



(12) 发明专利

(10) 授权公告号 CN 108351840 B

(45) 授权公告日 2022.06.10

(21) 申请号 201680055509.3

(72) 发明人 月館统宙 阿部雄介 福田毅

(22) 申请日 2016.10.26

蛇名朋仁 成泽文雄

(65) 同一申请的已公布的文献号

申请公布号 CN 108351840 A

(74) 专利代理机构 上海华诚知识产权代理有限公司 31300

专利代理人 肖华

(43) 申请公布日 2018.07.31

(51) Int.CI.

G06F 12/16 (2006.01)

(30) 优先权数据

2015-229375 2015.11.25 JP

(56) 对比文件

JP 2007226640 A, 2007.09.06

(85) PCT国际申请进入国家阶段日

CN 104094233 A, 2014.10.08

2018.03.23

JP H04125753 A, 1992.04.27

(86) PCT国际申请的申请数据

CN 101681286 A, 2010.03.24

PCT/JP2016/081655 2016.10.26

JP 2015184796 A, 2015.10.22

(87) PCT国际申请的公布数据

CN 101030360 A, 2007.09.05

W02017/090364 JA 2017.06.01

US 2010162042 A1, 2010.06.24

(73) 专利权人 日立汽车系统株式会社

审查员 宁雪莹

地址 日本茨城县

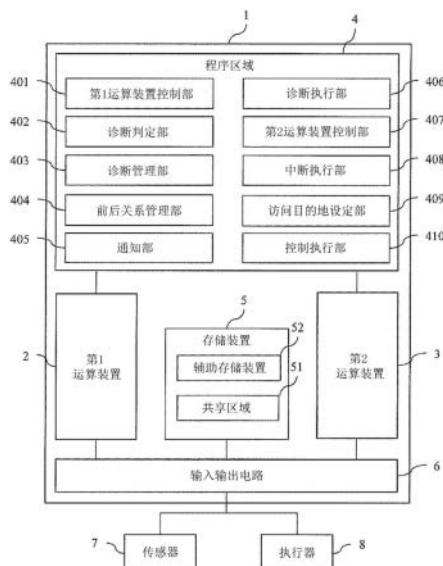
权利要求书2页 说明书10页 附图16页

(54) 发明名称

车辆控制装置

(57) 摘要

本发明在采用多个运算装置的车辆控制装置中抑制诊断共享存储区域时的运算效率的降低。本发明的车辆控制装置在诊断存储装置所具有的共享存储区域的期间内变更对于该存储装置的访问目的地，由此抑制运算效率的降低。



1. 一种车辆控制装置,其控制车辆的动作,该车辆控制装置的特征在于,具备:

第1运算装置及第2运算装置,它们执行控制所述车辆的动作的控制运算;

存储诊断部,其诊断所述第1运算装置及第2运算装置共享的共享存储区域;

共享存储装置,其具有所述共享存储区域;

辅助存储装置,其为不同于所述共享存储装置的存储装置,具有存储副本的辅助存储区域,所述副本为所述存储诊断部所诊断的诊断对象区域所存储的数据的副本,并以所述辅助存储区域的形式构成辅助存储部;以及

访问目的地设定部,其以如下方式设定访问目的地地址,即,在所述存储诊断部诊断所述诊断对象区域的期间内,所述第1运算装置及第2运算装置使用所述辅助存储部内存存储的所述副本代替所述诊断对象区域内存存储的数据来执行所述控制运算,

所述辅助存储装置由可靠性比所述共享存储装置高的存储装置构成,

所述辅助存储装置是以在某一运算装置写入数据的期间内排除来自另一运算装置的访问的排他性存储装置的形式构成,由此构成为具有比所述共享存储装置高的可靠性的存储装置。

2. 根据权利要求1所述的车辆控制装置,其特征在于,

所述存储诊断部是以安装有诊断所述共享存储区域的处理的存储诊断程序的形式构成,

所述第1运算装置通过执行所述存储诊断部来诊断所述共享存储区域,

所述车辆控制装置还具备通知部,当所述第1运算装置开始执行所述存储诊断部时,所述通知部对所述访问目的地设定部通知所述共享存储区域处于诊断中这一情况,

当所述访问目的地设定部从所述通知部收到所述共享存储区域处于诊断中这一情况的通知时,以所述第2运算装置访问所述辅助存储部而不是所述诊断对象区域的方式设定访问目的地地址。

3. 根据权利要求2所述的车辆控制装置,其特征在于,

当所述第1运算装置执行完所述存储诊断部时,所述通知部对所述访问目的地设定部通知所述共享存储区域的诊断已完成这一情况,

当所述访问目的地设定部从所述通知部收到所述共享存储区域的诊断已完成这一情况的通知时,以所述第2运算装置访问所述诊断对象区域而不是所述辅助存储部的方式设定访问目的地地址。

4. 根据权利要求1所述的车辆控制装置,其特征在于,

所述共享存储区域存储有诊断个数数据,所述诊断个数数据指定所述存储诊断部统一进行诊断的所述诊断对象区域的个数,

所述辅助存储部具备能够存储所述诊断个数数据所指定的所述个数以上的所述诊断对象区域的副本的存储容量,

所述存储诊断部统一诊断所述诊断个数数据所指定的所述个数的所述诊断对象区域,

所述访问目的地地址设定部以如下方式设定访问目的地地址,即,在从所述存储诊断部开始所述共享存储区域的诊断起到诊断完所述诊断个数数据所指定的所述个数的所述诊断对象区域为止的期间内,所述第1运算装置及第2运算装置使用所述辅助存储部内存存储的所述副本代替所述诊断对象区域内存存储的数据来执行所述控制运算。

5. 根据权利要求1所述的车辆控制装置,其特征在于,

所述共享存储区域存储保存目的地地址数据,所述保存目的地地址数据记述存储有所述副本的所述辅助存储部上的地址,

所述第1运算装置及第2运算装置从所述保存目的地地址数据所记述的所述辅助存储部上的地址获取所述副本。

6. 根据权利要求5所述的车辆控制装置,其特征在于,

所述辅助存储部存储保存源地址数据,所述保存源地址数据记述存储有所述诊断对象区域的所述共享存储区域上的地址,

在所述共享存储区域的诊断完成之后,所述第1运算装置获取所述保存目的地地址数据所记述的所述辅助存储部上的地址所存储的数据,并对所述保存源地址数据所记述的地址回写该获取到的数据。

7. 根据权利要求1所述的车辆控制装置,其特征在于,

所述存储诊断部是以安装有诊断所述共享存储区域的处理的存储诊断程序的形式构成,

所述第1运算装置及第2运算装置对所述共享存储区域中的自身写入数据的区域执行所述存储诊断部,由此实施所述诊断。

8. 根据权利要求1所述的车辆控制装置,其特征在于,

所述存储诊断部是以安装有诊断所述共享存储区域的处理的存储诊断程序的形式构成,

所述第1运算装置及第2运算装置对所述共享存储区域中的自身写入数据的比例高于另一运算装置的区域执行所述存储诊断部,由此实施所述诊断。

车辆控制装置

技术领域

[0001] 本发明涉及一种车辆控制装置。

背景技术

[0002] 近年来,汽车控制系统等之类的嵌入式系统因多功能化而导致运算量逐年增加,所需要的CPU(Central Processing Unit)的运算性能有增无减。在个人计算机中,对于这种处理量的增加,是通过增加CPU的核心数(多核心化)来加以应对。嵌入式系统也不例外,例如在像汽车导航或手机等这样运算量大、实时性的制约相对宽松的面向消费者的系统中,多核心化在不断推进。随着嵌入式系统的升级、复杂化,预料到这些运算量将会超过单核心的极限,因此,业界在探讨采用多核心。

[0003] 另一方面,为了实现汽车业界内的软件品质级别的统一化和安全性认证的容易化,于2011年制定了功能安全标准ISO26262(以下记作功能安全标准)。本标准涵盖包括硬件和软件在内的整个系统,对故障率算出方法、软件设计方法等进行了规定。要遵循本标准,就必须展示安全已得到确保的依据。通常是通过归纳现有设计中的见解和实绩作为证据来遵循该标准。

[0004] 在ISO26262中,要求防止安全要求不同的软件间的干扰。一般的车辆控制系统是由各种控制应用构成的,因此时间保护功能、存储器保护功能等用以防止构成系统的软件间的相互作用的机制近年来受到关注。具体而言,为如下功能:在某一软件失控的情况下,防止该失控的软件访问存储有其他软件所使用的数据的存储区域而破坏该数据。我们知道,在一般的车辆控制装置中,若运用AUTOSAR架构,则车辆控制系统会混存各种ASIL的软件。因而,现有的软件要遵循ISO26266,就需要防止软件间的干扰的机制和与其相关联的处理的高速化、轻量化、可靠性提高等。

[0005] 下述专利文献1揭示了一种用以在具有多核心处理器(MPU)的汽车用电子控制装置中提高诊断处理等重要运算处理的可靠性而提高汽车控制的安全性的技术。在该文献中,将存储区域划分为控制程序用的正常控制区域(正常运算区域)和诊断程序用的高安全区域(重要运算区域)。在高安全区域内安装进行高安全区域的存储诊断的高安全区域用诊断程序以及进行全区域的存储诊断的正常诊断用程序。以双重方式对高安全区域实施存储诊断。

[0006] 现有技术文献

[0007] 专利文献

[0008] 专利文献1:日本专利特开2015-022622号公报

发明内容

[0009] 发明要解决的问题

[0010] 在多核心系统中,各核心独立地进行动作,由此能够并行实施运算处理而提高运算效率。但在各核心共享存储装置(例如存储器)的情况下,在这些核心之间会发生对该共

