(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113453959 B
(45)授权公告日 2024.06.21

(21)申请号 202080014751.2
(22)申请日 2020.02.27
(65)同一申请的已公布的文献号
申请公布号 CN 113453959 A
(43)申请公布日 2021.09.28
(30)优先权数据
2019-038882 2019.03.04 JP
(85)PCT国际申请进入国家阶段日
2021.08.16
(86)PCT国际申请的申请数据
PCT/JP2020/007925 2020.02.27
(87)PCT国际申请的公布数据
WO2020/179592 JA 2020.09.10
(73)专利权人 株式会社自动网络技术研究所
地址 日本三重县
专利权人 住友电装株式会社
住友电气工业株式会社
(72)发明人 小林拓也
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
专利代理师 熊传芳 苏卉
(51)Int.Cl.
B60R 16/02(2006.01)
G06F 8/65(2006.01)
G06F 13/00(2006.01)
(56)对比文件
JP 2007011734 A,2007.01.18
JP 2011003020 A,2011.01.06
审查员 曹巧双

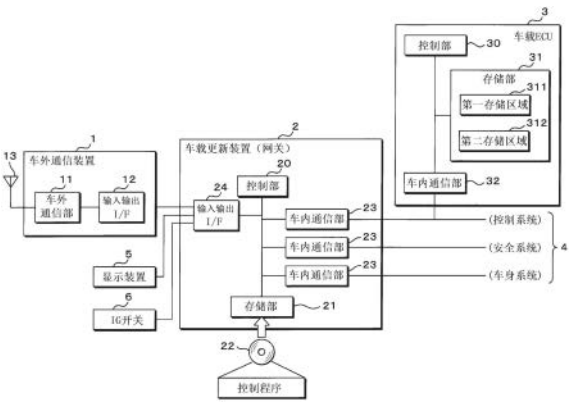
权利要求书2页 说明书9页 附图4页

(54)发明名称

车载更新装置、更新处理程序及程序的更新方法

(57)摘要

车载更新装置取得从车外的外部服务器发送的更新程序,并进行用于对搭载于车辆的车载控制装置的程序进行更新的处理,车载更新装置具备存储部和控制部,在上述存储部中存储有所取得的上述更新程序,上述控制部控制所取得的上述更新程序向上述车载控制装置的发送,上述控制部根据上述车辆的停止而中断上述发送,对基于上述中断的前后存储在上述存储部中的上述更新程序而导出的各导出值进行比较,基于比较结果来对存储在上述存储部中的上述更新程序的正当性进行判定。



CN 113453959 B

1.一种车载更新装置,取得从车外的外部服务器发送的更新程序,并进行用于对搭载于车辆的车载控制装置的程序进行更新的处理,

所述车载更新装置具备存储部和控制部,

在所述存储部中存储有所取得的所述更新程序,

所述控制部控制所取得的所述更新程序向所述车载控制装置的发送,

所述控制部根据所述车辆的停止而中断所述发送,

所述控制部对基于所述中断的前后存储在所述存储部中的所述更新程序而导出的各导出值进行比较,

所述控制部基于比较结果,来对在所述中断的期间存在存储在所述存储部中的所述更新程序被变更而成为不正当的程序的可能性进行判定。

2.根据权利要求1所述的车载更新装置,其中,

在所述中断的前后的各所述导出值不同的情况下,

所述控制部判定为存储在所述存储部中的所述更新程序不正当,

从所述外部服务器从头取得所述更新程序。

3.根据权利要求1所述的车载更新装置,其中,

在所述中断的前后的各所述导出值相同的情况下,

所述控制部判定为存储在所述存储部中的所述更新程序正当,

从中断点重新开始所述发送。

4.根据权利要求2所述的车载更新装置,其中,

在所述中断的前后的各所述导出值相同的情况下,

所述控制部判定为存储在所述存储部中的所述更新程序正当,

从中断点重新开始所述发送。

5.根据权利要求3所述的车载更新装置,其中,

所述中断点基于取得的所述更新程序中包含的检查点而导出。

6.根据权利要求4所述的车载更新装置,其中,

所述中断点基于取得的所述更新程序中包含的检查点而导出。

7.根据权利要求1至6中的任一项所述的车载更新装置,其中,

在所述更新程序被发送到所述车载控制装置之后,所述控制部从所述存储部中删除存储在所述存储部中的所述更新程序。

8.一种计算机程序产品,包括计算机程序,其特征在于,该计算机程序使计算机执行如下的处理:

取得从车外的外部服务器发送的更新程序,

将所取得的该更新程序存储到存储部中,

向车载控制装置发送所述更新程序,

对基于所述发送中断的前后存储在所述存储部中的所述更新程序而导出的各导出值进行比较,

基于比较结果,来对在所述中断的期间存在存储在所述存储部中的所述更新程序被变更而成为不正当的程序的可能性进行判定。

9.一种程序的更新方法,

取得从车外的外部服务器发送的更新程序，

将所取得的该更新程序存储到存储部中，

向车载控制装置发送所述更新程序，

对基于所述发送中断的前后存储在所述存储部中的所述更新程序而导出的各导出值进行比较，

基于比较结果，来对在所述中断的期间存在存储在所述存储部中的所述更新程序被变更而成为不正当的程序的可能性进行判定。

车载更新装置、更新处理程序及程序的更新方法

技术领域

[0001] 本公开涉及一种车载更新装置、更新处理程序及程序的更新方法。

[0002] 本申请要求基于2019年3月4日提出申请的日本申请第2019-38882号的优先权,并援引上述日本申请所记载的全部记载内容。

背景技术

[0003] 在车辆中搭载有用于对发动机控制等动力传动系统、空调控制等车身系统的车载设备进行控制的车载控制装置,例如搭载有车载ECU(Electronic Control Unit:电子控制单元)。车载控制装置包含MPU(Micro Processing Unit:微处理单元)等运算处理部、RAM(Random Access Memory:随机存取存储器)等能够改写的非易失性的存储部及用于与其他车载控制装置进行通信的通信部,通过读取并执行在存储部中存储的控制程序来进行车载设备的控制。在车辆中还安装有具备无线通信的功能的中继装置(车载更新装置)。中继装置与连接于车外的网络的外部服务器等程序提供装置进行通信,并从该程序提供装置下载(接收)车载控制装置的控制程序。所下载的程序存储在中继装置的存储部中。将存储在存储部中的程序向该车载控制装置发送,来更新(reprogramming:重编程)该车载控制装置的控制程序。(参照专利文献1)

