



(12) 发明专利

(10) 授权公告号 CN 101329580 B

(45) 授权公告日 2012.02.29

(21) 申请号 200810130043.6

(22) 申请日 2006.06.09

(30) 优先权数据

2005-170275 2005.06.10 JP

2005-190874 2005.06.30 JP

(62) 分案原申请数据

200610091732.1 2006.06.09

(73) 专利权人 株式会社日立制作所

地址 日本东京

专利权人 日立信息控制系统有限公司

(72) 发明人 阪东明 小仓真 梅原敬

小林正光 长山久雄 益子直也

石川雅一 白石雅裕 小野塙明弘

远藤浩通 山田勉 船木觉

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 曲瑞

(51) Int. Cl.

G06F 11/16 (2006.01)

(56) 对比文件

JP 特开平 6-290066 A, 1994.10.18, 参见说明书第 0010-0023 段, 附图 1, 2.

WO 2005/045664 A2, 2005.05.19, 参见说明书第 5 页第 8 行 - 第 9 页第 21 行, 附图 1.

US 6779128 B1, 2004.08.17, 全文.

CN 1550988 A, 2004.12.01, 全文.

审查员 吴少鸿

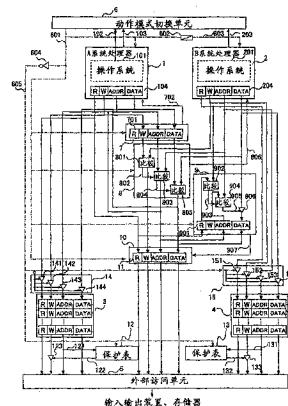
权利要求书 1 页 说明书 11 页 附图 6 页

(54) 发明名称

控制装置的任务管理装置和方法

(57) 摘要

本发明提供了一种控制装置的任务管理装置和方法,对于多个处理器,针对共同的数据处理对象,输入以可互换的方式运算的处理结果,在从任何一个处理器接收到开始信号后,对于向处理器输出运算指示信号的运算指示信号,输出为一个处理器和另一个处理器的动作定时不同。之后,将一个处理器与另一个处理器的运算效果进行比较。由于采用这种结构,对于多个处理器,可兼顾小型高性能化和安全性,并实现高可靠性。



1. 一种控制装置的任务管理装置,对于共同的数据处理对象,以由至少 2 个系统执行的处理结果为输入,所述处理结果是由所述至少 2 个系统以相互可互换的方式运算得到的,对于不同的数据处理对象,以由所述至少 2 个系统执行了不同的运算处理的处理结果为输入,其特征在于,所述任务管理装置具有:

动作模式切换单元,在从所述至少 2 个系统中的任意一个接收到对照模式开始指令后,以来自所述至少 2 个系统的处理器的准备完毕信号同时成立为条件向所述至少 2 个系统输出对照模式指令;以及

对照单元,对根据所述对照模式开始指令输出的、由所述至少 2 个系统执行的处理结果进行相对比较,在处理结果一致的情况下允许输出,

所述动作模式切换单元具有:

第 1 计时器,按照上述对照模式开始指令启动,利用来自所述至少 2 个系统的多个处理器的准备完毕信号复位;以及

第 2 计时器,利用来自所述至少 2 个系统的多个处理器的准备完毕信号而复位启动,

其中,所述第 1 计时器和所述第 2 计时器的输出超过设定范围时,进行异常输出。

2. 如权利要求 1 所述的控制装置的任务管理装置,其特征在于,在接收到表示所述不同运算处理已经结束的信号后,输出允许所述可互换的运算的信号。

3. 如权利要求 1 所述的控制装置的任务管理装置,其特征在于,在接收到表示所述可互换的运算已经结束的信号后,输出允许所述不同运算处理的信号。

4. 一种控制装置的任务管理方法,对于共同的数据处理对象,以由至少 2 个系统执行的处理结果为输入,所述处理结果是由所述至少 2 个系统以相互可互换的方式运算得到的,对于不同的数据处理对象,以由所述至少 2 个系统执行了不同的运算处理的处理结果为输入,在从所述至少 2 个系统中的任意一个接收到对照模式开始指令后,以来自所述至少 2 个系统的处理器的准备完毕信号同时成立为条件向所述至少 2 个系统输出对照模式指令,并对根据所述对照模式开始指令输出的、由所述至少 2 个系统执行的处理结果进行相对比较,在处理结果一致的情况下以允许输出,

其中,向所述至少 2 个系统输出对照模式指令的步骤中,还包括:

第 1 计时,按照上述对照模式开始指令启动第 1 计时器,利用来自所述至少 2 个系统的多个处理器的准备完毕信号复位所述第 1 计时器;以及

第 2 计时,利用来自所述至少 2 个系统的多个处理器的准备完毕信号而复位启动第 2 计时器,

其中,所述第 1 计时器和所述第 2 计时器的输出超过设定范围时,进行异常输出。

控制装置的任务管理装置和方法

[0001] 本申请是申请号为 200610091732.1、申请日为 2006 年 6 月 9 日、发明名称为“控制装置的任务管理装置和方法”的申请的分案申请。

技术领域

[0002] 本发明涉及控制装置的任务管理装置、输入输出控制装置、信息控制装置、控制装置的任务管理方法、输入输出控制方法以及信息控制方法。

背景技术

[0003] 以电子和信息领域的技术进步、在单一装置内追求功能的复杂化和复合化为原动力,可编程电子装置的应用范围变宽,同时,所要求的可靠性也提高。

[0004] 为实现一般所知的高可靠化,包括可编程电子装置的多重化和多个处理器的多重化。

[0005] 作为可编程电子装置的多重化,常用系统・备用系统的结构是已知的。通过在常用系统检测出故障时切换到备用系统,可以提高可用性。

[0006] 另一方面,特开 2004-234144 号公报中公开了作为使用多个处理器的可编程电子装置提高安全性的技术。

[0007] 另外,在原子能设备和化学设备等潜在危险性高的处理设备中,为了在万一的情况下减少对操作员和周边环境的影响,采取了利用隔壁等防护设备的被动对策和利用紧急停止装置等安全装置的主动对策。其中,安全装置等的控制单元由现有的继电器等电磁・机械单元来实现。但是,近年来,伴随着以可编程逻辑控制器 (PLC) 为代表的可编程控制设备的技术发展,将它们用作安全控制系统的控制单元的需求增加。

[0008] IEC61508-1 ~ 7, “Functional Safety of electrical/electronic/programmable electronic safety-related systems” part1-part7(简称为 IEC 61508) 是对应上述动向而发布的国际标准,它规定了在安全控制系统的一部分中使用电气 / 电子 / 可编程电子装置的情况下的必要条件。在 IEC61508 中,作为安全控制系统的能力尺度,定义了 Safety Integrity Level(SIL : 安全完整性等级),并规定了与从 1 到 4 的等级相对应水平的要求事项。它表示 SIL 越高,可以降低处理设备所具有的潜在危险性的程度越大。即,意味着在检测出处理设备的异常时,可以多可靠地实施规定的安全控制。

[0009] 要求安全控制装置在通常运转状态下为非活性,而在处理设备发生异常时立即活性。为此,经常执行自诊断、连续检查自身的健全性是非常重要的。在要求高 SIL 的安全控制系统中,为使由于未检测出的故障导致系统不动作的概率极小化,必须实施宽范围、高精度的自诊断。

[0010] 在 IEC61508 中,对构成安全控制装置的要素部件的每个种类,介绍了各自应用的自诊断技术,并以诊断率的形式来表示各种技术的有效性。诊断率表示各构成要素的所有故障中、采用该诊断技术时可检测出的故障的比例。例如,利用美国专利 6779128 号公报中记载的 RAM 诊断技术“abraham”,可主张最高 99% 的诊断率。

[0011] 另外,作为各构成要素之一的处理器的故障检测方法,使用多个处理器来监视相互的输出结果的一致性的方法是有效的。

[0012] 作为对多个处理器进行相互诊断的方法,各处理器同时执行同样的控制处理并确认其输出一致的方法是有效的。

[0013] 作为其代表性例子,如特开平6-290066号公报中所记载的那样,例举了下述方法:利用在使2个处理器同步执行的同时,通过使输入值也为相同信息而使输出一致的方法来确认处理器的健全性。

发明内容

[0014] 可编程电子装置所要求的可靠性的要素包括可用性和安全型,但在设备的控制中,可用性很重要,在设备的保护中,安全性很重要。由于这2个要素的实现方法是相悖(二律背反)的,因此,很难同时满足可用性和安全性。可将负责可用性的装置部分和负责安全性的装置部分分开,但是,这不仅使装置大型化,而且运转、维护作业的重复、复杂化还导致人的要素的可靠性降低。

[0015] 可编程电子装置所要求的可靠性的要素内包括可用性和安全性。在设备的控制中,可用性很重要,在设备的保护中,安全性很重要。这2个要素的实现方法相悖的部分很多。

[0016] 为此,目前将负责可用性的装置部分和负责安全性的装置部分分开,这是常识。因此,不仅使装置大型化,而且运转、维护作业的重复、复杂化还导致人的要素的可靠性降低。

[0017] 在要求高安全性的控制系统中,如特开平6-290066号公报(专利文献1)所记载,采用下述方法:通过对照多个处理器的输出来确认处理器的健全性,仅在一致的情况下,才输出到后级存储器和I/O。