享存储装置的访问竞争。多核心系统通常以如下方式设计：当发生访问竞争时，一核心会待机直至另一核心的处理完成。因而，有可能对吞吐量产生影响。

[0011] 本发明是鉴于上述那样的问题而成，其目的在于在采用多个运算装置的车辆控制装置中抑制诊断共享存储区域时的运算效率的降低。

[0012] 解决问题的技术手段

[0013] 本发明的车辆控制装置在诊断存储装置所具有的共享存储区域的期间内变更对该存储装置的访问目的地，由此抑制运算效率的降低。

[0014] 发明的效果

[0015] 根据本发明的车辆控制装置，一方面能够抑制诊断共享存储区域时的由运算装置间的访问竞争引起的运算效率的降低，另一方面能够高效地诊断存储区域。

附图说明

[0016] 图1为实施方式1的车辆控制装置(ECU)1的构成图。

[0017] 图2为表示存储装置5的地址空间50000的图。

[0018] 图3为表示共享区域51所存储的标记管理表51100的构成和数据例的图。

[0019] 图4为表示共享区域51所存储的诊断参数表51200的构成和数据例的图。

[0020] 图5为表示共享区域51所存储的诊断进展管理表51300的构成和数据例的图。

[0021] 图6为表示共享区域51所存储的共享区域管理表51400的构成和数据例的图。

[0022] 图7为表示辅助存储区域52所存储的辅助存储区域管理表52100的构成和数据例的图。

[0023] 图8为说明第1运算装置控制部401的动作的流程图。

[0024] 图9为说明诊断判定部402的动作的流程图。

[0025] 图10为说明诊断管理部403的动作的流程图。

[0026] 图11为说明前后关系管理部404的动作的流程图。

[0027] 图12为说明通知部405的动作的流程图。

[0028] 图13为说明诊断执行部406的动作的流程图。

[0029] 图14为说明第2运算装置控制部407的动作的流程图。

[0030] 图15为说明中断执行部408的动作的流程图。

[0031] 图16为说明访问目的地设定部409的动作的流程图。

[0032] 图17为说明控制执行部410的动作的流程图。

具体实施方式

[0033] <实施方式1>

[0034] 图1为本发明的实施方式1的车辆控制装置(ECU)1的构成图。ECU 1例如为发动机控制装置等这样的控制车辆的动作的装置，具备第1运算装置2、第2运算装置3、程序区域4、存储装置5及输入输出电路6。此处，作为连接有ECU 1连接的设备，例示的是节气门传感器7和执行器8，但并不限于此。

[0035] 第1运算装置2和第2运算装置3是执行程序区域4所存储的程序的运算装置。第1运算装置2和第2运算装置3能够并行执行程序区域4所存储的程序，进而能够并行访问程序区

域4和存储装置5。

[0036] 程序区域4例如为构成于ROM(Read Only Memory)等非易失性存储装置上的存储区域。程序区域4存储第1运算装置控制部401、诊断判定部402、诊断管理部403、前后关系管理部404、通知部405、诊断执行部406、第2运算装置控制部407、中断执行部408、访问目的地设定部409及控制执行部410。

[0037] 存储装置5例如为RAM(Random Access Memory)等存储装置。存储装置5具有共享区域51和辅助存储区域52作为配置在相同地址空间内的存储区域。共享区域51存储控制执行部410执行控制运算所使用的数据,而且存储后文叙述的图3~图6中说明的数据表。辅助存储区域52存储后文叙述的图7中说明的数据表。这些存储区域所存储的数据的具体例将于后文叙述。

[0038] 图2为表示存储装置5的地址空间50000的图。地址空间50000具有辅助存储区域地址50200和共享区域地址50100。共享区域地址50100是存储共享区域51所记录的数据的区域。辅助存储区域地址50200是存储辅助存储区域52所记录的数据的区域。

[0039] 图3为表示共享区域51所存储的标记管理表51100的构成和数据例的图。标记管理表51100是存储表示后文叙述的各程序的动作状态的标记的数据表。标记管理表51100具有名称字段51101和当前值字段51102。

[0040] 名称字段51101保持标记管理表51100所管理的标记的名称。当前值字段51102保持标记的当前值。图3所示的各标记及其值将与后文叙述的各程序的动作一并进行说明。

[0041] 图4为表示共享区域51所存储的诊断参数表51200的构成和数据例的图。诊断参数表51200为存储与对于共享区域51的存储诊断有关的参数的数据表。诊断参数表51200具有名称字段51201和值字段51202。

[0042] 名称字段51201保持诊断参数表51200所管理的参数的名称。值字段51202保持参数的值。图4所示的参数及其值将与后文叙述的各程序的动作一并进行说明。

[0043] 图5为表示共享区域51所存储的诊断进展管理表51300的构成和数据例的图。诊断进展管理表51300为用以管理对于共享区域51的存储诊断的进展的数据表。诊断进展管理表51300具有名称字段51301和当前值字段51302。

[0044] 名称字段51301保持诊断进展管理表51300所管理的进展参数的名称。当前值字段51302保持进展参数的值。图5所示的参数及其值将与后文叙述的各程序的动作一并进行说明。

[0045] 图6为表示共享区域51所存储的共享区域管理表51400的构成和数据例的图。共享区域管理表51400为在共享区域51侧对共享区域51所存储的数据与辅助存储区域52所存储的数据之间的对应关系进行管理的数据表。共享区域管理表51400具有名称字段51401、地址字段51402、保存目的地地址字段51403、数据字段51404及诊断结果字段51405。

[0046] 名称字段51401保持共享区域管理表51400所管理的数据(共享区域51所存储的数据)的名称。地址字段51402为存储共享区域管理表51400所管理的数据的共享区域51上的地址。保存目的地地址字段51403保持通过后文叙述的处理步骤将共享区域51上的数据保存至辅助存储区域52时的辅助存储区域52上的存储目的地地址。数据字段51404保持共享区域管理表51400所管理的数据的值。诊断结果字段51405保持对于地址字段51402所指定的存储区域的存储诊断的结果。

[0047] 共享区域51存储与图6的各记录相对应的数据。设想图6的各记录对应于共享区域51内的1个存储区域、1个存储区域存储1个数据值。

[0048] 图7为表示辅助存储区域52所存储的辅助存储区域管理表52100的构成和数据例的图。辅助存储区域管理表52100为在辅助存储区域52侧对共享区域51所存储的数据与辅助存储区域52所存储的数据之间的对应关系进行管理的数据表。辅助存储区域管理表52100具有名称字段52101、地址字段52102、保存源地址字段52103及保存源数据52104。

[0049] 名称字段52101保持辅助存储区域管理表52100所管理的数据(辅助存储区域52所存储的数据)的名称。并非必须与名称字段51401所记述的名称一致。地址字段52102保持存储辅助存储区域管理表52100所管理的数据的辅助存储区域52上的地址。保存源地址字段52103保持通过后文叙述的处理步骤将共享区域51上的数据保存至辅助存储区域52时的共享区域51上的存储源地址。保存源数据52104保持辅助存储区域管理表52100所管理的数据的值。

[0050] 以上,对ECU 1的构成进行了说明。下面,假定第1运算装置2实施对于共享区域51的存储诊断、第2运算装置3实施控制运算,对各程序的动作进行说明。

[0051] 图8为说明第1运算装置控制部401的动作的流程图。第1运算装置2例如周期性地执行本流程图,由此实施对于共享区域51的存储诊断。下面,对图8的各步骤进行说明。

[0052] (图8:步骤S401000)

[0053] 第1运算装置控制部401将存储装置5所管理的各表格(标记管理表51100、诊断进展管理表51300、共享区域管理表51400、辅助存储区域管理表52100)初始化。

[0054] (图8:步骤S401001)

[0055] 第1运算装置控制部401调用诊断判定部402。诊断判定部402的动作将于后文叙述的图9中进行说明。诊断判定部402具有判定是否为应实施存储诊断的时刻的作用。

[0056] (图8:步骤S401002)

[0057] 第1运算装置控制部401调用诊断管理部403。诊断管理部403的动作将于后文叙述的图10中进行说明。诊断管理部403具有控制存储诊断的整体动作的作用。

[0058] (图8:步骤S401003)

[0059] 第1运算装置控制部401判定是否已满足结束条件。若已满足,则结束本流程图,若未满足,则返回至步骤S401001。结束条件例如为输入有断开ECU 1的电源的命令等。

[0060] 图9为说明诊断判定部402的动作的流程图。下面,对图9的各步骤进行说明。

[0061] (图9:步骤S402000)

[0062] 诊断判定部402从诊断进展管理表51300获取定时计数器的当前值字段51302。诊断判定部402对定时计数器的值进行递增,并对诊断进展管理表51300的对应的字段存储递增后的值。

[0063] (图9:步骤S402001)

[0064] 诊断判定部402从诊断参数表51200获取诊断执行周期的值字段51202(图示的例子中为200)。诊断判定部402算出获取到的定时计数器除以获取到的诊断执行周期而得的余数。若算出的余数为0,则进入至步骤S402001,在其他情况下,结束本流程图。

[0065] (图9:步骤S402002)

[0066] 诊断判定部402对标记管理表51100所存储的诊断开始标记的当前值字段51102存

储1(表示开始存储诊断这一情况的值)。诊断管理部403在后文叙述的步骤S403000中确认该诊断开始标记的值,由此可以判定是否已到达应开始存储诊断的时刻。

[0067] 图10为说明诊断管理部403的动作的流程图。下面,对图10的各步骤进行说明。

[0068] (图10:步骤S403000)

[0069] 诊断管理部403从标记管理表51100获取诊断开始标记的当前值字段51102。若诊断开始标记为1,则进入至步骤S403001,在其他情况下,结束本流程图。

[0070] (图10:步骤S403001)

[0071] 诊断管理部403调用前后关系管理部404。前后关系管理部404的动作将于后文叙述的图11中进行说明。前后关系管理部404具有将共享区域51所存储的数据保存至辅助存储区域52、或者将已保存的数据从辅助存储区域52送回至共享区域51的作用。在本步骤中,将数据保存至辅助存储区域52。

[0072] (图10:步骤S403002)

[0073] 诊断管理部403调用通知部405。通知部405的动作将在后文叙述的图12中进行说明。通知部405具有如下作用:在任一运算装置实施对于共享区域51的存储诊断时,通过中断处理对另一运算装置通知这一情况,或者在诊断完成后通知这一情况。在本步骤中,通知诊断开始。

[0074] (图10:步骤S403003)

[0075] 诊断管理部403调用诊断执行部406。诊断执行部406的动作将在后文叙述的图13中进行说明。诊断执行部406具有实际实施对于共享区域51的存储诊断的作用。

[0076] (图10:步骤S403004)

