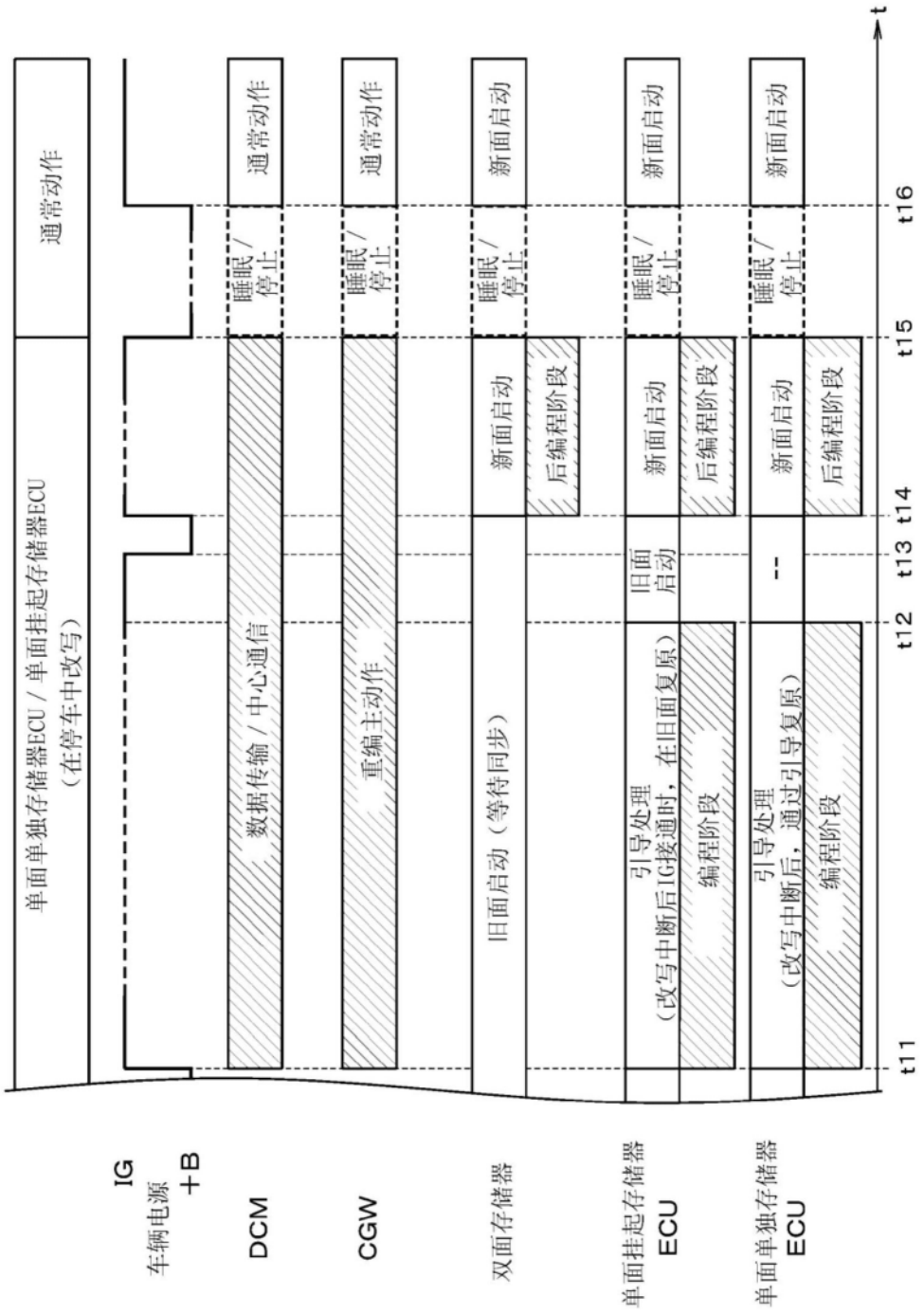

IG
车辆电源
+B
DCM
CGW
双面存储器
单面挂起存储器
ECU
单面单独存储器
ECU
t
t11
t12
t13
t14
t15
t16
单面单独存储器ECU / 单面挂起存储器ECU
（在停车中改写）
通常动作
睡眠 / 停止
通常动作
数据传输 / 中心通信
睡眠 / 停止
通常动作
重编主动作
睡眠 / 停止
新面启动
旧面启动（等待同步）
后编程阶段
睡眠 / 停止
新面启动
引导处理
（改写中断后IG接通时，在旧面复原）
旧面启动
编程阶段
后编程阶段
睡眠 / 停止
新面启动
引导处理
（改写中断后，通过引导复原）
--
编程阶段
后编程阶段

图27

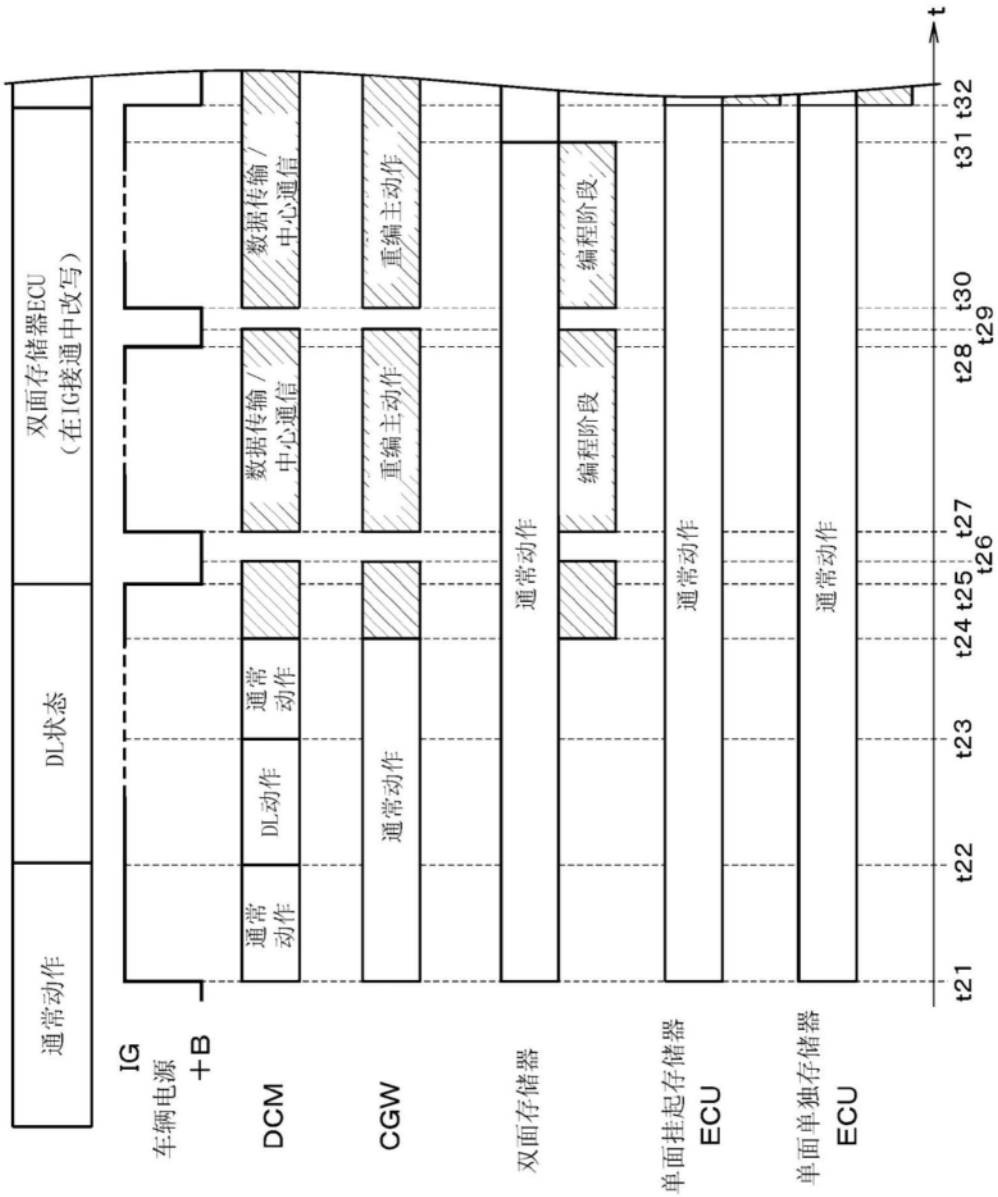

通常动作
DL状态
双面存储器ECU
（在IG接通中改写）
IG
车辆电源
+B
DCM
通常动作
DL动作
通常动作
数据传输/中心通信
CGW
通常动作
重编主动作
数据传输/中心通信
双面存储器
通常动作
编程阶段
重编主动作
单面挂起存储器ECU
通常动作
编程阶段
单面单独存储器ECU
通常动作
t
t21
t22
t23
t24
t25
t26
t27
t28
t29
t30
t31
t32

图28

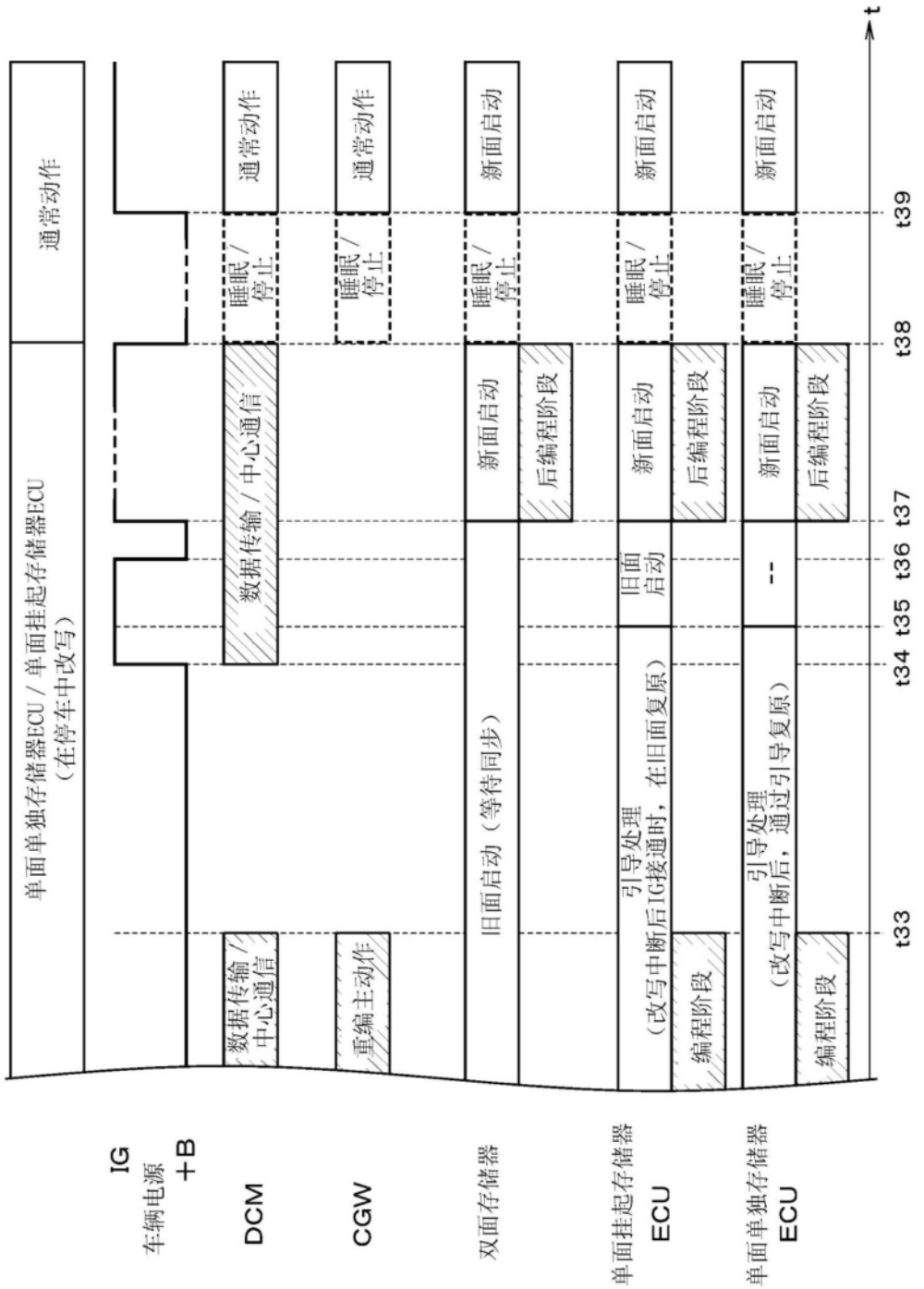

IG
车辆电源
+B
DCM
CGW
双面存储器
单面挂起存储器
ECU
单面单独存储器
ECU
单面单独存储器ECU / 单面挂起存储器ECU
（在停车中改写）
通常动作
数据传输 /
中心通信
睡眠 /
停止
通常动作
重编主动作
睡眠 /
停止
通常动作
旧面启动（等待同步）
新面启动
后编程阶段
睡眠 /
停止
新面启动
引导处理
（改写中断后IG接通时，在旧面复原）
编程阶段
旧面
启动
新面启动
后编程阶段
睡眠 /
停止
新面启动
引导处理
（改写中断后，通过引导复原）
编程阶段
--
新面启动
后编程阶段
t
t33
t34
t35
t36
t37
t38
t39

图29

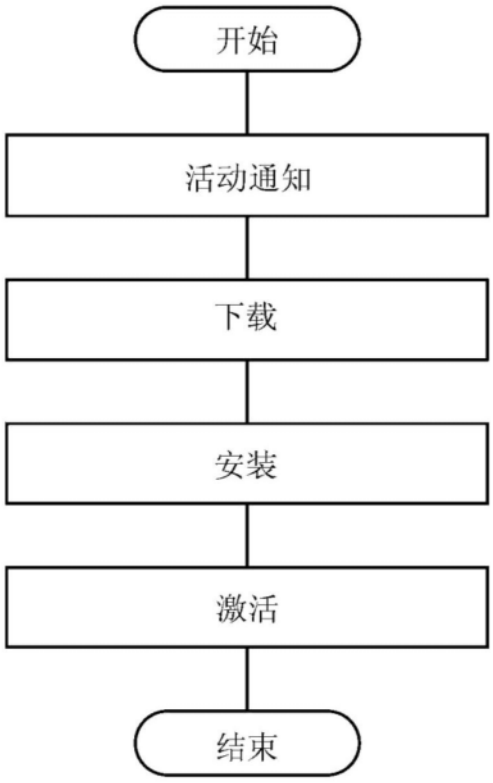

开始
活动通知
下载
安装
激活
结束

图30

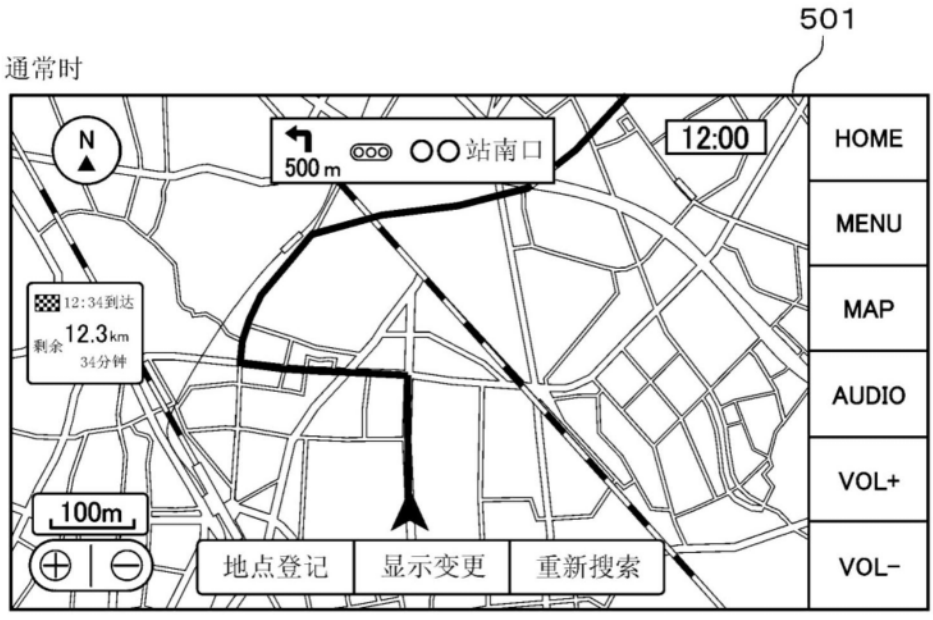

501
通常时
N
500 m
〇〇站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34到达
剩余 12.3km
34分钟
100m
地点登记
显示变更
重新搜索

图31

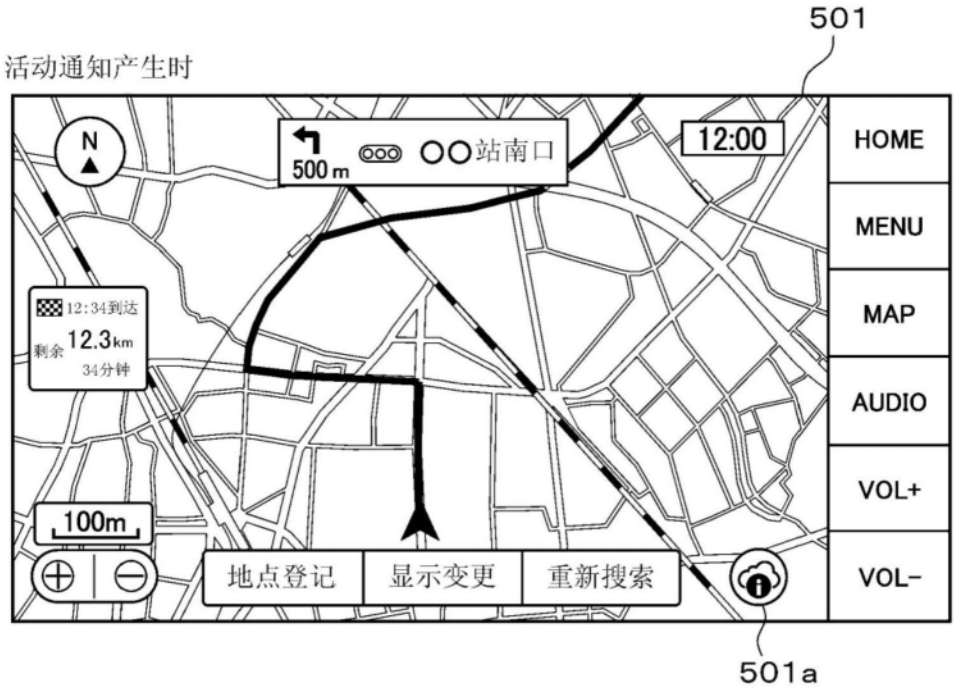

活动通知产生时
501
N
500 m
〇〇站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34到达
剩余 12.3km
34分钟
100m
地点登记
显示变更
重新搜索
501a

图32

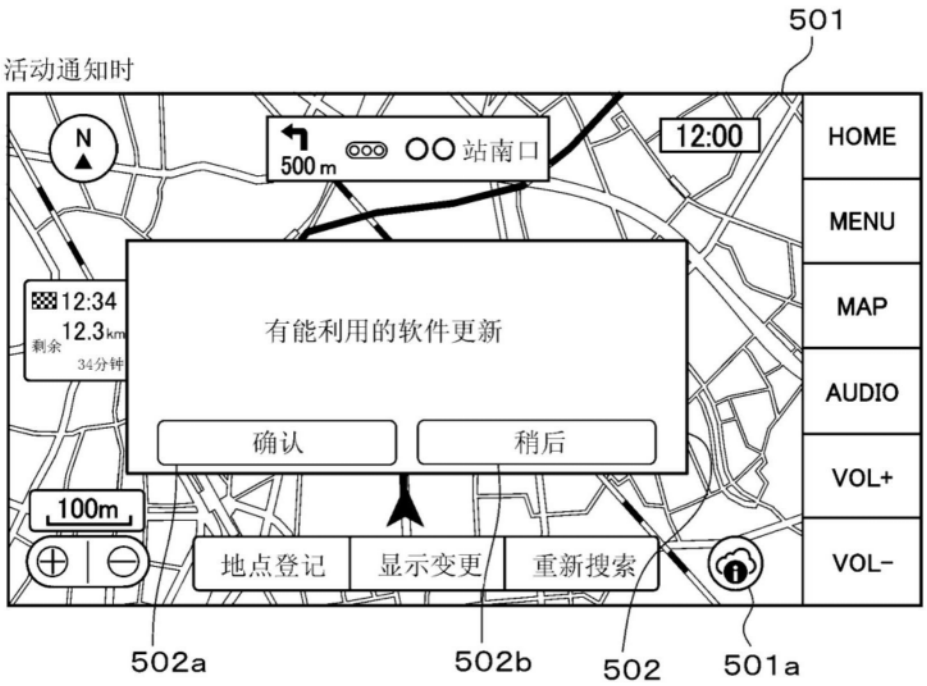

活动通知时
501
N
500 m
〇〇站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
剩余 12.3km
34分钟
有能利用的软件更新
确认
稍后
100m
地点登记
显示变更
重新搜索
502a
502b
502
501a

图33

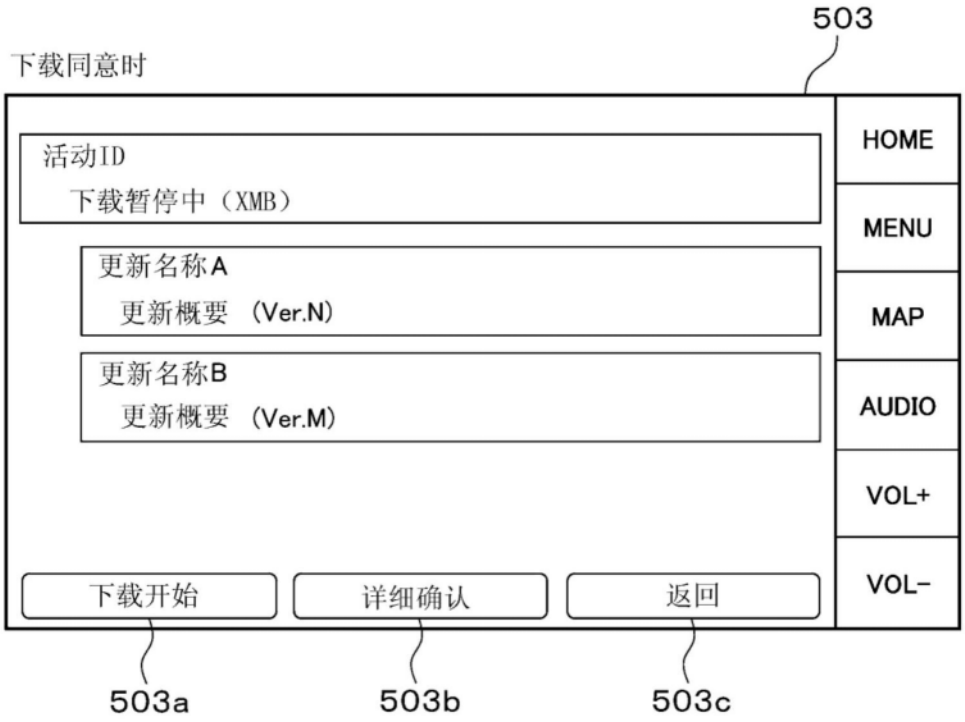

503
下载同意时
活动ID
下载暂停中（XMB）
更新名称A
更新概要 (Ver.N)
更新名称B
更新概要 (Ver.M)
HOME
MENU
MAP
AUDIO
VOL+
VOL-
下载开始
详细确认
返回
503a
503b
503c

图34

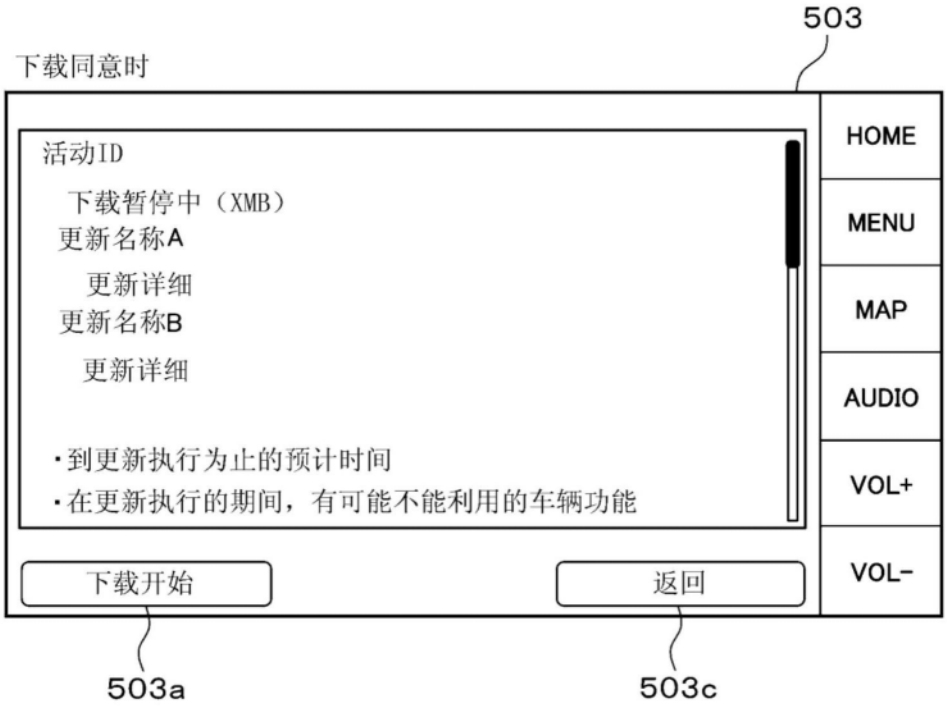

503
下载同意时
活动ID
下载暂停中（XMB）
更新名称A
更新详细
更新名称B
更新详细
·到更新执行为止的预计时间
·在更新执行的期间，有可能不能利用的车辆功能
HOME
MENU
MAP
AUDIO
VOL+
VOL-
下载开始
返回
503a
503c

图35

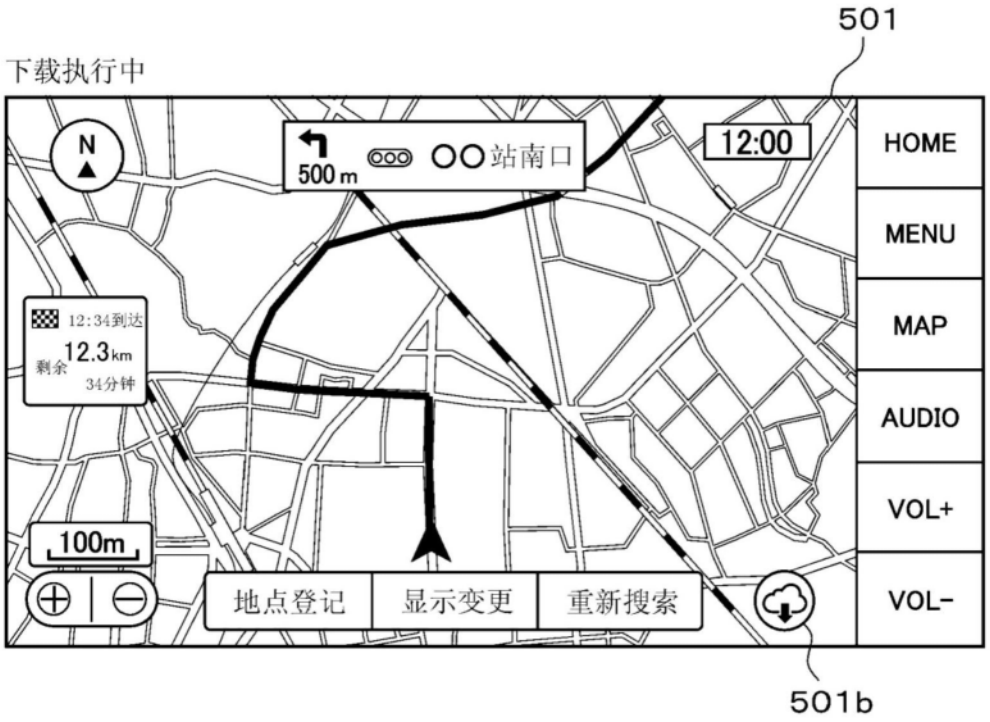

501
下载执行中
N
500 m
〇〇站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34到达
剩余 12.3km
34分钟
100m
地点登记
显示变更
重新搜索
501b

图36

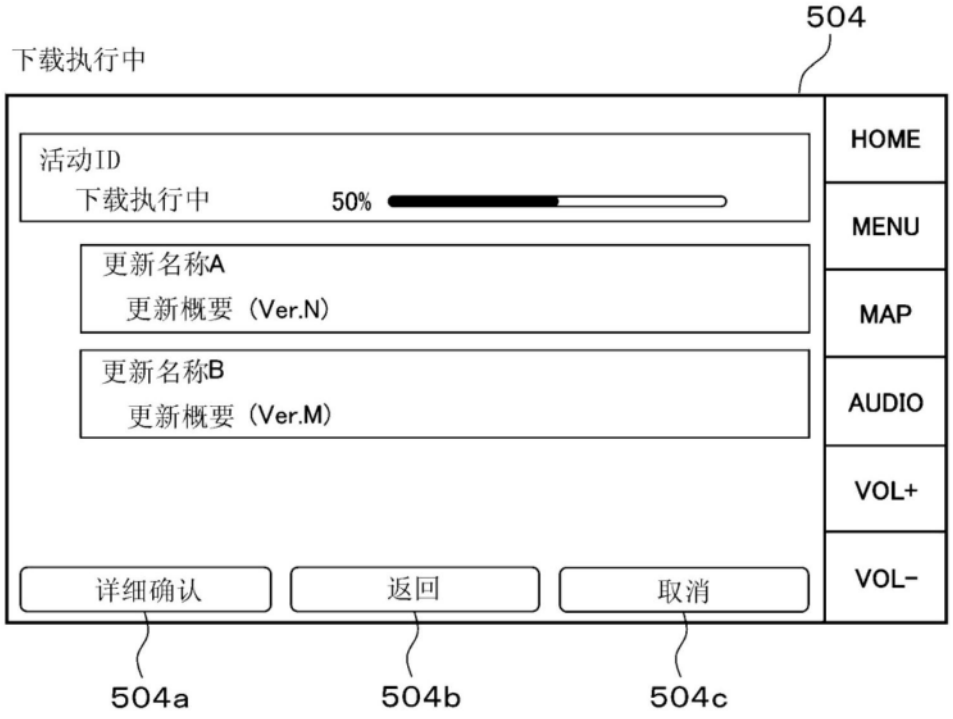

504
下载执行中
活动ID
下载执行中
50%
更新名称A
更新概要（Ver.N）
更新名称B
更新概要（Ver.M）
HOME
MENU
MAP
AUDIO
VOL+
VOL-
详细确认
返回
取消
504a
504b
504c

图37

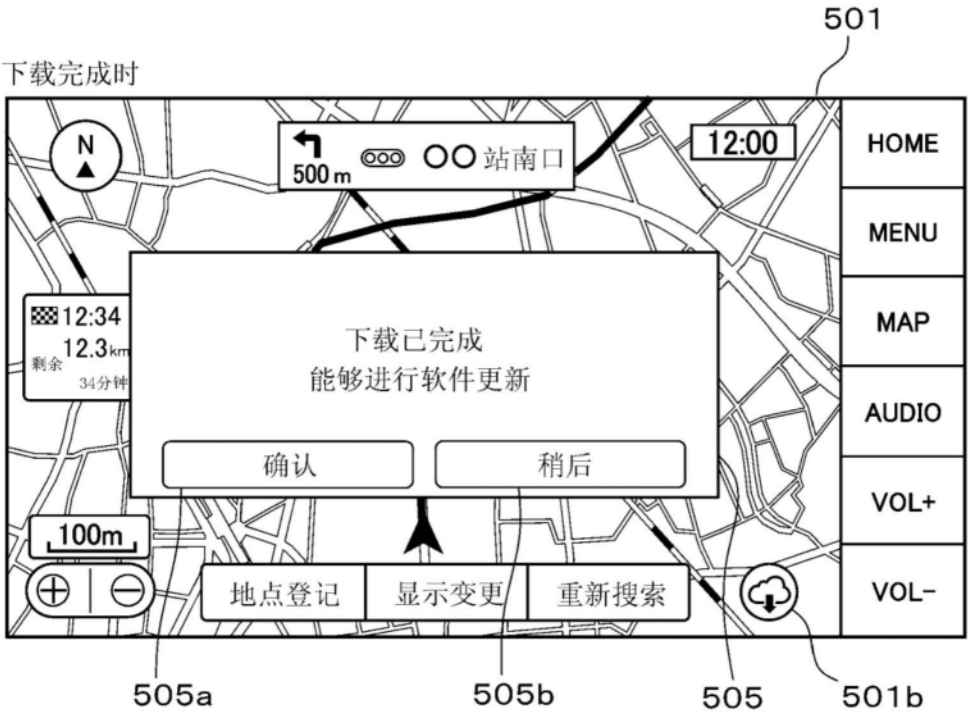

501
下载完成时
N
500 m
OO站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34
剩余
12.3km
34分钟
下载已完成
能够进行软件更新
确认
稍后
100m
地点登记
显示变更
重新搜索
505a
505b
505
501b

图38


506
安装同意时
506a
立即更新
506b
预约更新
时间表设定
00
:
00
AM
预定所需时间
约30分钟
注意事项
在更新执行的期间，有可能不能利用的车辆功能
用于车辆用户安全地执行更新而所需的指示
返回
506c
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图39

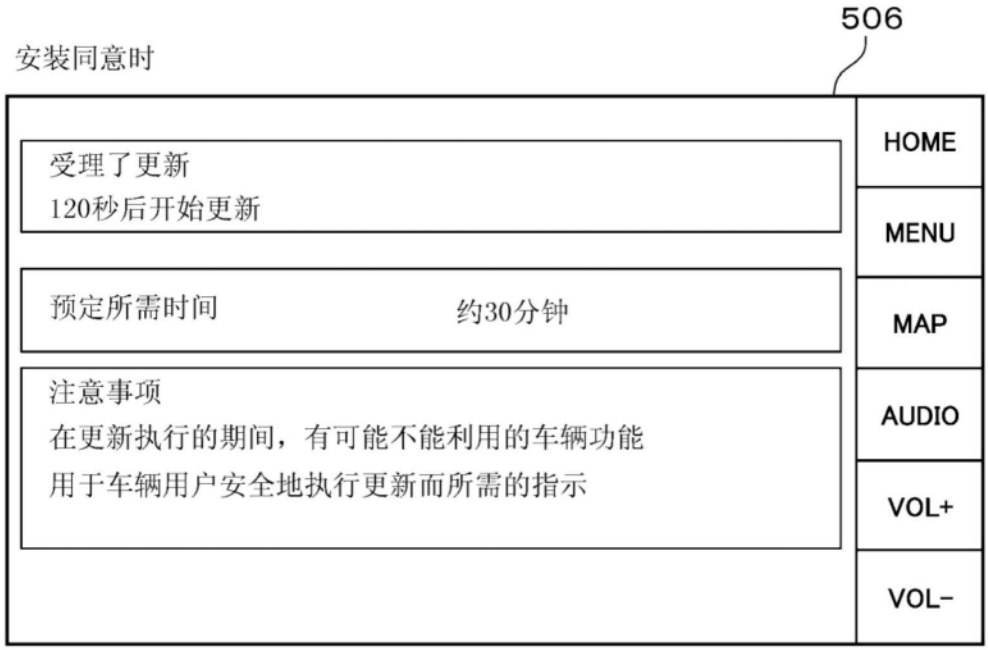

506
安装同意时
受理了更新
120秒后开始更新
预定所需时间
约30分钟
注意事项
在更新执行的期间，有可能不能利用的车辆功能
用于车辆用户安全地执行更新而所需的指示
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图40

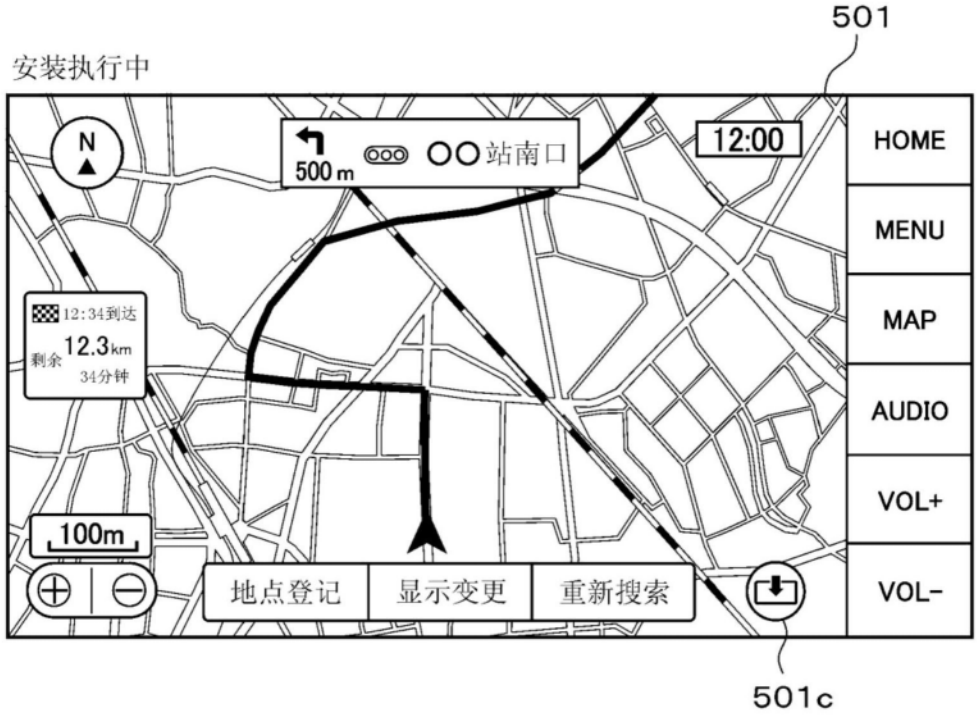

501
安装执行中
N
500 m
○○站南口
12:00
12:34到达
剩余 12.3km
34分钟
100m
地点登记
显示变更
重新搜索
HOME
MENU
MAP
AUDIO
VOL+
VOL-
501c

图41


507
安装执行中
更新执行中
预定所需时间
约30分钟
注意事项
在更新执行的期间，有可能不能利用的车辆功能
用于车辆用户安全地执行更新而所需的指示
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图42

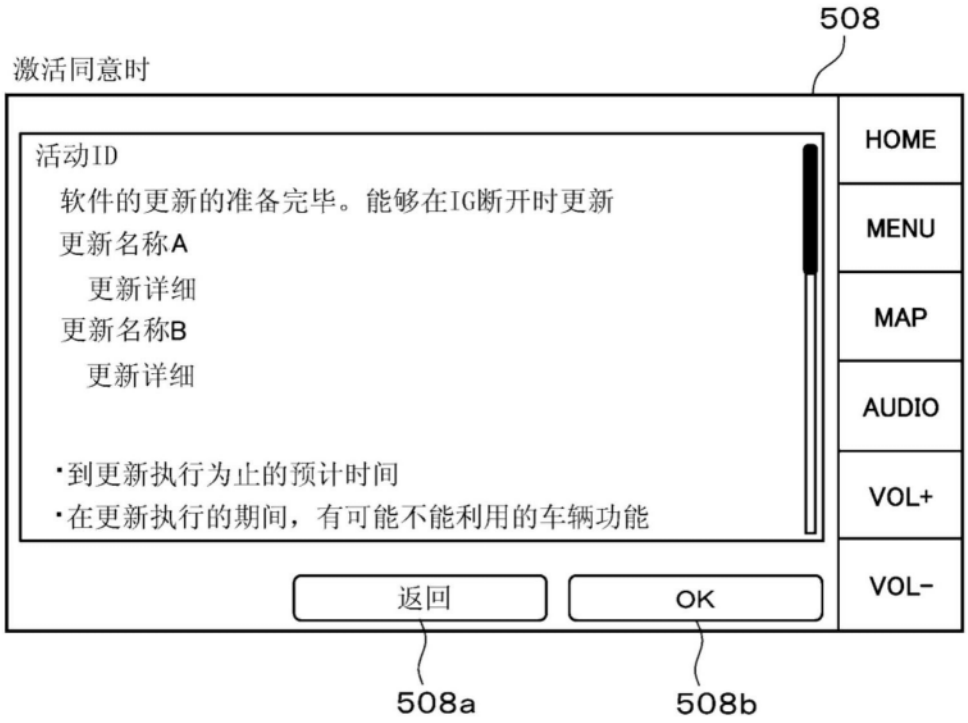

508
激活同意时
活动ID
软件的更新的准备完毕。能够在IG断开时更新
更新名称A
更新详细
更新名称B
更新详细
·到更新执行为止的预计时间
·在更新执行的期间，有可能不能利用的车辆功能
返回
OK
508a
508b
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图43

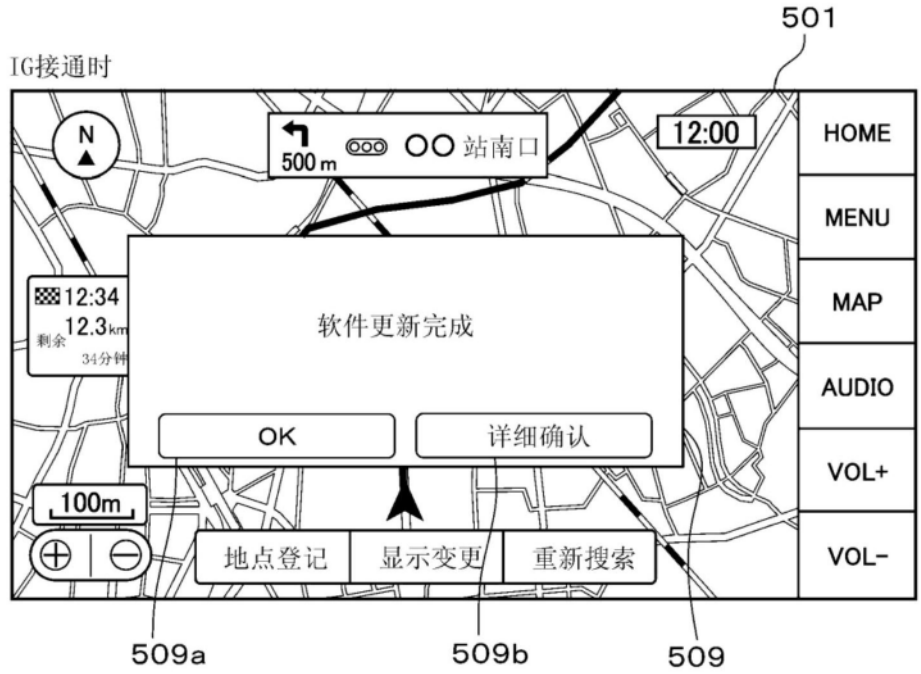

501
IG接通时
N
500 m
OO站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34
12.3km
剩余
34分钟
软件更新完成
OK
详细确认
100m
地点登记
显示变更
重新搜索
509a
509b
509

图44

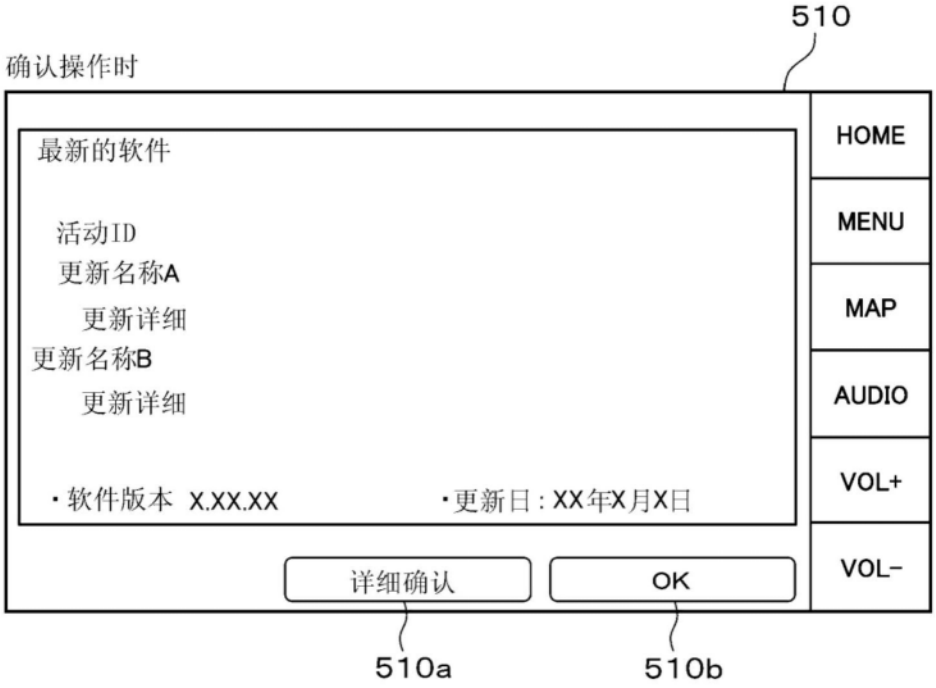

510
确认操作时
最新的软件
活动ID
更新名称A
更新详细
更新名称B
更新详细
·软件版本 X.XX.XX
·更新日：XX年X月X日
详细确认
OK
HOME
MENU
MAP
AUDIO
VOL+
VOL-
510a
510b

图45

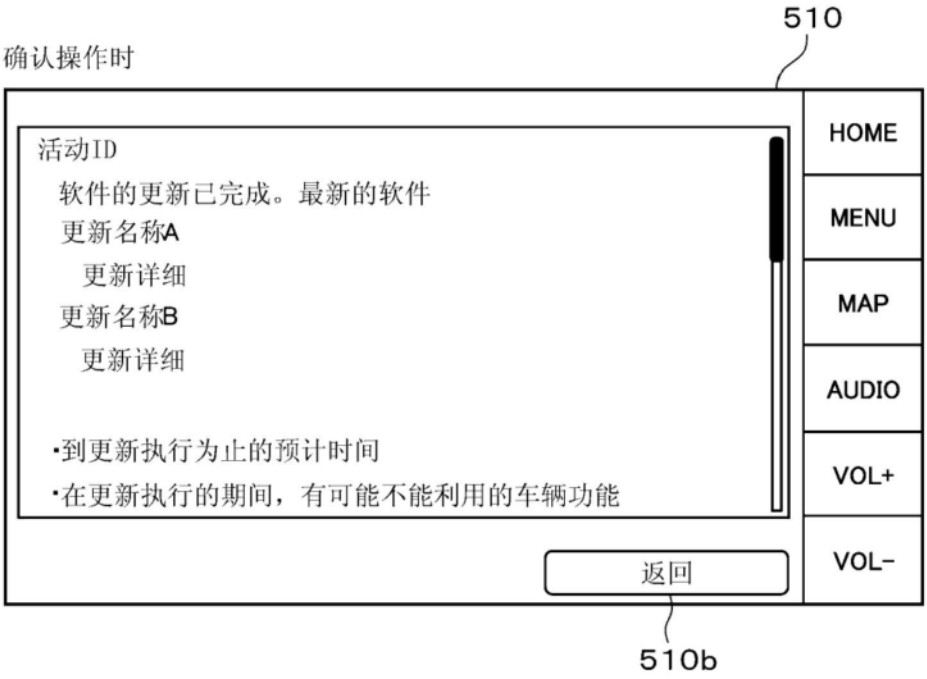

确认操作时
510
活动ID
软件的更新已完成。最新的软件
更新名称A
更新详细
更新名称B
更新详细
·到更新执行为止的预计时间
·在更新执行的期间，有可能不能利用的车辆功能
返回
510b
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图46

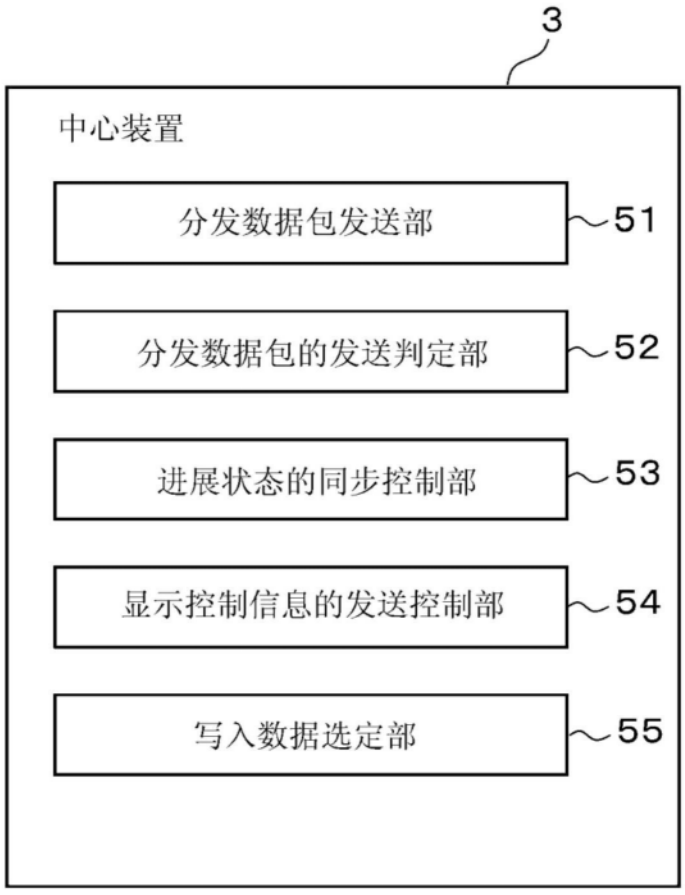

3
中心装置
分发数据包发送部
51
分发数据包的发送判定部
52
进展状态的同步控制部
53
显示控制信息的发送控制部
54
写入数据选定部
55

图47

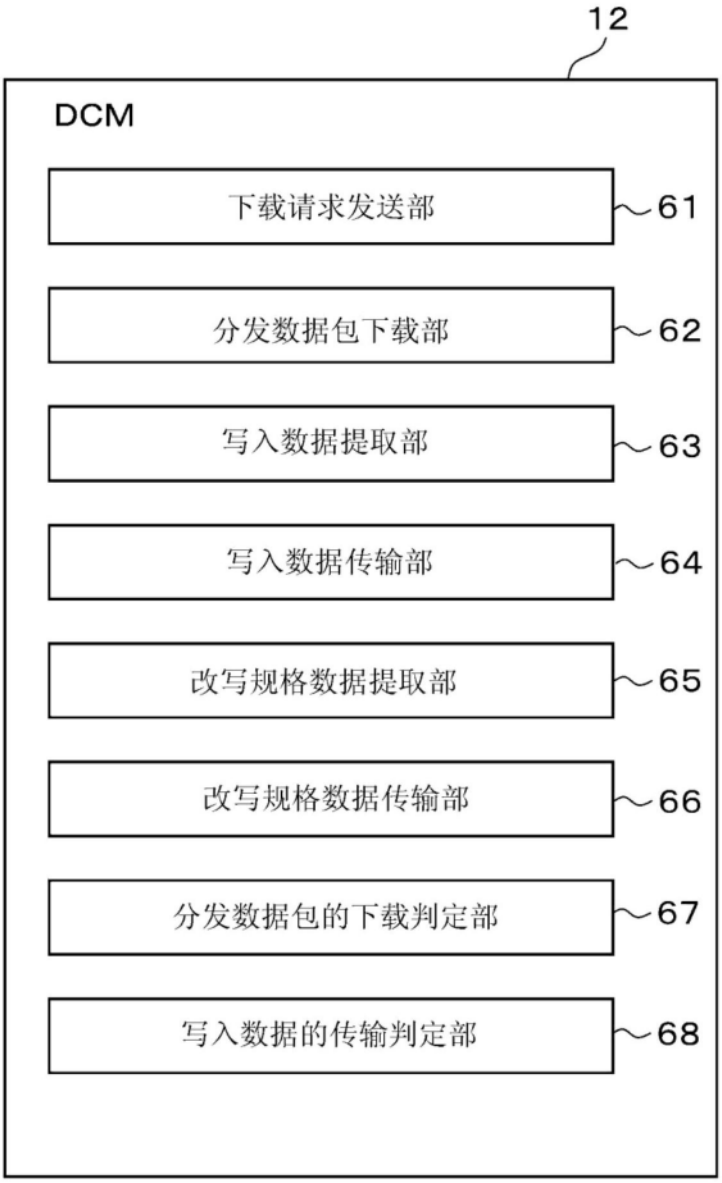

12
DCM
下载请求发送部
61
分发数据包下载部
62
写入数据提取部
63
写入数据传输部
64
改写规格数据提取部
65
改写规格数据传输部
66
分发数据包的下载判定部
67
写入数据的传输判定部
68

图48

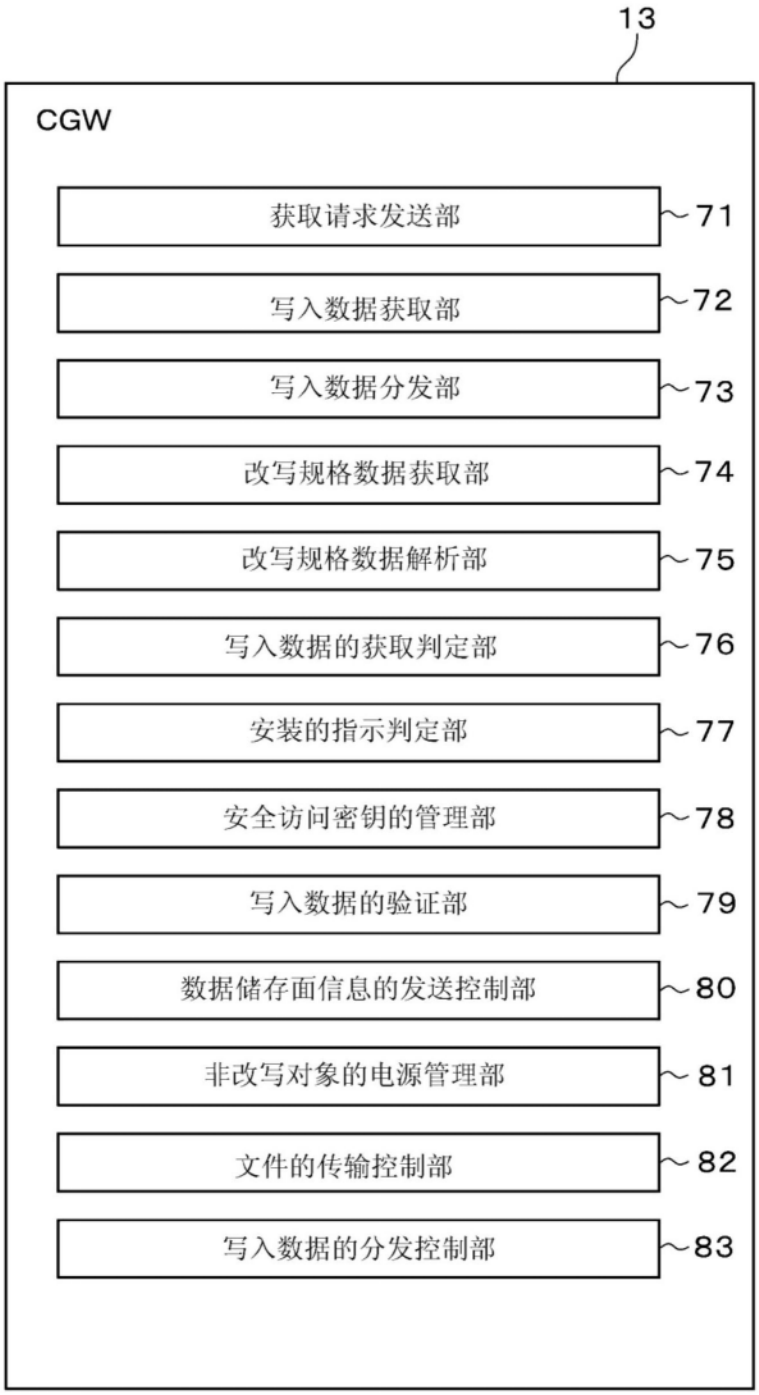

13
CGW
获取请求发送部
71
写入数据获取部
72
写入数据分发部
73
改写规格数据获取部
74
改写规格数据解析部
75
写入数据的获取判定部
76
安装的指示判定部
77
安全访问密钥的管理部
78
写入数据的验证部
79
数据储存面信息的发送控制部
80
非改写对象的电源管理部
81
文件的传输控制部
82
写入数据的分发控制部
83

图49

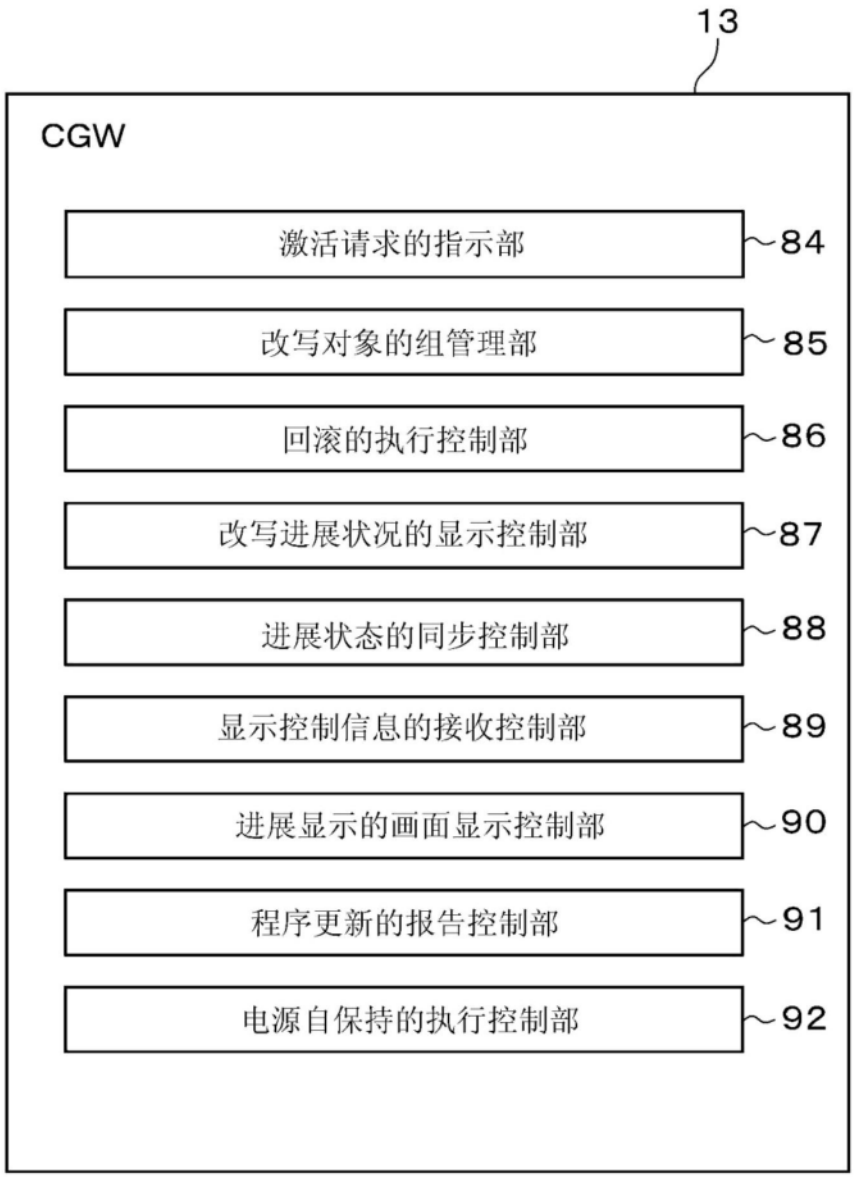

13
CGW
激活请求的指示部
84
改写对象的组管理部
85
回滚的执行控制部
86
改写进展状况的显示控制部
87
进展状态的同步控制部
88
显示控制信息的接收控制部
89
进展显示的画面显示控制部
90
程序更新的报告控制部
91
电源自保持的执行控制部
92

图50

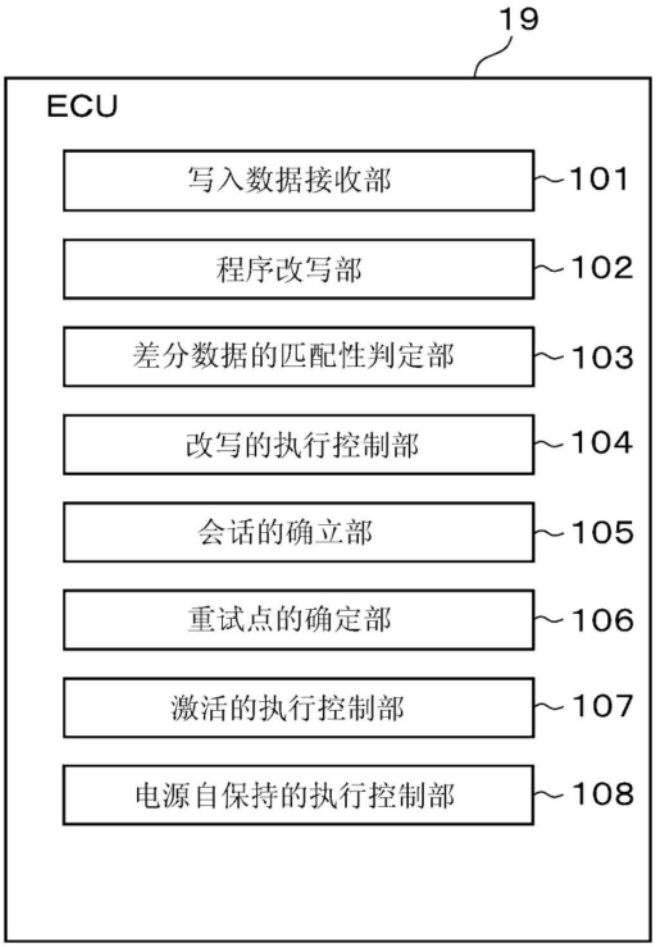

19
ECU
写入数据接收部
101
程序改写部
102
差分数据的匹配性判定部
103
改写的执行控制部
104
会话的确立部
105
重试点的确定部
106
激活的执行控制部
107
电源自保持的执行控制部
108

图51

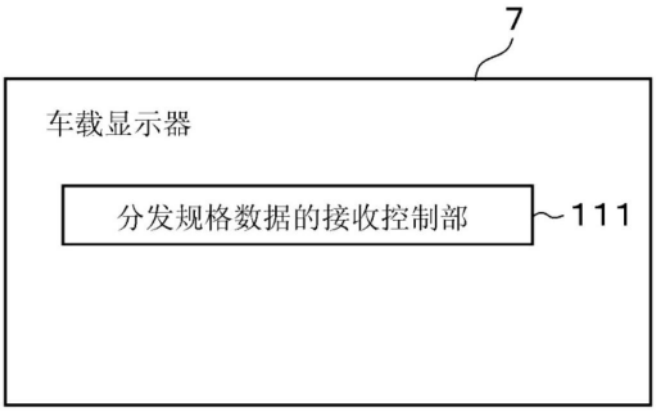

7
车载显示器
分发规格数据的接收控制部
111

图52

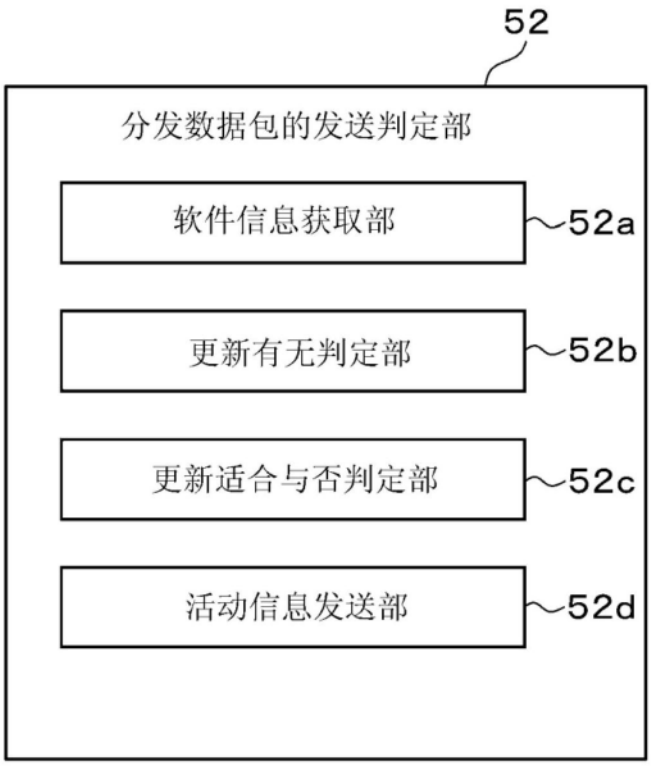

52
分发数据包的发送判定部
软件信息获取部
52a
更新有无判定部
52b
更新适合与否判定部
52c
活动信息发送部
52d

图53

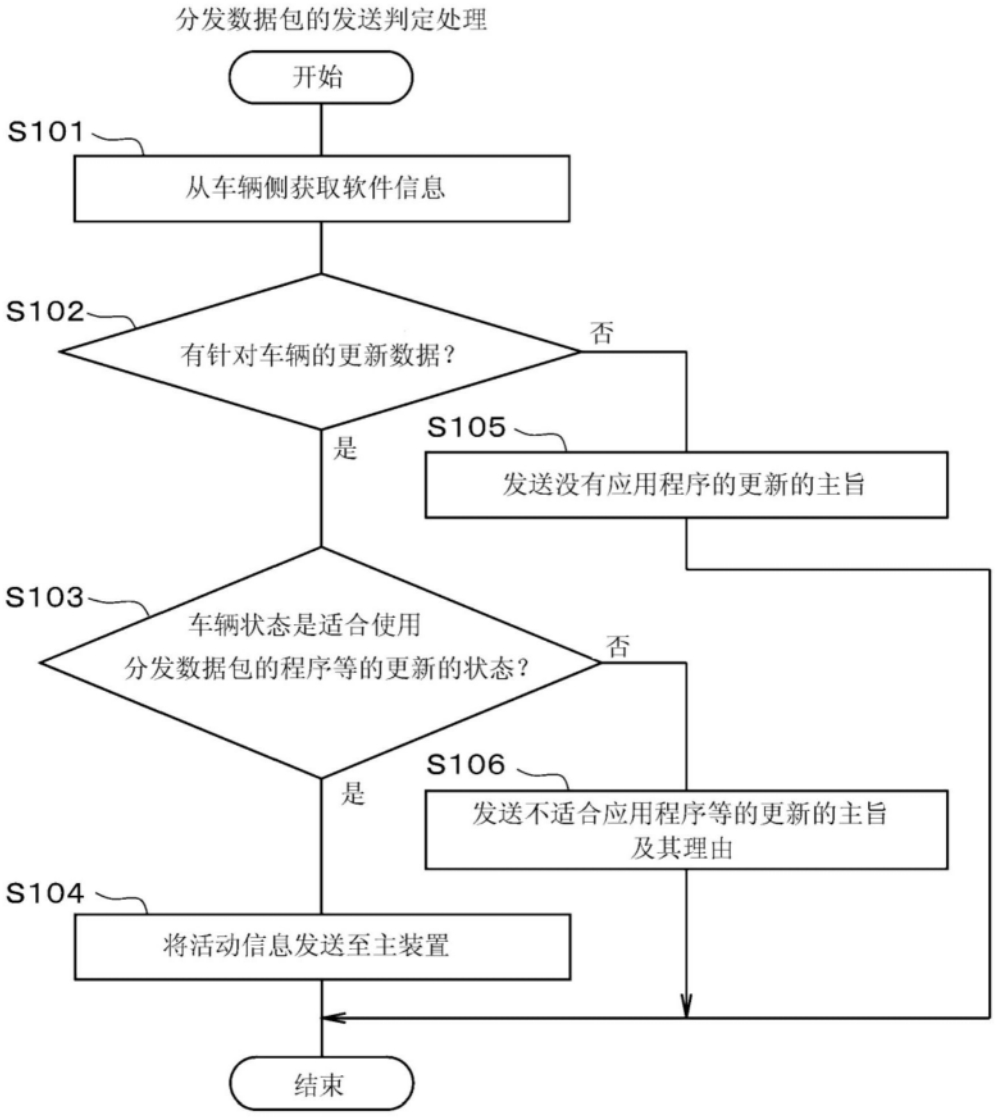

分发数据包的发送判定处理
开始
S101
从车辆侧获取软件信息
S102
有针对车辆的更新数据？
否
是
S105
发送没有应用程序的更新的主旨
S103
车辆状态是适合使用
分发数据包的程序等的更新的状态？
否
是
S106
发送不适合应用程序等的更新的主旨
及其理由
S104
将活动信息发送至主装置
结束

图54

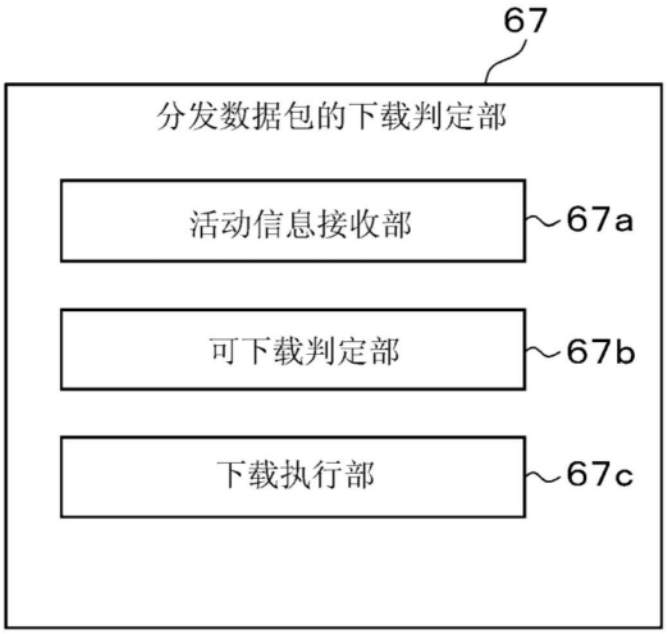


图55

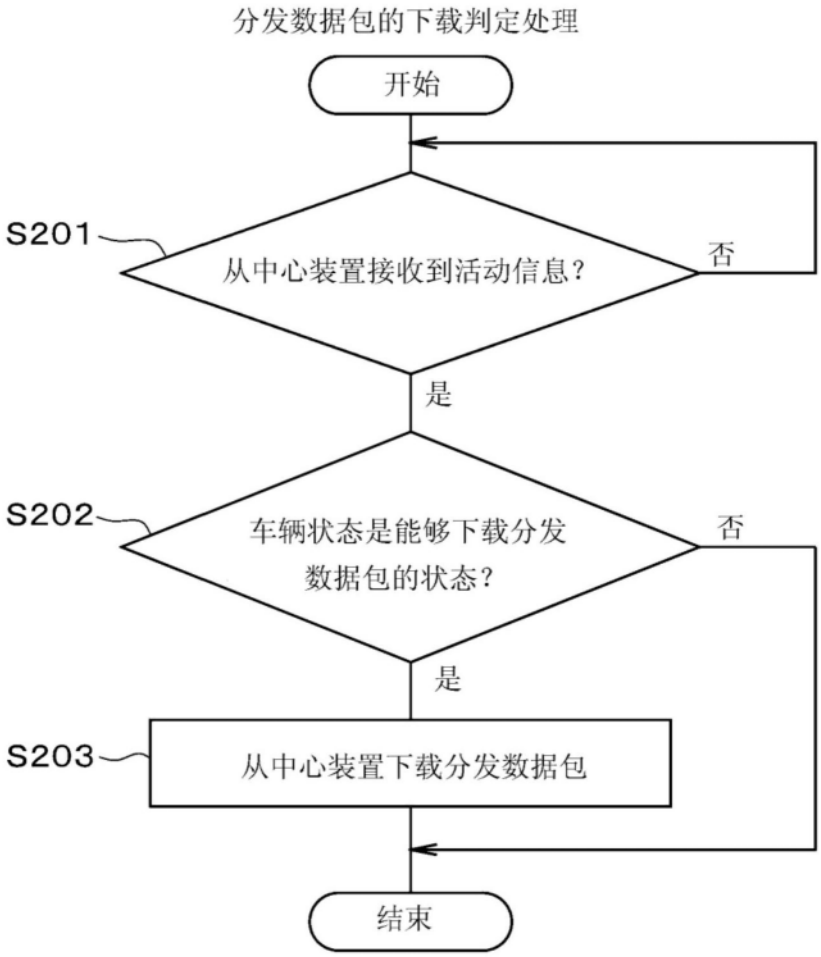

分发数据包的下载判定处理
开始
S201
从中心装置接收到活动信息？
否
是
S202
车辆状态是能够下载分发数据包的状态？
否
是
S203
从中心装置下载分发数据包
结束

图56

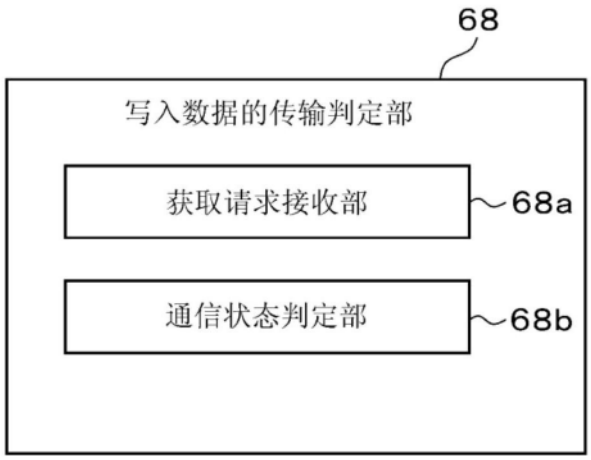

68
写入数据的传输判定部
获取请求接收部
68a
通信状态判定部
68b

图57

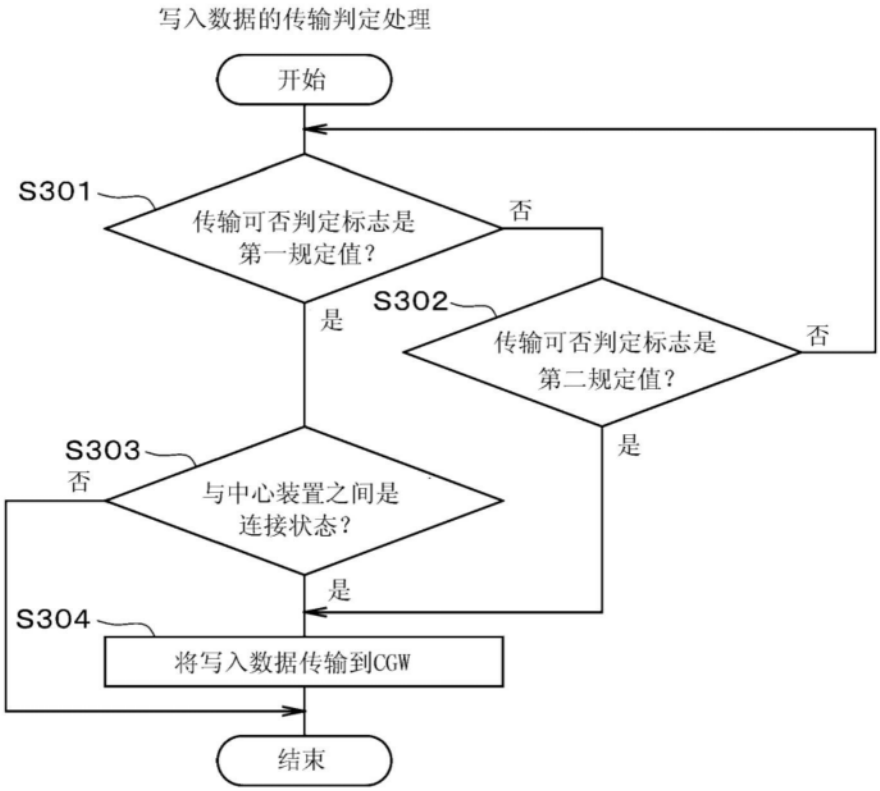

写入数据的传输判定处理
开始
S301
传输可否判定标志是
第一规定值?
否
是
S302
传输可否判定标志是
第二规定值?
否
是
S303
否
与中心装置之间是
连接状态?
是
S304
将写入数据传输到CGW
结束

图58

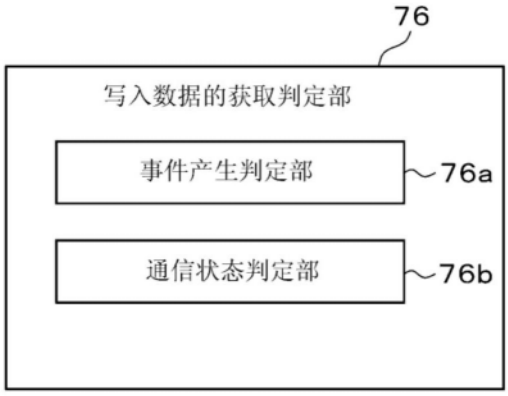

76
写入数据的获取判定部
事件产生判定部
76a
通信状态判定部
76b

图59

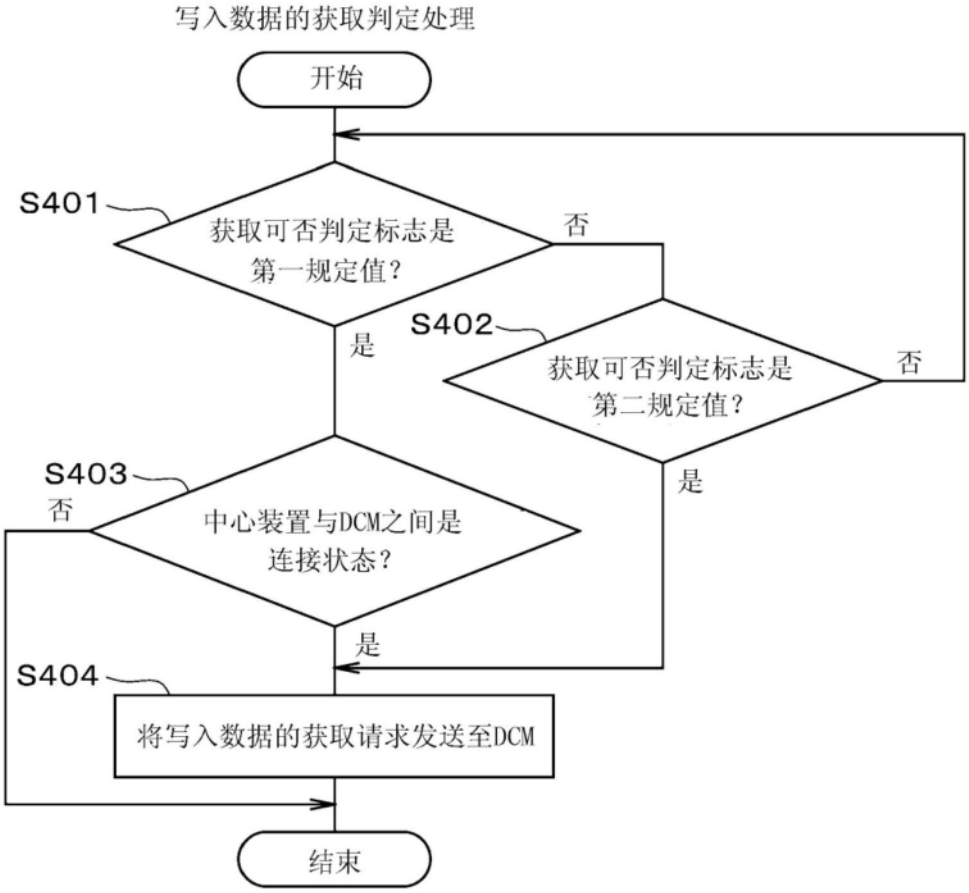

写入数据的获取判定处理
开始
S401
获取可否判定标志是
第一规定值?
否
是
S402
获取可否判定标志是
第二规定值?
否
是
S403
否
中心装置与DCM之间是
连接状态?
是
S404
将写入数据的获取请求发送至DCM
结束

图60

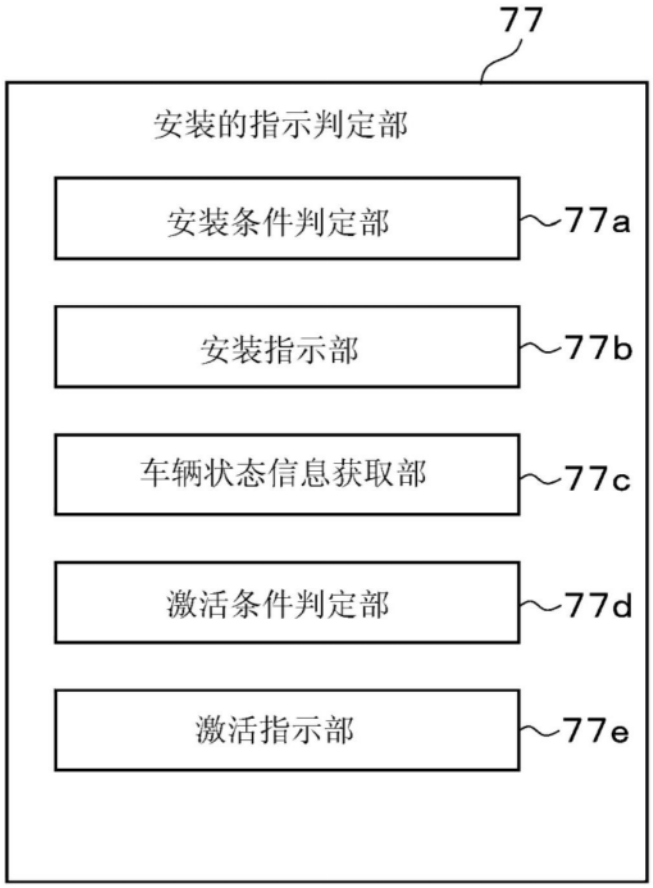

77
安装的指示判定部
安装条件判定部
77a
安装指示部
77b
车辆状态信息获取部
77c
激活条件判定部
77d
激活指示部
77e

图61

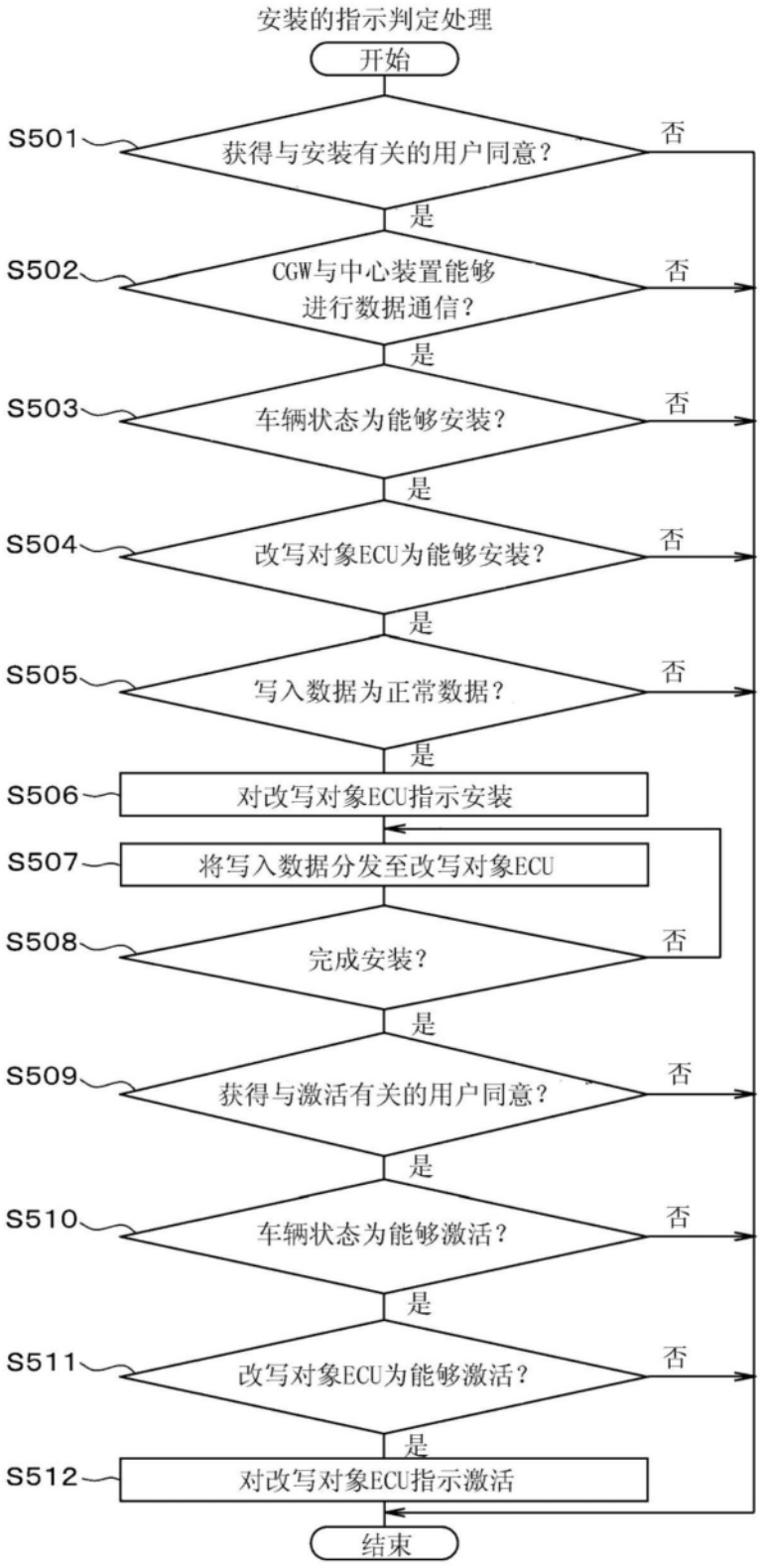

安装的指示判定处理
开始
S501
获得与安装有关的用户同意？
否
是
S502
CGW与中心装置能够
进行数据通信？
否
是
S503
车辆状态为能够安装？
否
是
S504
改写对象ECU为能够安装？
否
是
S505
写入数据为正常数据？
否
是
S506
对改写对象ECU指示安装
S507
将写入数据分发至改写对象ECU
S508
完成安装？
否
是
S509
获得与激活有关的用户同意？
否
是
S510
车辆状态为能够激活？
否
是
S511
改写对象ECU为能够激活？
否
是
S512
对改写对象ECU指示激活
结束

图62

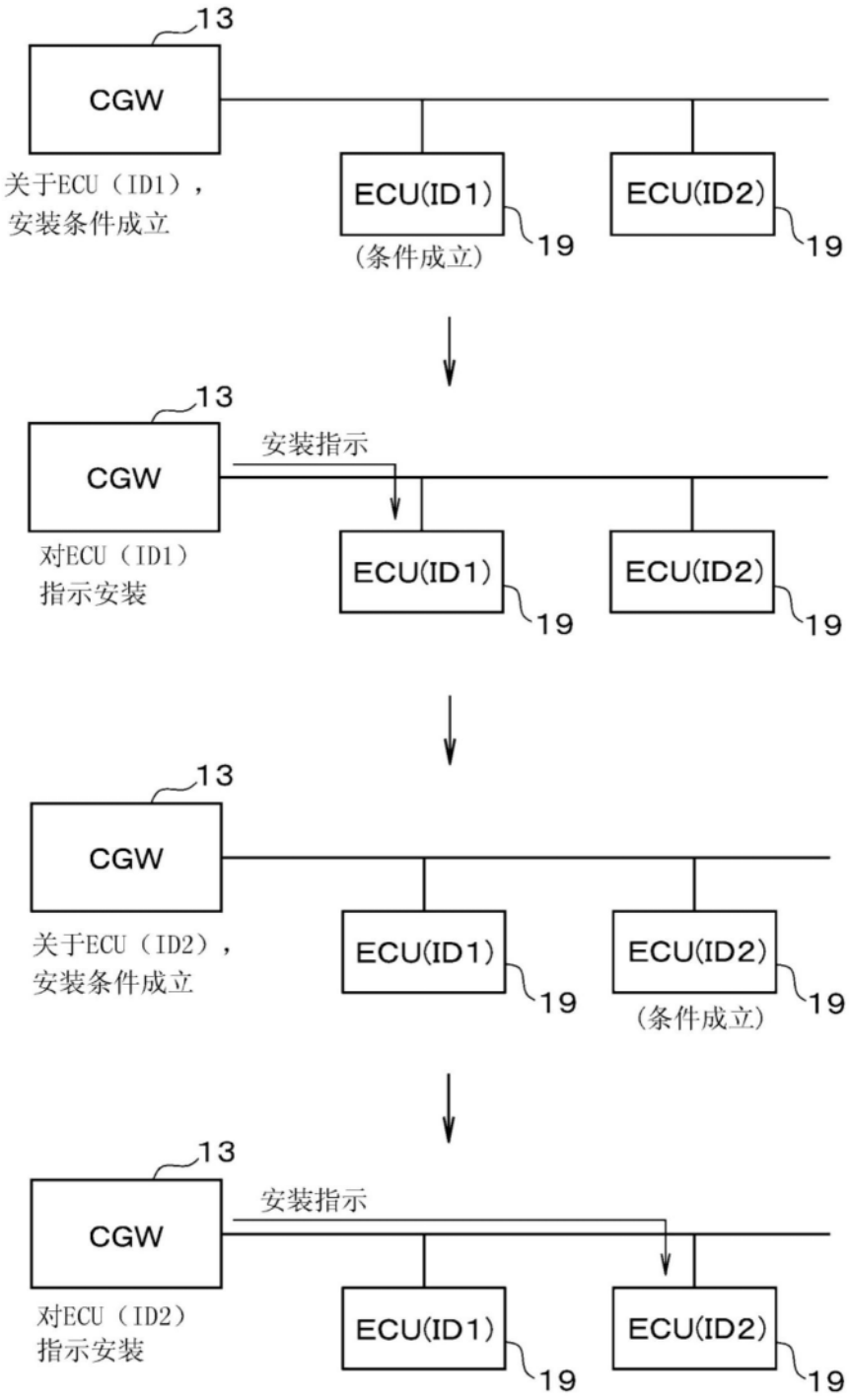

13
CGW
关于ECU（ID1），
安装条件成立
ECU(ID1)
19
（条件成立）
ECU(ID2)
19
13
CGW
安装指示
对ECU（ID1）
指示安装
ECU(ID1)
19
ECU(ID2)
19
13
CGW
关于ECU（ID2），
安装条件成立
ECU(ID1)
19
ECU(ID2)
19
（条件成立）
13
CGW
安装指示
对ECU（ID2）
指示安装
ECU(ID1)
19
ECU(ID2)
19