[0004] 现有技术文献

[0005] 专利文献1:日本特开2017-97851号公报

发明内容

[0006] 本公开的一个方式涉及一种车载更新装置,取得从车外的外部服务器发送的更新程序,并进行用于对搭载于车辆的车载控制装置的程序进行更新的处理,上述车载更新装置具备存储部和控制部,在上述存储部中存储有所取得的上述更新程序,上述控制部控制所取得的上述更新程序向上述车载控制装置的发送,上述控制部根据上述车辆的停止而中断上述发送,上述控制部对基于上述中断的前后存储在上述存储部中的上述更新程序而导出的各导出值进行比较,上述控制部基于比较结果来对存储在上述存储部中的上述更新程序的正当性进行判定。

附图说明

[0007] 图1是表示实施方式1涉及的车载更新系统的结构的示意图。

[0008] 图2是表示实施方式1涉及的车载更新装置等的结构的框图。

[0009] 图3是例示车载更新装置的控制部的处理的流程图。

[0010] 图4是表示在程序提供装置、车载更新装置及车载控制装置之间收发的通信信号及更新程序的时序图。

具体实施方式

[0011] [本公开要解决的课题]

[0012] 在车载更新装置从外部服务器取得程序并将程序发送到作为重编程对象的车载控制装置为止的期间内重编程中断时,在中断的期间存在存储在车载更新装置的存储部中的程序被篡改而成为不正当的程序的可能性。但是,专利文献1未考虑与发生了上述中断的情况下的存储在车载更新装置的存储部中的程序的正当性相关的问题。

[0013] 本公开鉴于上述情形而作出,其目的在于,提供一种能够确保存储在车载更新装置的存储部中的程序的正当性的车载更新装置等。

[0014] [本公开的效果]

[0015] 根据本公开的一个方式,能够提供一种能够确保存储在车载更新装置的存储部中的程序的正当性的车载更新装置。

[0016] [本公开的实施方式的说明]

[0017] 首先,列举本公开的实施方式来进行说明。另外,也可以任意地组合以下记载的实施方式中的至少一部分。

[0018] (1)本公开的一个方式涉及一种车载更新装置,取得从车外的外部服务器发送的更新程序,并进行用于对搭载于车辆的车载控制装置的程序进行更新的处理,上述车载更新装置具备存储部和控制部,在上述存储部中存储有所取得的上述更新程序,上述控制部控制所取得的上述更新程序向上述车载控制装置的发送,上述控制部根据上述车辆的停止而中断上述发送,上述控制部对基于上述中断的前后存储在上述存储部中的上述更新程序而导出的各导出值进行比较,上述控制部基于比较结果来对存储在上述存储部中的上述更新程序的正当性进行判定。

[0019] 在本方式中,当存储在存储部中的更新程序向车载控制装置的发送在中断之后重新开始时,控制部对存储在存储部中的更新程序的正当性进行判定。因此,能够在重新开始上述发送时确保存储在存储部中的更新程序的正当性。例如,能够确保在中断的期间内更新程序未变更为不正当。

[0020] (2)本公开的一个方式涉及的车载更新装置中,在上述中断的前后的各上述导出值不同的情况下,上述控制部判定为存储在上述存储部中的上述更新程序不正当,从上述外部服务器从头取得上述更新程序。

[0021] 在本方式中,控制部在判定为存储在存储部中的更新程序不正当的情况下,从外部服务器从头取得更新程序而重新开始车载控制装置的更新。因此,能够防止不正当的更新程序向车载控制装置的发送。

[0022] (3)本公开的一个方式涉及的车载更新装置中,在上述中断的前后的各上述导出值相同的情况下,上述控制部判定为存储在上述存储部中的上述更新程序正当,从中断点重新开始上述发送。

[0023] 在本方式中,控制部在将存储在存储部中的更新程序判断为正当的情况下,使用存储在存储部中的更新程序来重新开始车载控制装置的更新。因此,在确保了存储在存储部中的更新程序的适当性的基础上无需再次取得更新程序,能够减少用于取得的通信成本及处理时间。

[0024] (4)本公开的一个方式涉及的车载更新装置中,上述中断点基于取得的上述更新

程序中包含的检查点而导出。

[0025] 在本方式中,从根据更新程序中包含的检查点而导出的中断点重新开始车载控制装置的更新。因此,高效地重新开始更新。

[0026] (5)本公开的一个方式涉及的车载更新装置中,在上述更新程序被发送到上述车载控制装置之后,上述控制部从上述存储部中删除存储在上述存储部中的上述更新程序。

[0027] 在本方式中,在更新程序被发送到车载控制装置之后删除存储在存储部中的更新程序,因此能够防止存储部被更新程序压缩空间。

[0028] (6)本公开的一个方式涉及一种更新处理程序,使计算机执行如下的处理:取得从车外的外部服务器发送的更新程序,将所取得的该更新程序存储到存储部中,向车载控制装置发送上述更新程序,对基于上述发送中断的前后存储在上述存储部中的上述更新程序而导出的各导出值进行比较,基于比较结果来对存储在上述存储部中的上述更新程序的正当性进行判定。

[0029] 在本方式中,能够使计算机作为本公开的一个方式的车载更新装置发挥功能。

[0030] (7)本公开的一个方式涉及一种程序的更新方法,取得从车外的外部服务器发送的更新程序,将所取得的该更新程序存储到存储部中,向车载控制装置发送上述更新程序,对基于上述发送中断的前后存储在上述存储部中的上述更新程序而导出的各导出值进行比较,基于比较结果来对存储在上述存储部中的上述更新程序的正当性进行判定。

[0031] 在本方式中,当存储在存储部中的更新程序向车载控制装置的发送中断之后重新开始时,对存储在存储部中的更新程序的正当性进行判定。因此,能够提供一种能够在重新开始上述发送时确保存储在存储部中的更新程序的正当性的程序的更新方法。

[0032] [本公开的实施方式的详情]

[0033] 关于本公开,基于表示其实施方式的附图来具体地进行说明。以下参照附图对本公开的实施方式涉及的车载更新装置2进行说明。另外,本公开不限于这些示例,而由权利要求书示出,意在包含与权利要求书等同含义及范围内的全部变更。

[0034] (实施方式1)