[0077] 诊断管理部403重新调用前后关系管理部404。在本步骤中,将已保存到辅助存储区域52的数据回写至共享区域51。

[0078] (图10:步骤S403005)

[0079] 诊断管理部403调用通知部405。在本步骤中,通知诊断完成。

[0080] 图11为说明前后关系管理部404的动作的流程图。下面,对图11的各步骤进行说明。

[0081] (图11:步骤S404000)

[0082] 前后关系管理部404从诊断进展管理表51300获取诊断区域地址的当前值字段51302。诊断区域地址为表示当前成为实施存储诊断的对象的诊断对象区域的地址的值。在未设置诊断区域地址的情况下,从诊断参数表51200获取开始地址的值字段51202,并将其作为诊断区域地址的当前值字段51302加以存储。开始地址是指定应诊断的存储区域的开头地址的值,例如指定共享区域51的开头地址。

[0083] (图11:步骤S404001)

[0084] 前后关系管理部404从标记管理表51100获取诊断完成标记的当前值字段51102。若诊断完成标记为0,则进入至步骤S404002,在不为0的情况下,进入至步骤S404006。诊断完成标记是表示是否已完成对于共享区域51整体的存储诊断的标记。

[0085] (图11:步骤S404002)

[0086] 前后关系管理部404从诊断参数表51200获取结束地址的值字段51202。结束地址是指定应诊断的存储区域的终点地址的值,例如指定共享区域51的终点地址。前后关系管

理部404对当前的诊断区域地址与结束地址进行比较。在一致的情况下,进入至步骤S404003,在不一致的情况下,进入至步骤S404004。

[0087] (图11:步骤S404003)

[0088] 前后关系管理部404从诊断参数表51200获取开始地址的值字段51202,作为诊断进展管理表51300的诊断区域地址的当前值字段51302加以存储。本步骤用以在完成存储诊断之后使开始地址退回至开头。

[0089] (图11:步骤S404004)

[0090] 前后关系管理部404将诊断区域地址的当前值字段51302更新至下一诊断对象区域的地址。例如,使用后文叙述的诊断执行部406一次能够诊断的存储区域的个数乘以各存储区域的大小而得的数值对诊断区域地址进行递增。诊断执行部406一次能够诊断的存储区域的个数可以通过诊断参数表51200的可诊断地址数的值字段51202来指定。考虑到对辅助存储区域52保存数据这一情况,诊断执行部406一次能够诊断的存储区域的个数较理想为保存目的地的数据大小为辅助存储区域52的最大大小以下。

[0091] (图11:步骤S404005)

[0092] 前后关系管理部404将诊断区域地址所存储的数据保存至辅助存储区域52。具体而言,将从诊断区域地址的当前值开始到可诊断地址数乘以各存储区域的大小而得的数值的地址为止之间的存储区域内存储的数据复制到辅助存储区域52。前后关系管理部404将保存数据的辅助存储区域52上的地址存储至保存目的地地址字段51403,而且将保存前的共享区域51上的地址和已保存的数据分别存储至保存源地址字段52103和保存源数据52104。

[0093] (图11:步骤S404006)

[0094] 前后关系管理部404将保存目的地地址字段51403和保存源地址字段52103分别用作复制源地址和复制目的地地址,由此对共享区域51复制已保存在辅助存储区域52内的数据。由此,能够恢复已保存的数据。但还存在像后文所述那样控制执行部410对辅助存储区域52上的数据进行覆盖的情况,因此,复制前后的数据值未必相同。

[0095] (图11:步骤S40407)

[0096] 前后关系管理部404对标记管理表51100的诊断完成标记的当前值字段51102存储0。

[0097] 图12为说明通知部405的动作的流程图。下面,对图12的各步骤进行说明。

[0098] (图12:步骤S405000)

[0099] 通知部405产生对第2运算装置3通知已开始共享区域51的诊断这一情况的中断处理。为了避免通知延迟,较理想为使用中断处理,但只要能预估延迟处于容许范围内,则也可使用其他方法来进行通知。

[0100] 图13为说明诊断执行部406的动作的流程图。下面,对图13的各步骤进行说明。

[0101] (图13:步骤S406000)

[0102] 诊断执行部406从诊断参数表51200获取诊断用测试数据的值字段51202。诊断执行部406将获取到的诊断用测试数据写入至诊断区域地址。

[0103] (图13:步骤S406001)

[0104] 诊断执行部406从诊断区域地址读出数据。

[0105] (图13:步骤S406002~S406003)

[0106] 诊断执行部406对步骤S406001中读出的数据与步骤S406000中写入的诊断用测试数据进行比较(S406002)。在两者一致的情况下,进入至步骤S406005,在不一致的情况下,进入至步骤S406004。

[0107] (图13:步骤S406004)

[0108] 诊断执行部406对共享区域管理表51400的诊断结果字段51405记录表示该区域异常这一情况的值(例如0为正常、1为异常等)。

[0109] (图13:步骤S406000~S406004:补充)

[0110] 诊断执行部406能够并行实施可诊断地址数所指定的个数程度的这些步骤。例如,能从诊断开始地址开始对32个存储区域并行实施这些步骤。由此,能够统一实施可诊断地址数的个数程度的存储诊断。通过一边以内部方式对对象地址进行递增一边反复实施这些步骤来代替并行实施,同样也能进行统一诊断。

[0111] (图13:步骤S406005)

[0112] 诊断执行部406对标记管理表51100的诊断完成标记的当前值字段51102存储1。

[0113] 图14为说明第2运算装置控制部407的动作的流程图。第2运算装置3例如周期性地执行本流程图,由此实施控制运算。下面,对图14的各步骤进行说明。

[0114] (图14:步骤S407000)

[0115] 第2运算装置控制部407调用控制执行部410。控制执行部410的动作将在后文叙述的图17中进行说明。控制执行部410具有实施控制运算的作用。

[0116] (图14:步骤S407001)

[0117] 第2运算装置控制部407判定是否已满足结束条件。若已满足,则结束本流程图,若未满足,则返回至步骤S407000。结束条件例如为输入有断开ECU 1的电源的命令等。

[0118] 图15为说明中断执行部408的动作的流程图。当发生步骤S405000中说明过的中断处理时,第2运算装置3开始本流程图而执行中断执行部408。下面,对图15的各步骤进行说明。

[0119] (图15:步骤S408000)

[0120] 中断执行部408调用访问目的地设定部409。访问目的地设定部409的动作将在后文叙述的图16中进行说明。访问目的地设定部409具有切换是使用共享区域51所存储的数据来实施控制运算还是使用辅助存储区域52所存储的数据来实施控制运算的作用。

[0121] 图16为说明访问目的地设定部409的动作的流程图。下面,对图16的各步骤进行说明。

[0122] (图16:步骤S409000)

[0123] 访问目的地设定部409从标记管理表51100获取访问目的地变更标记的当前值字段51102。若访问目的地变更标记的值为0,则进入至步骤S409001,若为1,则进入至步骤S409003。

[0124] (图16:步骤S409001)

[0125] 访问目的地设定部409从诊断进展管理表51300获取诊断区域地址的当前值字段51302,而且从诊断参数表51200获取可诊断地址数的值字段51202。访问目的地设定部409针对共享区域管理表51400所管理的存储区域当中与获取到的诊断区域地址和可诊断地址

数相对应的部分,以控制执行部410对辅助存储区域52的对应的存储区域读写数据的方式变更访问目的地。由于执行本流程图的是第2运算装置3,因此可由第2运算装置3自身变更访问目的地,也可将表示应访问哪一存储区域的标记等数据保持在适当的存储区域上。

[0126] (图16:步骤S409002)

[0127] 访问目的地设定部409将标记管理表51100的访问目的地变更标记的当前值字段51102更新为1。

[0128] (图16:步骤S409003)

[0129] 访问目的地设定部409从诊断进展管理表51300获取诊断区域地址的当前值字段51302,而且从诊断参数表51200获取可诊断地址数的值字段51202。访问目的地设定部409针对共享区域管理表51400所管理的存储区域当中与获取到的诊断区域地址和可诊断地址数相对应的部分,以控制执行部410对共享区域51的对应的存储区域读写数据的方式变更访问目的地。具体的方法与步骤S409001相同。

[0130] (图16:步骤S409004)

[0131] 访问目的地设定部409将标记管理表51100的访问目的地变更标记的当前值字段51102更新为0。

[0132] 图17为说明控制执行部410的动作的流程图。下面,对图17的各步骤进行说明。

[0133] (图17:步骤S410000)

[0134] 控制执行部410从共享区域51或辅助存储区域52获取控制运算中需要的数据。从哪一存储区域获取数据是在步骤S409001或S409003中指定的。向辅助存储区域52保存数据的期间内的访问目的地地址可以从保存目的地地址字段51403获取。

[0135] (图17:步骤S410001)

[0136] 控制执行部410使用步骤S410000中获取到的数据来实施控制运算。

[0137] (图17:步骤S410002)

[0138] 控制执行部410将控制运算的结果写入至步骤S410000中获取到数据的存储区域。即便在对辅助存储区域52写入运算结果的情况下,也会通过步骤S404006而对共享区域51反映该写入的数据,因此能够保持控制运算的一致性。

[0139] <实施方式1:总结>

[0140] 本实施方式1的ECU 1在对共享区域51实施存储诊断的期间内将诊断对象区域内的数据保存至辅助存储区域52,运算装置使用所保存的数据来实施控制运算。由此,即便在存储诊断中,也能提高运算装置的利用效率。

[0141] 本实施方式1的ECU 1在对辅助存储区域52保存数据的期间内对辅助存储区域52写入控制运算的结果,当存储诊断结束时,将该写入的运算结果回写至共享区域51。由此,能够在维持运算装置的利用效率的情况下实施存储诊断,而且能在存储诊断的前后保持控制运算的一致性。

[0142] <实施方式2>

[0143] 在实施方式1中,共享区域51和辅助存储区域52作为存储装置5的一部分而构成,但也可以将这些存储区域构成于互不相同的存储装置上。例如,可以将共享区域51构建于RAM上,并将辅助存储区域52构建于可靠性比RAM高的存储装置上。该另一存储装置可配置在ECU 1内,也可设置在ECU 1的外部而从ECU 1进行访问。