图63

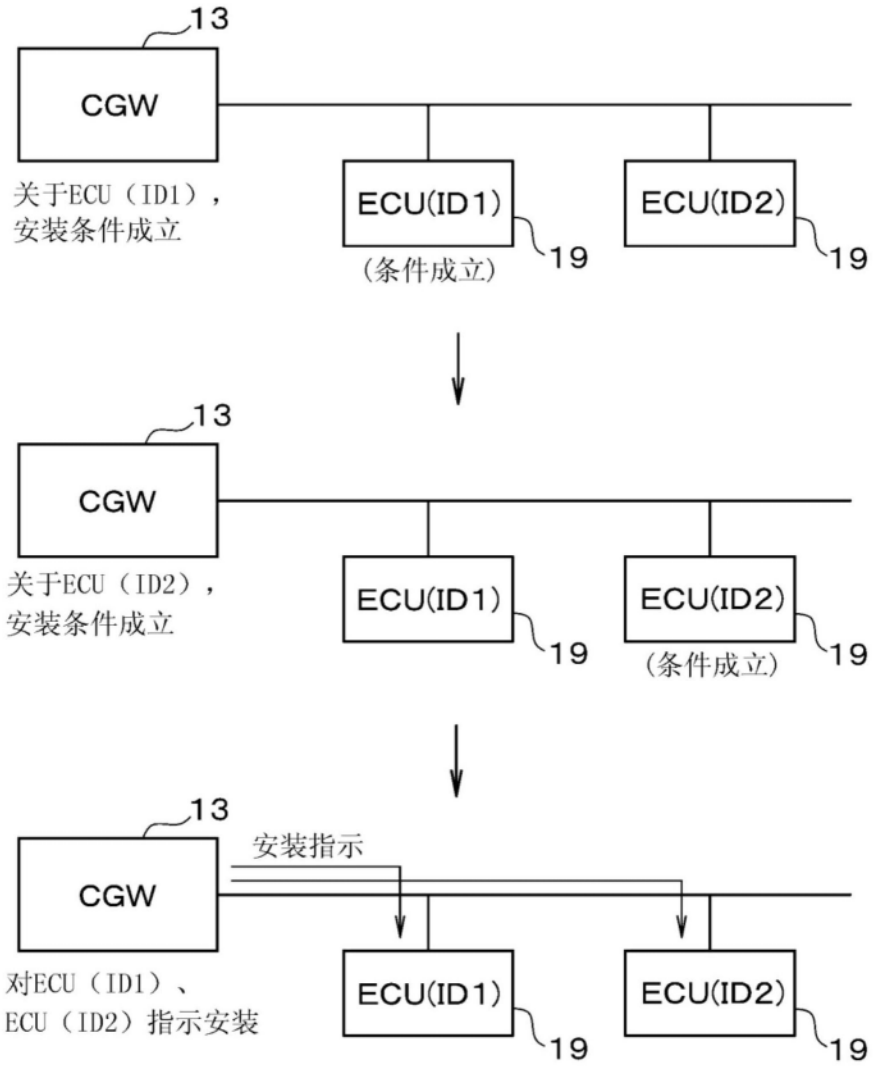

13
CGW
关于ECU（ID1），
安装条件成立
ECU(ID1)
19
（条件成立）
ECU(ID2)
19
13
CGW
关于ECU（ID2），
安装条件成立
ECU(ID1)
19
ECU(ID2)
（条件成立）
19
13
安装指示
CGW
对ECU（ID1）、
ECU（ID2）指示安装
ECU(ID1)
19
ECU(ID2)
19

图64

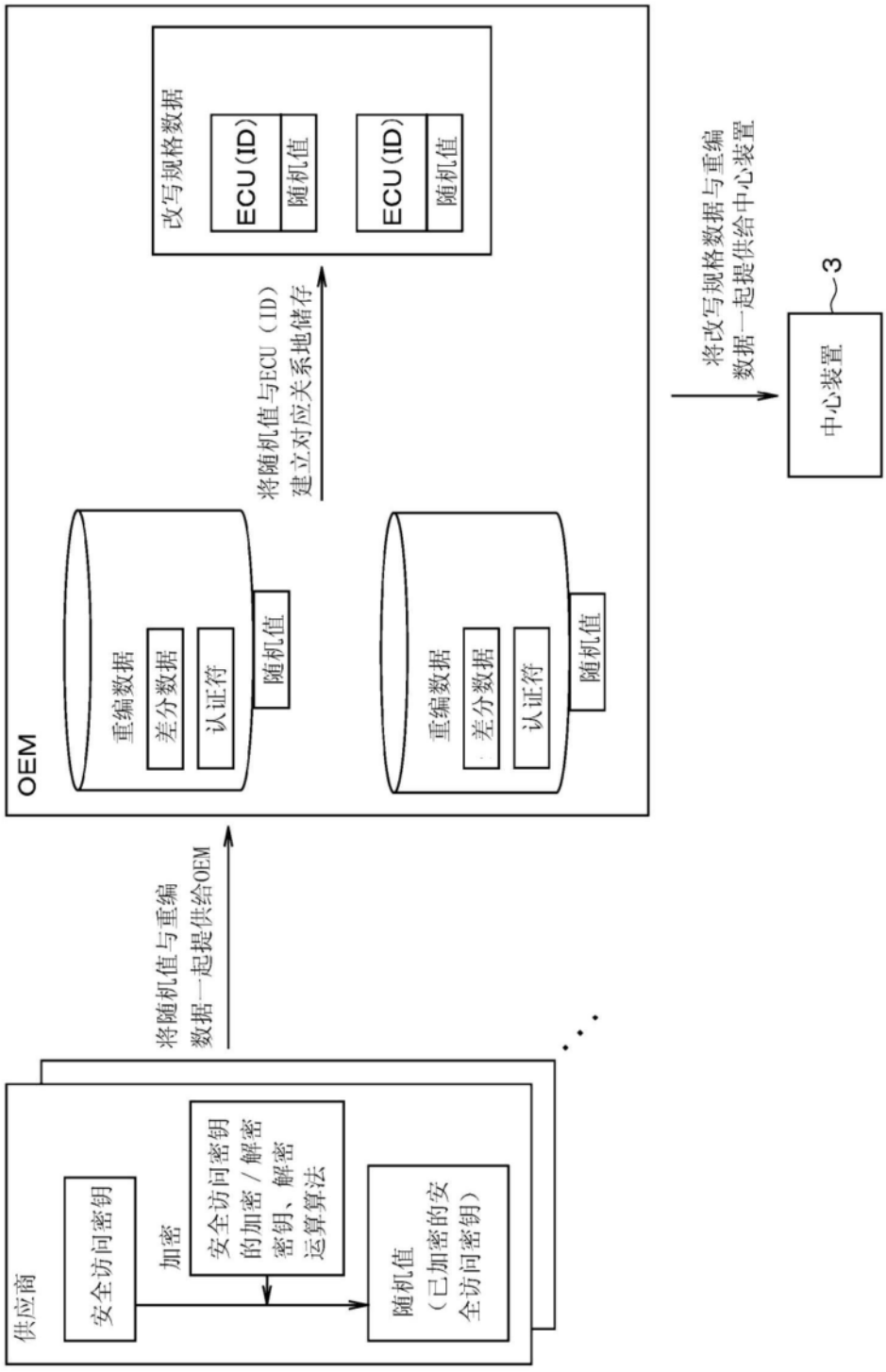

供应商
安全访问密钥
加密
安全访问密钥的加密/解密密钥、解密运算算法
随机值（已加密的安全访问密钥）
将随机值与重编数据一起提供给OEM
OEM
重编数据
差分数据
认证符
随机值
将随机值与ECU（ID）建立对应关系地储存
改写规格数据
ECU(ID)
随机值
将改写规格数据与重编数据一起提供给中心装置
中心装置
3

图65

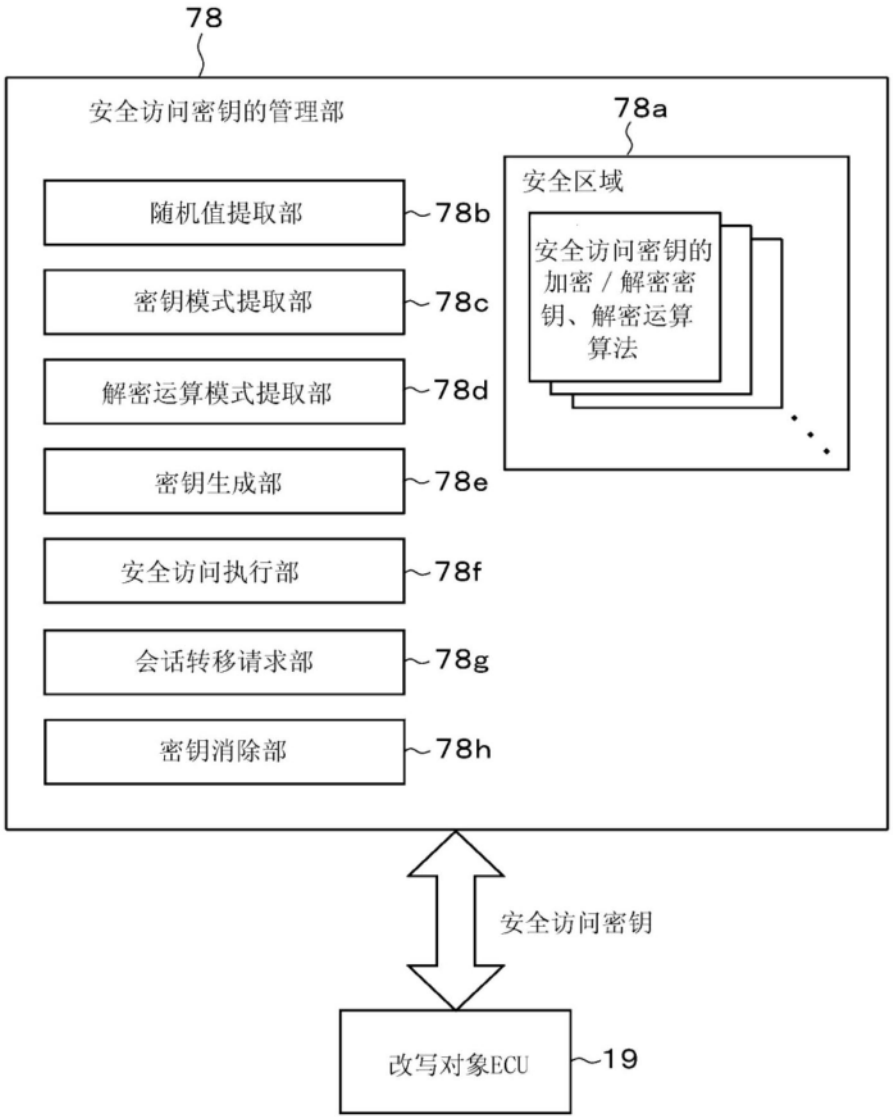

78
安全访问密钥的管理部
78a
安全区域
随机值提取部
78b
密钥模式提取部
78c
解密运算模式提取部
78d
密钥生成部
78e
安全访问执行部
78f
会话转移请求部
78g
密钥消除部
78h
安全访问密钥的加密／解密密钥、解密运算算法
安全访问密钥
改写对象ECU
19

图66

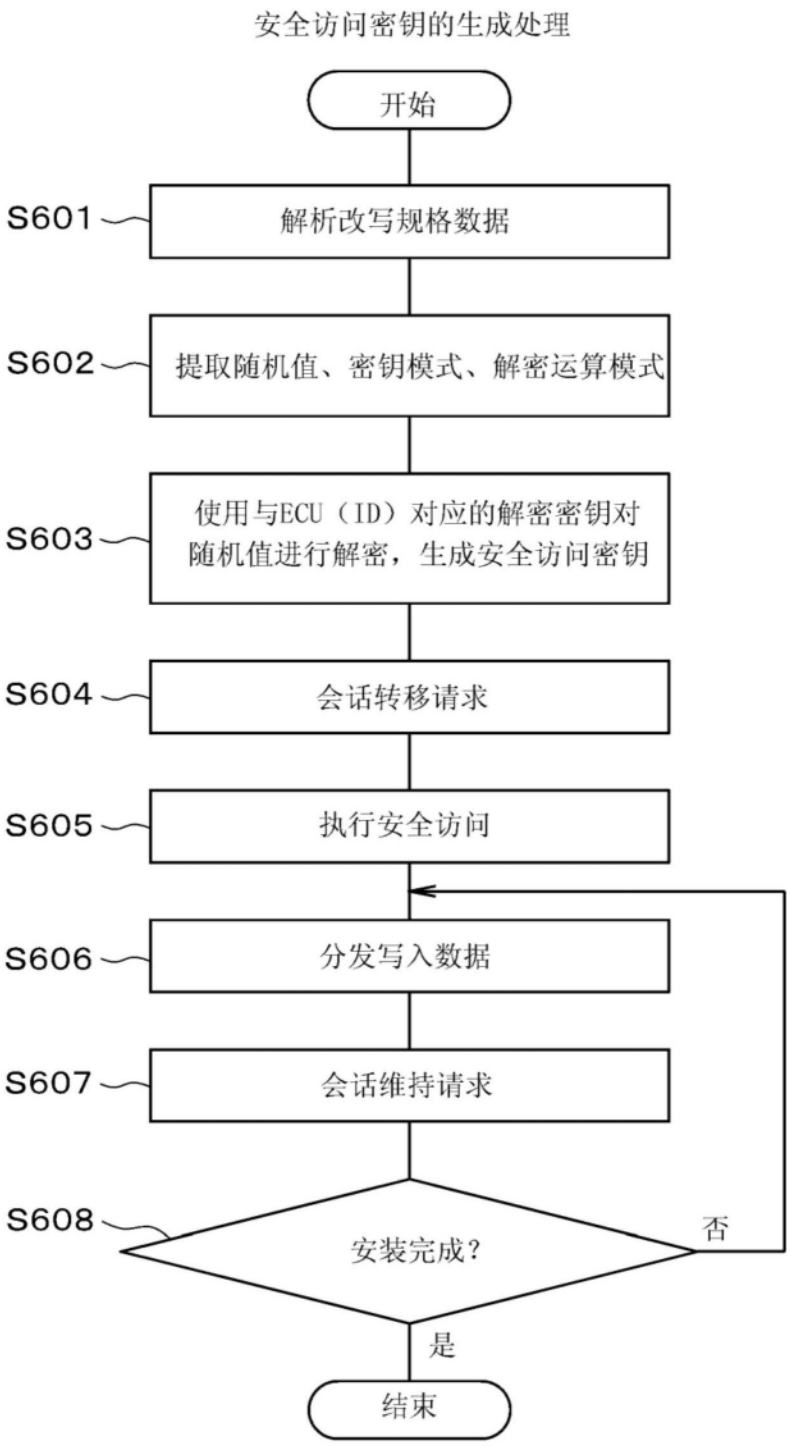

安全访问密钥的生成处理
开始
S601
解析改写规格数据
S602
提取随机值、密钥模式、解密运算模式
S603
使用与ECU（ID）对应的解密密钥对随机值进行解密，生成安全访问密钥
S604
会话转移请求
S605
执行安全访问
S606
分发写入数据
S607
会话维持请求
S608
安装完成？
否
是
结束

图67

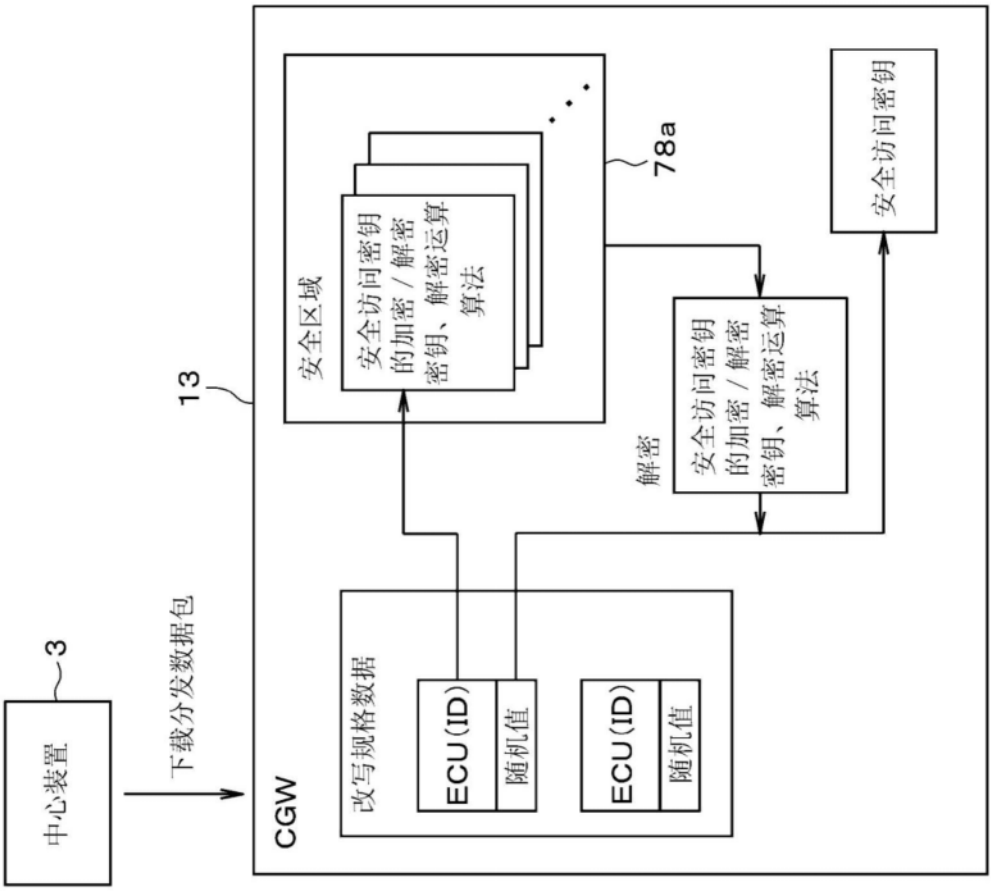

3
中心装置
下载分发数据包
13
CGW
改写规格数据
ECU(ID)
随机值
ECU(ID)
随机值
安全区域
安全访问密钥的加密/解密密钥、解密运算算法
78a
解密
安全访问密钥的加密/解密密钥、解密运算算法
安全访问密钥

图68

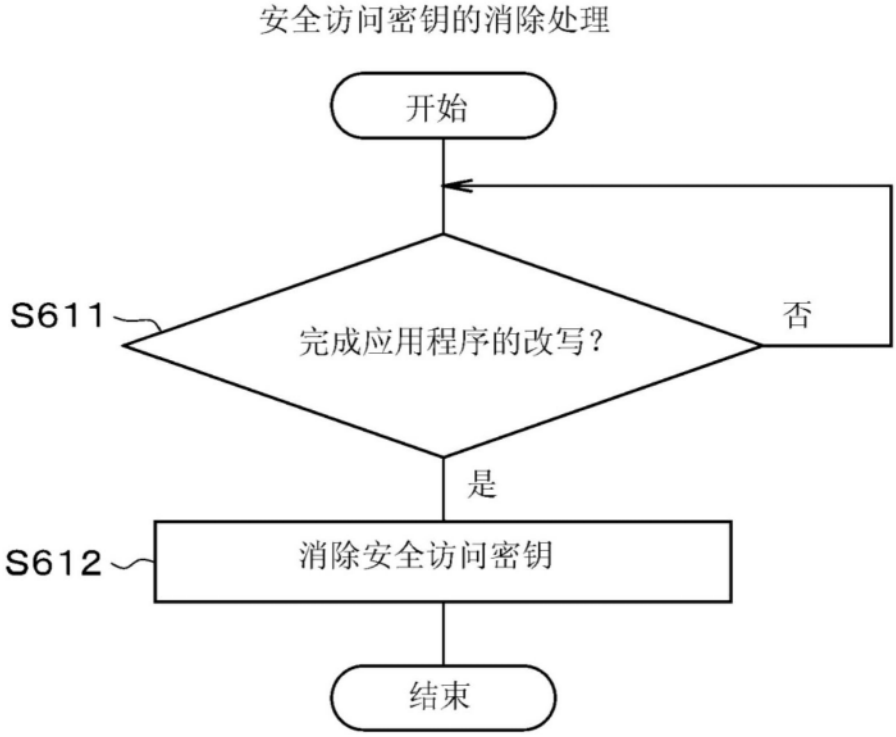


图69

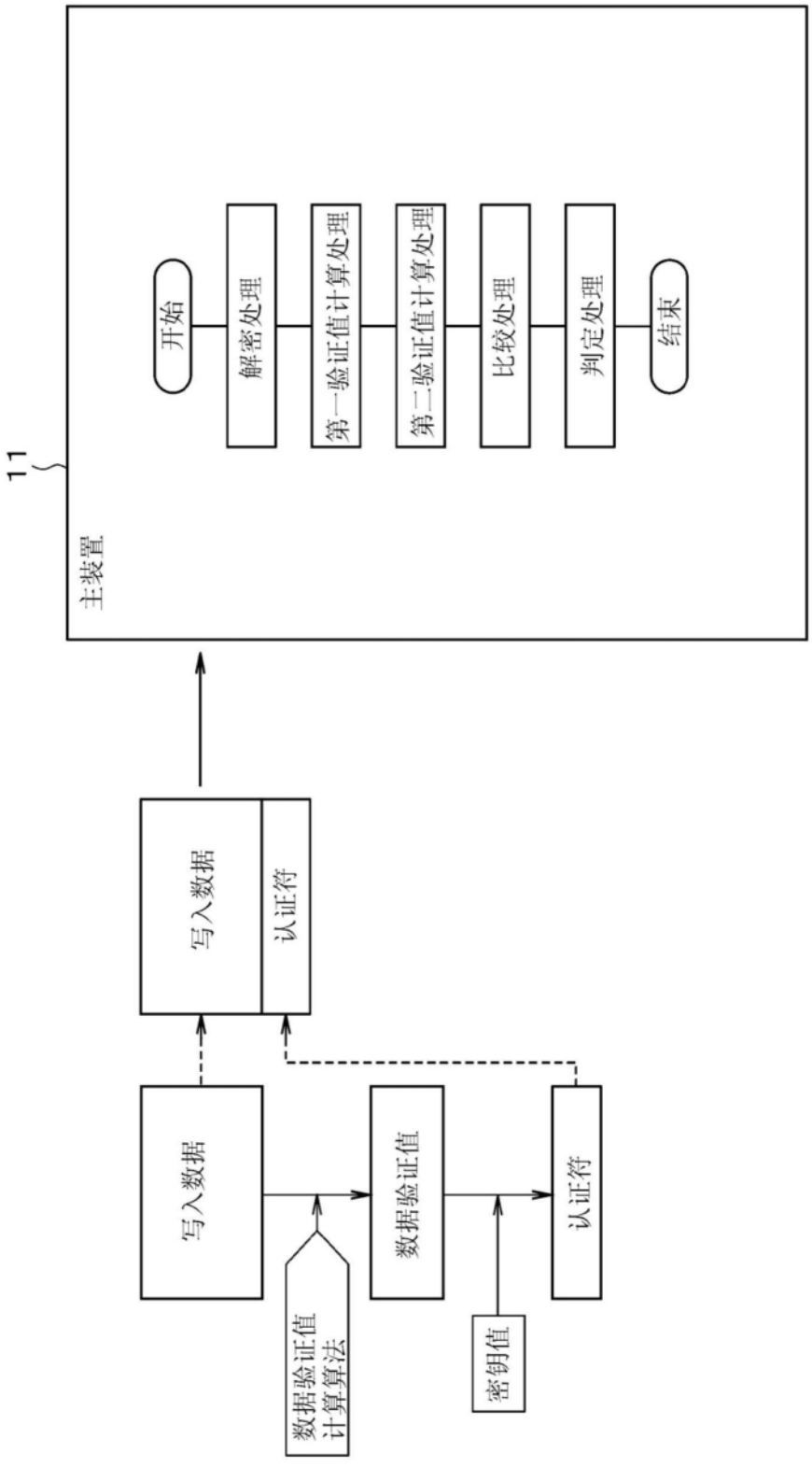

11
主装置
开始
解密处理
第一验证值计算处理
第二验证值计算处理
比较处理
判定处理
结束
写入数据
认证符
写入数据
数据验证值
计算算法
数据验证值
密钥值
认证符

图70

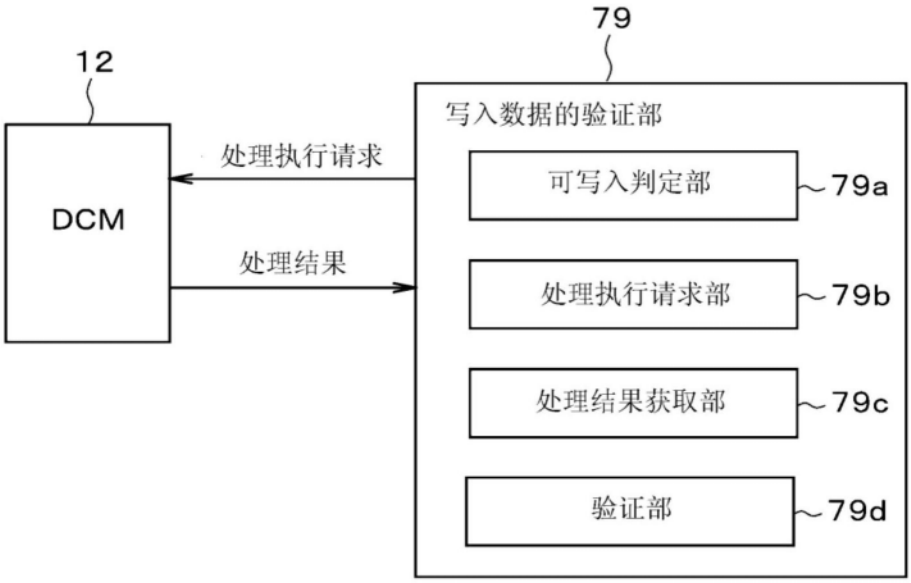

79
12
写入数据的验证部
处理执行请求
DCM
可写入判定部
79a
处理结果
处理执行请求部
79b
处理结果获取部
79c
验证部
79d

图71

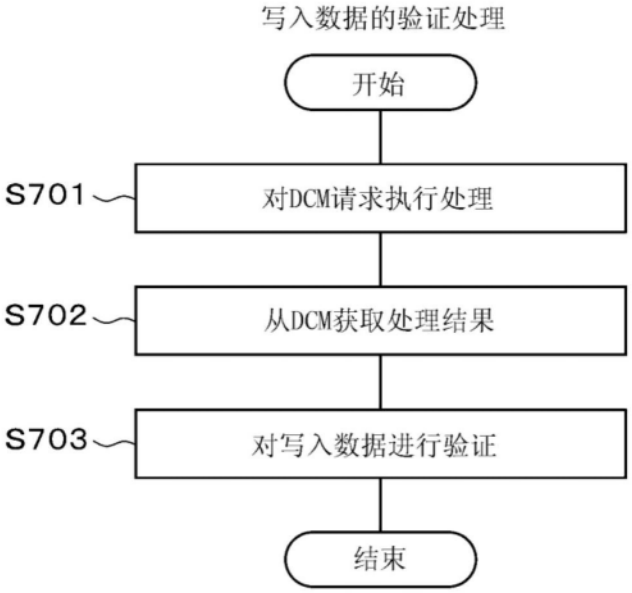

写入数据的验证处理
开始
S701
对DCM请求执行处理
S702
从DCM获取处理结果
S703
对写入数据进行验证
结束

图72

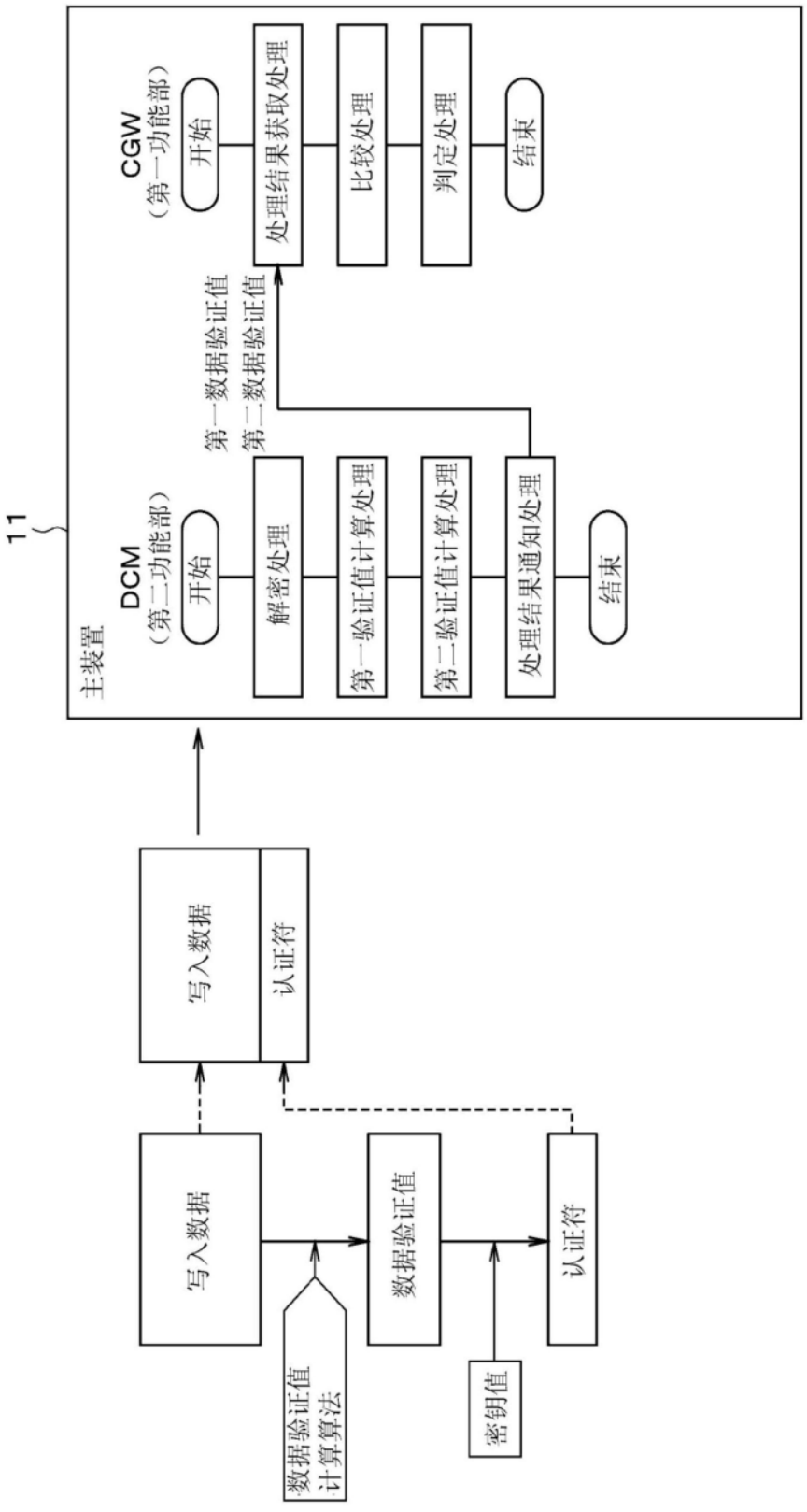

11
主装置
DCM
（第二功能部）
开始
解密处理
第一验证值计算处理
第二验证值计算处理
处理结果通知处理
结束
第一数据验证值
第二数据验证值
CGW
（第一功能部）
开始
处理结果获取处理
比较处理
判定处理
结束
写入数据
认证符
写入数据
数据验证值
计算算法
数据验证值
密钥值
认证符

图73

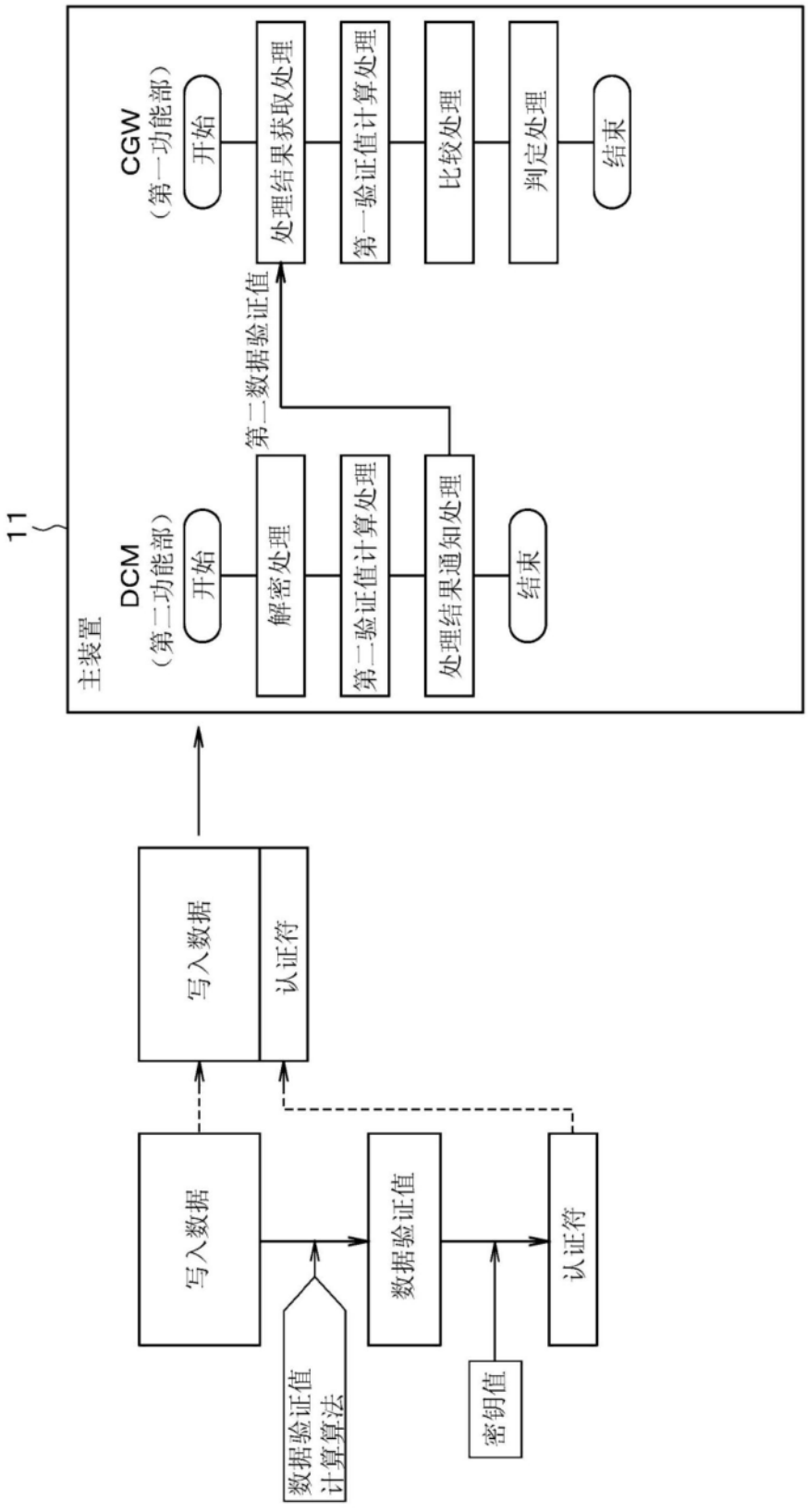

11
主装置
DCM
（第二功能部）
开始
解密处理
第二验证值计算处理
处理结果通知处理
结束
第二数据验证值
CGW
（第一功能部）
开始
处理结果获取处理
第一验证值计算处理
比较处理
判定处理
结束
写入数据
认证符
写入数据
数据验证值
计算算法
数据验证值
密钥值
认证符

图74

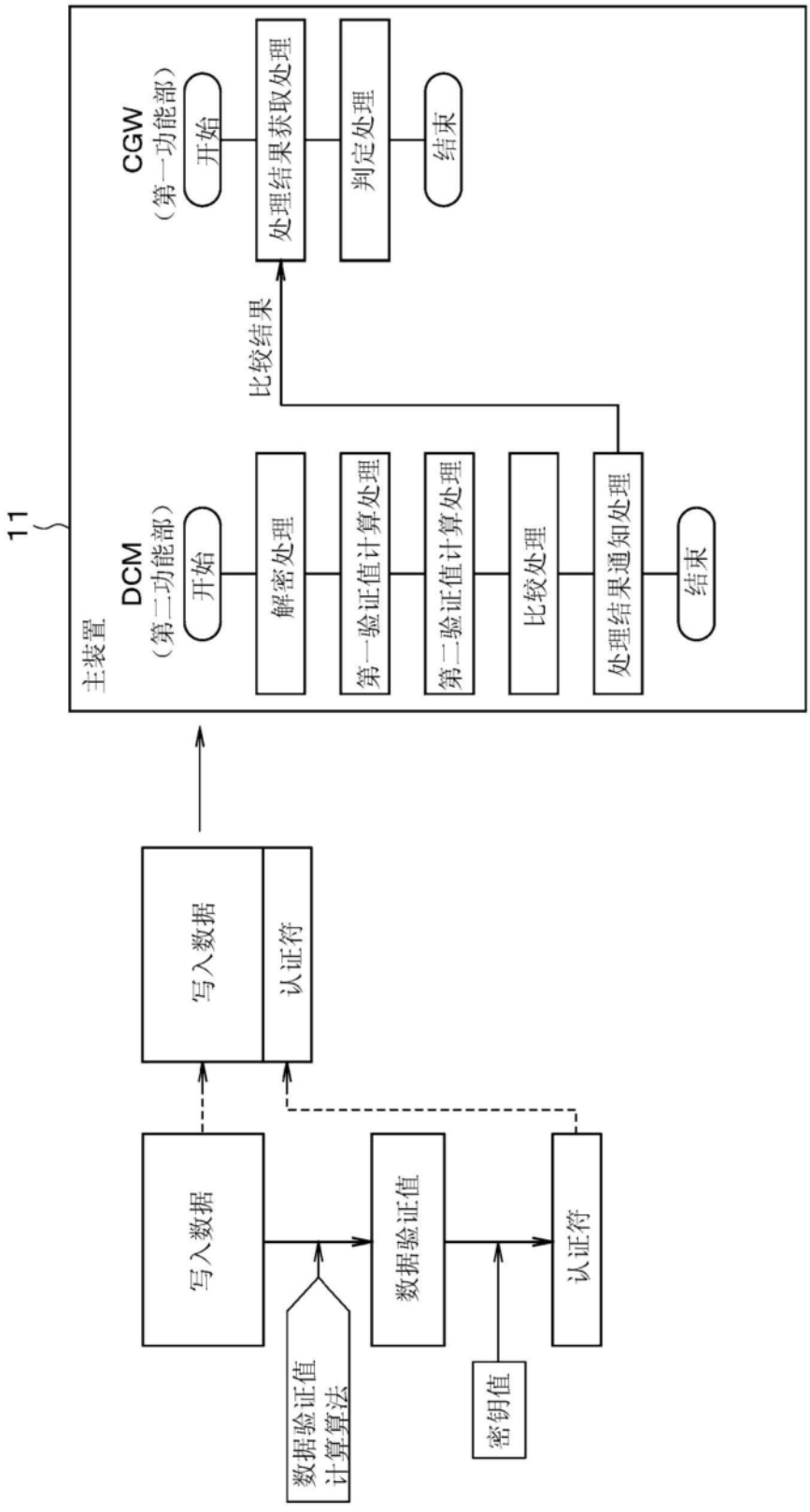

11
主装置
DCM
（第二功能部）
开始
解密处理
第一验证值计算处理
第二验证值计算处理
比较处理
处理结果通知处理
结束
比较结果
CGW
（第一功能部）
开始
处理结果获取处理
判定处理
结束
写入数据
认证符
写入数据
数据验证值
计算算法
数据验证值
密钥值
认证符

图75

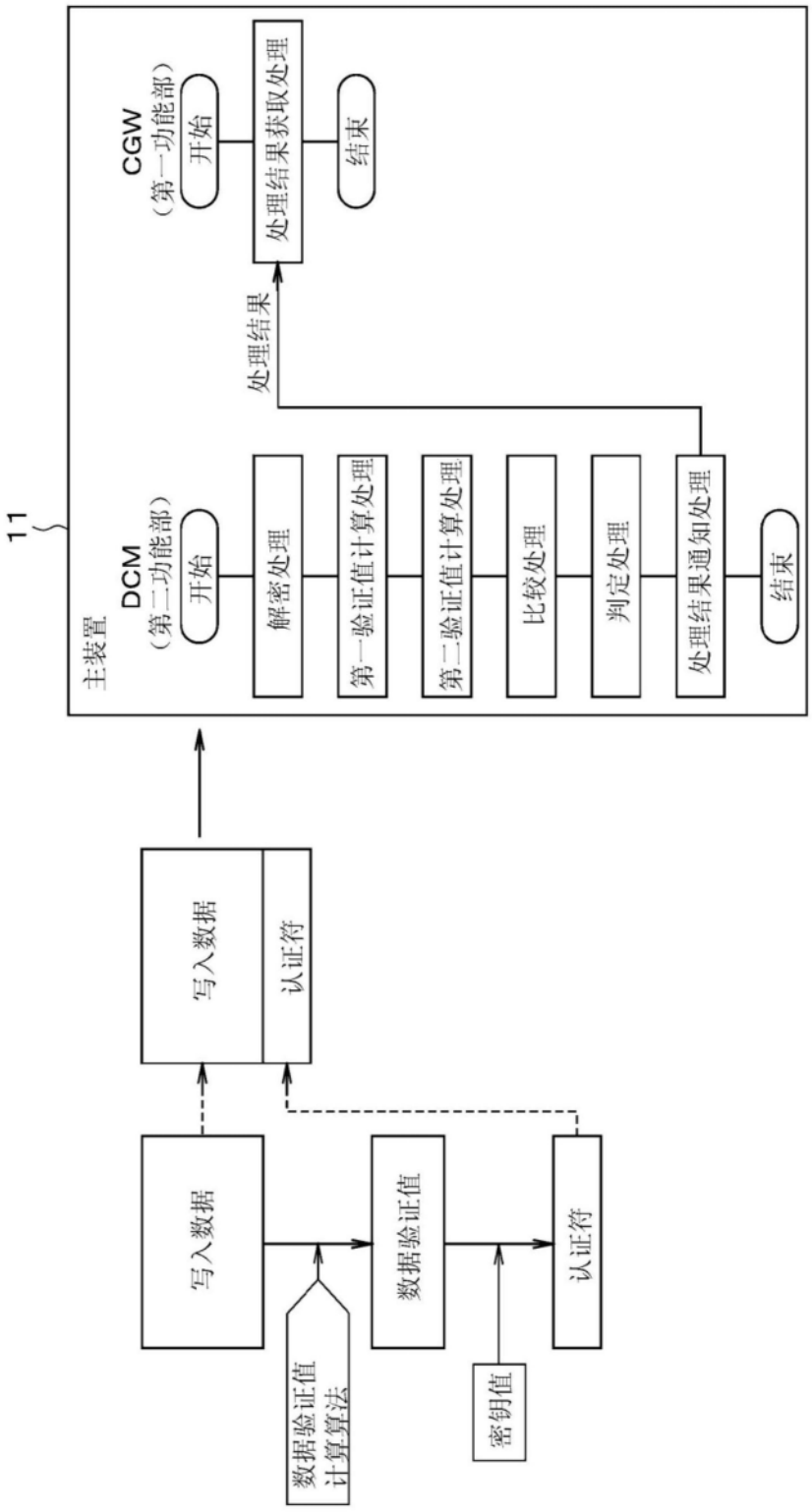

11
主装置
DCM
（第二功能部）
开始
解密处理
第一验证值计算处理
第二验证值计算处理
比较处理
判定处理
处理结果通知处理
结束
处理结果
CGW
（第一功能部）
开始
处理结果获取处理
结束
写入数据
认证符
写入数据
数据验证值计算算法
数据验证值
密钥值
认证符

图76

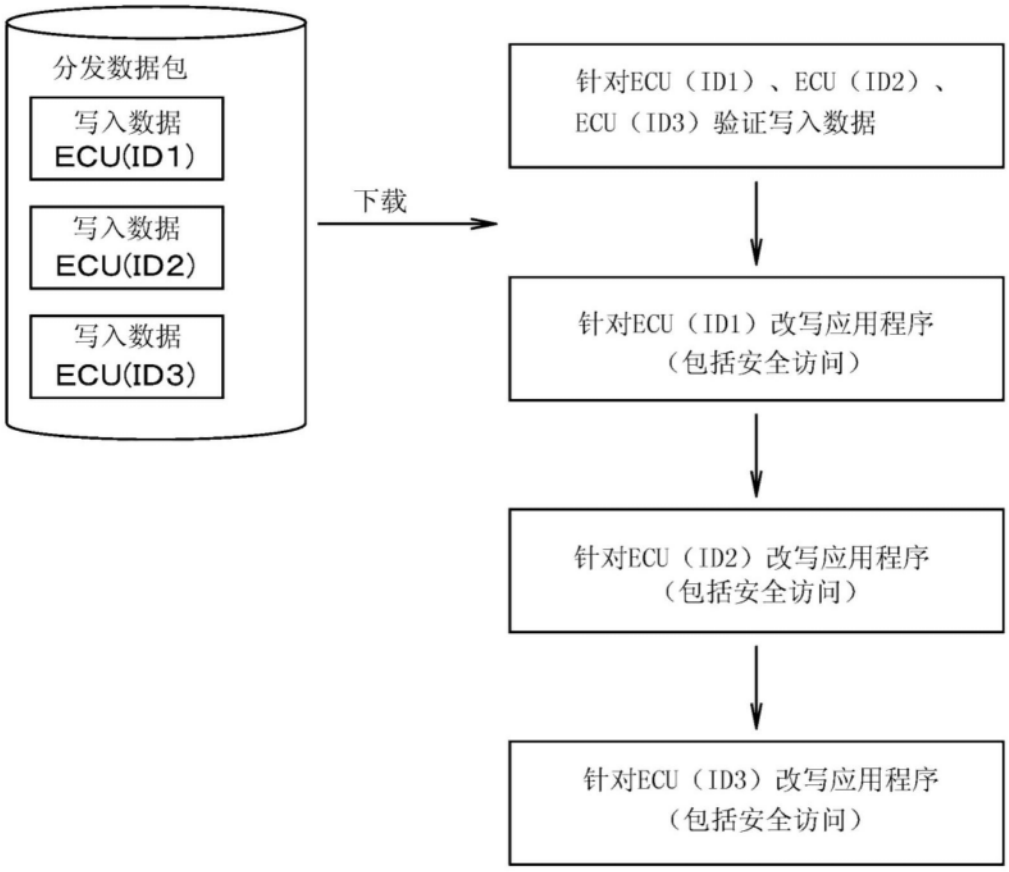

分发数据包
写入数据
ECU(ID1)
写入数据
ECU(ID2)
写入数据
ECU(ID3)
下载
针对ECU（ID1）、ECU（ID2）、
ECU（ID3）验证写入数据
针对ECU（ID1）改写应用程序
（包括安全访问）
针对ECU（ID2）改写应用程序
（包括安全访问）
针对ECU（ID3）改写应用程序
（包括安全访问）

图77

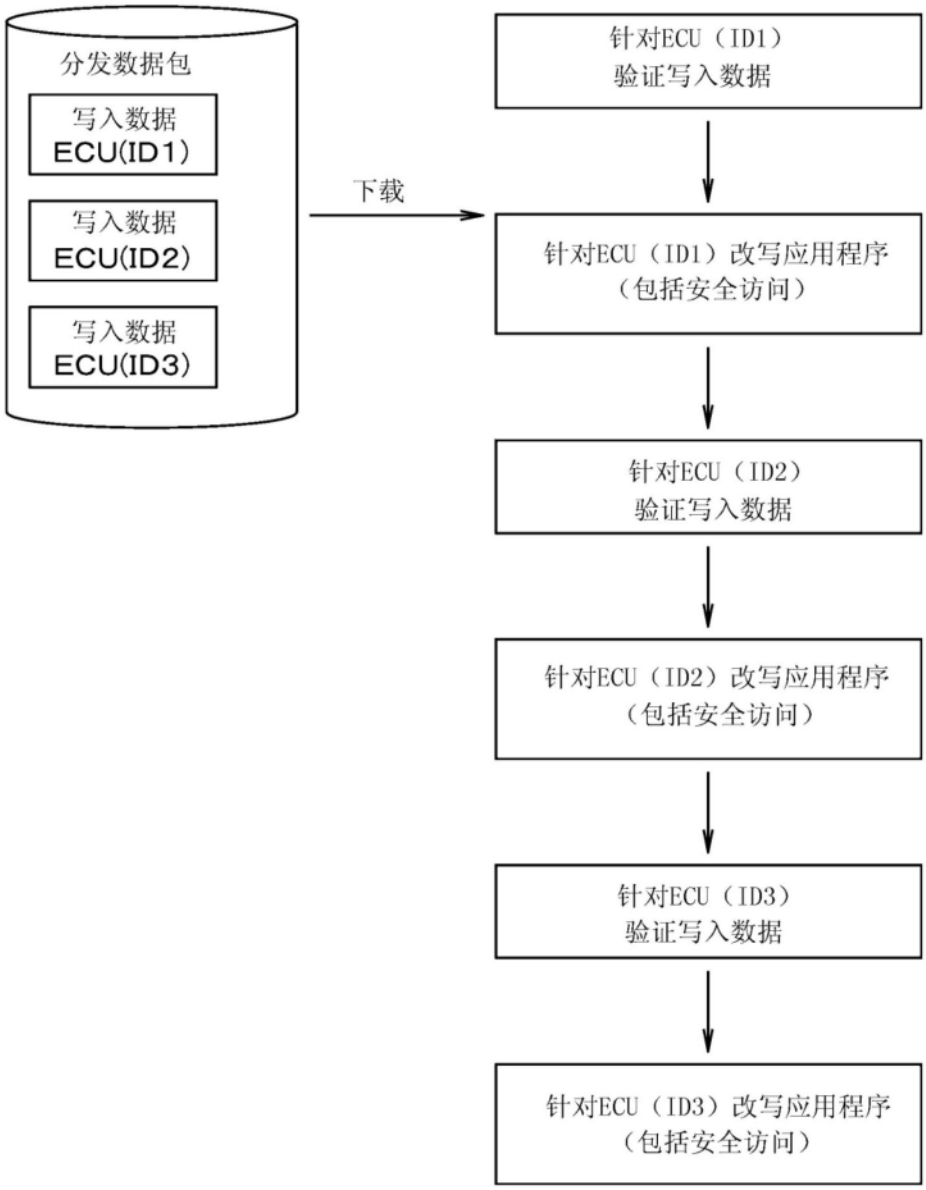

分发数据包
写入数据
ECU(ID1)
写入数据
ECU(ID2)
写入数据
ECU(ID3)
下载
针对ECU（ID1）
验证写入数据
针对ECU（ID1）改写应用程序
（包括安全访问）
针对ECU（ID2）
验证写入数据
针对ECU（ID2）改写应用程序
（包括安全访问）
针对ECU（ID3）
验证写入数据
针对ECU（ID3）改写应用程序
（包括安全访问）

图78

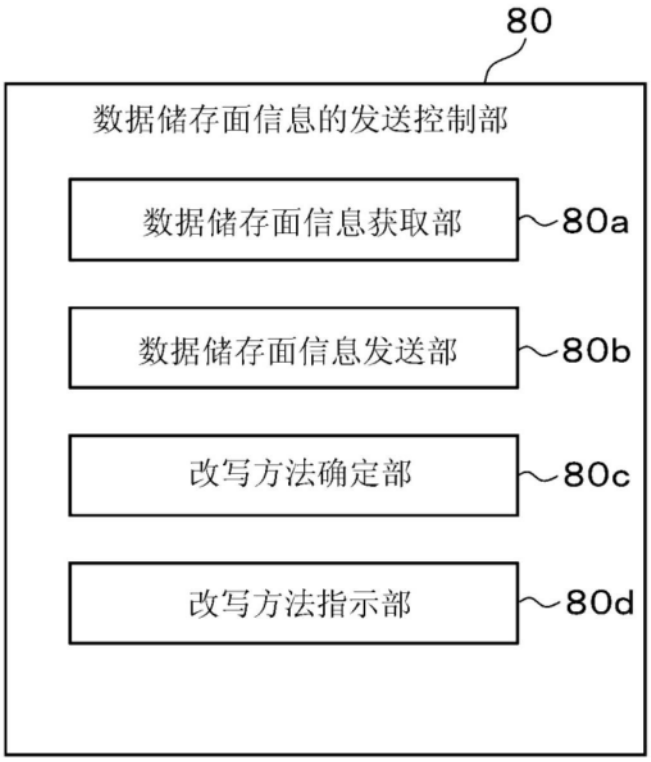

80
数据储存面信息的发送控制部
数据储存面信息获取部
80a
数据储存面信息发送部
80b
改写方法确定部
80c
改写方法指示部
80d

图79

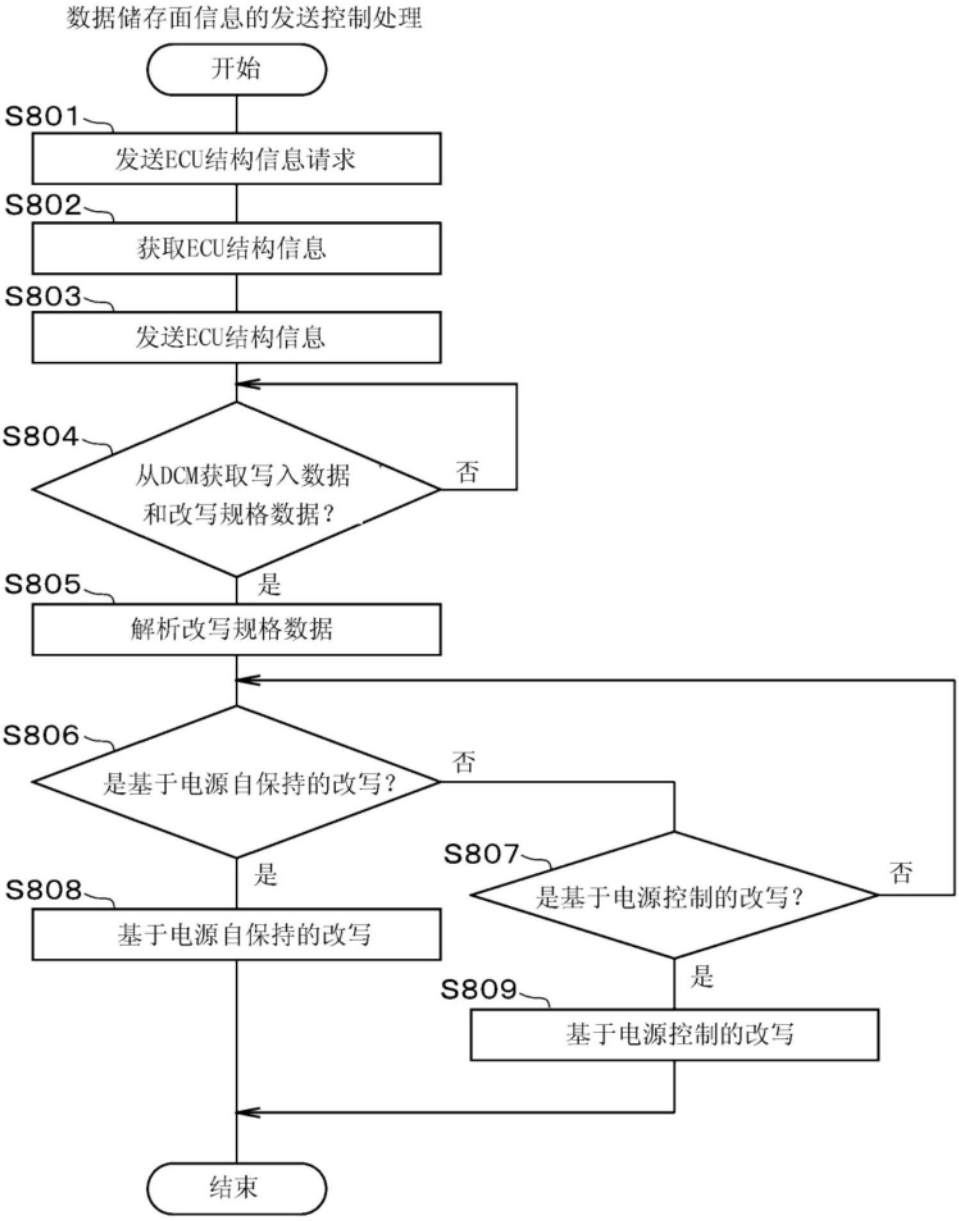

数据储存面信息的发送控制处理
开始
S801
发送ECU结构信息请求
S802
获取ECU结构信息
S803
发送ECU结构信息
S804
从DCM获取写入数据
和改写规格数据？
否
是
S805
解析改写规格数据
S806
是基于电源自保持的改写？
否
是
S807
是基于电源控制的改写？
否
是
S808
基于电源自保持的改写
S809
基于电源控制的改写
结束

图80

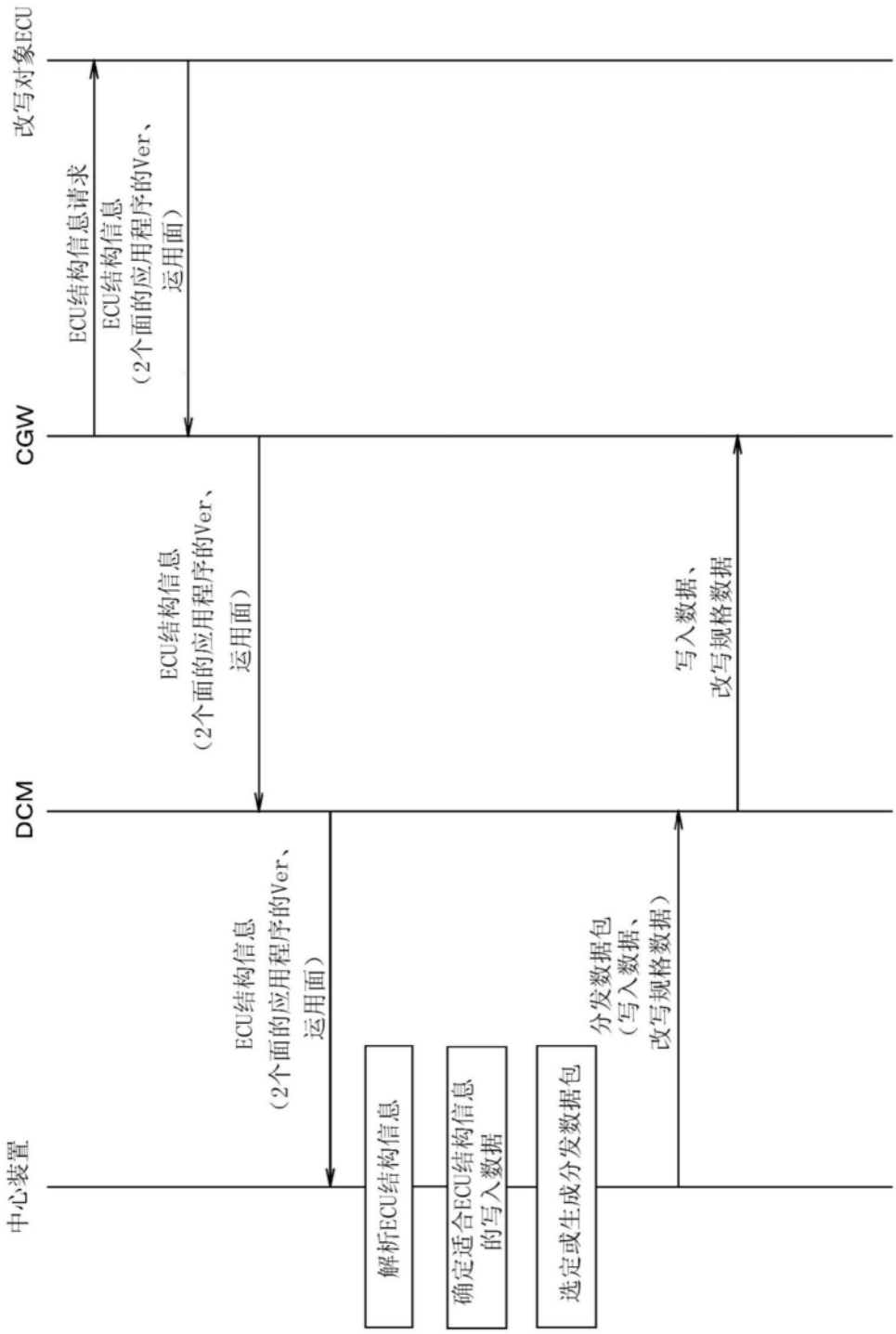

改写对象ECU
CGW
DCM
中心装置
ECU结构信息请求
ECU结构信息
（2个面的应用程序的Ver、
运用面）
ECU结构信息
（2个面的应用程序的Ver、
运用面）
ECU结构信息
（2个面的应用程序的Ver、
运用面）
解析ECU结构信息
确定适合ECU结构信息
的写入数据
选定或生成分发数据包
分发数据包
（写入数据、
改写规格数据）
写入数据、
改写规格数据

图81

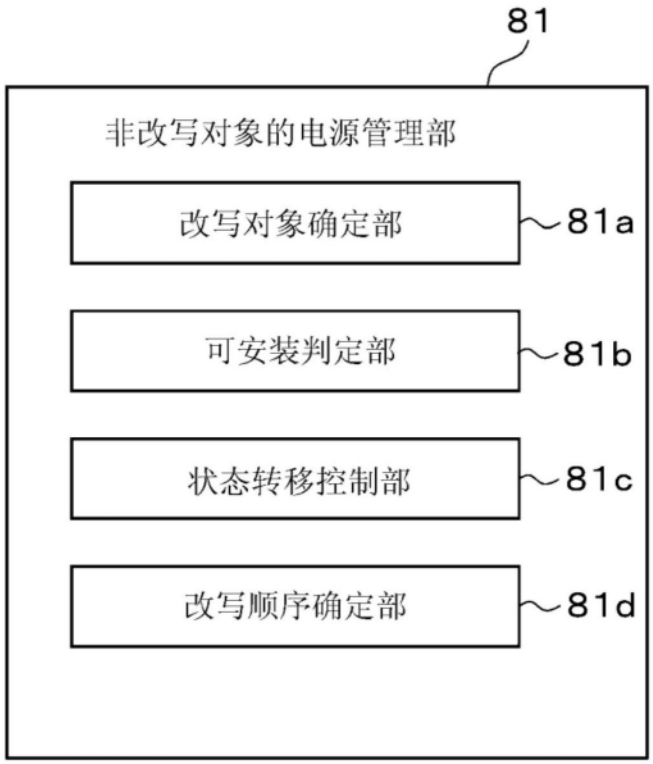

81
非改写对象的电源管理部
改写对象确定部
81a
可安装判定部
81b
状态转移控制部
81c
改写顺序确定部
81d

图82

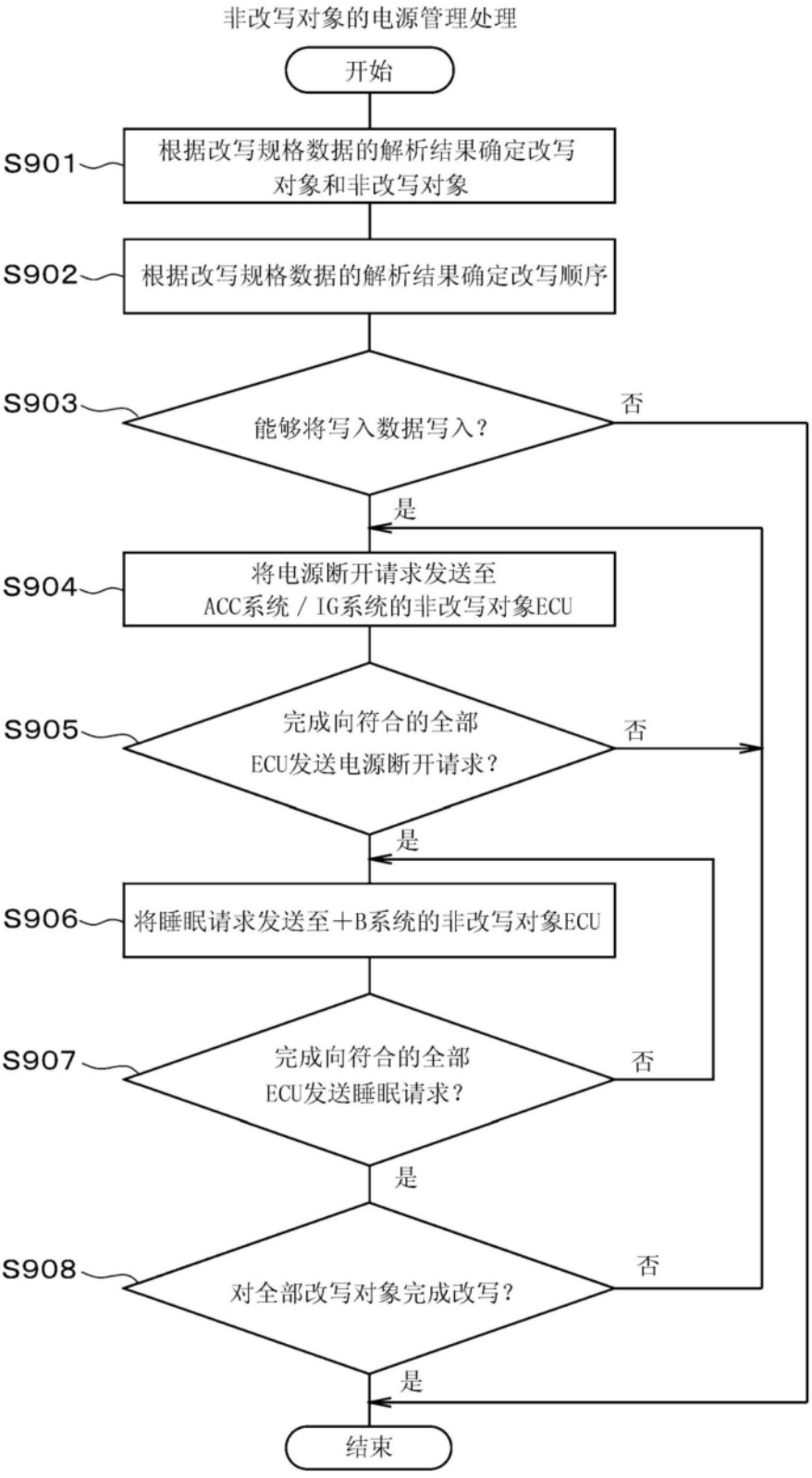

非改写对象的电源管理处理
开始
S901
根据改写规格数据的解析结果确定改写对象和非改写对象
S902
根据改写规格数据的解析结果确定改写顺序
S903
能够将写入数据写入？
否
是
S904
将电源断开请求发送至ACC系统／IG系统的非改写对象ECU
S905
完成向符合的全部ECU发送电源断开请求？
否
是
S906
将睡眠请求发送至＋B系统的非改写对象ECU
S907
完成向符合的全部ECU发送睡眠请求？
否
是
S908
对全部改写对象完成改写？
否
是
结束

图83


改写对象ECU
ECU(ID1)
ECU(ID2)
ECU(ID3)
等待改写
停止 / 睡眠
等待改写
启动
改写中
启动
改写完成
停止 / 睡眠
改写完成
停止 / 睡眠
等待改写
停止 / 睡眠
等待改写
启动
等待改写
停止 / 睡眠
改写中
启动
改写完成
停止 / 睡眠
等待改写
启动
等待改写
停止 / 睡眠
等待改写
停止 / 睡眠
改写中
启动
改写完成
停止 / 睡眠

图84

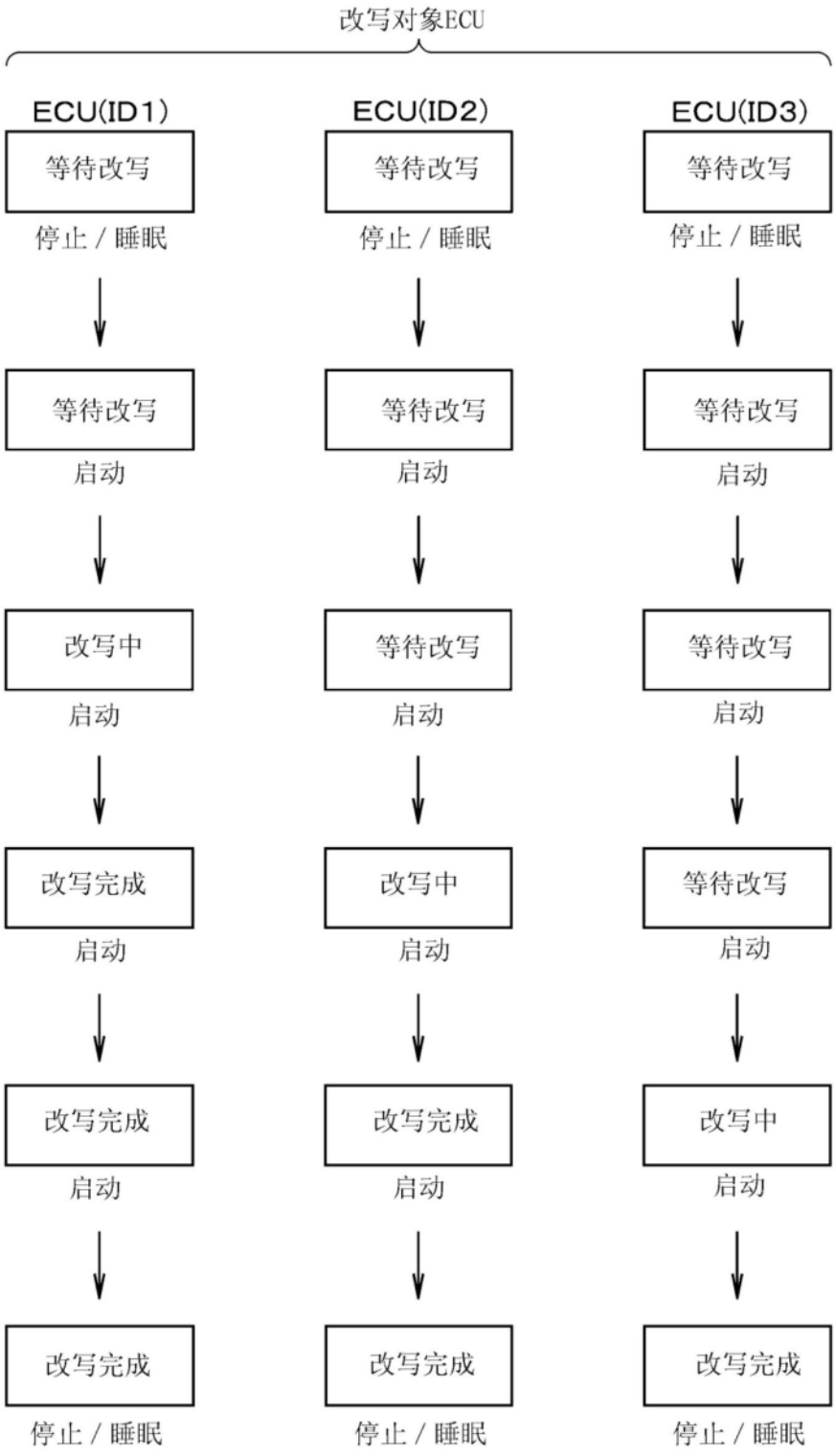

改写对象ECU
ECU(ID1)
ECU(ID2)
ECU(ID3)
等待改写
停止 / 睡眠
等待改写
启动
改写中
启动
改写完成
启动
改写完成
启动
改写完成
停止 / 睡眠

图85

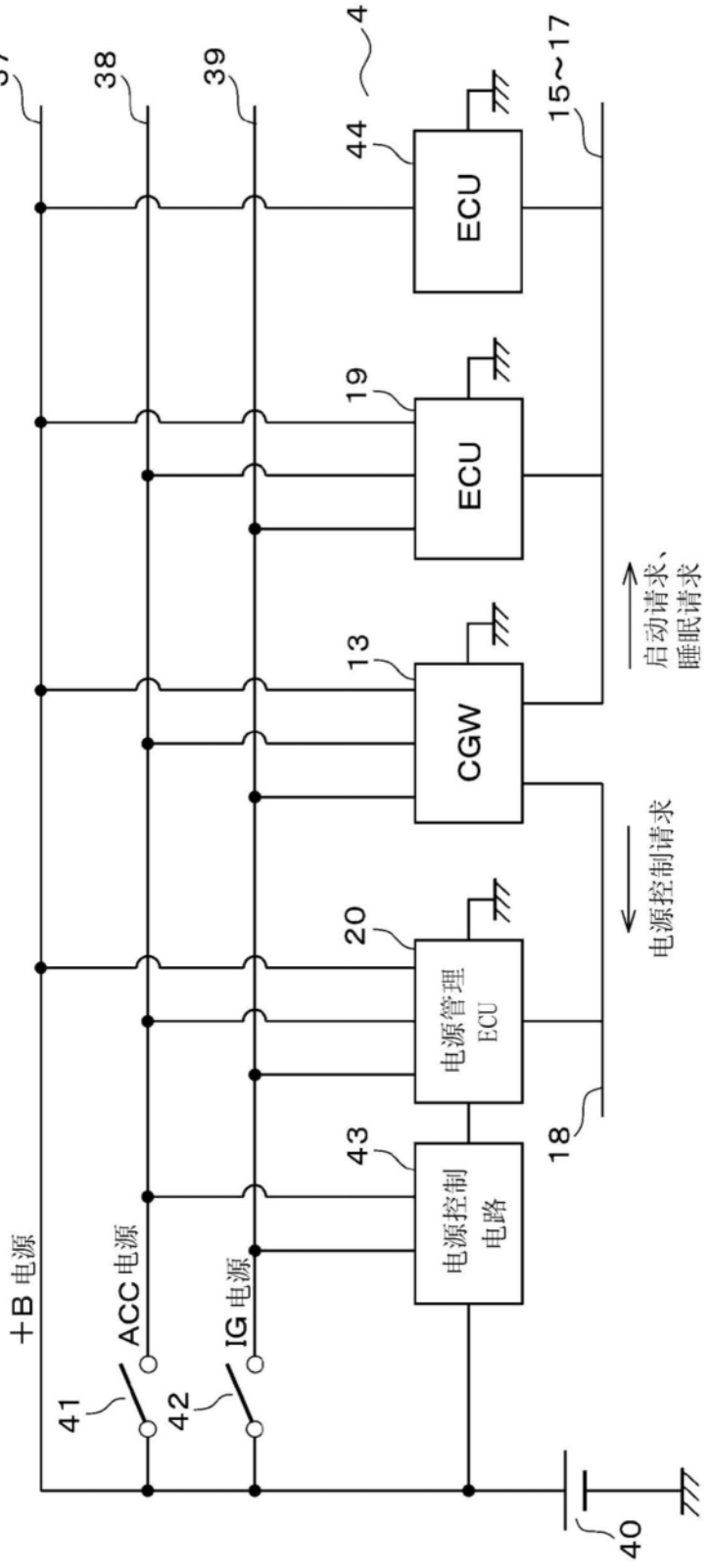

37
38
39
4
44
ECU
15~17
19
ECU
13
CGW
启动请求、
睡眠请求
20
电源管理
ECU
电源控制请求
18
43
电源控制
电路
+B 电源
ACC 电源
IG 电源
41
42
40

图86

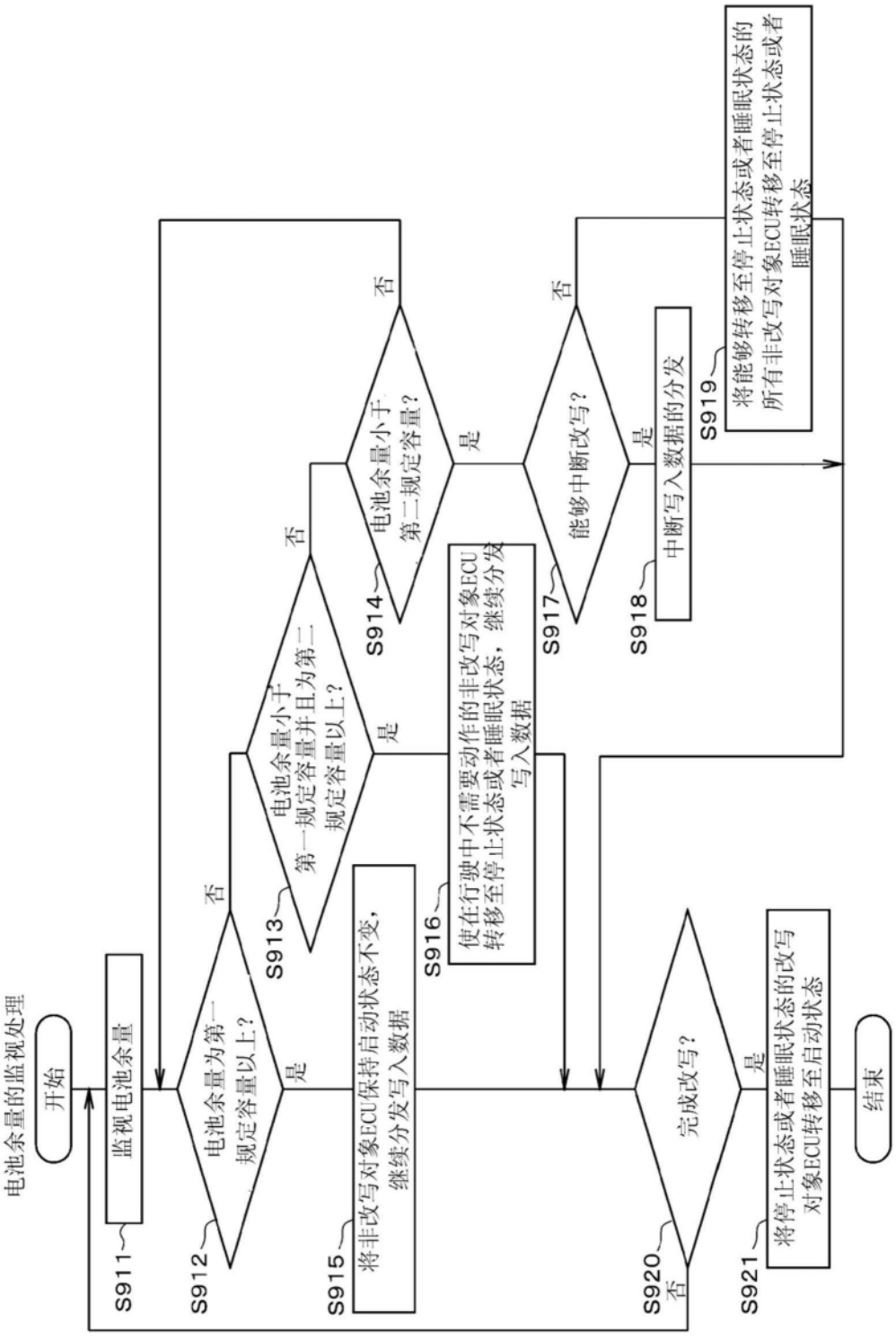

电池余量的监视处理
开始
监视电池余量
S911
电池余量为第一规定容量以上?
S912
否
是
电池余量小于第一规定容量并且为第二规定容量以上?
S913
否
是
电池余量小于第二规定容量?
S914
否
是
能够中断改写?
S917
否
是
中断写入数据的分发
S918
将能够转移至停止状态或者睡眠状态的所有非改写对象ECU转移至停止状态或者睡眠状态
S919
将非改写对象ECU保持启动状态不变，继续分发写入数据
S915
使在行驶中不需要动作的非改写对象ECU转移至停止状态或者睡眠状态，继续分发写入数据
S916
完成改写?
S920
否
是
将停止状态或者睡眠状态的改写对象ECU转移至启动状态
S921
结束

图87

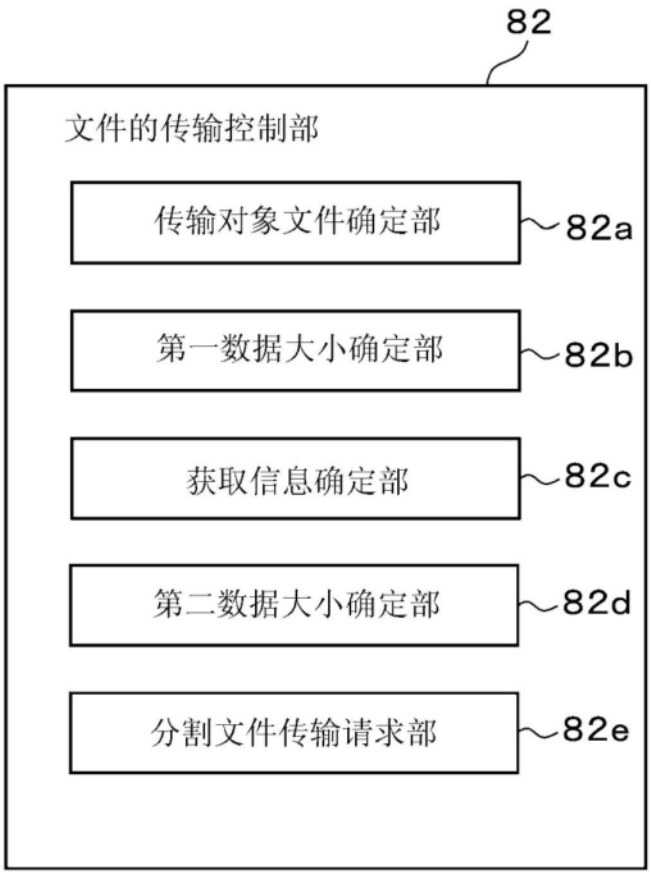

82
文件的传输控制部
传输对象文件确定部
82a
第一数据大小确定部
82b
获取信息确定部
82c
第二数据大小确定部
82d
分割文件传输请求部
82e

图88

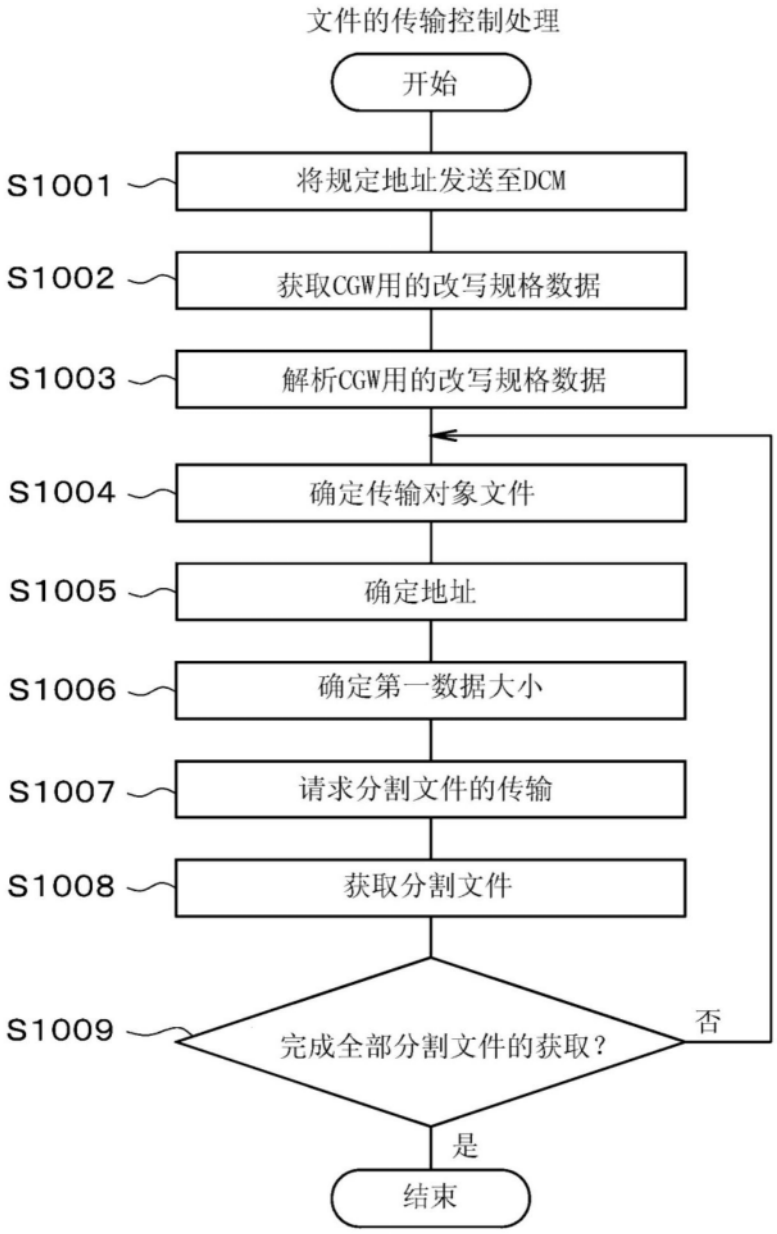

文件的传输控制处理
开始
S1001
将规定地址发送至DCM
S1002
获取CGW用的改写规格数据
S1003
解析CGW用的改写规格数据
S1004
确定传输对象文件
S1005
确定地址
S1006
确定第一数据大小
S1007
请求分割文件的传输
S1008
获取分割文件
S1009
完成全部分割文件的获取？
否
是
结束

图89

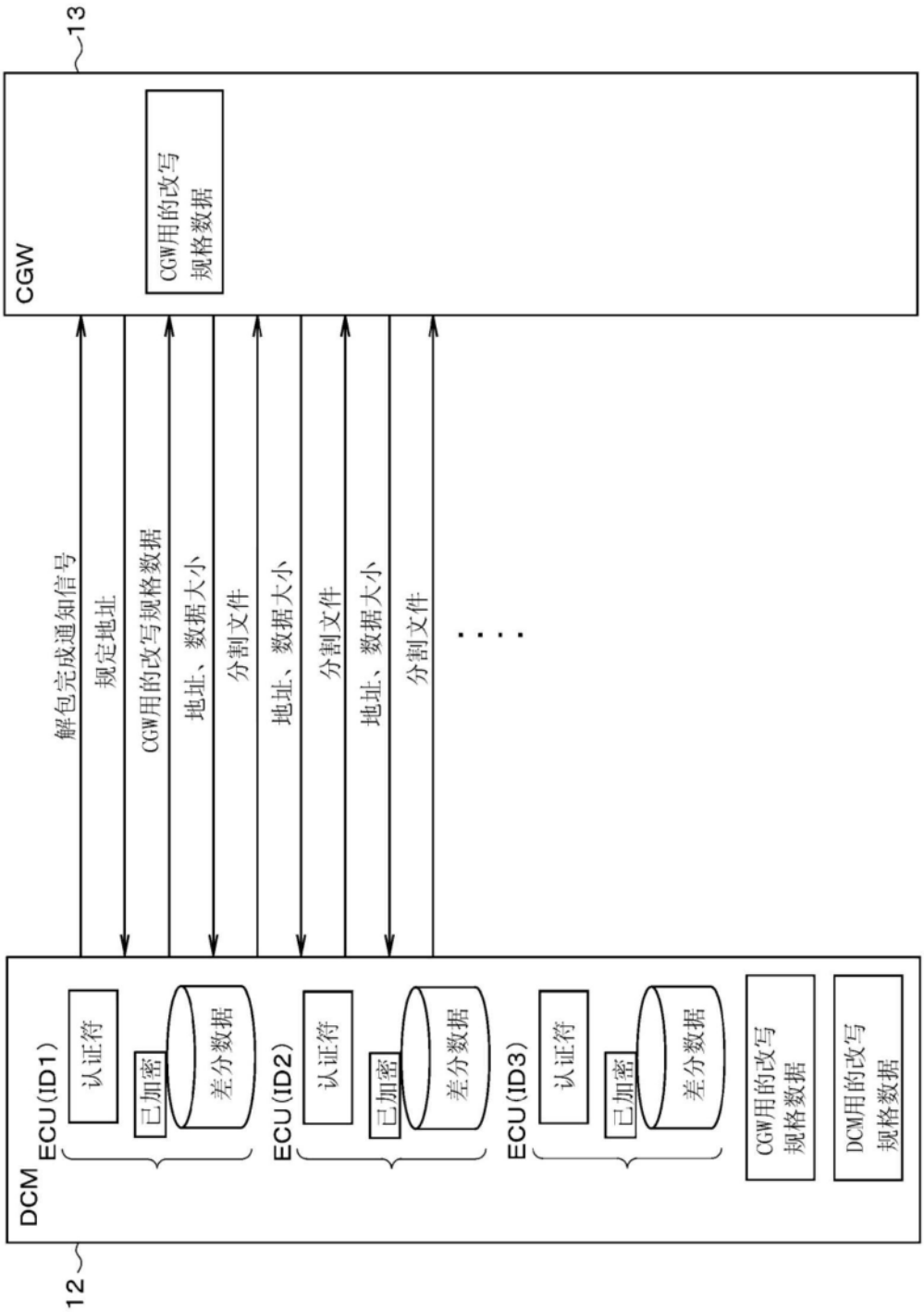

13
CGW
CGW用的改写
规格数据
解包完成通知信号
规定地址
CGW用的改写规格数据
地址、数据大小
分割文件
地址、数据大小
分割文件
地址、数据大小
分割文件
DCM
ECU(ID1)
认证符
已加密
差分数据
ECU(ID2)
认证符
已加密
差分数据
ECU(ID3)
认证符
已加密
差分数据
CGW用的改写
规格数据
DCM用的改写
规格数据
12