[0035] 以下,基于附图对实施方式进行说明。图1是表示实施方式1涉及的车载更新系统S的结构的示意图。图2是表示实施方式1涉及的车载更新装置2等的结构的框图。车载更新系统S包含搭载于车辆C的车外通信装置1及车载更新装置2,且向搭载于车辆C的车载控制装置3(车载ECU)发送从经由车外网络N连接的程序提供装置S1取得的程序或数据。

[0036] 程序提供装置S1是例如连接于因特网或公共线路网等车外网络N的服务器等计算机,具备基于RAM、ROM(Read Only Memory:只读存储器)或硬盘等的存储部S11,相当于车外的外部服务器。在程序提供装置S1的存储部S11中保存有由车载控制装置3的制造商等制作的用于控制该车载控制装置3的程序或数据。该程序或数据作为更新程序如后文所述地发送到车辆C,用于对搭载于车辆C车载控制装置3的程序或数据进行更新。这样构成的程序提供装置S1(外部服务器)也称为OTA(Over The Air:空中下载)服务器。搭载于车辆C的车载控制装置3取得通过无线通信从程序提供装置S1发送的更新程序,并将该更新程序作为执行的程序而应用,由此能够对自身控制装置执行的程序进行更新(重编程)。

[0037] 以下,程序作为包含如下的外部文件进行说明:记载有程序代码及在执行该程序代码时参照的数据,上述程序代码包含用于使车载控制装置3进行处理的控制语句等。在发

送更新程序时,记载有这些程序代码及数据的外部文件例如作为加密的档案文件从程序提供装置S1发送。

[0038] 在车辆C中搭载有:车外通信装置1、车载更新装置2、显示装置5、IG(点火)开关6及用于控制各种车载设备的多个车载控制装置3。车外通信装置1与车载更新装置2通过例如串行电缆等线束以能够通信的方式连接。车载更新装置2及车载控制装置3通过与CAN(Controller Area Network:控域网/注册商标)或EtherNet(注册商标)等通信协议对应的车内LAN4以能够通信的方式连接。

[0039] 车外通信装置1包含车外通信部11及用于与车载更新装置2进行通信的输入输出I/F(接口)12。车外通信部11是用于使用3G、LTE、4G、WiFi等移动体通信的协议来进行无线通信的通信装置,经由连接于车外通信部11的天线13而与程序提供装置S1进行数据的收发。车外通信装置1与程序提供装置S1之间的通信经由例如公共线路网或因特网等外部网络而进行。

[0040] 输入输出I/F12是用于车外通信装置1与车载更新装置2进行例如串行通信的通信接口。车外通信装置1与车载更新装置2经由与输入输出I/F12及车载更新装置2所具备的输入输出I/F24连接的串行电缆等线束而相互进行通信。在本实施方式中,车外通信装置1设为与车载更新装置2不同的装置,并通过输入输出I/F12等将这些装置以能够通信的方式连接,但不限于此。车外通信装置1也可以作为车载更新装置2的一个构成部位而内置在车载更新装置2中。

[0041] 车载更新装置2包含:控制部20、存储部21及车内通信部23。车载更新装置2构成为,从车外通信装置1取得车外通信装置1通过无线通信从程序提供装置S1接收到的更新程序,并经由车内LAN4而将该更新程序向预定(更新对象)的车载控制装置3发送。车载更新装置2是统括例如控制系统的车载控制装置3、安全系统的车载控制装置3及车身系统的车载控制装置3等多个系统的区段并对这些区段之间的车载控制装置3彼此的通信进行中继的网关(中继器)。或者,车载更新装置2也可以构成为对车辆C整体进行控制的车身ECU的一个功能部。

[0042] 控制部20由CPU(Central Processing Unit:中央处理单元)或MPU等构成,通过读取并执行预先存储在存储部21中的控制程序及数据来进行各种控制处理及运算处理等。控制部20经由车内通信部23而向车载控制装置3发送更新程序。控制部20基于存储在存储部21中的更新程序而导出导出值以及对导出的导出值进行比较来判定存储在存储部21中的更新程序的正当性。控制部20进行存储在存储部21中的更新程序的删除。

[0043] 存储部21由RAM等易失性存储器元件或ROM、EEPROM(Electrically Erasable Programmable ROM:电可擦可编程只读存储器)、闪存等非易失性的存储器元件构成,预先存储有控制程序及在处理时参照的数据。存储在存储部21中的控制程序可以存储有从车载更新装置2能够读取的记录介质22中读取的控制程序。另外,也可以是,从与未图示的通信网连接的未图示的外部计算机下载控制程序并使其存储在存储部21中。详情后述,但在存储部21中存储有用于将导出值导出的程序或数据,且存储有从程序提供装置S1取得的更新程序。

[0044] 车内通信部23是使用CAN(注册商标)或EtherNet(注册商标)等通信协议的输入输出接口,控制部20经由车内通信部23而与连接于车内LAN4的车载控制装置3或其他中继装

置等车载设备相互通信。车内通信部23设有多个(在附图上为三个),在车内通信部23分别连接有构成车内LAN4的通信线。通过这样设置多个车内通信部23,车内LAN4被分成多个区段,在各区段分别根据车载控制装置3的功能(控制系统功能、安全系统功能、车身系统功能)而连接该车载控制装置3。

[0045] 车载控制装置3包含:控制部30、存储部31及车内通信部32。存储部31由RAM等易失性存储器元件或ROM、EEPROM、闪存等非易失性存储器元件构成,存储有车载控制装置3的程序或数据。该程序或数据是由从车载更新装置2发送的更新程序更新的对象。

[0046] 存储部31包含第一存储区域(第一面)311及第二存储区域(第二面)312。在存储部31中存储有在现状下车载控制装置3执行(应用)的程序(当前版本)及在当前版本以前引用的程序(旧版本)这两个程序。这些当前版本的程序和旧版本的程序被分配并存储在第一存储区域311与第二存储区域312中的某一个存储区域中。即,在第一存储区域311中存储当前版本的程序的情况下,在第二存储区域312中存储旧版本的程序。在第一存储区域311中存储旧版本的程序的情况下,在第二存储区域312中存储当前版本的程序。这样,通过将当前版本及旧版本这两个程序存储为所谓的双面存储,在万一当前版本的程序发生了问题的情况下,控制部30也能够通过读取并执行(切换)以前应用过并正常地动作的旧版本的程序来确保车载控制装置3的可靠性。