[0144] 作为可靠性比RAM高的存储装置,例如考虑具备排他控制功能的寄存存储器等。在该情况下,在任一运算装置对该寄存存储器写入数据的期间内,寄存存储器自身将拒绝来自其他运算装置的数据写入(或者读取和写入双方)。由此,能够防止由数据写入的竞争引起的存储区域的破坏,与一般的RAM相比,存储区域的可靠性提高。

[0145] 在将共享区域51与辅助存储区域52构成于互不相同的存储装置上的情况下,地址空间50000可以使用共通的地址空间。由此,仅通过访问目的地地址便能控制访问哪一存储装置,因此可以通过与实施方式1同样的处理来发挥同样的效果。

[0146] <实施方式3>

[0147] 在实施方式1~2中,对第1运算装置2实施对于共享区域51的存储诊断、第2运算装置3实施控制运算的情况进行了说明,但也可为两个运算装置均实施存储诊断和控制运算,也可为任一运算装置仅实施存储诊断且另一运算装置实施存储诊断和控制运算。

[0148] 例如,考虑对共享区域51内的存储区域写入数据的运算装置自行实施对于该存储区域的存储诊断。在对各存储区域写入数据的运算装置预先固定的情况下,该方法较为有用。或者,考虑对共享区域51内的存储区域写入数据的频率最高的运算装置自行实施对该存储区域的存储诊断。

[0149] <关于本发明的变形例>

[0150] 本发明包含各种变形例,并不限定于上述实施方式。例如,上述实施方式是为了以易于理解的方式说明本发明所作的详细说明,并非一定限于具备说明过的所有构成。此外,可以将某一实施方式的构成的一部分替换为其他实施方式的构成,此外,也可以对某一实施方式的构成加入其他实施方式的构成。此外,可以对各实施方式的构成的一部分进行进行其他构成的追加、删除、替换。

[0151] 在以上的实施方式中,ECU 1具备2个运算装置,但运算装置的个数并不限于2个。在1个组件内具备3个以上的处理器或处理器核心的系统、由具有处理器核心的多个组件构成的系统也是本发明的对象。

[0152] 在以上的实施方式中,作为ECU 1的构成,例示了图1,但也可以具备其他构成。例如,也可以具备用以保存数据的非易失性存储器(备份RAM)、各运算装置能够高速地访问的本地存储器、图1的示例以外的传感器等。

[0153] 图2中,作为地址空间50000所管理的存储区域,例示了共享区域51和辅助存储区域52,但也可以在地址空间50000上管理其他存储区域。例如,也可以在地址空间50000上管理各运算装置的本地存储器、外部存储装置、寄存器等的地址。

[0154] 共享区域51所存储的各表格所保持的数据中的至少一部分字段也可以存储在别的存储装置上。例如,也可以在各运算装置所具有的本地存储区域内存储这些字段。

[0155] 在以上的实施方式中,设置保存目的地地址字段51403作为存储对辅助存储区域52保存数据时的保存目的地地址的字段,但管理保存目的地地址的方法并不限于此。例如,可以使用距平常存储数据的地址的相对地址等来管理保存目的地地址。

[0156] 在以上的实施方式中,是利用例如0(正常)和1(异常)这2个值来表示存储诊断结果,但作为诊断结果加以存储的值并不限于此。例如,也可根据检测到异常的频率和累计次数而存储表示各不相同的诊断结果的值。

[0157] 在步骤S405000中,是通过产生对运算装置的中断处理来通知诊断开始或结束,但

通知方法并不限于此。例如,可以通过对地址空间50000内的某一存储区域存储通知诊断开始/结束的标记来进行通知。图3的第4行的标记为其示例。

[0158] 在以上的实施方式中,对通过能否写入测试用数据并读出相同值来实施存储诊断的情况进行了说明,但存储诊断方法并不限于此,可以使用其他适当的方法。

[0159] 符号说明

[0160] 1 车辆控制装置(ECU)、2 第1运算装置、3 第2运算装置、4 程序区域、401 第1运算装置控制部、402 诊断判定部、403 诊断管理部、404 前后关系管理部、405 通知部、406 诊断执行部、407 第2运算装置控制部、408 中断执行部、409 访问目的地设定部、410 控制执行部、5 存储装置、6 输入输出电路、7 节气门传感器、8 执行器。