图90

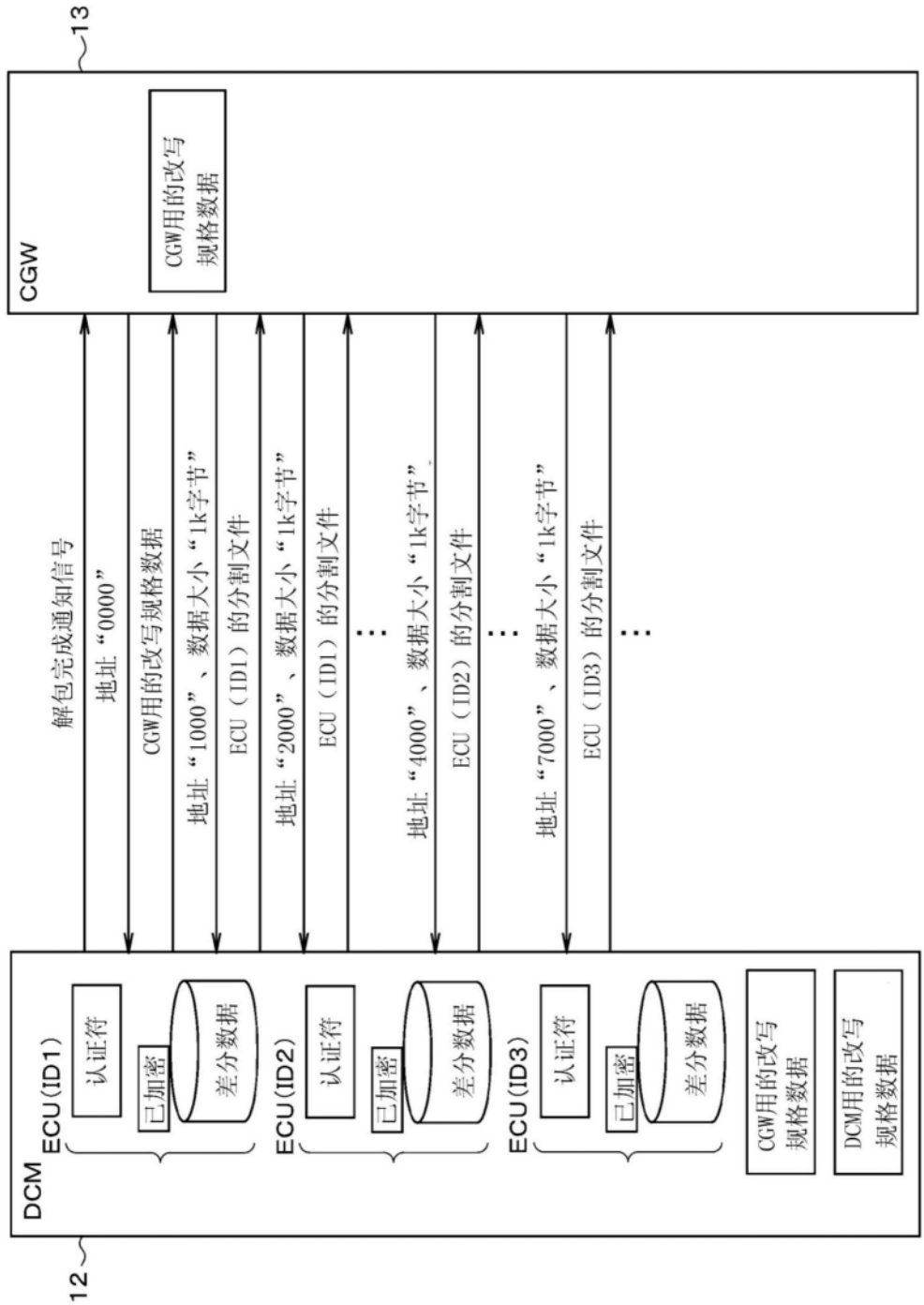

13
CGW
CGW用的改写规格数据
解包完成通知信号
地址“0000”
CGW用的改写规格数据
地址“1000”、数据大小“1k字节”
ECU（ID1）的分割文件
地址“2000”、数据大小“1k字节”
ECU（ID1）的分割文件
地址“4000”、数据大小“1k字节”
ECU（ID2）的分割文件
地址“7000”、数据大小“1k字节”
ECU（ID3）的分割文件
DCM
ECU(ID1)
认证符
已加密
差分数据
ECU(ID2)
认证符
已加密
差分数据
ECU(ID3)
认证符
已加密
差分数据
CGW用的改写规格数据
DCM用的改写规格数据
12

图91

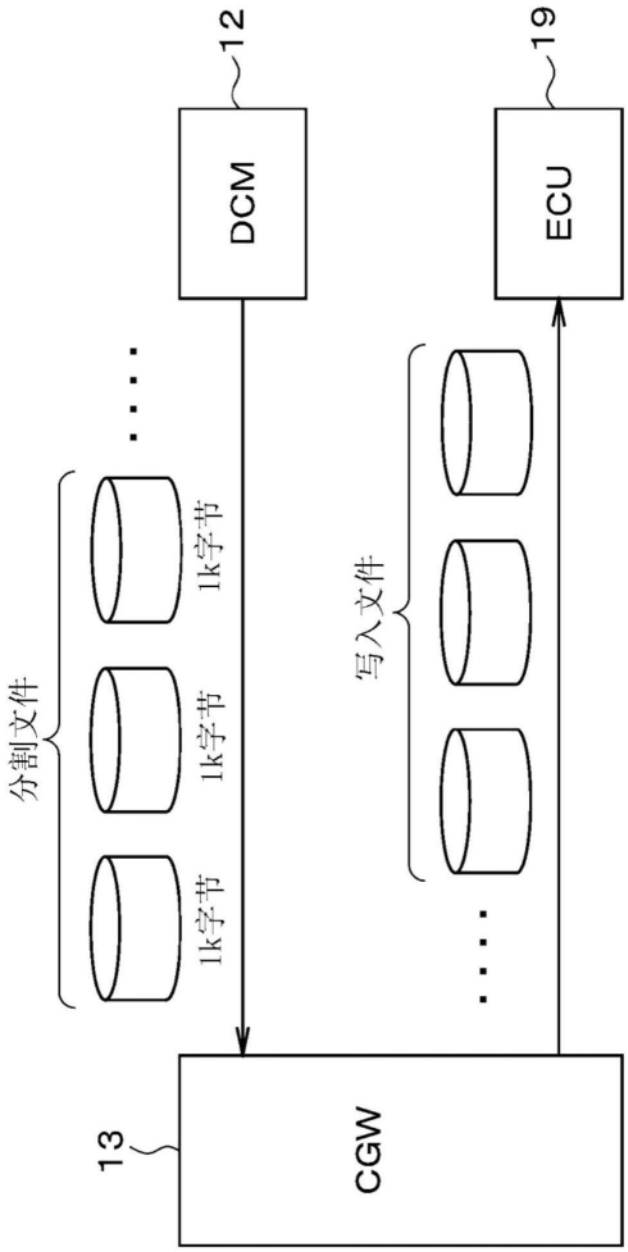


图92

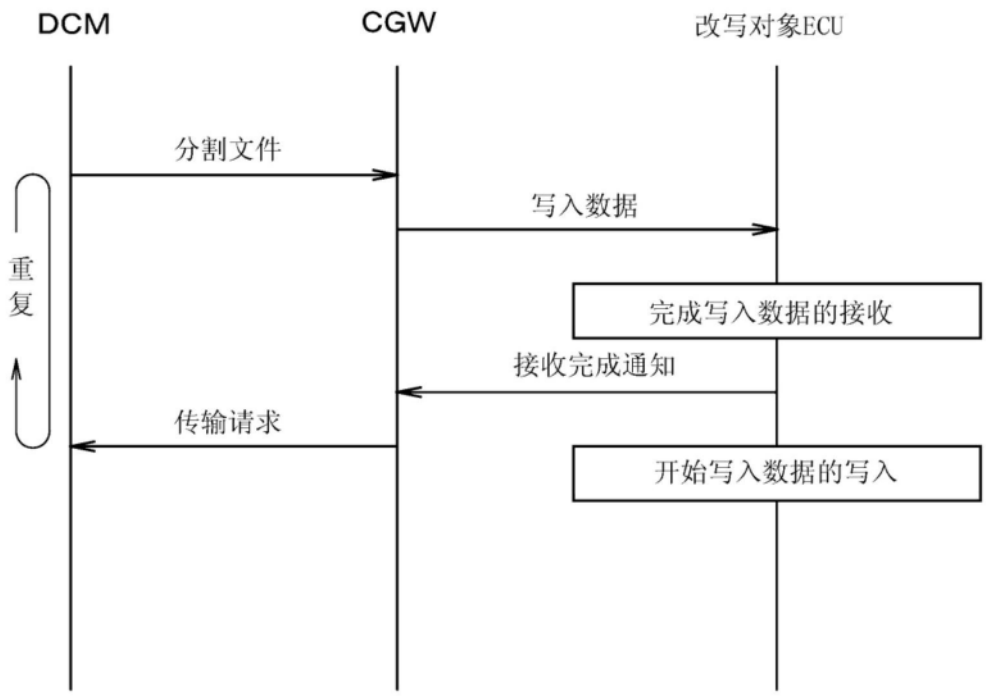

DCM
CGW
改写对象ECU
分割文件
写入数据
重复
完成写入数据的接收
接收完成通知
传输请求
开始写入数据的写入

图93

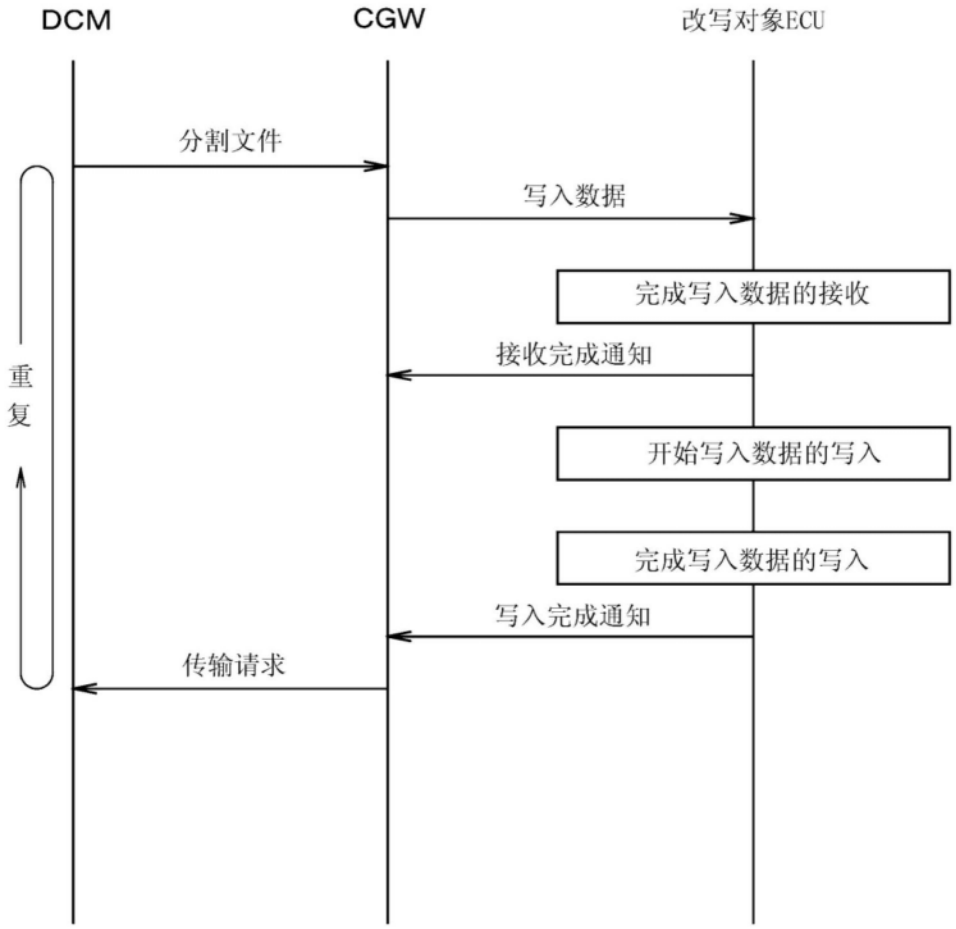

DCM
CGW
改写对象ECU
分割文件
写入数据
完成写入数据的接收
接收完成通知
重复
开始写入数据的写入
完成写入数据的写入
写入完成通知
传输请求

图94

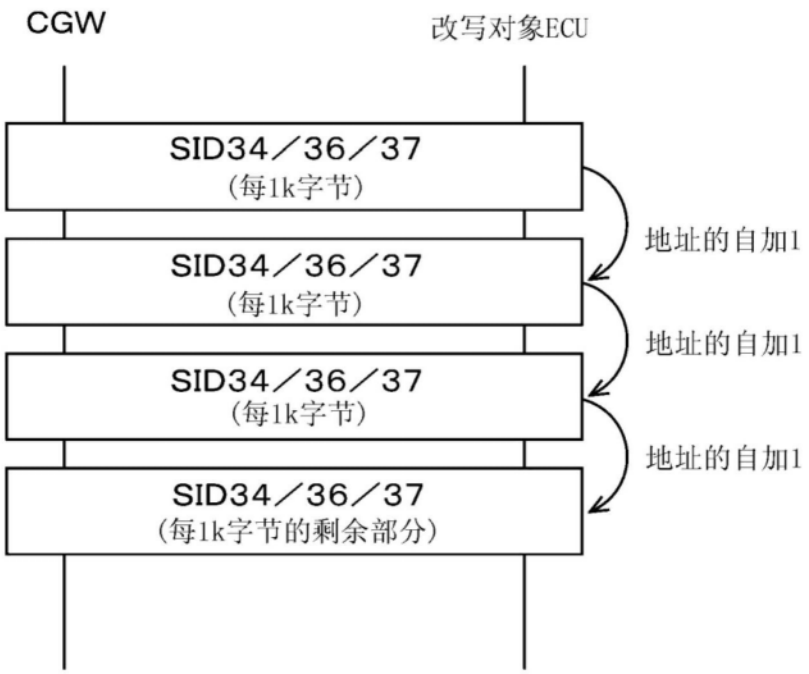

CGW
改写对象ECU
SID34／36／37
(每1k字节)
SID34／36／37
(每1k字节)
SID34／36／37
(每1k字节)
SID34／36／37
(每1k字节的剩余部分)
地址的自加1
地址的自加1
地址的自加1

图95

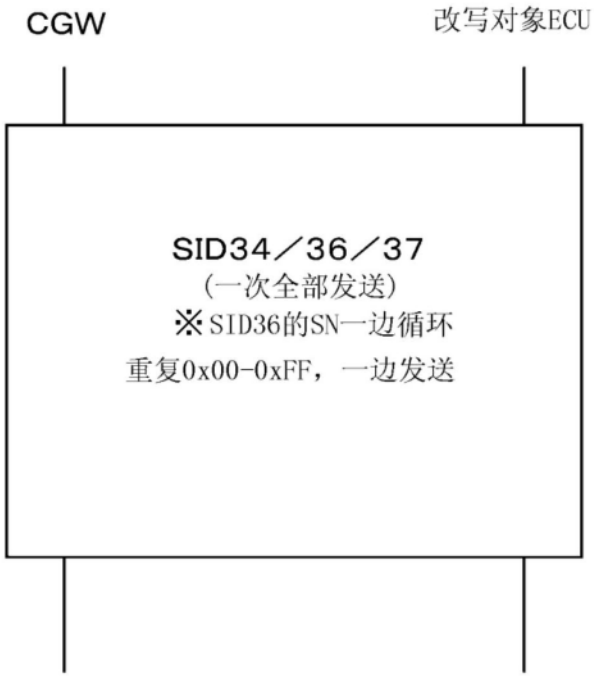

CGW
改写对象ECU
SID34／36／37
(一次全部发送)
※SID36的SN一边循环
重复0x00-0xFF，一边发送

图96

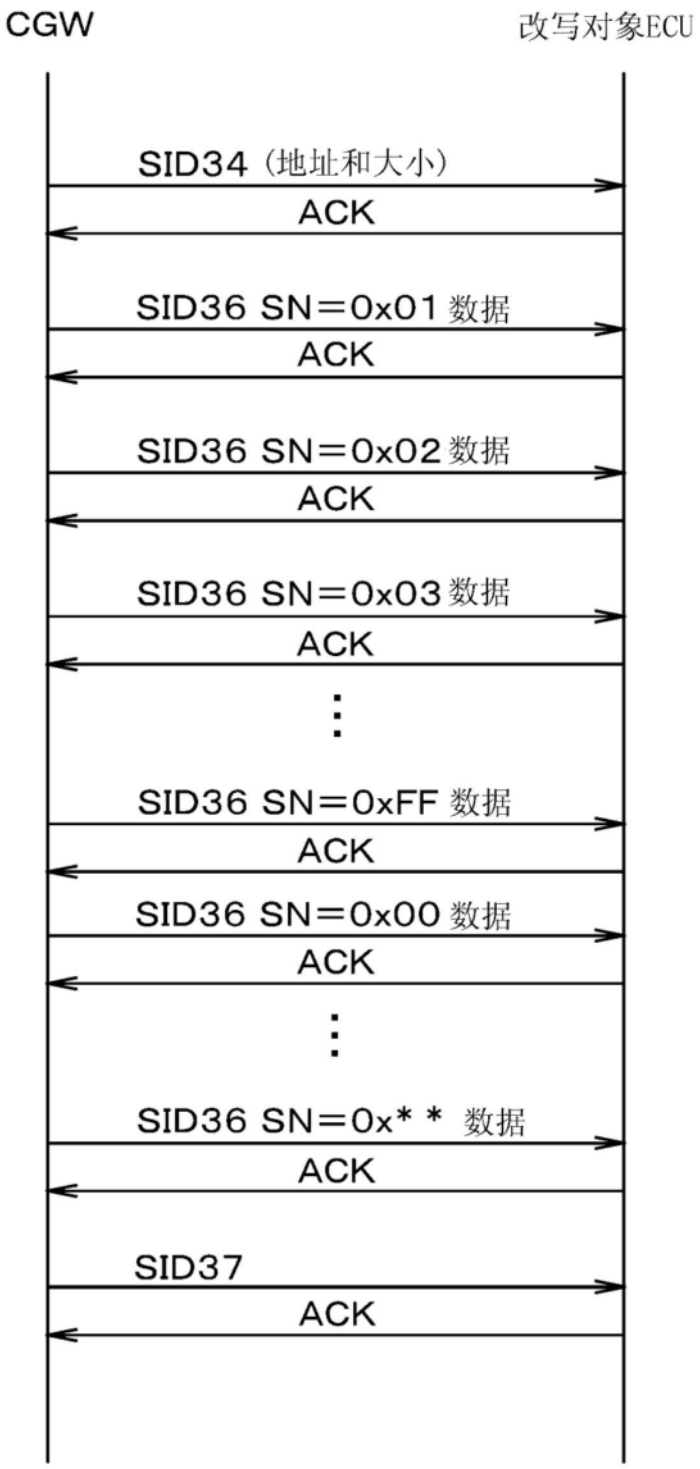

CGW
改写对象ECU
SID34（地址和大小）
ACK
SID36 SN＝0x01 数据
ACK
SID36 SN＝0x02 数据
ACK
SID36 SN＝0x03 数据
ACK
SID36 SN＝0xFF 数据
ACK
SID36 SN＝0x00 数据
ACK
SID36 SN＝0x* * 数据
ACK
SID37
ACK

图97

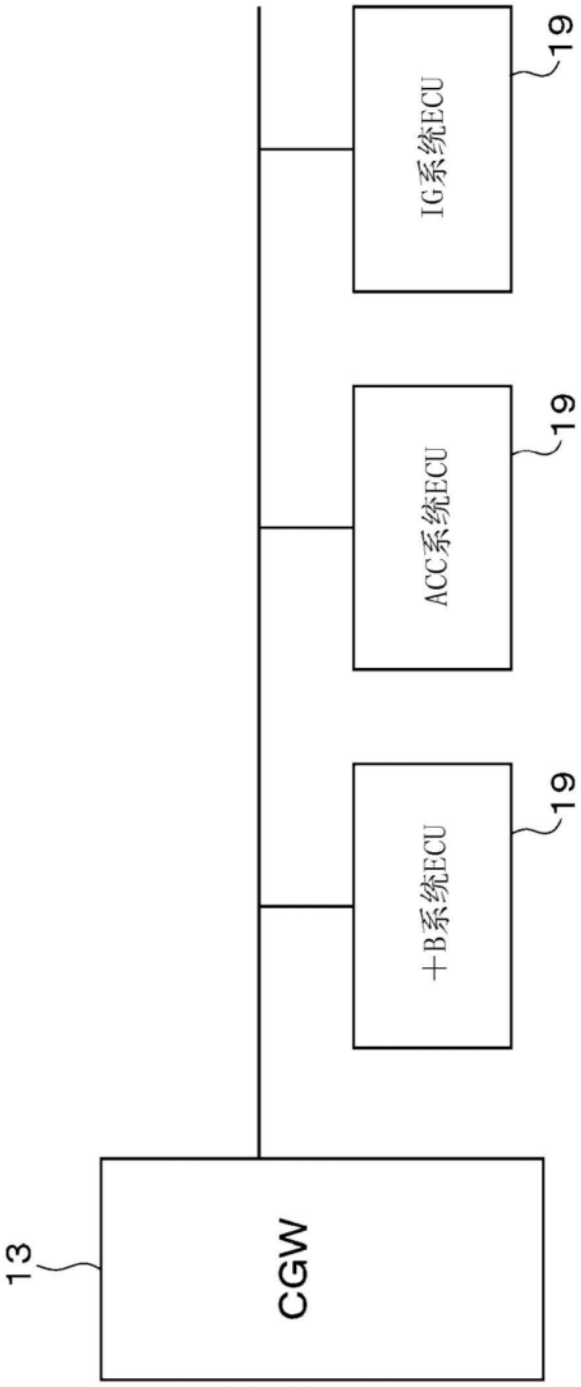


图98

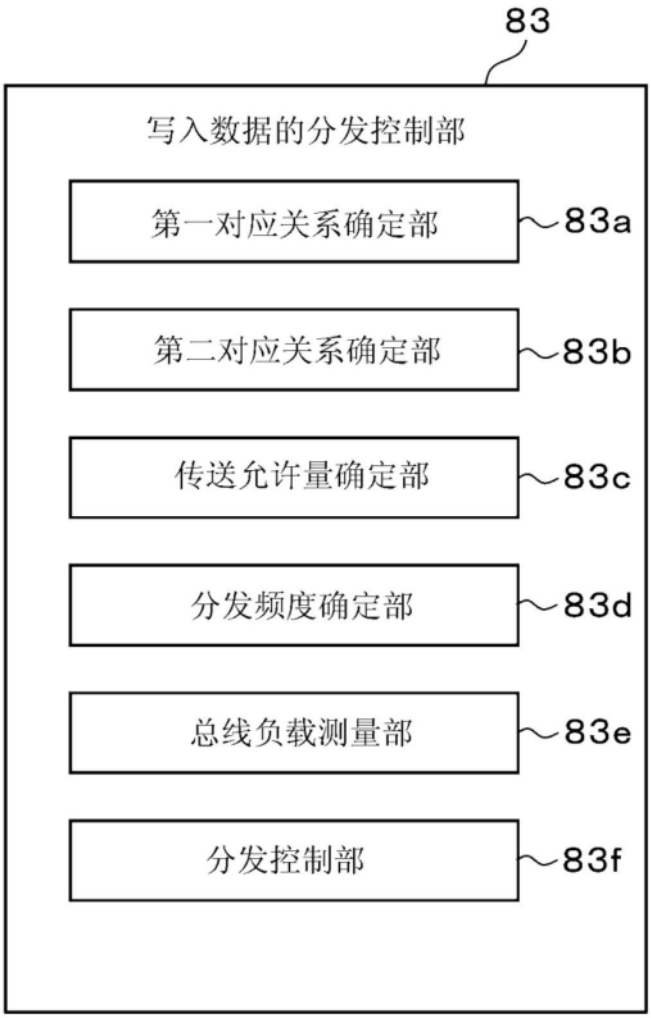

83
写入数据的分发控制部
第一对应关系确定部
83a
第二对应关系确定部
83b
传送允许量确定部
83c
分发频度确定部
83d
总线负载测量部
83e
分发控制部
83f

图99

总线负载表（第一对应关系）

传送允许量		第一总线	第二总线	第三总线
IG 电源状态	车辆控制数据	50%	20%	40%
	写入数据	30%	50%	50%
ACC 电源状态	车辆控制数据	30%	30%	20%
	写入数据	50%	40%	70%
+B 电源状态	车辆控制数据	20%	10%	50%
	写入数据	60%	60%	40%

图100

改写对象ECU所属表（第二对应关系）

	所属总线	+B 电源状态	ACC 电源状态	IG 电源状态
第一改写对象ECU	第一总线	启动	启动	启动
第二改写对象ECU	第二总线	睡眠	启动	启动
第三改写对象ECU	第三总线	睡眠	睡眠	启动

图101

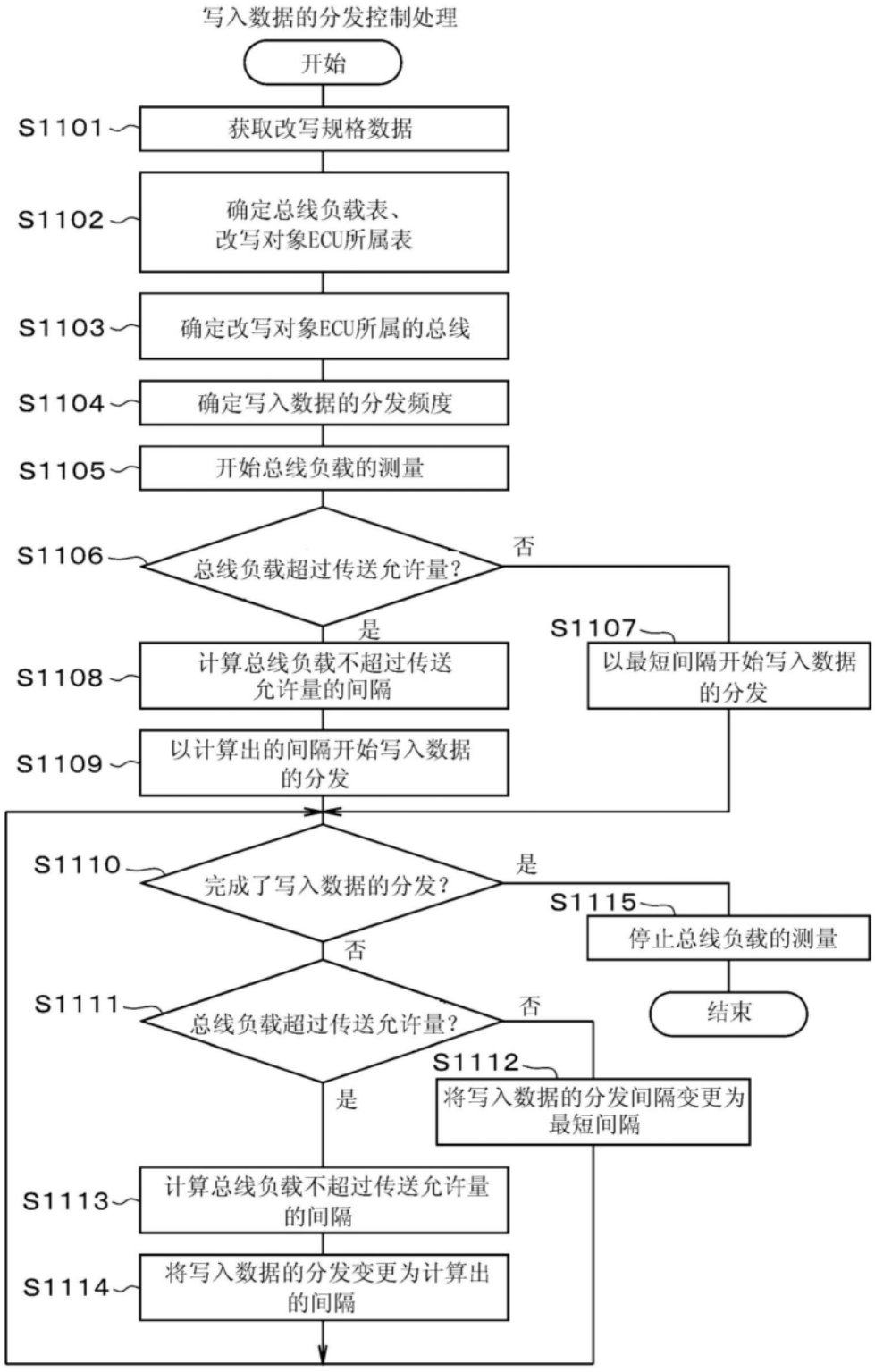

写入数据的分发控制处理
开始
S1101
获取改写规格数据
S1102
确定总线负载表、
改写对象ECU所属表
S1103
确定改写对象ECU所属的总线
S1104
确定写入数据的分发频度
S1105
开始总线负载的测量
S1106
总线负载超过传送允许量?
否
是
S1107
以最短间隔开始写入数据
的分发
S1108
计算总线负载不超过传送
允许量的间隔
S1109
以计算出的间隔开始写入数据
的分发
S1110
完成了写入数据的分发?
是
S1115
停止总线负载的测量
结束
否
S1111
总线负载超过传送允许量?
否
S1112
将写入数据的分发间隔变更为
最短间隔
是
S1113
计算总线负载不超过传送允许量
的间隔
S1114
将写入数据的分发变更为计算出
的间隔

图102

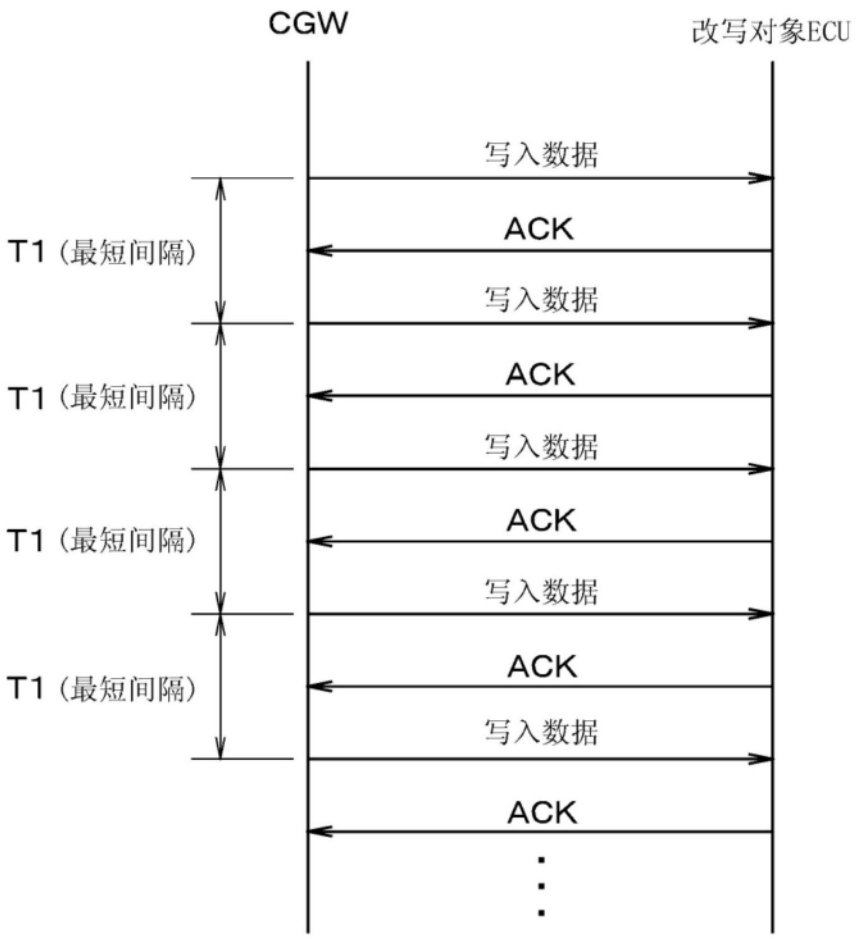

CGW
改写对象ECU
写入数据
ACK
T1（最短间隔）
写入数据
ACK
T1（最短间隔）
写入数据
ACK
T1（最短间隔）
写入数据
ACK
T1（最短间隔）
写入数据
ACK

图103

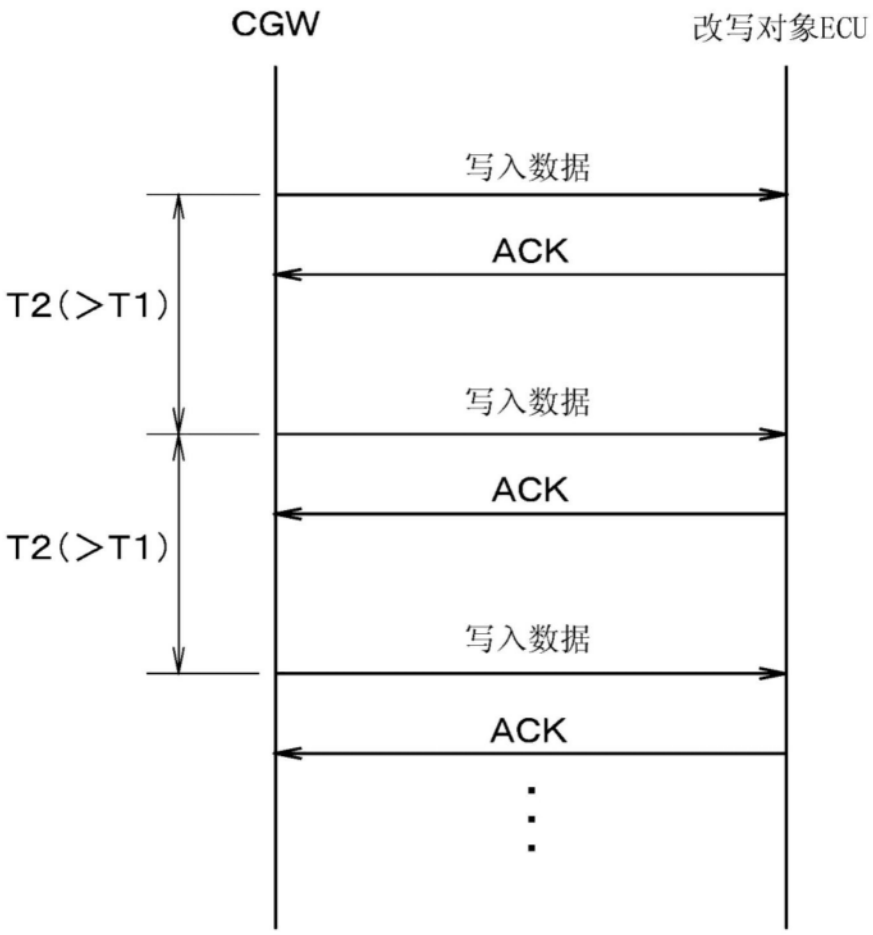


图104

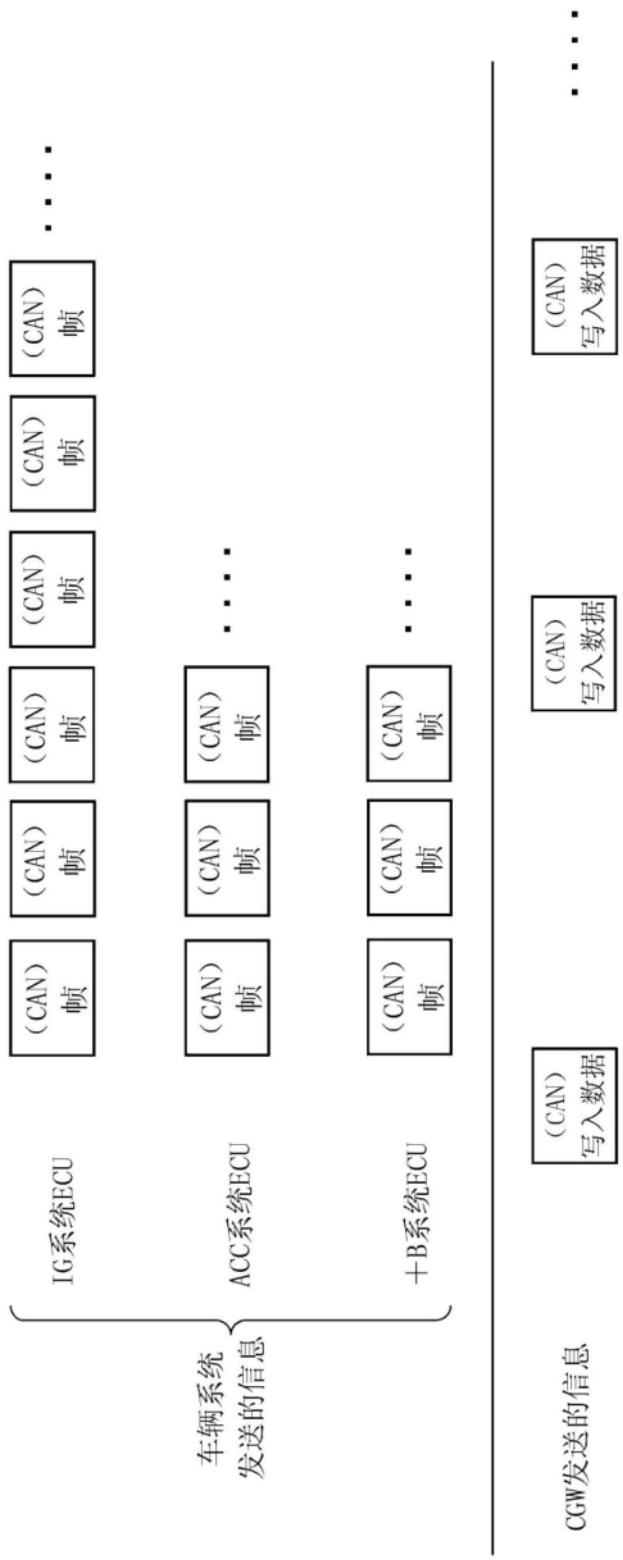


图105

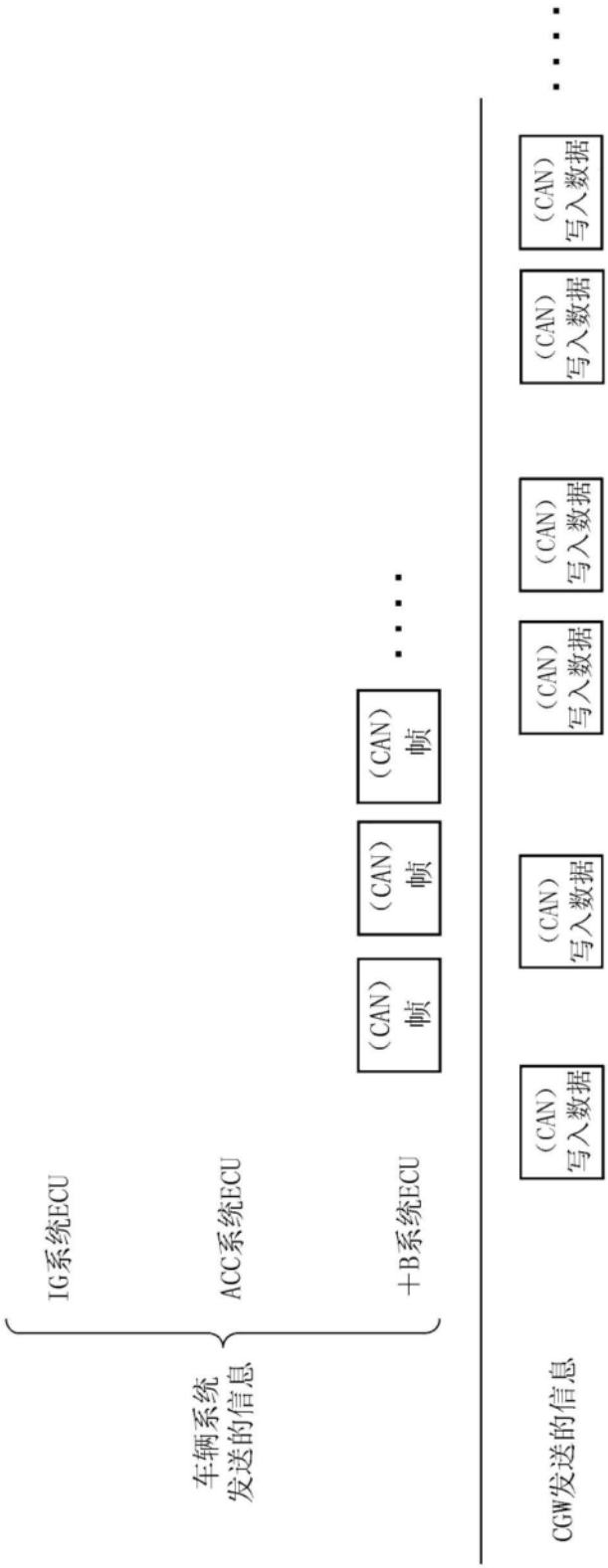


图106

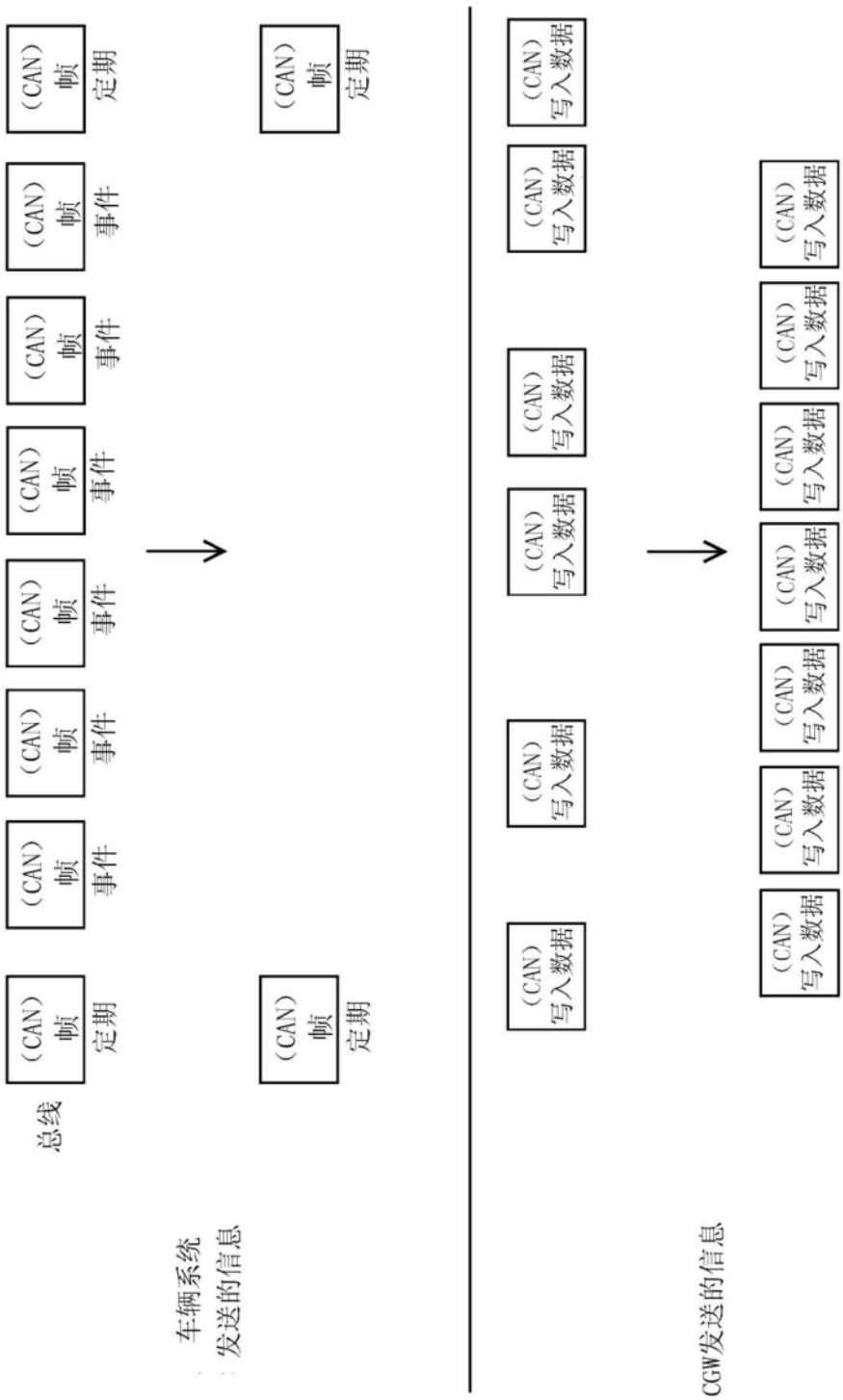


图107

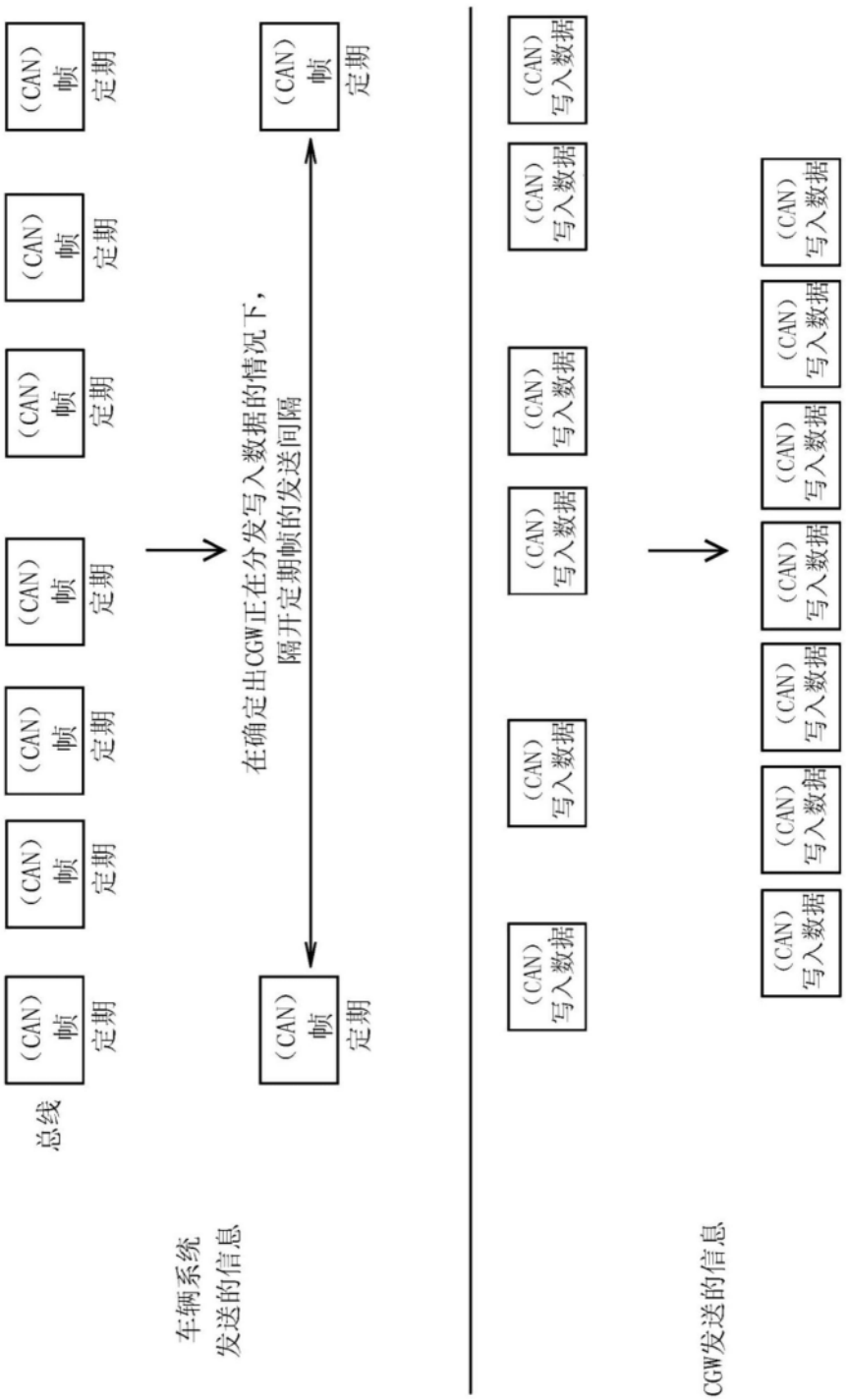

总线
车辆系统
发送的信息
(CAN)
帧
定期
在确定出CGW正在分发写入数据的情况下，
隔开定期帧的发送间隔
CGW发送的信息
(CAN)
写入数据

图108

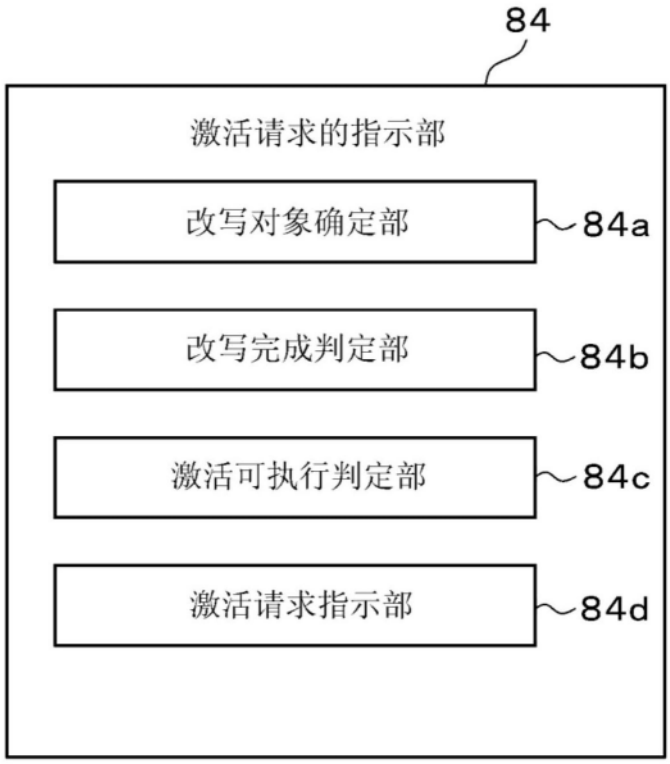

84
激活请求的指示部
改写对象确定部
84a
改写完成判定部
84b
激活可执行判定部
84c
激活请求指示部
84d

图109

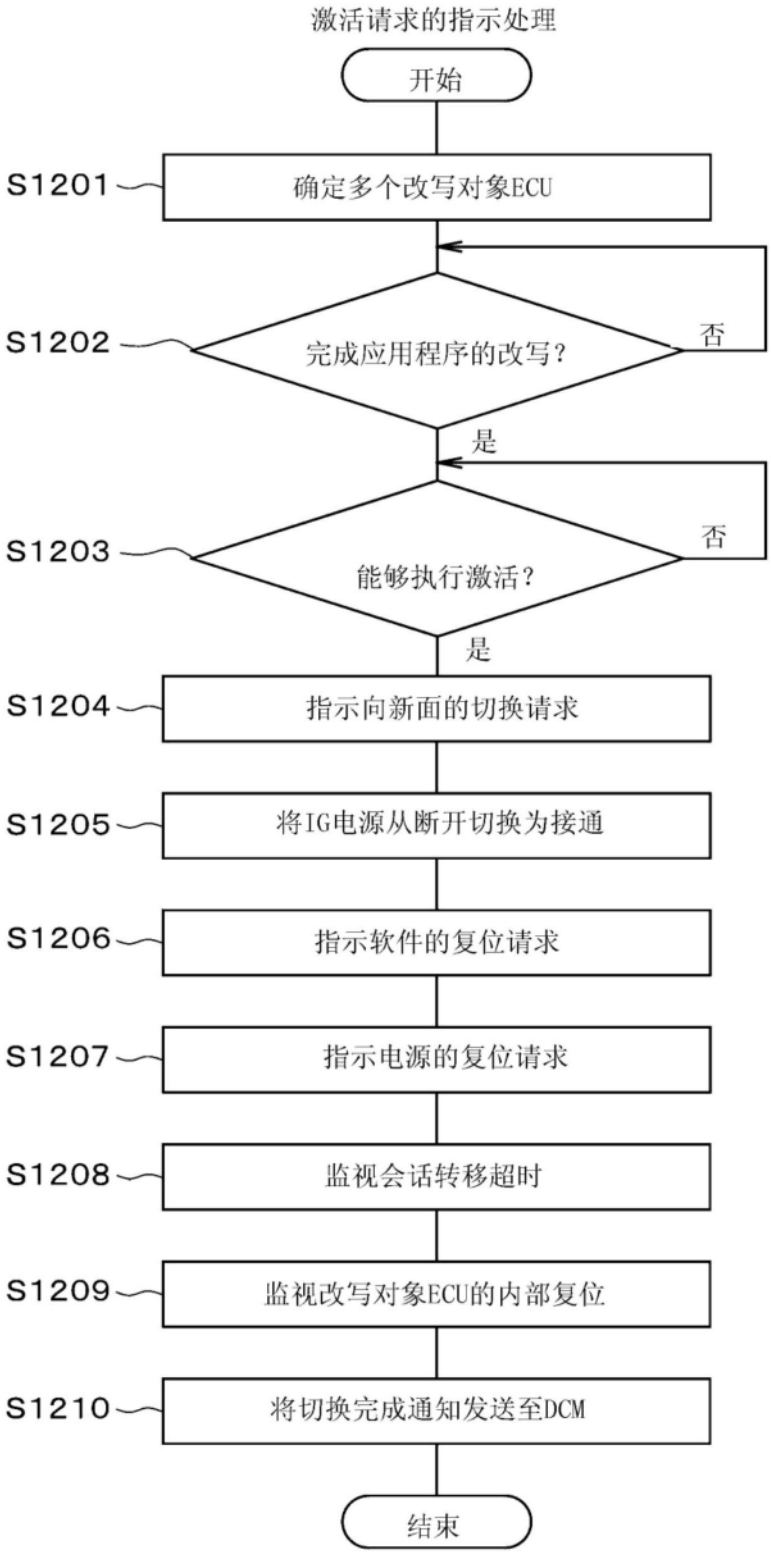

激活请求的指示处理
开始
S1201
确定多个改写对象ECU
S1202
完成应用程序的改写？
否
是
S1203
能够执行激活？
否
是
S1204
指示向新面的切换请求
S1205
将IG电源从断开切换为接通
S1206
指示软件的复位请求
S1207
指示电源的复位请求
S1208
监视会话转移超时
S1209
监视改写对象ECU的内部复位
S1210
将切换完成通知发送至DCM
结束

图110

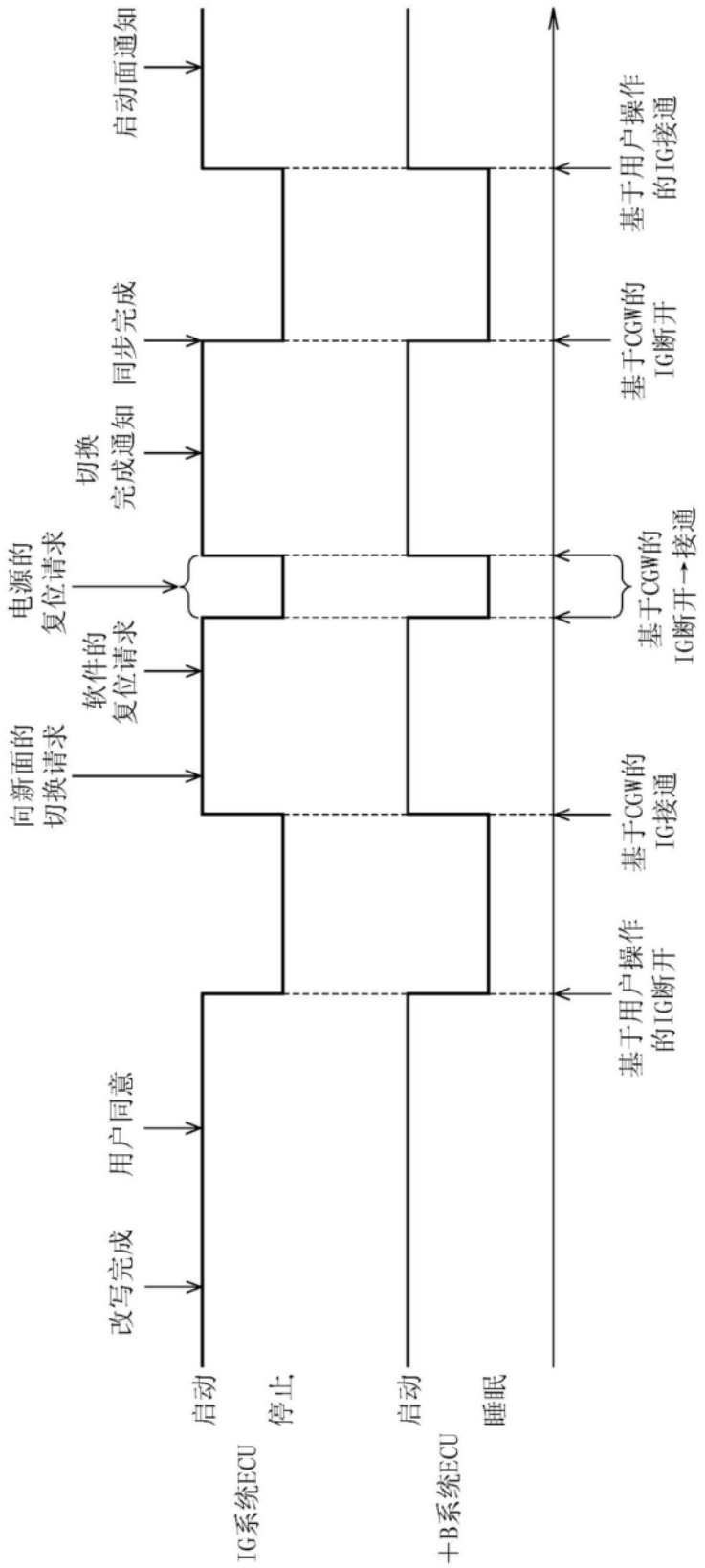

IG系统ECU
+B系统ECU
启动
停止
启动
睡眠
改写完成
用户同意
向新面的
切换请求
软件的
复位请求
电源的
复位请求
切换
完成通知
同步完成
启动面通知
基于用户操作
的IG断开
基于CGW的
IG接通
基于CGW的
IG断开→接通
基于CGW的
IG断开
基于用户操作
的IG接通

图111

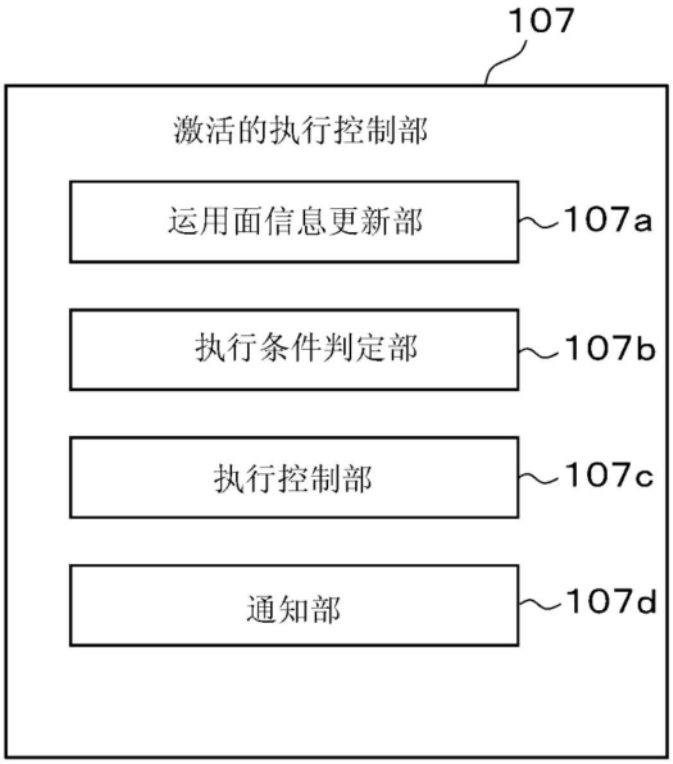

107
激活的执行控制部
运用面信息更新部
107a
执行条件判定部
107b
执行控制部
107c
通知部
107d

图112

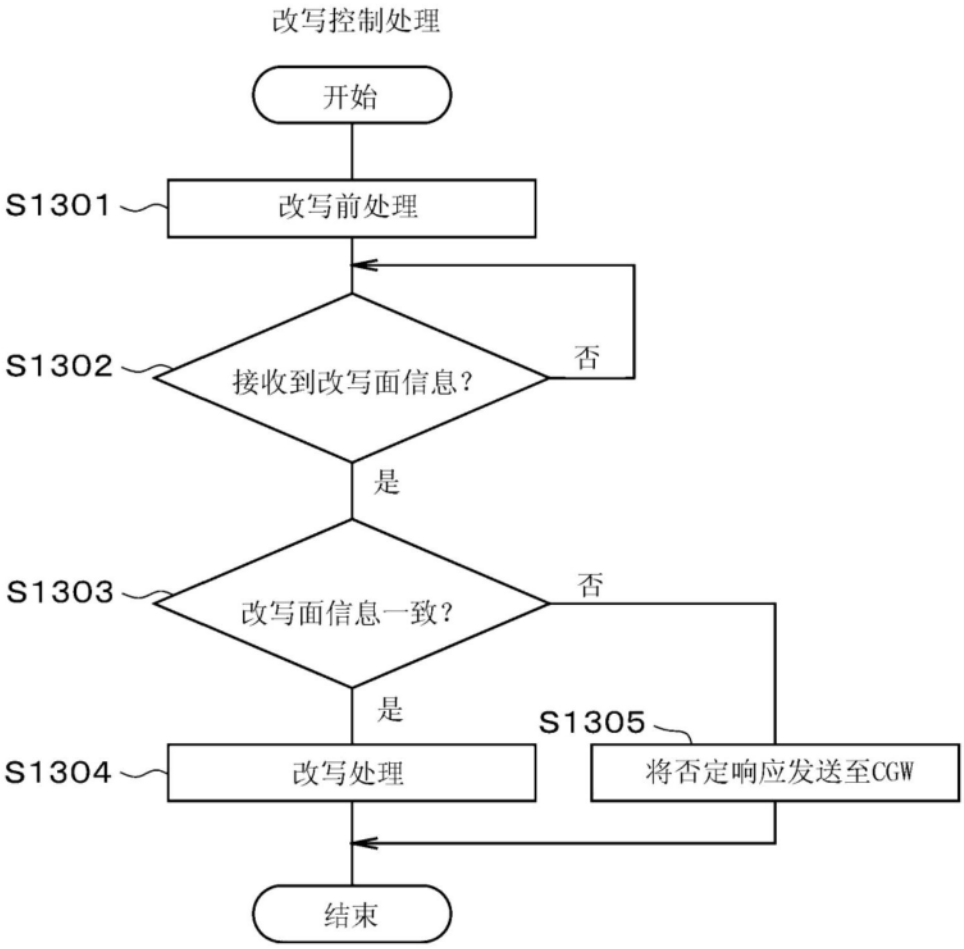

改写控制处理
开始
S1301
改写前处理
S1302
接收到改写面信息？
否
是
S1303
改写面信息一致？
否
是
S1305
S1304
改写处理
将否定响应发送至CGW
结束

图113

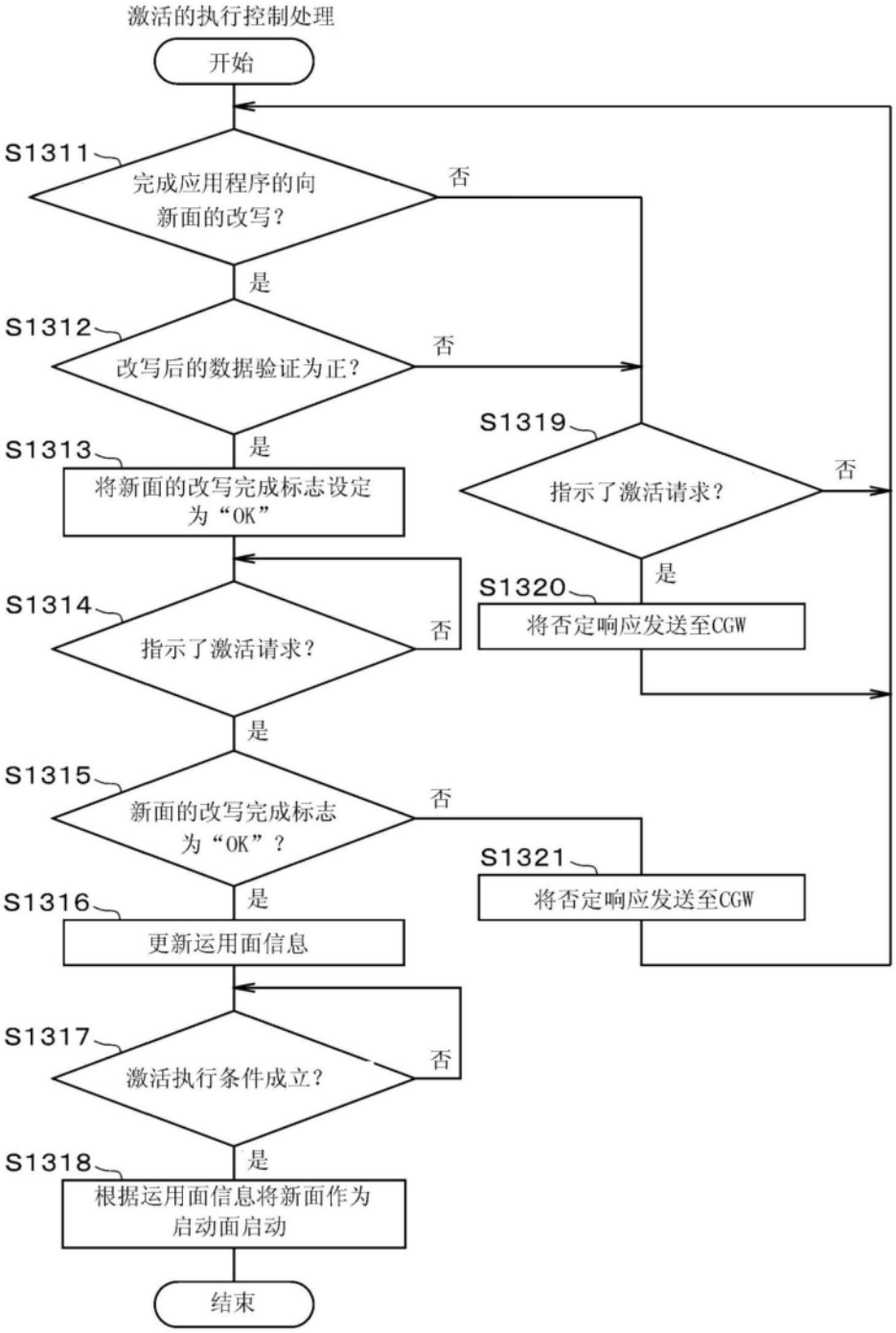

激活的执行控制处理
开始
S1311
完成应用程序的向新面的改写？
否
是
S1312
改写后的数据验证为正？
否
是
S1313
将新面的改写完成标志设定为“OK”
S1314
指示了激活请求？
否
是
S1315
新面的改写完成标志为“OK”？
否
是
S1316
更新运用面信息
S1317
激活执行条件成立？
否
是
S1318
根据运用面信息将新面作为启动面启动
结束
S1319
指示了激活请求？
否
是
S1320
将否定响应发送至CGW
S1321
将否定响应发送至CGW

图114

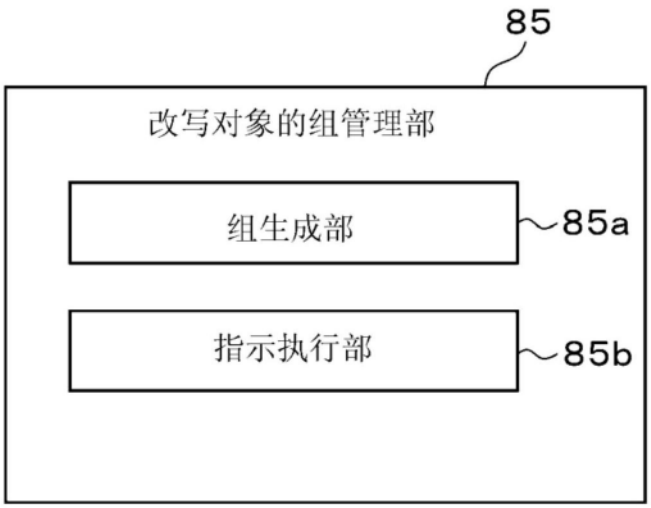


图115

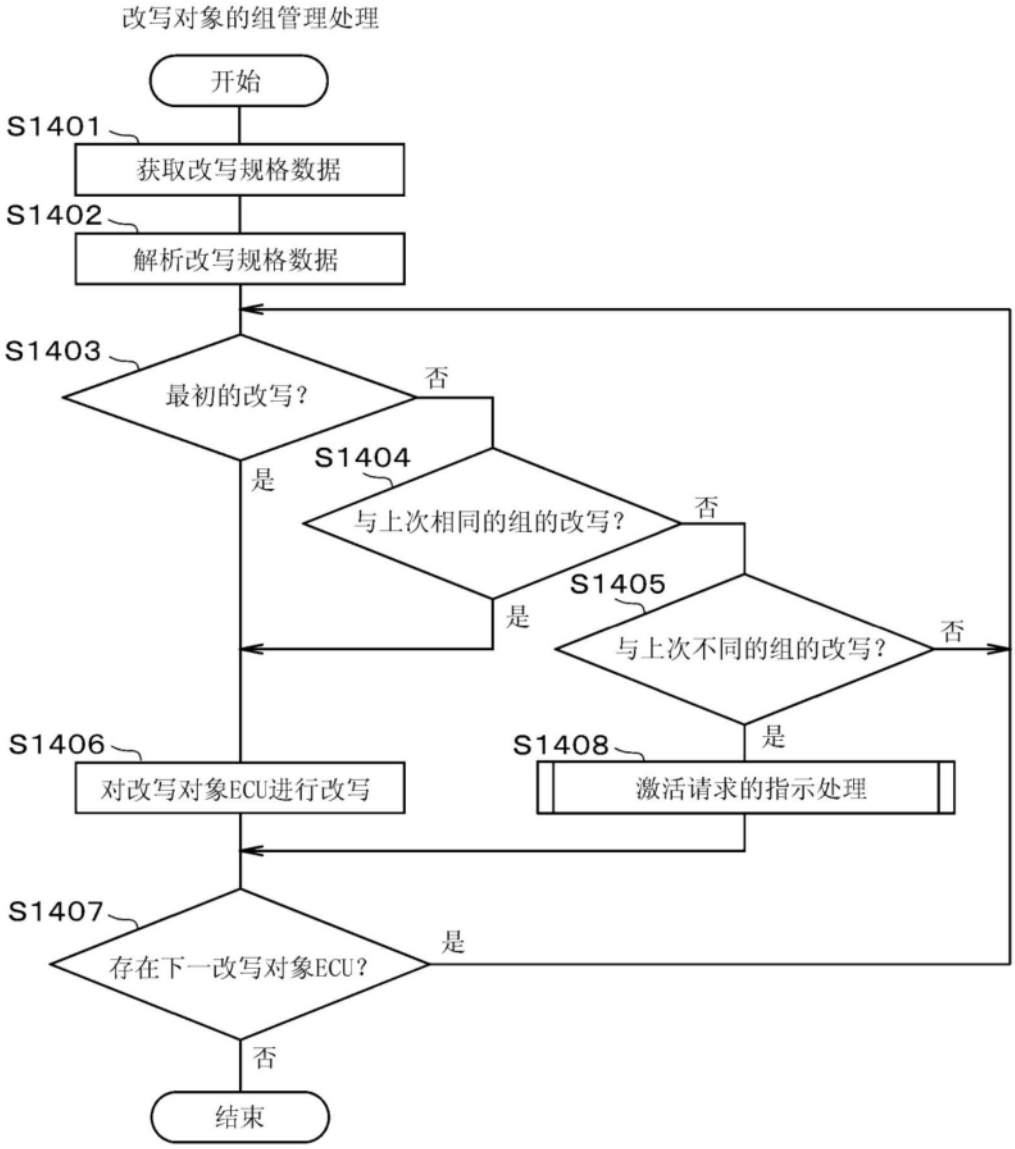

改写对象的组管理处理
开始
S1401
获取改写规格数据
S1402
解析改写规格数据
S1403
最初的改写？
否
是
S1404
与上次相同的组的改写？
否
是
S1405
与上次不同的组的改写？
否
是
S1406
对改写对象ECU进行改写
S1408
激活请求的指示处理
S1407
存在下一改写对象ECU？
是
否
结束

图116

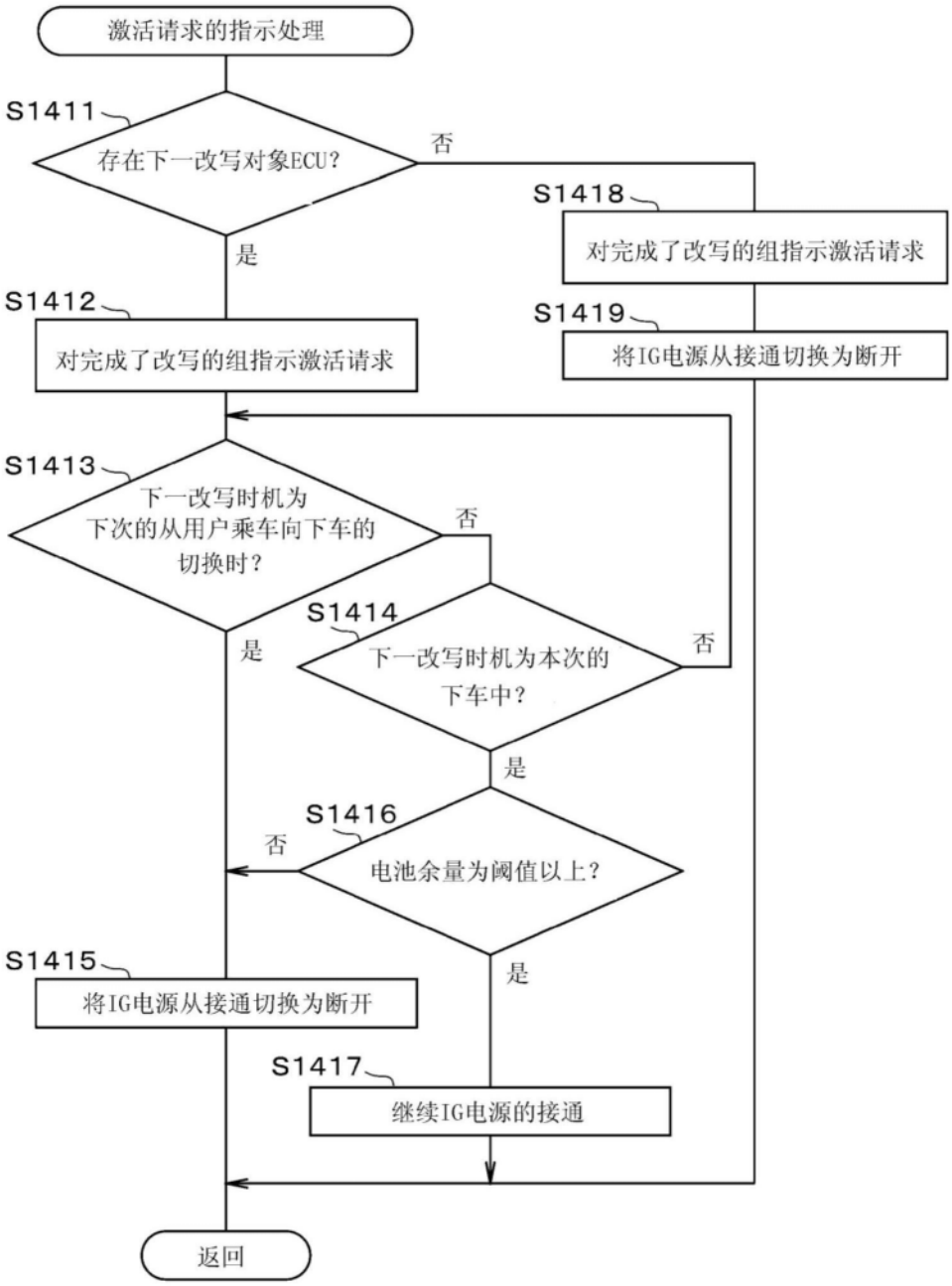

激活请求的指示处理
S1411
存在下一改写对象ECU?
否
是
S1418
对完成了改写的组指示激活请求
S1412
对完成了改写的组指示激活请求
S1419
将IG电源从接通切换为断开
S1413
下一改写时机为
下次的从用户乘车向下车的
切换时?
否
是
S1414
下一改写时机为本次的
下车中?
否
是
S1416
否
电池余量为阈值以上?
是
S1415
将IG电源从接通切换为断开
S1417
继续IG电源的接通
返回

图117

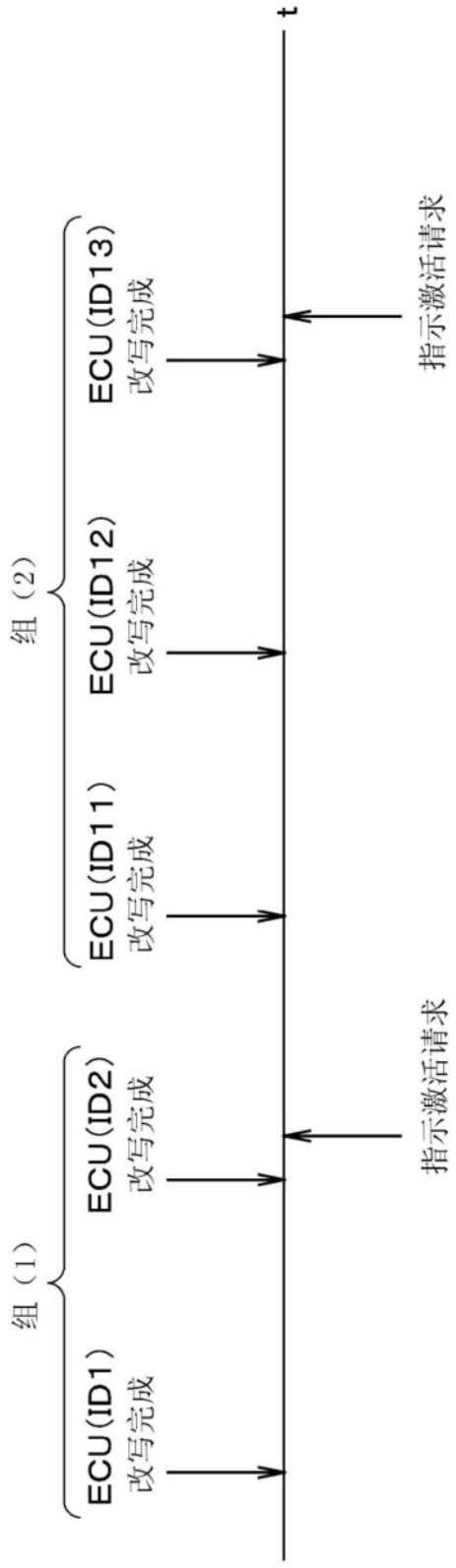

t
组（1）
ECU(ID1)
改写完成
ECU(ID2)
改写完成
指示激活请求
组（2）
ECU(ID11)
改写完成
ECU(ID12)
改写完成
ECU(ID13)
改写完成
指示激活请求

图118

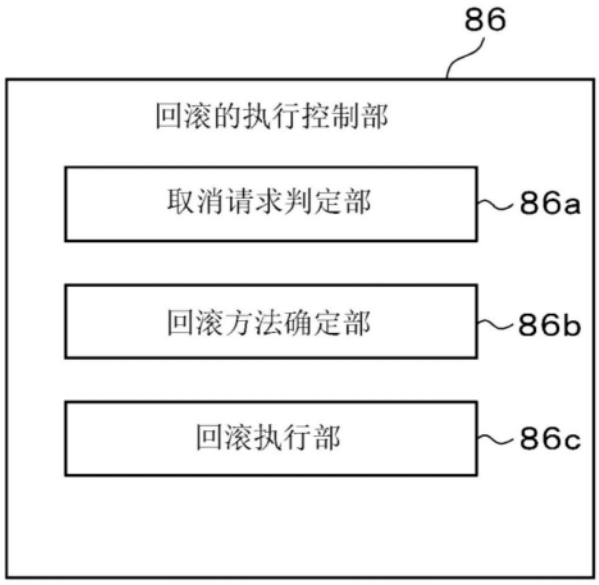

86
回滚的执行控制部
取消请求判定部
86a
回滚方法确定部
86b
回滚执行部
86c

图119

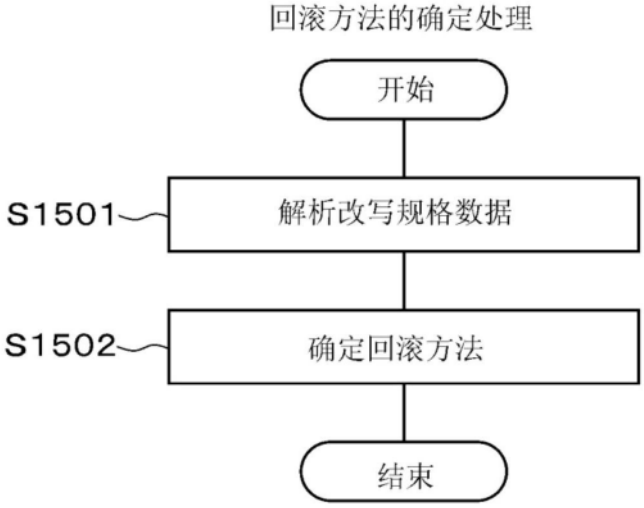

回滚方法的确定处理
开始
S1501
解析改写规格数据
S1502
确定回滚方法
结束

图120

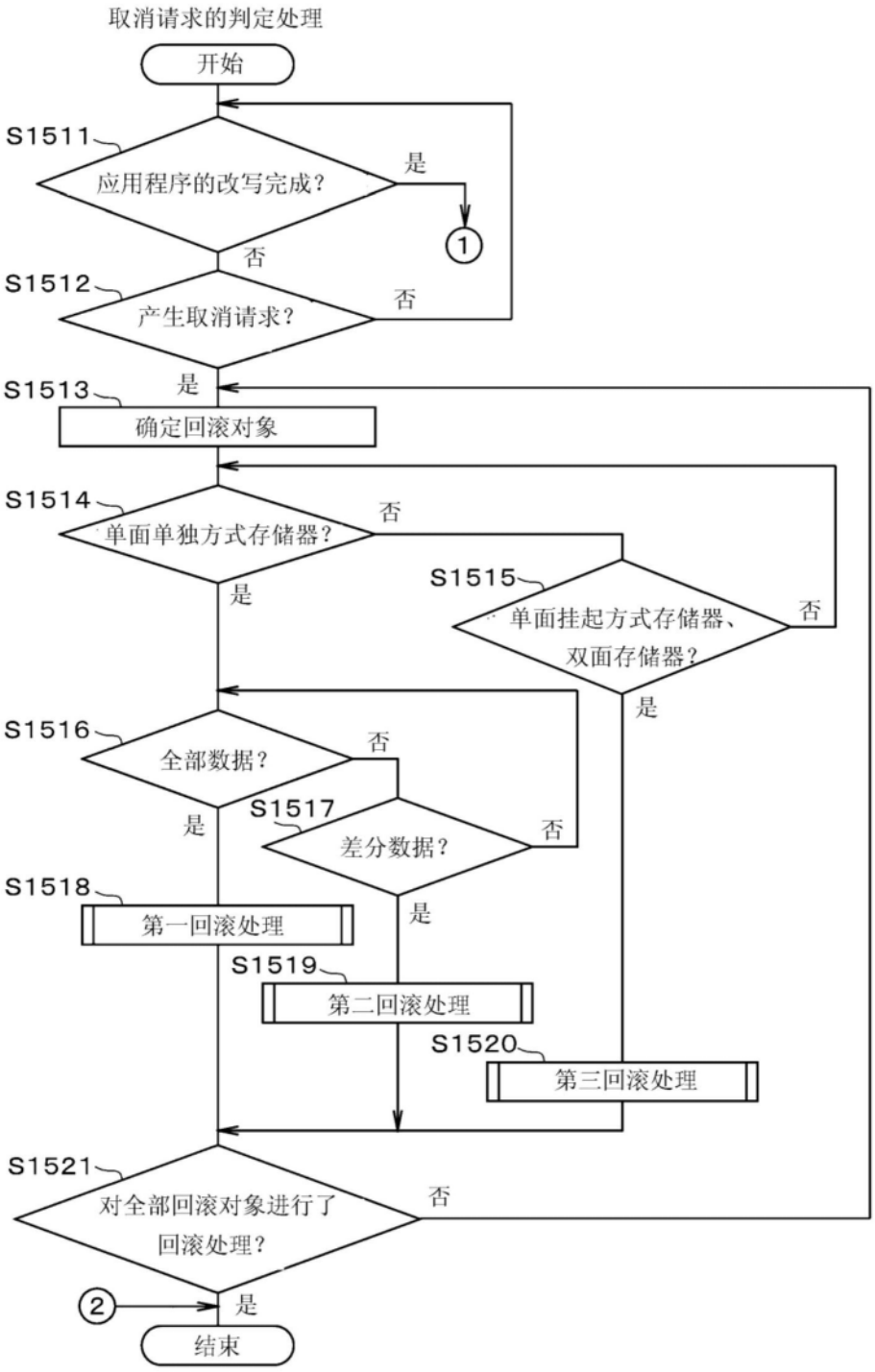

取消请求的判定处理
开始
S1511
应用程序的改写完成？
是
否
①
S1512
产生取消请求？
否
是
S1513
确定回滚对象
S1514
单面单独方式存储器？
否
是
S1515
单面挂起方式存储器、
双面存储器？
否
是
S1516
全部数据？
否
是
S1517
差分数据？
否
是
S1518
第一回滚处理
S1519
第二回滚处理
S1520
第三回滚处理
S1521
对全部回滚对象进行了
回滚处理？
否
②
是
结束

图121

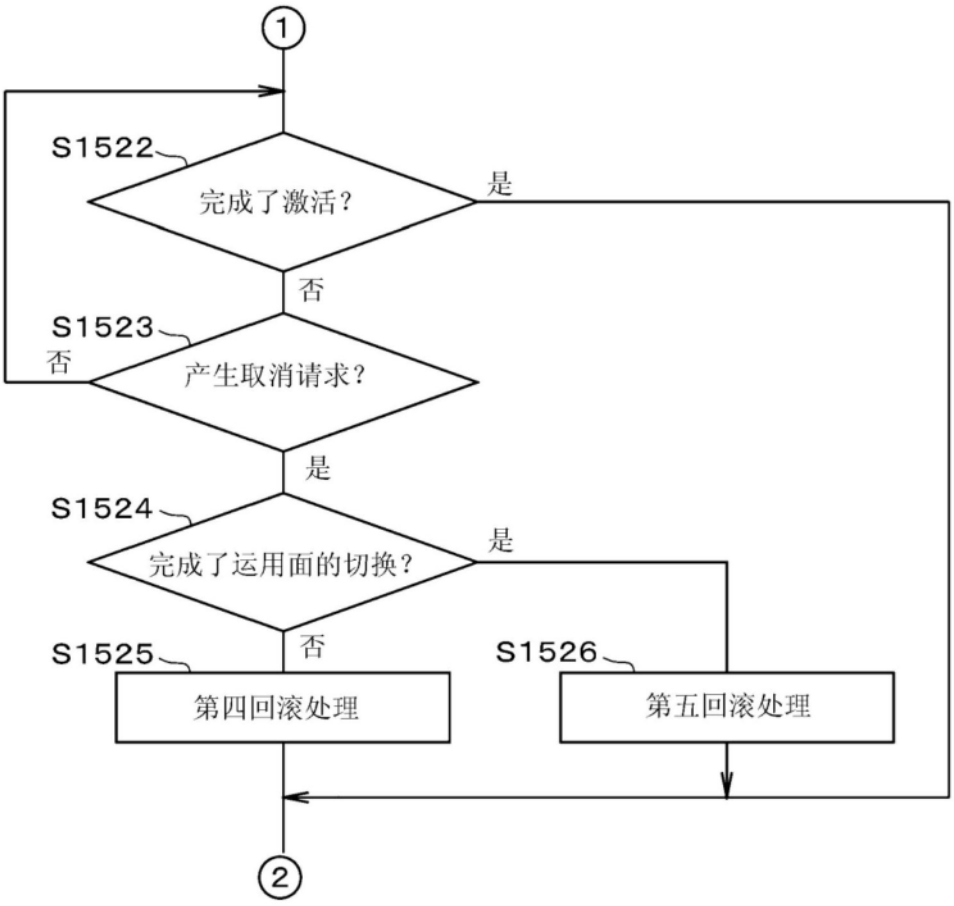

①
S1522
完成了激活？
是
否
S1523
否
产生取消请求？
是
S1524
完成了运用面的切换？
是
否
S1525
第四回滚处理
S1526
第五回滚处理
②