[0047] 在存储部31中存储有与当前版本及旧版本这两个程序各自的版本相关的信息及与存储有当前执行(应用)的程序的区域(动作面)相关的信息。即,在现状下执行存储在第一存储区域(第一面)311中的程序的情况下,在存储部31中存储成动作面为第一存储区域(第一面)311。在现状下执行存储在第二存储区域(第二面)312中的程序的情况下,在存储部31中存储成动作面为第二存储区域(第二面)312。在存储部31中存储有与程序(当前版本及旧版本)的版本信息及动作面相关的信息。

[0048] 控制部30由CPU或MPU等构成,读取并执行存储在存储部31(动作面)中的程序及数据来进行控制处理等,控制包含该车载控制装置3的车载设备或促动器等。

[0049] 车载控制装置3的控制部30经由车内通信部32而接收从车载更新装置2发送的更新程序,取得该更新程序。因此,车载控制装置3的控制部30经由车外通信装置1及车载更新装置2而取得从程序提供装置S1发送的更新程序。控制部30将取得的更新程序存储在非动作面的存储区域(第一存储区域311或第二存储区域312)中。即,控制部30在取得从车载更新装置2发送的更新程序时,作为该取得的准备处理而删除存储在不是动作面的存储区域(非动作面)中的程序。通常,存储在不是动作面的存储区域中的程序为在当前版本的程序以前执行的旧版本的程序,因此,控制部30在不使车载控制装置3对车载装置的控制功能停止的情况下删除该旧版本的程序,并将从车载更新装置2发送的更新程序存储在该非动作面中。

[0050] 详情后述,关于车载更新装置2对来自程序提供装置S1的更新程序的取得及更新程序从车载更新装置2向车载控制装置3的发送,例如以按预定的数据尺寸分割的块单位进行该更新程序。对取得及发送的各个块附有用于单独地识别该块的块ID,车载更新装置2的控制部20能够通过将取得及发送的块ID存储到存储部21中,使用块ID作为检查点来确定上次更新程序的取得及发送中断的中断点。车载控制装置3的控制部30也可以将接收到的块ID存储到存储部31中。

[0051] 车载控制装置3的控制部30在正常结束了更新程序的接收即正常结束了分割的全部块的接收之后,进行动作面的切换,将接收到的更新程序作为当前版本的程序来应用并执行。控制部30在正常结束了更新程序的接收且正常地进行了动作面的切换的情况下,将程序的更新完成(正常结束)这一情况存储到存储部31中,进而向车载更新装置2发送(通知)。

[0052] 车载控制装置3的控制部30在向更新程序的切换失败了的情况下,进行回滚处理即将存储有更新程序的前版本(旧版本)的程序的非动作面的存储区域切换为动作面的存储区域(回滚),执行(应用)该前版本的程序。控制部30也可以在向更新程序的切换失败了的情况下,将更新失败(异常结束)这一情况存储到存储部31中,进而向车载更新装置2发送(通知)。

[0053] 显示装置5是例如汽车导航的显示屏等HMI(Human Machine Interface:人机接口)装置。显示装置5通过串行电缆等线束而与车载更新装置2的输入输出I/F24以能够通信的方式连接。显示装置5显示从车载更新装置2的控制部20经由输入输出I/F24而输出的数据或信息。显示装置5与车载更新装置2之间的连接方式不限于基于输入输出I/F24的连接方式,显示装置5与车载更新装置2也可以是经由车内LAN4的连接方式。

[0054] IG开关6是对车辆C的发动机等原动机(未图示)的动作状态进行切换的开关。例如用户将IG开关6从断开向接通切换而使车辆C起动,开始车辆C的行驶。然后,结束车辆C的行驶,用户将IG开关6从接通向断开切换,使车辆停止。IG开关6通过串行电缆等线束而与车载更新装置2的输入输出I/F24以能够通信的方式连接。经由输入输出I/F24向车载更新装置2的控制部20通知IG开关6的切换状态(接通或断开)。例如,从IG开关6经由输入输出I/F24而向车载更新装置2的控制部20输入表示IG开关6的接通或断开的信号。IG开关6与车载更新装置2之间的连接方式不限于基于输入输出I/F24的连接方式,IG开关6与车载更新装置2也可以是经由车内LAN4的连接方式。

[0055] 图3是例示车载更新装置2的控制部20的处理的流程图。图4是表示在程序提供装置S1、车载更新装置2及车载控制装置3之间收发的通信信号及更新程序的时序图。车载更新装置2的控制部20在车辆C为起动状态(IG开关接通)的情况下,经由车外通信装置1而与程序提供装置S1定期或非定期地进行通信,在程序提供装置S1中准备有应该更新的程序或数据即更新程序的情况下,进行以下的处理。或者,控制部20也可以基于经由车外通信装置1而取得的来自程序提供装置S1的更新通知来进行以下的处理。也可以是,控制部20使显示装置5显示更新通知,基于经由显示装置5所具备的触摸屏等输入终端由车辆C的操作者输入的更新的授权来进行以下的处理。

[0056] 车载更新装置2的控制部20在从程序提供装置S1通知了更新信息时向程序提供装置S1要求更新程序的发送。控制部20从程序提供装置S1以块单位取得(接收)更新程序(S11),并将取得的更新程序以块单位向车载控制装置3发送。详细而言,控制部20经由车外通信装置1而以块单位取得更新程序,并将取得的更新程序存储到存储部21中。存储在存储部21中的更新程序通过控制部20经由车内LAN4而以块单位向车载控制装置3发送。取得的更新程序也可以施加例如公共密钥方式或公开密钥方式的加密等隐秘化处理。加密的更新程序存储在存储部21中,通过控制部20来解码。解码后的更新程序存储在存储部21中,通过控制部20以块单位向车载控制装置3发送。

[0057] 车载更新装置2的控制部20将更新程序以按预定的数据尺寸分割的块单位向车载控制装置3发送。或者,也可以是,控制部20提取更新程序所包含的分隔符,并基于该分隔符来将更新程序分割成块。控制部20以相同地分割的块单位取得更新程序。对块附有用于识别各个块的块ID。控制部20将取得及发送的块的块ID存储到存储部21中。

[0058] 车载更新装置2的控制部20判定所发送的块是否为最后的块。控制部20在例如将更新程序按预定的数据尺寸分割成块时,确定所生成的块的个数。该确定的块的个数作为块ID的末尾的编号,控制部20根据本次发送的块的块ID是否为末尾的编号,在使更新程序的发送完成时判定是否为最后的块。