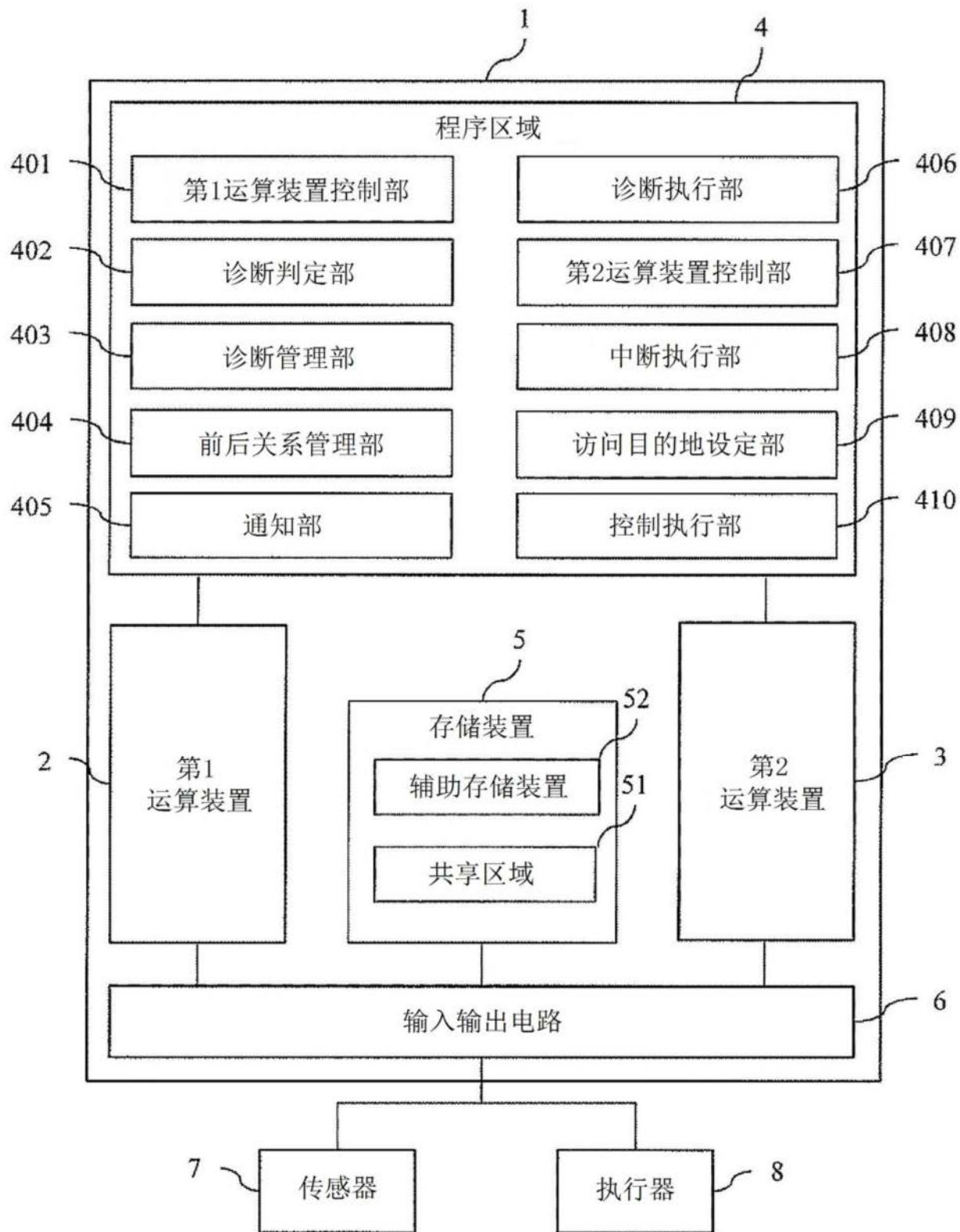


图1

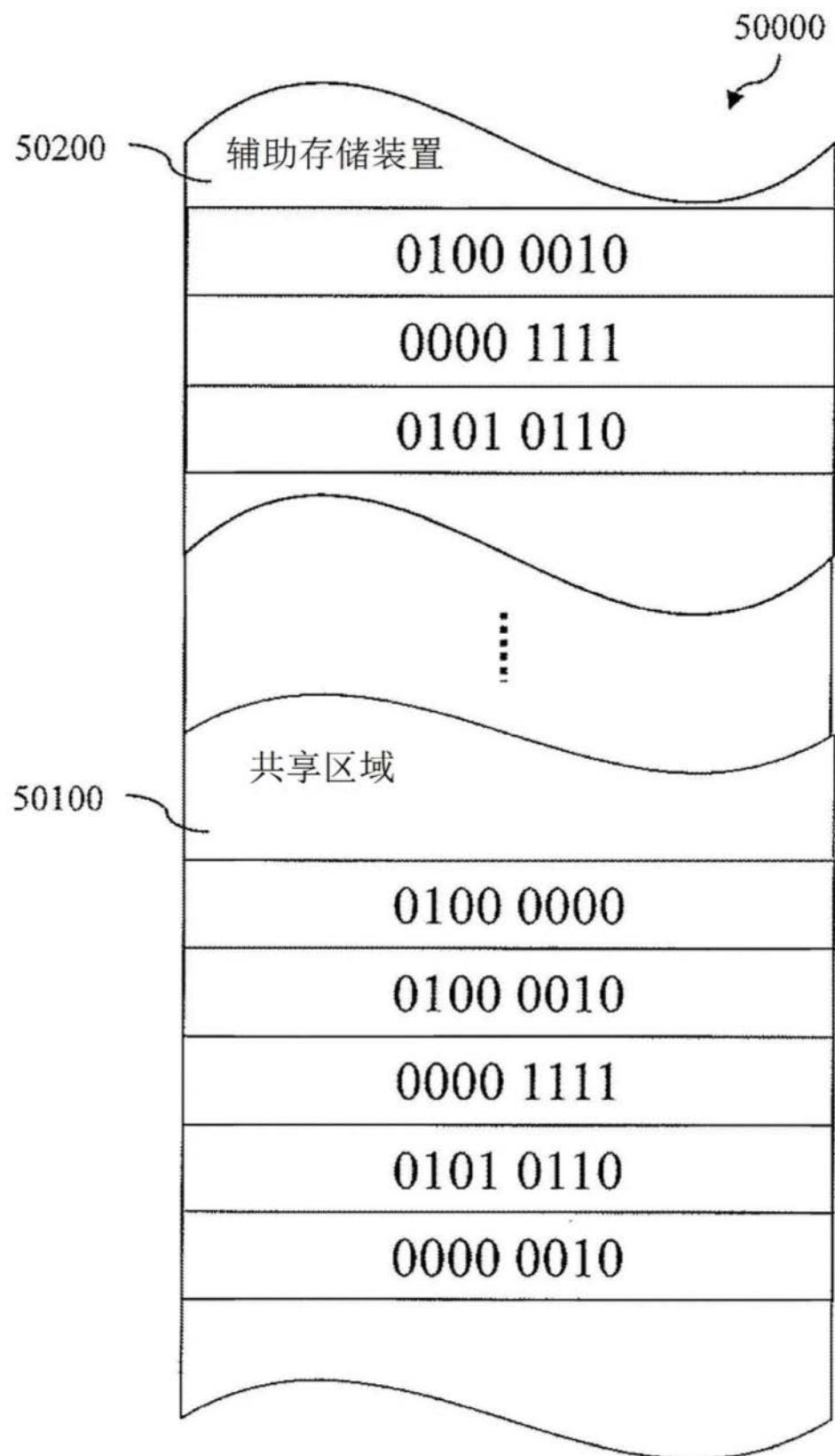


图2

The diagram illustrates the mapping of memory addresses to their current values. Three memory locations are shown at the top: 51100, 51101, and 51102. Curved arrows point from these addresses to the corresponding columns in a table below. The table has two columns: '名称' (Name) and '当前值' (Current Value). The data is as follows:

名称	当前值
诊断开始标记	1
诊断完成标记	0
访问目的地变更标记	0
核心间中断标记	1

图3

The diagram illustrates three memory locations: 51200, 51201, and 51202. Each location is represented by a small box with a curved arrow pointing to a corresponding row in a table below. The table has two columns: '名称' (Name) and '值' (Value). The rows are as follows:

名称	值
诊断执行周期	200
诊断用测试数据	0010 0011
可诊断地址数	32
开始地址	0010 0011
结束地址	0010 0011

图4

名称	当前值
定时计数器	20
诊断区域地址	0x FFFF FFF

图5

名称	地址	保存目的 地地址	数据	诊断结果
发动机转速				
扭矩变换				
点火时间				
喷射量				
:				

图6

The diagram illustrates a memory structure with five addresses: 52100, 52101, 52102, 52103, and 52104. Arrows point from each address to the corresponding column in the table below. The table has four columns: 名称 (Name), 地址 (Address), 保存源地址 (Source Address), and 保存源数据 (Source Data). The rows represent memory regions: 区域0, 区域1, 区域2, :, and 区域N.