[0018] 使用该方法,在使各处理器的动作定时一致的同时,对控制输入信息也进行核对,以向各处理器传递同一值,从而使输出一致。

[0019] 但是,随着控制对象变复杂,处理器也变为高性能,在由多个处理器构成的控制系统中,即便将1个时钟输入到多个处理器,也不能保证分别输出的时钟在频率、相位上是一样的。

[0020] 这样,由于在今后的由多个处理器构成的控制装置中,处理器输出的同步化变得困难,因此,在对多个处理器的输出进行对照来诊断处理器的健全性的过程中,需要有与处理器的输出同步、非同步无关地对输出进行对照的方法。另外,为了在处理器的输出之间进行比较,必须在多个处理器中执行1个处理,从而每台处理器的处理性能与通常的处理相比降低了一半。

[0021] 另一方面,在可编程电子设备中,除了安全性等可靠性之外,还要求高速地执行网络处理、或不要求在处理器的输出之间进行对照这样的可靠性的通常控制处理,以提高方便性。特别是,在希望高速地执行控制处理的情况下、或在希望执行处理大量数据的网络处理的情况下,有必要分割执行这些处理的可编程电子装置和执行要求可靠性的处理的可编程电子装置。

[0022] 本发明的目的在于提供可解决上述问题中任意一个的装置和方法。具体而言,本发明的目的在于,使用多个处理器,兼顾装置的小型高性能化和安全性,并实现高可靠性。

[0023] 本发明的目的在于提供了一种高可靠的可编程电子装置,其中使用多个处理器,兼顾装置的小型高性能化和安全性。

[0024] 为了达到上述目的,本发明构成为:对于共同的数据处理对象,输入以相互可互换的方式运算的、至少2个系统的处理结果,从所述至少2个系统之一接收到开始信号后,向所述至少2个系统输出运算指示信号。

[0025] 或者构成为,对于共同的数据处理对象,输入以相互可互换的方式运算的、至少2个系统的处理结果,对于不同的数据处理对象,输入由至少2个系统执行了不同运算处理后的处理结果,输出表示是由所述至少2个系统执行了不同运算处理、还是以可互换的方式执行了多重运算处理的切换信号,在所述信号表示由至少2个系统执行了不同运算处理的情况下,判断为允许所述至少2个系统的不同处理结果中的至少1个的输出。

[0026] 或者构成为:对于共同的数据处理对象,输入以可互换的方式运算的、至少2个系统的处理结果,将用于识别所述至少2个系统中规定系统的数据处理对象的识别数据存储到第1识别数据区域;将用于识别所述至少2个系统中任意另一个系统的数据处理对象的识别数据存储到第2识别数据区域;将作为所述至少2个系统中规定系统的处理结果的第1处理数据存储到第1处理数据区域;并将作为所述至少2个系统中任意另一个系统的处理结果的第2处理数据存储到第2处理数据区域内,其中,在对照所述第1识别数据和所述第2识别数据的同时,还对照所述第1处理数据和所述第2处理数据。

[0027] 或者是构成为:针对共同的数据处理对象,输入由至少2个系统以可互换的方式执行了多重运算处理后的处理结果,针对不同的数据处理对象,输入由至少2个系统执行了不同运算处理后的处理结果,并输出表示是由所述至少2个系统执行了不同运算处理、还是以可互换的方式执行了运算处理的切换信号。

[0028] 更具体地说,构成为:在具有输入输出装置、多个处理器和存储器的可编程电子装置中,具有多个处理器的动作模式切换单元、多个处理器的输出对照单元、以及由表规定的区域的存储器写入保护单元,响应动作模式切换单元的输出,使输出对照单元动作·停止,在输出对照单元停止时,使存储器写入保护单元动作。

[0029] 根据该结构,通过在输出对照单元停止时使多个处理器独立地动作,可以提高控制运算性能,同时还可以防止对安全产生影响的输出的误写入。并且可以防止在输出对照单元动作时由于处理器的错误运算而引起的危险侧信号输出,从而可以提高可靠性。

[0030] 另外构成为:在动作模式切换单元内具有计时器,第1计时器按照对照动作开始指令启动,利用来自多个处理器的对照动作开始信号复位。第2计时器利用来自多个处理器的对照动作开始信号而复位启动,在2个计时器的输出超过设定范围时,进行异常输出。

[0031] 利用该结构,可以检测出输出对照单元的停止,从而可以提高可靠性。

[0032] 另外构成为:具有用于诊断总线的粘合断线的总线诊断单元,以多个处理器的独立动作全部结束为条件,开始总线诊断,以诊断的正常结束为比较对照处理的动作开始条件。由此,不仅可以防止处理器的运算误动作,而且可以防止由于总线故障引起的危险侧信号输出,从而可以提高可靠性。