[0059] 在发送的块不是最后的块的情况下,车载更新装置2的控制部20发送作为上次发送的块的块ID的下一个块ID的块。控制部20将按预定的数据尺寸分割的更新程序的块依次发送到作为更新对象的车载控制装置3。

[0060] 接收到从车载更新装置2发送来的更新程序的块的作为更新对象的车载控制装置3将该块存储到非动作面的存储区域(第一存储区域311或第二存储区域312)中。车载控制装置3也可以将接收到的块的块ID存储到存储部31中。

[0061] 在依次进行以块为单位的更新程序的取得及发送的期间内车辆C停止即IG开关变为断开的情况下(S12:是),该块单位的更新程序的取得及发送中断。并且,在车载更新装置2的存储部21中留下更新程序和最后取得及发送的块的块ID的信息。

[0062] 车载更新装置2的控制部20能够将存储的块ID用作更新程序的取得及发送的检查点,并基于该检查点来导出更新程序的取得及发送中断的中断点。

[0063] 更新程序也可以包含多个检查点及表示该更新程序的文件的末端的信息的EOF(End Of File:文件结束符)。控制部20可以从EOF向该文件的最前头回溯来检测检查点,基于最初检测(确认)到的检查点来导出中断点。检查点可以使用例如预定的字符代码或对该文件内的区段进行分割的分隔符。中断点的导出不限于基于检查点的导出,也可以是,控制部20与程序提供装置S1通信来进行中断点的导出。

[0064] 车载更新装置2的控制部20在车辆C停止之后使用蓄存在车载更新装置2的蓄电装置(未图示)中的电,基于存储在存储部21中的更新程序而导出第一导出值(S13)。即,第一导出值是基于在更新程序的取得及发送的中断前存储在存储部21中的更新程序而导出的导出值。将导出的第一导出值存储在存储部21中。第一导出值例如是散列值或MAC(Message Authentication Code:消息认证码)值。作为散列值的第一导出值基于存储在存储部21中的更新程序,使用存储在存储部21中的散列函数而导出。作为MAC值的第一导出值基于存储在存储部21中的更新程序,使用存储在存储部21中的公共密钥(共享密钥)及MAC算法而导出。导出值的导出不限于基于控制部20的导出,也可以是,车载更新装置2具备与控制部20以能够通信的方式连接的专用处理器,该处理器对导出值进行导出。

[0065] 在车辆C为停止状态即IG开关未接通的情况下(S14:否),车载更新装置2的控制部20为了再次进行S14的判定而进行循环处理。在进行该循环处理时,控制部20也可以执行预定时间的待机处理(睡眠)。

[0066] 在车辆C重新成为起动状态即IG开关接通的情况下(S14:是),车载更新装置2的控制部20基于存储在存储部21中的更新程序而导出第二导出值(S15)。即,第二导出值基于在更新程序的取得及发送中断后存储在存储部21中的更新程序而导出。将导出的第二导出值

存储在存储部21中。第二导出值为以与上述的第一导出值相同的方法导出的导出值,例如为散列值或MAC值。

[0067] 车载更新装置2的控制部20对存储在存储部21中的第一导出值与第二导出值进行比较,判定是否为相同的值(S16)。在第一导出值与第二导出值相同的情况下,控制部20判定为存储在存储部21中的更新程序正当。即,判定为存储在存储部21中的更新程序未由于篡改等而变更。通过对基于中断前后存储在存储部21中的更新程序导出的导出值(第一导出值及第二导出值)进行比较,能够在发送重新开始前判定存储在存储部21中的更新程序的适当性。

[0068] 在第一导出值与第二导出值相同的情况下(S16:是),控制部20从上述的中断点起重新开始更新(更新程序的取得及发送)。详细而言,控制部20向程序提供装置S1要求从在上次(中断前)更新程序的取得中作为最后取得的块ID的下一个块的发送,重新开始以块为单位的更新程序的取得。将取得的更新程序存储在存储部21中。存储在存储部21中的更新程序以块单位向车载控制装置3发送。或者,控制部20将在上次更新程序的发送中作为最后发送的块的块ID的下一个块向车载控制装置3发送,重新开始向车载控制装置3的以块为单位的更新程序的发送。即,重新开始车载控制装置3的更新。

[0069] 从中断点起重新开始更新,从而无需对在上次更新程序的取得及发送中已经取得及发送的块重新进行取得及发送的处理,能够缩短从更新的重新开始到完成为止所需的需要时间,且能够抑制车内LAN4中的通信量的增加。

[0070] 车载更新装置2的控制部20经由输入输出I/F24而使显示装置5显示更新重新开始的通知,并对车辆C的操作者通知更新重新开始(S18)。

[0071] 在第一导出值与第二导出值不同的情况下(S16:否),车载更新装置2的控制部20判定为存储在存储部21中的更新程序不正当。即,判定为存储在存储部21中的更新程序由于篡改等而变更为不正当。因此,控制部20为了发送正当的更新程序,从程序提供装置S1从头取得更新程序(S161)。详细而言,控制部20向程序提供装置S1要求从具备开头的块ID的块起发送更新程序。控制部20从程序提供装置S1以块单位取得更新程序,并将取得的更新程序存储到存储部21中。存储在存储部21中的更新程序以块单位向车载控制装置3发送。通过从头得更新程序,能够防止变更为了不正当的更新程序向车载控制装置3发送的情况。

[0072] 车载更新装置2的控制部20经由输入输出I/F24而在显示装置5上显示在车辆C停止时更新程序变更为不正当的情况,对车辆C的操作者进行通知(S162)。控制部20也可以使显示装置5显示从头取得更新程序,对车辆C的操作者进行通知。控制部20也可以向程序提供装置S1发送(通知)所存储的更新程序变更为不正当的情况。

[0073] 在发送的更新程序的块为最后的块的情况下,车载更新装置2的控制部20通过发送最后的块来结束向车载控制装置3的更新程序的发送(S19)。因为发送所取得的更新程序,所以在发送最后的块之前结束更新程序的取得,这是不言而喻的。控制部20将该车载控制装置3的更新完成的情况存储到存储部21中。虽然在图3中省略,在更新程序的发送结束之前车辆C再次成为停止状态(IG开关6断开)的情况下进行S13的处理。