名称	地址	保存源地址	保存源数据
区域0	0x FFFF FFFF	0x 0111 0000	
区域1			
区域2			
:			
区域N			

图7

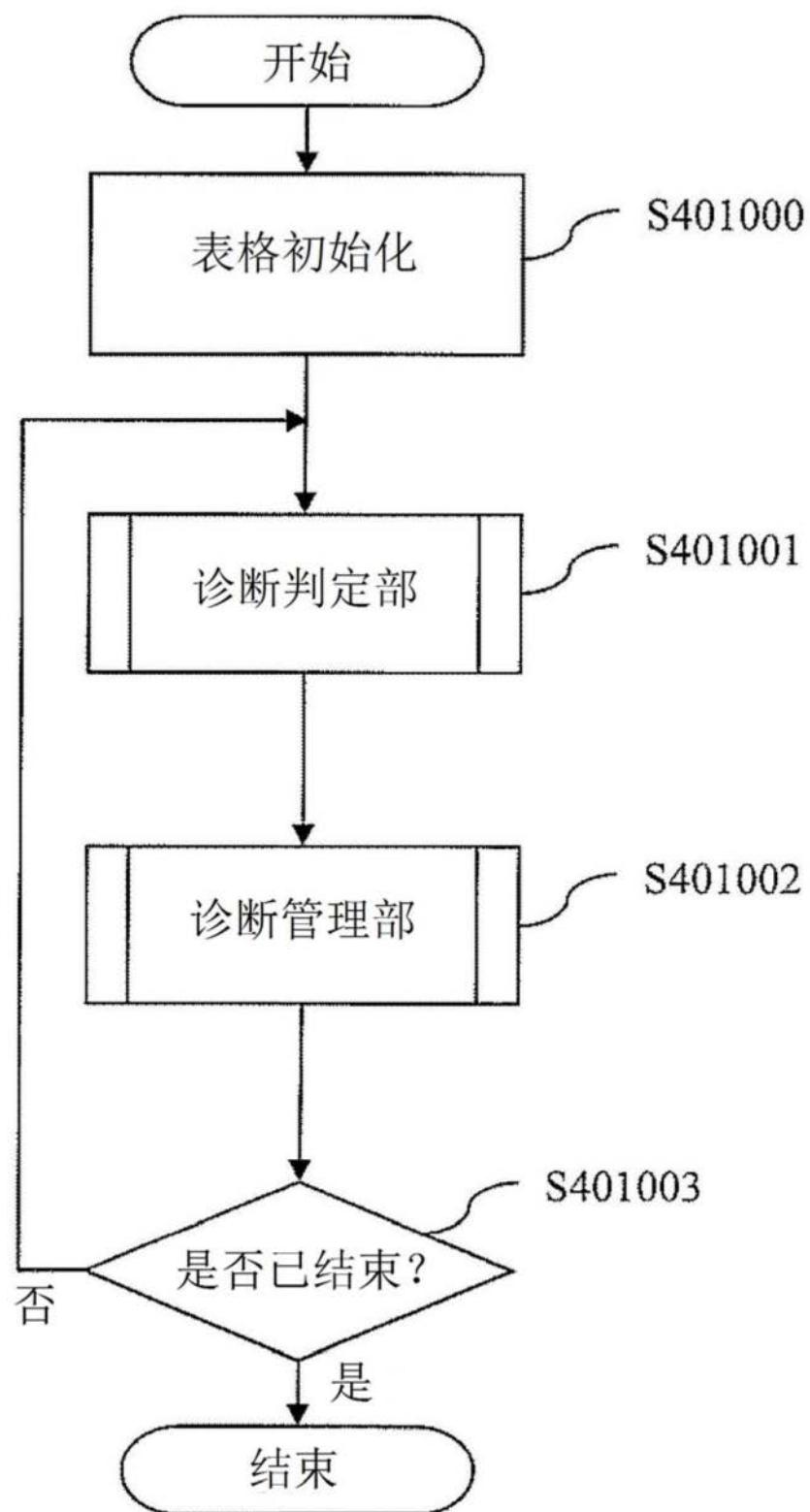


图8

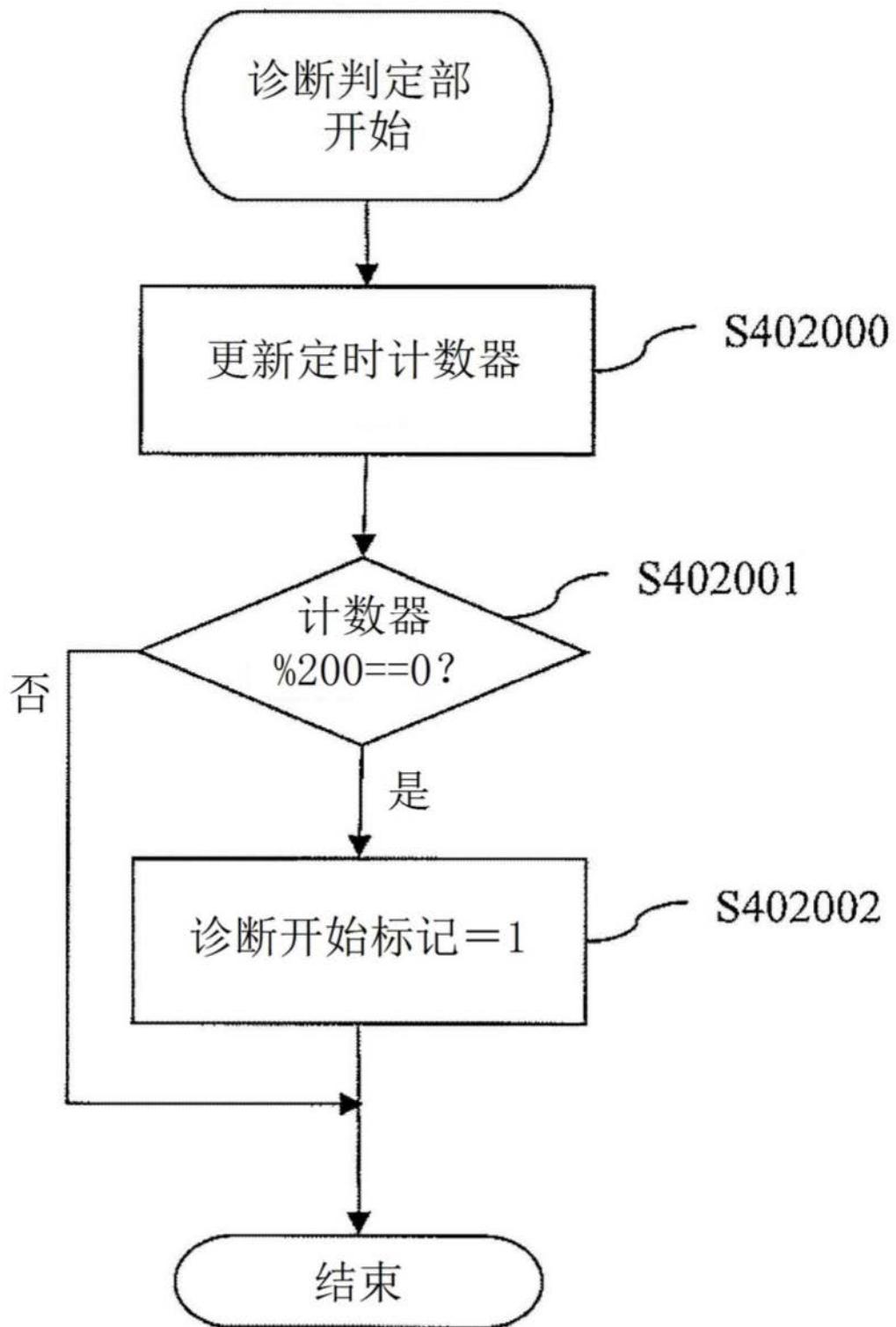


图9