[0033] 该输出对照单元具有:来自多个处理器的独立动作结束检测单元;设置规定的时间差、向多个处理器发出对照动作程序的动作开始指令的单元;使对照程序的下一步骤的执行进行待机的指令输出单元;保持来自多个处理器的比较处理用信号的保持单元;以及

被保持在保持单元内的比较处理用信号的比较对照处理单元，该输出对照单元以多个处理器的独立动作全部结束为条件，开始程序动作。给予先行动作处理器的待机指令在向保持单元的输出结束时解除。另外构成为，给予后发动作处理器的待机指令在比较对照处理结束时解除。

[0034] 利用该结构，可以减少用于保持来自先行动作处理器的比较信号处理用信号的容量。另外，通过对运算、保持、比较处理的各动作执行流水线处理，可以实现高速化。

[0035] 或者构成为：在出现了可靠性相对较高的运算的请求的情况下，针对所述多个处理器中的至少一个，指示从可靠性相对较低的运算转而执行可靠性相对较高的运算，使多个处理器执行相同的运算，并对所述多个处理器的运算结果进行比较，基于所述比较结果，许可输出与所述处理器的运算有关的数据。

[0036] 如此，可以兼顾小型高性能化和安全性，同时可以实现高可靠性。

[0037] 另外，在安全型性可靠性之外，可以高速地执行网络处理或不要求在处理器的输出之间进行对照这样的可靠性的通常控制处理，从而可以提高便利性。

附图说明

[0038] 图 1 是整体结构图。

[0039] 图 2 是动作切换单元的细节图。

[0040] 图 3 是各部分动作说明图。

[0041] 图 4 是本发明的计算机系统的结构。

[0042] 图 5 是表示本发明的系统总线接口部的动作的状态转换图。

[0043] 图 6 是表示本发明的错误检测部的动作的状态转换图。

[0044] 图 7 是表示本发明的 2 个处理器的处理动作的时刻图。

具体实施方式

[0045] 接下来，参照附图来说明本发明的实施例。

[0046] 图 1 表示本发明的实施例的结构。

[0047] 首先，说明整体结构和各部分动作的概要。

[0048] 在该图中，可编程电子装置具有 2 台处理器。A 系统处理器 1 和 B 系统处理器 2 分别经由缓冲器 3、缓冲器 4 连接到外部访问单元 5，外部访问单元 5 与输入输出装置以及存储器连接。

[0049] A 系统处理器 1 和 B 系统处理器 2 借助动作模式切换单元 6，交互地在对照模式和独立模式这 2 种模式下动作。

[0050] 在对照模式时，在 A 系统处理器 1 和 B 系统处理器 2 上执行同一程序。在向外部访问单元 5 输出时，在由数据保持单元 7 和输出对照单元 8 确认了来自 A 系统处理器 1 和 B 系统处理器 2 的数据的一致性后输出。在从外部访问单元 5 输入时，利用数据同步单元 9 向 A 系统处理器 1 和 B 系统处理器 2 输入相同数据。输出数据与输入数据都经由对照缓冲器单元 10 输入输出至外部访问单元 5。

[0051] 数据保持单元 7、输出对照单元 8、同步单元 9、对照缓冲器单元 10 都以对照模式指令 601 为 H 电平为条件动作并进行信号输出。

[0052] 在独立模式时,在 A 系统处理器 1 和 B 系统处理器 2 上独立地执行不同的程序。A 系统处理器 1 的输入输出经由缓冲器 3 输入输出至外部单元 5。保护表 12 在独立模式时动作,在缓冲器 3 的地址数据处于预先定义的物理地址页的保护范围时,禁止写入。同样,B 系统处理器 2 的输入输出经由缓冲器 4 输入输出至外部单元,但由保护表 1~3 禁止保护范围的写入。

[0053] 输出开关单元 14 和 15 仅在 NOT 电路 604 的输出 605 为 H 电平时,将来自寄存器 104 和 204 的输入信号输出至输出缓冲器 3 和 4。

[0054] 以下,使用图 1 和图 3 来说明各部分的动作细节。

[0055] 开始,根据来自 A 系统处理器 1 的操作系统 101 的指示,向动作模式切换单元 6 发出 (H 电平) 对照模式开始指令 102(t1)。接收到对照模式开始指令 102 的动作模式切换单元 6 以来自 A 系统处理器的对照模式准备完毕信号 103 成立 (t2)、同样来自 B 系统处理器的准备完毕信号 203 同时成立 (H 电平) (t3) 为条件,输出 (H 电平) 对照模式指令 601(t4)。由此,A 系统处理器开始对照模式运算 (t5)。在对照模式运算 105 上升时,准备完毕信号被复位 (t6)。