[0074] 车载控制装置3在接收从车载更新装置2发送的最后的块之后,将自控制装置的更新完成这一情况存储到存储部31中。车载控制装置3对接收最后的块而完成接收的更新程序的切换即将动作面切换成存储有更新程序的存储区域,然后向车载更新装置2发送(通

知)对更新程序的切换完成(更新完成)这一情况。车载更新装置2的控制部20也可以将作为更新对象的车载控制装置3向更新程序的切换完成这一情况存储到存储部21中。控制部20向程序提供装置S1发送(通知)作为更新对象的车载控制装置3的更新完成这一情况。控制部20也可以经由输入输出I/F24使显示装置5显示作为更新对象的车载控制装置3的更新完成这一情况,并对车辆C的操作者进行通知。

[0075] 控制部20在更新程序的发送结束之后将存储在存储部21中的更新程序删除(S20)。通过更新程序的删除,能够防止存储部21被更新程序压缩空间。

[0076] 在更新程序的取得或发送的期间内车辆C为起动状态即IG开关未断开的情况下(S12:否),控制部20为了再次进行S12的判定而进行循环处理。在该循环处理的期间内控制部20继续更新程序的取得及发送,在更新程序的发送完成的情况下,控制部20也可以进行S20的处理。

[0077] 应该认为,本次公开的实施方式在全部方面均为示例性的而不是限制性的。本发明的范围不由上述的意思示出,而由权利要求书示出,意在包含与权利要求书等同含义及范围内的全部变更。

[0078] 附图标记说明

[0079] C车辆

[0080] S车载更新系统

[0081] S1程序提供装置(外部服务器)