图122

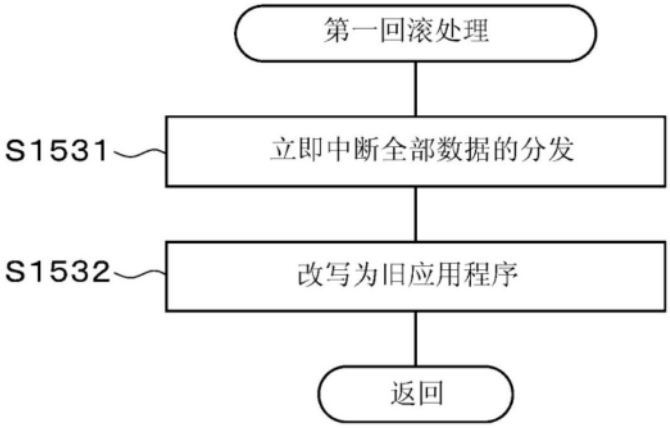

第一回滚处理
S1531
立即中断全部数据的分发
S1532
改写为旧应用程序
返回

图123

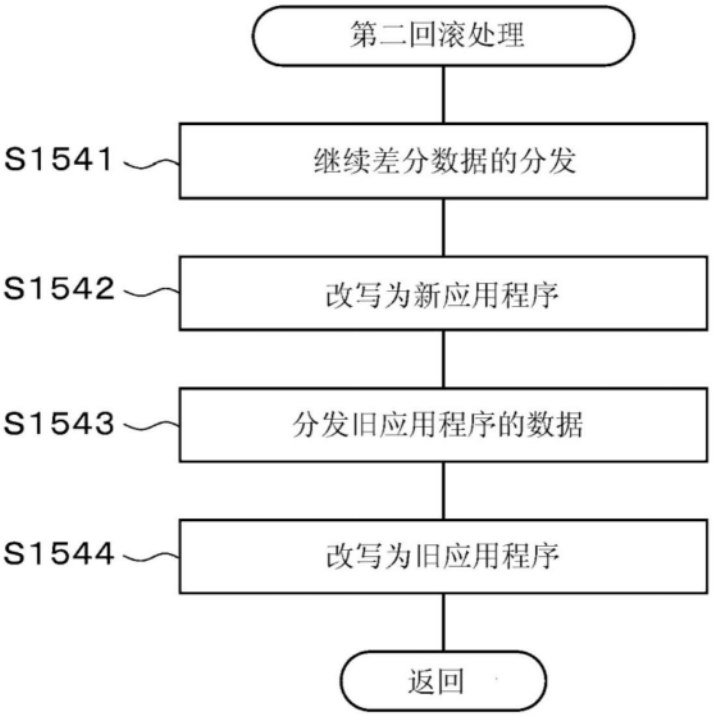

第二回滚处理
S1541
继续差分数据的分发
S1542
改写为新应用程序
S1543
分发旧应用程序的数据
S1544
改写为旧应用程序
返回

图124

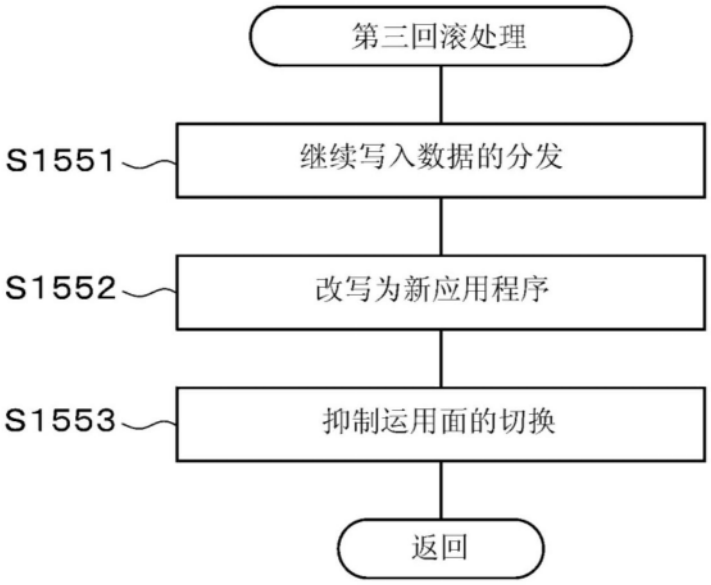

第三回滚处理
S1551
继续写入数据的分发
S1552
改写为新应用程序
S1553
抑制运用面的切换
返回

图125


安装中
运用面
Ver1.0
非运用面
向Ver2.0改写中
取消请求
运用面
Ver1.0
非运用面
返回到向Ver2.0
改写之前

图126

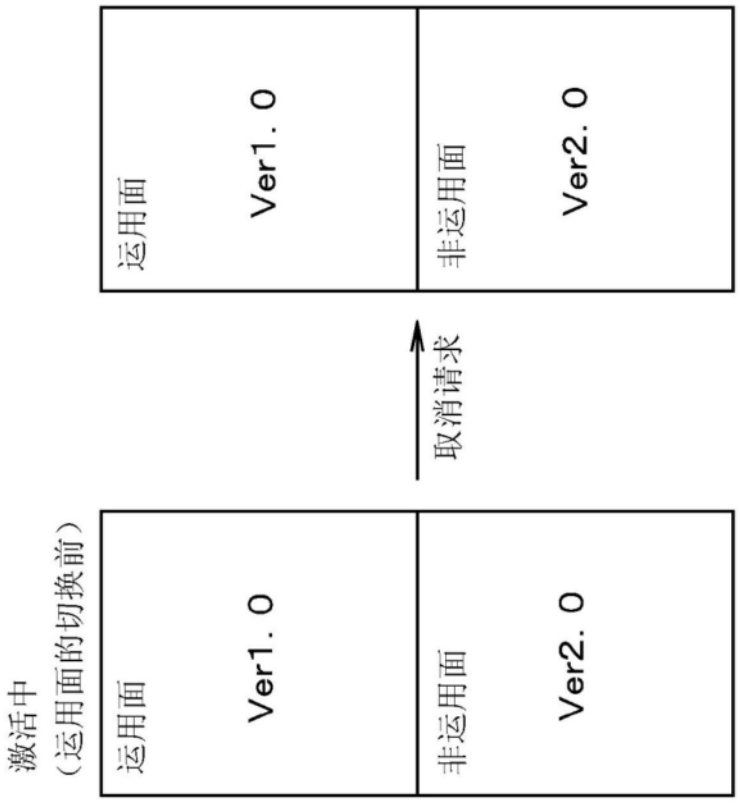


图127

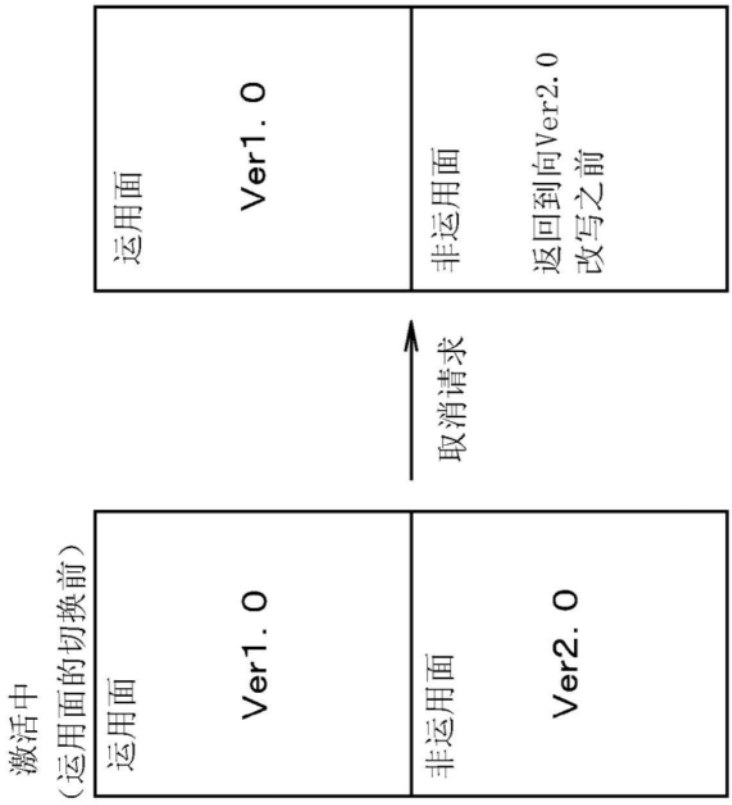

激活中
（运用面的切换前）
运用面
Ver1.0
非运用面
Ver2.0
取消请求
运用面
Ver1.0
非运用面
返回到向Ver2.0
改写之前

图128

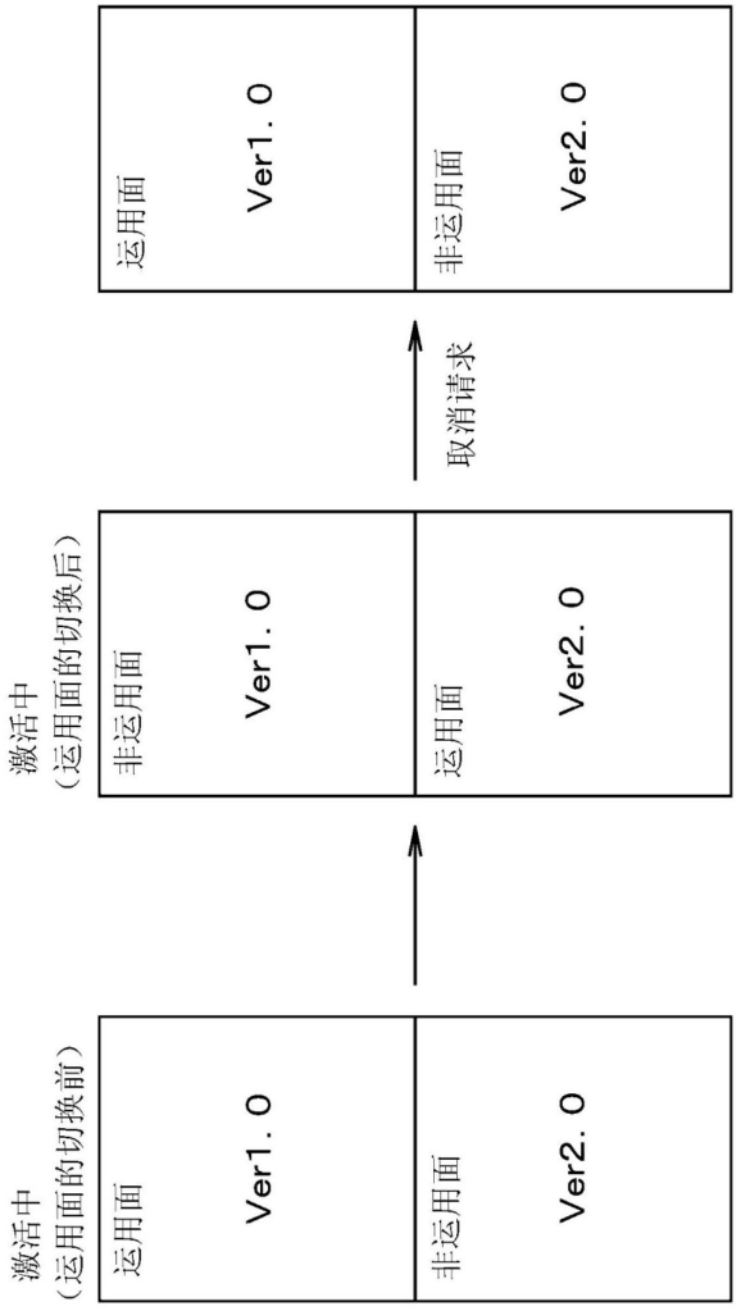

激活中
（运用面的切换前）
运用面
Ver1.0
非运用面
Ver2.0
激活中
（运用面的切换后）
非运用面
Ver1.0
运用面
Ver2.0
取消请求
运用面
Ver1.0
非运用面
Ver2.0

图129

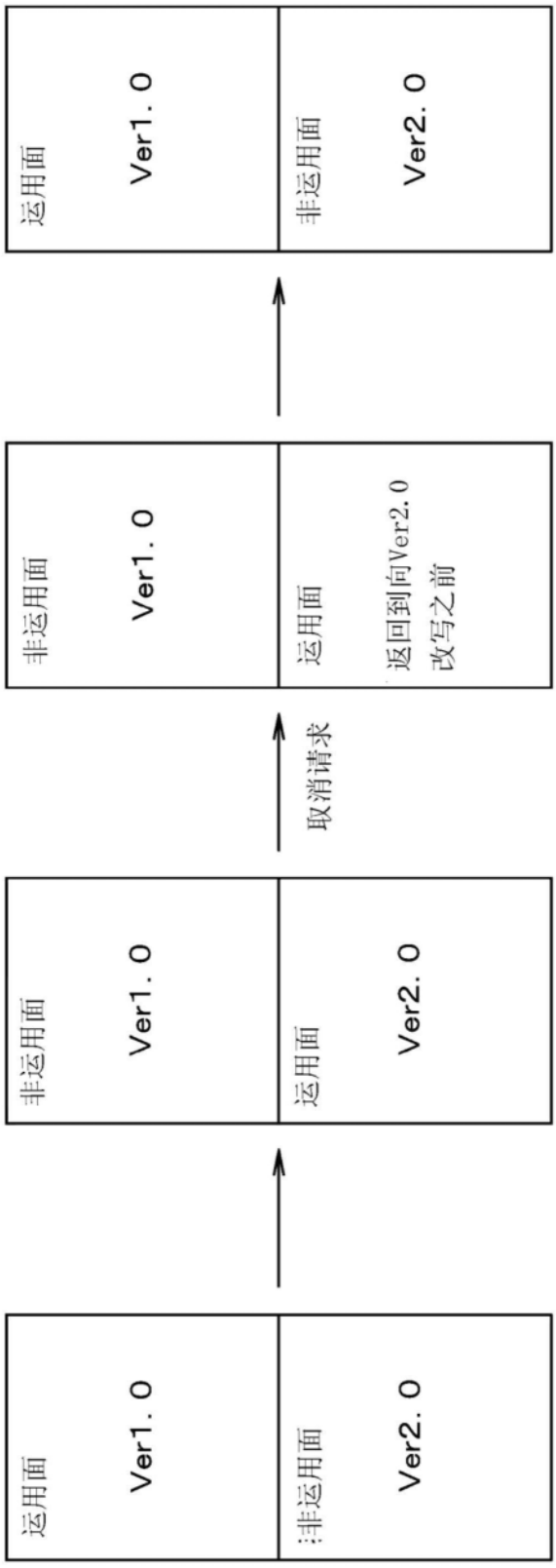

运用面
Ver1.0
非运用面
Ver2.0
非运用面
Ver1.0
运用面
返回到向Ver2.0
改写之前
取消请求
非运用面
Ver1.0
运用面
Ver2.0
运用面
Ver1.0
非运用面
Ver2.0

图130

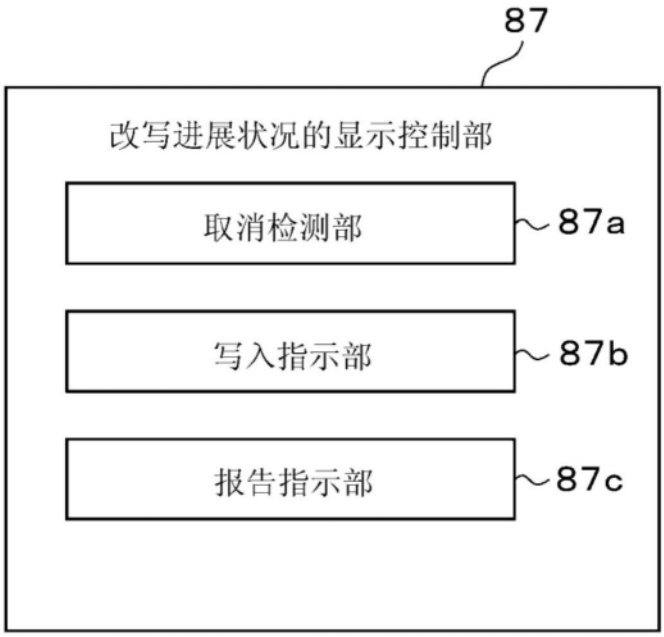


图131

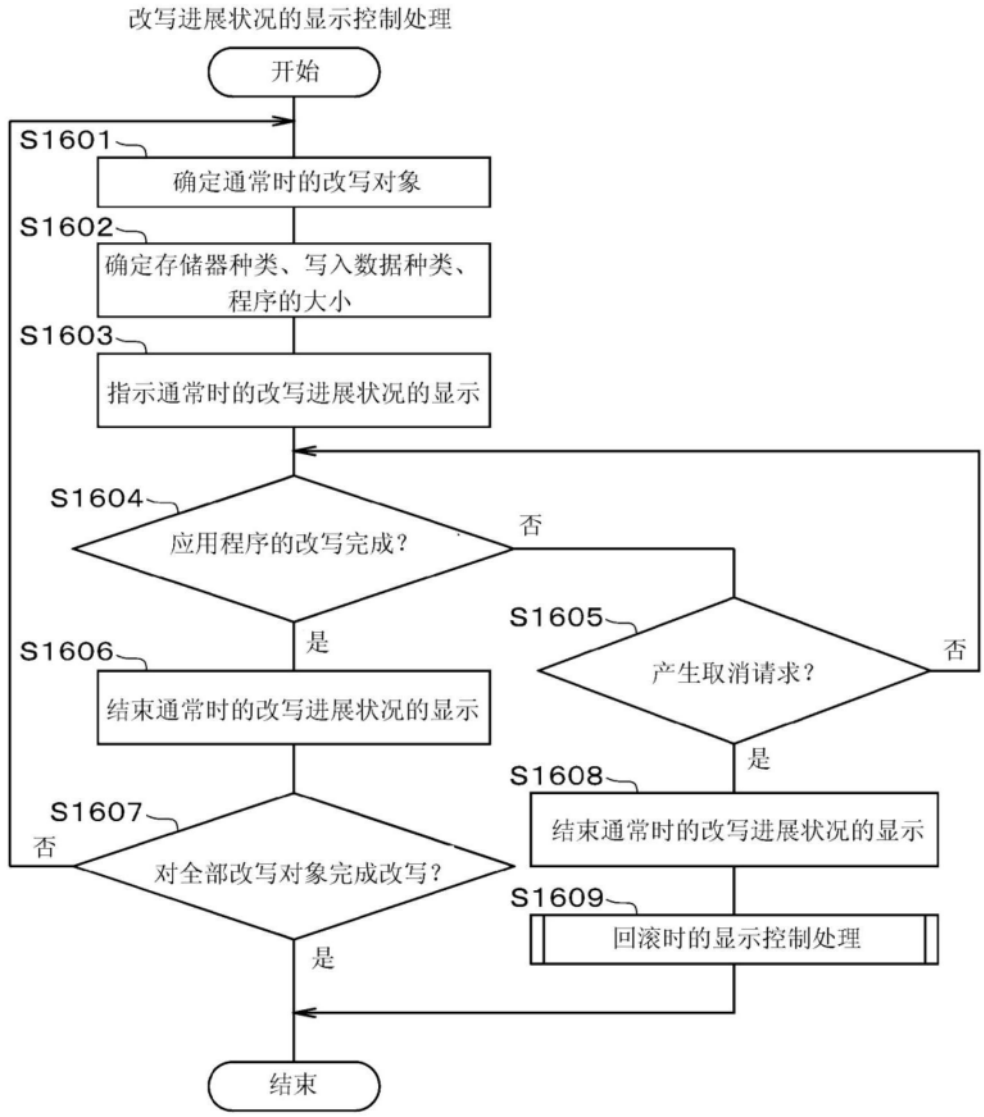

改写进展状况的显示控制处理
开始
S1601
确定通常时的改写对象
S1602
确定存储器种类、写入数据种类、程序的大小
S1603
指示通常时的改写进展状况的显示
S1604
应用程序的改写完成？
否
是
S1605
产生取消请求？
否
是
S1606
结束通常时的改写进展状况的显示
S1607
对全部改写对象完成改写？
否
是
S1608
结束通常时的改写进展状况的显示
S1609
回滚时的显示控制处理
结束

图132

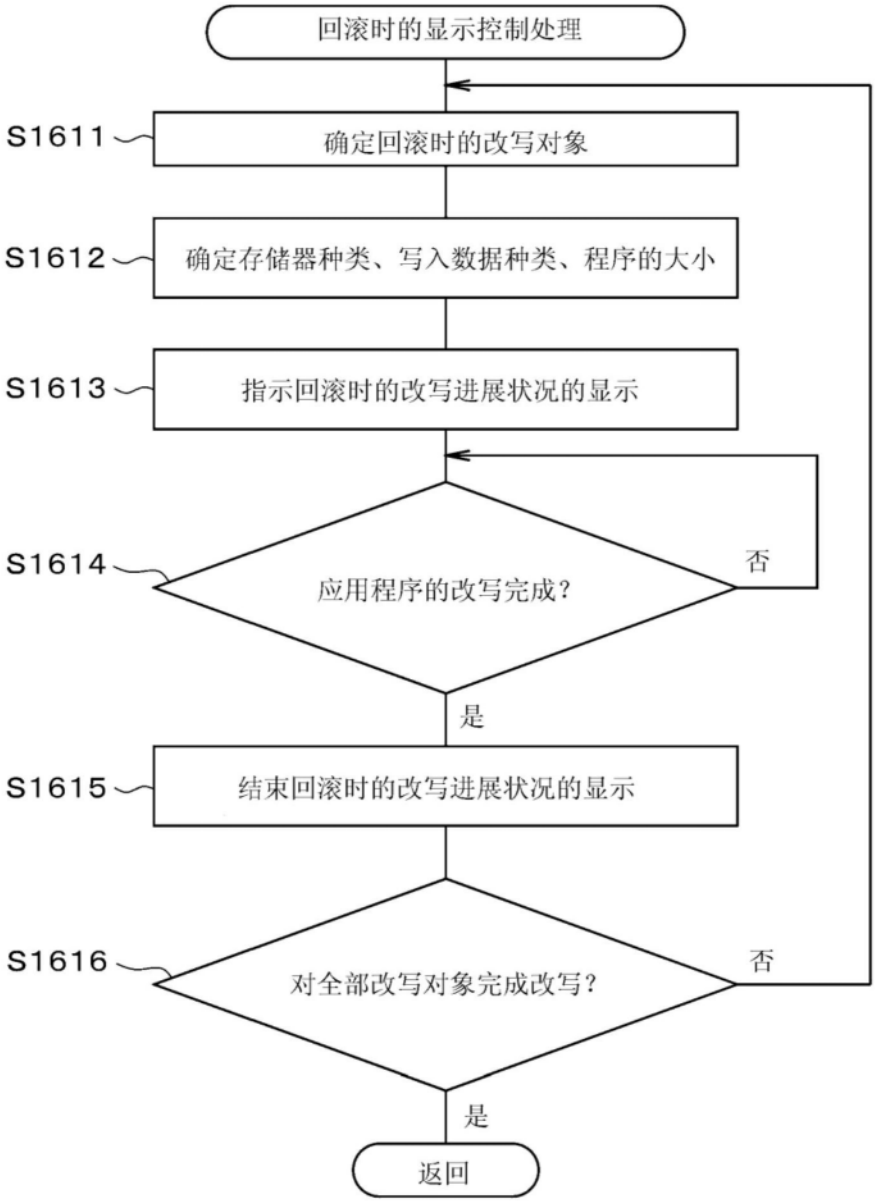

回滚时的显示控制处理
S1611
确定回滚时的改写对象
S1612
确定存储器种类、写入数据种类、程序的大小
S1613
指示回滚时的改写进展状况的显示
S1614
应用程序的改写完成？
否
是
S1615
结束回滚时的改写进展状况的显示
S1616
对全部改写对象完成改写？
否
是
返回

图133

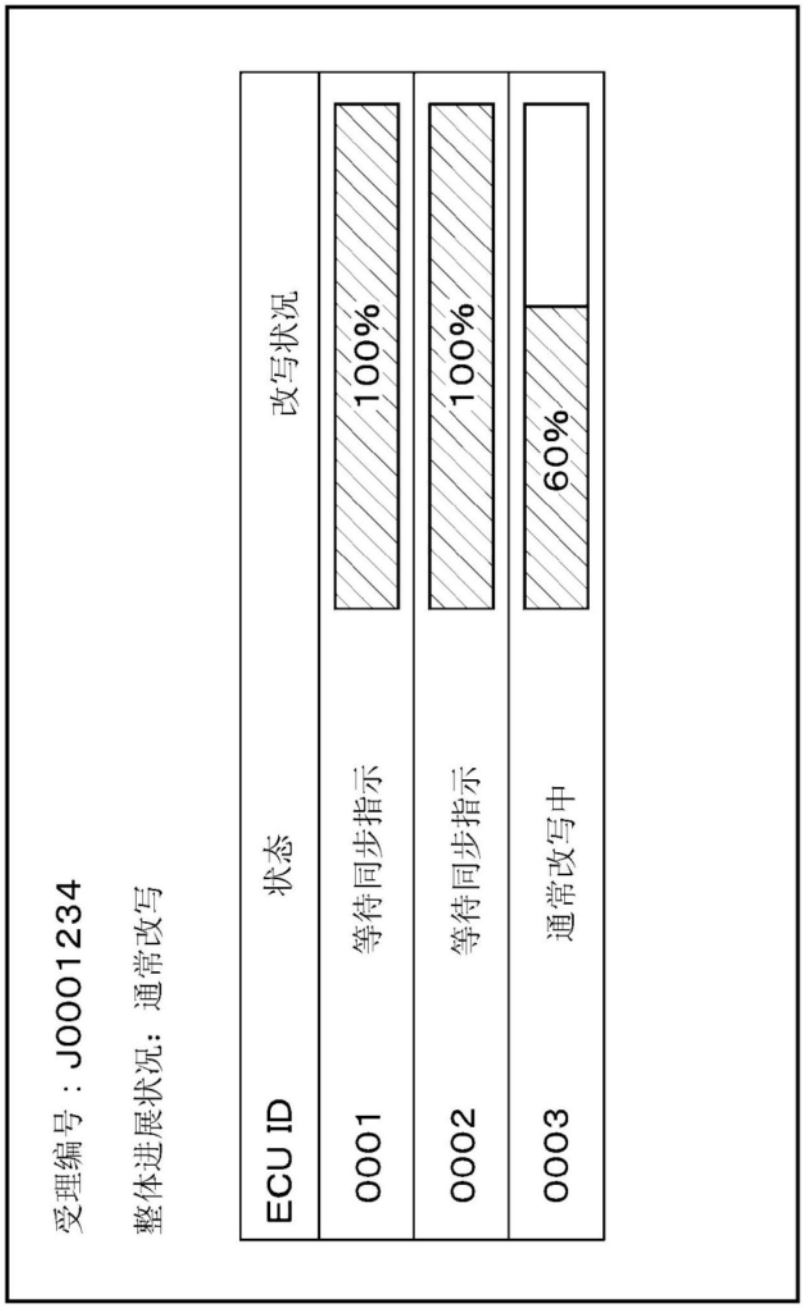

受理编号：J0001234
整体进展状况：通常改写
ECU ID
状态
改写状况
0001
等待同步指示
100%
0002
等待同步指示
100%
0003
通常改写中
60%

图134

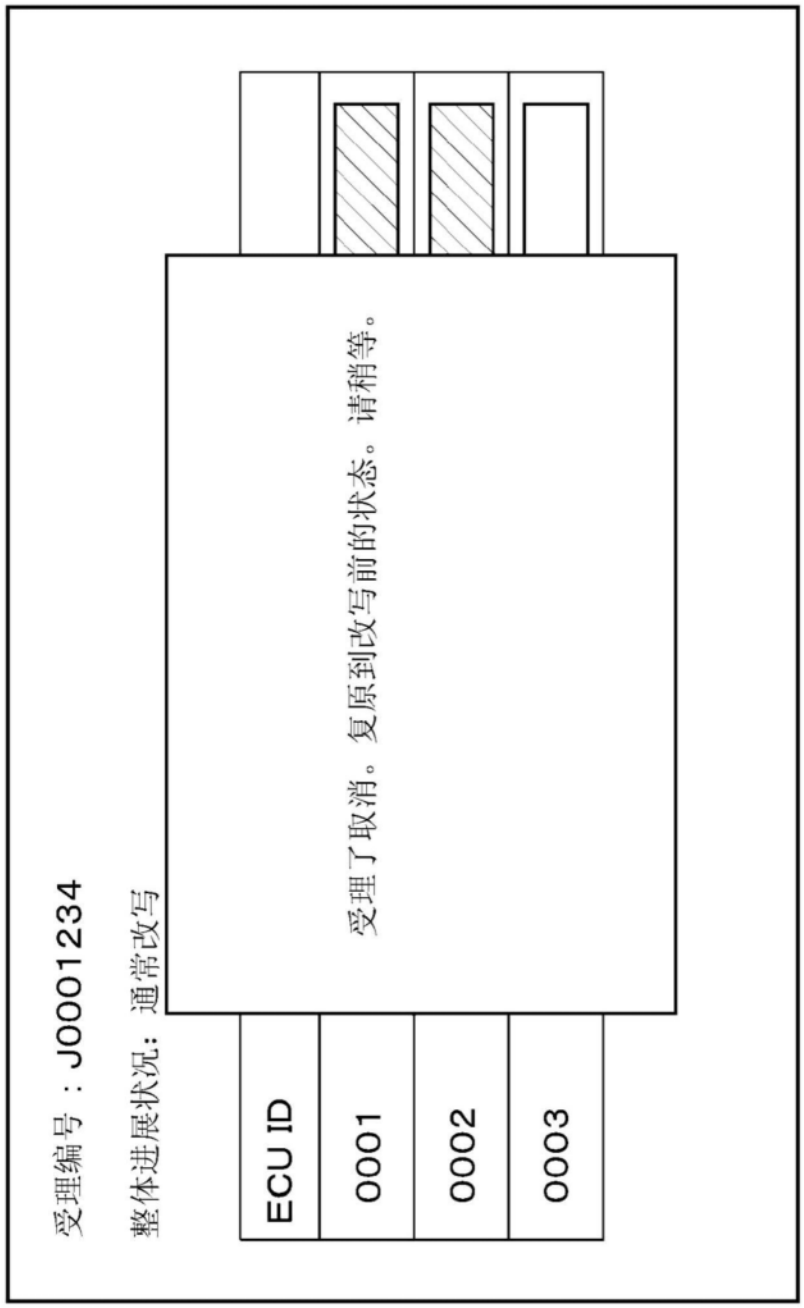

受理编号 ：J0001234
整体进展状况：通常改写
受理了取消。复原到改写前的状态。请稍等。
ECU ID
0001
0002
0003

图135

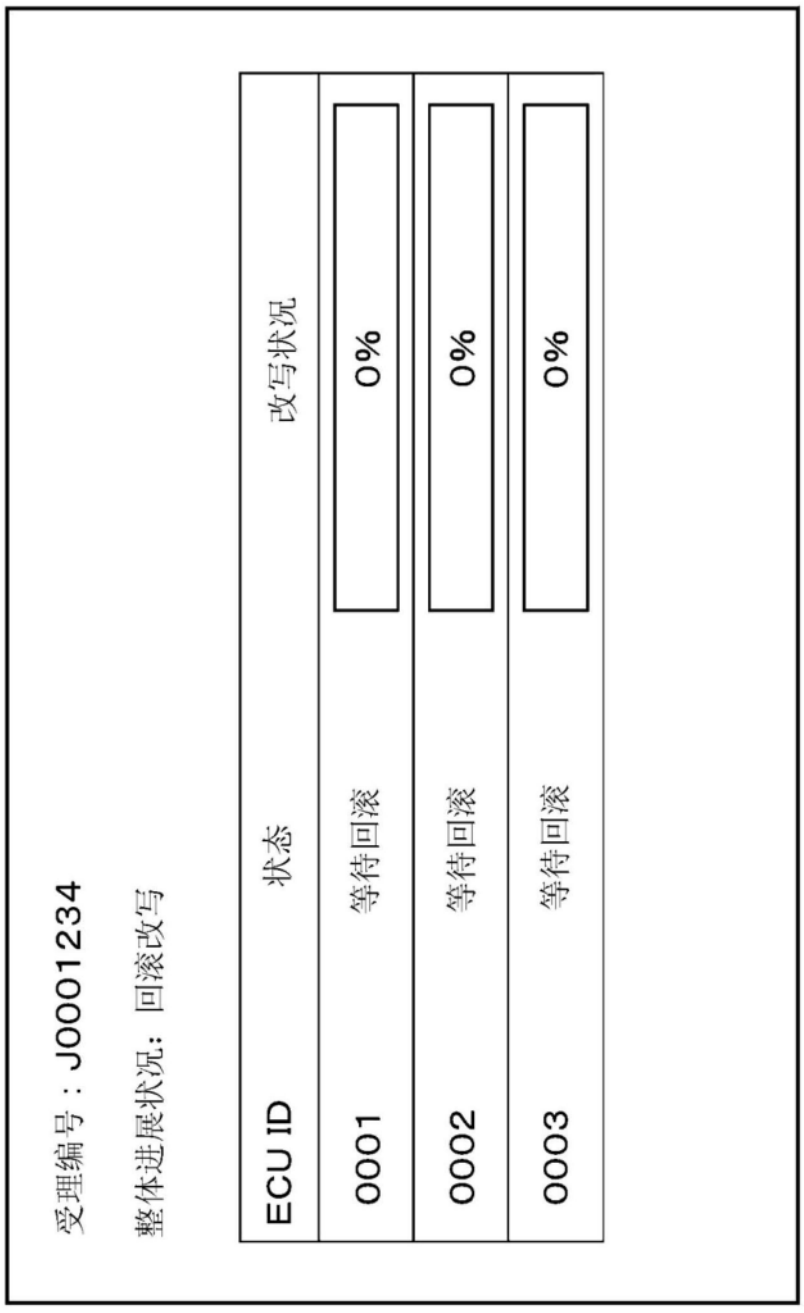

受理编号：J0001234
整体进展状况：回滚改写
ECU ID
状态
改写状况
0001
等待回滚
0%
0002
等待回滚
0%
0003
等待回滚
0%

图136

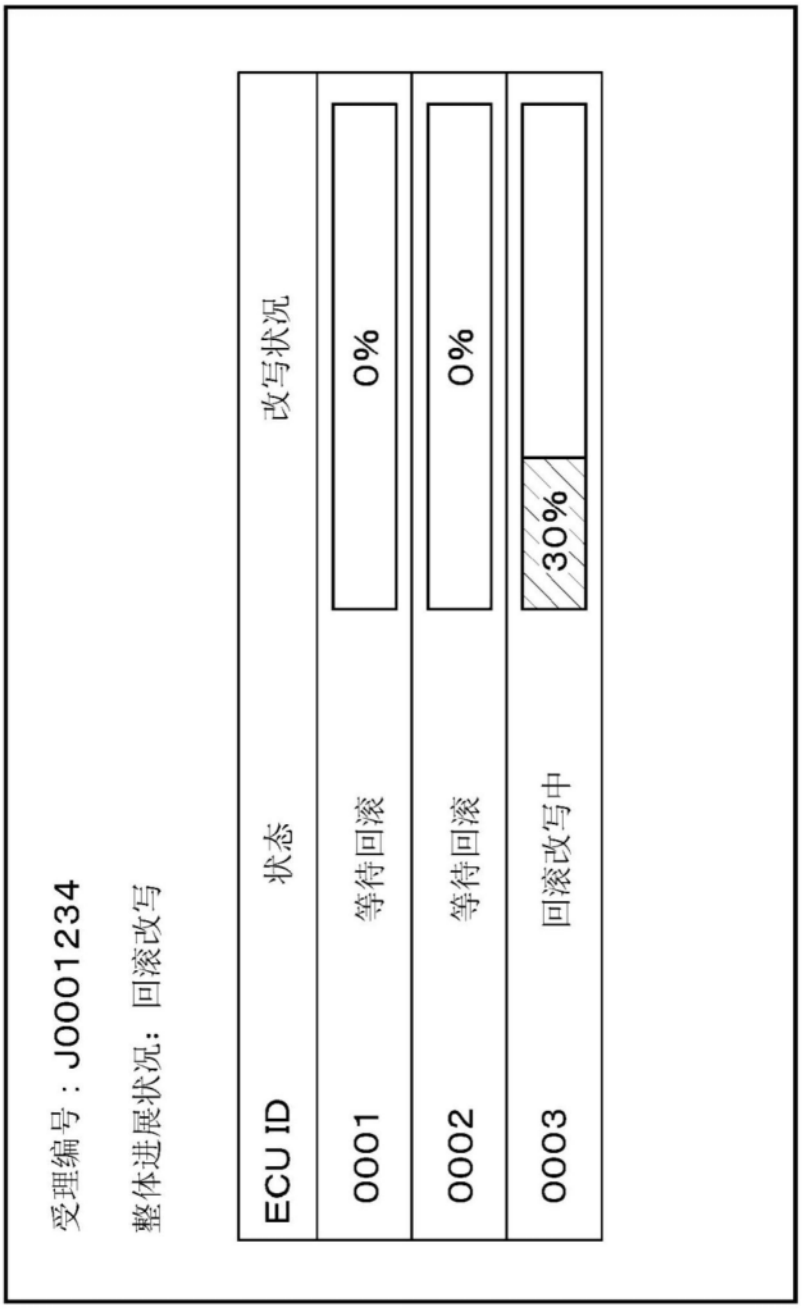

受理编号：J0001234
整体进展状况：回滚改写
ECU ID
状态
改写状况
0001
等待回滚
0%
0002
等待回滚
0%
0003
回滚改写中
30%

图137

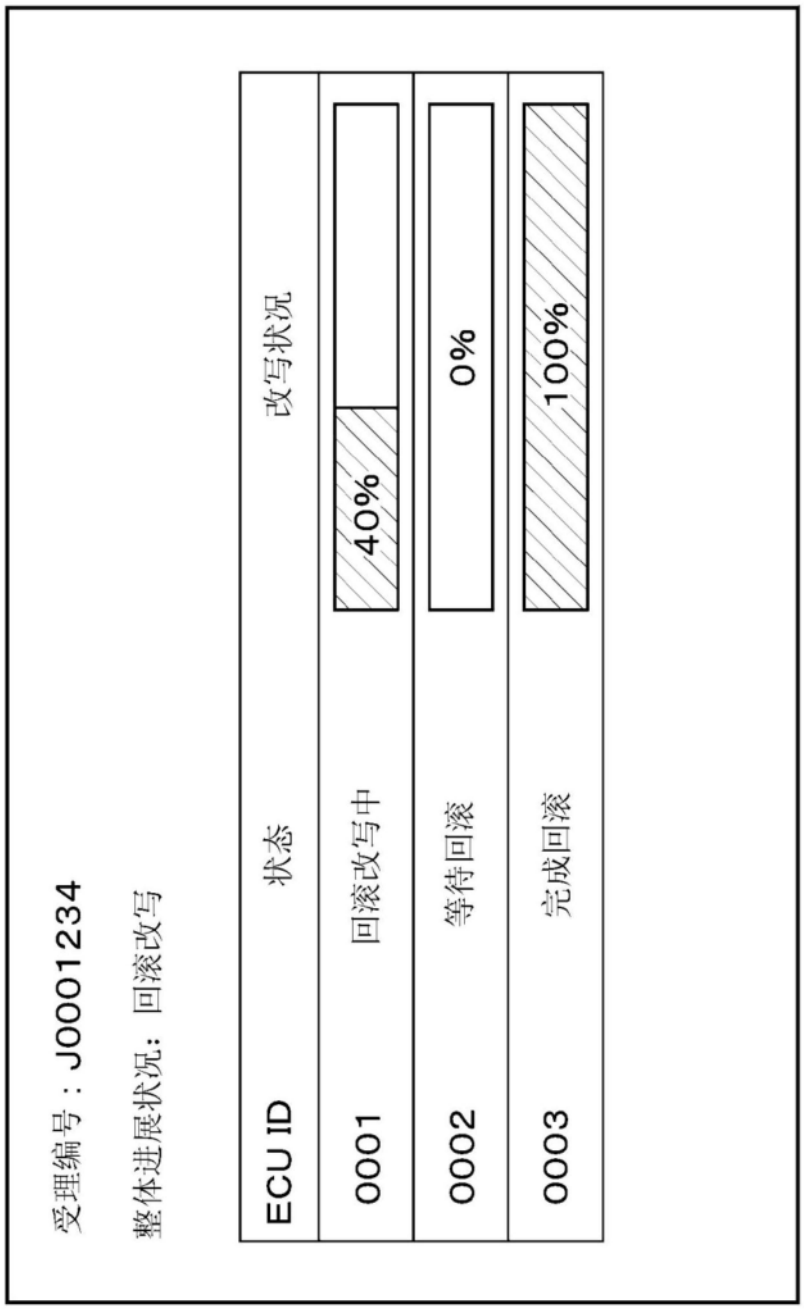

受理编号：J0001234
整体进展状况：回滚改写
ECU ID
状态
改写状况
0001
回滚改写中
40%
0002
等待回滚
0%
0003
完成回滚
100%

图138

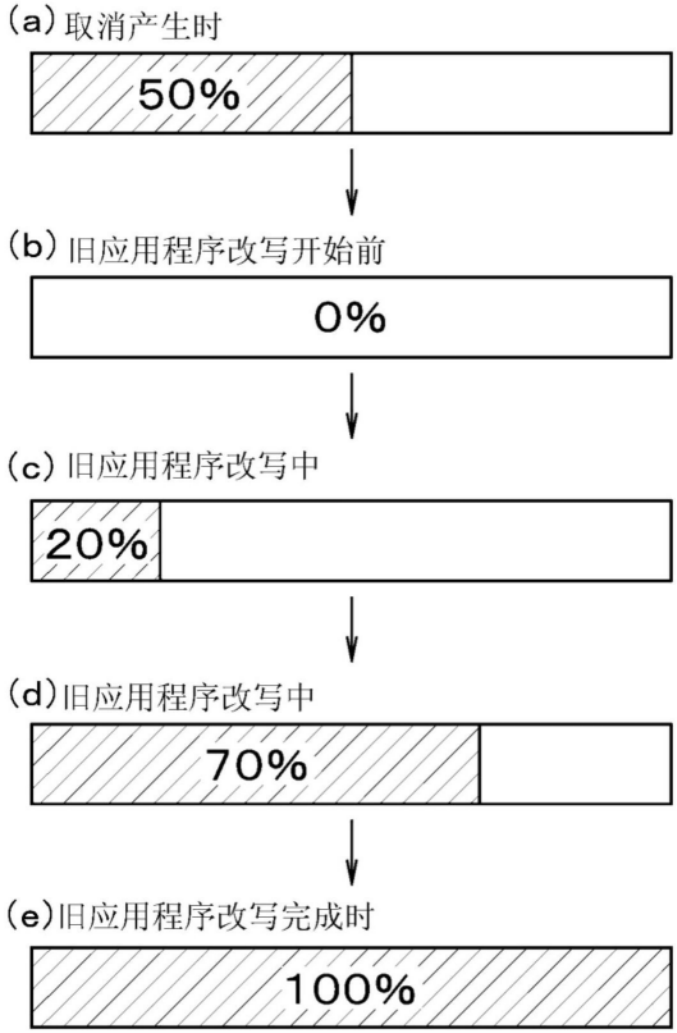

(a)取消产生时
50%
(b)旧应用程序改写开始前
0%
(c)旧应用程序改写中
20%
(d)旧应用程序改写中
70%
(e)旧应用程序改写完成时
100%

图139

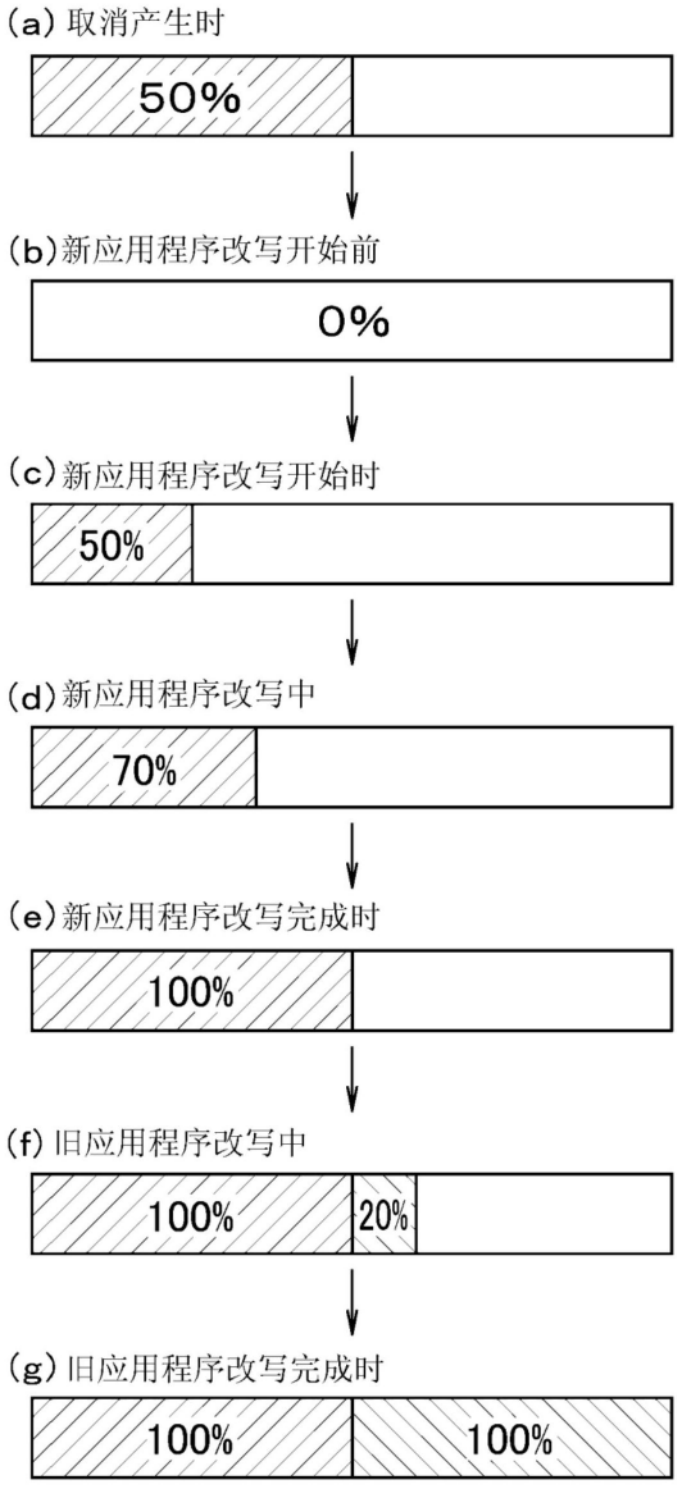

(a) 取消产生时
50%
(b)新应用程序改写开始前
0%
(c)新应用程序改写开始时
50%
(d)新应用程序改写中
70%
(e)新应用程序改写完成时
100%
(f) 旧应用程序改写中
100%
20%
(g) 旧应用程序改写完成时
100%
100%

图140

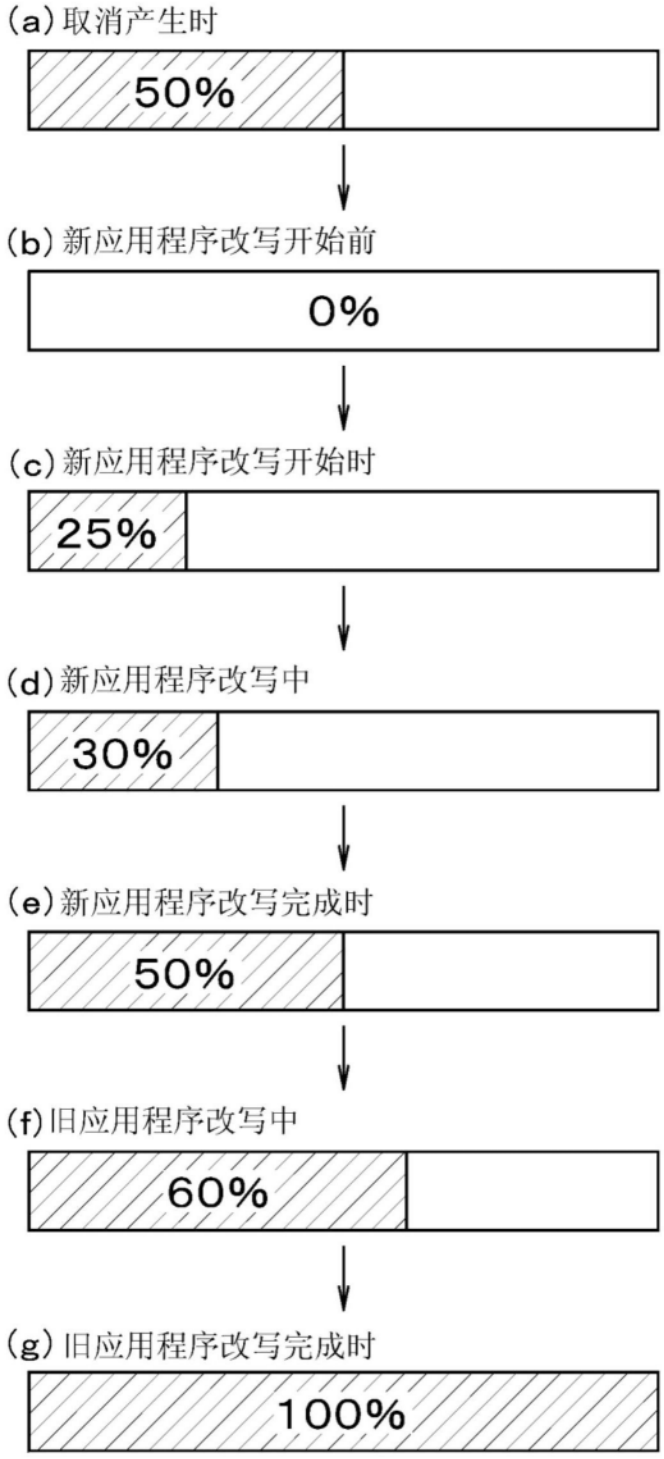

(a)取消产生时
50%
(b)新应用程序改写开始前
0%
(c)新应用程序改写开始时
25%
(d)新应用程序改写中
30%
(e)新应用程序改写完成时
50%
(f)旧应用程序改写中
60%
(g)旧应用程序改写完成时
100%

图141

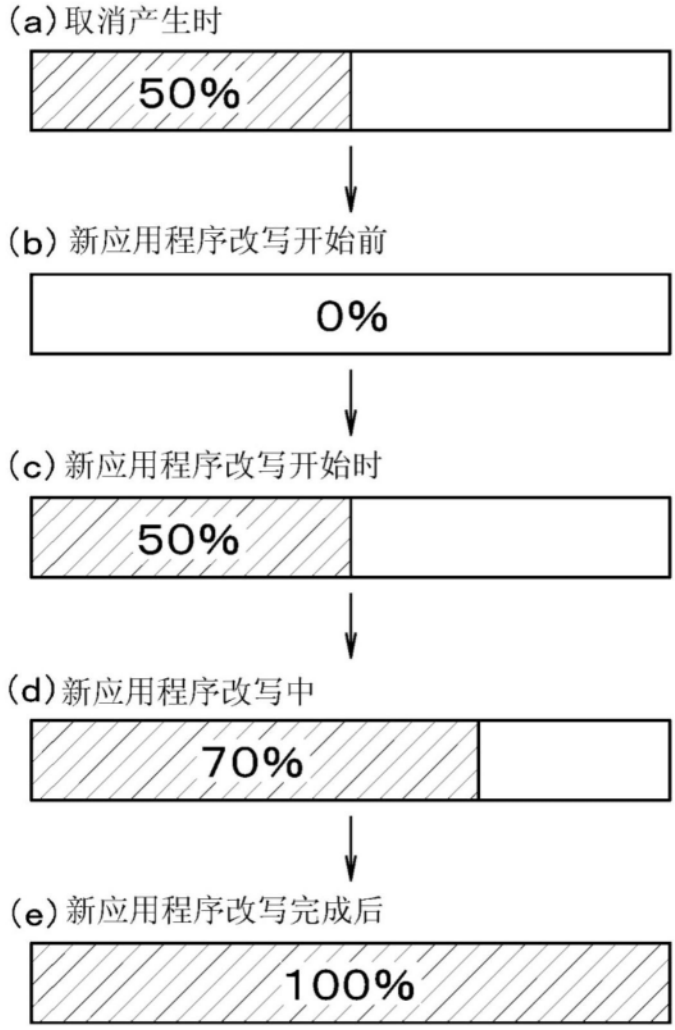

(a)取消产生时
50%
(b)新应用程序改写开始前
0%
(c)新应用程序改写开始时
50%
(d)新应用程序改写中
70%
(e)新应用程序改写完成后
100%

图142

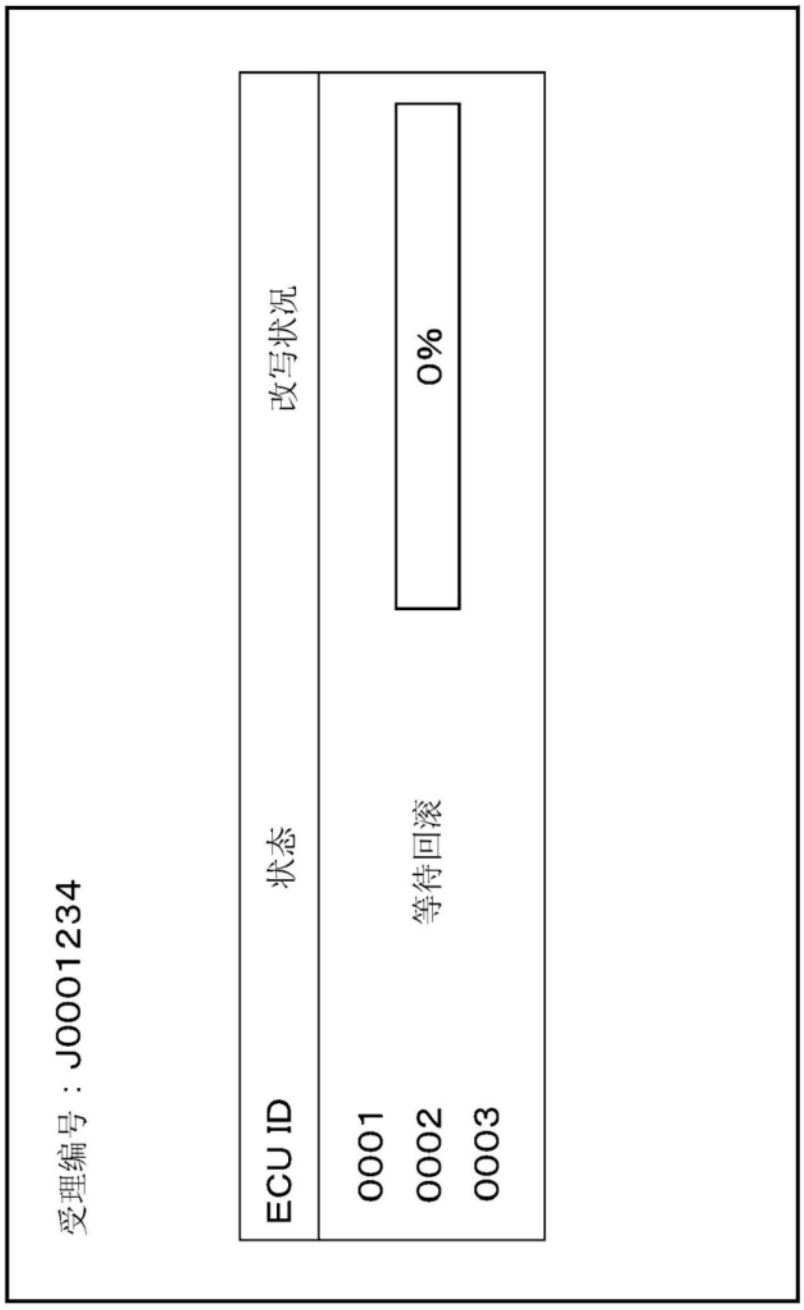


图143

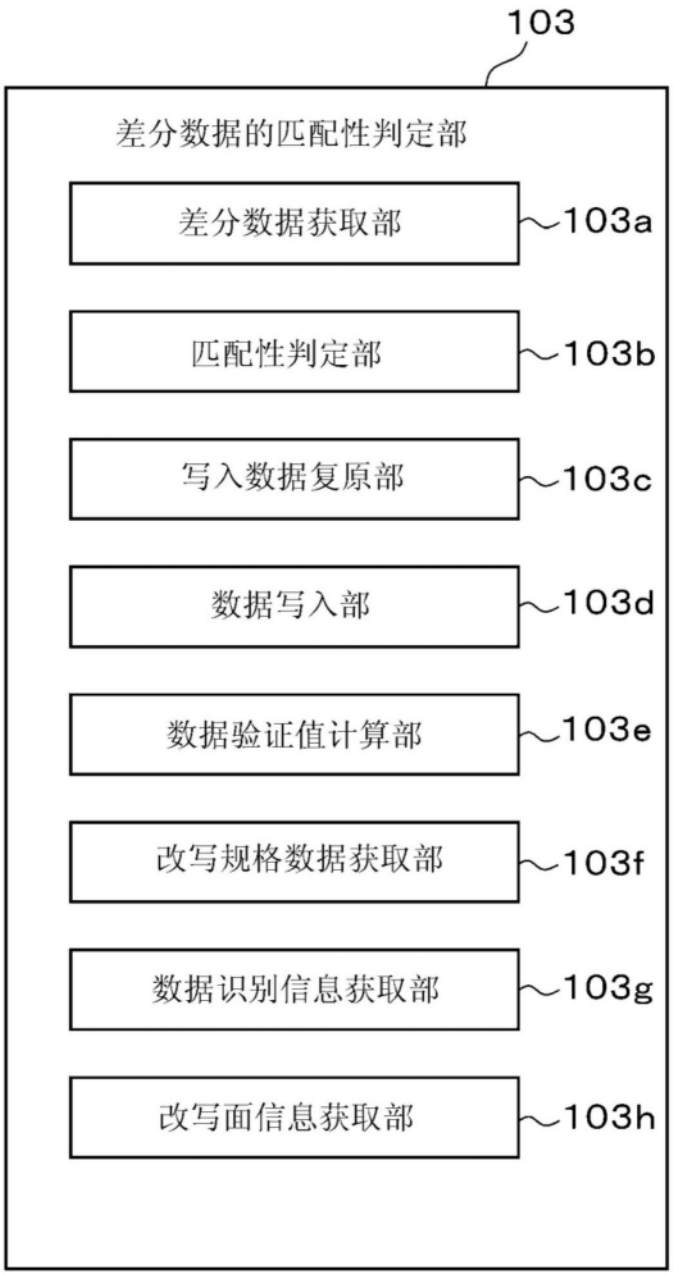

103
差分数据的匹配性判定部
差分数据获取部
103a
匹配性判定部
103b
写入数据复原部
103c
数据写入部
103d
数据验证值计算部
103e
改写规格数据获取部
103f
数据识别信息获取部
103g
改写面信息获取部
103h

图144

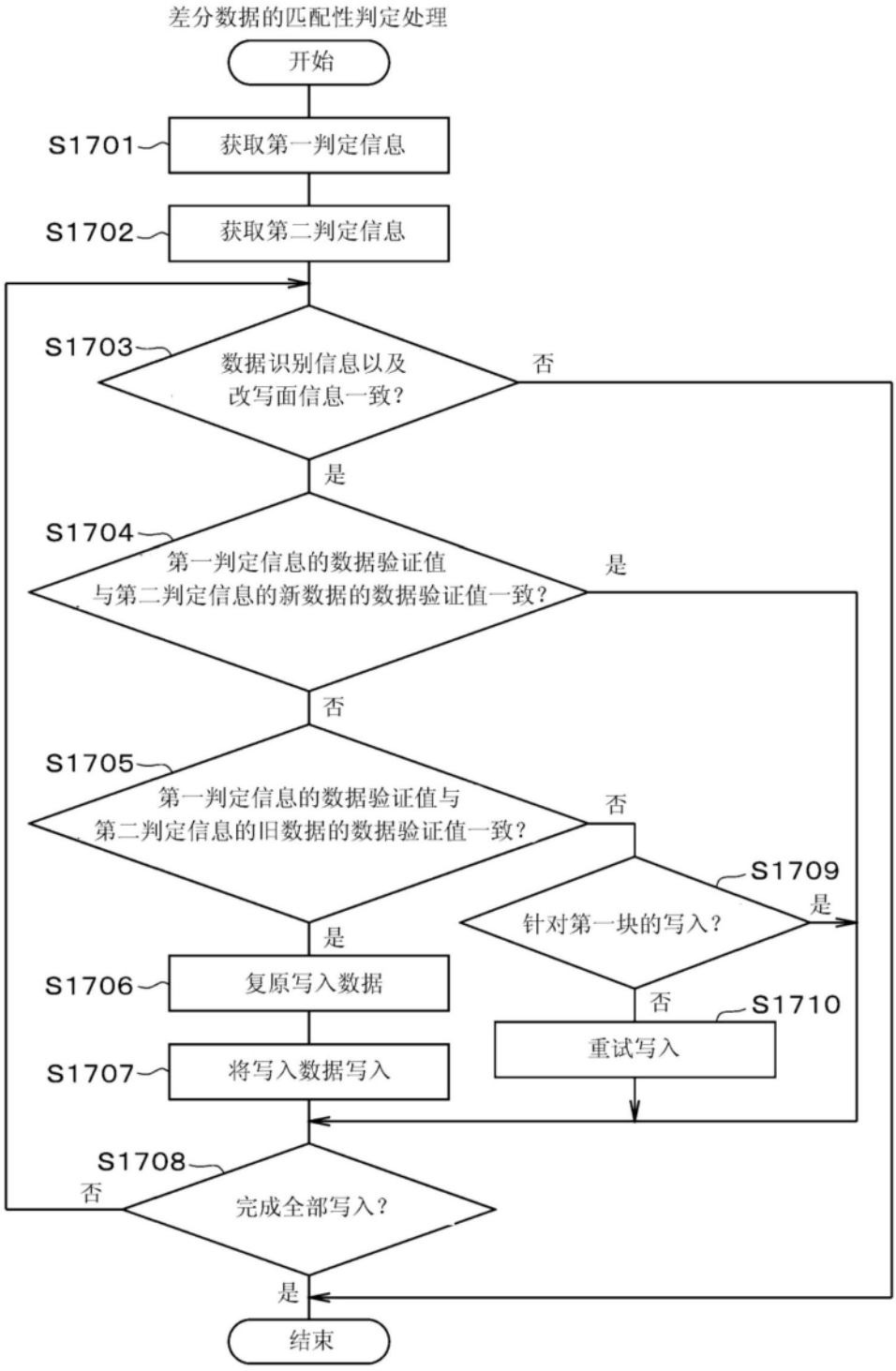

差分数据的匹配性判定处理
开始
S1701
获取第一判定信息
S1702
获取第二判定信息
S1703
数据识别信息以及
改写面信息一致?
否
是
S1704
第一判定信息的数据验证值
与第二判定信息的新数据的数据验证值一致?
是
否
S1705
第一判定信息的数据验证值与
第二判定信息的旧数据的数据验证值一致?
否
S1709
针对第一块的写入?
是
是
S1706
复原写入数据
否
S1710
重试写入
S1707
将写入数据写入
S1708
否
完成全部写入?
是
结束

图145

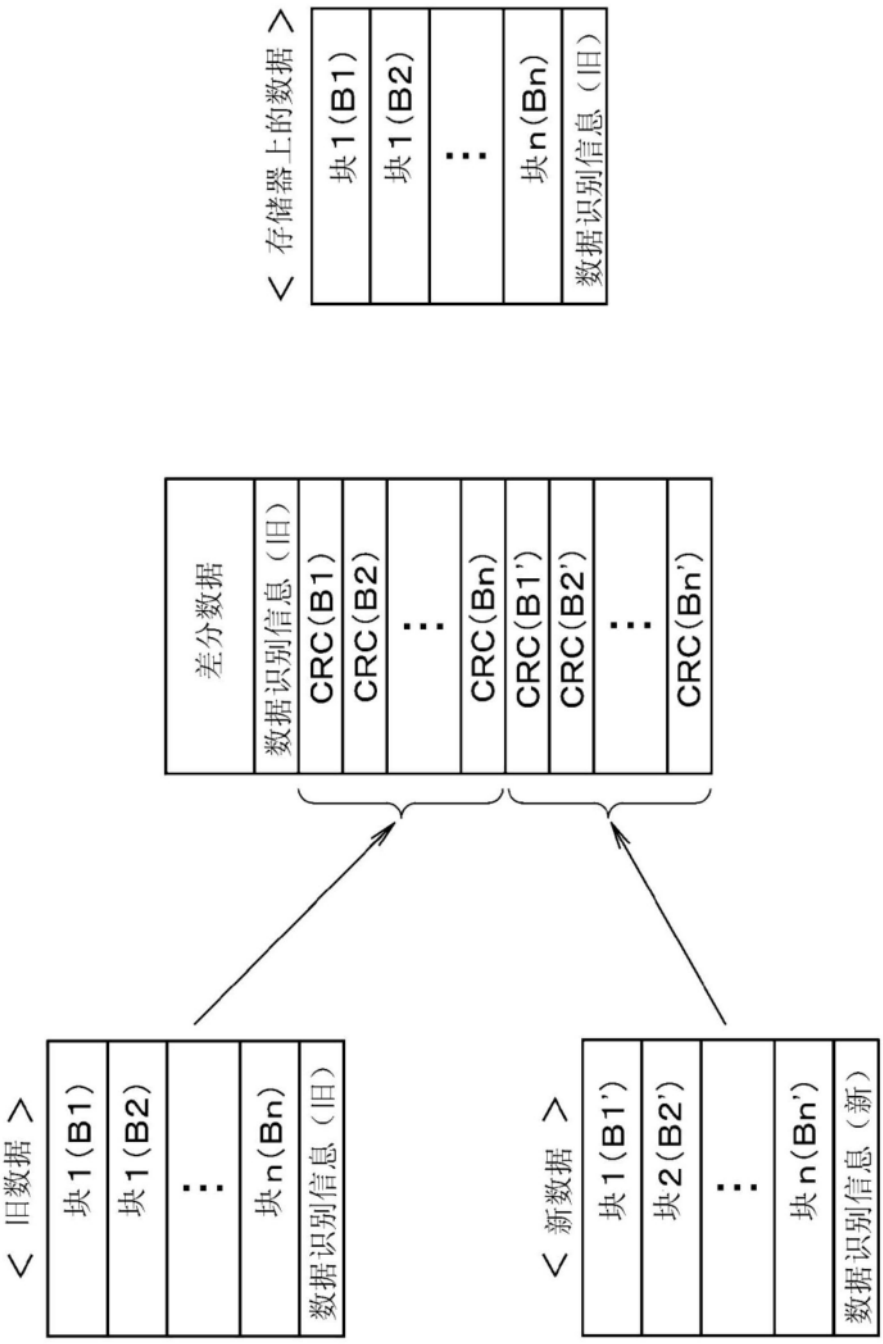

< 存储器上的数据 >
块1(B1)
块1(B2)
块n(Bn)
数据识别信息（旧）
差分数据
数据识别信息（旧）
CRC(B1)
CRC(B2)
CRC(Bn)
CRC(B1')
CRC(B2')
CRC(Bn')
< 旧数据 >
块1(B1)
块1(B2)
块n(Bn)
数据识别信息（旧）
< 新数据 >
块1(B1')
块2(B2')
块n(Bn')
数据识别信息（新）

图146

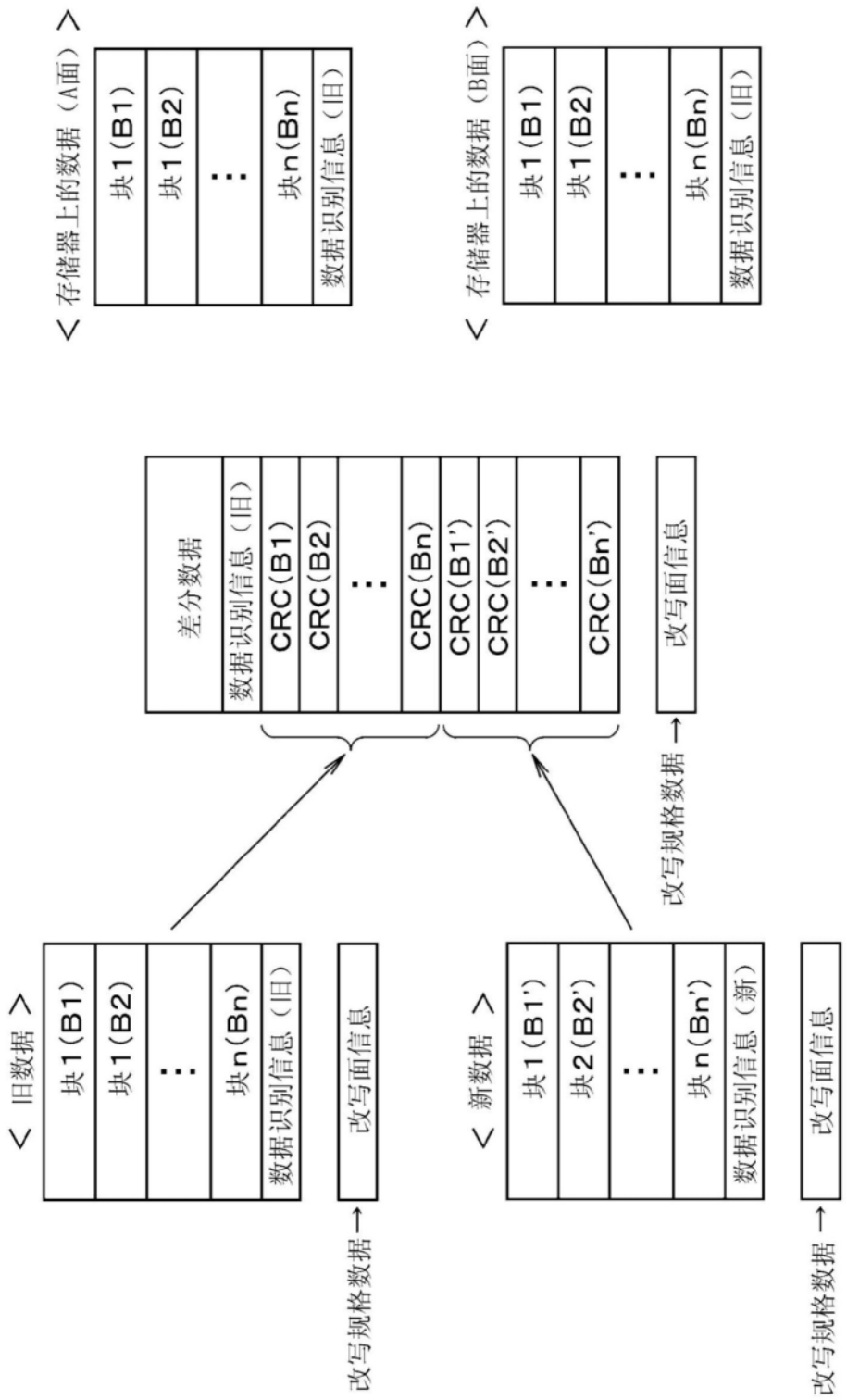

< 存储器上的数据（A面）>
块1(B1)
块1(B2)
块n(Bn)
数据识别信息（旧）
< 存储器上的数据（B面）>
块1(B1)
块1(B2)
块n(Bn)
数据识别信息（旧）
差分数据
数据识别信息（旧）
CRC(B1)
CRC(B2)
CRC(Bn)
CRC(B1')
CRC(B2')
CRC(Bn')
改写面信息
改写规格数据
< 旧数据 >
块1(B1)
块1(B2)
块n(Bn)
数据识别信息（旧）
改写面信息
改写规格数据
< 新数据 >
块1(B1')
块2(B2')
块n(Bn')
数据识别信息（新）
改写面信息
改写规格数据

图147

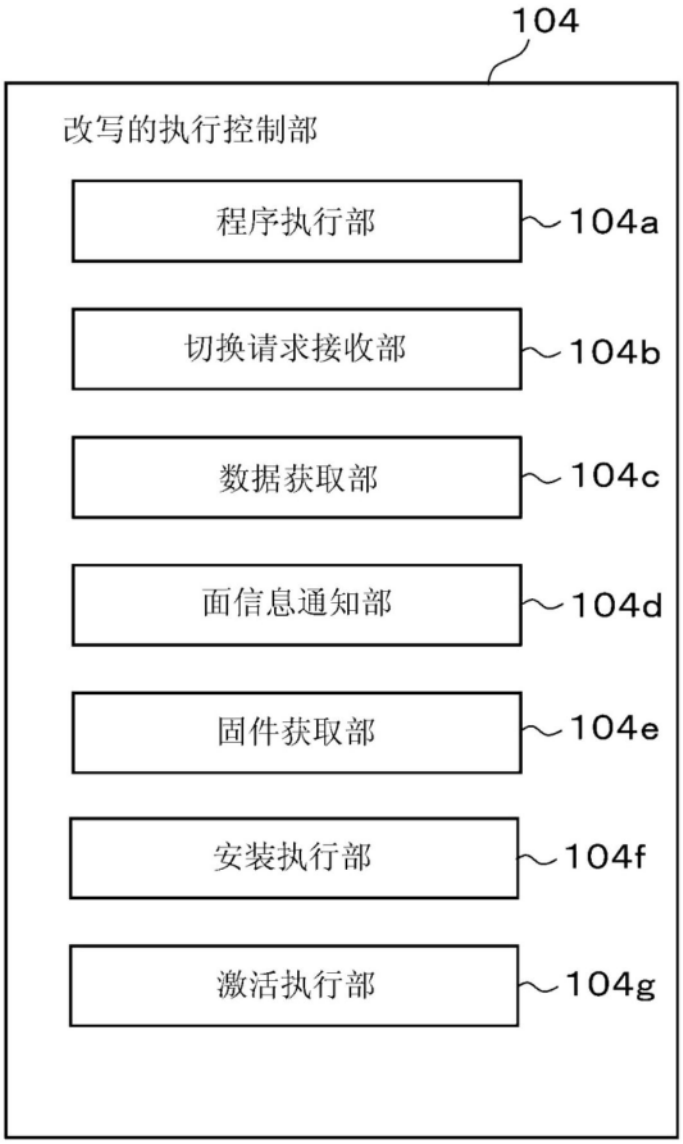

104
改写的执行控制部
程序执行部
104a
切换请求接收部
104b
数据获取部
104c
面信息通知部
104d
固件获取部
104e
安装执行部
104f
激活执行部
104g

图148

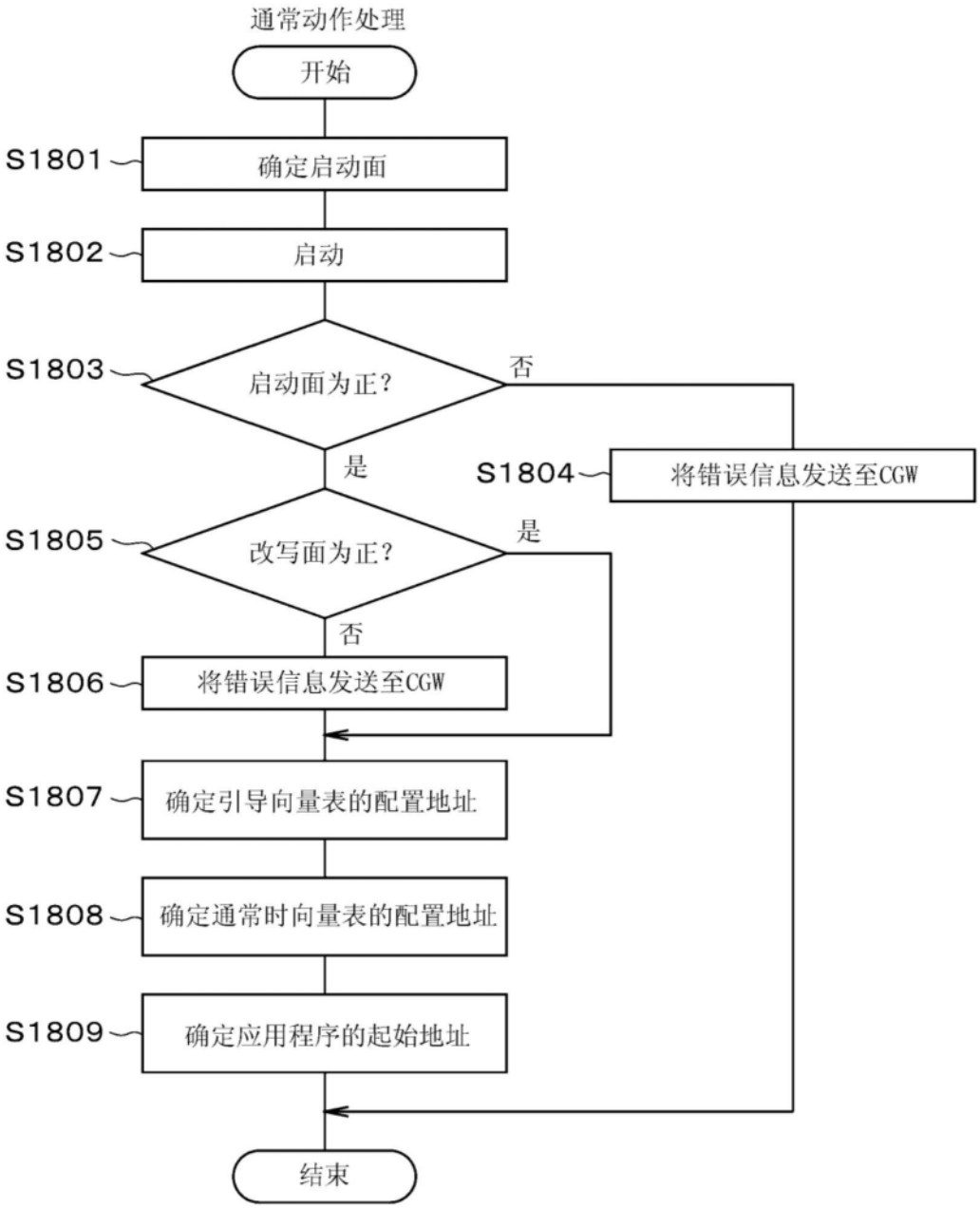

通常动作处理
开始
S1801
确定启动面
S1802
启动
S1803
启动面为正？
否
是
S1804
将错误信息发送至CGW
S1805
改写面为正？
是
否
S1806
将错误信息发送至CGW
S1807
确定引导向量表的配置地址
S1808
确定通常时向量表的配置地址
S1809
确定应用程序的起始地址
结束

图149

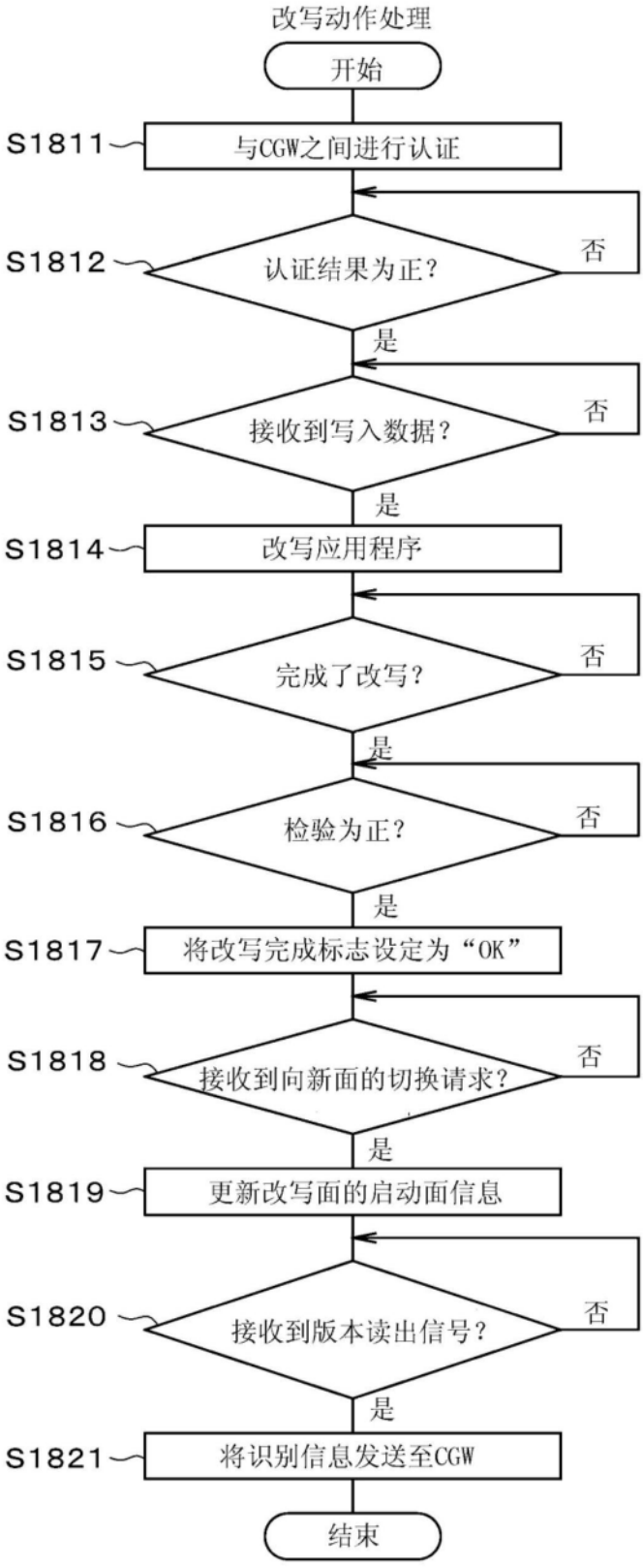

改写动作处理
开始
S1811
与CGW之间进行认证
S1812
认证结果为正？
否
是
S1813
接收到写入数据？
否
是
S1814
改写应用程序
S1815
完成了改写？
否
是
S1816
检验为正？
否
是
S1817
将改写完成标志设定为“OK”
S1818
接收到向新面的切换请求？
否
是
S1819
更新改写面的启动面信息
S1820
接收到版本读出信号？
否
是
S1821
将识别信息发送至CGW
结束

图150

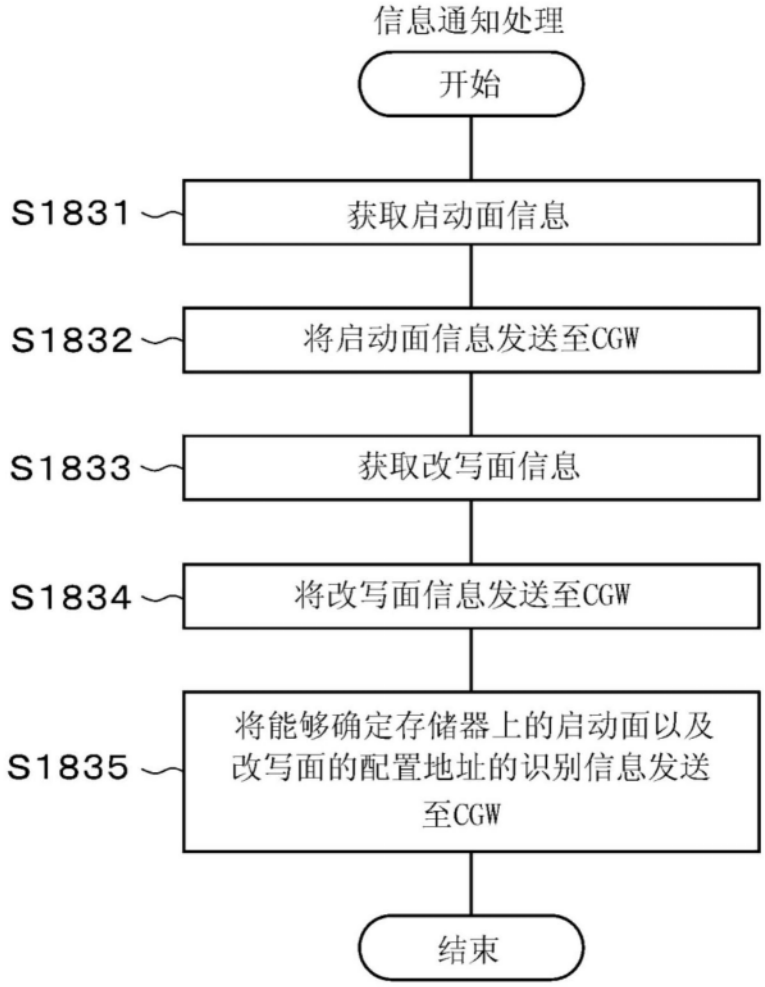

信息通知处理
开始
S1831
获取启动面信息
S1832
将启动面信息发送至CGW
S1833
获取改写面信息
S1834
将改写面信息发送至CGW
S1835
将能够确定存储器上的启动面以及改写面的配置地址的识别信息发送至CGW
结束

图151

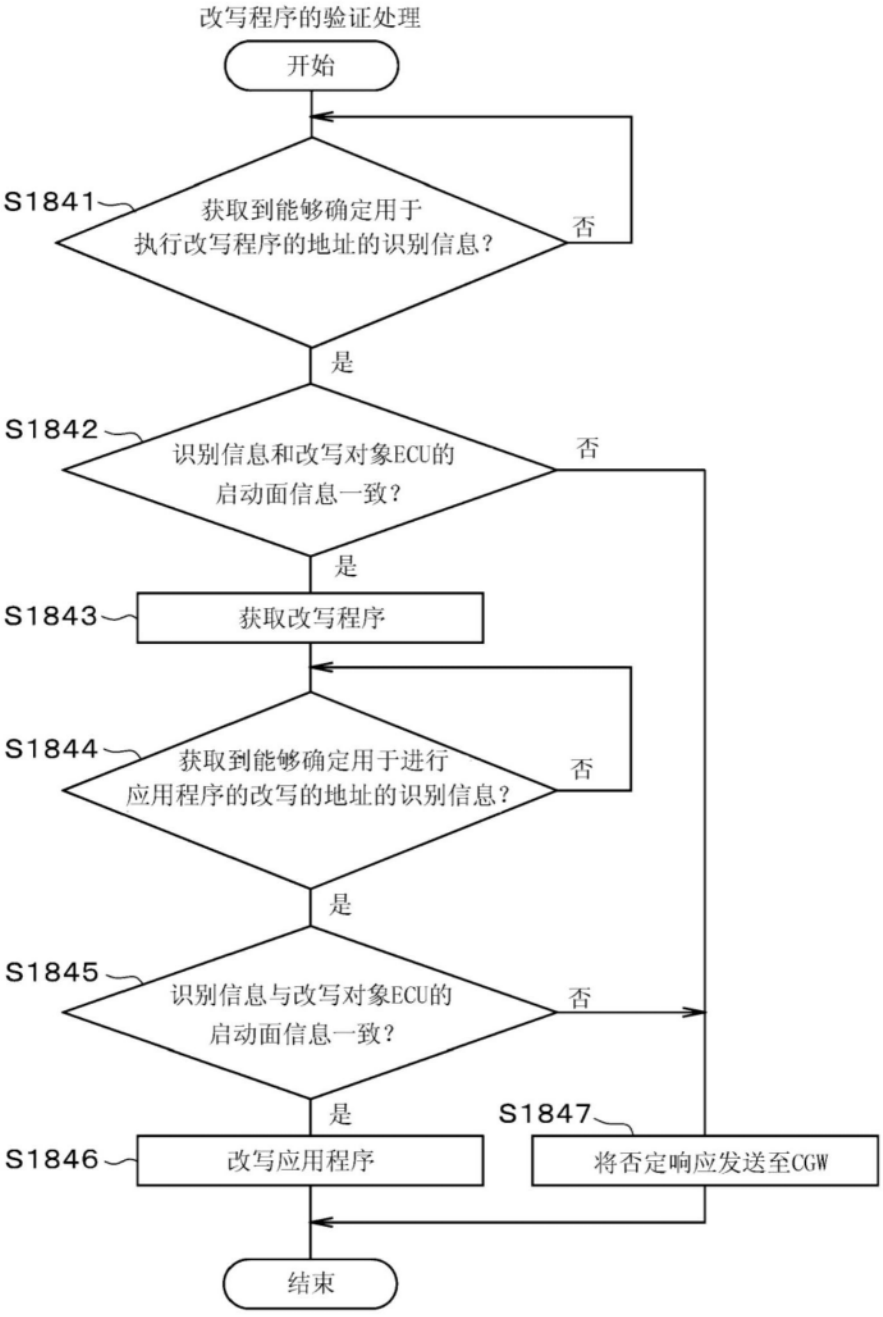

改写程序的验证处理
开始
S1841
获取到能够确定用于执行改写程序的地址的识别信息？
否
是
S1842
识别信息和改写对象ECU的启动面信息一致？
否
是
S1843
获取改写程序
S1844
获取到能够确定用于进行应用程序的改写的地址的识别信息？
否
是
S1845
识别信息与改写对象ECU的启动面信息一致？
否
是
S1846
改写应用程序
S1847
将否定响应发送至CGW
结束