[0056] 这里,对照模式准备完毕信号 103 和 203 是以各 A 系统处理器 1 和 B 系统处理器的独立模式运算结束以及高速缓冲存储器的清除为条件而被输出的。由此,可以不产生由于对照模式开始前的程序动作的不同而引起的运算时间的偏差。

[0057] 对照模式指令 601 直接输入到 A 系统处理器 1,另一方面,向 B 系统处理器 2 输入由时限电路 602 延迟了设定时间 (Td) 的信号 603(t7)。由此,B 系统处理器开始对照模式运算 (t8)。在对照模式运算 205 上升时,准备完毕信号被复位 (t9)。

[0058] 通过将延迟时间设定为动作模式切换单元 6 的 2 个总线周期,可在始终使 A 系统处理器的运算先行的同时,将由于对照所引起的运算延迟抑制为最小。

[0059] 接下来,说明输出数据的对照动作。

[0060] A 系统处理器 1 的寄存器 104 的输出被写入数据保持单元 7 的寄存器 701 中。在向寄存器 701 的写入结束时,解除写入等待信号 702,从而可以向 A 系统处理器的寄存器 104 执行再写入。

[0061] 另一方面,在利用输出对照单元 8 的比较电路 801 对 B 系统处理器 2 的寄存器 204 的写入控制信号 W 和寄存器 701 的写入控制信号 W 作出一致确认后,向对照缓冲器单元 10 的寄存器 11 输出写入控制信号 W。同时,解除等待信号 802,从而比较电路 803 可以输出。

[0062] 在利用比较电路 803 对保持在寄存器 701 内的、来自 A 系统处理器 1 的地址信号 701 和来自 B 系统处理器 2 的地址信号 204 作出了一致确认后,向对照缓冲器单元 10 的寄存器 11 输出地址信号。同时,解除等待信号 804,从而使比较电路 804 可以输出。

[0063] 在利用比较电路 805 对保持在寄存器 701 内的、来自 A 系统处理器 1 的数据 701 和来自 B 系统处理器 2 的数据 204 作出了一致确认后,向对照缓冲器单元 10 的寄存器 11 输出数据信号。同时,解除来自输出对照单元 8 的等待信号 806,从而可以执行 B 系统处理器 2 的寄存器 204 的再写入。

[0064] 接下来,说明输入数据的分配动作。A 系统处理器 1 的寄存器 104 的读入控制信号 R 经由对照缓冲器单元 10 的寄存器 11 的读入控制信号 R,被传送到外部访问单元 5,地址信号和数据信号经由寄存器 11 被读入寄存器 104。

[0065] 然后,寄存器 11 被传送到数据同步单元 9 的寄存器 901。利用比较电路 902 对寄存器 901 的读入控制信号 R 和 B 系统处理器 2 的寄存器 204 的读入控制信号 R 进行对照,在一致的情况下,解除等待信号 903。利用比较电路 904 对寄存器 901 的地址信号和寄存器 204 的地址信号进行对照。在两者一致的情况下,解除等待信号 905,从而门电路 906 动作,寄存器 901 的数据信号被传送到寄存器 204。传送数据后,等待信号 907 被解除,从而可重写对照缓冲器单元 10。

[0066] 在检测到 A 系统处理器的对照模式的运算结束 (t10)、B 系统处理器的对照模式的运算结束 (t11) 后,对照模式指令 601 变为 L 电平 (t12),由于 AND 电路 620,对照模式指令 630 也同时变为 L 电平。由此,开始独立动作模式 (t14)。

[0067] 在图 2 的实施例中,示出下述情况:在 A 系统处理器独立模式运算 106 结束 (t14)、对照模式开始指令 102 再次上升的时刻 (t15),B 系统处理器独立运算模式 206 继续。在这种情况下,在检测出 B 系统处理器独立模式运算 206 结束 (t16) 后,开始对照电路的自诊断动作 (t17)。自诊断动作结束后,A 系统处理器对照模式准备完毕 103 和 B 系统处理器对照模式准备完毕 203 变为 H 电平 (t18)。由此,通过在对照模式运算之前执行对照电路的自诊断动作,具有可提高对照电路的安全性的效果。

[0068] 输出开关单元 14 和 15 由各个门电路 141-144、151-154 构成,在对照模式指令 601 的反转信号 605 为 H 电平时,可以执行寄存器 104 和 204 以及缓冲器 3 和缓冲器 4 之间的输入输出。

[0069] 保护表 12 和 13 构成为:在对照模式指令 601 的反转信号 605 为 H 电平时动作,参照地址信号 121 和 131,在处于规定的物理地址范围时输出访问保护信号 122 和 132,利用带否定电路的门电路 123 和 133 来防止向保护范围的写入。