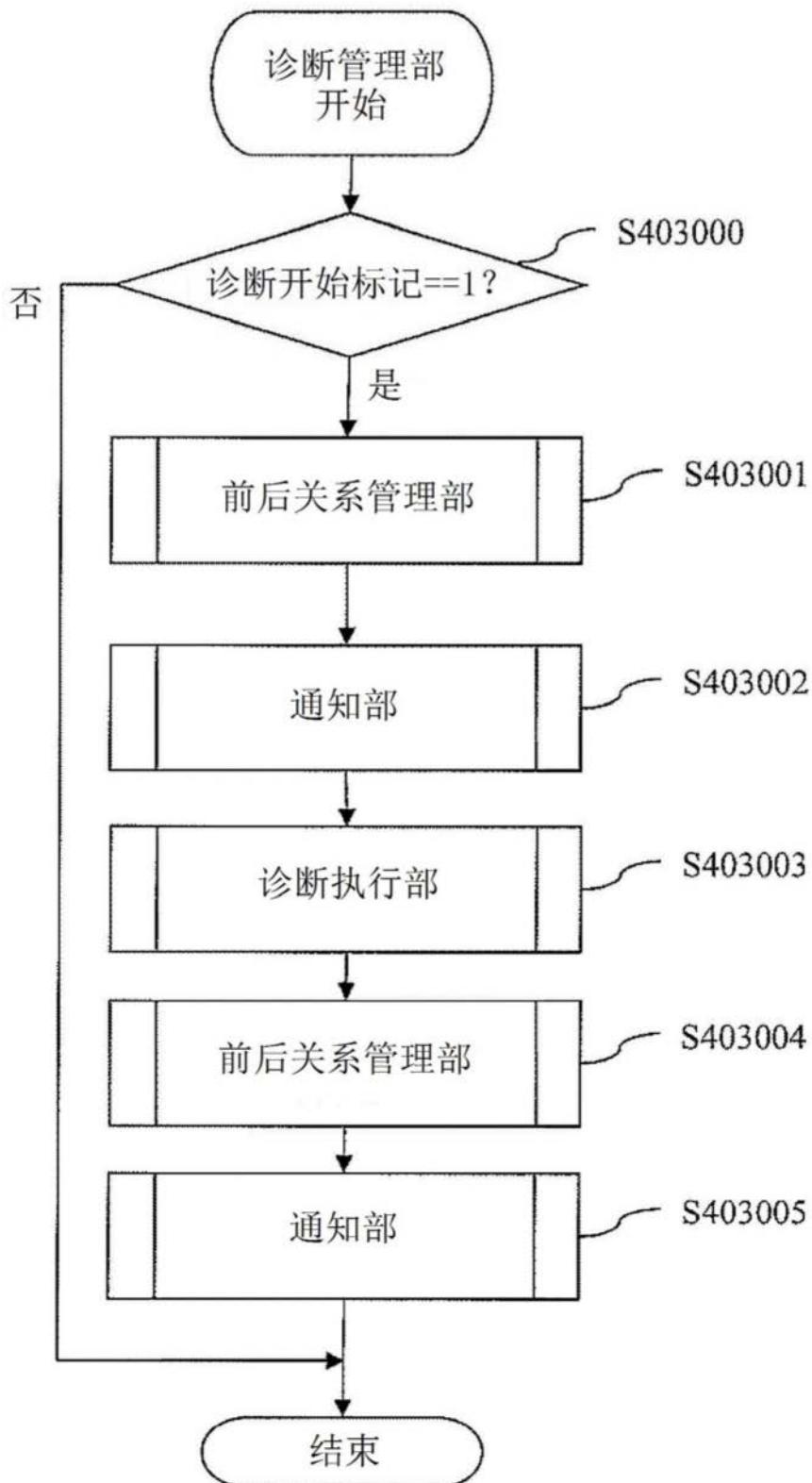


图10

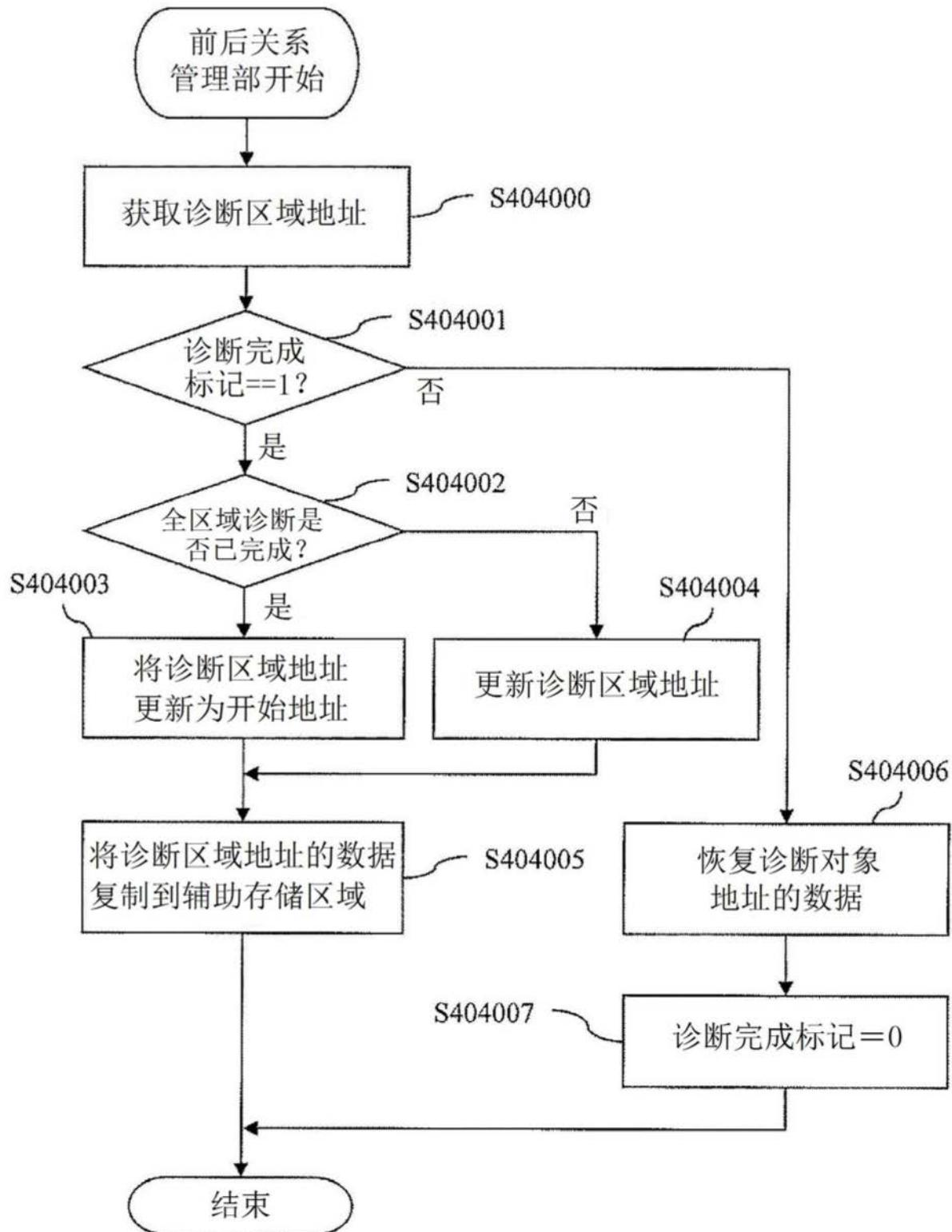


图11

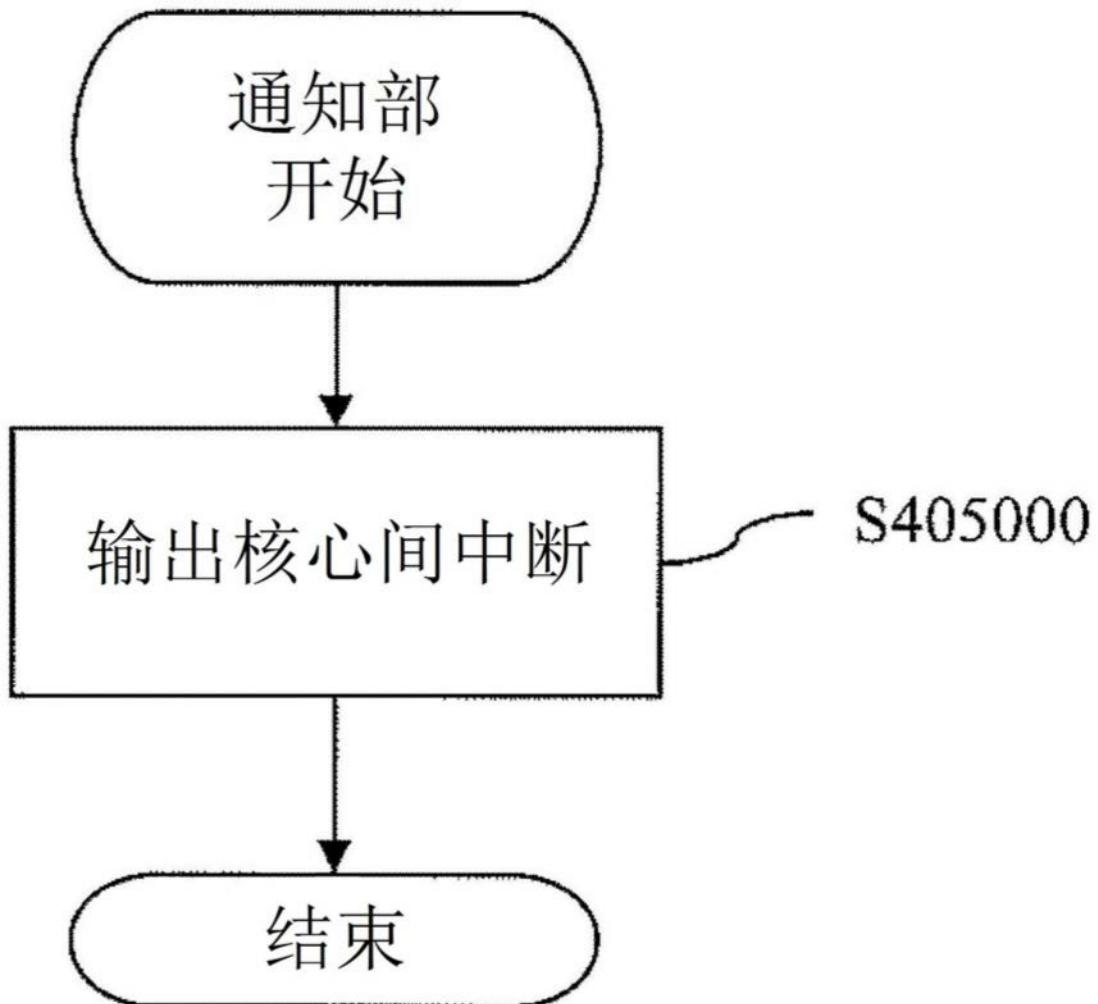


图12

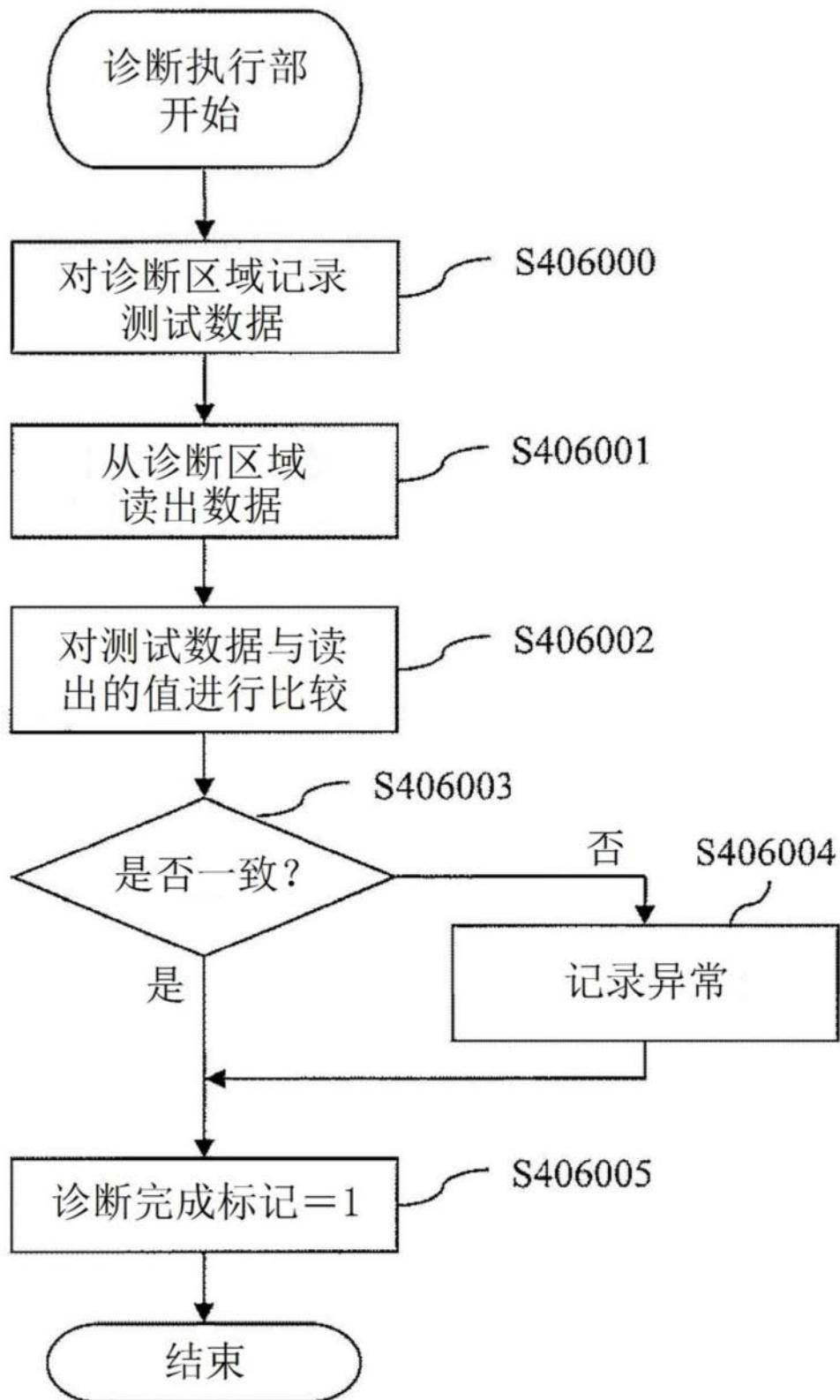


图13