图152

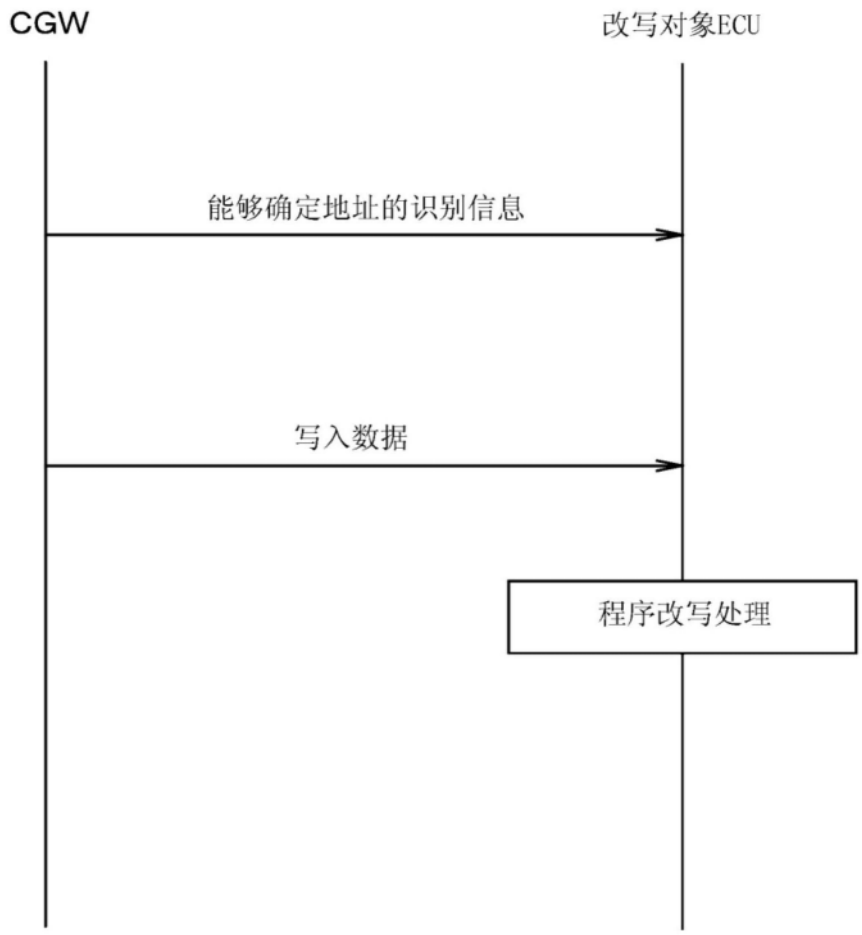


图153

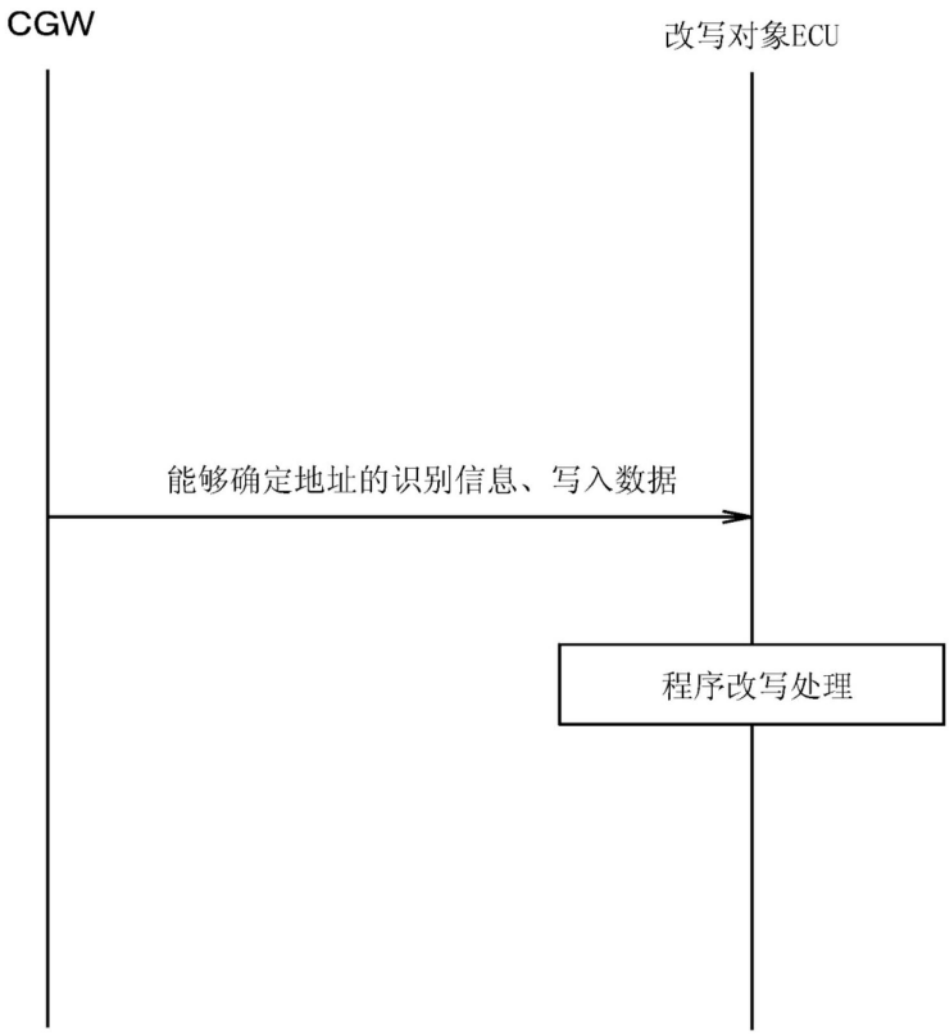


图154

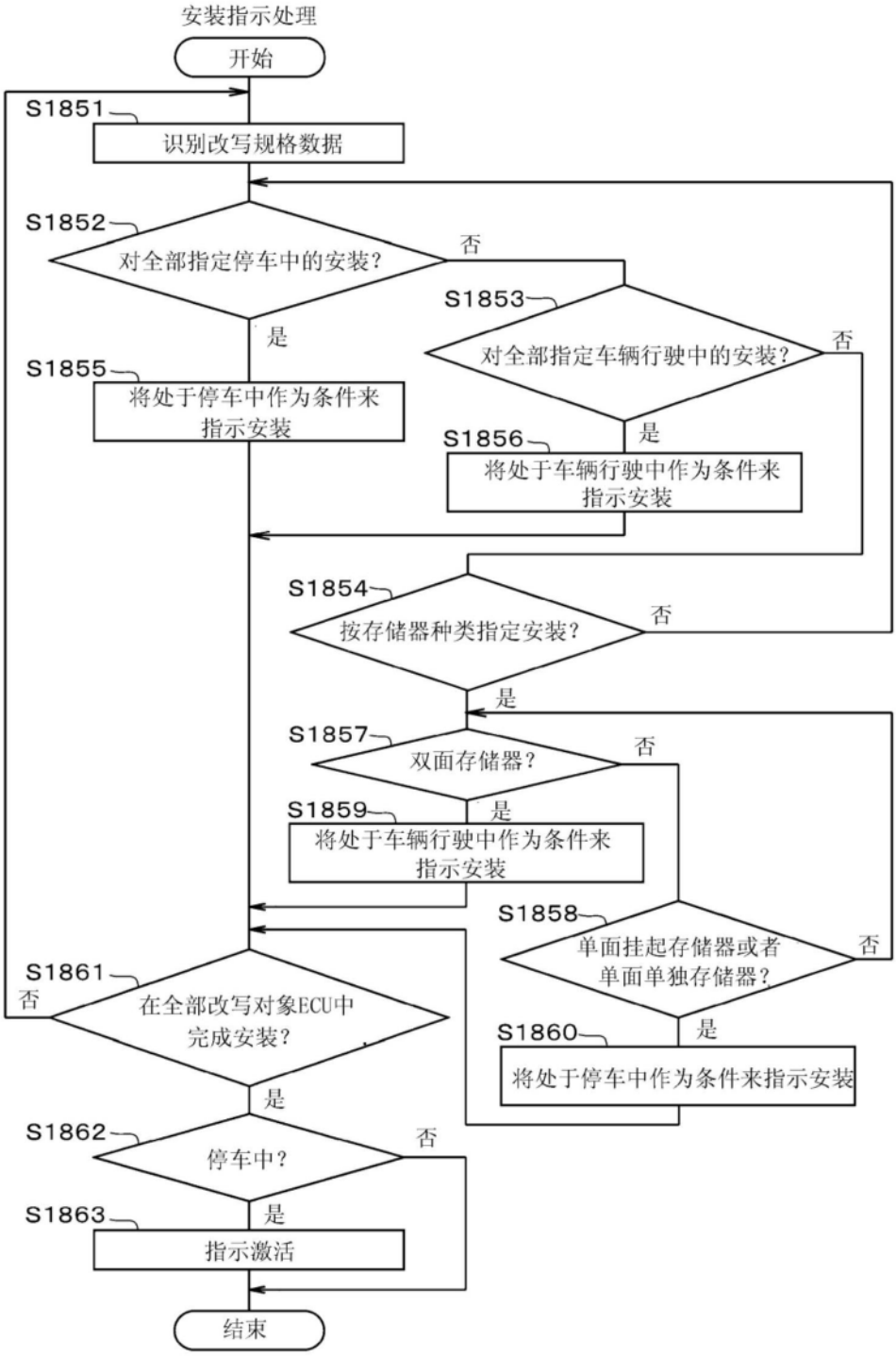

安装指示处理
开始
S1851
识别改写规格数据
S1852
对全部指定停车中的安装?
否
是
S1853
对全部指定车辆行驶中的安装?
否
是
S1855
将处于停车中作为条件来指示安装
S1856
将处于车辆行驶中作为条件来指示安装
S1854
按存储器种类指定安装?
否
是
S1857
双面存储器?
否
是
S1859
将处于车辆行驶中作为条件来指示安装
S1858
单面挂起存储器或者单面单独存储器?
否
是
S1860
将处于停车中作为条件来指示安装
S1861
在全部改写对象ECU中完成安装?
否
是
S1862
停车中?
否
是
S1863
指示激活
结束

图155

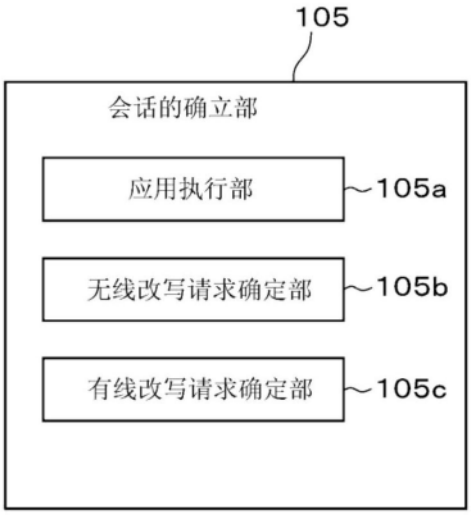

105
会话的确立部
应用执行部
105a
无线改写请求确定部
105b
有线改写请求确定部
105c

图156

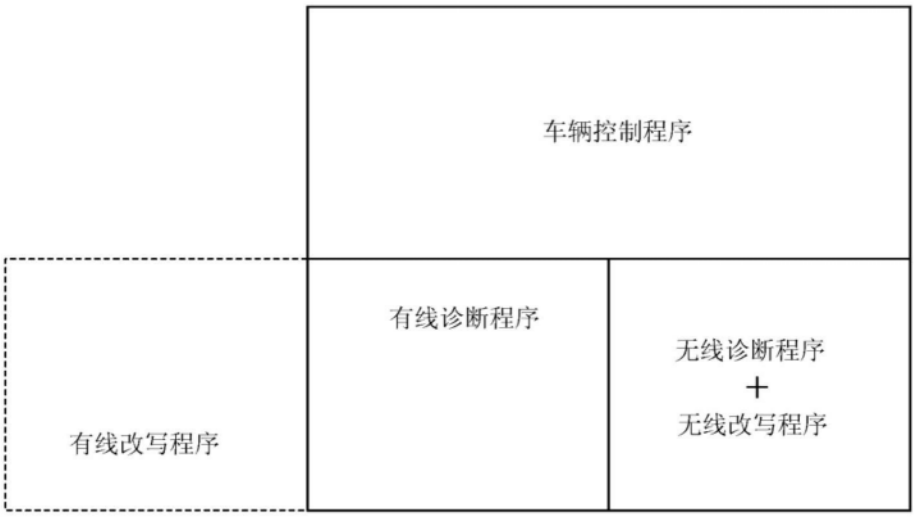

车辆控制程序
有线诊断程序
无线诊断程序
+
无线改写程序
有线改写程序

图157

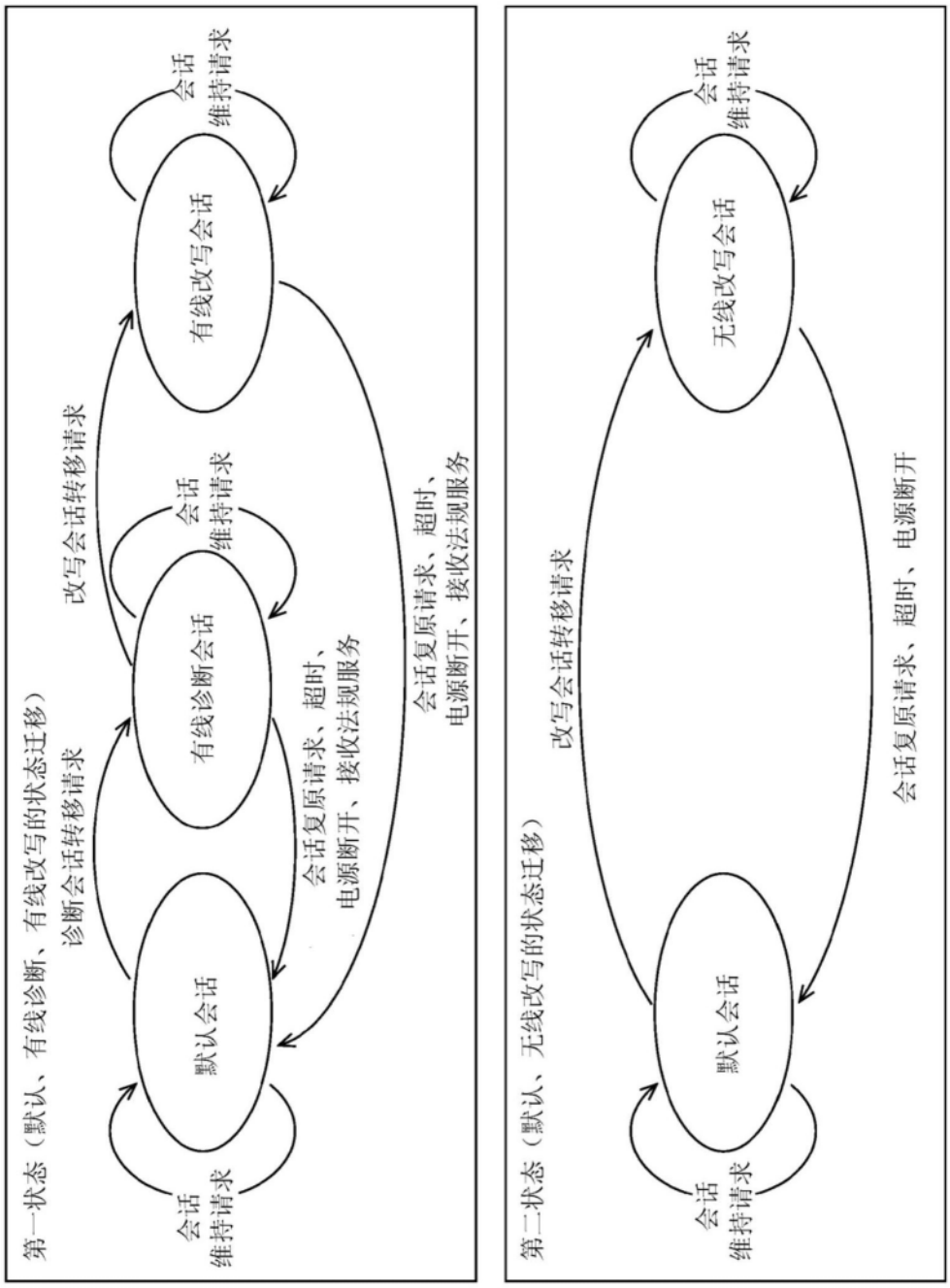

第一状态（默认、有线诊断、有线改写的状态迁移）
默认会话
有线诊断会话
有线改写会话
会话
维持请求
诊断会话转移请求
改写会话转移请求
会话复原请求、超时、
电源断开、接收法规服务
第二状态（默认、无线改写的状态迁移）
默认会话
无线改写会话
改写会话转移请求
会话复原请求、超时、电源断开

图158

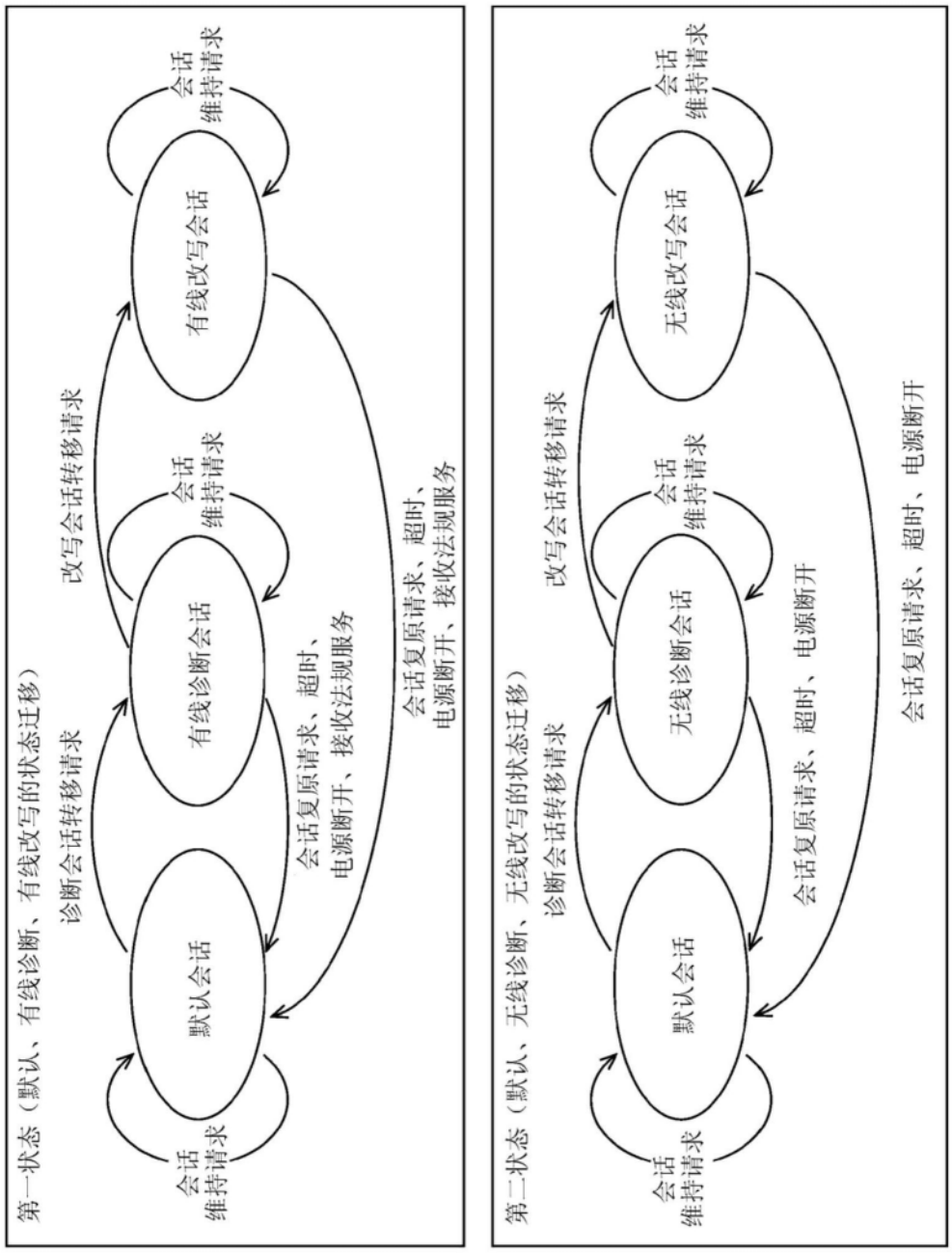

第一状态（默认、有线诊断、有线改写的状态迁移）
默认会话
有线诊断会话
有线改写会话
会话
维持请求
诊断会话转移请求
改写会话转移请求
会话复原请求、超时、
电源断开、接收法规服务
第二状态（默认、无线诊断、无线改写的状态迁移）
默认会话
无线诊断会话
无线改写会话
会话
维持请求
诊断会话转移请求
改写会话转移请求
会话复原请求、超时、电源断开

图159

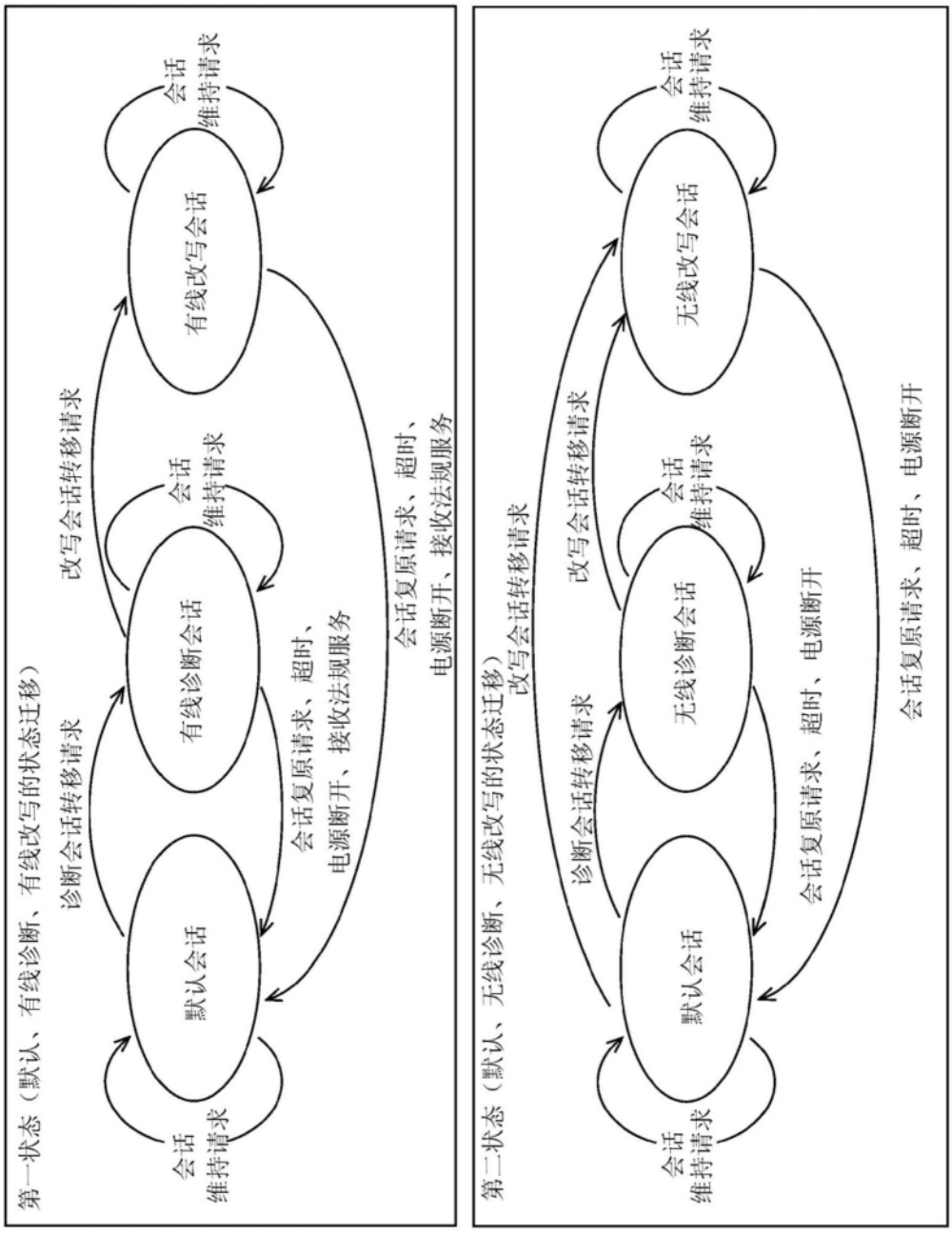
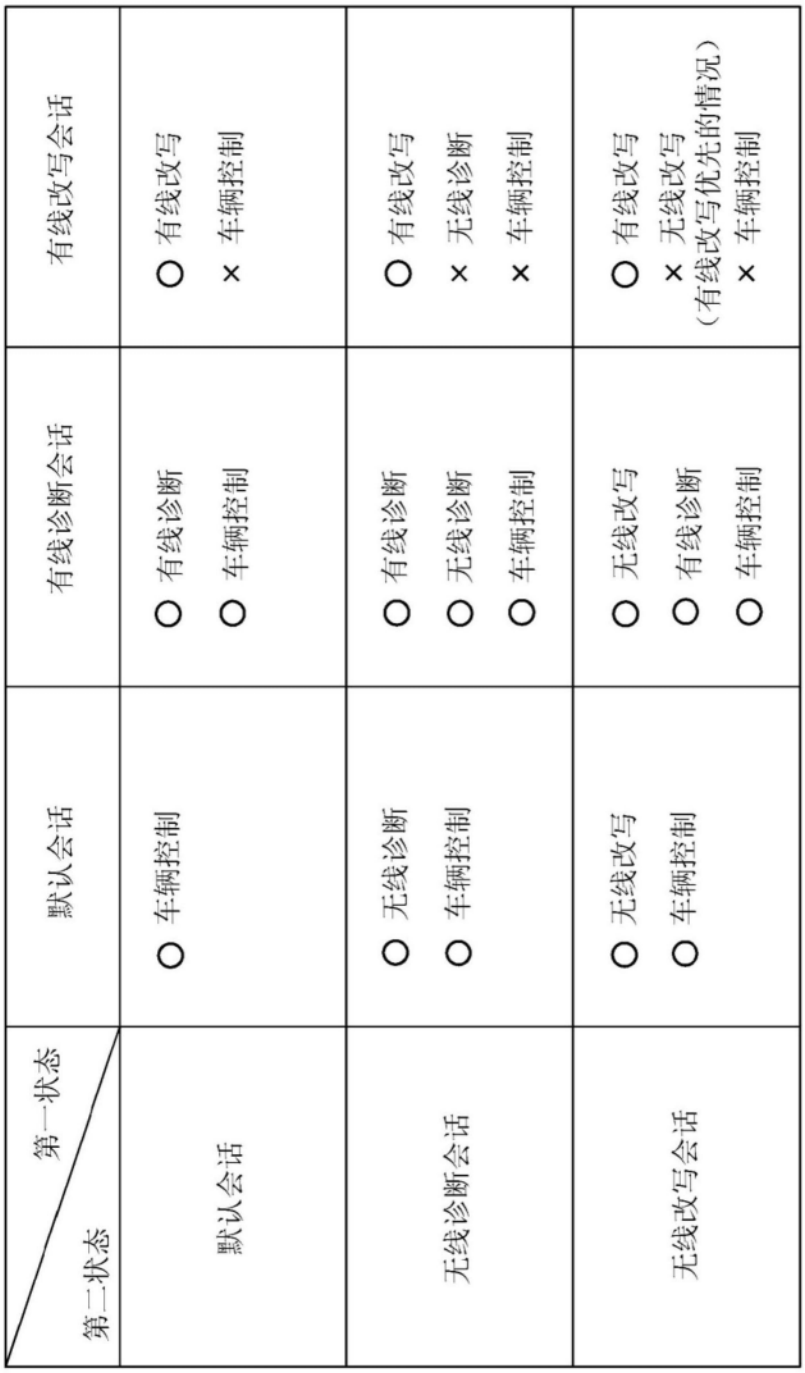

第一状态（默认、有线诊断、有线改写的状态迁移）
诊断会话转移请求
改写会话转移请求
会话
维持请求
默认会话
有线诊断会话
有线改写会话
会话复原请求、超时、
电源断开、接收法规服务
第二状态（默认、无线诊断、无线改写的状态迁移）
诊断会话转移请求
改写会话转移请求
无线诊断会话
无线改写会话
会话复原请求、超时、电源断开

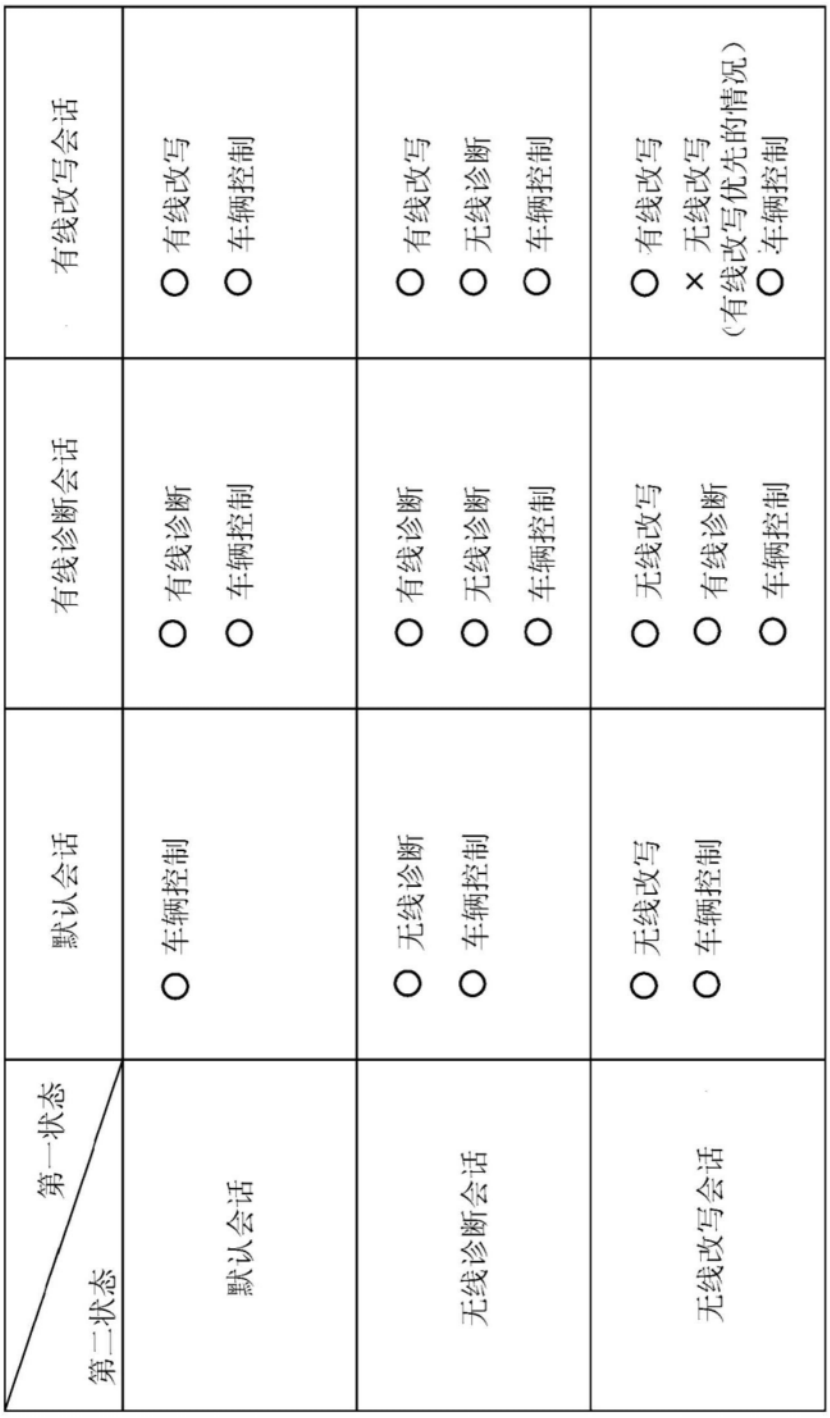
图160



第二状态 \ 第一状态	默认会话	有线诊断会话	有线改写会话
默认会话	○ 车辆控制	○ 有线诊断 ○ 车辆控制	○ 有线改写 × 车辆控制
无线诊断会话	○ 无线诊断 ○ 车辆控制	○ 有线诊断 ○ 无线诊断 ○ 车辆控制	○ 有线改写 × 无线诊断 × 车辆控制
无线改写会话	○ 无线改写 ○ 车辆控制	○ 无线改写 ○ 有线诊断 ○ 车辆控制	○ 有线改写 × 无线改写 （有线改写优先的情况） × 车辆控制

○：能够执行
×：不能执行

图161



第一状态 / 第二状态	默认会话	有线诊断会话	有线改写会话
默认会话	○ 车辆控制	○ 有线诊断 ○ 车辆控制	○ 有线改写 ○ 车辆控制
无线诊断会话	○ 无线诊断 ○ 车辆控制	○ 有线诊断 ○ 无线诊断 ○ 车辆控制	○ 有线改写 ○ 无线诊断 ○ 车辆控制
无线改写会话	○ 无线改写 ○ 车辆控制	○ 无线改写 ○ 有线诊断 ○ 车辆控制	○ 有线改写 × 无线改写 （有线改写优先的情况） ○ 车辆控制

○：能够执行
×：不能执行

图162

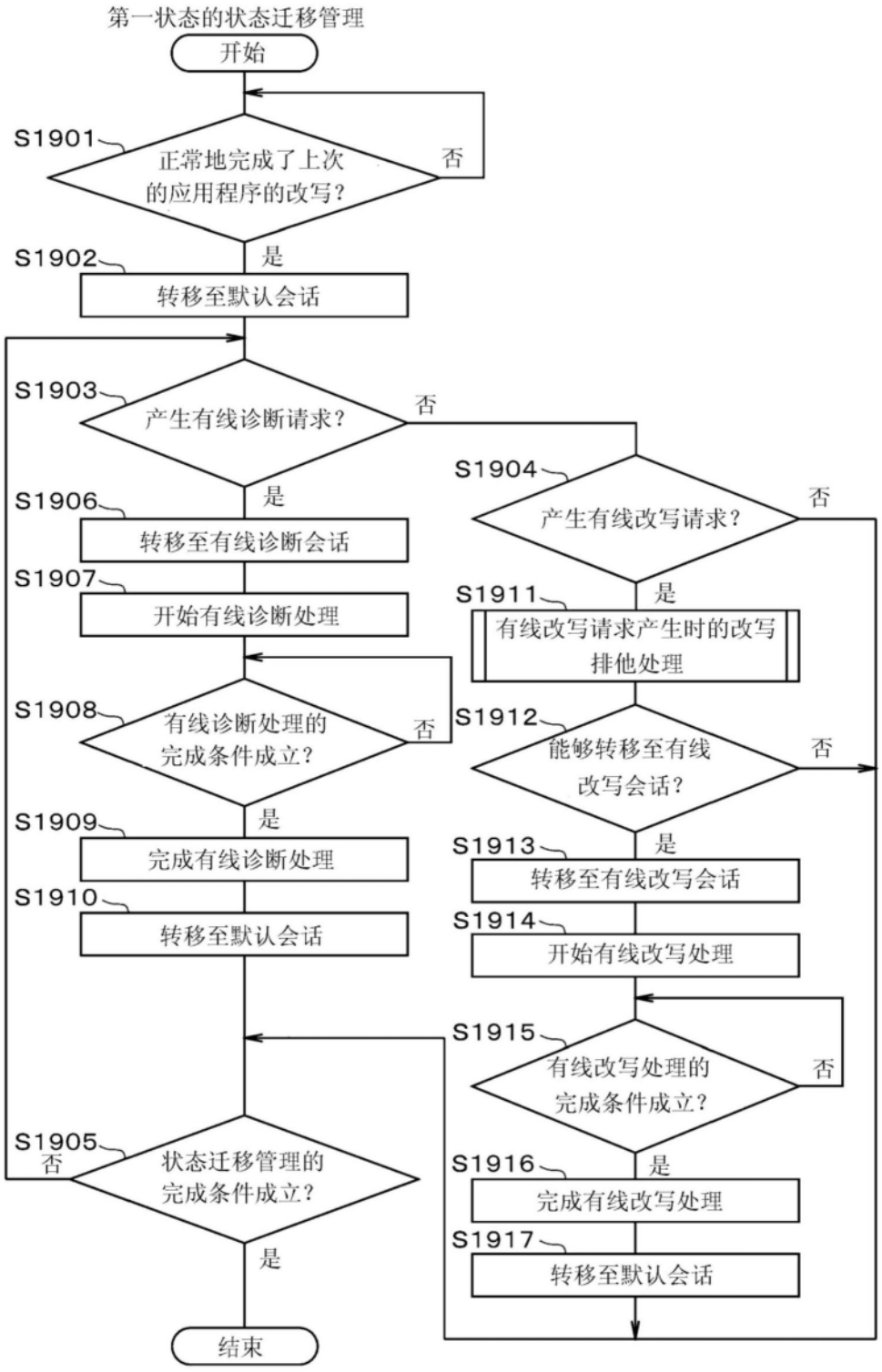

第一状态的状态迁移管理
开始
S1901
正常地完成了上次的应用程序的改写？
否
是
S1902
转移至默认会话
S1903
产生有线诊断请求？
否
是
S1904
产生有线改写请求？
否
是
S1906
转移至有线诊断会话
S1907
开始有线诊断处理
S1908
有线诊断处理的完成条件成立？
否
是
S1909
完成有线诊断处理
S1910
转移至默认会话
S1911
有线改写请求产生时的改写排他处理
S1912
能够转移至有线改写会话？
否
是
S1913
转移至有线改写会话
S1914
开始有线改写处理
S1915
有线改写处理的完成条件成立？
否
是
S1916
完成有线改写处理
S1917
转移至默认会话
S1905
否
状态迁移管理的完成条件成立？
是
结束

图163

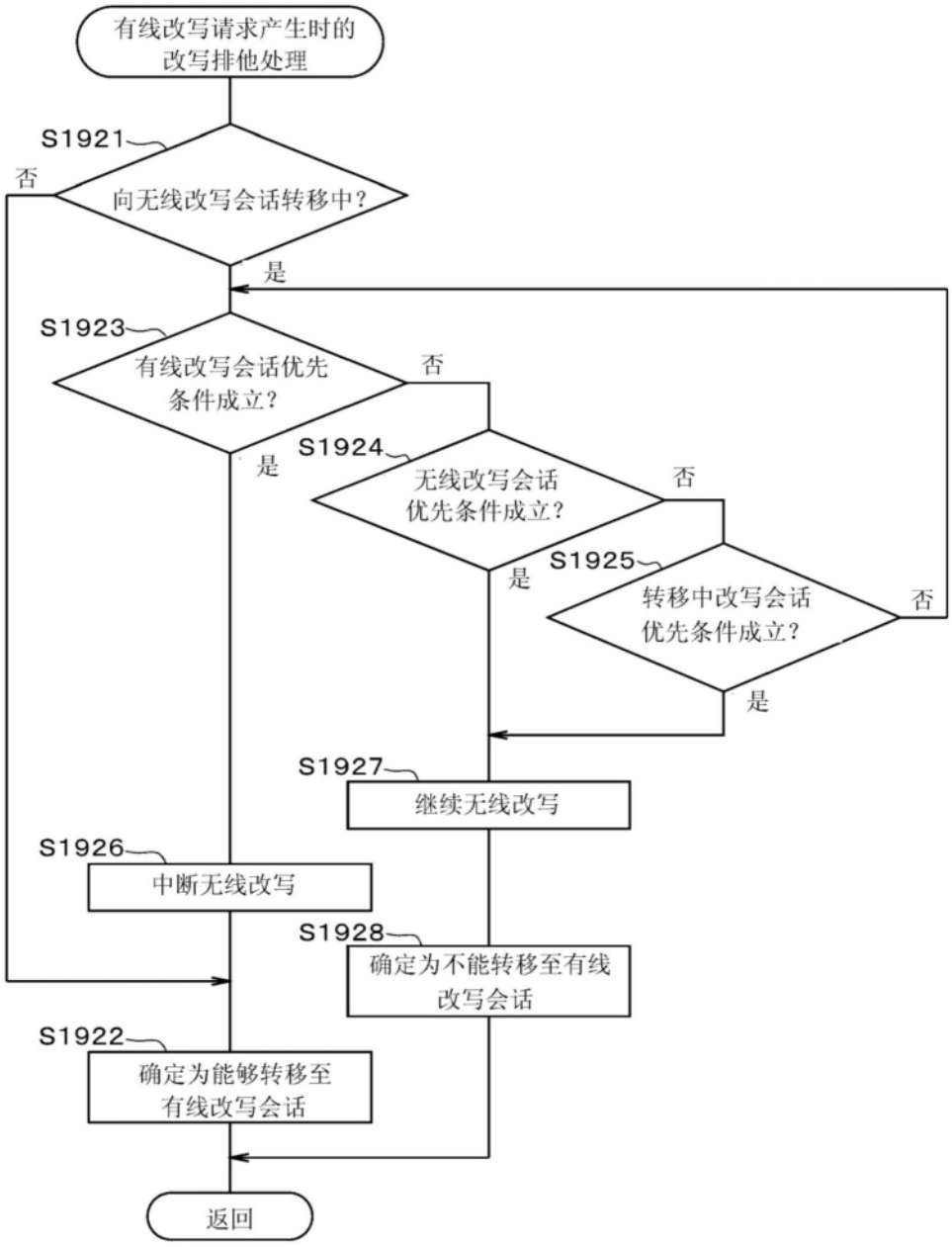

有线改写请求产生时的
改写排他处理
S1921
向无线改写会话转移中?
否
是
S1923
有线改写会话优先
条件成立?
否
是
S1924
无线改写会话
优先条件成立?
否
是
S1925
转移中改写会话
优先条件成立?
否
是
S1927
继续无线改写
S1926
中断无线改写
S1928
确定为不能转移至有线
改写会话
S1922
确定为能够转移至
有线改写会话
返回

图164

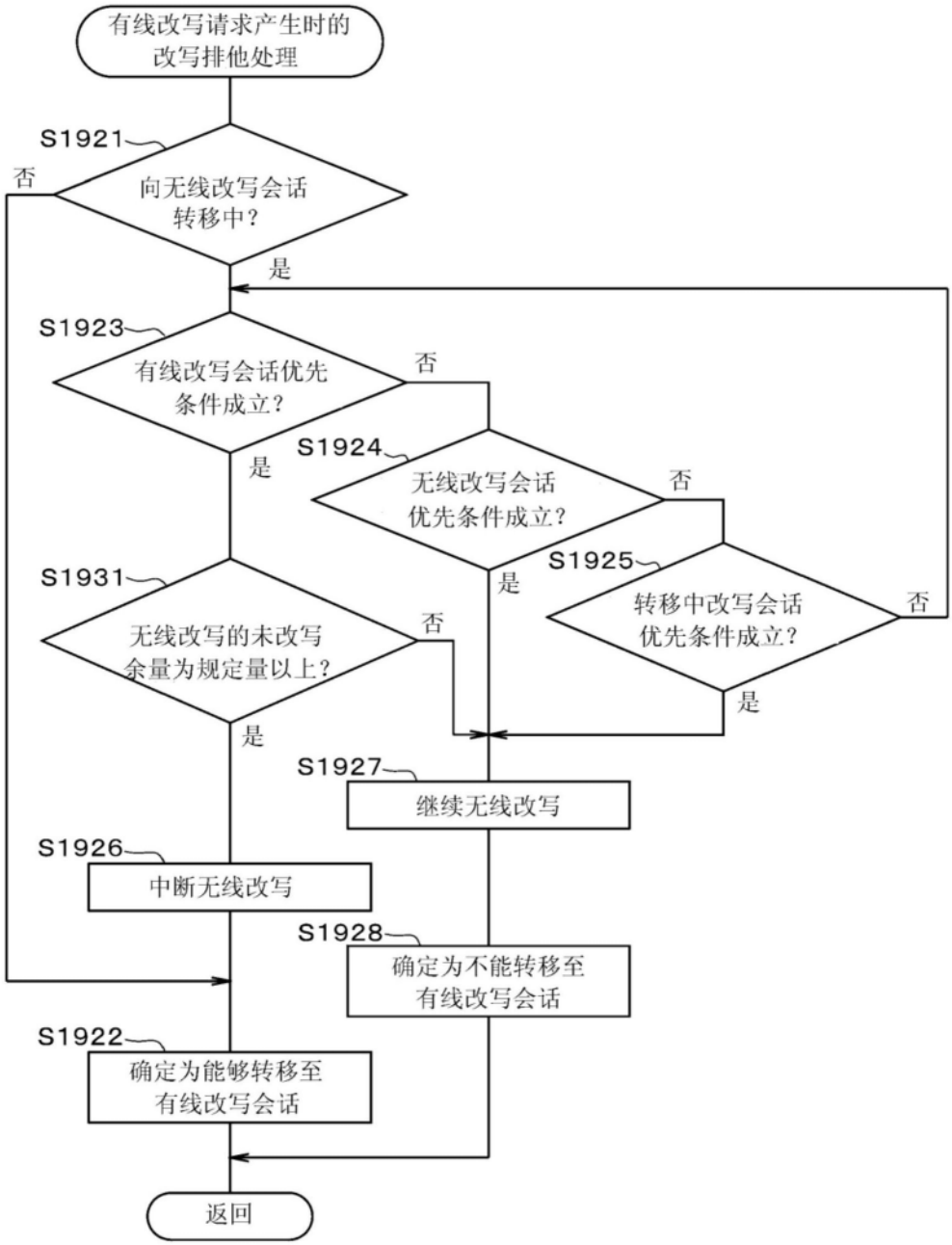

有线改写请求产生时的
改写排他处理
S1921
向无线改写会话
转移中？
否
是
S1923
有线改写会话优先
条件成立？
否
是
S1924
无线改写会话
优先条件成立？
否
是
S1925
转移中改写会话
优先条件成立？
否
是
S1931
无线改写的未改写
余量为规定量以上？
否
是
S1927
继续无线改写
S1926
中断无线改写
S1928
确定为不能转移至
有线改写会话
S1922
确定为能够转移至
有线改写会话
返回

图165

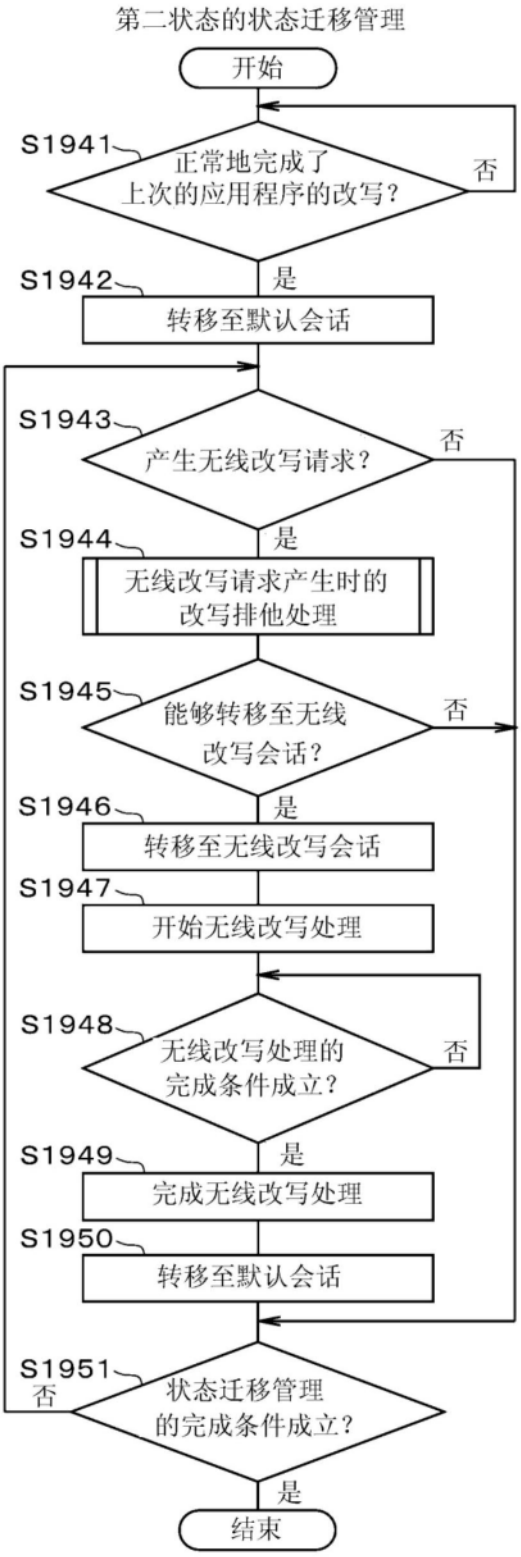

第二状态的状态迁移管理
开始
S1941
正常地完成了
上次的应用程序的改写？
否
是
S1942
转移至默认会话
S1943
产生无线改写请求？
否
是
S1944
无线改写请求产生时的
改写排他处理
S1945
能够转移至无线
改写会话？
否
是
S1946
转移至无线改写会话
S1947
开始无线改写处理
S1948
无线改写处理的
完成条件成立？
否
是
S1949
完成无线改写处理
S1950
转移至默认会话
S1951
状态迁移管理
的完成条件成立？
否
是
结束

图166

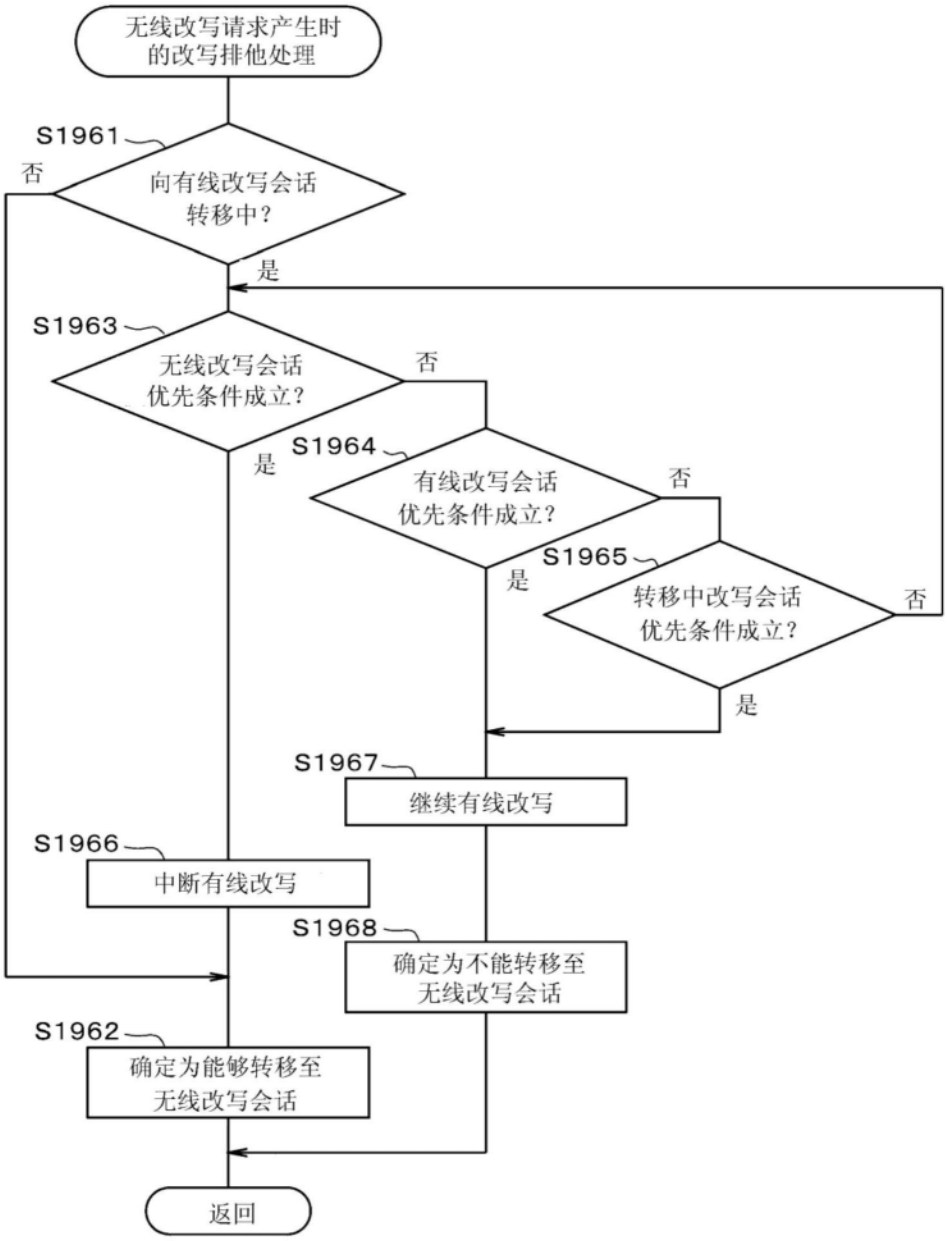

无线改写请求产生时
的改写排他处理
S1961
向有线改写会话
转移中？
否
是
S1963
无线改写会话
优先条件成立？
否
是
S1964
有线改写会话
优先条件成立？
否
是
S1965
转移中改写会话
优先条件成立？
否
是
S1967
继续有线改写
S1966
中断有线改写
S1968
确定为不能转移至
无线改写会话
S1962
确定为能够转移至
无线改写会话
返回

图167

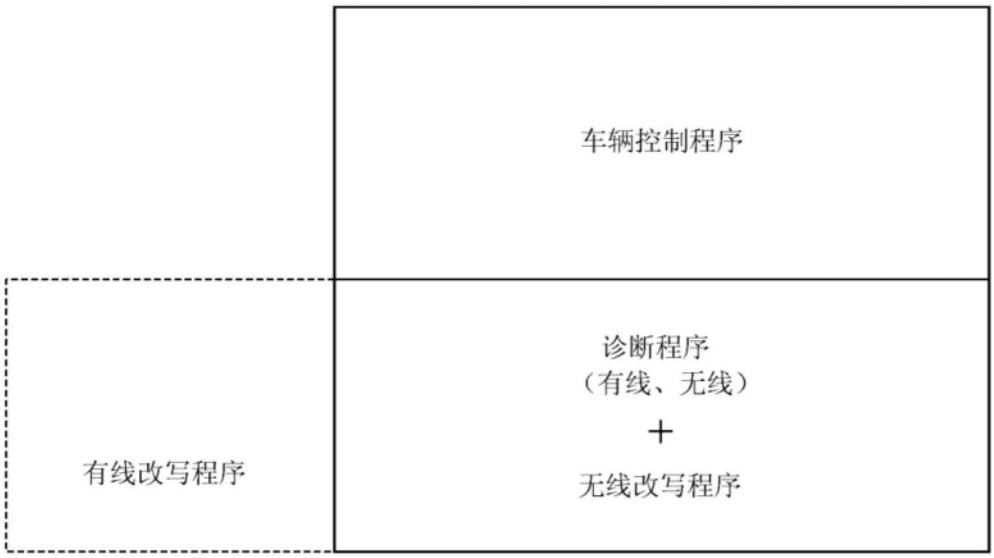


图168

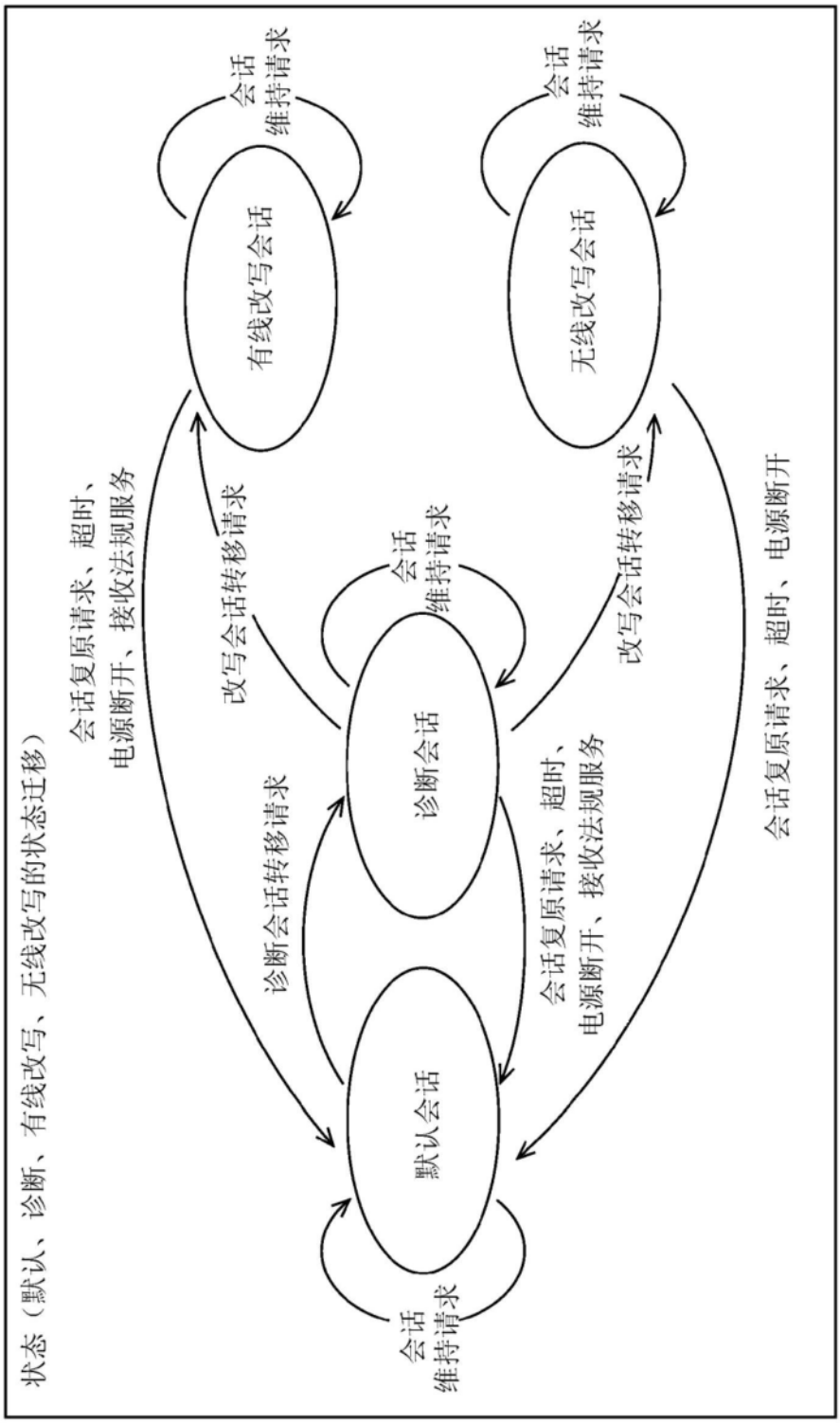

状态（默认、诊断、有线改写、无线改写的状态迁移）
会话
维持请求
有线改写会话
会话
维持请求
无线改写会话
会话复原请求、超时、
电源断开、接收法规服务
改写会话转移请求
会话
维持请求
改写会话转移请求
诊断会话转移请求
诊断会话
会话复原请求、超时、
电源断开、接收法规服务
会话复原请求、超时、电源断开
默认会话
会话
维持请求

图169

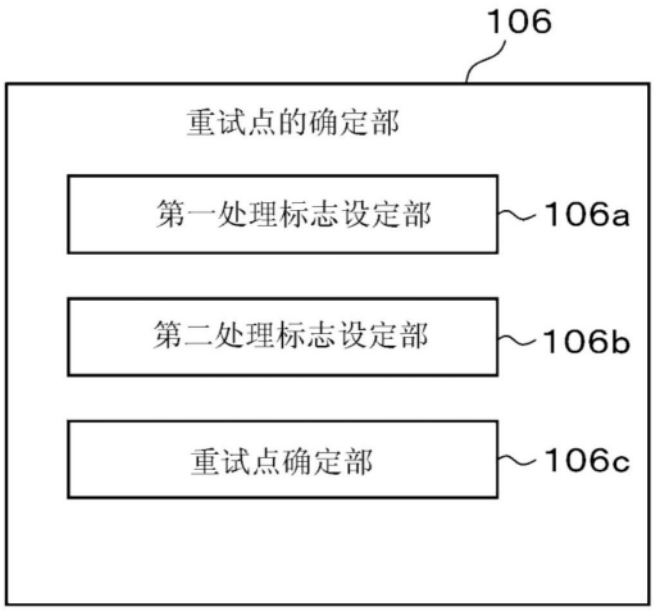

106
重试点的确定部
第一处理标志设定部
106a
第二处理标志设定部
106b
重试点确定部
106c

图170

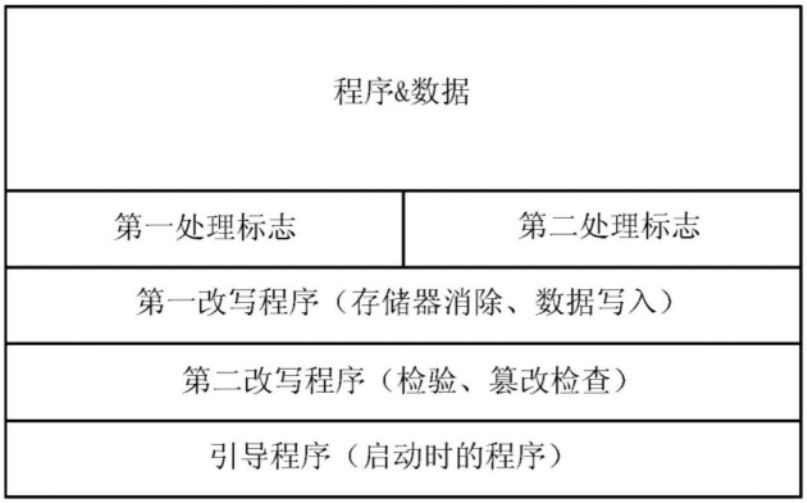

程序&数据
第一处理标志
第二处理标志
第一改写程序（存储器消除、数据写入）
第二改写程序（检验、篡改检查）
引导程序（启动时的程序）

图171

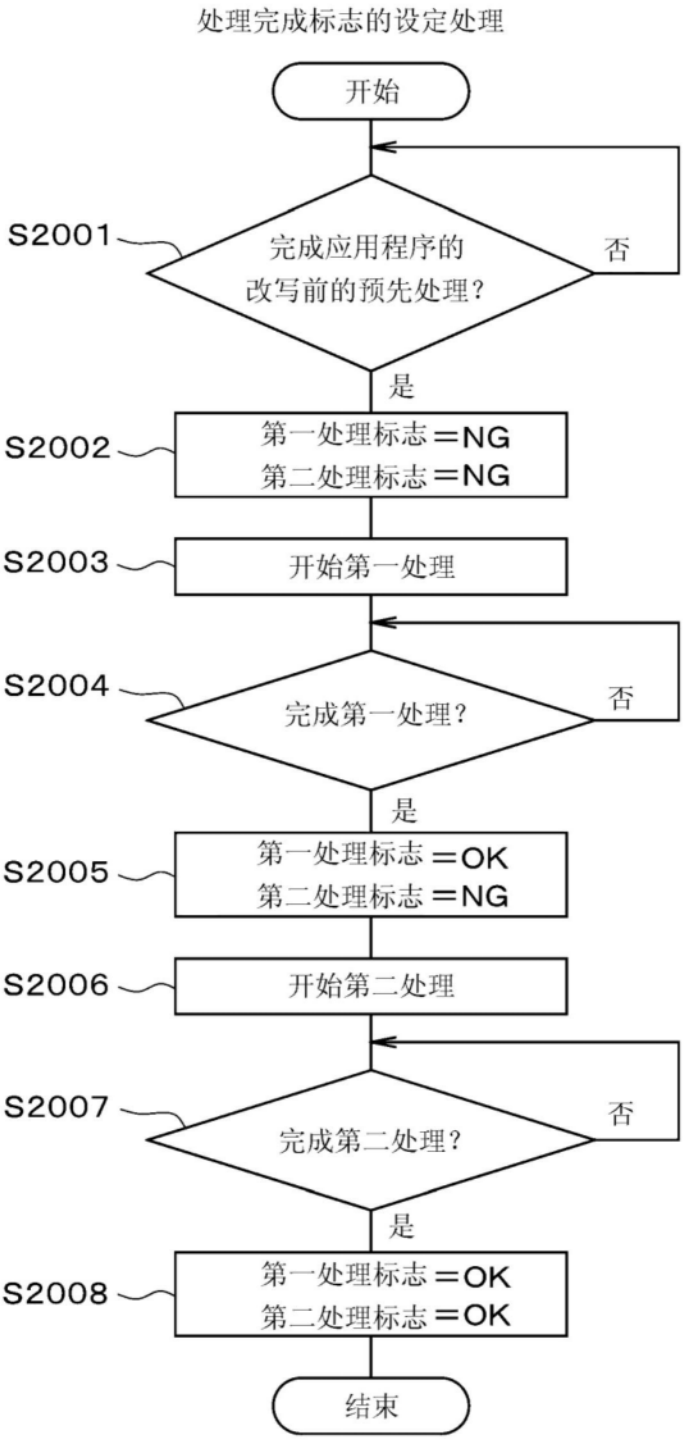

处理完成标志的设定处理
开始
S2001
完成应用程序的
改写前的预先处理？
否
是
S2002
第一处理标志＝NG
第二处理标志＝NG
S2003
开始第一处理
S2004
完成第一处理？
否
是
S2005
第一处理标志＝OK
第二处理标志＝NG
S2006
开始第二处理
S2007
完成第二处理？
否
是
S2008
第一处理标志＝OK
第二处理标志＝OK
结束

图172

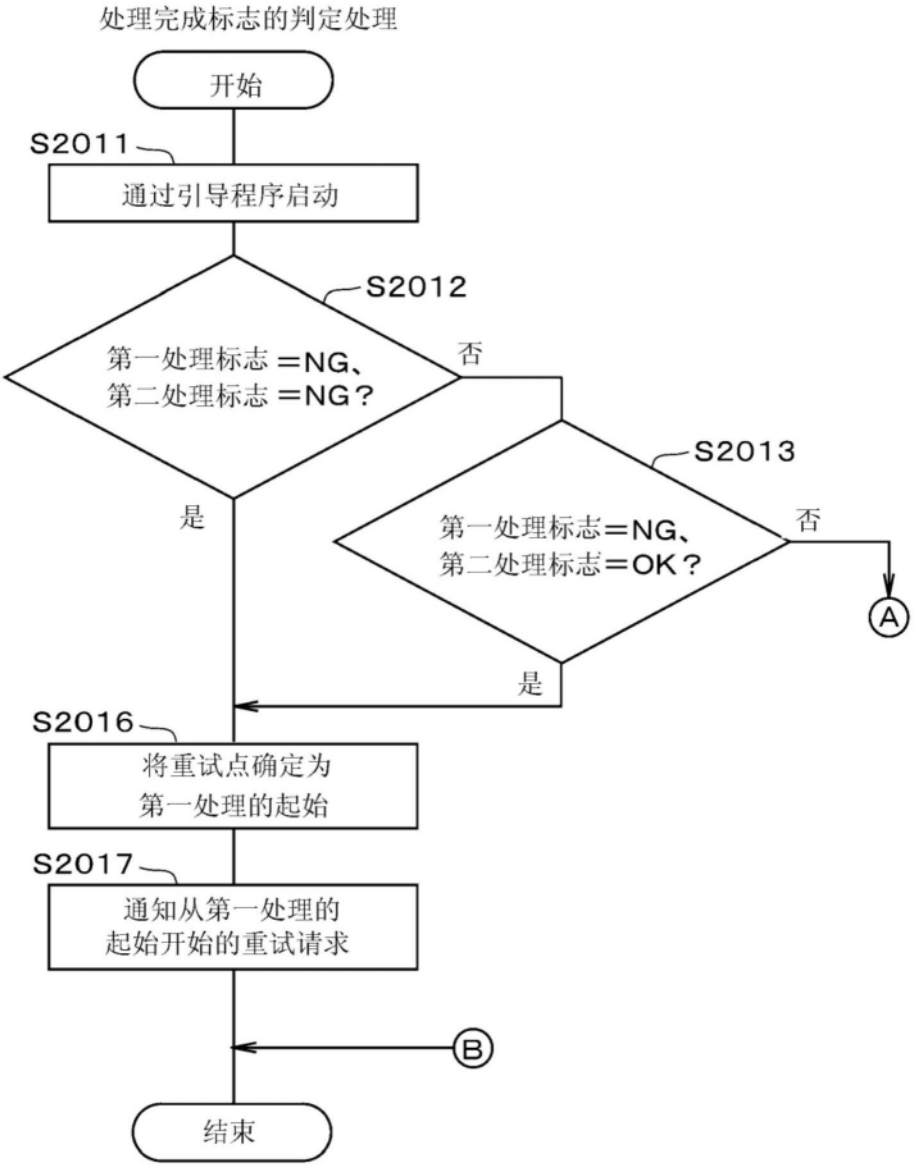

处理完成标志的判定处理
开始
S2011
通过引导程序启动
S2012
第一处理标志 =NG、
第二处理标志 =NG？
否
是
S2013
第一处理标志=NG、
第二处理标志=OK？
否
A
是
S2016
将重试点确定为
第一处理的起始
S2017
通知从第一处理的
起始开始的重试请求
B
结束

图173

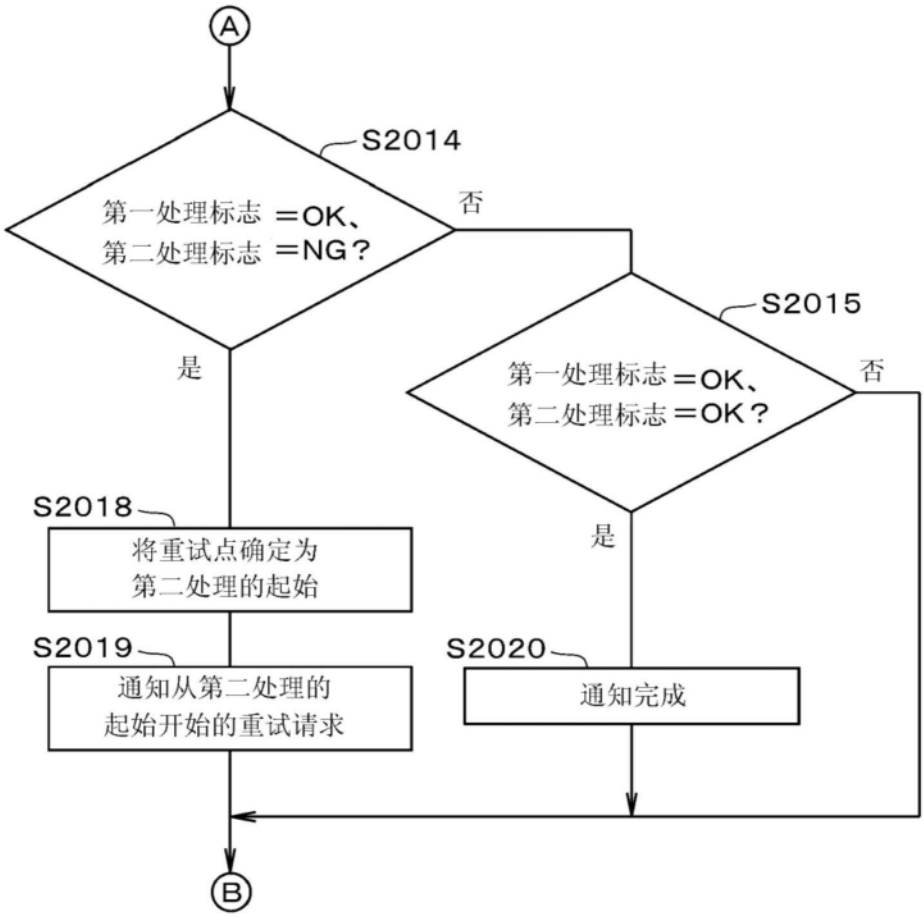

A
S2014
第一处理标志 =OK、
第二处理标志 =NG？
否
是
S2015
第一处理标志 =OK、
第二处理标志 =OK？
否
是
S2018
将重试点确定为
第二处理的起始
S2019
通知从第二处理的
起始开始的重试请求
S2020
通知完成
B

图174

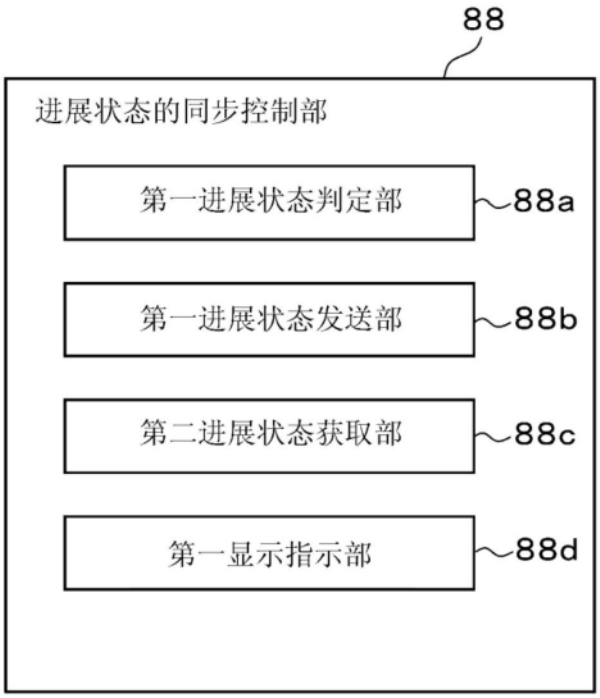

88
进展状态的同步控制部
第一进展状态判定部
88a
第一进展状态发送部
88b
第二进展状态获取部
88c
第一显示指示部
88d

图175

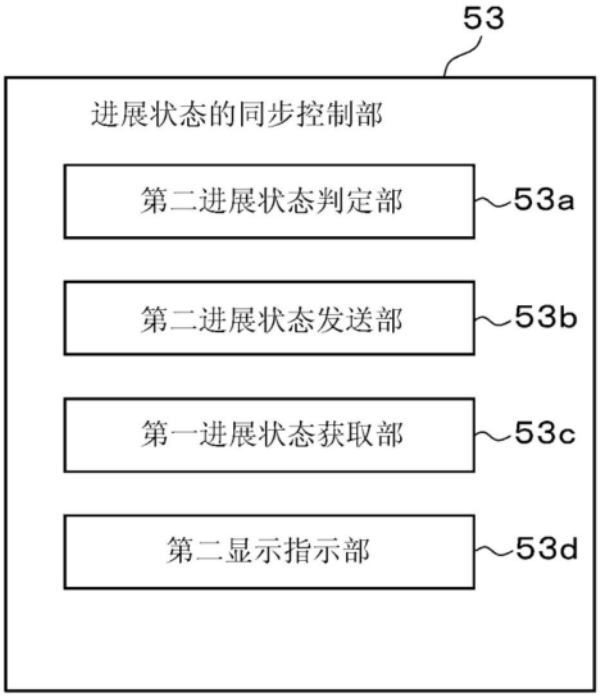

53
进展状态的同步控制部
第二进展状态判定部
53a
第二进展状态发送部
53b
第一进展状态获取部
53c
第二显示指示部
53d

图176

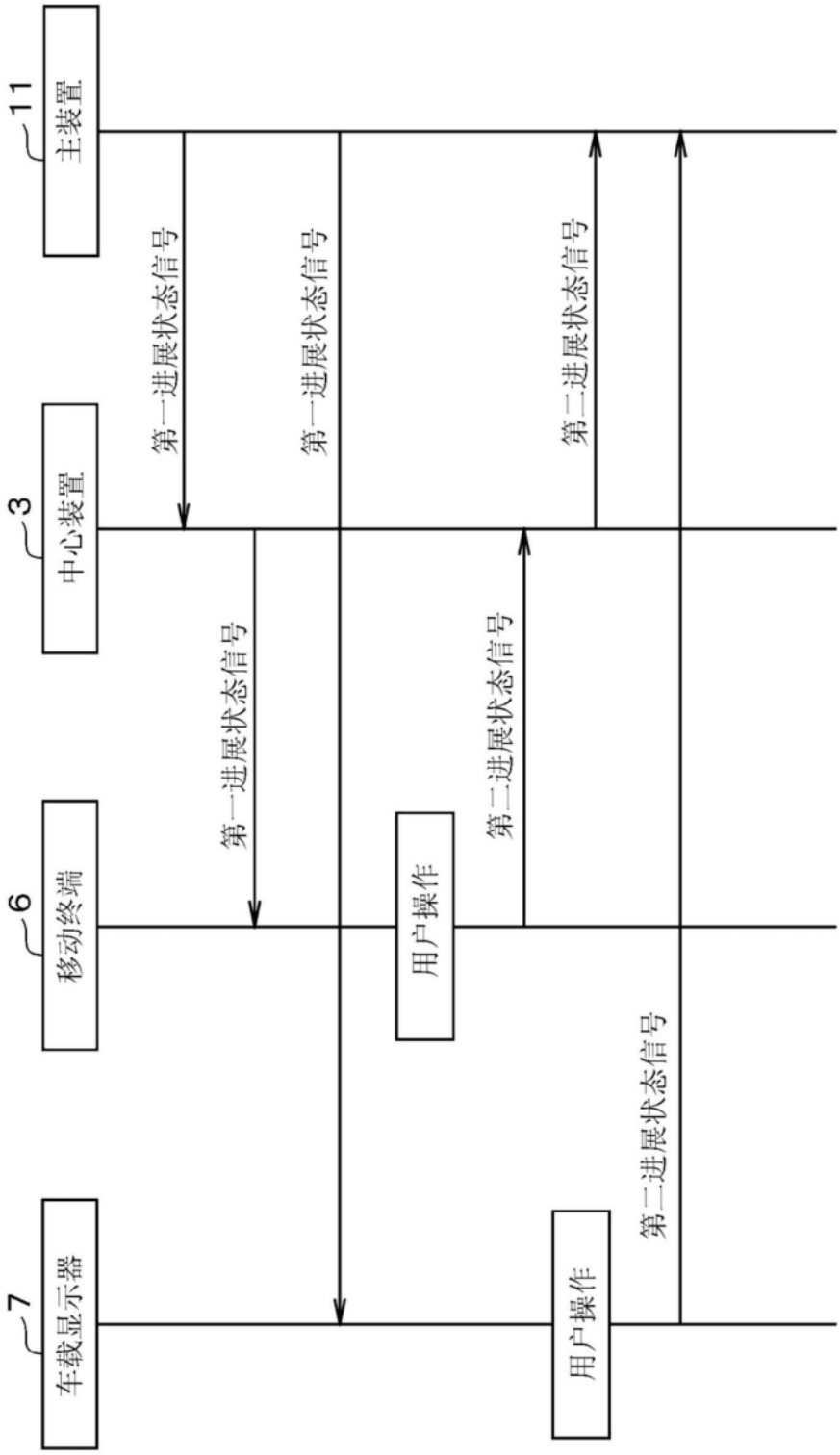

11
主装置
3
中心装置
6
移动终端
7
车载显示器
第一进展状态信号
第一进展状态信号
第二进展状态信号
第一进展状态信号
第二进展状态信号
用户操作
用户操作
第二进展状态信号

图177

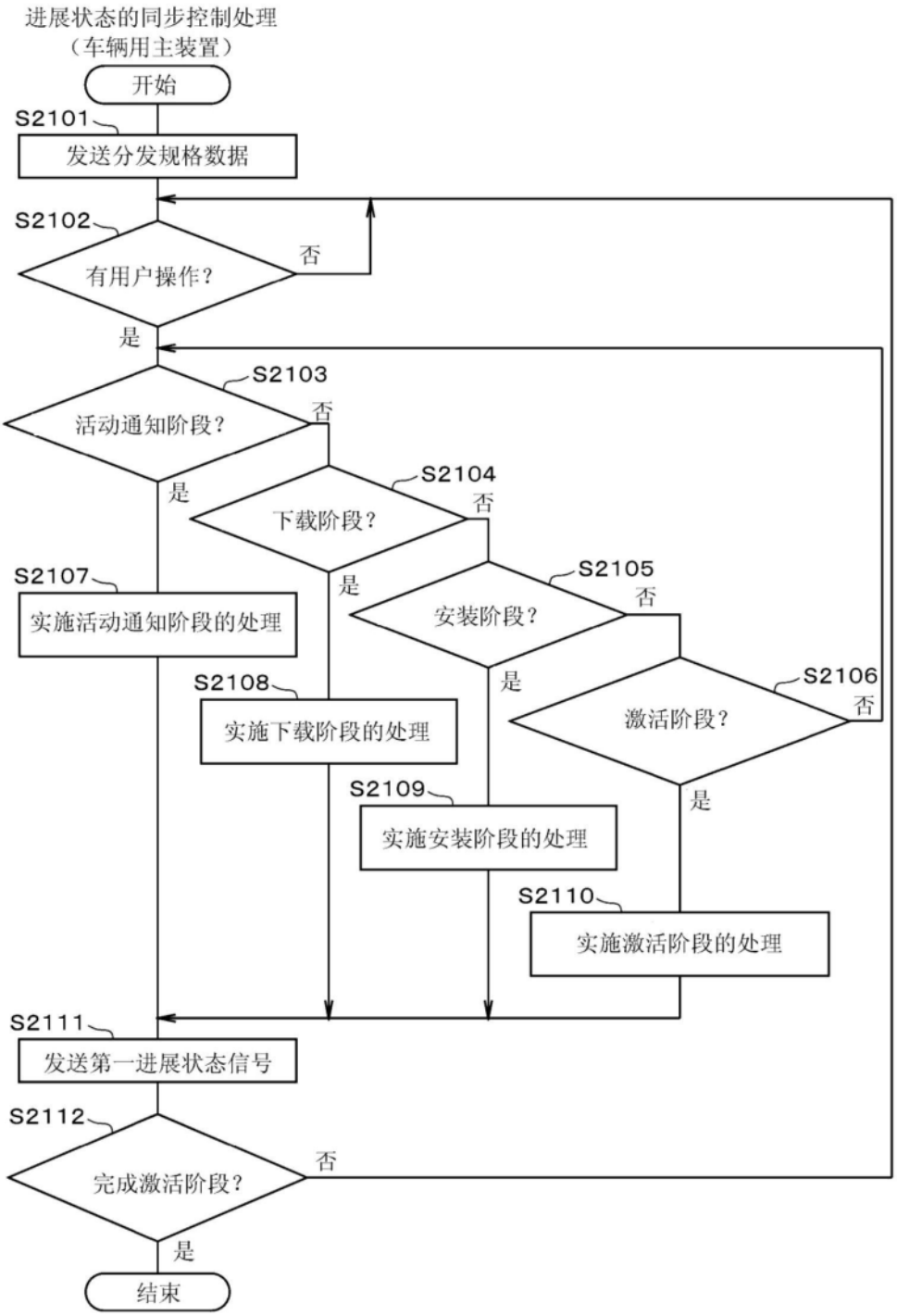

进展状态的同步控制处理
（车辆用主装置）
开始
S2101
发送分发规格数据
S2102
有用户操作？
否
是
S2103
活动通知阶段？
否
是
S2104
下载阶段？
否
是
S2105
安装阶段？
否
是
S2106
激活阶段？
否
是
S2107
实施活动通知阶段的处理
S2108
实施下载阶段的处理
S2109
实施安装阶段的处理
S2110
实施激活阶段的处理
S2111
发送第一进展状态信号
S2112
完成激活阶段？
否
是
结束

图178

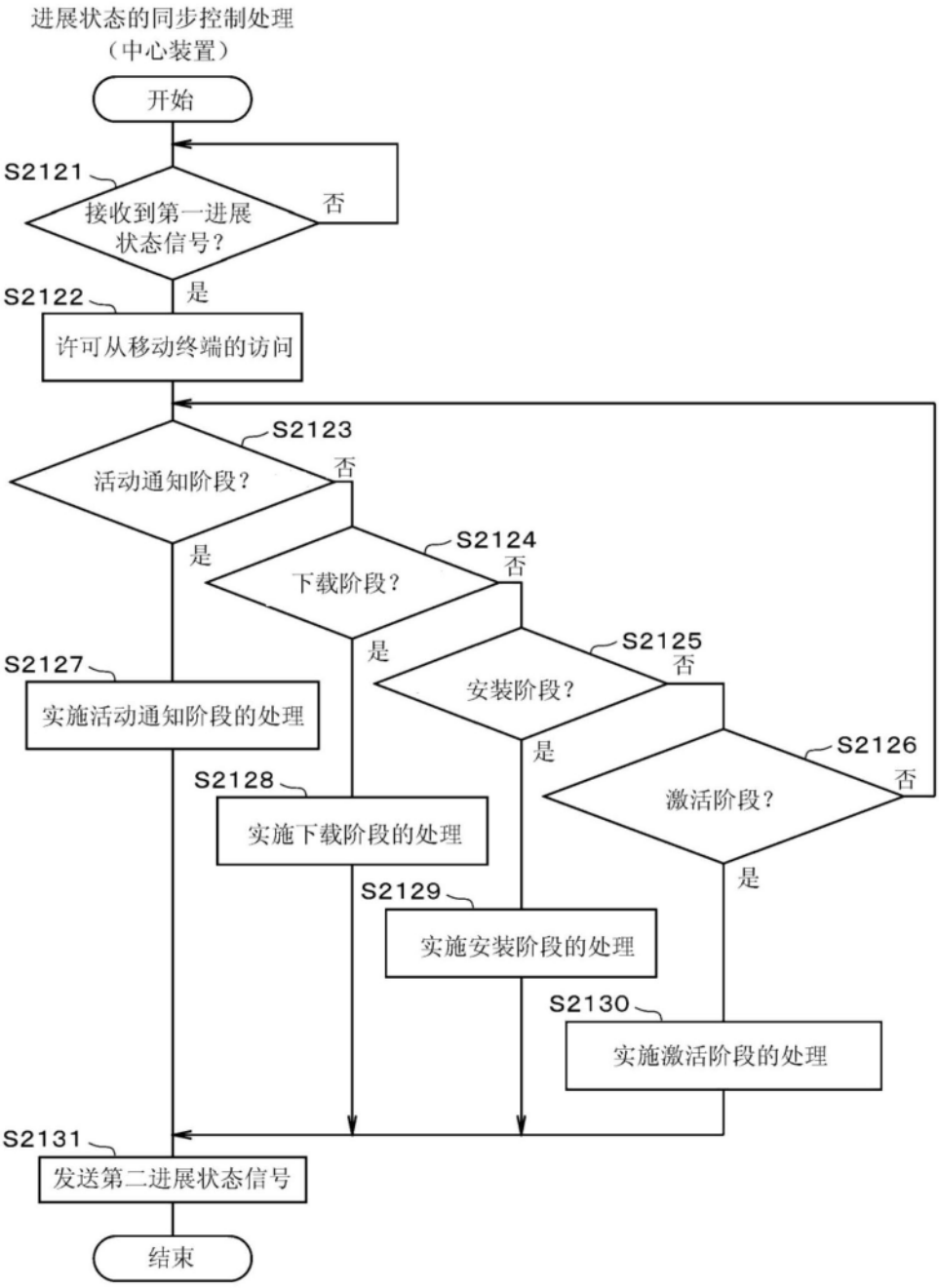

进展状态的同步控制处理
（中心装置）
开始
S2121
接收到第一进展状态信号？
否
是
S2122
许可从移动终端的访问
S2123
活动通知阶段？
否
是
S2124
下载阶段？
否
是
S2125
安装阶段？
否
是
S2126
激活阶段？
否
是
S2127
实施活动通知阶段的处理
S2128
实施下载阶段的处理
S2129
实施安装阶段的处理
S2130
实施激活阶段的处理
S2131
发送第二进展状态信号
结束

图179

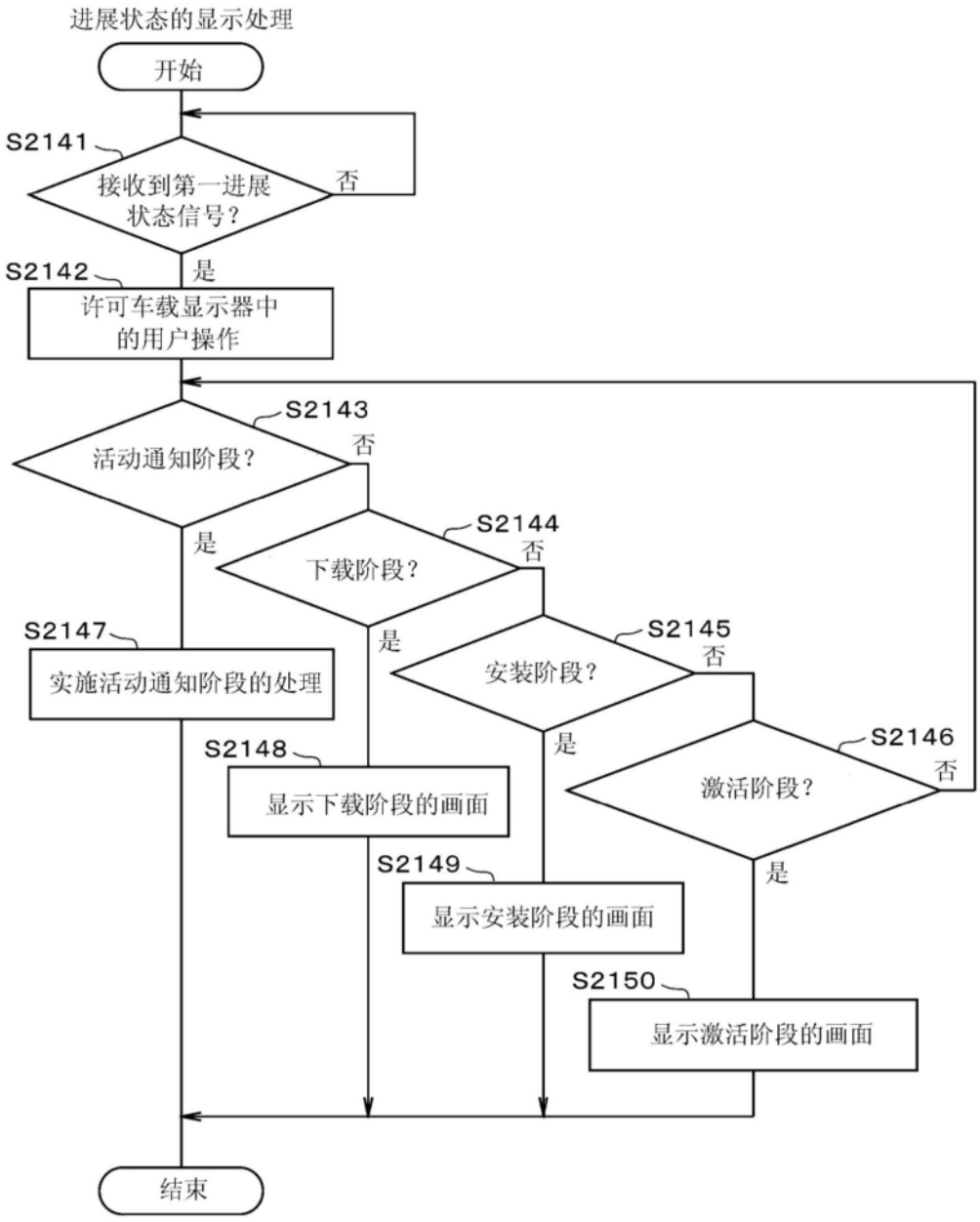

进展状态的显示处理
开始
S2141
接收到第一进展状态信号？
否
是
S2142
许可车载显示器中的用户操作
S2143
活动通知阶段？
否
是
S2144
下载阶段？
否
是
S2145
安装阶段？
否
是
S2146
激活阶段？
否
是
S2147
实施活动通知阶段的处理
S2148
显示下载阶段的画面
S2149
显示安装阶段的画面
S2150
显示激活阶段的画面
结束