[0070] 由此,在独立模式时的运算中,可使对照模式的运算结果不受影响地得到保护。

[0071] 图 2 表示本发明的其他实施例。

[0072] 利用由输入了来自 A 系统处理器 1 的操作系统 101 的对照模式开始指令 102 的上升检测器 606 检测出的置位脉冲信号 607,计时器 609 启动。将来自 A 系统处理器的对照模式准备完毕信号 103 以及来自 B 系统处理器的 203 输入 AND 电路 607,利用该输出信号 608,计时器 609 复位。将计时器 609 的输出 610 输入比较器 611,在输出 610 超过设定范围时,输出异常输出 612。由此检测出对照动作的启动阻塞。

[0073] 设置计时器 615,该计时器 615 利用由输入了 AND 电路 607 的输出信号 608 的上升检测器 613 输出的脉冲信号复位并同时启动。

[0074] 将计时器 615 的输出 616 输入比较器 617,在输出 616 超过设定范围时,输出异常输出 618。由此检测出对照运算周期的异常。

[0075] 在以上的实施方式中,可以构成为:具有由于诊断总线的粘合断线的总线诊断单元,以多个处理器的独立动作全部结束为条件,开始总线诊断,诊断的正常结束是比较对照处理的动作开始条件。由此,不仅可以防止处理器的运算误动作,还可以防止由于总线故障引起的危险侧信号输出,从而可提高可靠性。

[0076] 该输出对照单元具有:来自多个处理器的独立动作结束检测单元;设置规定的时间差、向多个处理器发出对照动作程序的动作开始指令的单元;使对照程序的下一步骤的执行进行待机的指令输出单元;保持来自多个处理器的比较处理用信号的保持单元;以及

被保持在保持单元内的比较处理用信号的比较对照处理单元,该输出对照单元以多个处理器的独立动作全部结束为条件,开始程序动作。给予先行动作处理器的待机指令在向保持单元的输出结束时解除。另外构成为,给予后发动作处理器的待机指令在比较对照处理结束时解除。

[0077] 利用该结构,可以减少用于保持来自先行动作处理器的比较信号处理用信号的容量。另外,通过对运算、保持、比较处理的各动作执行流水线处理,可以实现高速化。

[0078] 接着说明其他实施方式,但在说明时进行概念性说明时,实现具有以下功能的CPU输出对照:在需要高可靠和高性能的控制装置中,在需要高可靠的情况下,多个处理器动作,对其输出进行对照,对处理器进行诊断,从而确认处理器的健全性的功能;以及处理器执行独立的处理、实现性能提高的功能。

[0079] 更具体地说,特征在于以下几点。

[0080] (1) 在一个控制装置内具有多个处理器,并且具有:判断每个处理器所要访问的I/O是否期待高可靠控制结果的单元;比较多个处理器的输出并判定一致的单元;以及至少仅在多个处理器的输出结果一致的情况下,才许可处理器对期待高可靠控制结果的I/O的访问,在单独的处理器执行访问的情况下,使其等待,直到其他处理器输出同一输出结果的单元。

[0081] (2) 1个控制装置内具有的多个处理器具有:处理并执行针对每个处理器不同的功能的单元;以及用于从处理器中断其他处理器的处理的单元。

[0082] (3) 执行向要求可靠性的I/O输出的处理的处理器具有:使用中断其他处理器中的处理的单元,中断其他处理器的处理,执行向要求可靠性的I/O输出的处理的单元。

[0083] (实施例 1)

[0084] 以下使用附图来说明本发明的实施例。作为本发明第1实施方式的控制系统的结构显示在图4中。这里,就处理器是2个的情况进行说明,但在实际的实施方式中,处理器的台数没有限制,本发明不受其制约。

[0085] 这里说明的控制系统以连接到存储器电路为前提,从而没有特别明示。

[0086] A系统处理器1001执行控制任务,B系统处理器1003执行通信任务。另外,A系统处理器1001和B系统处理器1003不必按同一频率的同一相位来执行同步动作。

[0087] A系统处理器1001输出由地址信号、数据信号构成的A系统处理器总线1050。另外,A系统处理器1001在总线访问开始时,发出总线开始信号1051。A系统接口部1002持续发出A系统等待信号1052,直到A系统总线准备就绪信号1067或A系统中断控制准备就绪信号1068被发出。在A系统处理器1001执行写入访问的情况下,A系统处理器1001在A系统等待信号1052发出期间,向A系统处理器总线1050持续输出地址和数据。在A系统处理器执行读出的情况下,A系统处理器1001在A系统等待信号1052发出期间,向A系统处理器总线1050输出地址,并继续等待读出数据,A系统等待信号1052取消时,将A系统处理器总线1050上的数据值作为读出值取入。

[0088] B系统也同样,B系统处理器1003输出由地址信号、数据信号构成的B系统处理器总线1055。另外,B系统处理器1003在总线访问开始时,发出总线开始信号1057。B系统接口部1004在B系统总线准备就绪信号1065或B系统中断控制准备就绪信号1069被发出之前,持续发出B系统等待信号1056。在B系统处理器1003执行写入访问的情况下,B