[0082] S11存储部

[0083] 1车外通信装置

[0084] 11车外通信部

[0085] 12输入输出I/F

[0086] 13天线

[0087] 2车载更新装置

[0088] 20控制部

[0089] 21存储部

[0090] 22记录介质

[0091] 23车内通信部

[0092] 24输入输出I/F

[0093] 3车载控制装置

[0094] 30控制部

[0095] 31存储部

[0096] 311第一存储区域

[0097] 312第二存储区域

[0098] 32车内通信部

[0099] 4车内LAN

[0100] 5显示装置

[0101] 6 IG开关

[0102] N车外网络。

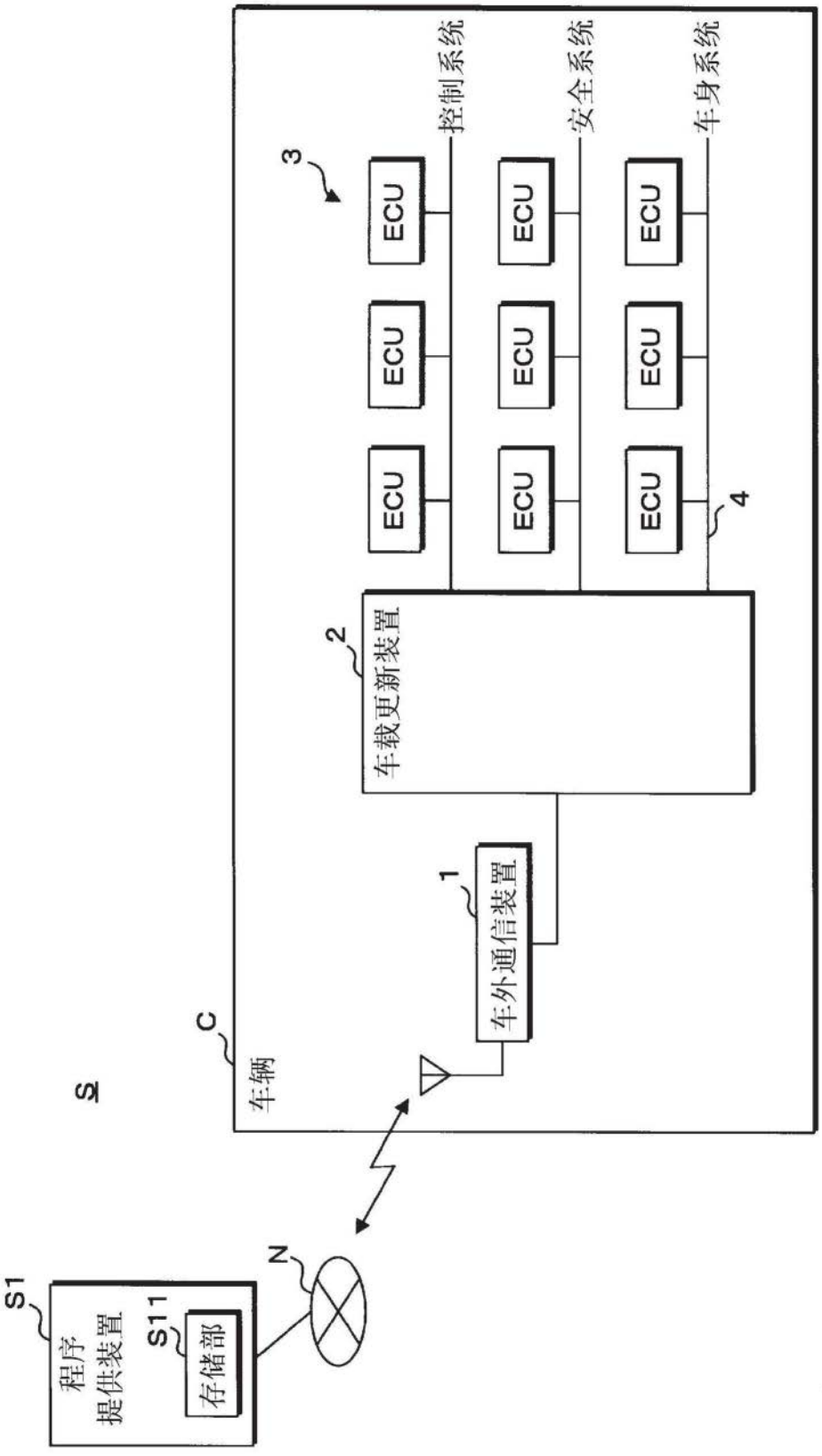

S
C
车辆
1
车外通信装置
2
车载更新装置
3
ECU
控制系统
安全系统
车身系统
4
N
S1
程序
提供装置
S11
存储部

图1

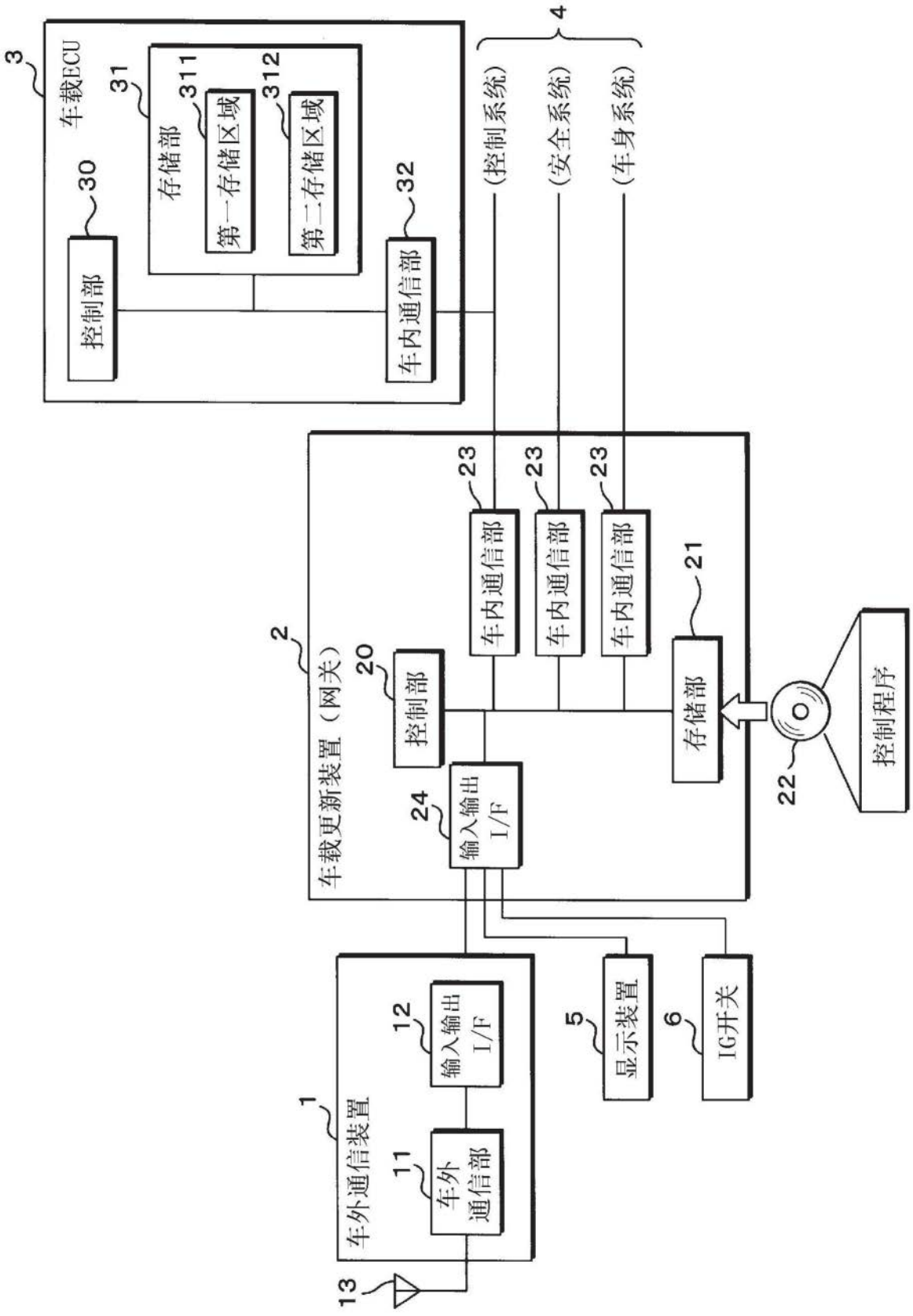

3
车载ECU
31
存储部
311
第一存储区域
312
第二存储区域
30
控制部
32
车内通信部
4
(控制系统)
(安全系统)
(车身系统)
2
车载更新装置（网关）
20
控制部
23
车内通信部
23
车内通信部
23
车内通信部
21
存储部
24
输入输出I/F
22
控制程序
1
车外通信装置
11
车外通信部
12
输入输出I/F
13
5
显示装置
6
IG开关