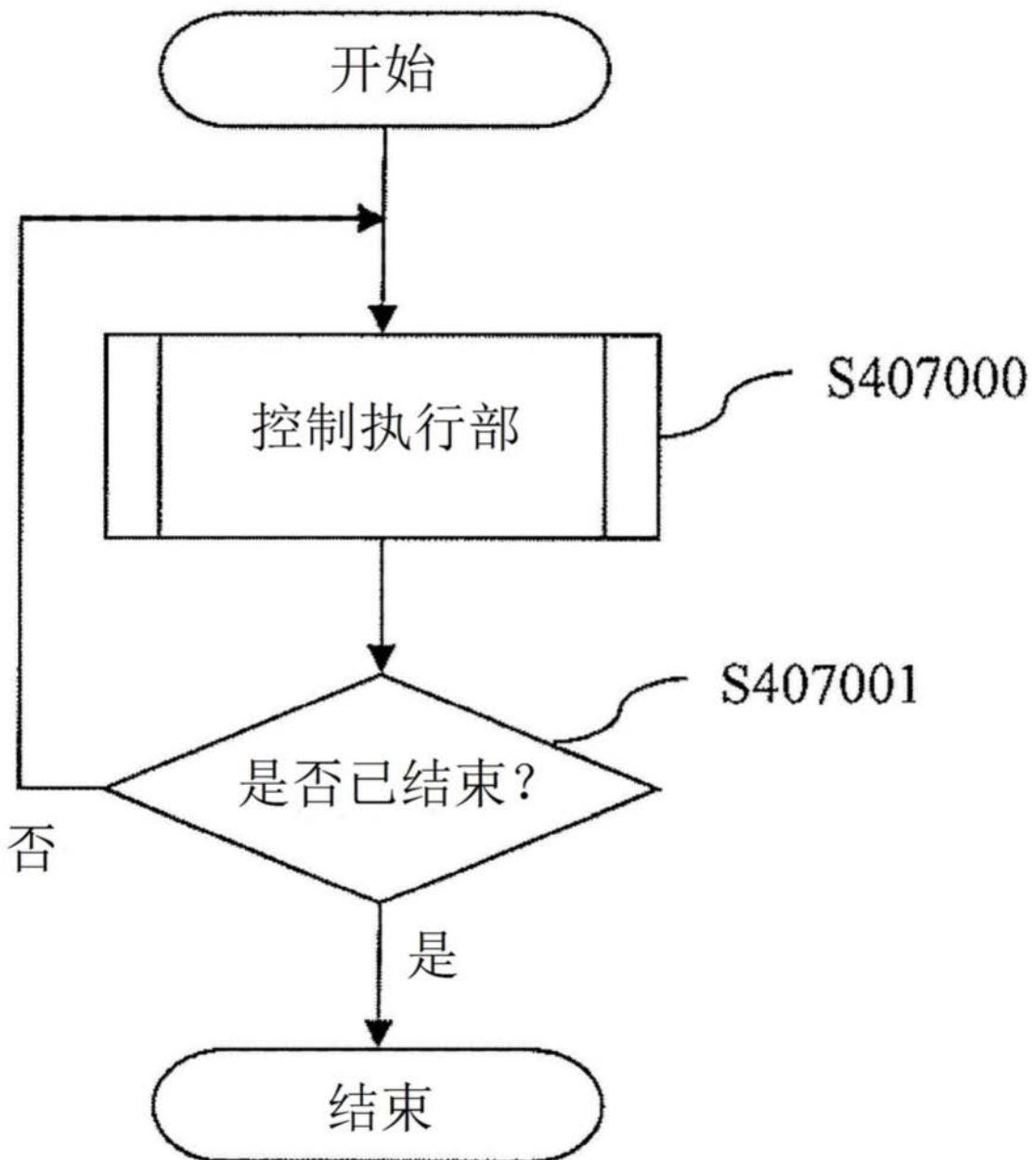


图14

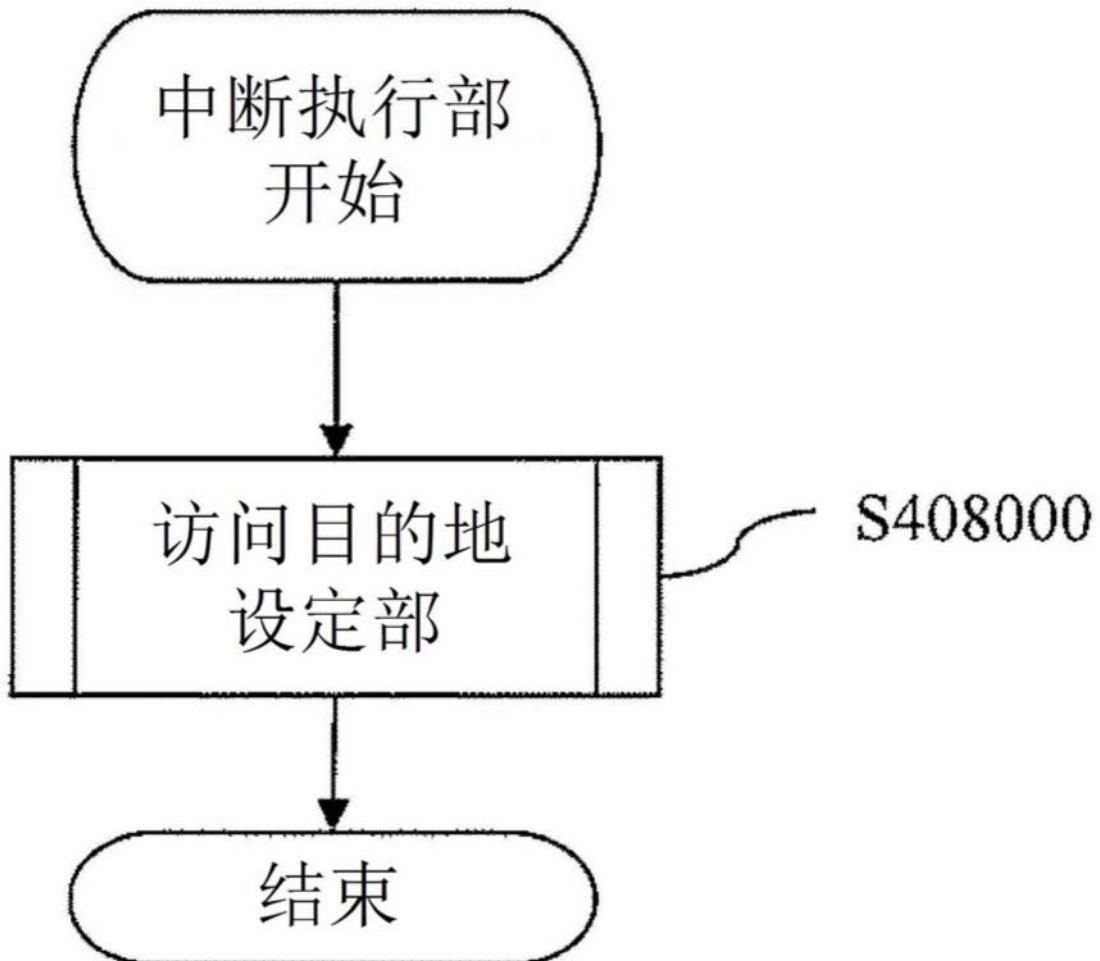


图15

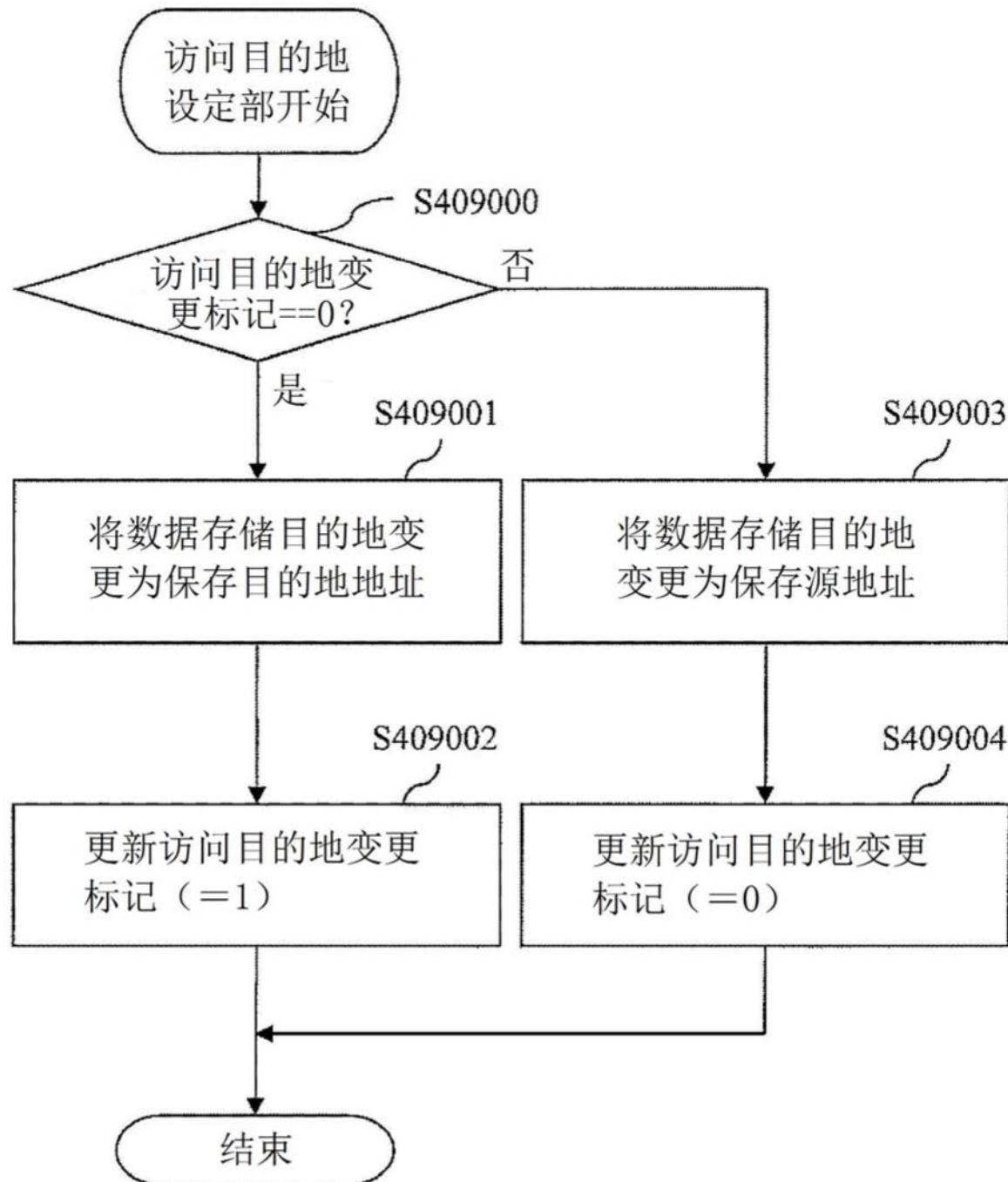


图16

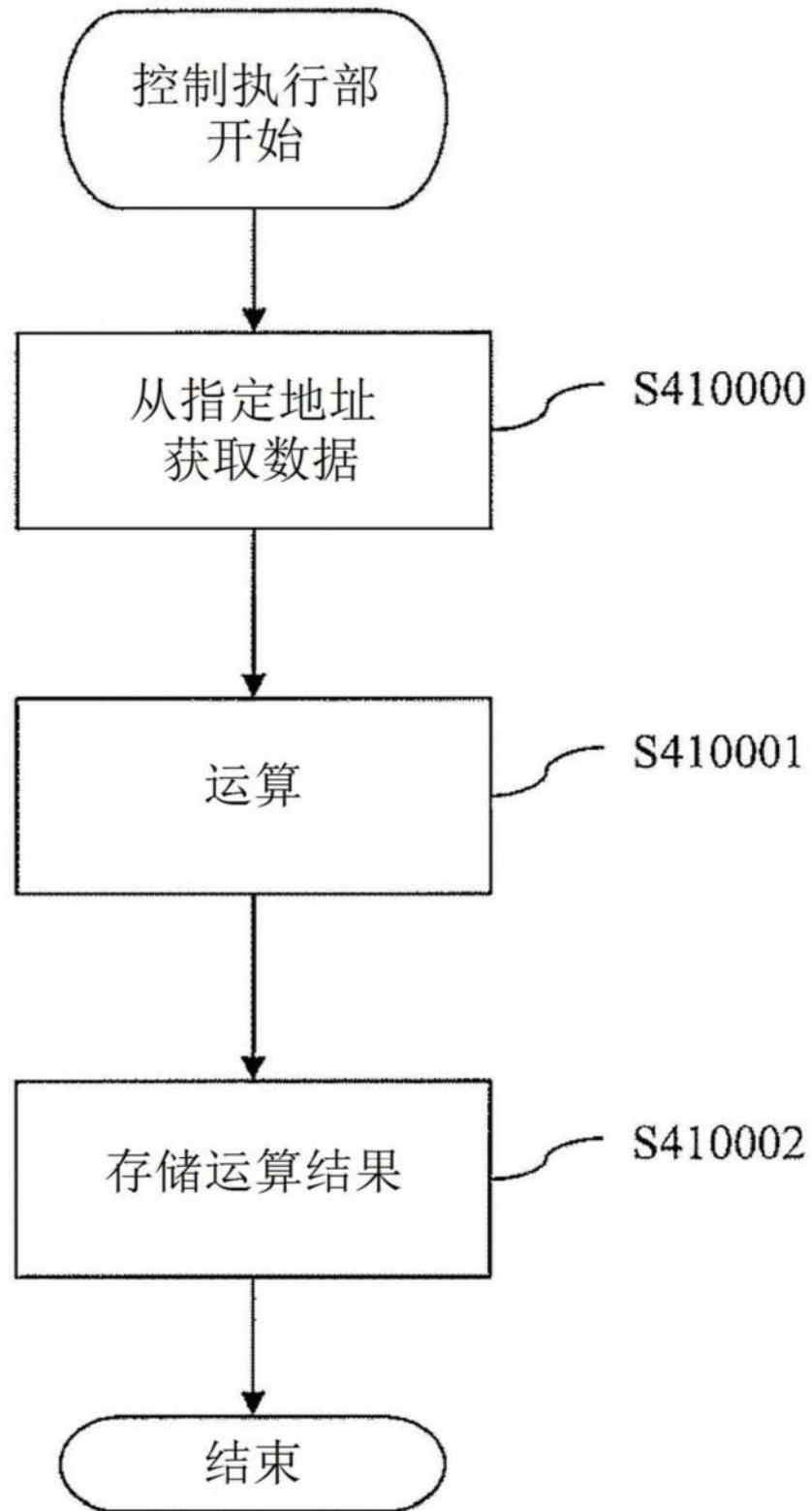


图17