系统处理器 1003 在等待信号 1057 发出期间,向 B 系统处理器总线 1055 持续输出地址和数据。在 B 系统处理器 1003 执行读出的情况下,B 系统处理器 1003 在等待信号 1056 发出期间,向 B 系统处理器总线 1055 输出地址,继续等待读出数据,在等待信号 1056 取消时,将 B 系统处理器总线 1055 上的数据值作为读出值取入。

[0089] A 系统区域判断部 1013 具有根据 A 系统处理器总线 1050 的地址值,来判断当前访问的设备是否是高可靠 IO 1018 的功能,在 A 系统处理器 1001 访问高可靠 IO 1018 的情况下,发出 A 系统高可靠访问信号 1060。

[0090] B 系统区域判断部 1014 具有根据 B 系统处理器总线 1055 的地址值,来判断当前访问的设备是否是高可靠 IO 1018 的功能,在 B 系统处理器 1003 访问高可靠 IO 1018 的情况下,发出 B 系统高可靠访问信号 1061。

[0091] 比较部 1015 具有对 A 系统处理器总线 1050 和 B 系统处理器总线 1055 进行比较的功能,对 A 系统处理器总线 1050 和 B 系统处理器总线 1055 的地址和写还是读的访问类型、写入数据进行比较,在一致的情况下,发出比较结果一致信号 1062。

[0092] 系统总线接口部 1016 根据 A 系统处理器总线 1050、B 系统处理器总线 1055、A 系统高可靠访问信号 1060、B 系统高可靠访问信号 1061、比较结果一致信号 1062,经由系统总线 1017,访问高可靠 IO1018、普通 IO 1020、网络 IO 1022。

[0093] 高可靠 IO 1018 连接到要求可靠性的输入输出装置 1019。

[0094] 普通 IO 1020 连接到普通的可靠性就可以的输入输出装置 1021。

[0095] 网络 IO 1022 是与网络 1023 的接口,是在需要接收处理等由处理器执行的处理的情况下,发出网络中断 1066,期待来自处理器的处理的装置。

[0096] 错误检测部 1012 具有以下功能:根据 A 系统高可靠访问信号 1060、B 系统高可靠访问信号 1061、比较结果一致信号 1062,来判断 A 系统处理器 1001 和 B 系统处理器 1003 是正常动作,还是发生故障。在判断为发生故障的情况下,发出故障报告信号 1064。

[0097] 中断控制部 1005 具有控制给予 A 系统处理器 1001 的 A 系统中断信号 1053 和给予 B 系统处理器 1003 的中断信号 1054 的功能,由用于发出 A 系统中断信号 1053 的 A 系统中断请求寄存器 1006、以及表示中断要因的 A 系统中断要因寄存器 1008 构成。另外,还具有用于发出 B 系统中断信号 1054 的 B 系统中断请求寄存器 1007、以及表示中断要因的 B 系统中断要因寄存器 1009。

[0098] 构成为可独立地向 A 系统处理器 1001、B 系统处理器 1003 提供中断的结构。另外,A 系统中断请求寄存器 1006、A 系统中断要因寄存器 1008、B 系统中断请求寄存器 1007、B 系统中断要因寄存器 1009 构成为可以从 A 系统处理器 1001 和 B 系统处理器 1003 进行访问的结构。

[0099] 另外,从外部输入故障报告信号 1064 以及网络中断 1066。A 系统中断信号 1053 传送从 A 系统中断请求寄存器 1006 发生的中断或由故障报告信号 1064 发生的中断。这里,由故障报告信号 1064 发生的中断优先于从 A 系统中断请求寄存器 1006 发生的中断。

[0100] B 系统中断信号 1054 传递从 B 系统中断请求寄存器 1007 发生的中断或由网络中断 1066、故障报告信号 1064 发生的中断。这里,由故障报告信号 1064 发生的中断优先于从 B 系统中断请求寄存器 1007 发生的中断,从 B 系统中断请求寄存器 1007 发生的中断优先于网络中断 1066。即,若按优先顺序排列,则为由故障报告信号 1064 产生的中断、从 B 系

统中断请求寄存器 1007 发生的中断、网络中断 1066 这样的顺序。

[0101] 图 5 是说明系统总线接口部 1016 的动作状态的状态转换图。

[0102] 系统总线接口部 1016 具有图 5 所示的 4 个状态。

[0103] 状态 1200 表示空闲状态, 表示 A 系统处理器 1001、B 系统处理器 1003 都没有访问系统总线 1017 的状态。

[0104] 状态 1201 表示 A 系统处理器访问状态, 表示 A 系统处理器 1001 访问普通 IO 1018。

[0105] 状态 1202 表示 B 系统处理器访问状态, 表示 B 系统处理器 1003 访问网络 IO 1022。

[0106] 状态 1203 表示 A 系统和 B 系统处理器访问高可靠 IO 1018 的状态。

[0107] 从状态 1200 转换到状态 1201 的转换条件 1204 在 A 系统处理器 1001 开始执行访问且 A 系统高可靠访问信号 1060 没有发出的条件下成立。