图180

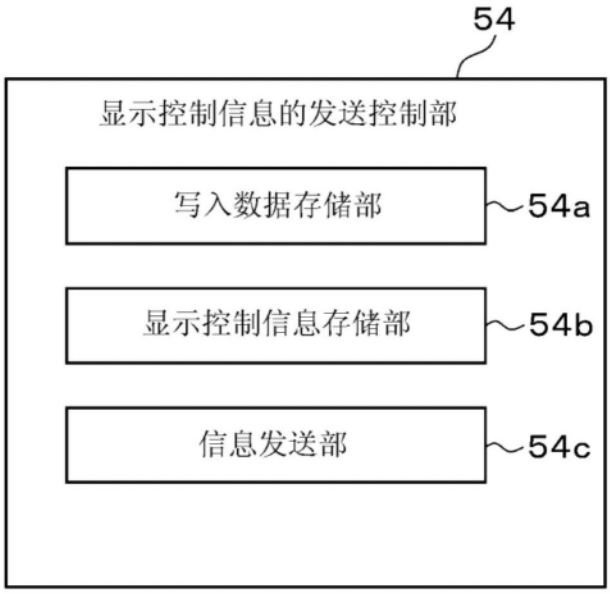

54
显示控制信息的发送控制部
写入数据存储部
54a
显示控制信息存储部
54b
信息发送部
54c

图181

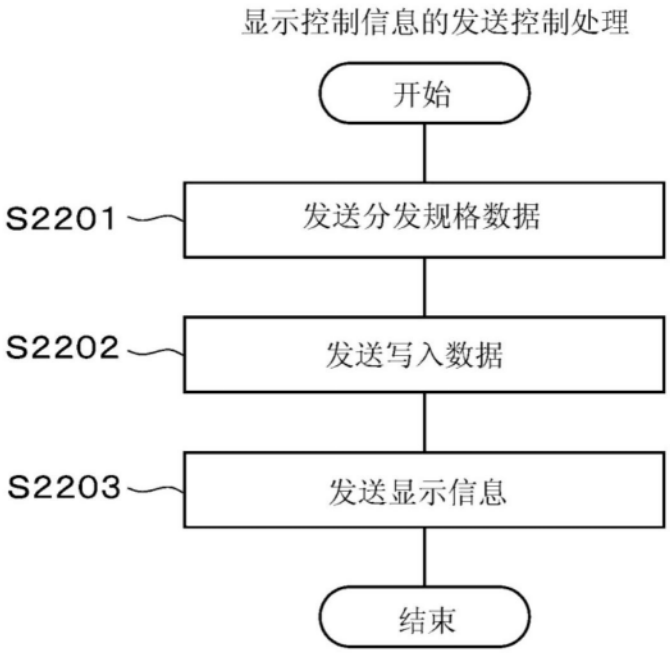

显示控制信息的发送控制处理
开始
S2201
发送分发规格数据
S2202
发送写入数据
S2203
发送显示信息
结束

图182

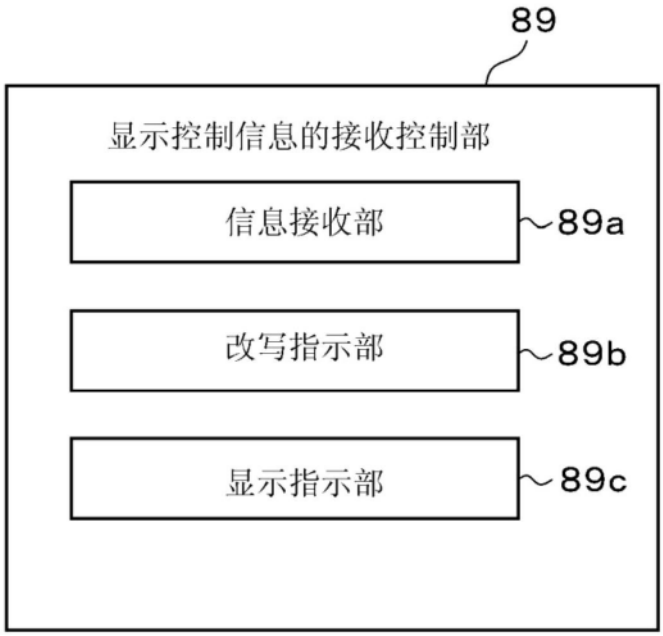


图183

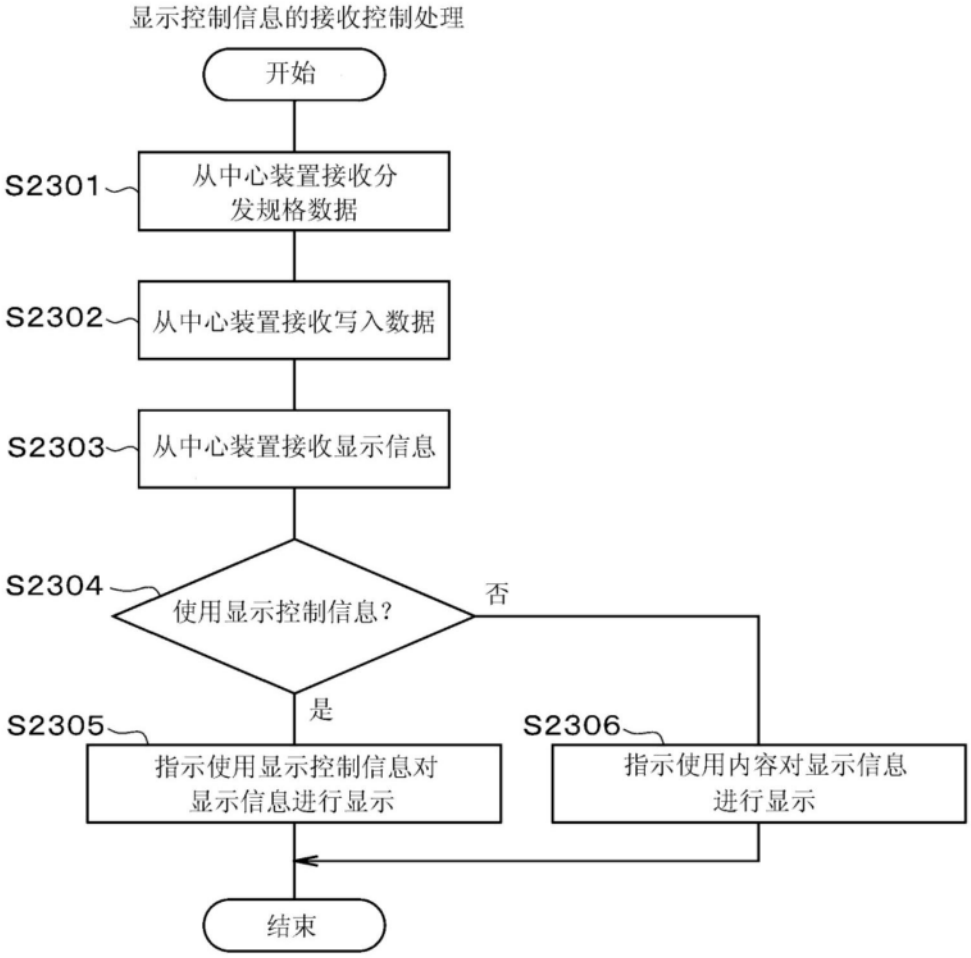

显示控制信息的接收控制处理
开始
S2301
从中心装置接收分发规格数据
S2302
从中心装置接收写入数据
S2303
从中心装置接收显示信息
S2304
使用显示控制信息？
否
是
S2305
指示使用显示控制信息对显示信息进行显示
S2306
指示使用内容对显示信息进行显示
结束

图184

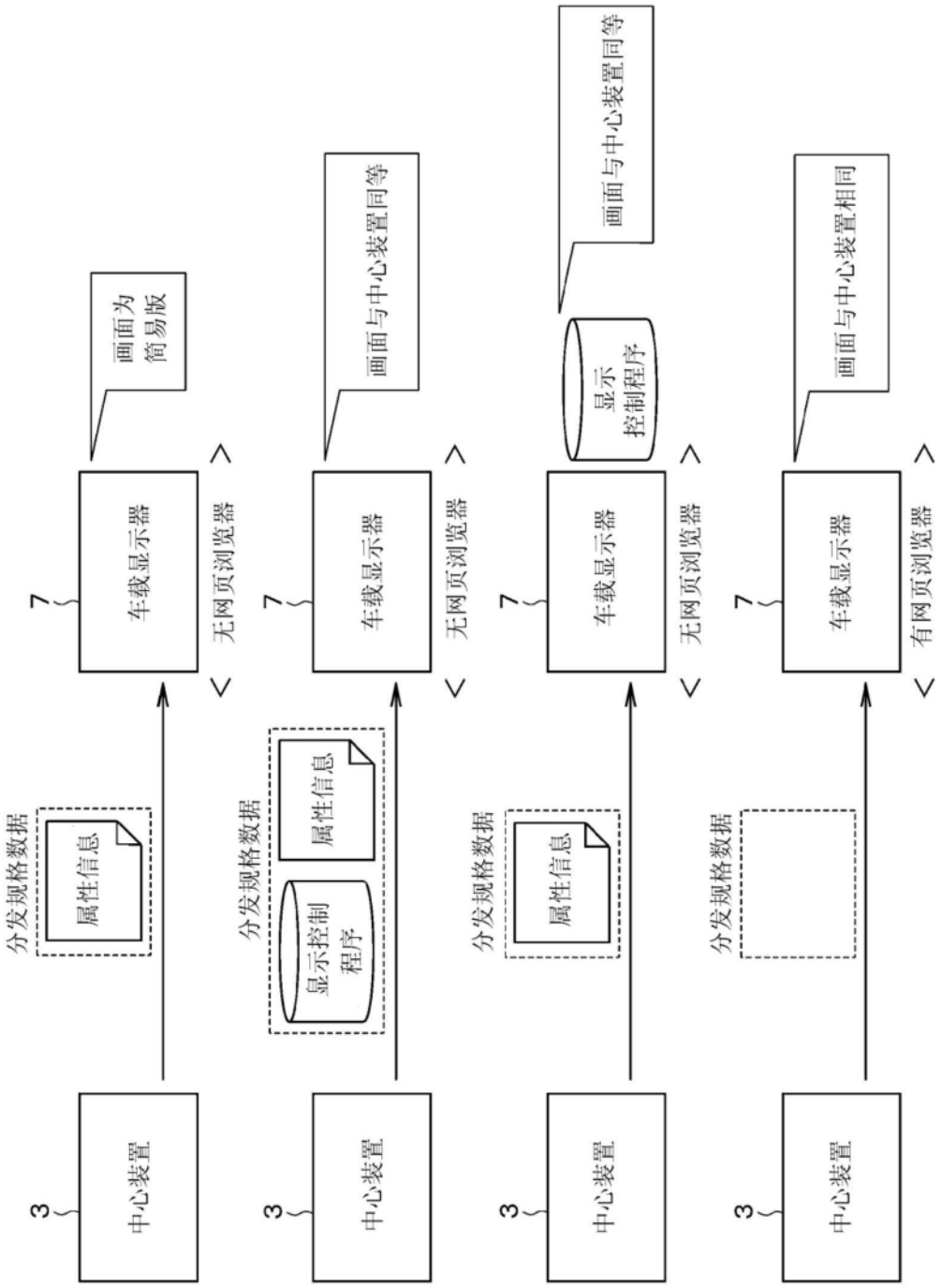

3
中心装置
分发规格数据
属性信息
7
车载显示器
画面为
简易版
无网页浏览器
3
中心装置
分发规格数据
显示控制
程序
属性信息
7
车载显示器
画面与中心装置同等
无网页浏览器
3
中心装置
分发规格数据
属性信息
7
车载显示器
显示
控制程序
画面与中心装置同等
无网页浏览器
3
中心装置
分发规格数据
7
车载显示器
画面与中心装置相同
有网页浏览器

图185

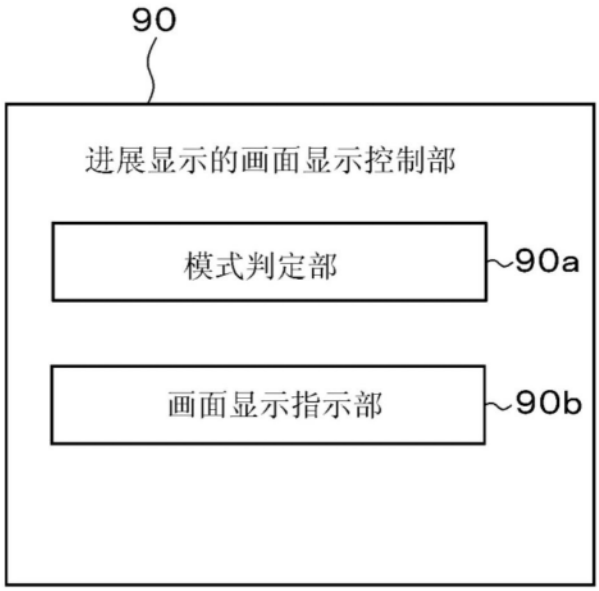


图186

改写规格数据

场景信息	召回标志
	经销商标志
	工厂标志
	功能更新通知标志
	强制执行标志
有效期限信息	
位置信息	

图187


菜单选择时
511
FOTA MENU
返回
软件更新
511a
更新结果确认
511b
软件版本一览
511c
更新历史
511d
用户信息登记（个人信息登记 / 初始化）
511e

图188

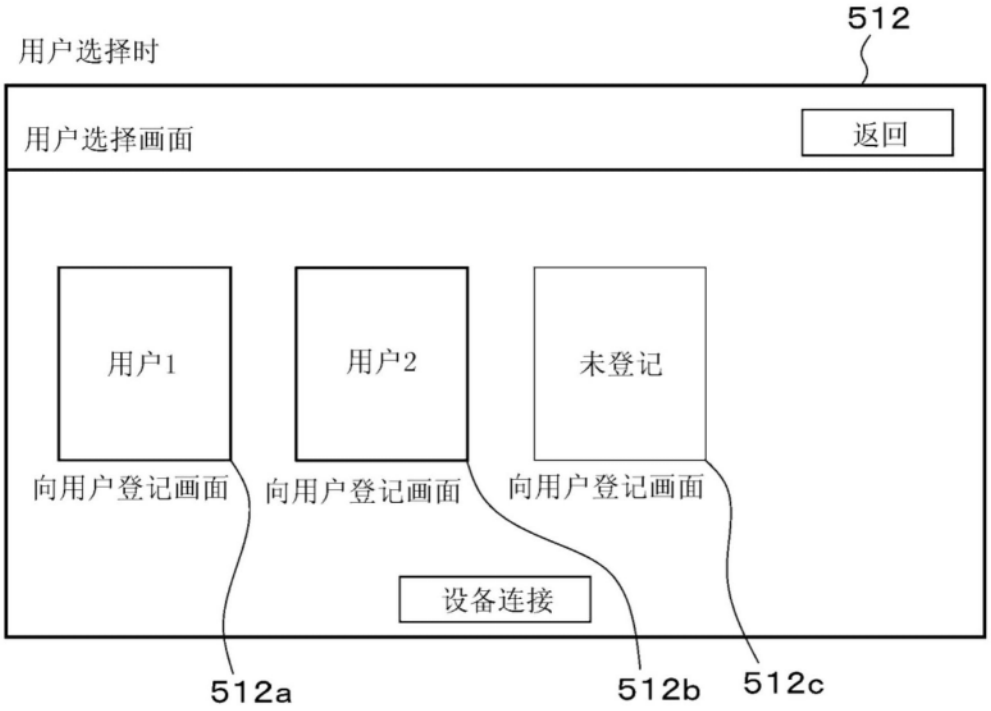

用户选择时
512
用户选择画面
返回
用户1
用户2
未登记
向用户登记画面
向用户登记画面
向用户登记画面
设备连接
512a
512b
512c

图189

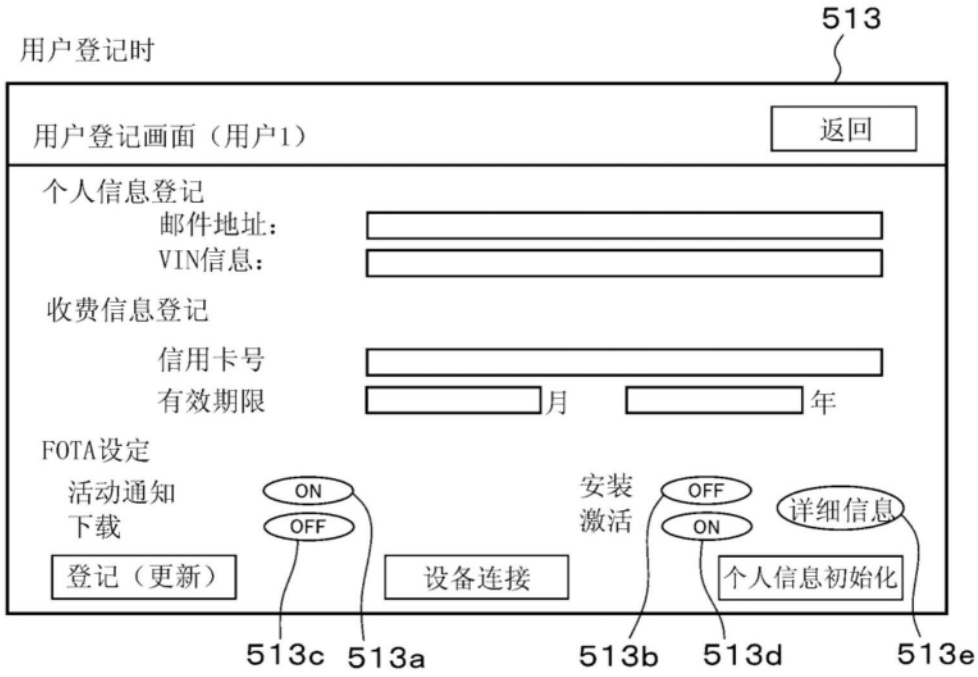

513
用户登记时
用户登记画面（用户1）
返回
个人信息登记
邮件地址：
VIN信息：
收费信息登记
信用卡号
有效期限
月
年
FOTA设定
活动通知
下载
ON
OFF
安装
激活
OFF
ON
详细信息
登记（更新）
设备连接
个人信息初始化
513c
513a
513b
513d
513e

图190

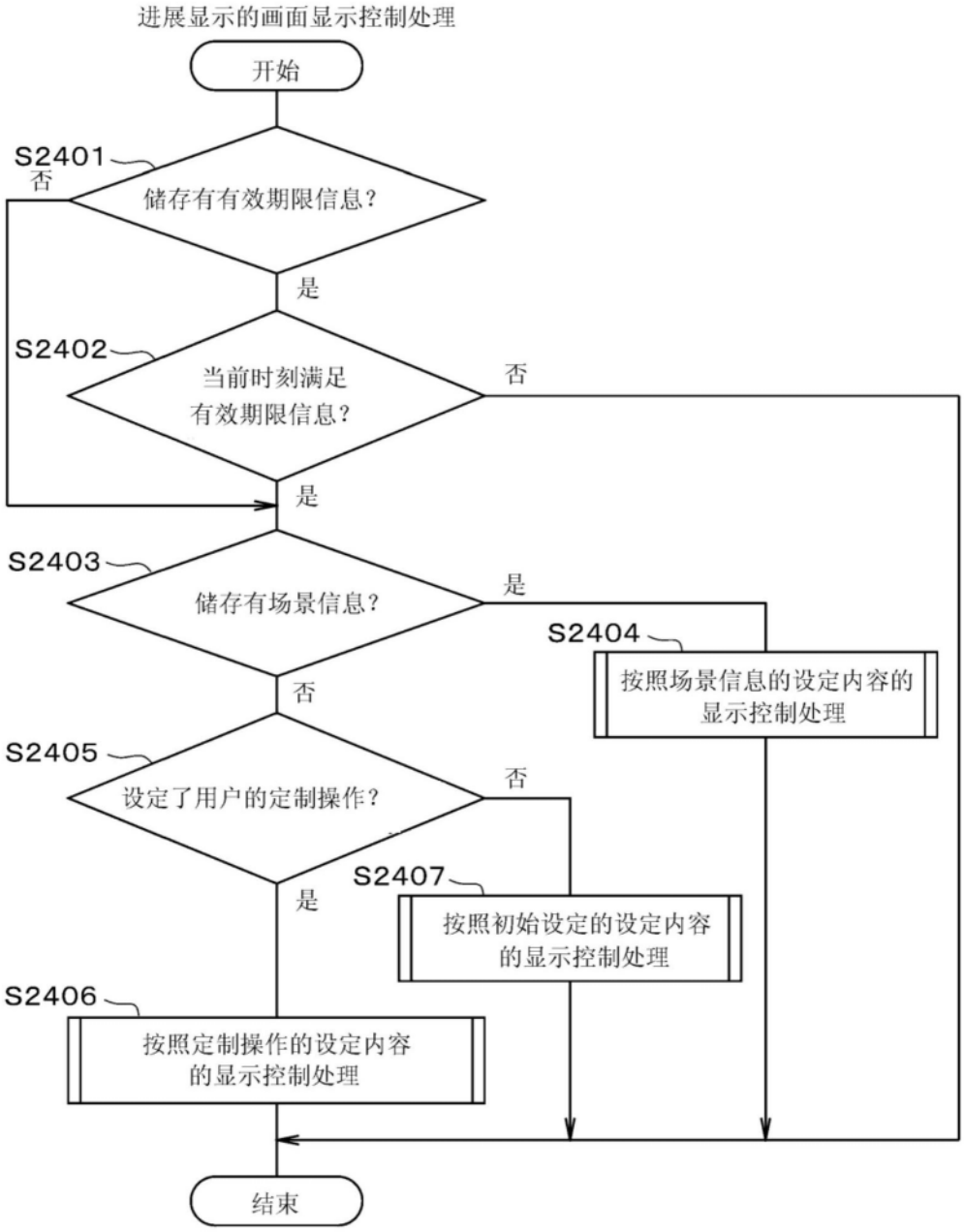

进展显示的画面显示控制处理
开始
S2401
储存有有效期限信息？
否
是
S2402
当前时刻满足
有效期限信息？
否
是
S2403
储存有场景信息？
是
S2404
按照场景信息的设定内容的
显示控制处理
否
S2405
设定了用户的定制操作？
否
是
S2407
按照初始设定的设定内容
的显示控制处理
S2406
按照定制操作的设定内容
的显示控制处理
结束

图191

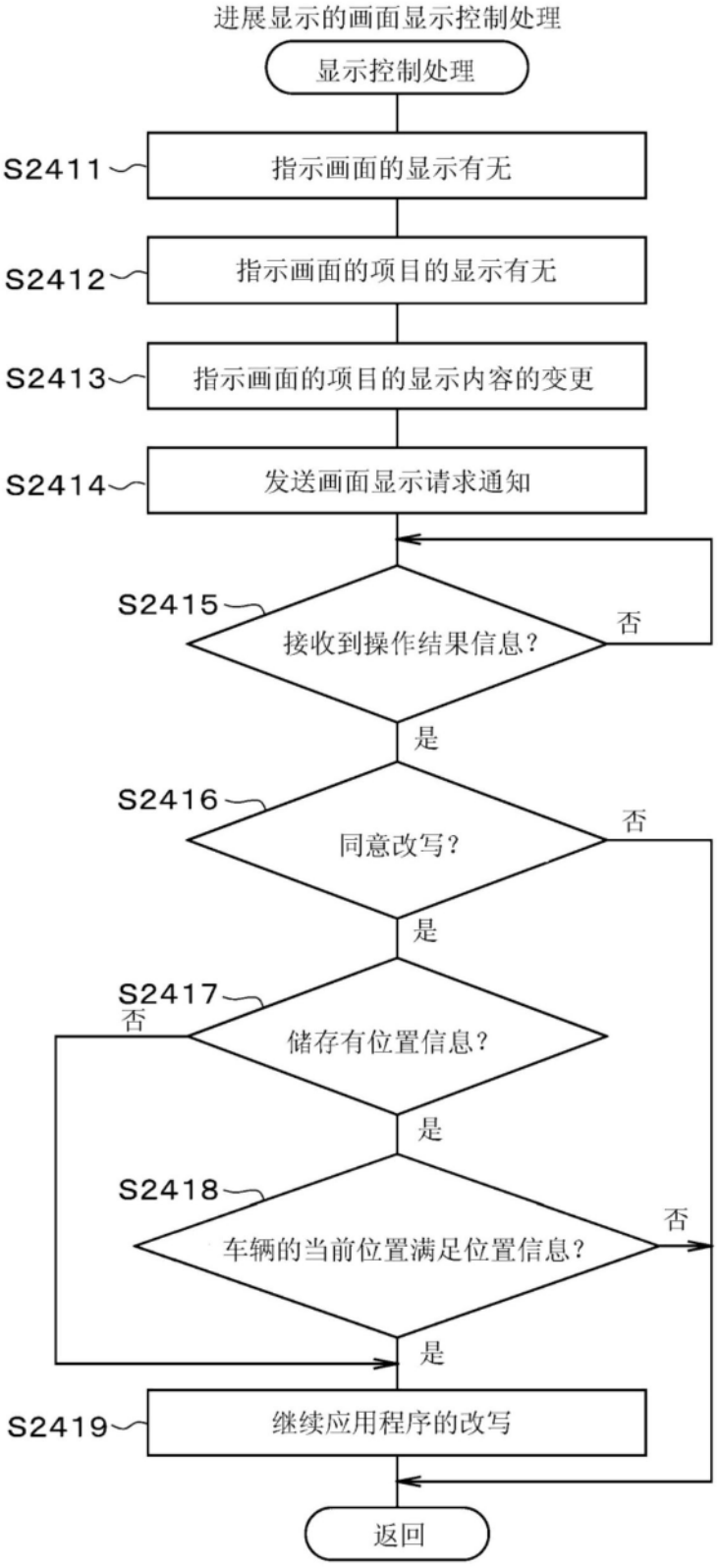

进展显示的画面显示控制处理
显示控制处理
S2411
指示画面的显示有无
S2412
指示画面的项目的显示有无
S2413
指示画面的项目的显示内容的变更
S2414
发送画面显示请求通知
S2415
接收到操作结果信息？
否
是
S2416
同意改写？
否
是
S2417
否
储存有位置信息？
是
S2418
车辆的当前位置满足位置信息？
否
是
S2419
继续应用程序的改写
返回

图192

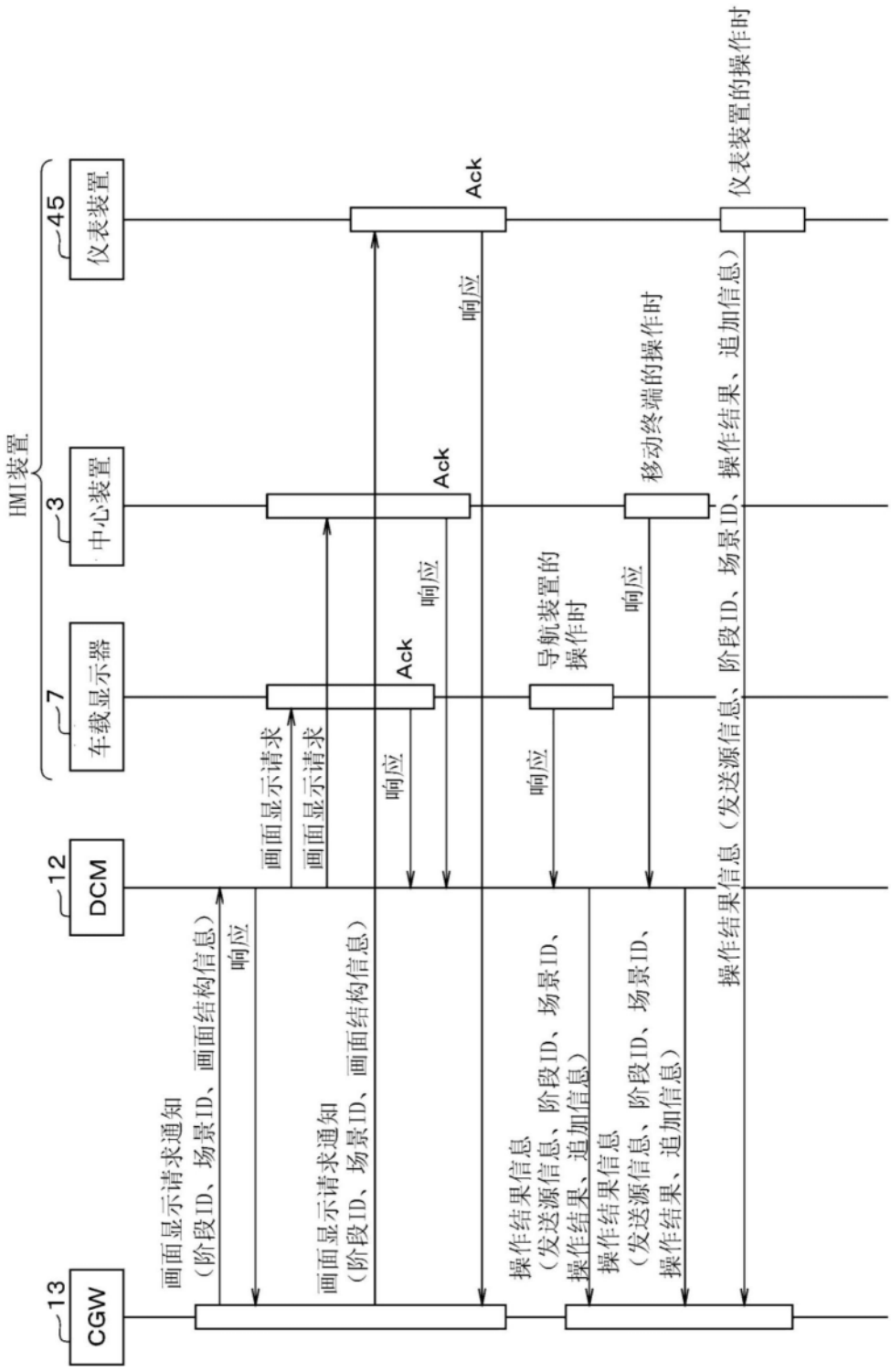

HMI装置
13 CGW
12 DCM
7 车载显示器
3 中心装置
45 仪表装置
画面显示请求通知
（阶段ID、场景ID、画面结构信息）
响应
画面显示请求
画面显示请求通知
（阶段ID、场景ID、画面结构信息）
响应
Ack
响应
Ack
操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
响应
导航装置的
操作时
操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
响应
移动终端的操作时
操作结果信息（发送源信息、阶段ID、场景ID、操作结果、追加信息）
Ack
仪表装置的操作时

图193



图194

项目	显示 / 非显示
活动 …	显示
更新名称A…	显示
更新名称B …	显示
详细确认	显示
返回	显示
OK	显示

图195

项目	显示 / 非显示
活动 …	显示
更新名称A…	显示
更新名称B…	显示
详细确认	显示
返回	非显示
OK	显示

图196

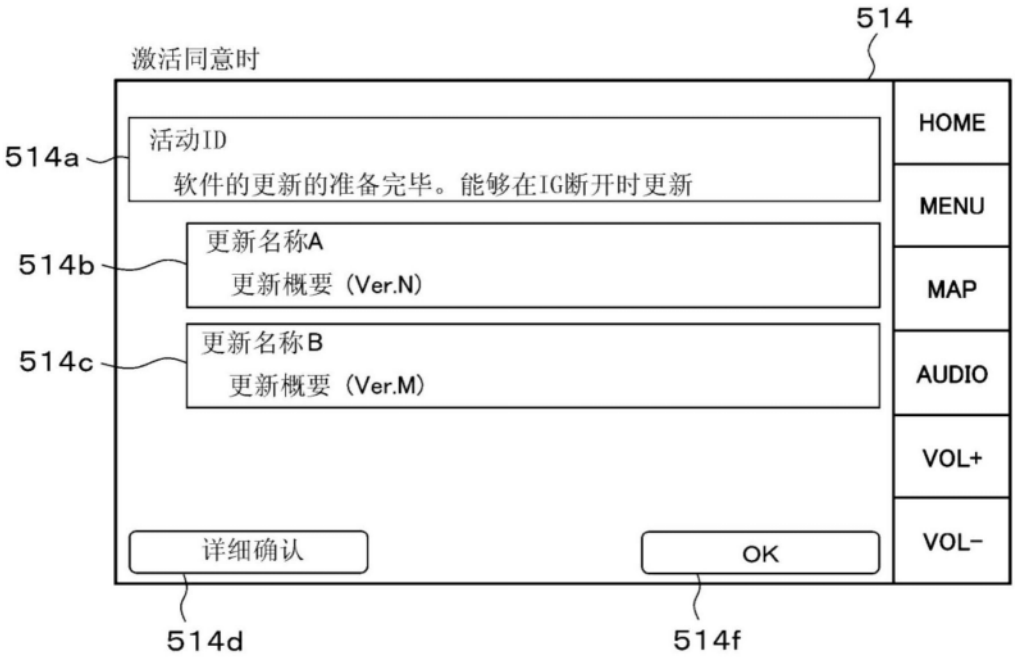


图197

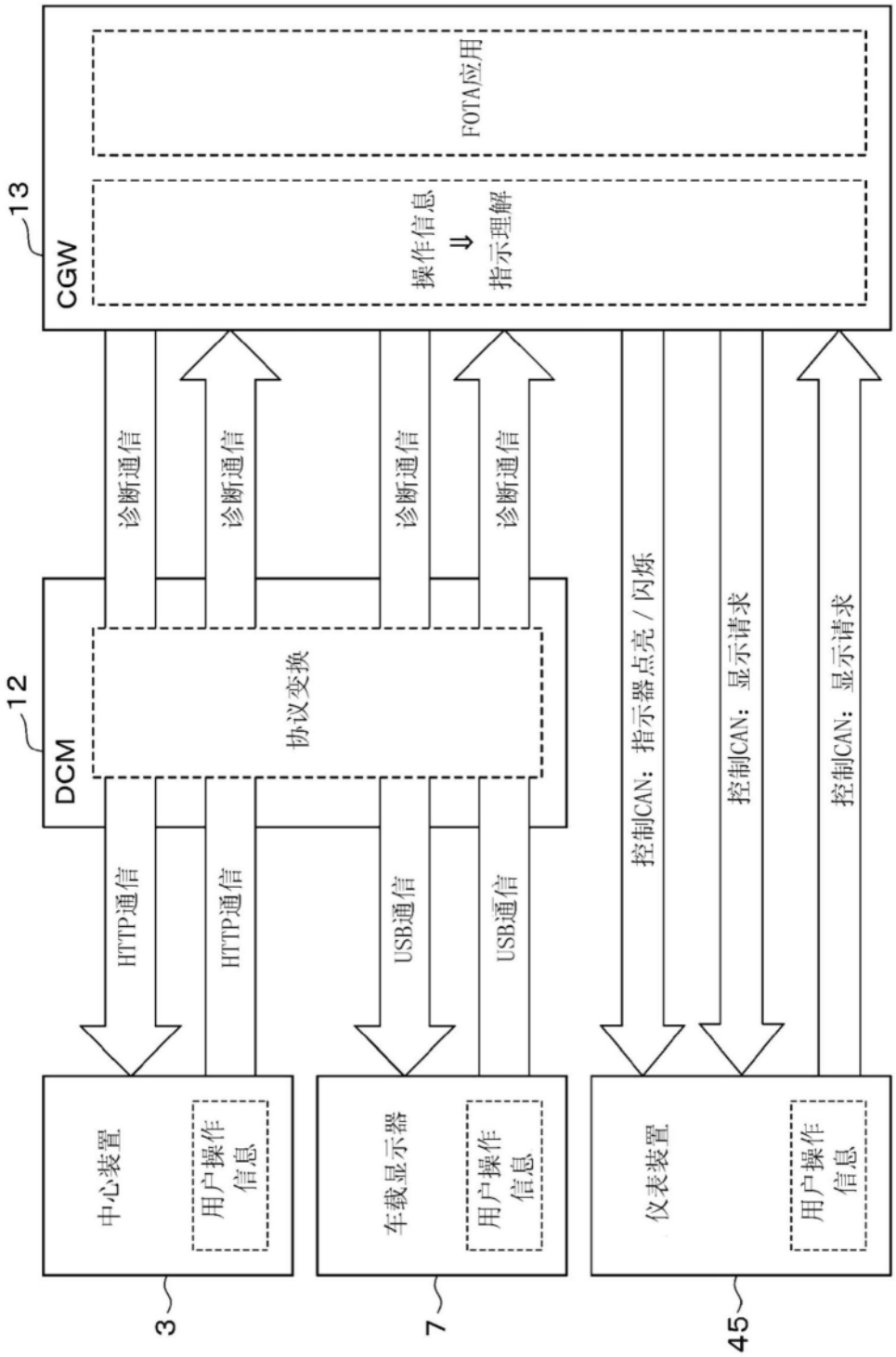

13
CGW
FOTA应用
操作信息
⇓
指示理解
诊断通信
诊断通信
诊断通信
诊断通信
12
DCM
协议变换
HTTP通信
HTTP通信
USB通信
USB通信
控制CAN：指示器点亮 / 闪烁
控制CAN：显示请求
控制CAN：显示请求
中心装置
用户操作信息
车载显示器
用户操作信息
仪表装置
用户操作信息
3
7
45

图198

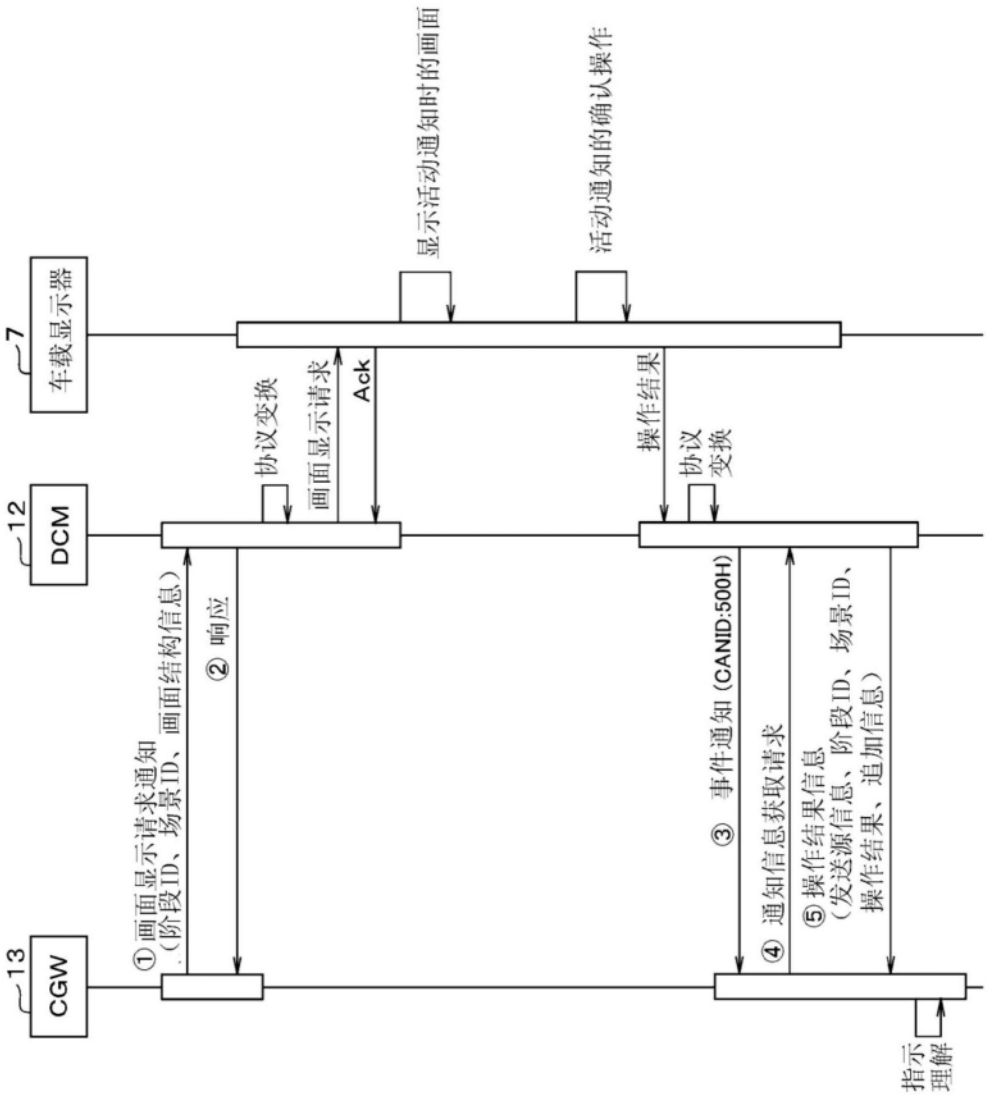

显示活动通知时的画面
活动通知的确认操作
7
车载显示器
协议变换
画面显示请求
Ack
操作结果
协议
变换
12
DCM
① 画面显示请求通知
（阶段ID、场景ID、画面结构信息）
② 响应
③ 事件通知（CANID:500H）
④ 通知信息获取请求
⑤操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
13
CGW
指示
理解

图199

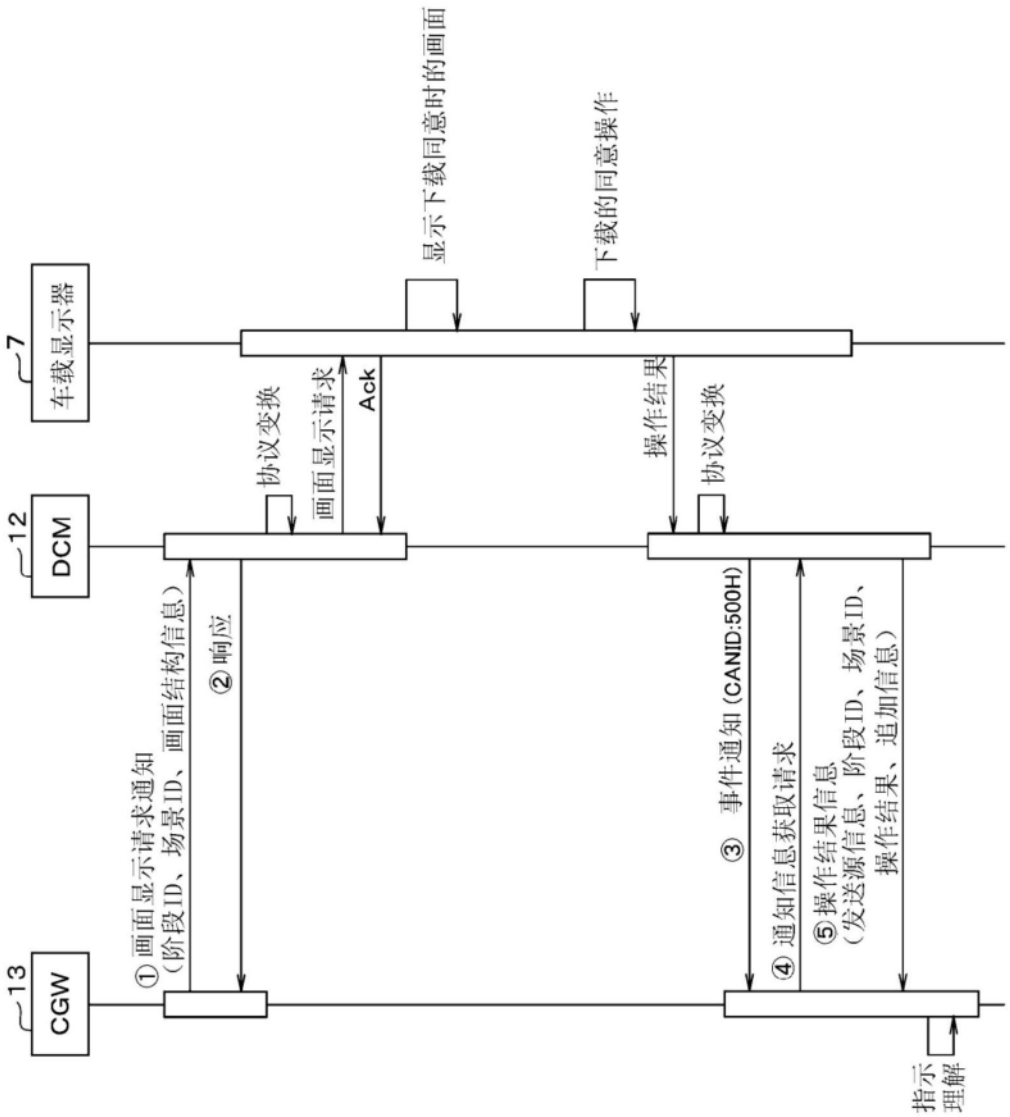

7
车载显示器
12
DCM
13
CGW
显示下载同意时的画面
下载的同意操作
协议变换
画面显示请求
Ack
操作结果
协议变换
① 画面显示请求通知
（阶段ID、场景ID、画面结构信息）
② 响应
③ 事件通知（CANID:500H）
④ 通知信息获取请求
⑤操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
指示
理解

图200

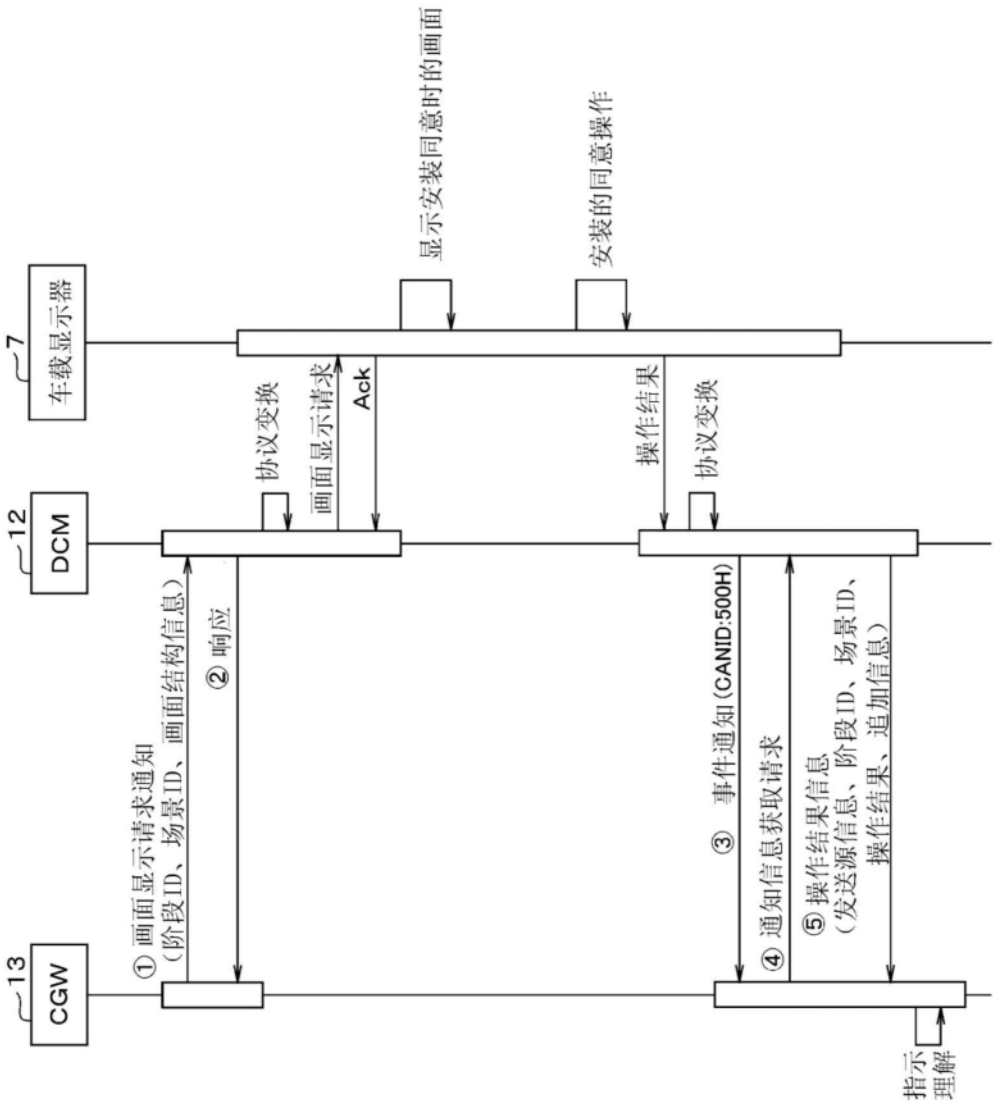

显示安装同意时的画面
安装的同意操作
7
车载显示器
协议变换
画面显示请求
Ack
操作结果
协议变换
12
DCM
① 画面显示请求通知
（阶段ID、场景ID、画面结构信息）
② 响应
③ 事件通知(CANID:500H)
④ 通知信息获取请求
⑤ 操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
13
CGW
指示
理解

图201

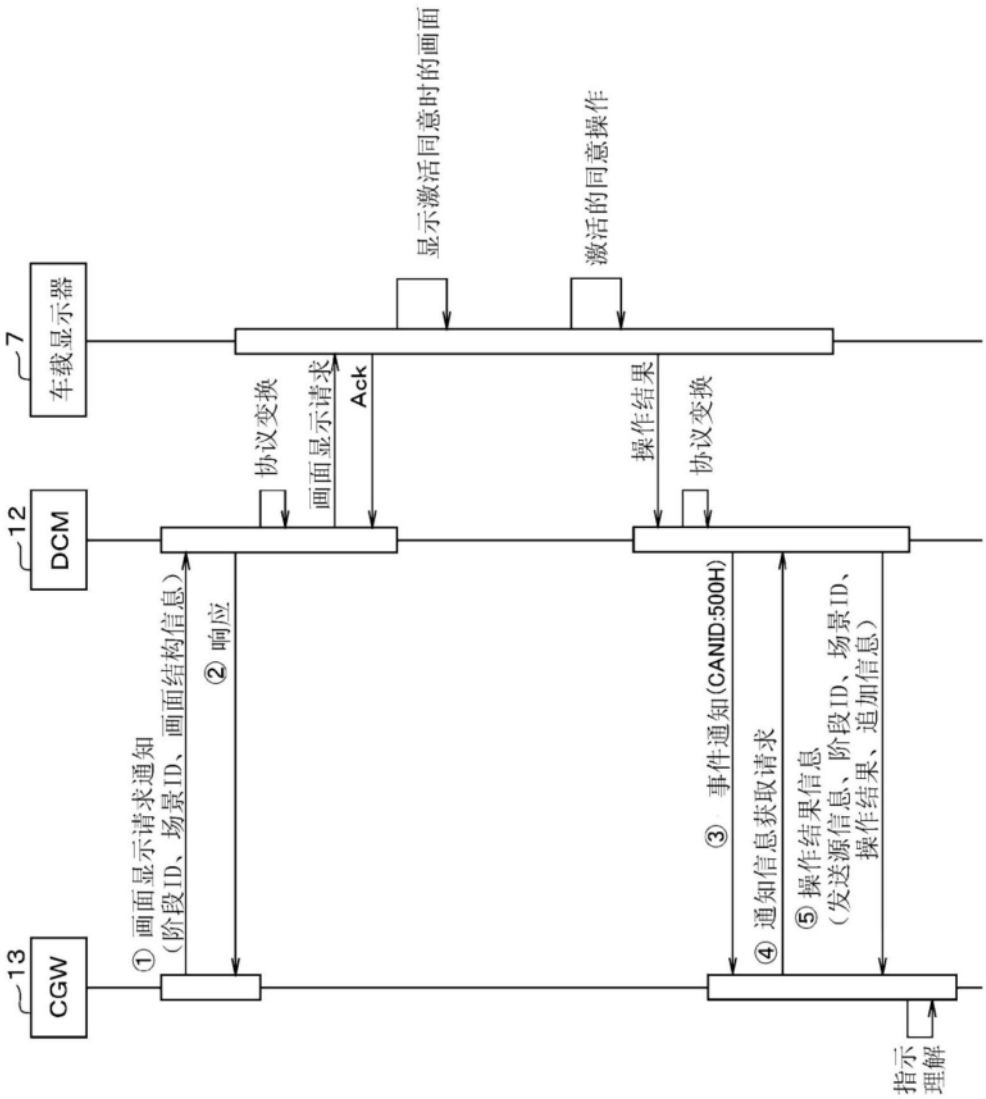

显示激活同意时的画面
激活的同意操作
7
车载显示器
协议变换
画面显示请求
Ack
操作结果
协议变换
12
DCM
① 画面显示请求通知
（阶段ID、场景ID、画面结构信息）
② 响应
③ 事作通知(CANID:500H)
④ 通知信息获取请求
⑤ 操作结果信息
（发送源信息、阶段ID、场景ID、
操作结果、追加信息）
13
CGW
指示
理解

图202

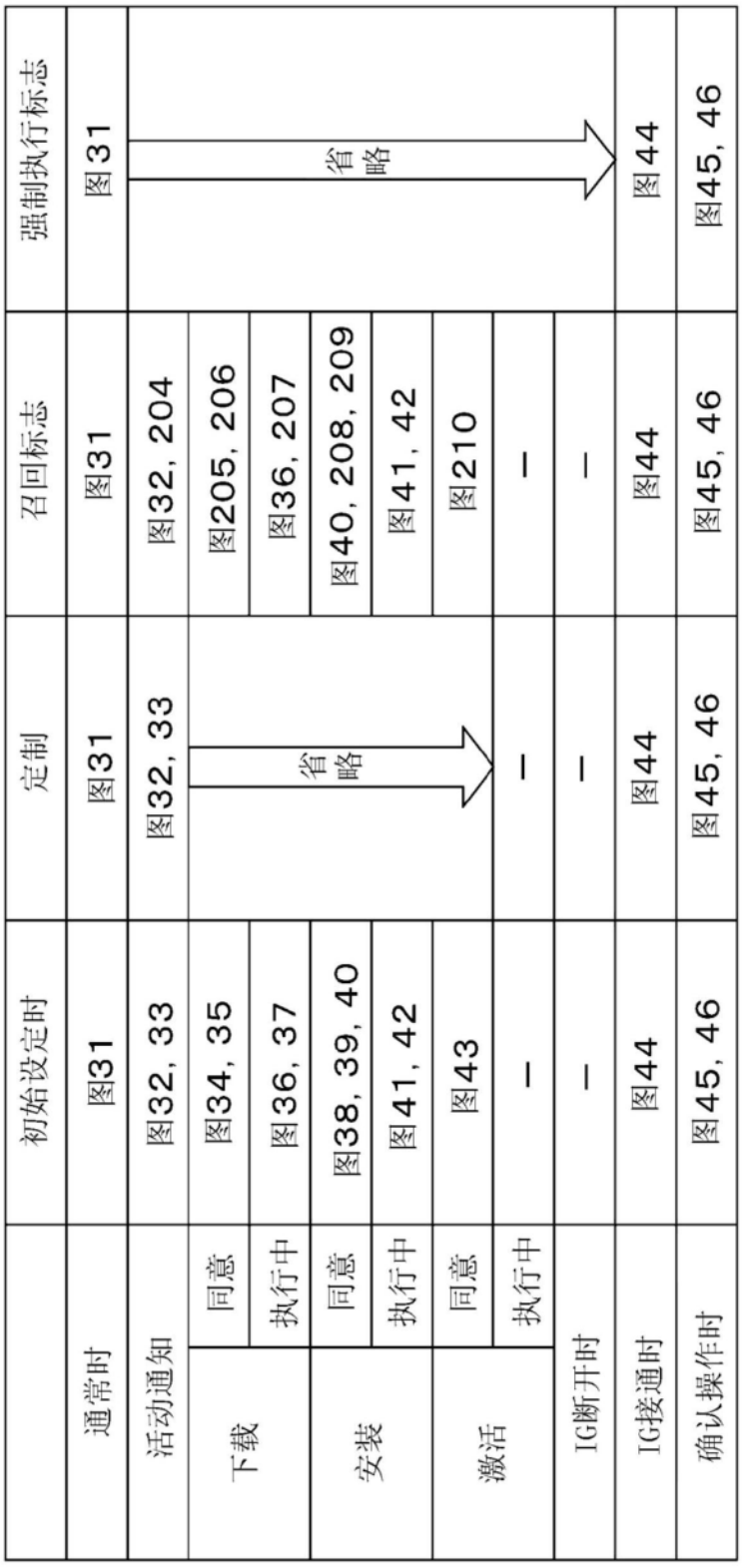

初始设定时
定制
召回标志
强制执行标志
通常时
图31
图31
图31
图31
活动通知
图32, 33
图32, 33
图32, 204
省略
下载
同意
图34, 35
图205, 206
执行中
图36, 37
图36, 207
安装
同意
图38, 39, 40
图40, 208, 209
执行中
图41, 42
图41, 42
激活
同意
图43
图210
执行中
—
—
IG断开时
—
—
—
—
IG接通时
图44
图44
图44
图44
确认操作时
图45, 46
图45, 46
图45, 46
图45, 46

图203

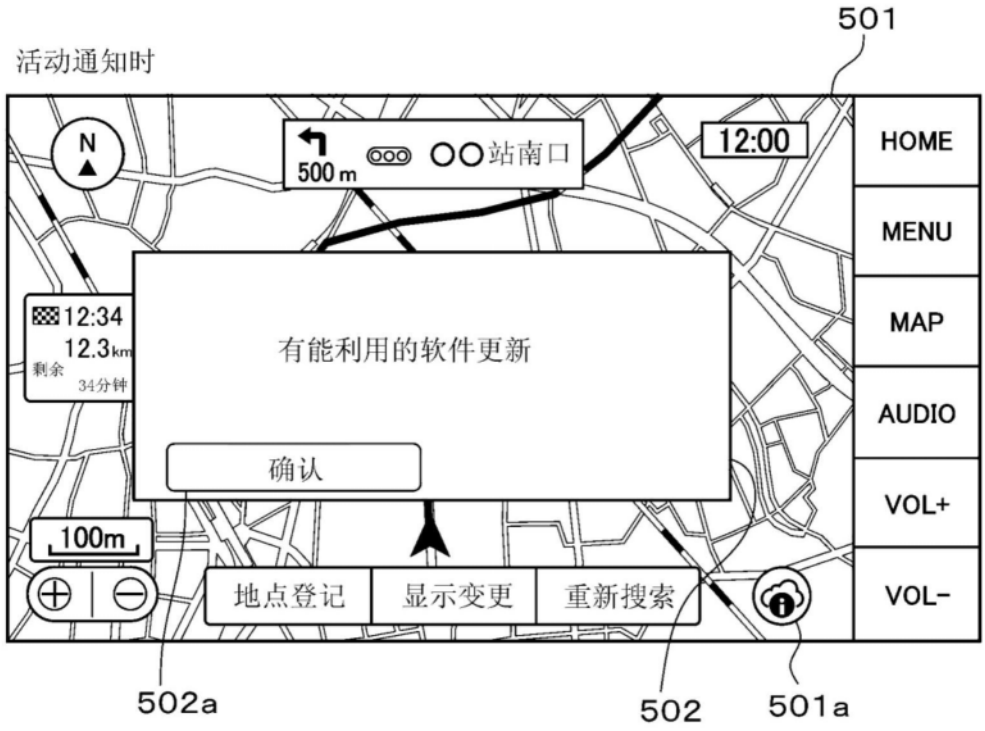

活动通知时
501
N
500 m
〇〇站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34
12.3km
剩余
34分钟
有能利用的软件更新
确认
100m
地点登记
显示变更
重新搜索
502a
502
501a

图204

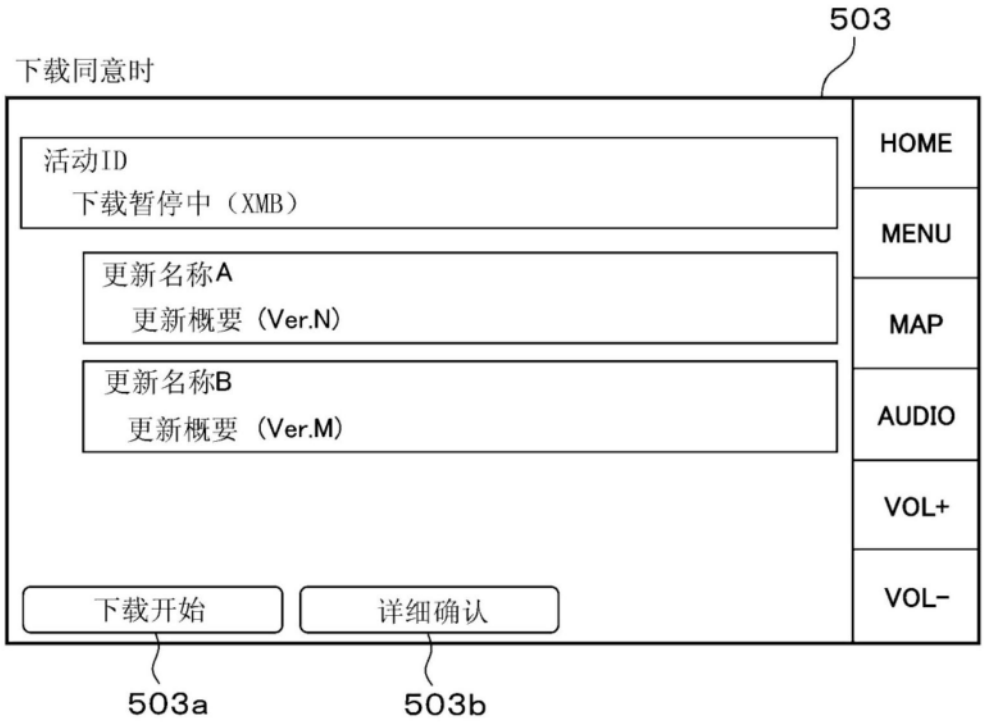

下载同意时
503
活动ID
下载暂停中（XMB）
更新名称A
更新概要（Ver.N）
更新名称B
更新概要（Ver.M）
HOME
MENU
MAP
AUDIO
VOL+
VOL-
下载开始
详细确认
503a
503b

图205

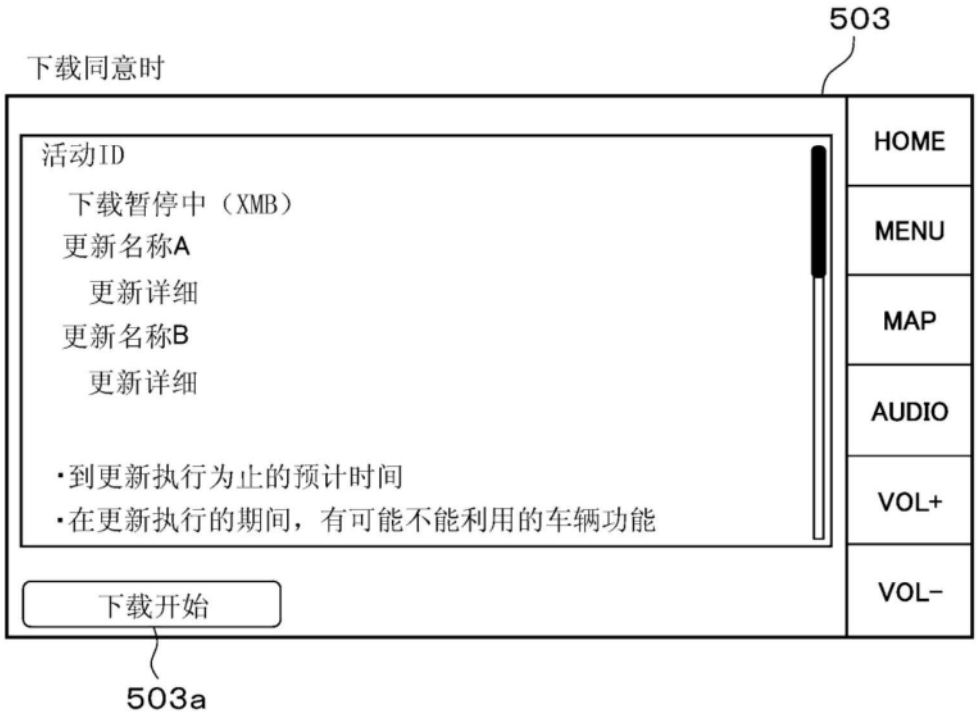

503
下载同意时
活动ID
下载暂停中（XMB）
更新名称A
更新详细
更新名称B
更新详细
·到更新执行为止的预计时间
·在更新执行的期间，有可能不能利用的车辆功能
下载开始
503a
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图206

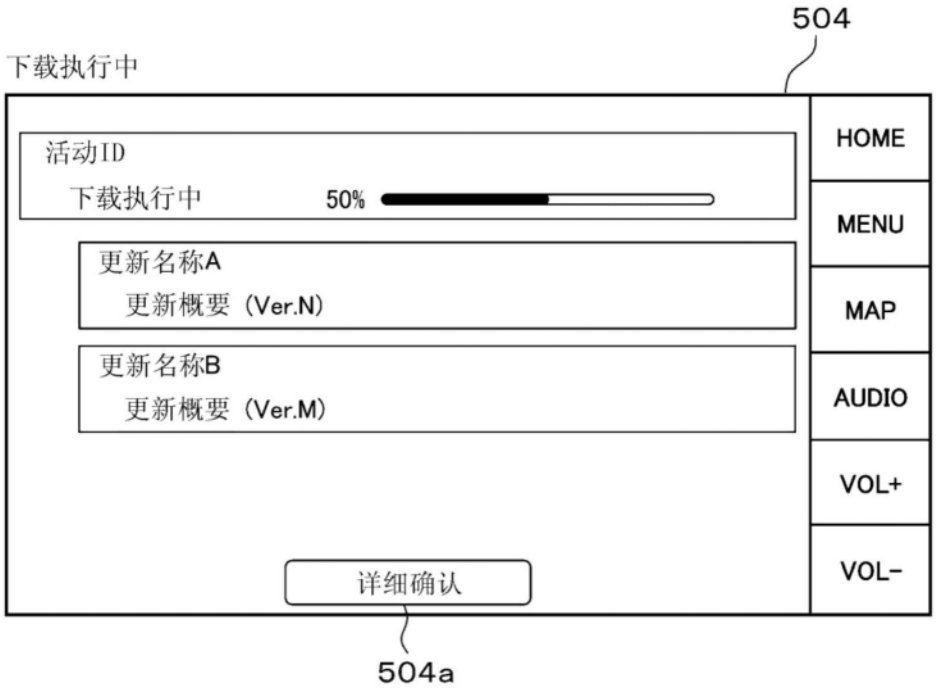

504
下载执行中
活动ID
下载执行中
50%
更新名称A
更新概要（Ver.N）
更新名称B
更新概要（Ver.M）
详细确认
504a
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图207

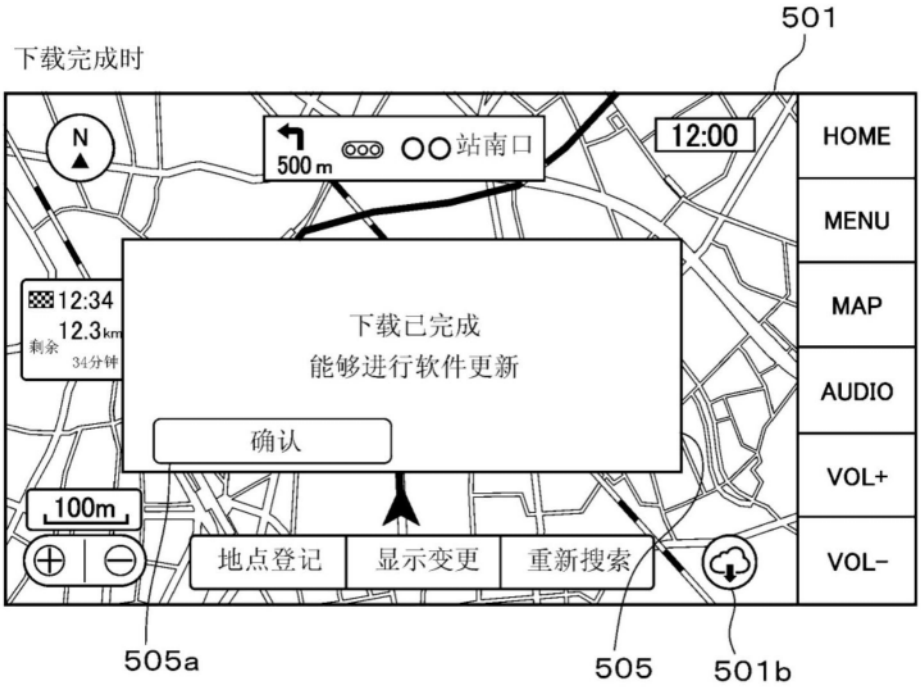

501
下载完成时
N
500 m
站南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL-
12:34
12.3km
剩余
34分钟
下载已完成
能够进行软件更新
确认
100m
地点登记
显示变更
重新搜索
505a
505
501b

图208

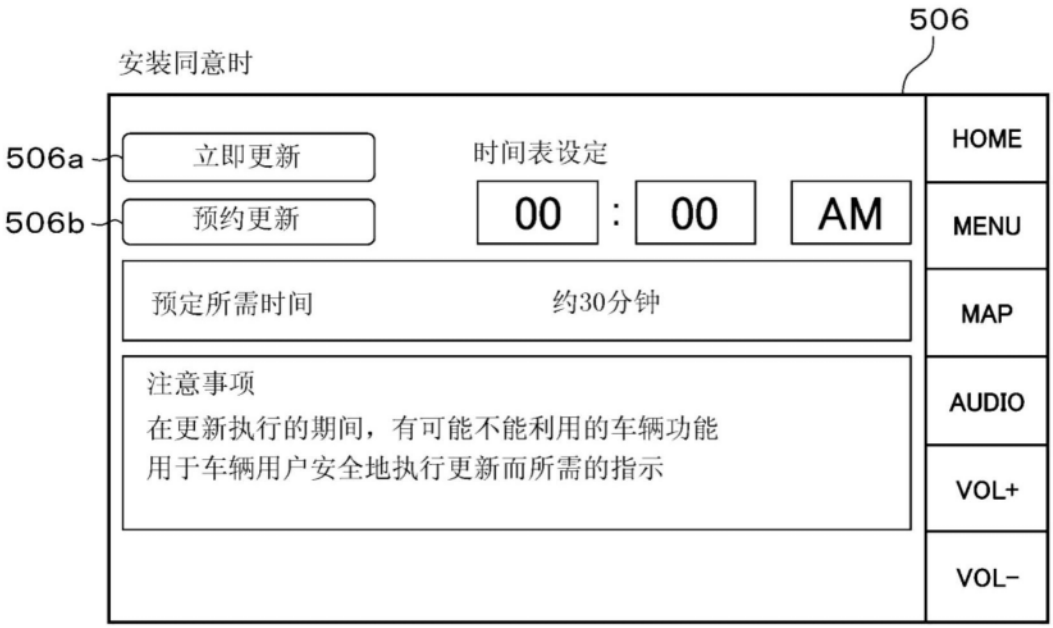

506
安装同意时
506a
立即更新
506b
预约更新
时间表设定
00
:
00
AM
预定所需时间
约30分钟
注意事项
在更新执行的期间，有可能不能利用的车辆功能
用于车辆用户安全地执行更新而所需的指示
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图209

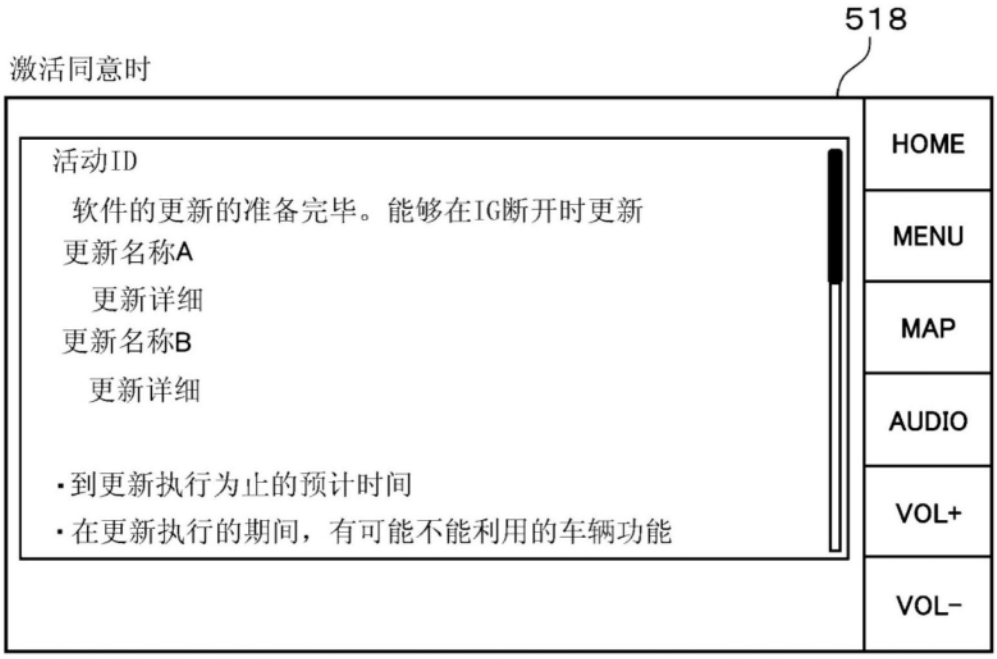

518
激活同意时
活动ID
软件的更新的准备完毕。能够在IG断开时更新
更新名称A
更新详细
更新名称B
更新详细
·到更新执行为止的预计时间
·在更新执行的期间，有可能不能利用的车辆功能
HOME
MENU
MAP
AUDIO
VOL+
VOL-

图210

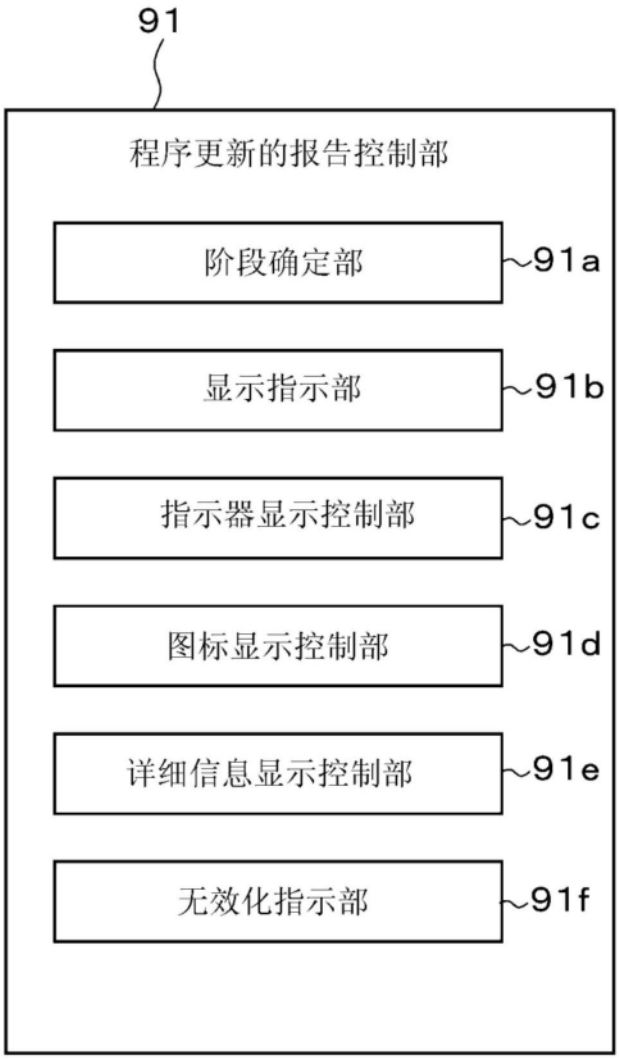

91
程序更新的报告控制部
阶段确定部
91a
显示指示部
91b
指示器显示控制部
91c
图标显示控制部
91d
详细信息显示控制部
91e
无效化指示部
91f

图211

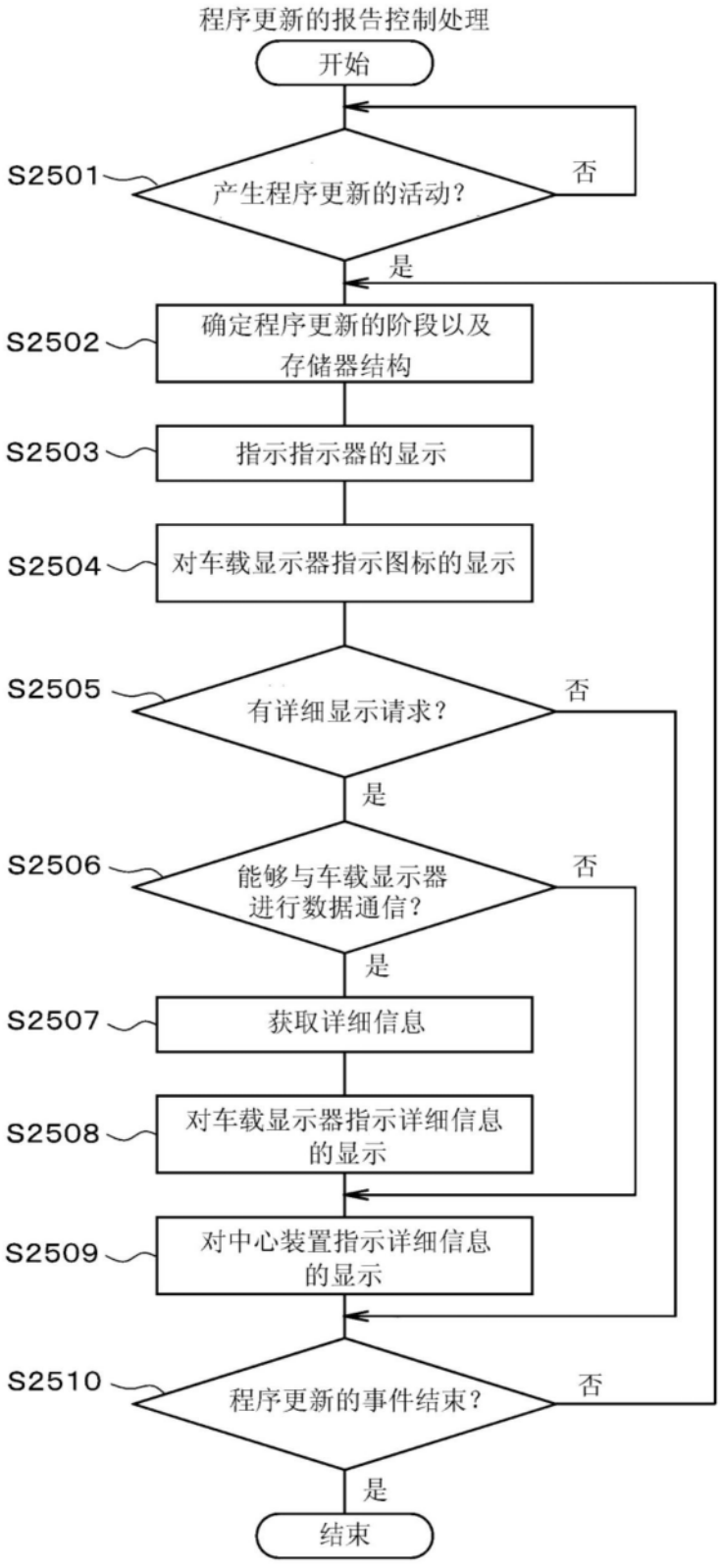

程序更新的报告控制处理
开始
S2501
产生程序更新的活动?
否
是
S2502
确定程序更新的阶段以及
存储器结构
S2503
指示指示器的显示
S2504
对车载显示器指示图标的显示
S2505
有详细显示请求?
否
是
S2506
能够与车载显示器
进行数据通信?
否
是
S2507
获取详细信息
S2508
对车载显示器指示详细信息
的显示
S2509
对中心装置指示详细信息
的显示
S2510
程序更新的事件结束?
否
是
结束

图212

		仪表装置		车载显示器
		双面存储器	单面挂起存储器	单面单独存储器	
通常时		熄灭	熄灭	熄灭	图31
活动通知		点亮	点亮	点亮	图32, 33
下载	同意	点亮	点亮	点亮	图34, 35
	执行中	点亮	点亮	点亮	图36, 37
安装	同意	点亮	点亮	点亮	图38, 39, 40
	执行中	点亮	点亮（IG接通）・闪烁（IG断开）	闪烁	图41, 42
激活	同意	点亮	闪烁	闪烁	图43
	执行中	闪烁	闪烁	闪烁	
IG断开时		熄灭	熄灭	熄灭	
IG接通时		点亮	点亮	点亮	图44
确认操作时		熄灭	熄灭	熄灭	图45, 46

图213

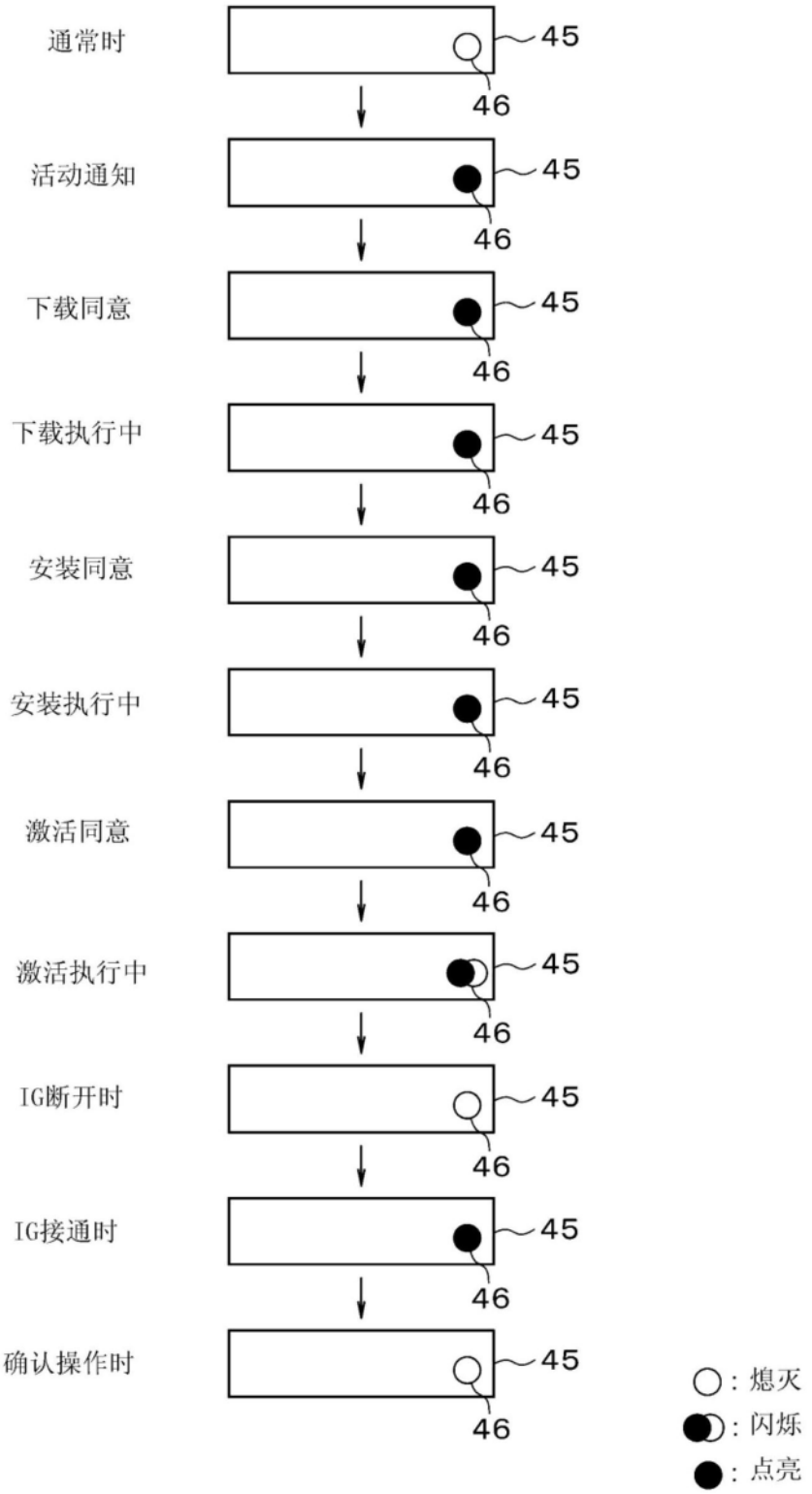

通常时
活动通知
下载同意
下载执行中
安装同意
安装执行中
激活同意
激活执行中
IG断开时
IG接通时
确认操作时
45
46
○：熄灭
◐：闪烁
●：点亮

图214

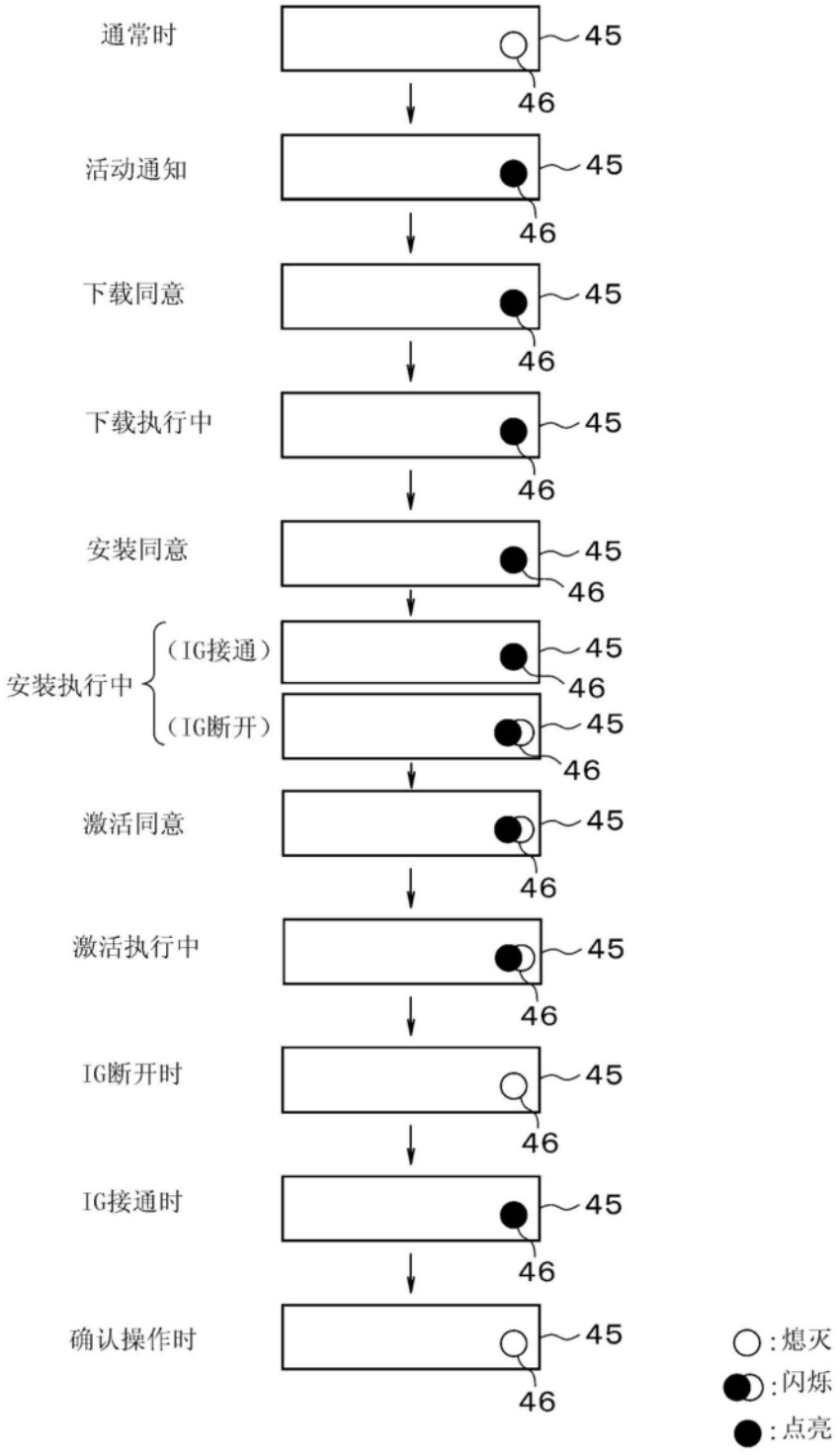

通常时
活动通知
下载同意
下载执行中
安装同意
安装执行中
（IG接通）
（IG断开）
激活同意
激活执行中
IG断开时
IG接通时
确认操作时
45
46
：熄灭
：闪烁
：点亮