图2

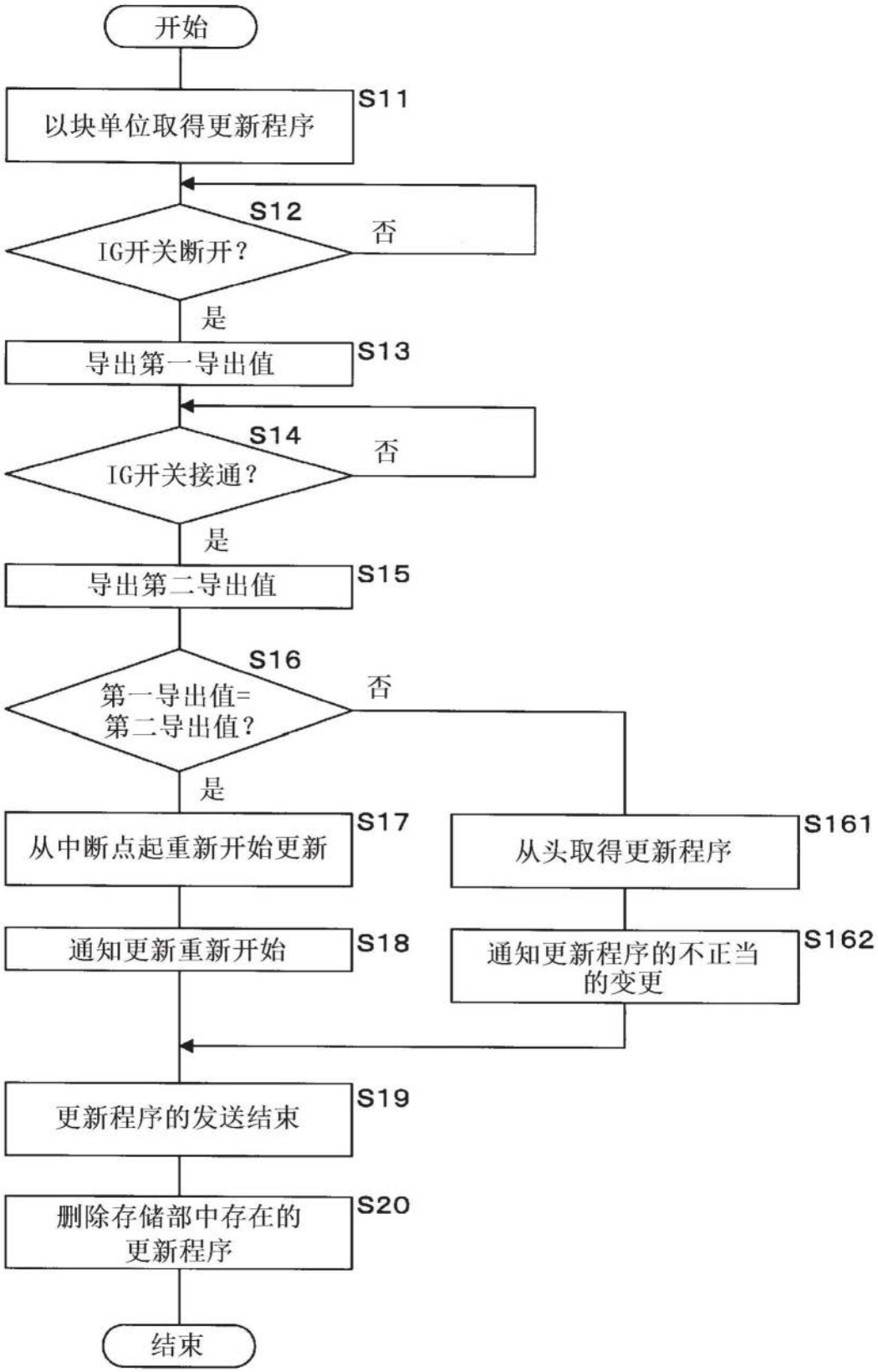

开始
以块单位取得更新程序
S11
S12
IG开关断开？
否
是
导出第一导出值
S13
S14
IG开关接通？
否
是
导出第二导出值
S15
S16
第一导出值=
第二导出值？
否
是
从中断点起重新开始更新
S17
从头取得更新程序
S161
通知更新重新开始
S18
通知更新程序的不正当
的变更
S162
更新程序的发送结束
S19
删除存储部中存在的
更新程序
S20
结束

图3

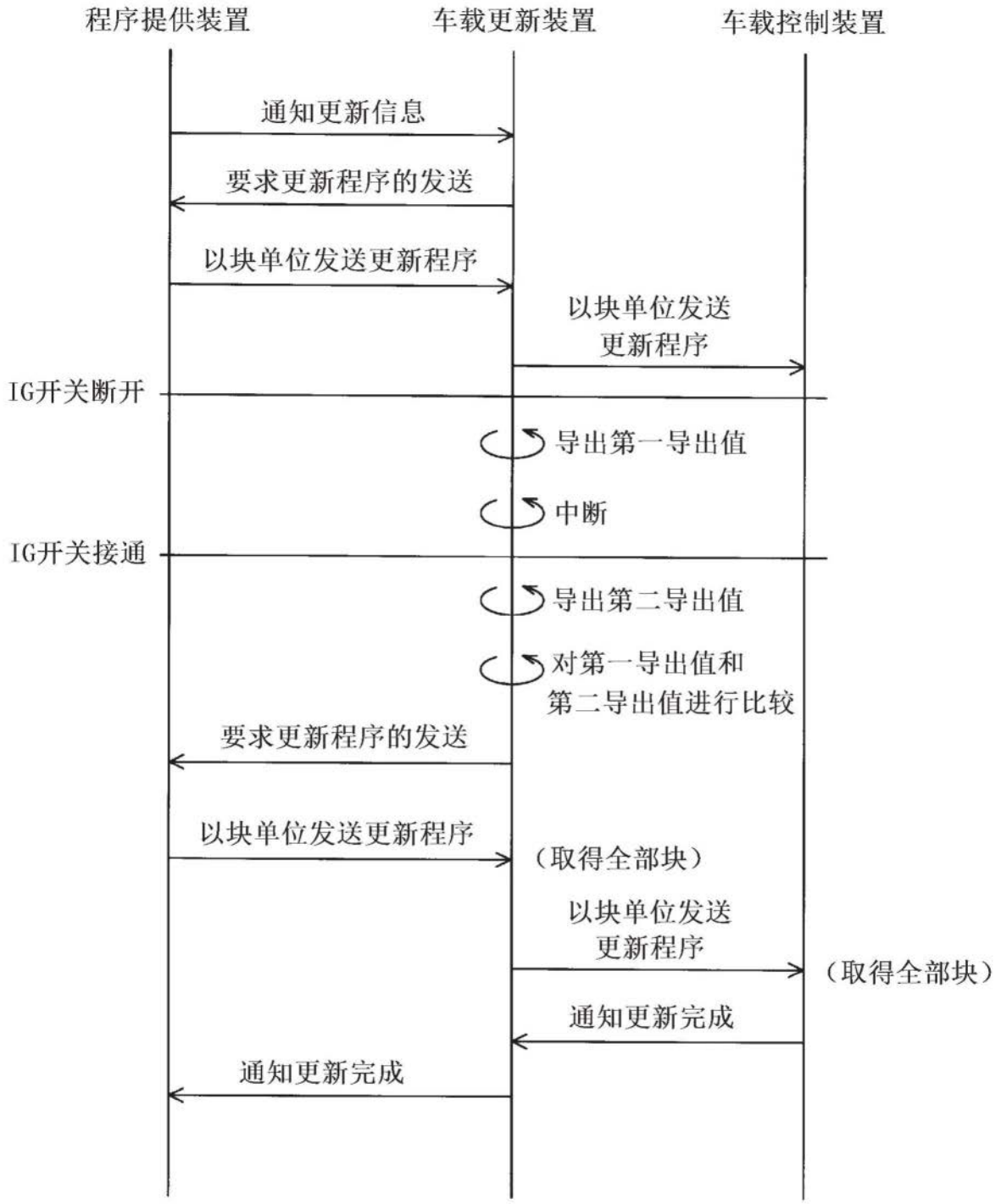

程序提供装置
车载更新装置
车载控制装置
通知更新信息
要求更新程序的发送
以块单位发送更新程序
以块单位发送
更新程序
IG开关断开
导出第一导出值
中断
IG开关接通
导出第二导出值
对第一导出值和
第二导出值进行比较
要求更新程序的发送
以块单位发送更新程序
（取得全部块）
以块单位发送
更新程序
（取得全部块）
通知更新完成
通知更新完成

图4