图215

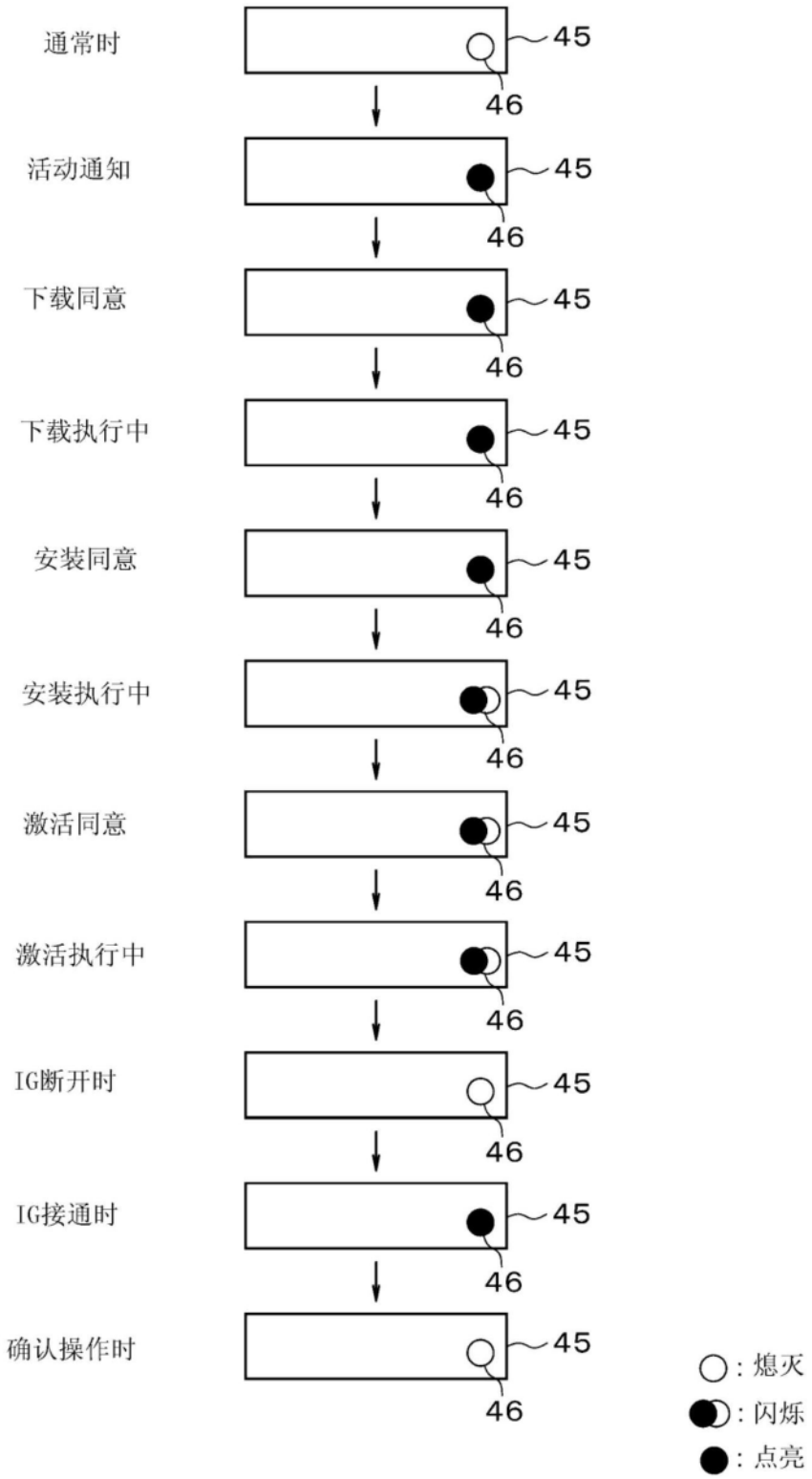

通常时
活动通知
下载同意
下载执行中
安装同意
安装执行中
激活同意
激活执行中
IG断开时
IG接通时
确认操作时
45
46
○：熄灭
：闪烁
●：点亮

图216

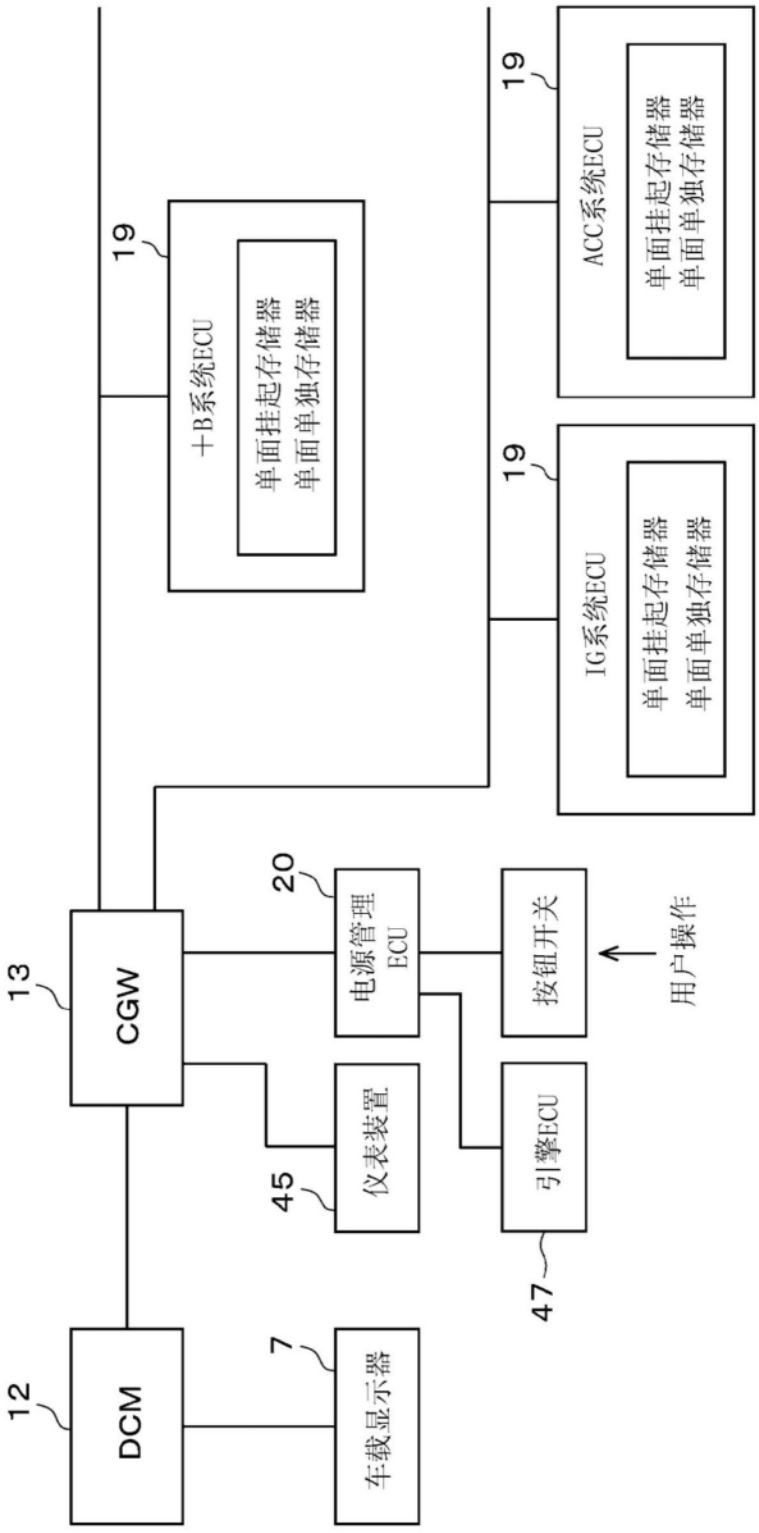

19
+B系统ECU
单面挂起存储器
单面单独存储器
19
ACC系统ECU
单面挂起存储器
单面单独存储器
19
IG系统ECU
单面挂起存储器
单面单独存储器
13
CGW
20
电源管理ECU
按钮开关
用户操作
45
仪表装置
引擎ECU
47
12
DCM
7
车载显示器

图217

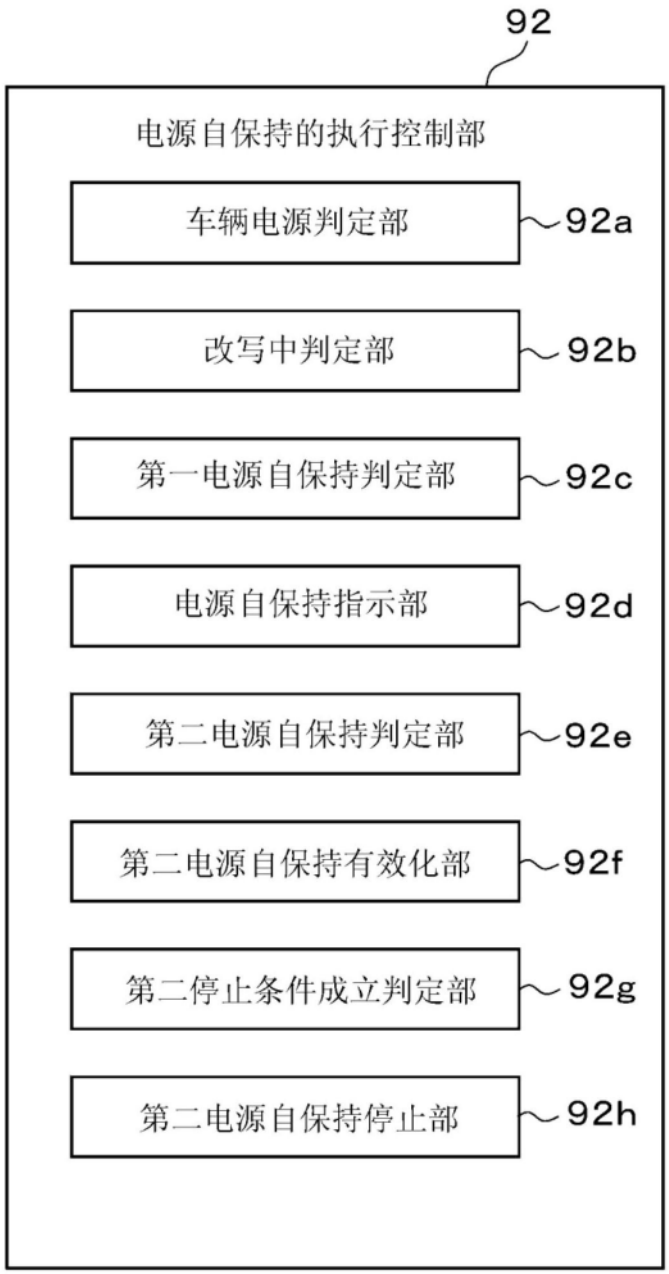

92
电源自保持的执行控制部
车辆电源判定部
92a
改写中判定部
92b
第一电源自保持判定部
92c
电源自保持指示部
92d
第二电源自保持判定部
92e
第二电源自保持有效化部
92f
第二停止条件成立判定部
92g
第二电源自保持停止部
92h

图218

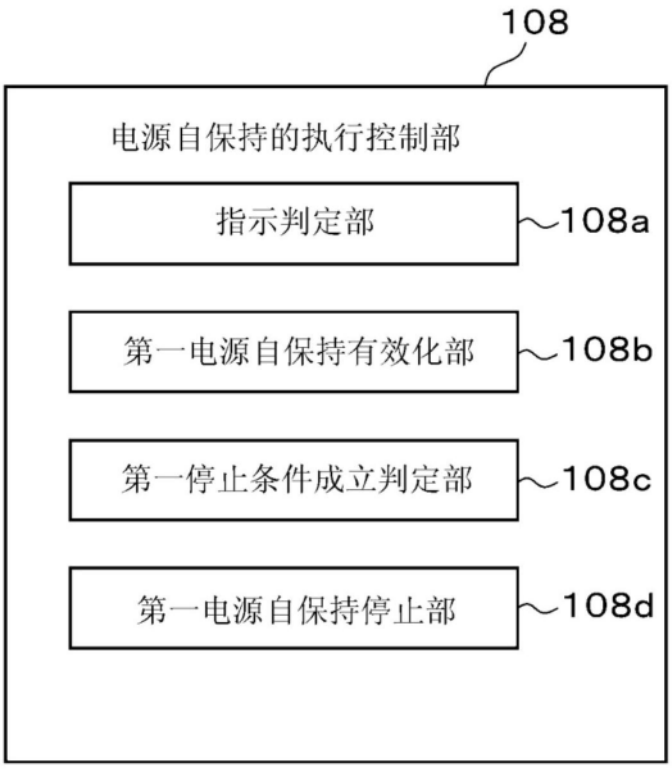

108
电源自保持的执行控制部
指示判定部
108a
第一电源自保持有效化部
108b
第一停止条件成立判定部
108c
第一电源自保持停止部
108d

图219

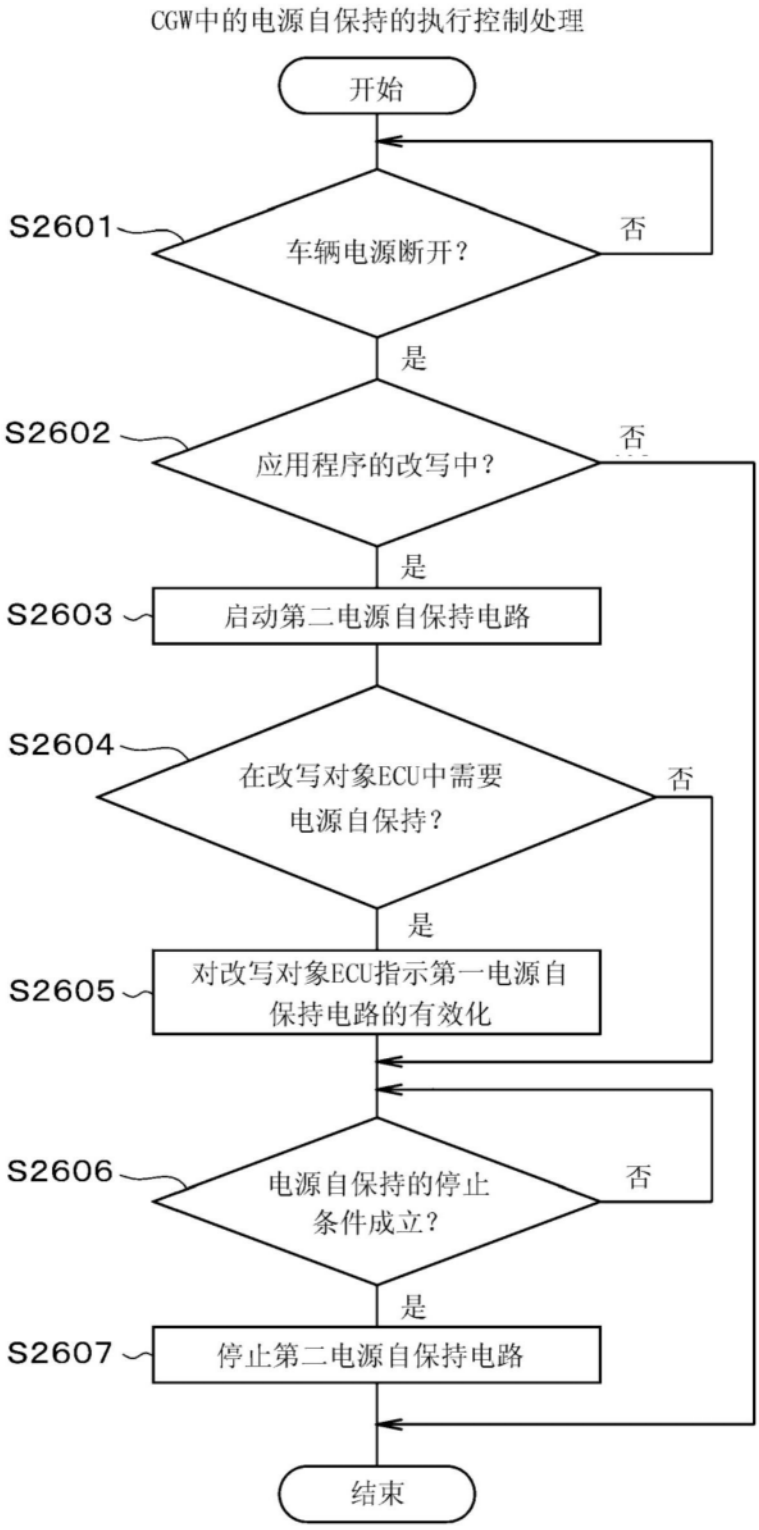

CGW中的电源自保持的执行控制处理
开始
S2601
车辆电源断开？
否
是
S2602
应用程序的改写中？
否
是
S2603
启动第二电源自保持电路
S2604
在改写对象ECU中需要电源自保持？
否
是
S2605
对改写对象ECU指示第一电源自保持电路的有效化
S2606
电源自保持的停止条件成立？
否
是
S2607
停止第二电源自保持电路
结束

图220

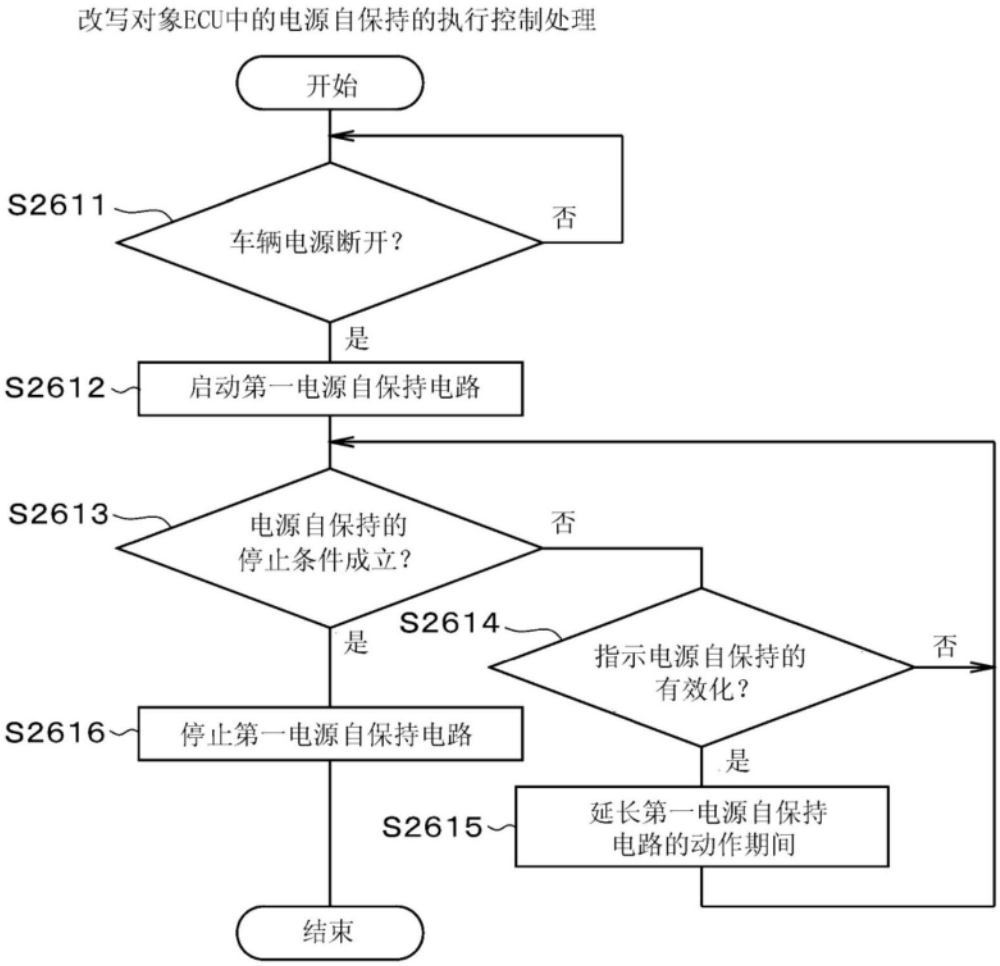

改写对象ECU中的电源自保持的执行控制处理
开始
S2611
车辆电源断开？
否
是
S2612
启动第一电源自保持电路
S2613
电源自保持的
停止条件成立？
否
是
S2614
指示电源自保持的
有效化？
否
是
S2615
延长第一电源自保持
电路的动作期间
S2616
停止第一电源自保持电路
结束

图221

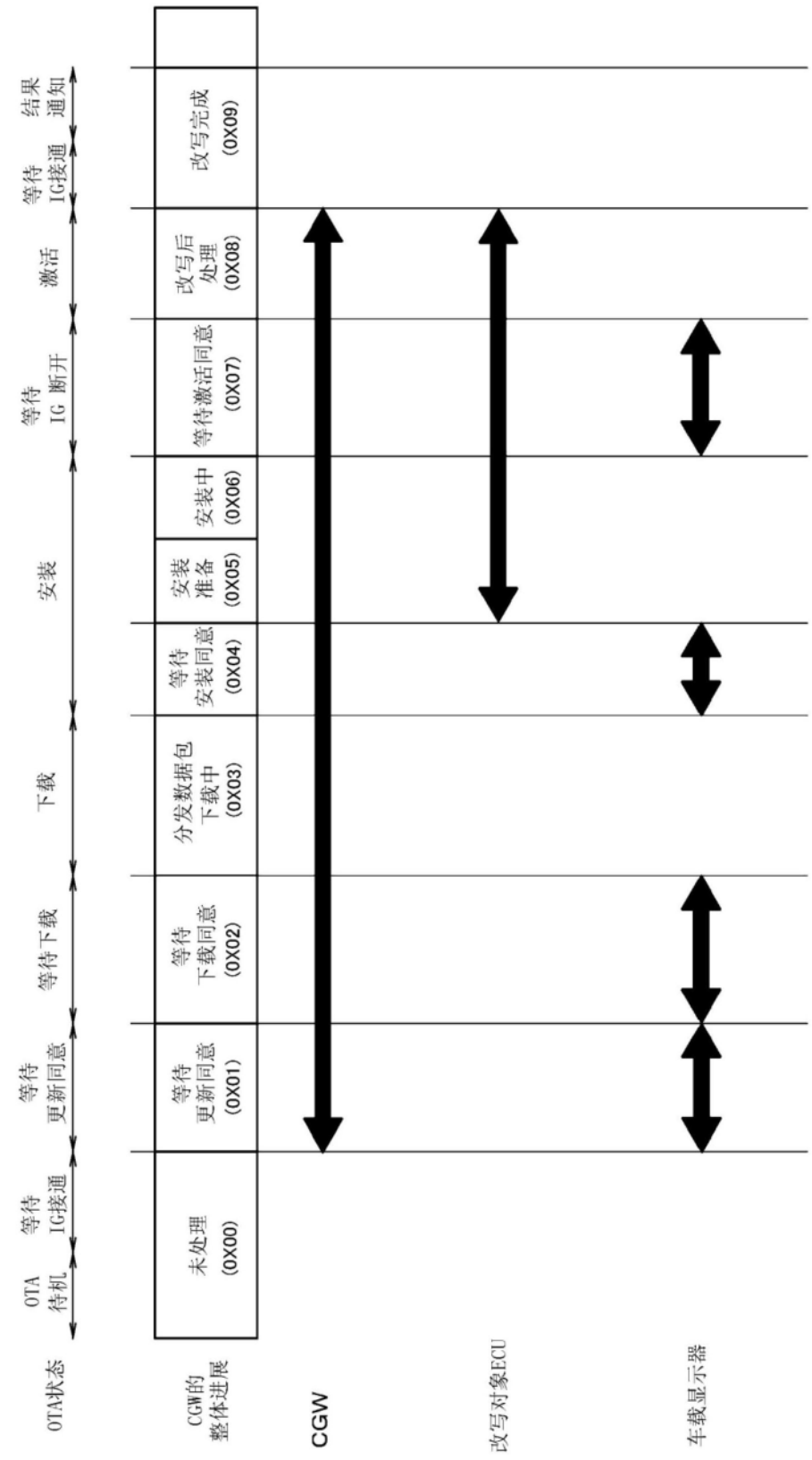

OTA状态
CGW的整体进展
CGW
改写对象ECU
车载显示器
OTA待机
等待IG接通
等待更新同意
等待下载
下载
等待安装同意
安装
等待IG 断开
激活
等待IG接通
结果通知
未处理 (0X00)
等待更新同意 (0X01)
等待下载同意 (0X02)
分发数据包下载中 (0X03)
等待安装同意 (0X04)
安装准备 (0X05)
安装中 (0X06)
等待激活同意 (0X07)
改写后处理 (0X08)
改写完成 (0X09)

图222

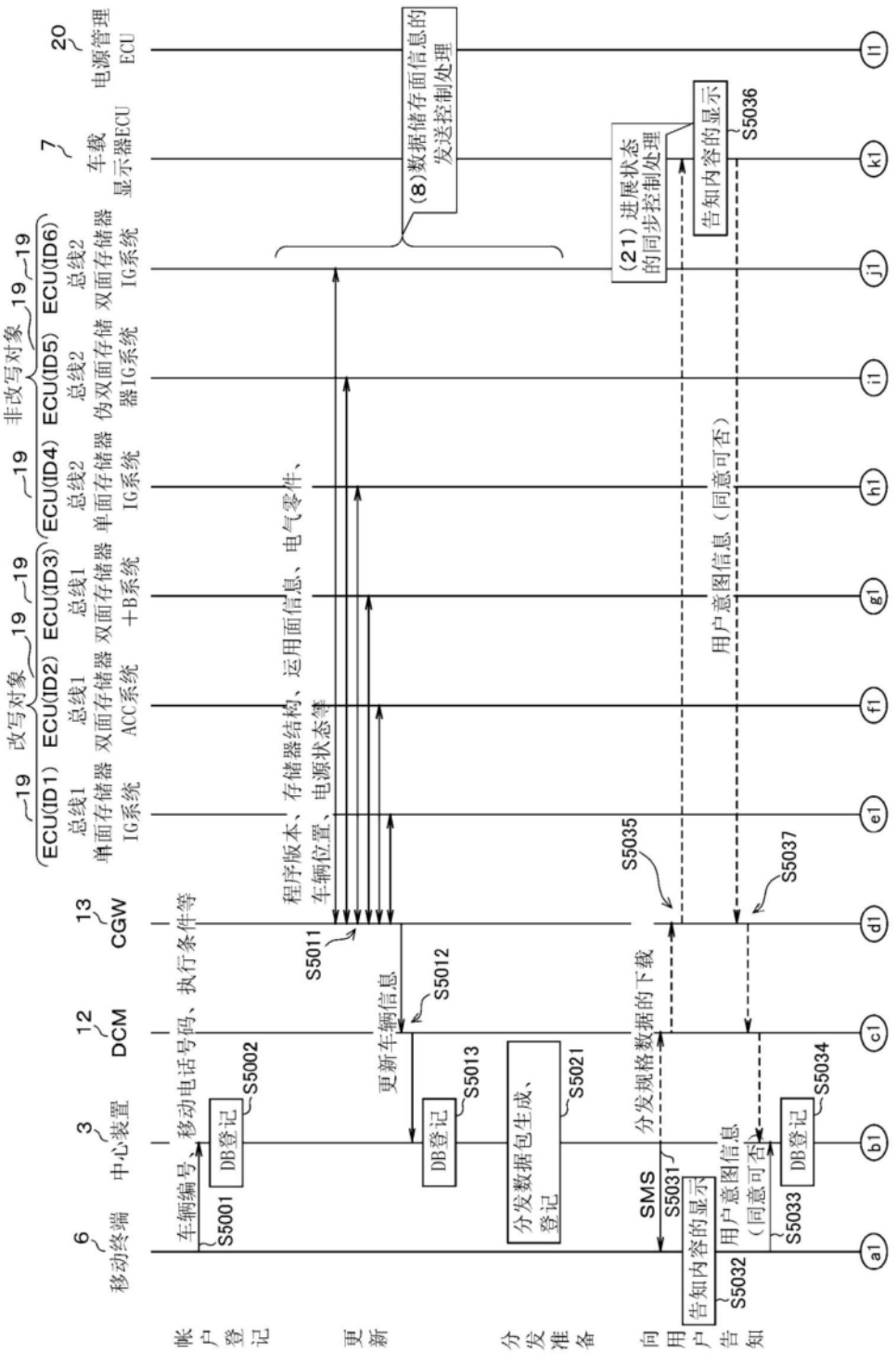

移动终端 6
中心装置 3
DCM 12
CGW 13
ECU(ID1) 19 单面存储器 总线1 IG系统
ECU(ID2) 19 双面存储器 总线1 ACC系统
ECU(ID3) 19 双面存储器 总线1 +B系统
ECU(ID4) 19 单面存储器 总线2 IG系统
ECU(ID5) 19 伪双面存储器 总线2 IG系统
ECU(ID6) 19 双面存储器 总线2 IG系统
车载显示器ECU 7
电源管理ECU 20
改写对象
非改写对象
车辆编号、移动电话号码、执行条件等
程序版本、存储器结构、运用面信息、电气零件、车辆位置、电源状态等
用户意图信息（同意可否）
S5001 DB登记
S5002
S5011
S5012 更新车辆信息
S5013 DB登记
S5021 分发数据包生成、登记
S5031 SMS 分发规格数据的下载
S5032 告知内容的显示
S5033 用户意图信息（同意可否）
S5034 DB登记
S5035
S5036 告知内容的显示
S5037
(8)数据储存面信息的发送控制处理
(21)进展状态的同步控制处理
a1 b1 c1 d1 e1 f1 g1 h1 i1 j1 k1 l1
帐户登记
更新
分发准备
向用户告知

图223

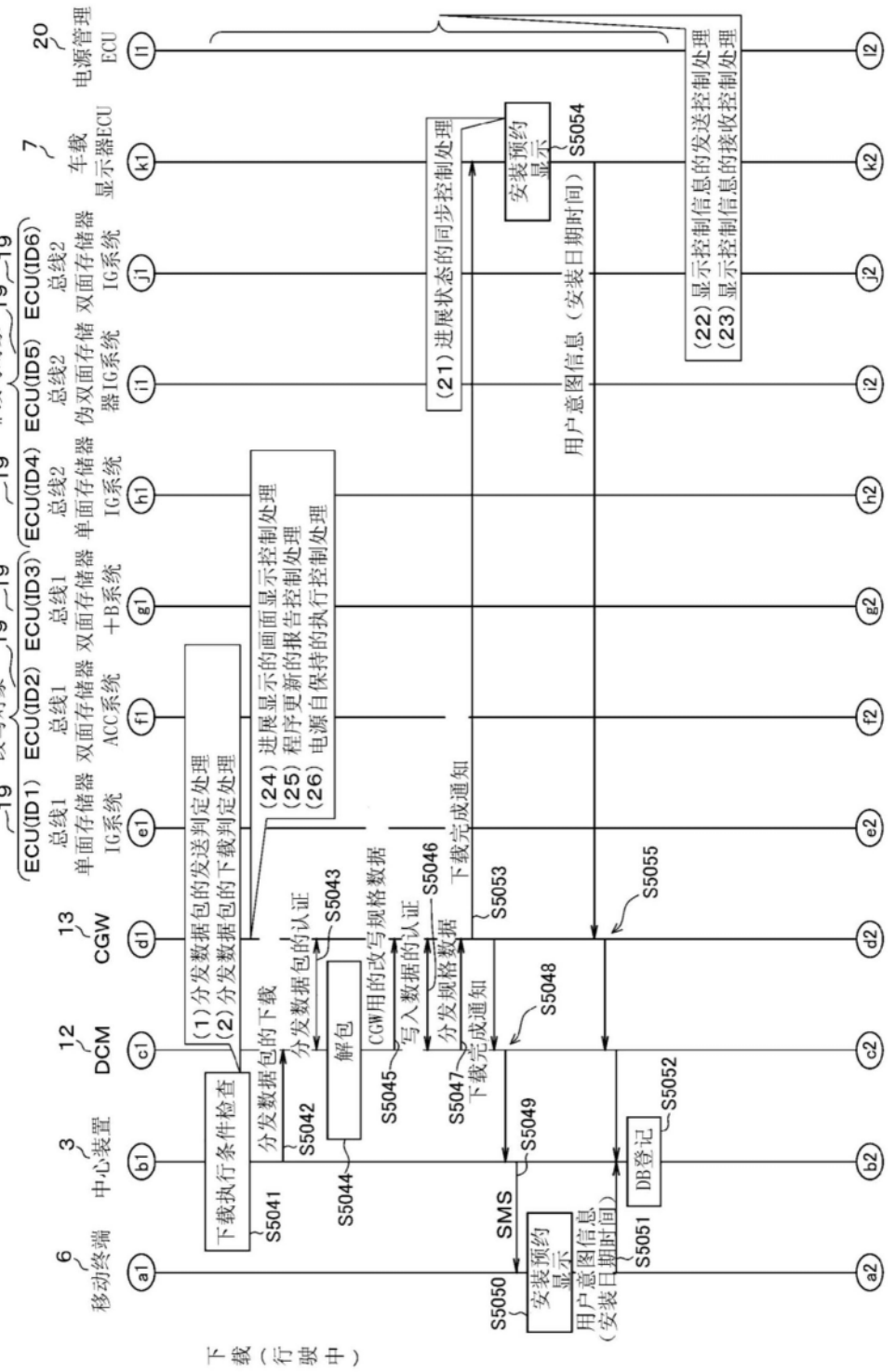

移动终端
中心装置
DCM
CGW
单面存储器 IG系统
双面存储器 ACC系统
双面存储器 +B系统
单面存储器 IG系统
伪双面存储器 IG系统
双面存储器 IG系统
车载显示器ECU
电源管理ECU
ECU(ID1) 总线1
ECU(ID2) 总线1
ECU(ID3) 总线1
ECU(ID4) 总线2
ECU(ID5) 总线2
ECU(ID6) 总线2
改写对象
非改写对象
(1)分发数据包的发送判定处理
(2)分发数据包的下载判定处理
(24)进展显示的画面显示控制处理
(25)程序更新的报告控制处理
(26)电源自保持的执行控制处理
(21)进展状态的同步控制处理
(22)显示控制信息的发送控制处理
(23)显示控制信息的接收控制处理
下载执行条件检查
分发数据包的下载
分发数据包的认证
解包
CGW用的改写规格数据
写入数据的认证
分发规格数据
下载完成通知
SMS
安装预约显示
用户意图信息（安装日期时间）
DB登记
S5041
S5042
S5043
S5044
S5045
S5046
S5047
S5048
S5049
S5050
S5051
S5052
S5053
S5054
S5055
下载（行驶中）

图224

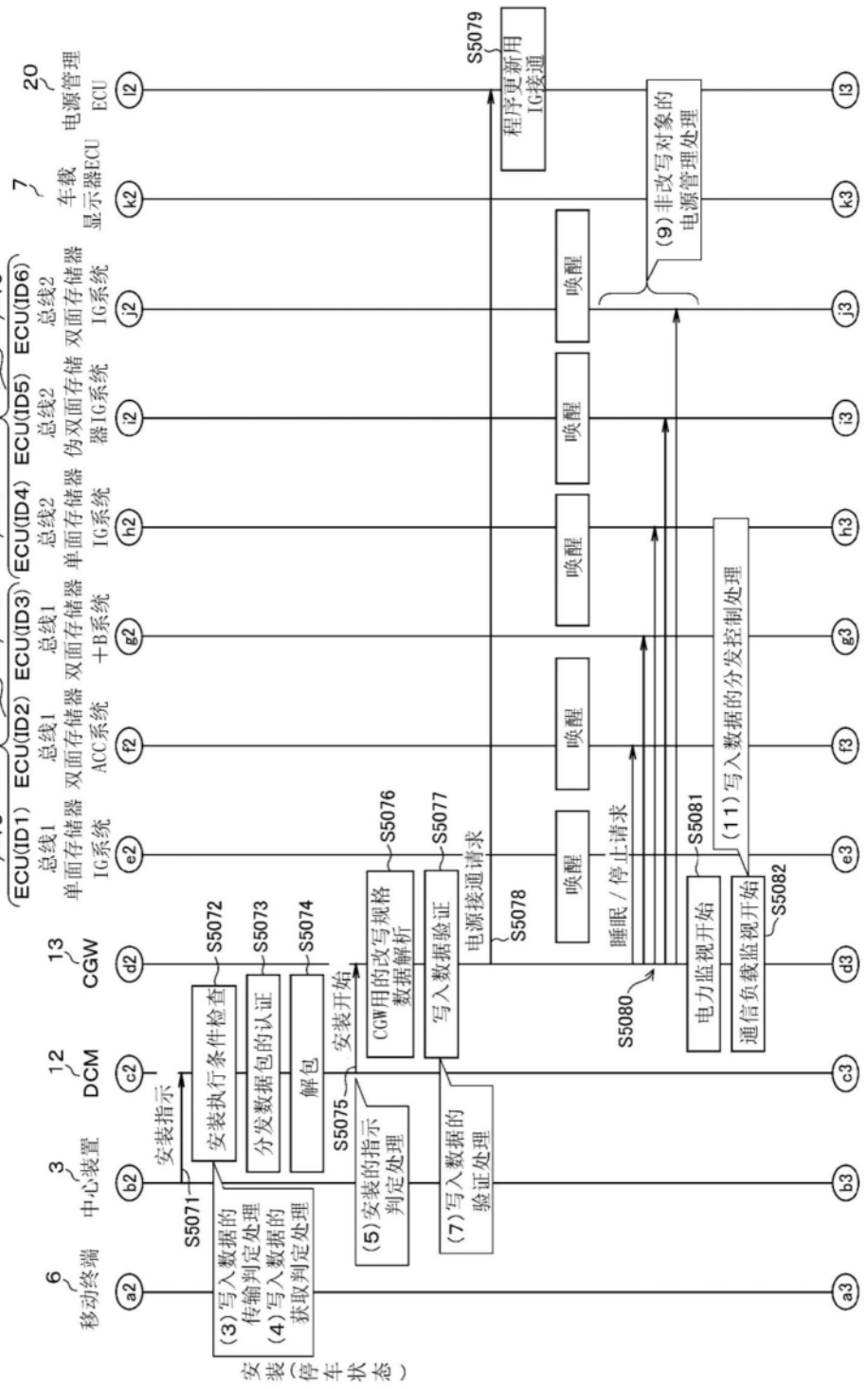

6
移动终端
3
中心装置
12
DCM
13
CGW
19
ECU(ID1)
总线1
单面存储器
IG系统
19
改写对象
ECU(ID2)
总线1
双面存储器
ACC系统
19
ECU(ID3)
总线1
双面存储器
+B系统
19
ECU(ID4)
总线2
单面存储器
IG系统
19
非改写对象
ECU(ID5)
总线2
伪双面存储器
IG系统
19
ECU(ID6)
总线2
双面存储器
IG系统
7
车载
显示器ECU
20
电源管理
ECU
a2
b2
c2
d2
e2
f2
g2
h2
i2
k2
l2
a3
b3
c3
d3
e3
f3
g3
h3
i3
k3
l3
S5071
S5072
S5073
S5074
S5075
S5076
S5077
S5078
S5079
S5080
S5081
S5082
安装指示
安装执行条件检查
分发数据包的认证
解包
安装开始
CGW用的改写规格数据解析
写入数据验证
电源接通请求
程序更新用IG接通
睡眠/停止请求
唤醒
唤醒
唤醒
唤醒
唤醒
(3)写入数据的传输判定处理
(4)写入数据的获取判定处理
(5)安装的指示判定处理
(7)写入数据的验证处理
电力监视开始
通信负载监视开始
(9)非改写对象的电源管理处理
(11)写入数据的分发控制处理
安装(停车状态)

图225

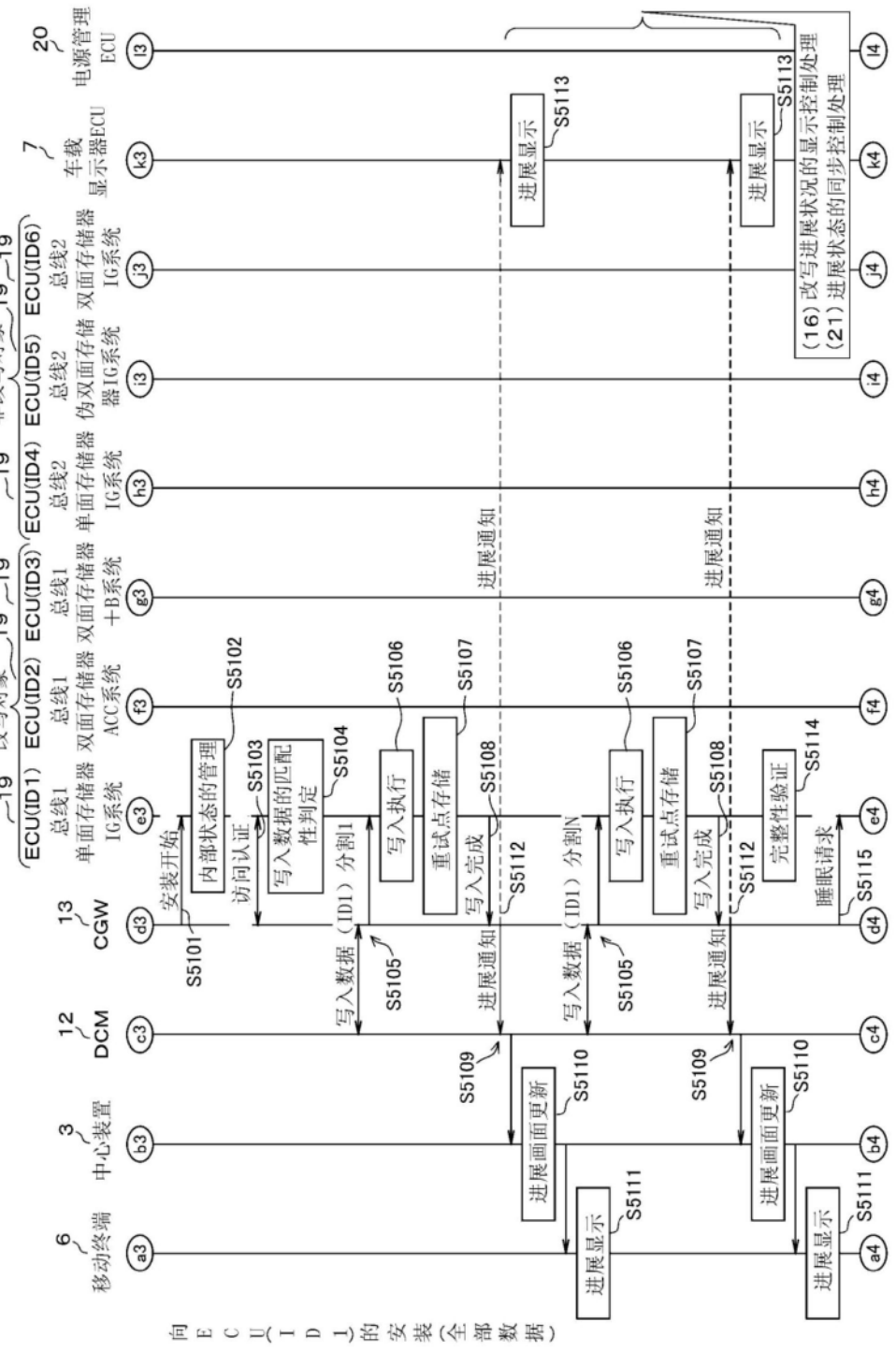

向ECU(ID1)的安装(全部数据)
移动终端
6
中心装置
3
DCM
12
CGW
13
车载显示器ECU
7
电源管理ECU
20
ECU(ID1) 总线1 单面存储器 IG系统
ECU(ID2) 总线1 双面存储器 ACC系统
ECU(ID3) 总线1 双面存储器 +B系统
ECU(ID4) 总线2 单面存储器 IG系统
ECU(ID5) 总线2 伪双面存储器 IG系统
ECU(ID6) 总线2 双面存储器 IG系统
改写对象
非改写对象
安装开始
内部状态的管理
访问认证
写入数据的匹配性判定
写入数据（ID1）分割1
写入执行
重试点存储
写入完成
写入数据（ID1）分割N
完整性验证
睡眠请求
进展通知
进展画面更新
进展显示
(16)改写进展状况的显示控制处理
(21)进展状态的同步控制处理
S5101
S5102
S5103
S5104
S5105
S5106
S5107
S5108
S5109
S5110
S5111
S5112
S5113
S5114
S5115

图226

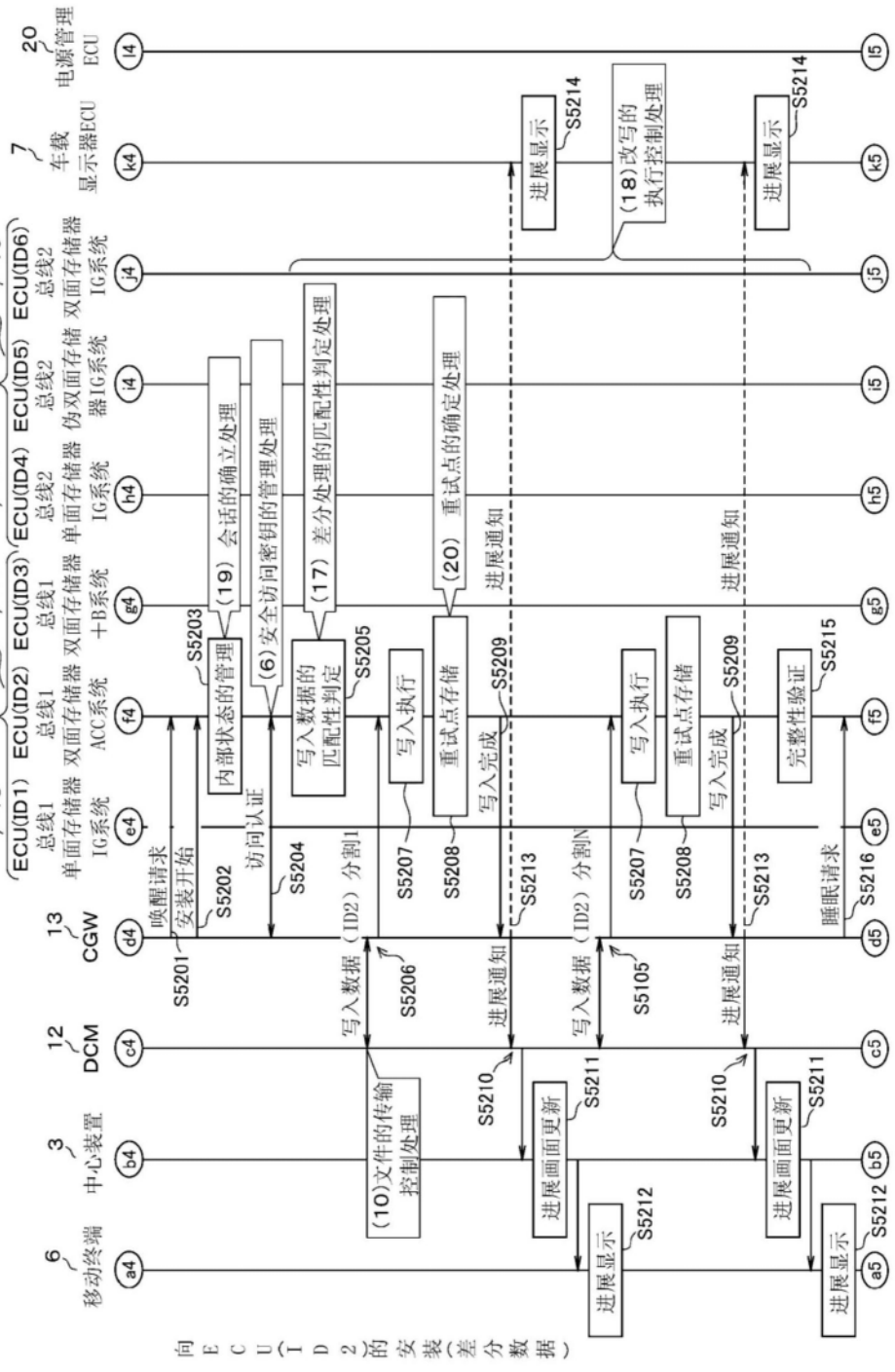

向ECU（ID2）的安装（差分数据）
移动终端
6
中心装置
3
DCM
12
CGW
13
车载显示器ECU
7
电源管理ECU
20
ECU(ID1) 总线1 单面存储器 IG系统
ECU(ID2) 总线1 双面存储器 ACC系统
ECU(ID3) 总线1 双面存储器 +B系统
ECU(ID4) 总线2 单面存储器 IG系统
ECU(ID5) 总线2 双面存储器 伪IG系统
ECU(ID6) 总线2 双面存储器 IG系统
改写对象
非改写对象
唤醒请求
安装开始
S5201
S5202
内部状态的管理
S5203
(19) 会话的确立处理
访向认证
S5204
(6) 安全访问密钥的管理处理
写入数据的匹配性判定
S5205
(17) 差分处理的匹配性判定处理
写入数据（ID2）分割1
S5206
写入执行
S5207
重试点存储
S5208
(20) 重试点的确定处理
写入完成
S5209
进展通知
S5210
(10)文件的传输控制处理
进展画面更新
S5211
进展显示
S5212
写入数据（ID2）分割N
S5105
S5213
进展显示
S5214
(18)改写的执行控制处理
睡眠请求
S5215
完整性验证
S5216

图227

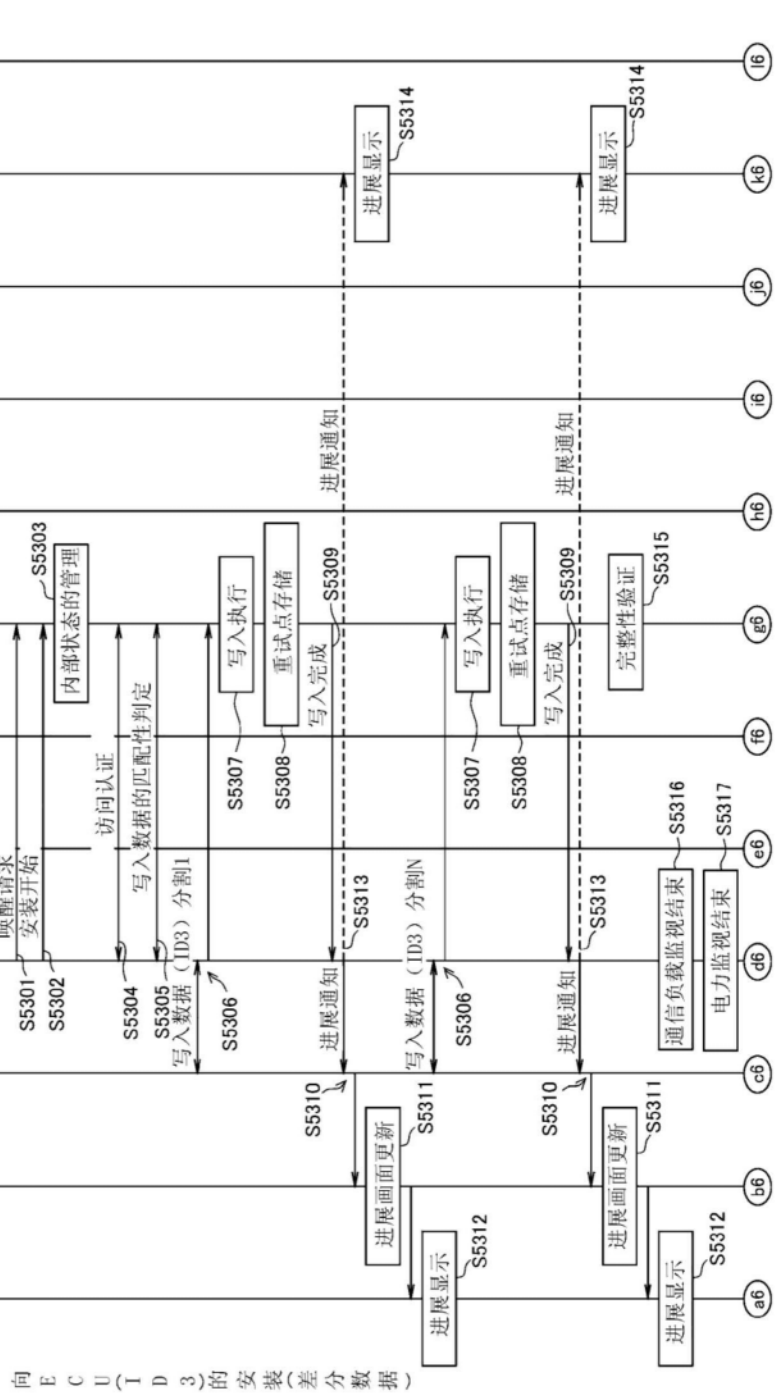

向ECU（ID3）的安装（差分数据）
移动终端
中心装置
DCM
CGW
ECU(ID1) 总线1 单面存储器 IG系统
ECU(ID2) 总线1 双面存储器 ACC系统
ECU(ID3) 总线1 双面存储器 +B系统
ECU(ID4) 总线2 单面存储器 IG系统
ECU(ID5) 总线2 伪双面存储器 IG系统
ECU(ID6) 总线2 双面存储器 IG系统
车载显示器ECU
电源管理ECU
改写对象
非改写对象
唤醒请求
安装开始
访问认证
内部状态的管理
写入数据的匹配性判定
写入数据（ID3）分割1
写入执行
重试点存储
写入完成
进展通知
写入数据（ID3）分割N
完整性验证
通信负载监视结束
电力监视结束
进展画面更新
进展显示
S5301
S5302
S5303
S5304
S5305
S5306
S5307
S5308
S5309
S5310
S5311
S5312
S5313
S5314
S5315
S5316
S5317

图228

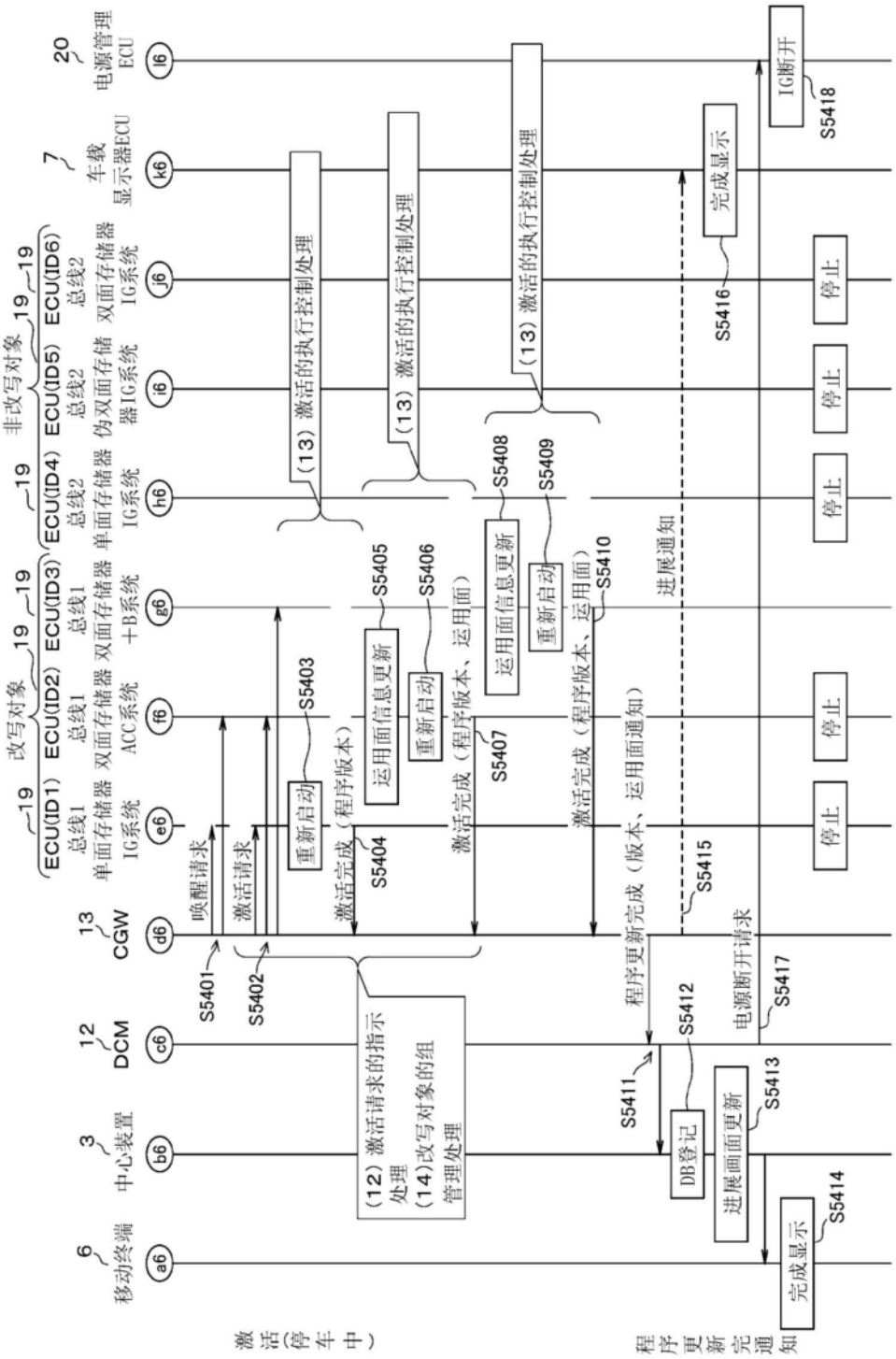

移动终端
6
中心装置
3
DCM
12
CGW
13
ECU(ID1)
ECU(ID2)
ECU(ID3)
ECU(ID4)
ECU(ID5)
ECU(ID6)
车载显示器ECU
7
电源管理ECU
20
改写对象
非改写对象
总线1
总线2
单面存储器IG系统
双面存储器ACC系统
双面存储器+B系统
伪双面存储器IG系统
双面存储器IG系统
唤醒请求
激活请求
重新启动
激活完成（程序版本）
运用面信息更新
重新启动
激活完成（程序版本、运用面）
运用面信息更新
重新启动
激活完成（程序版本、运用面）
进展通知
程序更新完成（版本、运用面通知）
电源断开请求
完成显示
IG断开
停止
(12) 激活请求的指示处理
(14)改写对象的组管理处理
(13) 激活的执行控制处理
(13) 激活的执行控制处理
(13) 激活的执行控制处理
DB登记
进展画面更新
完成显示
S5401
S5402
S5403
S5404
S5405
S5406
S5407
S5408
S5409
S5410
S5411
S5412
S5413
S5414
S5415
S5416
S5417
S5418
激活（停车中）
程序更新完通知

图229

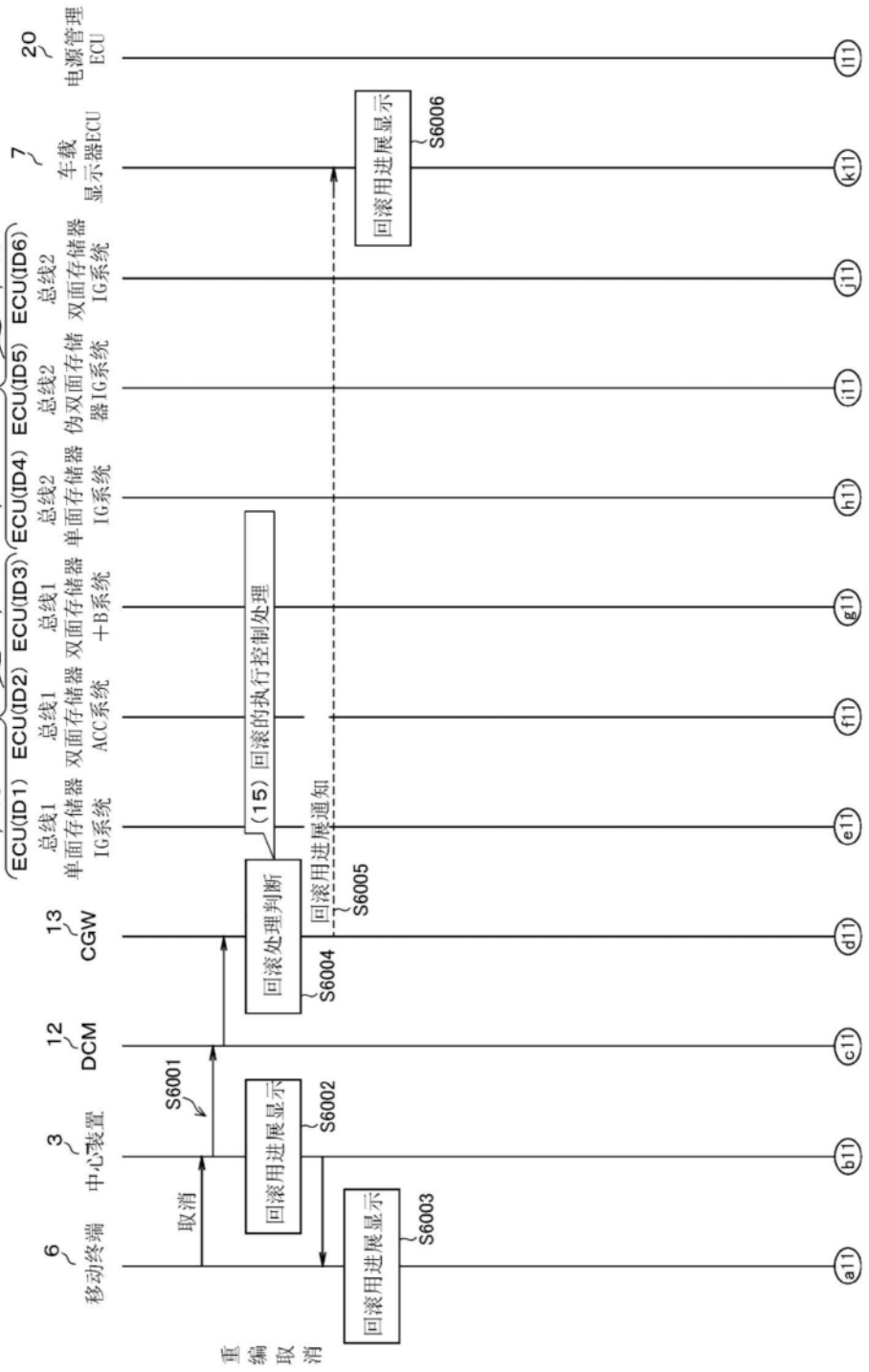

6
移动终端
3
中心装置
12
DCM
13
CGW
19
ECU(ID1)
总线1
单面存储器
IG系统
19
改写对象
ECU(ID2)
总线1
双面存储器
ACC系统
19
ECU(ID3)
总线1
双面存储器
+B系统
19
ECU(ID4)
总线2
单面存储器
IG系统
19
非改写对象
ECU(ID5)
总线2
伪双面存储器
IG系统
19
ECU(ID6)
总线2
双面存储器
IG系统
7
车载
显示器ECU
20
电源管理
ECU
重编取消
取消
S6001
回滚用进展显示
S6002
回滚用进展显示
S6003
回滚处理判断
S6004
(15) 回滚的执行控制处理
回滚用进展通知
S6005
回滚用进展显示
S6006
a11
b11
c11
d11
e11
f11
g11
h11
i11
j11
k11
l11

图230

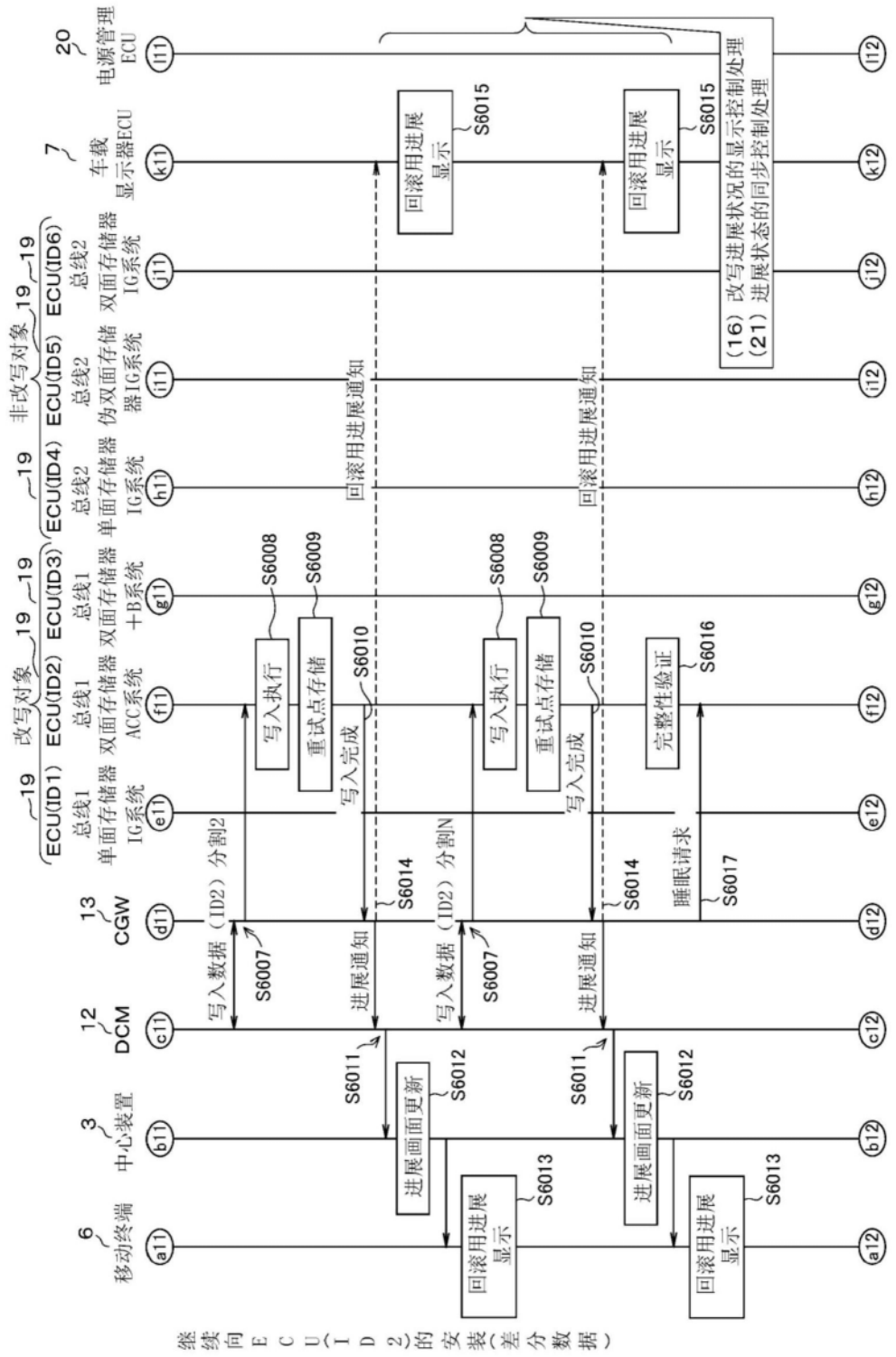

移动终端
中心装置
DCM
CGW
ECU(ID1)
总线1
单面存储器
IG系统
ECU(ID2)
总线1
双面存储器
ACC系统
ECU(ID3)
总线1
双面存储器
+B系统
ECU(ID4)
总线2
单面存储器
IG系统
ECU(ID5)
总线2
伪双面存储器
IG系统
ECU(ID6)
总线2
双面存储器
IG系统
车载显示器ECU
电源管理ECU
改写对象
非改写对象
进展画面更新
回滚用进展显示
写入数据（ID2）分割2
写入数据（ID2）分割N
进展通知
写入执行
重试点存储
写入完成
回滚用进展通知
完整性验证
睡眠请求
(16) 改写进展状况的显示控制处理
(21) 进展状态的同步控制处理
S6007
S6008
S6009
S6010
S6011
S6012
S6013
S6014
S6015
S6016
S6017
继续向ECU(ID2)的安装（差分数据）

图231

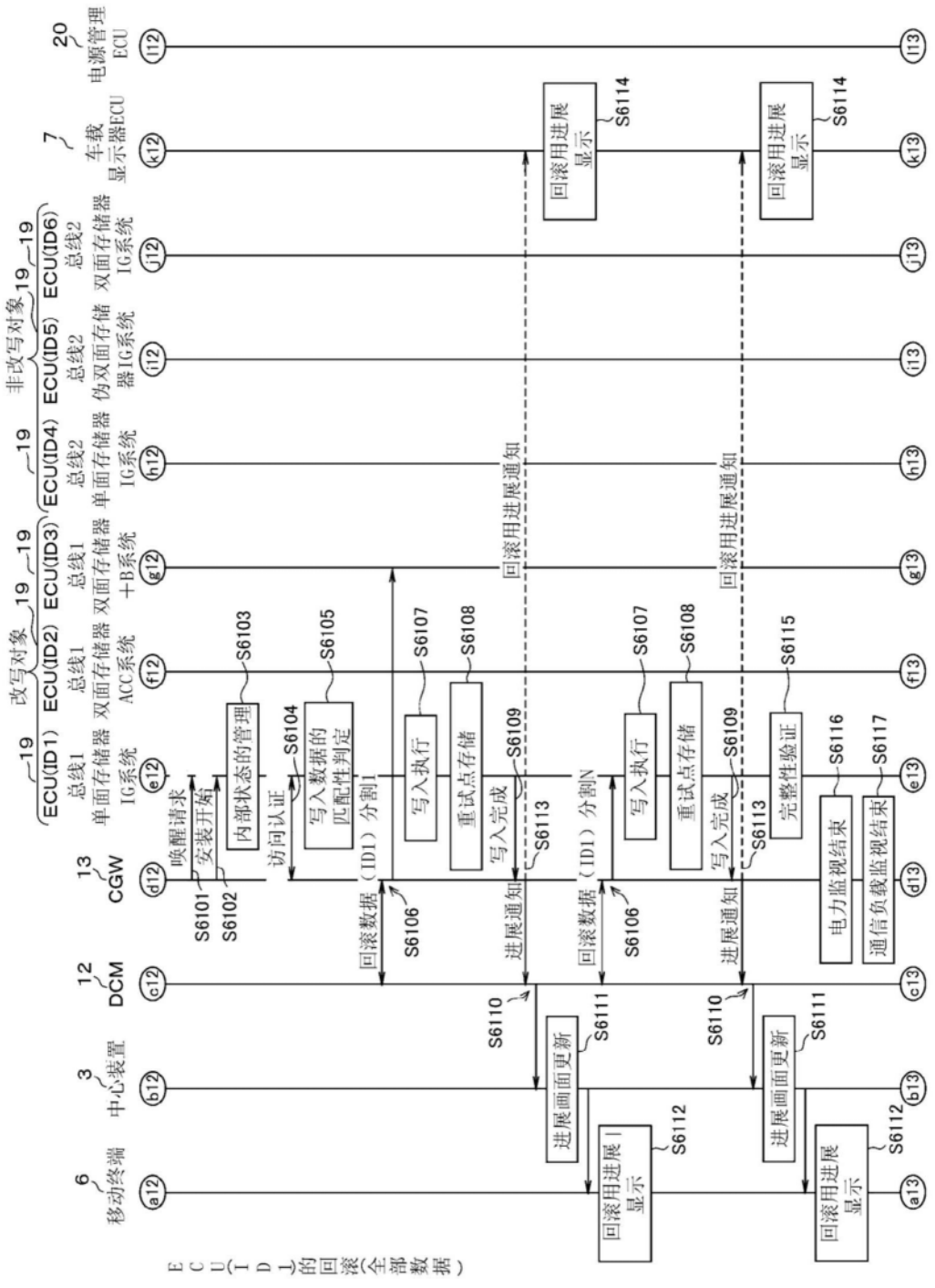

ECU(ID1)的回滚(全部数据)
6 移动终端
3 中心装置
12 DCM
13 CGW
19 ECU(ID1) 总线1 单面存储器 IG系统
19 ECU(ID2) 总线1 双面存储器 ACC系统
19 ECU(ID3) 总线1 双面存储器 +B系统
19 ECU(ID4) 总线2 单面存储器 IG系统
19 ECU(ID5) 总线2 伪双面存储器 IG系统
19 ECU(ID6) 总线2 双面存储器 IG系统
7 车载显示器ECU
20 电源管理ECU
改写对象
非改写对象
唤醒请求
安装开始
内部状态的管理
访问认证
写入数据的匹配性判定
写入执行
重试点存储
写入完成
回滚数据（ID1）分割1
回滚数据（ID1）分割N
进展通知
回滚用进展通知
完整性验证
电力监视结束
通信负载监视结束
进展画面更新
回滚用进展显示
S6101
S6102
S6103
S6104
S6105
S6106
S6107
S6108
S6109
S6110
S6111
S6112
S6113
S6114
S6115
S6116
S6117

图232

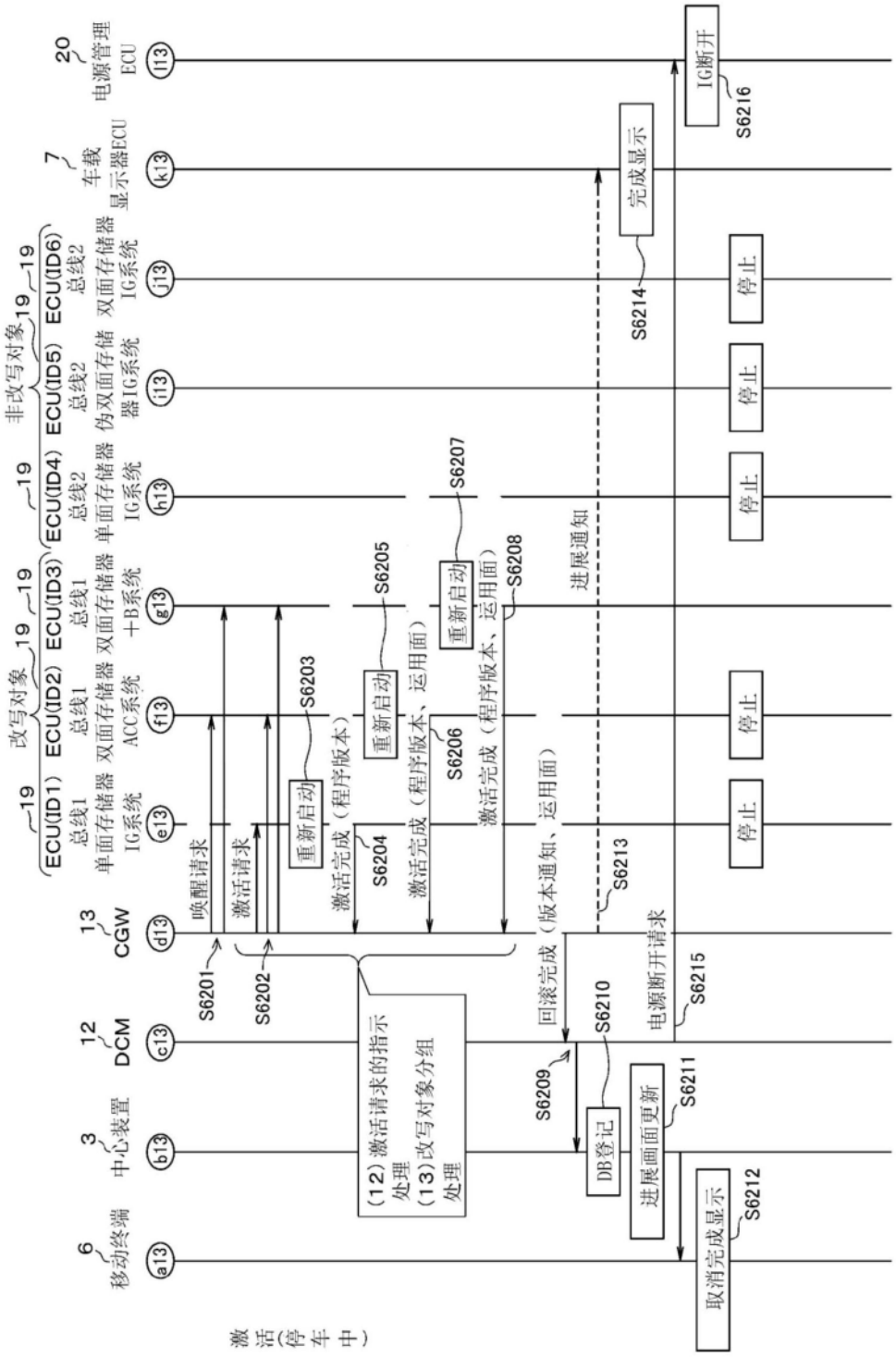

移动终端
6
中心装置
3
DCM
12
CGW
13
电源管理ECU
20
车载显示器ECU
7
非改写对象
改写对象
ECU(ID1) 总线1 单面存储器 IG系统
ECU(ID2) 总线1 双面存储器 ACC系统
ECU(ID3) 总线1 双面存储器 +B系统
ECU(ID4) 总线2 单面存储器 IG系统
ECU(ID5) 总线2 伪双面存储器 IG系统
ECU(ID6) 总线2 双面存储器 IG系统
19
a13
b13
c13
d13
e13
f13
g13
h13
i13
j13
k13
l13
激活(停车中)
唤醒请求
激活请求
重新启动（程序版本）
激活完成
重新启动
激活完成（程序版本、运用面）
重新启动
激活完成（程序版本、运用面）
进展通知
回滚完成（版本通知、运用面）
电源断开请求
(12)激活请求的指示处理
(13)改写对象分组处理
DB登记
进展画面更新
取消完成显示
完成显示
停止
IG断开
S6201
S6202
S6203
S6204
S6205
S6206
S6207
S6208
S6209
S6210
S6211
S6212
S6213
S6214
S6215
S6216

图233

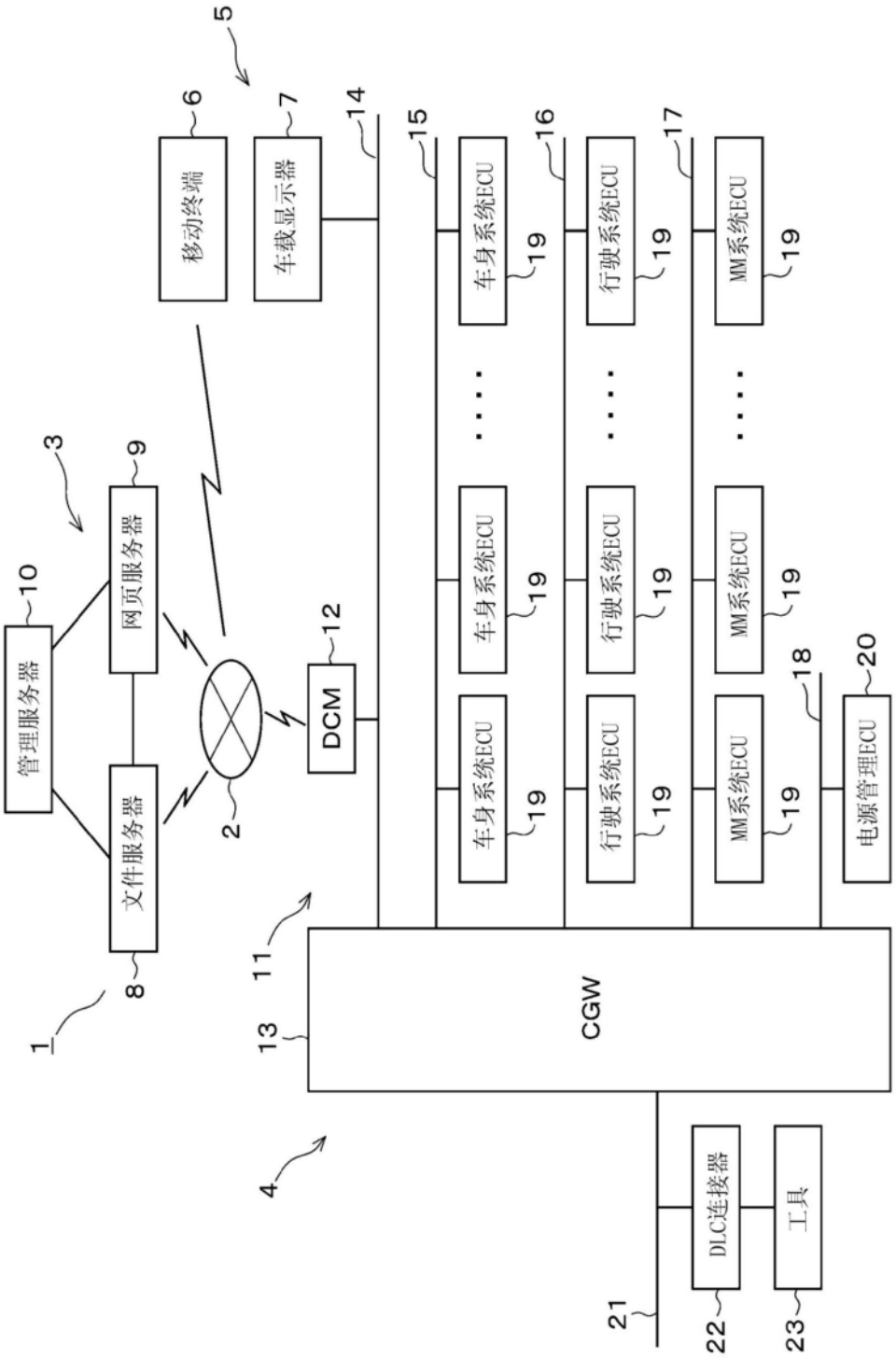

1
2
3
4
5
6
移动终端
7
车载显示器
8
文件服务器
9
网页服务器
10
管理服务器
11
12
DCM
13
CGW
14
15
车身系统ECU
16
行驶系统ECU
17
MM系统ECU
18
19
20
电源管理ECU
21
22
DLC连接器
23
工具

图234

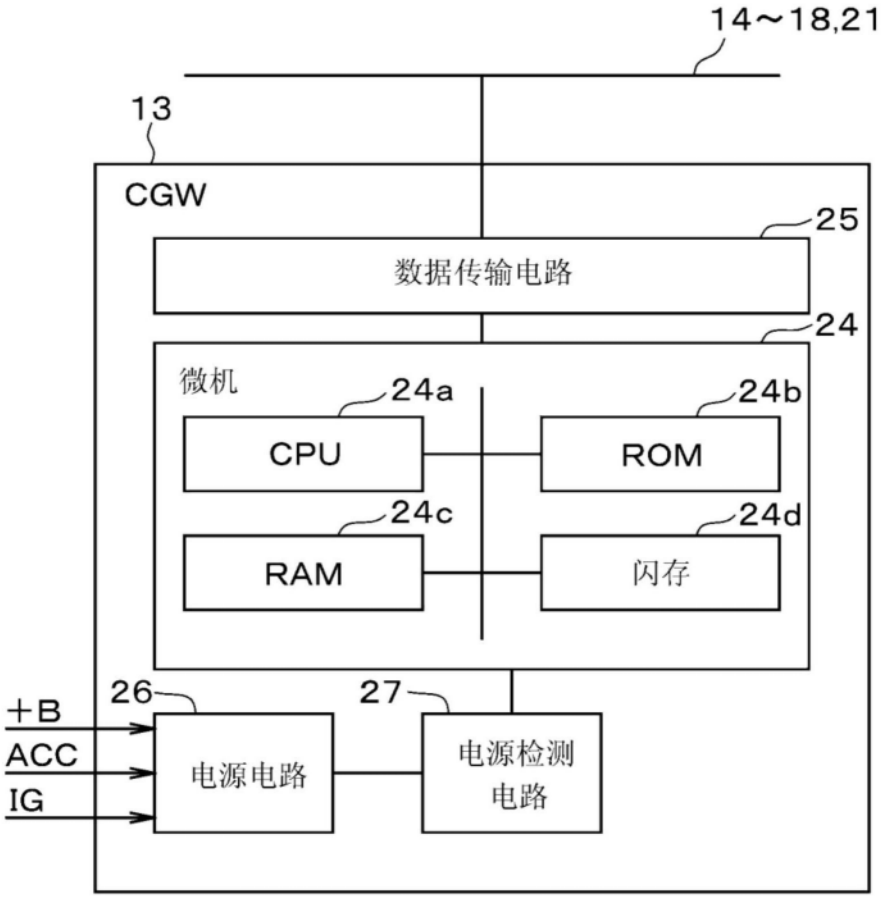

14～18,21
13
CGW
25
数据传输电路
24
微机
24a
CPU
24b
ROM
24c
RAM
24d
闪存
26
27
+B
ACC
IG
电源电路
电源检测电路

图235

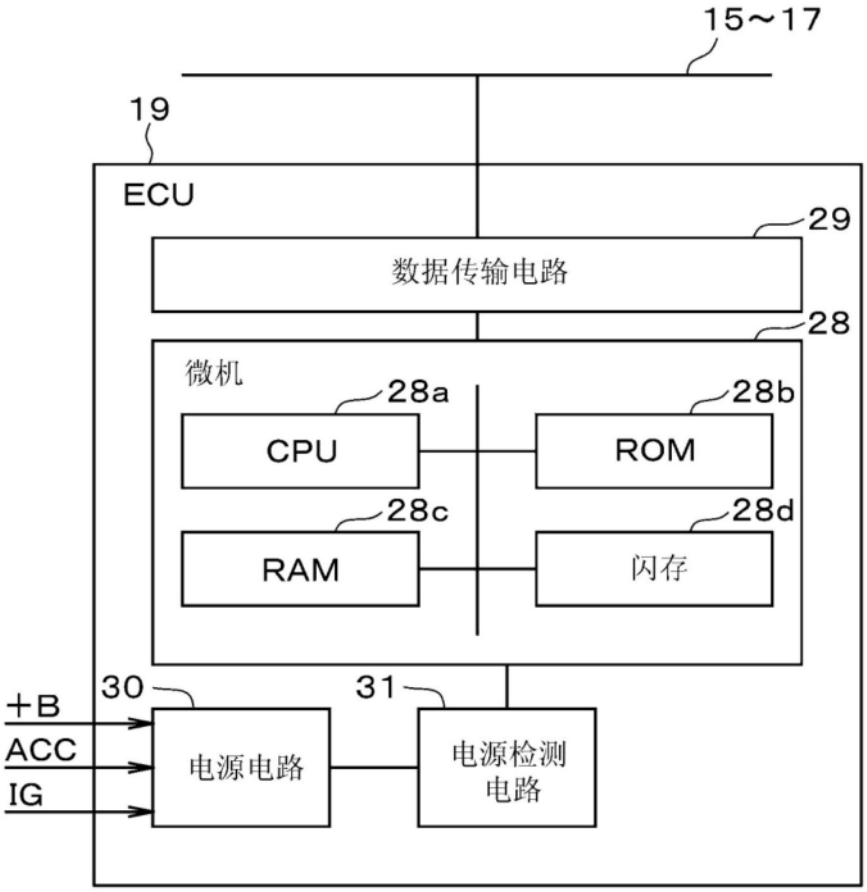

15～17
19
ECU
29
数据传输电路
28
微机
28a
CPU
28b
ROM
28c
RAM
28d
闪存
30
31
+B
ACC
IG
电源电路
电源检测电路

图236

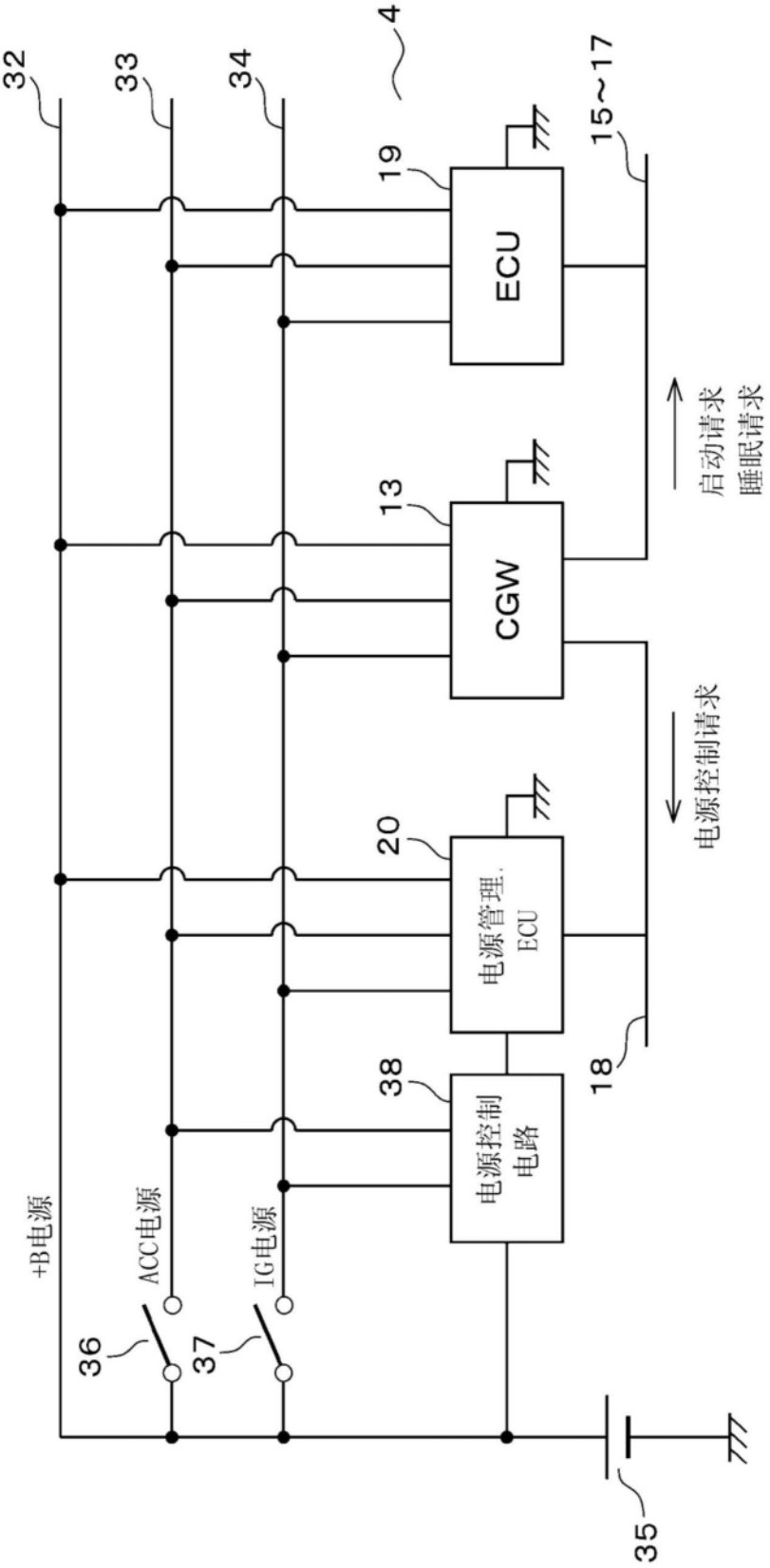

32
33
34
4
15~17
19
ECU
13
CGW
20
电源管理.
ECU
38
电源控制
电路
18
35
36
37
+B电源
ACC电源
IG电源
启动请求
睡眠请求
电源控制请求

图237

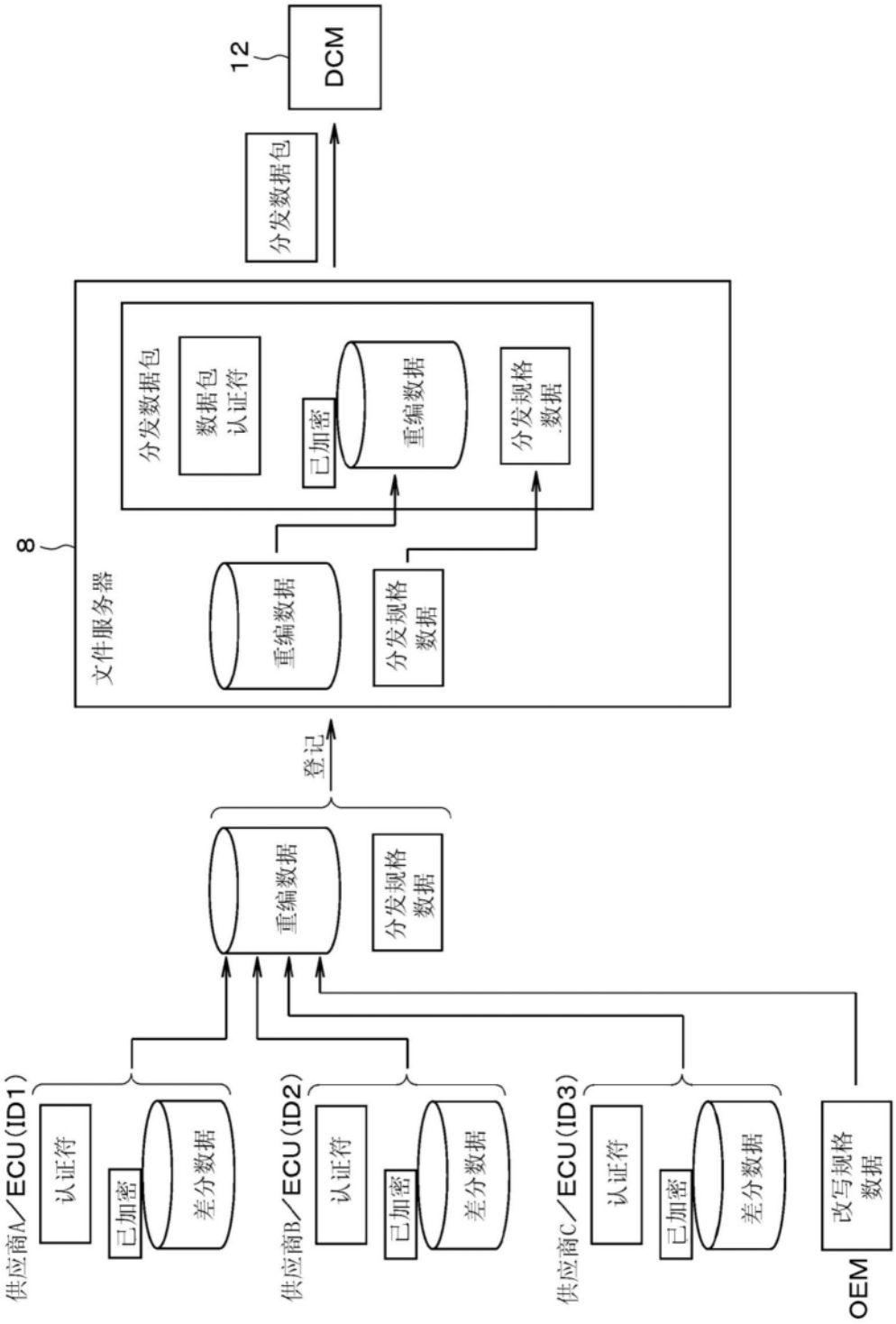

12
DCM
分发数据包
8
文件服务器
分发数据包
数据包
认证符
已加密
重编数据
分发规格
数据
重编数据
分发规格
数据
登记
重编数据
分发规格
数据
供应商A／ECU(ID1)
认证符
已加密
差分数据
供应商B／ECU(ID2)
认证符
已加密
差分数据
供应商C／ECU(ID3)
认证符
已加密
差分数据
改写规格
数据
OEM

图238

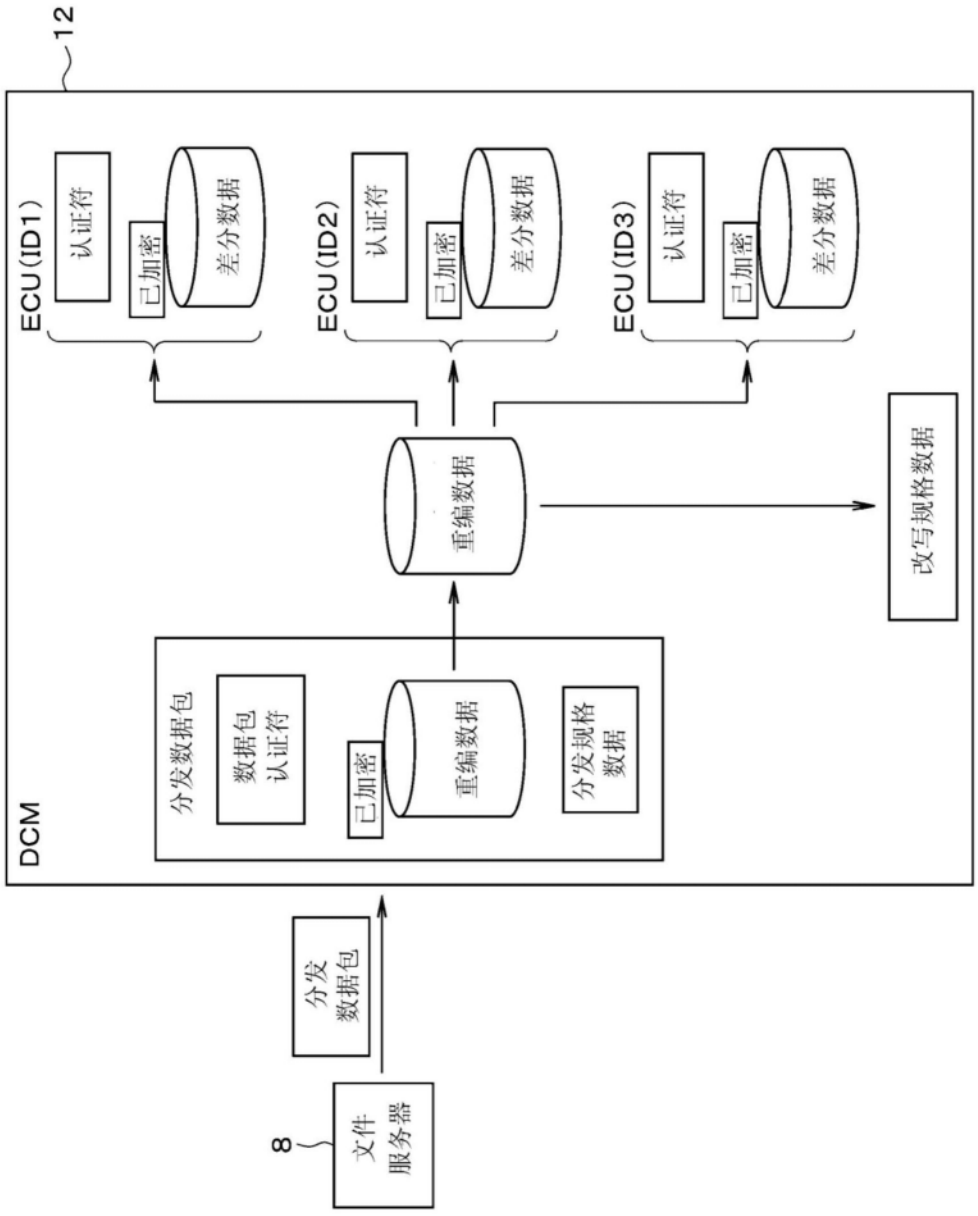

12
ECU(ID1)
认证符
已加密
差分数据
ECU(ID2)
认证符
已加密
差分数据
ECU(ID3)
认证符
已加密
差分数据
重编数据
改写规格数据
DCM
分发数据包
数据包认证符
已加密
重编数据
分发规格数据
分发数据包
8
文件服务器

图239

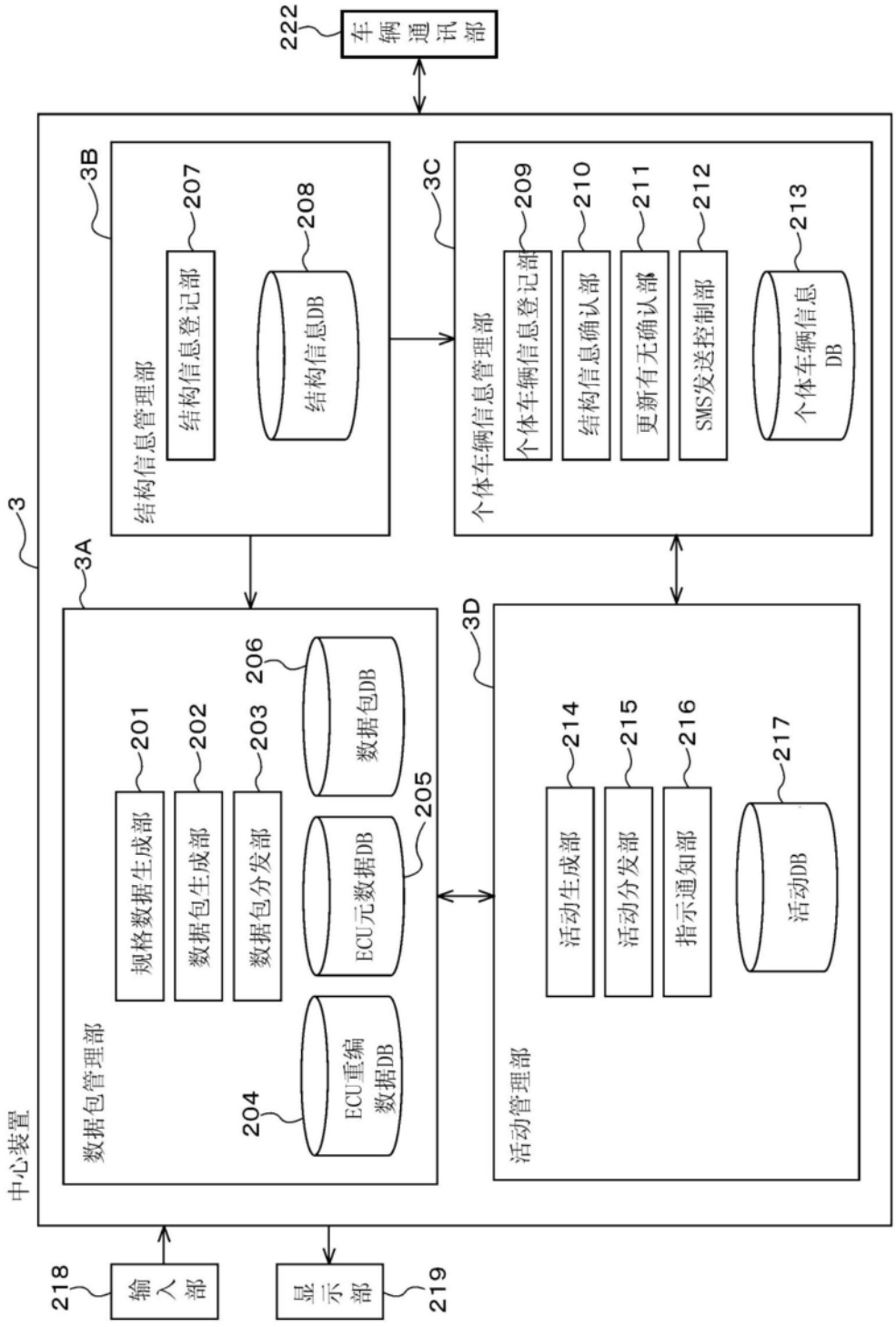

222
车辆通讯部
3
中心装置
3A
数据包管理部
201
规格数据生成部
202
数据包生成部
203
数据包分发部
206
数据包DB
205
ECU元数据DB
204
ECU重编数据DB
3B
结构信息管理部
207
结构信息登记部
208
结构信息DB
3C
个体车辆信息管理部
209
个体车辆信息登记部
210
结构信息确认部
211
更新有无确认部
212
SMS发送控制部
213
个体车辆信息DB
3D
活动管理部
214
活动生成部
215
活动分发部
216
指示通知部
217
活动DB
218
输入部
219
显示部

图240

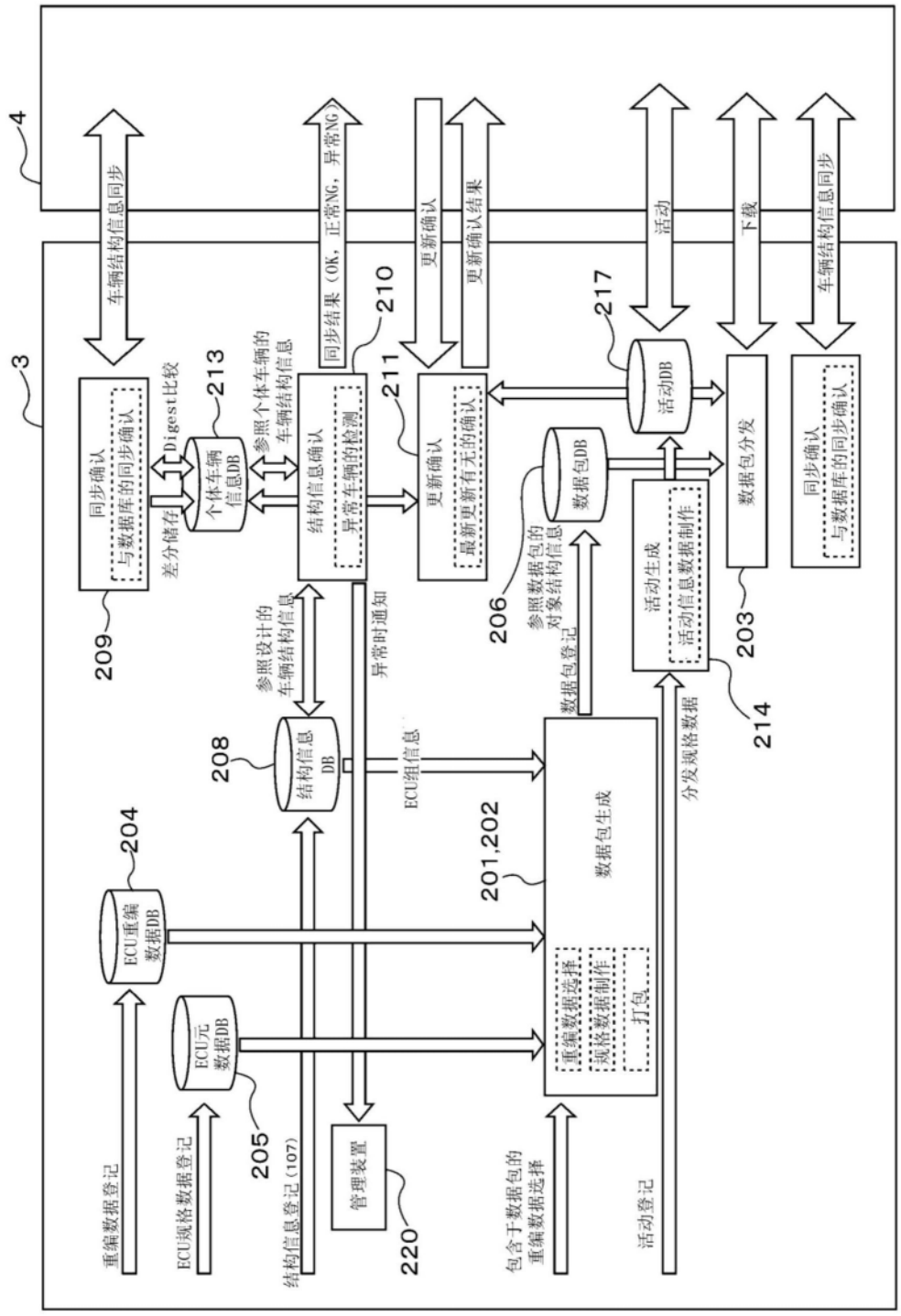
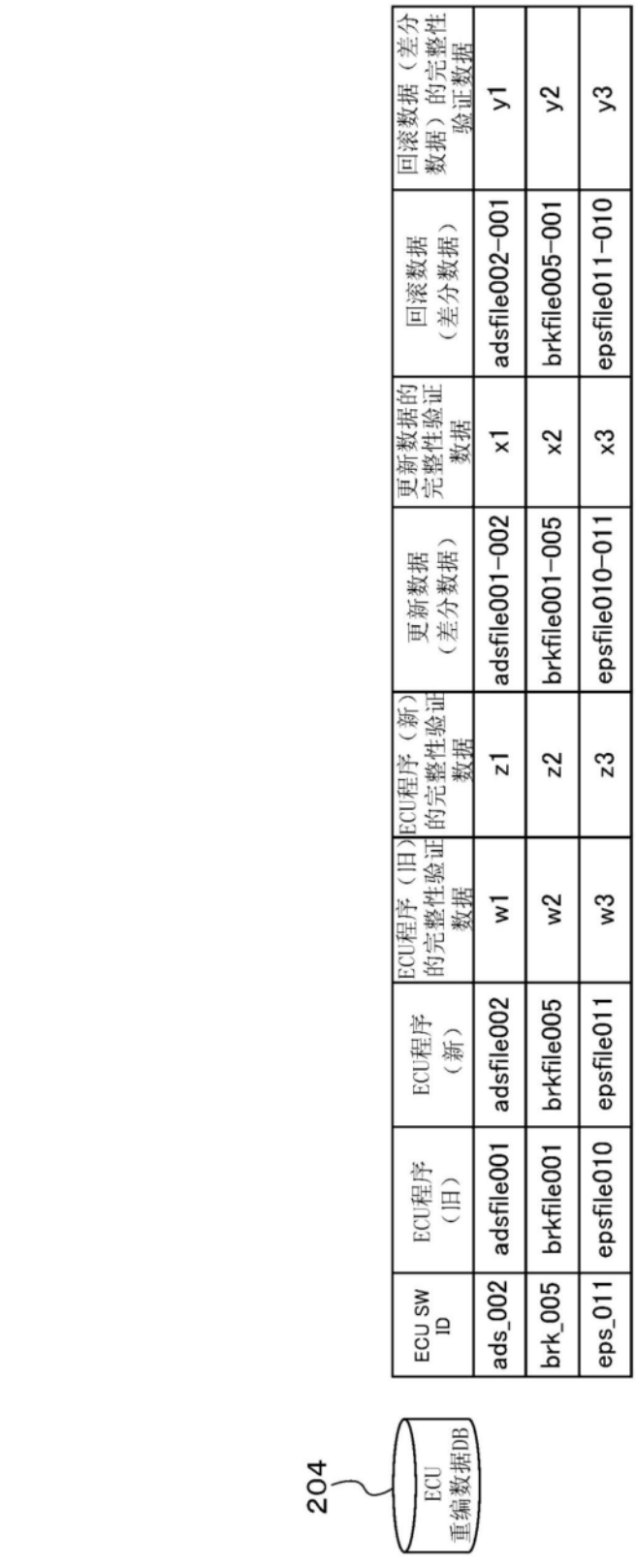

4
3
车辆结构信息同步
同步确认
与数据库的同步确认
209
差分储存
Digest比较
个体车辆
信息DB
213
参照个体车辆的
车辆结构信息
同步结果（OK，正常NG，异常NG）
210
结构信息确认
异常车辆的检测
211
更新确认
更新确认结果
更新确认
最新更新有无的确认
217
活动DB
活动
下载
数据包分发
同步确认
与数据库的同步确认
车辆结构信息同步
参照设计的
车辆结构信息
结构信息
DB
208
异常时通知
ECU组信息
206
参照数据包的
对象结构信息
数据包DB
数据包登记
活动生成
活动信息数据制作
203
214
ECU重编
数据DB
204
201,202
数据包生成
重编数据选择
规格数据制作
打包
分发规格数据
ECU元
数据DB
205
管理装置
220
重编数据登记
ECU规格数据登记
结构信息登记（107）
包含于数据包的
重编数据选择
活动登记

图241



车辆型号	Vehicle SW ID	Sys ID	ECU ID	ECU SW ID
aaa	0001	SA01_01	ADS	ads_001
aaa	0001	SA02_01	ENG	eng_010
aaa	0001	SA02_01	BRK	brk_001
aaa	0001	SA02_01	EPS	eps_010
⋮				
aaa	0002	SA01_02	ADS	ads_002
aaa	0002	SA02_02	ENG	eng_010
aaa	0002	SA02_02	BRK	brk_005
aaa	0002	SA02_02	EPS	eps_011
⋮				

图242



ECU SW ID	ECU程序（旧）	ECU程序（新）	ECU程序（旧）的完整性验证数据	ECU程序（新）的完整性验证数据	更新数据（差分数据）	更新数据的完整性验证数据	回滚数据（差分数据）	回滚数据（差分数据）的完整性验证数据
ads_002	adsfile001	adsfile002	w1	z1	adsfile001-002	x1	adsfile002-001	y1
brk_005	brkfile001	brkfile005	w2	z2	brkfile001-005	x2	brkfile005-001	y2
eps_011	epsfile010	epsfile011	w3	z3	epsfile010-011	x3	epsfile011-010	y3

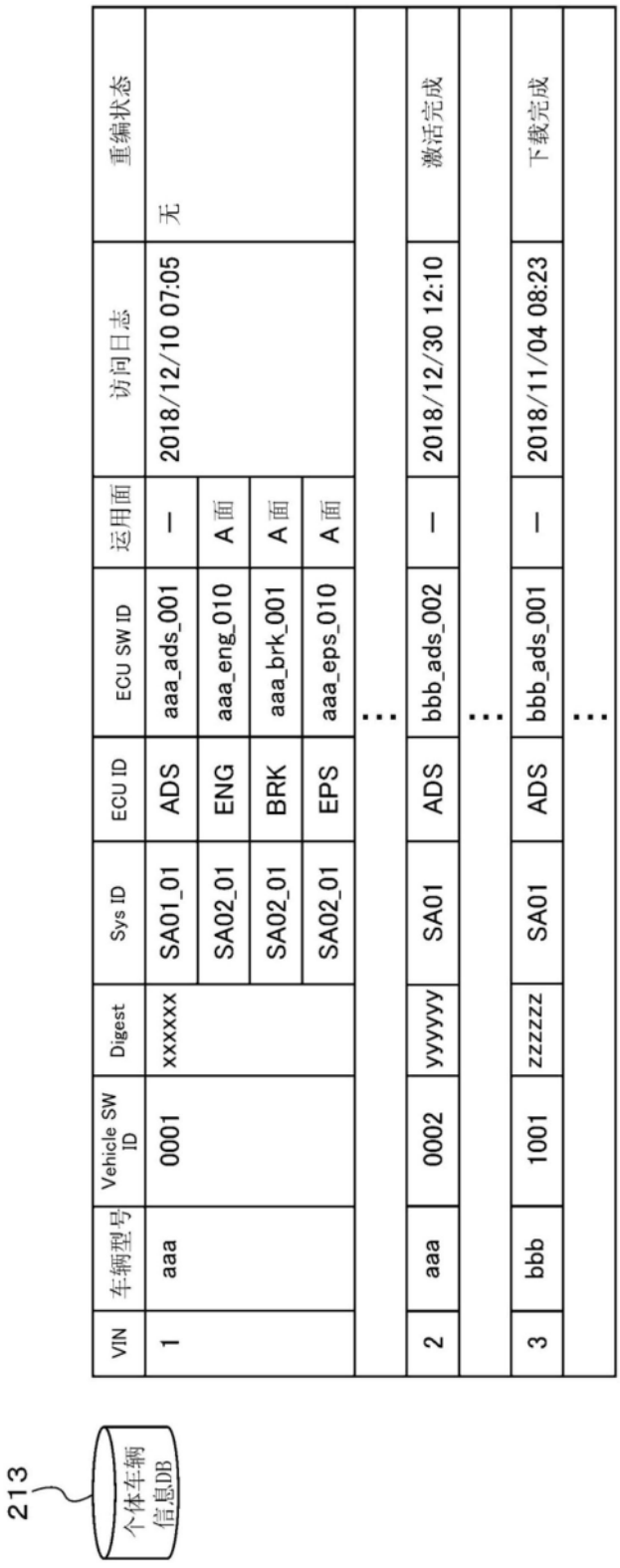
图243



ECU SW ID	更新数据大小	回滚数据大小	面	传输大小	读出用地址
ads_002	N1 M字节	M1 M字节	—	1K字节	****
brk_005	N2 M字节	M2 M字节	B面用	4K字节	****
eps_011	N3 M字节	M3 M字节	B面用	1K字节	****

车辆型号	ECU ID	存储器	总线	电源	密钥
aaa	ADS	单面	第二	IG	ads_key
aaa	ENG	双面	第一	ACC	eng_key
aaa	BRK	挂起	第一	+B	brk_key
aaa	EPS	双面	第一	+B	eps_key

图244



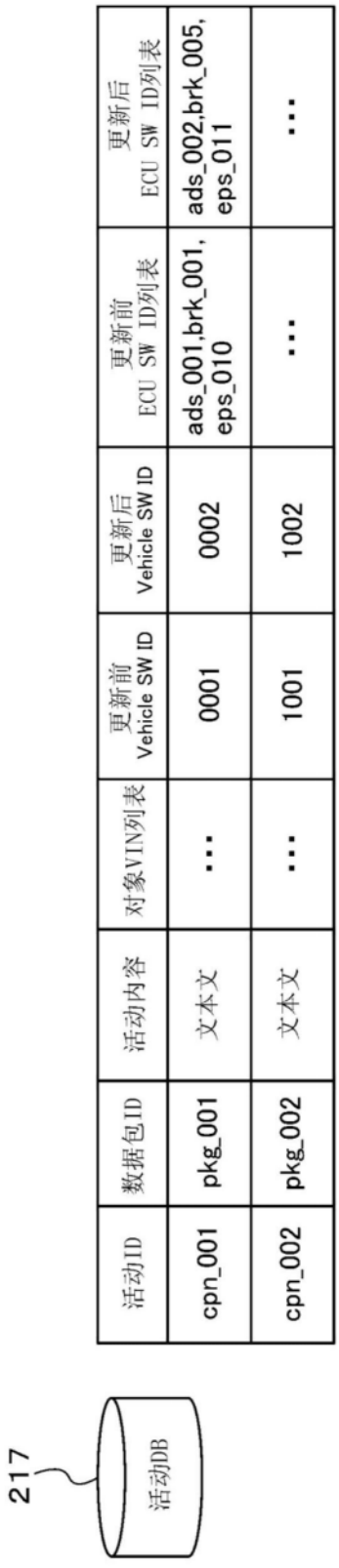
VIN	车辆型号	Vehicle SW ID	Digest	Sys ID	ECU ID	ECU SW ID	运用面	访问日志	重编状态
1	aaa	0001	xxxxxx	SA01_01	ADS	aaa_ads_001	—	2018/12/10 07:05	无
				SA02_01	ENG	aaa_eng_010	A面		
				SA02_01	BRK	aaa_brk_001	A面		
				SA02_01	EPS	aaa_eps_010	A面		
				⋮					
2	aaa	0002	yyyyyy	SA01	ADS	bbb_ads_002	—	2018/12/30 12:10	激活完成
				⋮					
3	bbb	1001	zzzzzz	SA01	ADS	bbb_ads_001	—	2018/11/04 08:23	下载完成
				⋮					

图245



数据包ID	文件	完整性验证数据
pkg_001	pkg001.dat	xx1.dat
pkg_002	pkg002.dat	xx2.dat

图246



活动ID	数据包ID	活动内容	对象VIN列表	更新前 Vehicle SW ID	更新后 Vehicle SW ID	更新前 ECU SW ID列表	更新后 ECU SW ID列表
cpn_001	pkg_001	文本文	...	0001	0002	ads_001,brk_001, eps_010	ads_002,brk_005, eps_011
cpn_002	pkg_002	文本文	...	1001	1002	...	...

图247

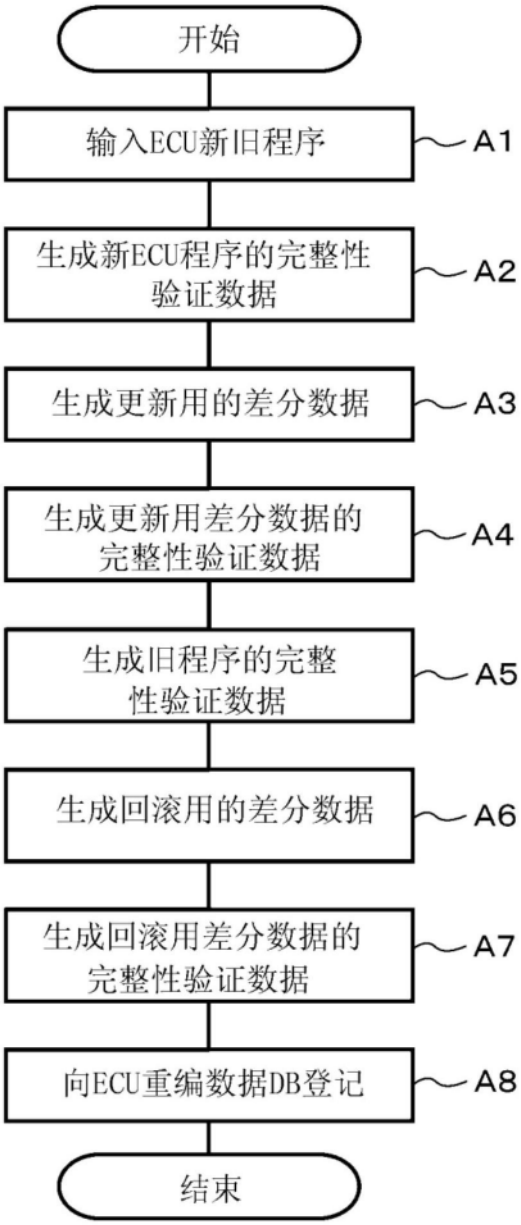

开始
输入ECU新旧程序
A1
生成新ECU程序的完整性验证数据
A2
生成更新用的差分数据
A3
生成更新用差分数据的完整性验证数据
A4
生成旧程序的完整性验证数据
A5
生成回滚用的差分数据
A6
生成回滚用差分数据的完整性验证数据
A7
向ECU重编数据DB登记
A8
结束

图248

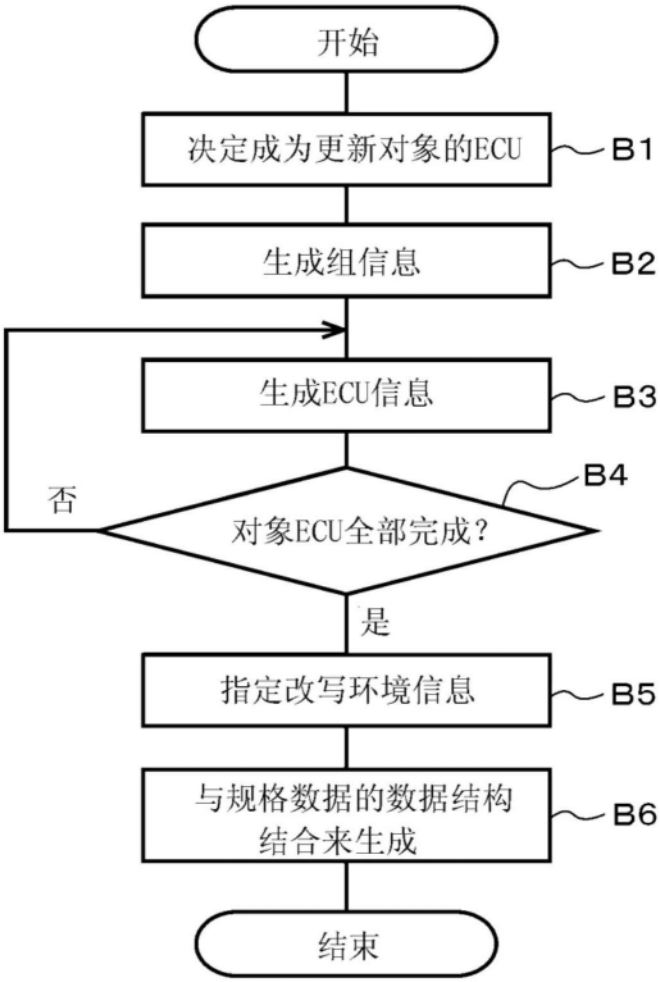

开始
决定成为更新对象的ECU
B1
生成组信息
B2
生成ECU信息
B3
B4
否
对象ECU全部完成？
是
指定改写环境信息
B5
与规格数据的数据结构
结合来生成
B6
结束

图249

规格数据

项目		值（例示）
改写环境	车辆状态	行驶中（IG接通中）可 / 仅停车中（IG断开中）
	电池负载（余量）	40%以上
	总线负载表	参照图251
组信息	第一组信息	ECU(ID1)→ECU(ID2)→ECU(ID3)
	第二组信息	ECU(ID4)→ECU(ID5)→ECU(ID6)
ECU（IDn）信息 n=1～6	ECU ID	ECU ID
	连接总线	第一总线
	连接电源	+B电源、ACC电源、IG电源
	存储器种类	单面存储器 / 伪双面存储器 / 双面存储器
	改写面信息	A面是启动面，B面是改写面
	安全访问密钥信息	随机值（密钥导出密钥）
		密钥模式
		解密运算模式
	改写方法	电源自保持 / 电源控制
	传输大小	1K字节
	更新程序版本	2.0
	更新程序获取地址	1
	更新程序大小	10M字节
	回滚程序版本	1.0
	回滚程序获取地址	0x80000
	回滚程序大小	10M字节
	写入数据种类	差分数据 / 全部数据
	写入面	B面用

图250

总线负载表

		第一总线	第二总线	第三总线
传送允许量		80%	70%	90%
IG 电源状态	车辆控制数据	50%	20%	40%
	写入数据	30%	50%	50%
ACC 电源状态	车辆控制数据	30%	30%	20%
	写入数据	50%	40%	70%
+B 电源状态	车辆控制数据	20%	10%	50%
	写入数据	60%	60%	40%

图251

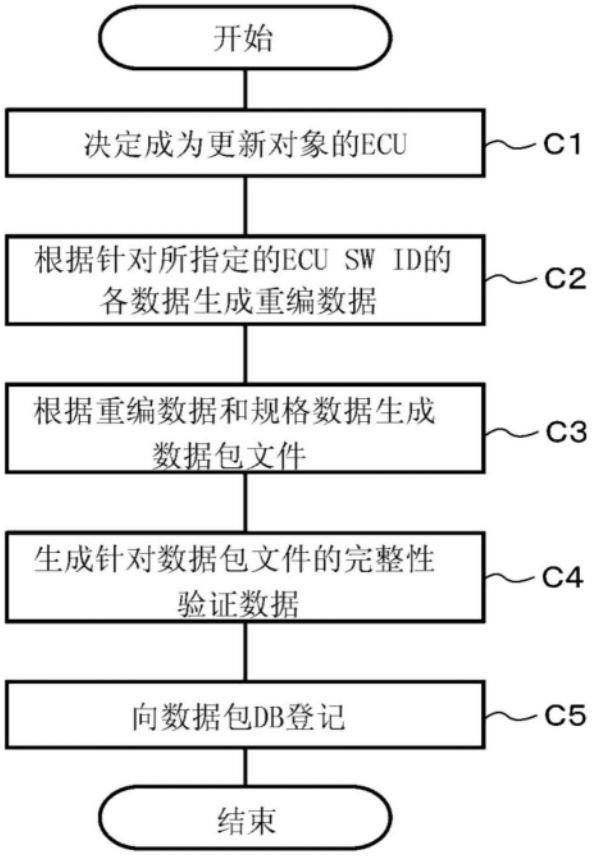


图252

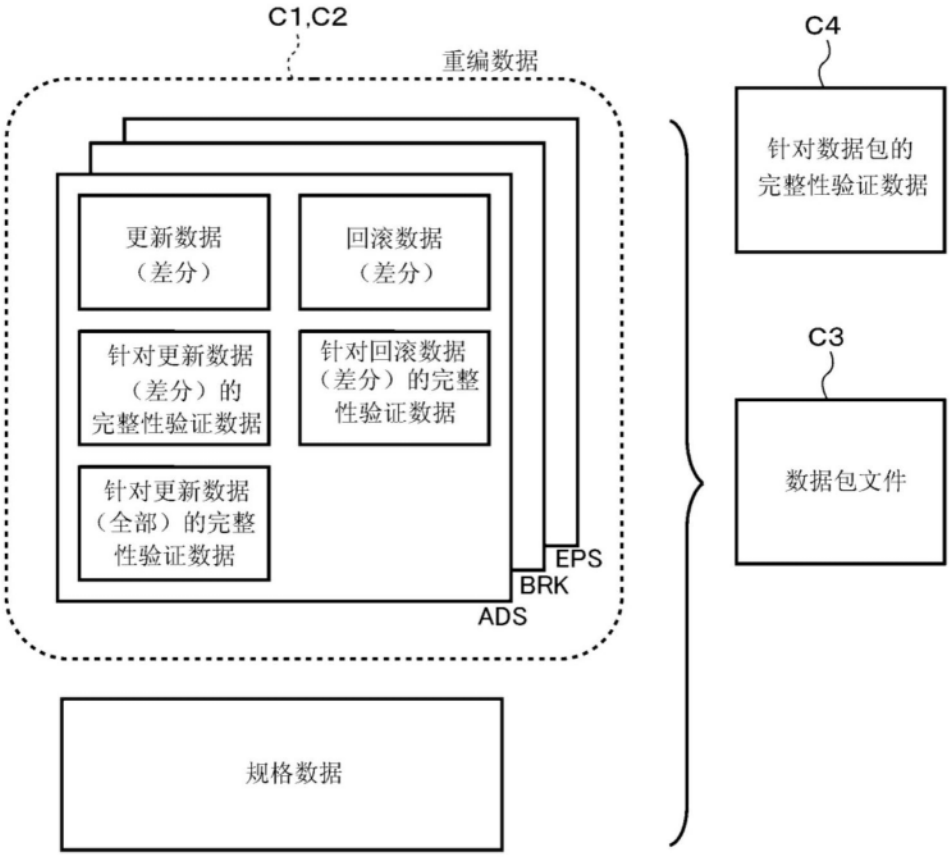

C1,C2
重编数据
更新数据
（差分）
回滚数据
（差分）
针对更新数据
（差分）的
完整性验证数据
针对回滚数据
（差分）的完整
性验证数据
针对更新数据
（全部）的完整
性验证数据
EPS
BRK
ADS
规格数据
C4
针对数据包的
完整性验证数据
C3
数据包文件

图253

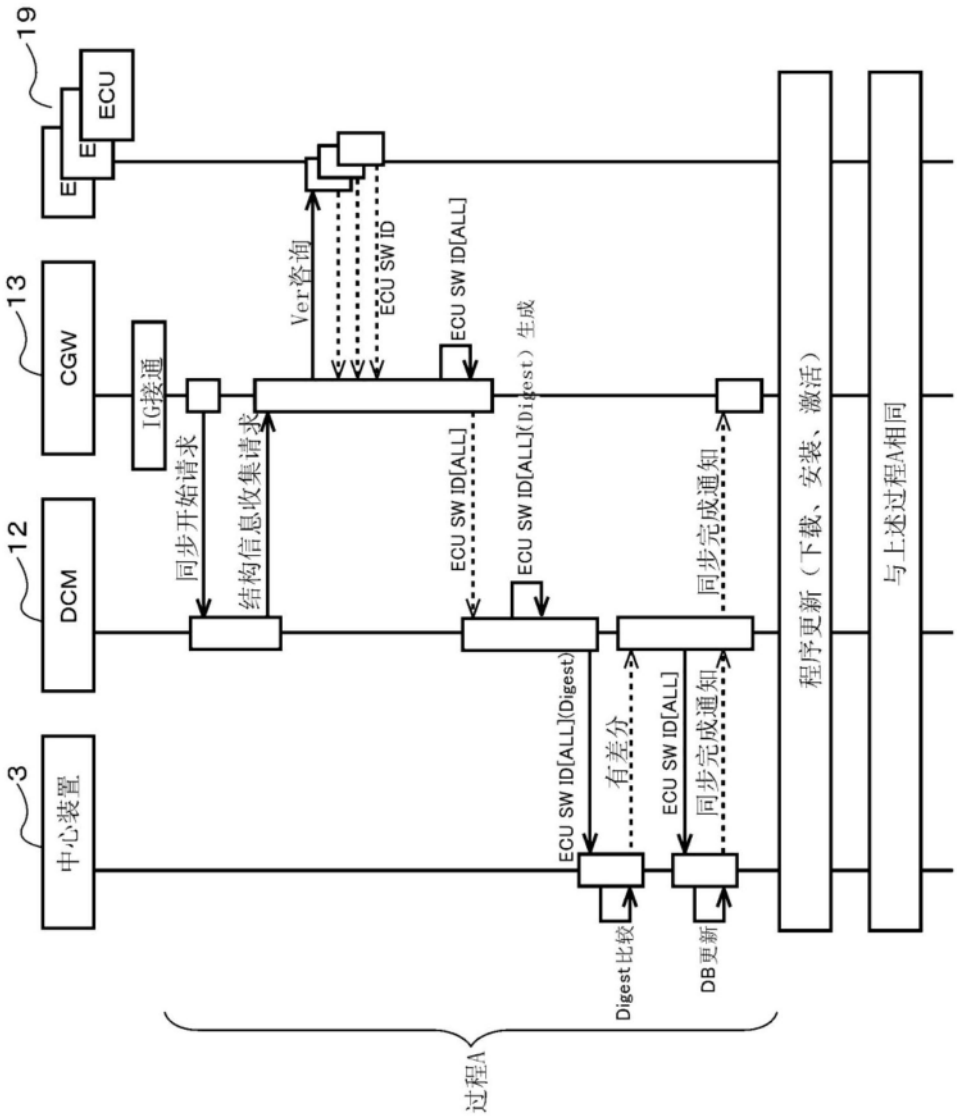

19
ECU
E
E
13
CGW
IG接通
12
DCM
3
中心装置
Ver咨询
ECU SW ID
ECU SW ID[ALL]
同步开始请求
结构信息收集请求
ECU SW ID[ALL]
ECU SW ID[ALL](Digest)生成
同步完成通知
ECU SW ID[ALL](Digest)
有差分
ECU SW ID[ALL]
同步完成通知
Digest比较
DB更新
程序更新（下载、安装、激活）
与上述过程A相同
过程A

图254

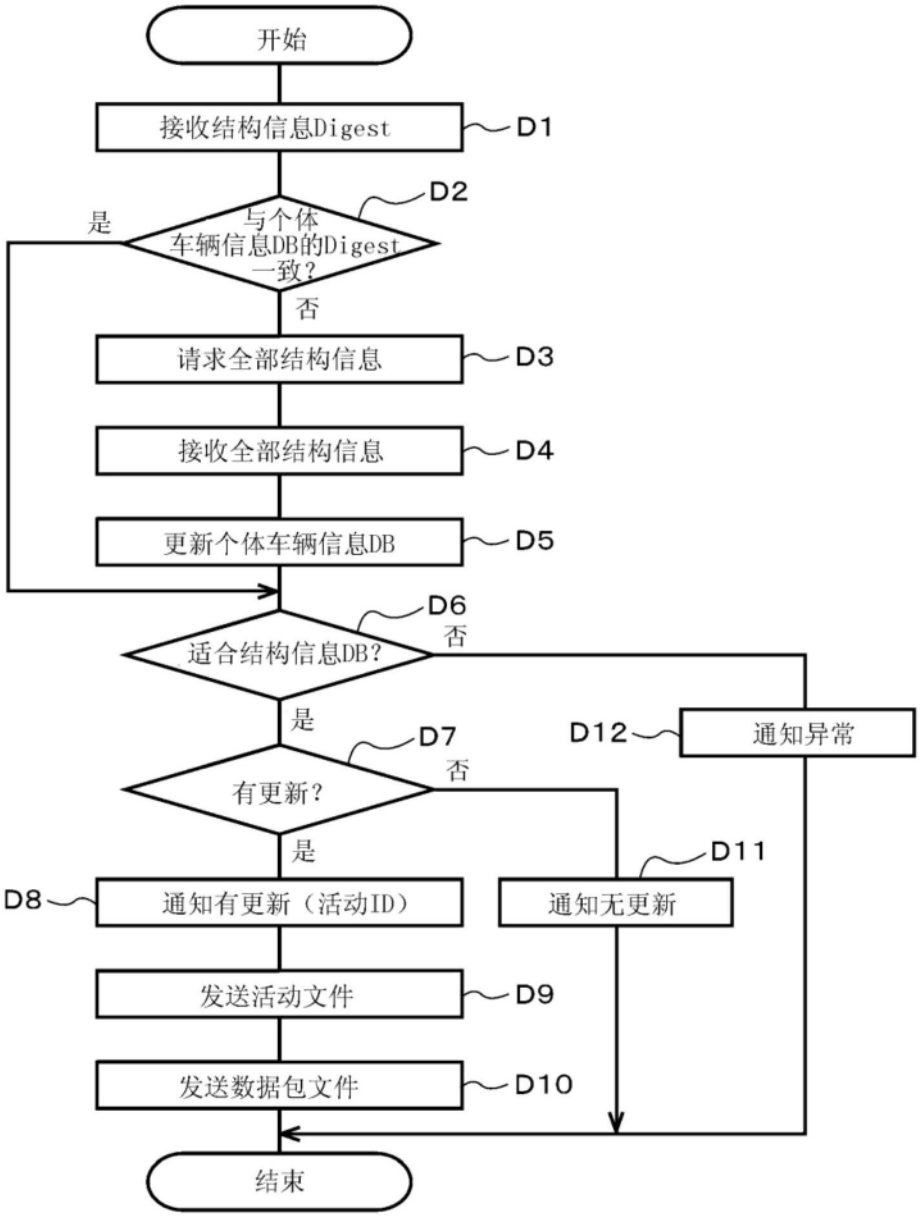

开始
接收结构信息Digest
D1
D2
是
与个体车辆信息DB的Digest一致？
否
请求全部结构信息
D3
接收全部结构信息
D4
更新个体车辆信息DB
D5
D6
适合结构信息DB？
否
是
D12
通知异常
D7
有更新？
否
是
D11
D8
通知有更新（活动ID）
通知无更新
发送活动文件
D9
发送数据包文件
D10
结束

图255

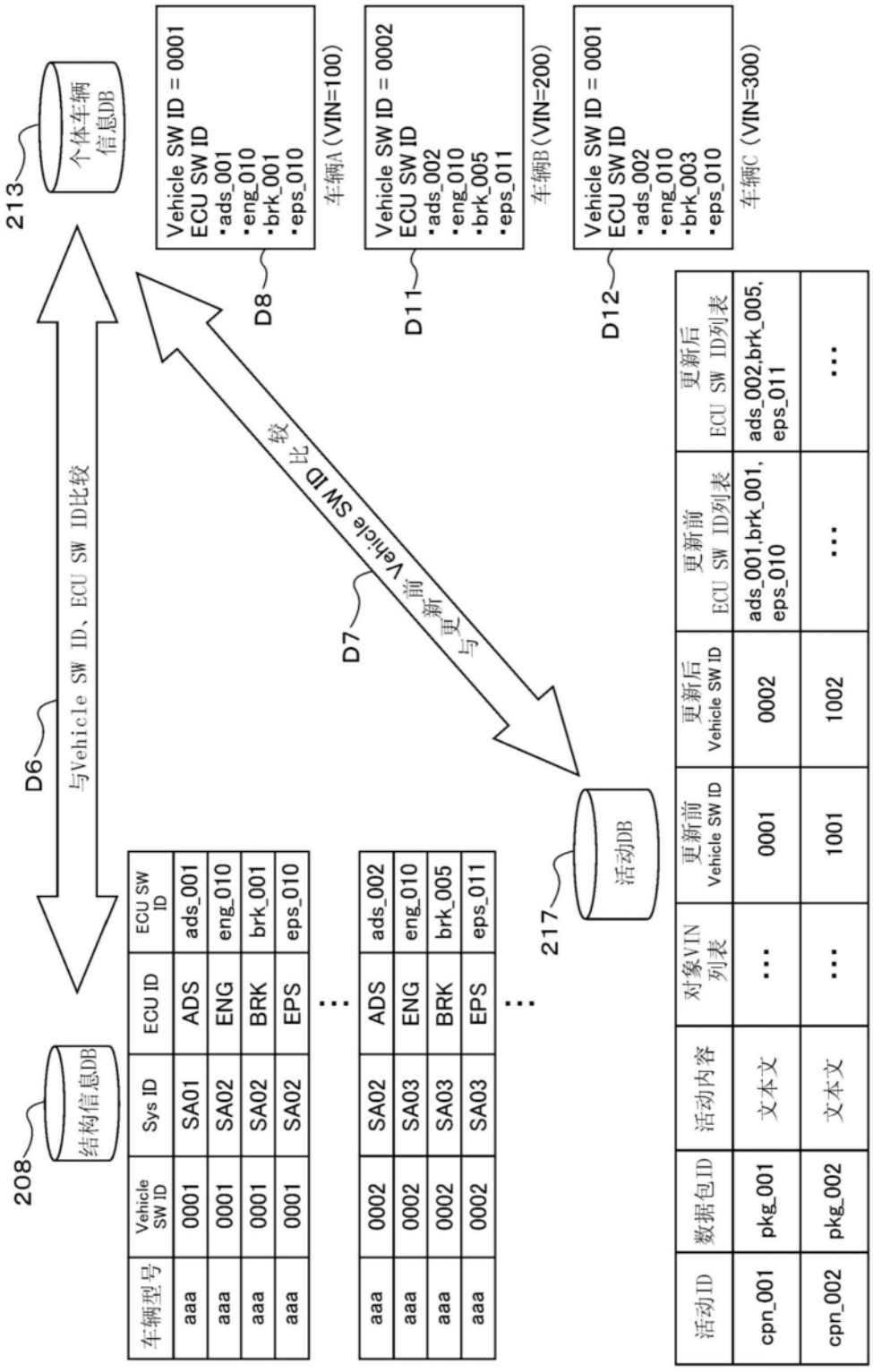

208
结构信息DB
213
个体车辆信息DB
D6
与Vehicle SW ID、ECU SW ID比较
D7
Vehicle SW ID 与前更新比较
D8
车辆A(VIN=100)
Vehicle SW ID = 0001
ECU SW ID
·ads_001
·eng_010
·brk_001
·eps_010
D11
车辆B(VIN=200)
Vehicle SW ID = 0002
ECU SW ID
·ads_002
·eng_010
·brk_005
·eps_011
D12
车辆C(VIN=300)
Vehicle SW ID = 0001
ECU SW ID
·ads_002
·eng_010
·brk_003
·eps_010
217
活动DB
车辆型号 | Vehicle SW ID | Sys ID | ECU ID | ECU SW ID
aaa | 0001 | SA01 | ADS | ads_001
aaa | 0001 | SA02 | ENG | eng_010
aaa | 0001 | SA02 | BRK | brk_001
aaa | 0001 | SA02 | EPS | eps_010
aaa | 0002 | SA02 | ADS | ads_002
aaa | 0002 | SA03 | ENG | eng_010
aaa | 0002 | SA03 | BRK | brk_005
aaa | 0002 | SA03 | EPS | eps_011
活动ID | 数据包ID | 活动内容 | 对象VIN列表 | 更新前 Vehicle SW ID | 更新后 Vehicle SW ID | 更新前 ECU SW ID列表 | 更新后 ECU SW ID列表
cpn_001 | pkg_001 | 文本文 | ... | 0001 | 0002 | ads_001,brk_001, eps_010 | ads_002,brk_005, eps_011
cpn_002 | pkg_002 | 文本文 | ... | 1001 | 1002 | ... | ...

图256

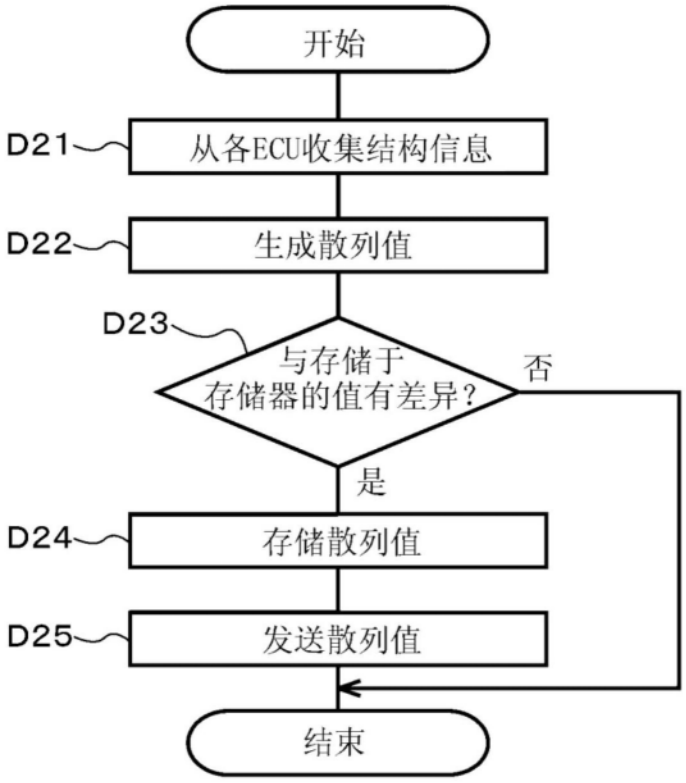

开始
D21
从各ECU收集结构信息
D22
生成散列值
D23
与存储于
存储器的值有差异?
否
是
D24
存储散列值
D25
发送散列值
结束

图257

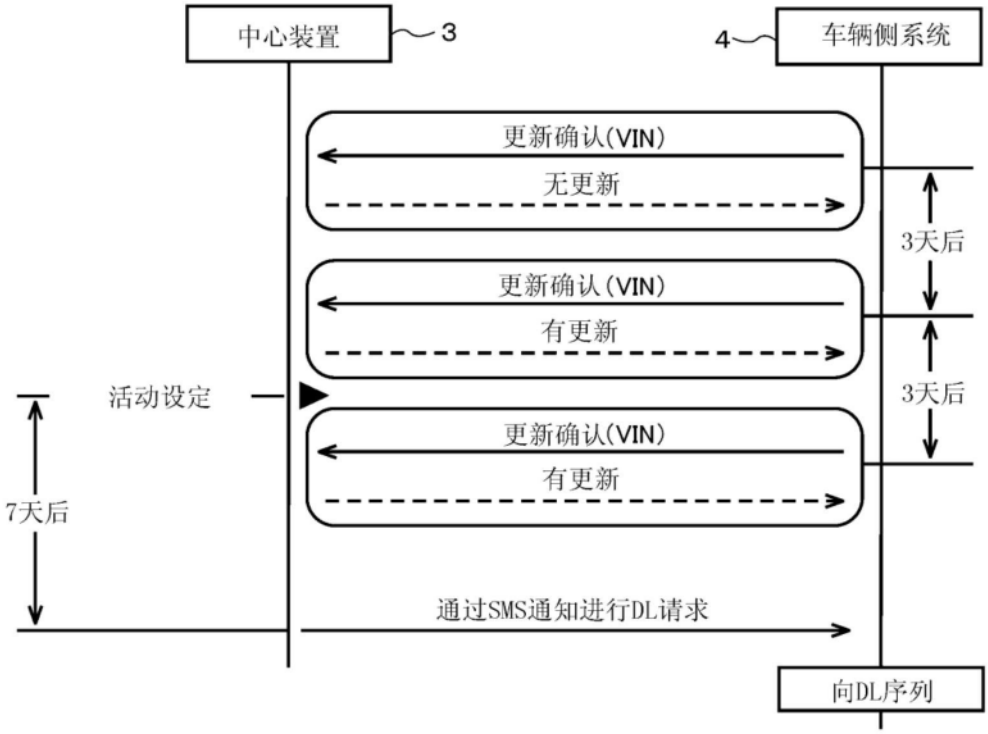

中心装置
3
4
车辆侧系统
更新确认(VIN)
无更新
3天后
更新确认(VIN)
有更新
活动设定
3天后
更新确认(VIN)
有更新
7天后
通过SMS通知进行DL请求
向DL序列

图258

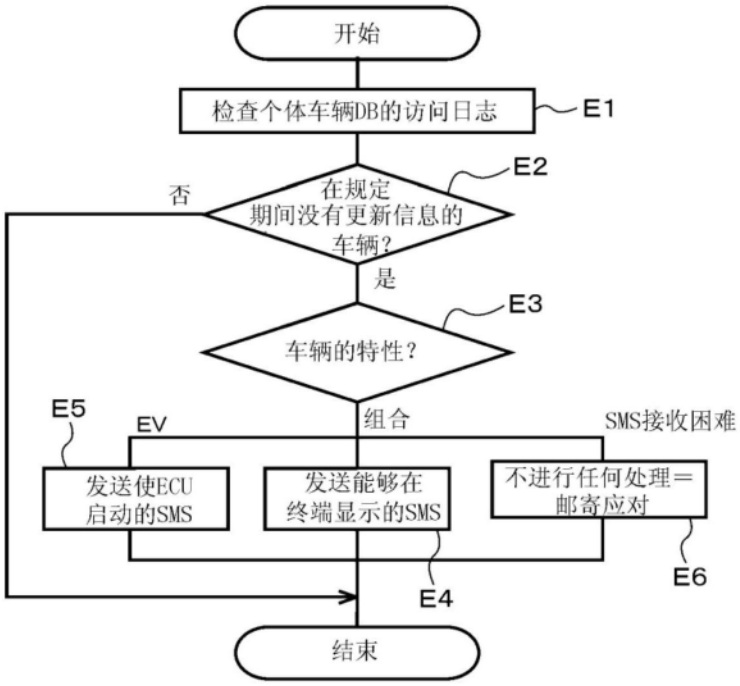

开始
检查个体车辆DB的访问日志
E1
在规定期间没有更新信息的车辆？
E2
否
是
车辆的特性？
E3
组合
EV
SMS接收困难
E5
发送使ECU启动的SMS
发送能够在终端显示的SMS
不进行任何处理＝邮寄应对
E6
E4
结束

图259

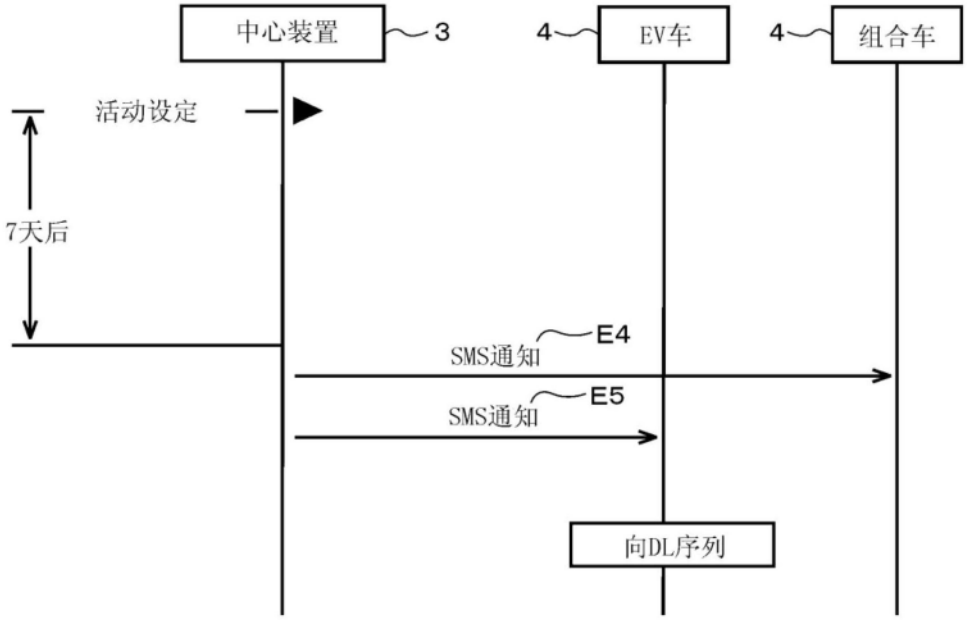

中心装置
3
4
EV车
4
组合车
活动设定
7天后
E4
SMS通知
E5
SMS通知
向DL序列

图260

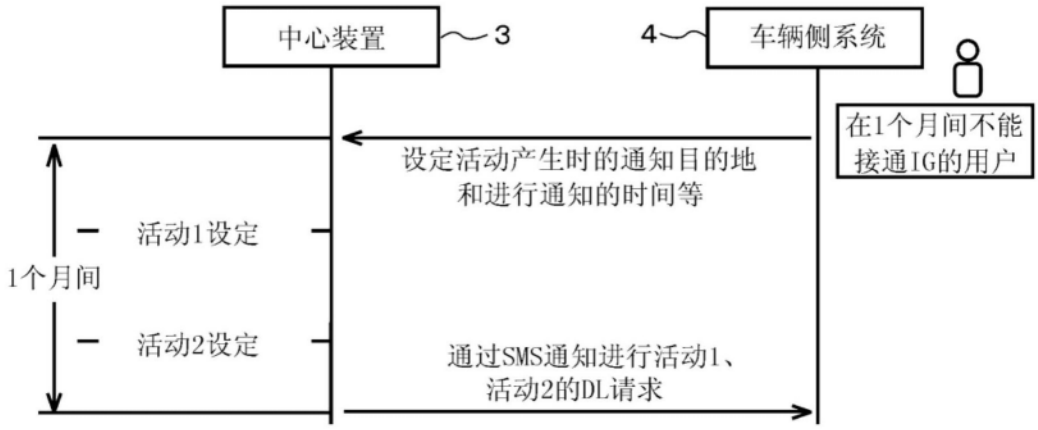

中心装置
3
4
车辆侧系统
在1个月间不能
接通IG的用户
设定活动产生时的通知目的地
和进行通知的时间等
活动1设定
1个月间
活动2设定
通过SMS通知进行活动1、
活动2的DL请求

图261

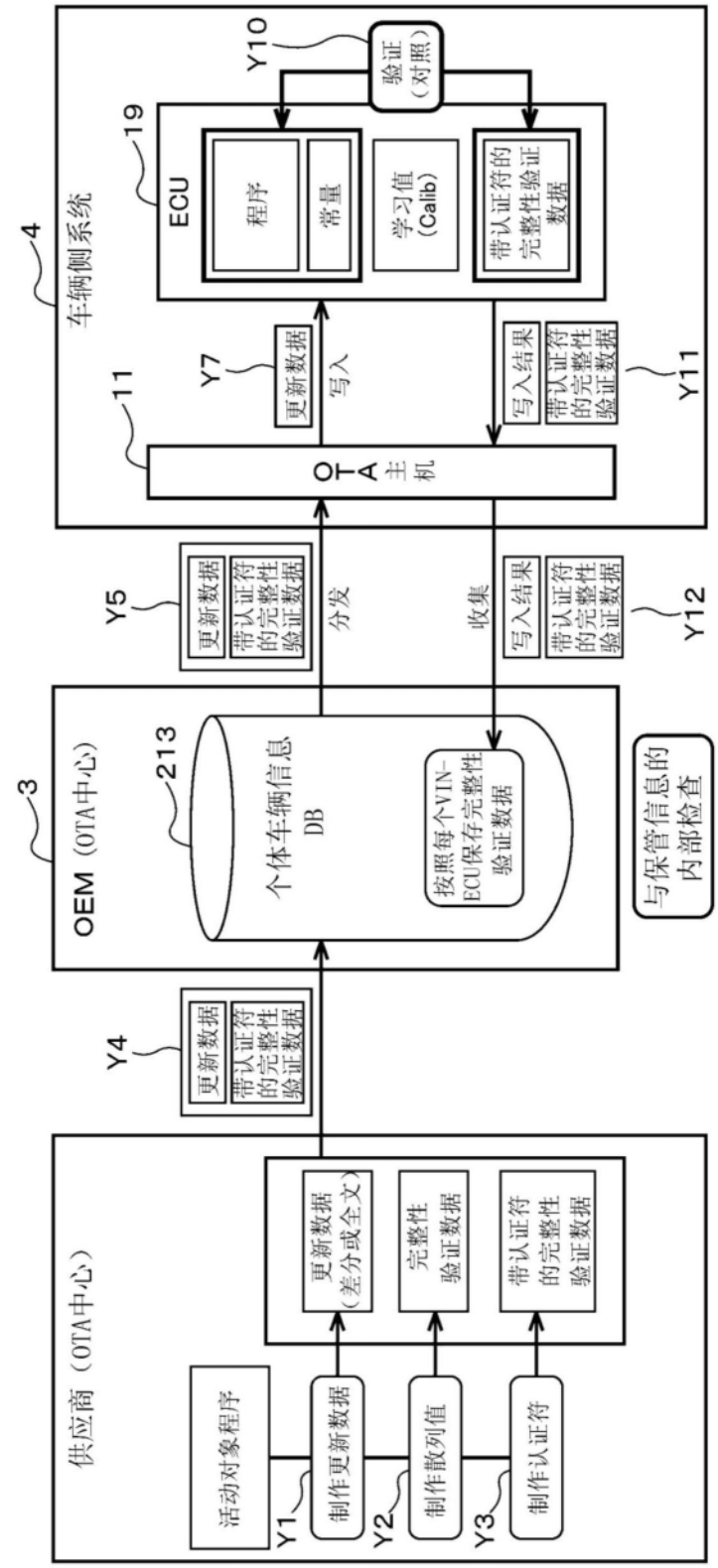

供应商（OTA中心）
活动对象程序
制作更新数据
制作散列值
制作认证符
Y1
Y2
Y3
更新数据（差分或全文）
完整性验证数据
带认证符的完整性验证数据
Y4
更新数据
带认证符的完整性验证数据
3
OEM（OTA中心）
213
个体车辆信息DB
按照每个VIN-ECU保存完整性验证数据
与保管信息的内部检查
Y5
更新数据
带认证符的完整性验证数据
分发
收集
写入结果
带认证符的完整性验证数据
Y12
4
车辆侧系统
11
OTA主机
Y7
更新数据
写入
写入结果
带认证符的完整性验证数据
Y11
19
ECU
程序
常量
学习值（Calib）
带认证符的完整性验证数据
Y10
验证（对照）

图262

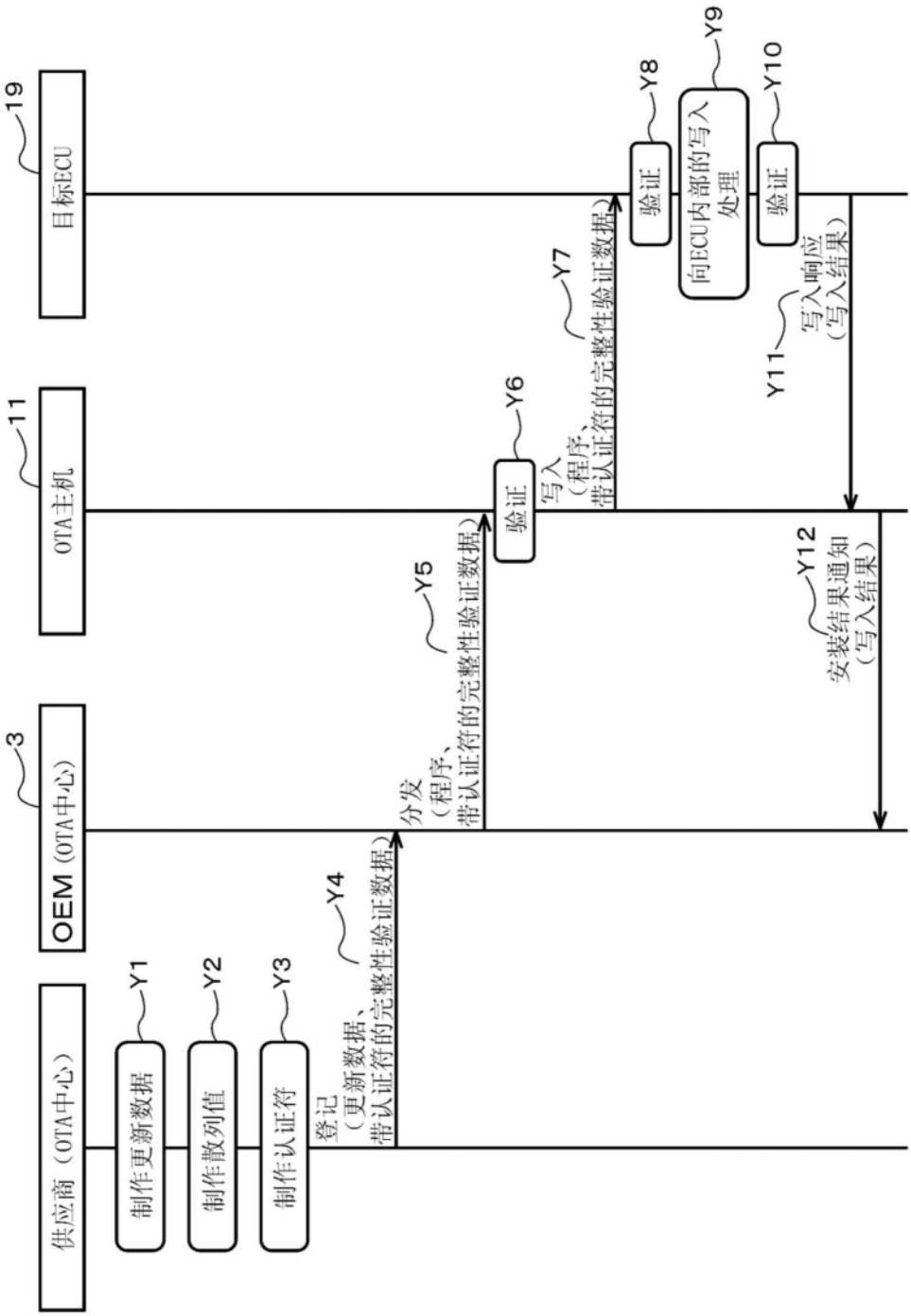

供应商（OTA中心）
OEM（OTA中心）
OTA主机
目标ECU
3
11
19
制作更新数据
制作散列值
制作认证符
Y1
Y2
Y3
登记
（更新数据、
带认证符的完整性验证数据）
Y4
分发
（程序、
带认证符的完整性验证数据）
Y5
验证
写入
（程序、
带认证符的完整性验证数据）
Y6
Y7
验证
向ECU内部的写入
处理
Y8
Y9
验证
Y10
写入响应
（写入结果）
Y11
安装结果通知
（写入结果）
Y12

图263

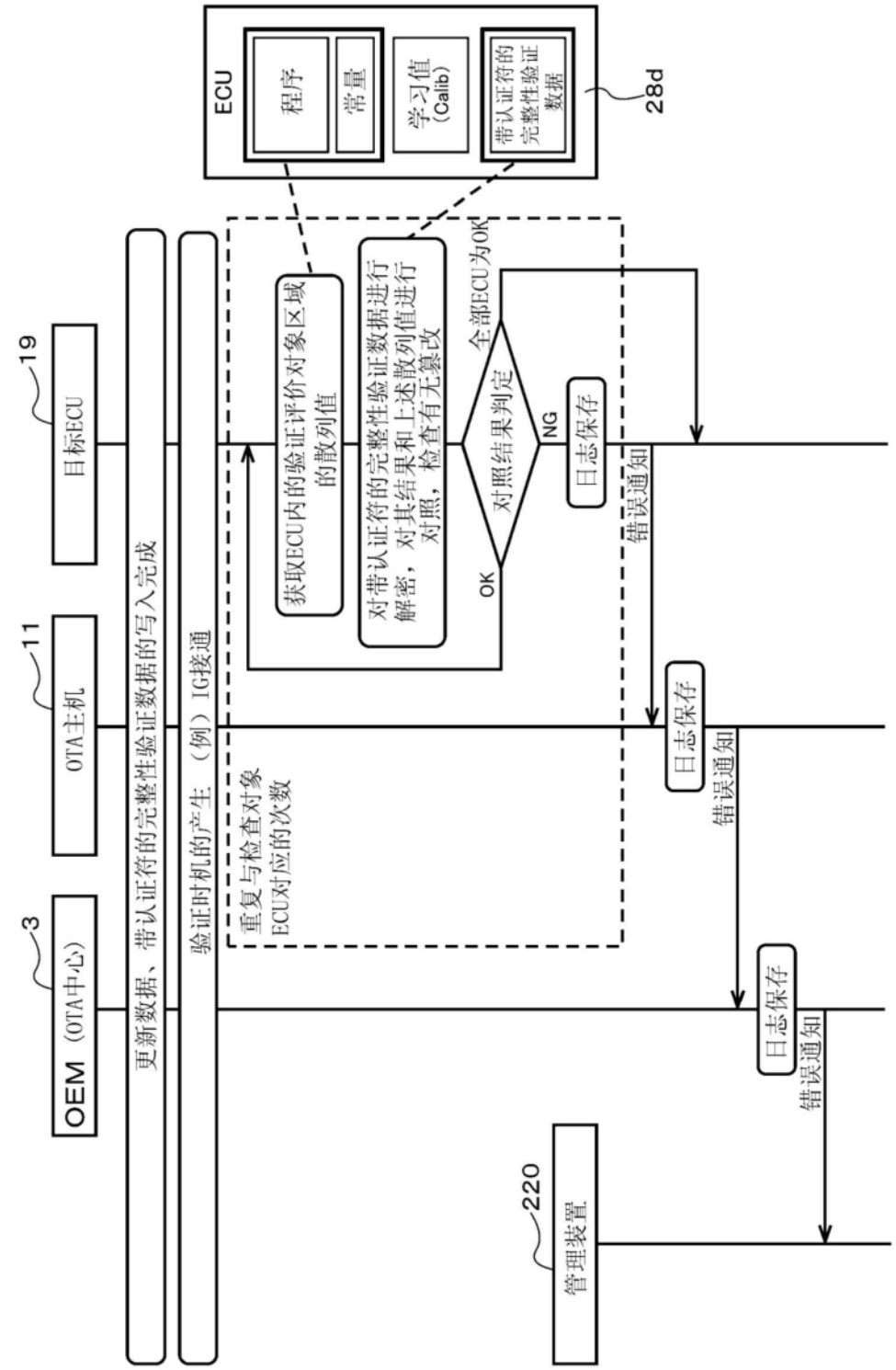

ECU
程序
常量
学习值
(Calib)
带认证符的
完整性验证
数据
28d
19
目标ECU
11
OTA主机
3
OEM（OTA中心）
更新数据、带认证符的完整性验证数据的写入完成
验证时机的产生（例）IG接通
重复与检查对象
ECU对应的次数
获取ECU内的验证评价对象区域
的散列值
对带认证符的完整性验证数据进行
解密，对其结果和上述散列值进行
对照，检查有无篡改
对照结果判定
OK
NG
全部ECU为OK
日志保存
错误通知
日志保存
错误通知
日志保存
错误通知
220
管理装置

图264

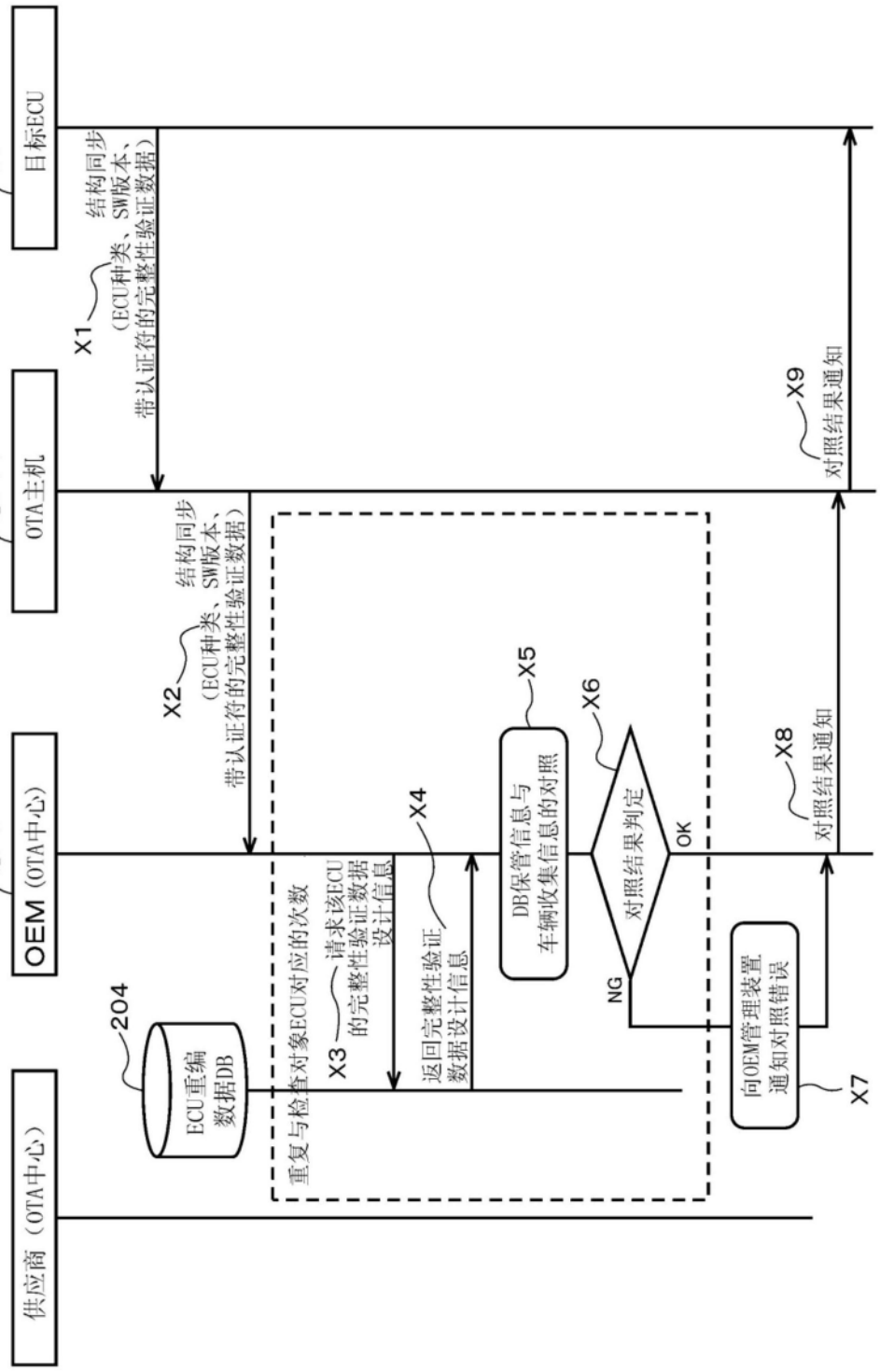
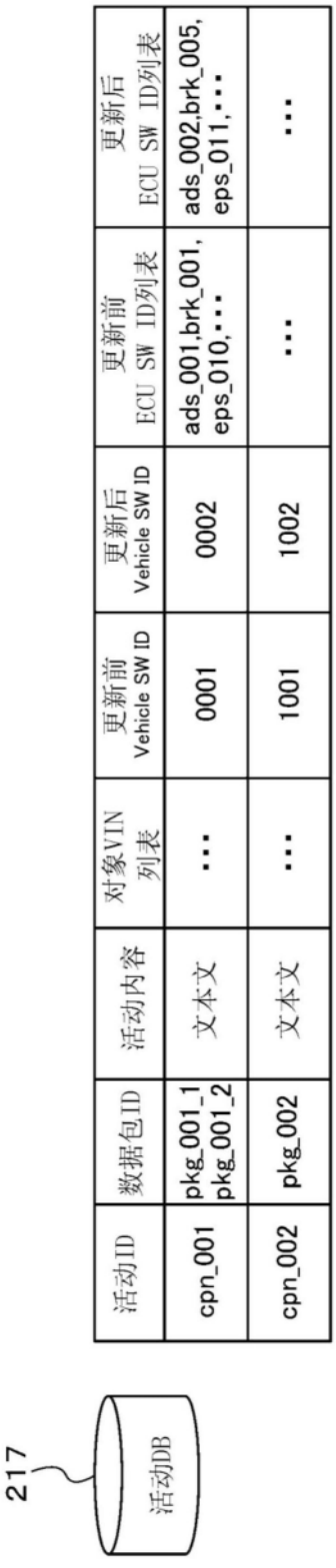

供应商（OTA中心）
OEM（OTA中心）
3
OTA主机
11
目标ECU
19
204
ECU重编
数据DB
重复与检查对象ECU对应的次数
X1
（ECU种类、SW版本、
带认证符的完整性验证数据）
结构同步
X2
（ECU种类、SW版本、
带认证符的完整性验证数据）
结构同步
X3
请求该ECU
的完整性验证数据
设计信息
X4
返回完整性验证
数据设计信息
X5
DB保管信息与
车辆收集信息的对照
X6
对照结果判定
NG
OK
X7
向OEM管理装置
通知对照错误
X8
对照结果通知
X9
对照结果通知

图265



数据包ID	文件	完整性验证数据
pkg_001_1	pkg001_1.dat	xx1_1.dat
pkg_001_2	pkg001_2.dat	xx1_2.dat
pkg_002	pkg002.dat	xx2.dat

图266



活动ID	数据包ID	活动内容	对象VIN列表	更新前 Vehicle SW ID	更新后 Vehicle SW ID	更新前 ECU SW ID列表	更新后 ECU SW ID列表
cpn_001	pkg_001_1 pkg_001_2	文本文	...	0001	0002	ads_001,brk_001, eps_010,...	ads_002,brk_005, eps_011,...
cpn_002	pkg_002	文本文	...	1001	1002	...	...

图267

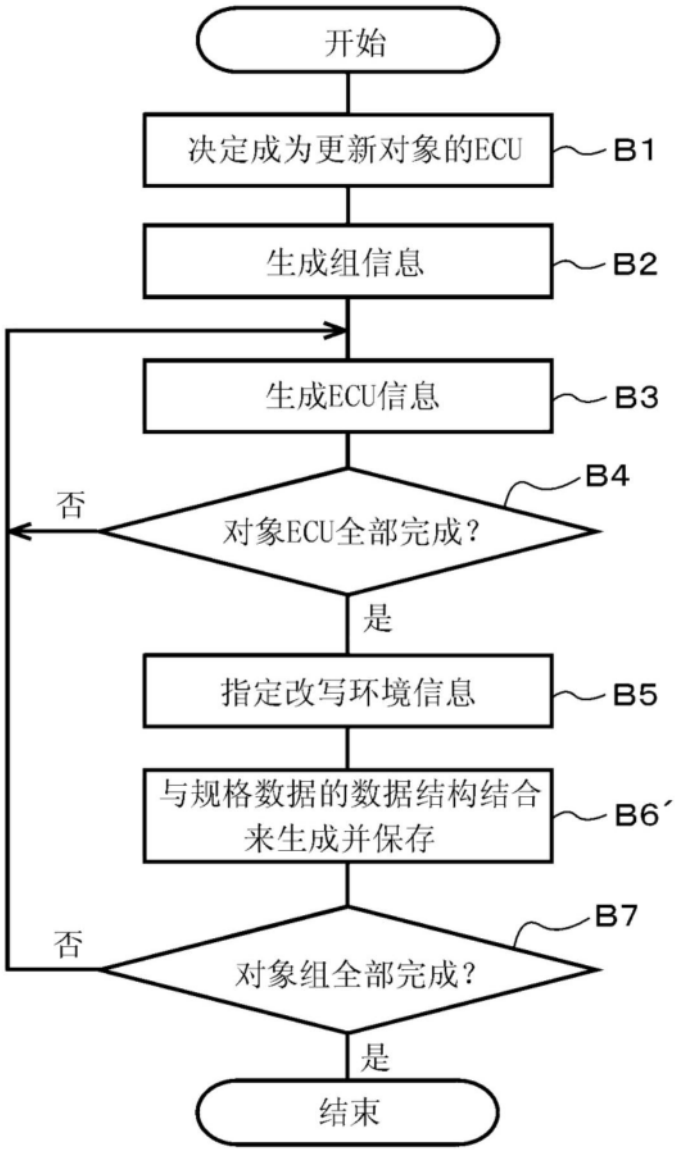

开始
决定成为更新对象的ECU
B1
生成组信息
B2
生成ECU信息
B3
B4
否
对象ECU全部完成？
是
指定改写环境信息
B5
与规格数据的数据结构结合来生成并保存
B6´
B7
否
对象组全部完成？
是
结束

图268

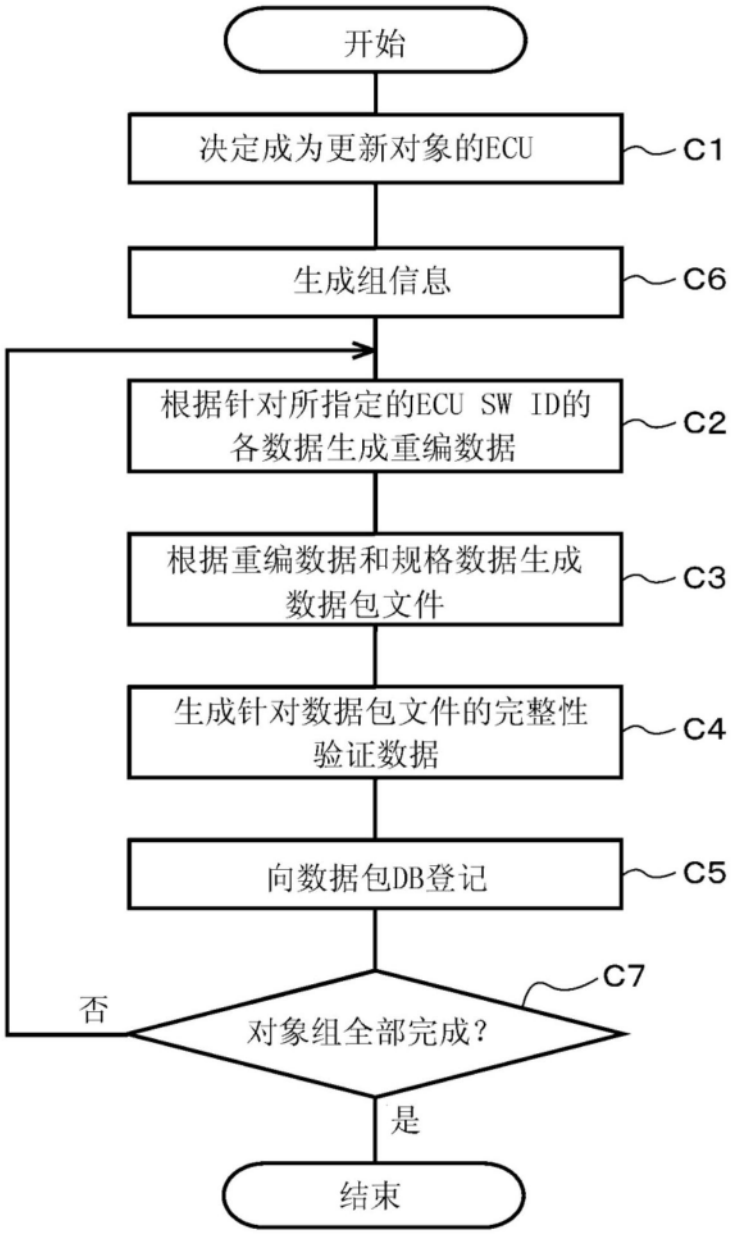

开始
决定成为更新对象的ECU
C1
生成组信息
C6
根据针对所指定的ECU SW ID的各数据生成重编数据
C2
根据重编数据和规格数据生成数据包文件
C3
生成针对数据包文件的完整性验证数据
C4
向数据包DB登记
C5
C7
否
对象组全部完成？
是
结束

图269

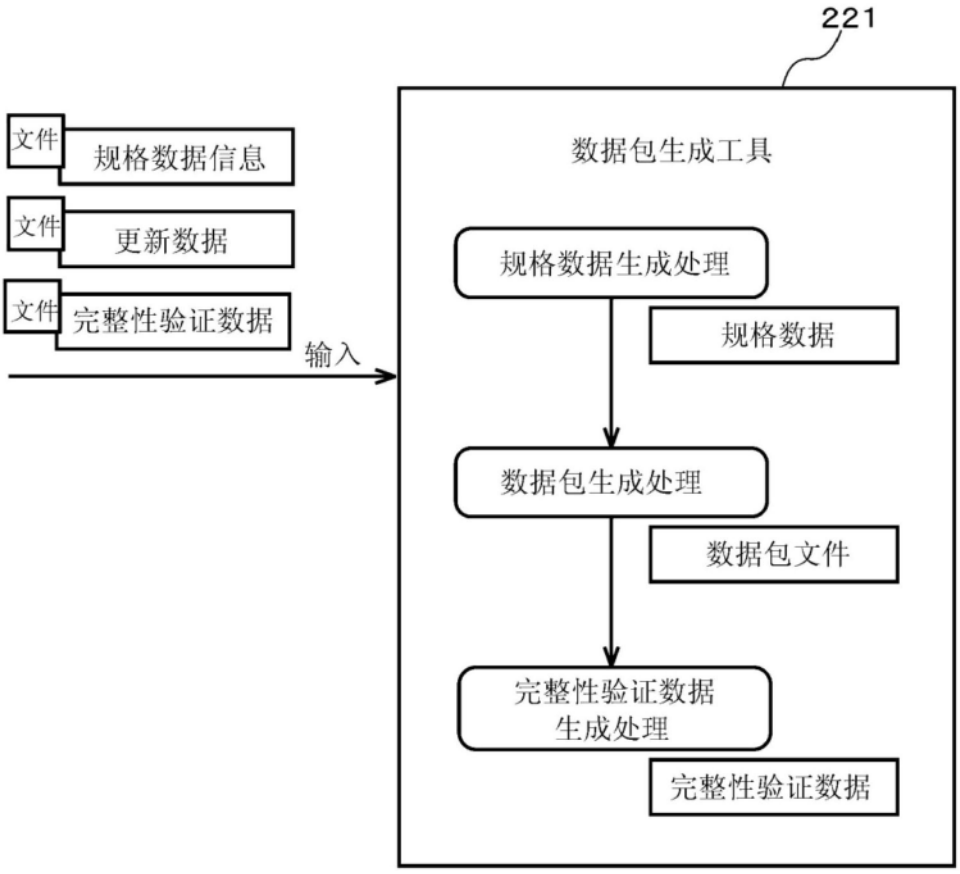

221
文件
规格数据信息
文件
更新数据
文件
完整性验证数据
输入
数据包生成工具
规格数据生成处理
规格数据
数据包生成处理
数据包文件
完整性验证数据
生成处理
完整性验证数据

图270