[0108] 从状态 1200 转换到状态 1202 的转换条件 1206 在 A 系统处理器 1001 没有开始执行访问、B 系统处理器 1003 开始执行访问、且 B 系统高可靠访问信号 1061 没有发出的条件下成立。

[0109] 从状态 1200 转换到状态 1203 的转换条件 1208 在 A 系统处理器 1001 开始执行访问、A 系统高可靠访问信号 1060 发出、且 B 系统处理器 1003 开始执行访问、B 系统高可靠访问信号 1061 发出、且比较结果一致信号 1062 发出的条件下成立。该条件表示 A 系统处理器 1001、B 系统处理器 1003 一起访问高可靠 IO 1018 的同一地址。

[0110] 转换条件 1205 由于从普通 IO 1020 经由系统总线 1017 发出的表示访问结束的报告而成立; 转换条件 1207 由于从网络 IO 1022 经由系统总线 1017 发出的表示访问结束的报告而成立; 转换条件 1209 由于从高可靠 IO 1018 经由系统总线 1017 发出的表示访问结束的报告而成立。

[0111] 由于该状态转换, 系统总线接口部 1016 依据 A 系统区域判断部 1013、B 系统区域判断部 1014 的判断结果, 应 A 系统处理器 1001、B 系统处理器 1003 的请求, 允许对连接到系统总线 1017 上的高可靠 IO 1018、普通 IO 1020、网络 IO 1022 中任何一个的访问。特别是, 对于高可靠 IO 1018 的访问, 必须使表示 A 系统处理器 1001、B 系统处理器 1003 共同访问高可靠 IO 1018 的同一地址的转换条件 1208 成立。

[0112] 另外, A 系统总线准备就绪信号 1067 在转换条件 1205 和转换条件 1209 成立时发出, B 系统总线准备就绪信号 1065 在转换条件 1207 和转换条件 1209 成立时发出。

[0113] 图 6 是表示错误检测部 1012 的动作的状态转换图。

[0114] 状态 1300 为空闲状态, 表示 A 系统处理器、B 系统处理器都不访问高可靠 IO 1018 的状态。

[0115] 状态 1301 是 A 系统处理器 1001 访问高可靠 IO 1018, 在 B 系统处理器 1003 输出与自身处理器的输出相同的输出之前一直等待的状态。

[0116] 状态 1302 是 A 系统处理器 1001 访问高可靠 IO 1018, 在 B 系统处理器 1003 输出与自身处理器的输出相同的输出之前待机, 但经过一定时间后, 判断为超时错误的状态。

[0117] 状态 1303 是 A 系统处理器 1001 和 B 系统处理器 1003 虽然访问了高可靠 IO 1018, 但各个处理器的输出不一致、判断为错误的状态。

[0118] 状态 1305 是 B 系统处理器 1003 访问高可靠 IO 1018, 在 A 系统处理器 1001 输出与自身处理器的输出相同的输出之前一直等待的状态。

[0119] 状态 1304 是 B 系统处理器 1003 访问高可靠 IO 1018，在 A 系统处理器 1001 输出与自身处理器的输出相同的输出之前一直等待，但经过一定时间后，判断为超时错误的状态。

[0120] 转换条件 1306 在 A 系统高可靠访问信号 1060 发出、B 系统高可靠访问信号 1061 没有发出的条件下成立。

[0121] 转换条件 1307 在 B 系统高可靠访问信号 1061 发出、比较结果一致信号 1062 发出的条件下成立。

[0122] 转换条件 1309 在 B 系统高可靠访问信号 1061 发出、比较结果一致信号 1062 没有发出的条件下成立。

[0123] 转换条件 1308 在转换条件 1307、1309 不成立、经过一定时间的条件下成立。

[0124] 转换条件 1316 在 B 系统高可靠访问信号 1061 发出、A 系统高可靠访问信号 1060 没有发出的条件下成立。

[0125] 转换条件 1315 在 A 系统高可靠访问信号 1060 发出、比较结果一致信号 1062 发出的条件下成立。

[0126] 转换条件 1312 在 A 系统高可靠访问信号 1060 发出、B 系统高可靠访问信号 1061 发出、比较结果一致信号 1062 没有发出的条件下成立。

[0127] 转换条件 1313 在转换条件 1315、1312 不成立、经过一定时间的条件下成立。

[0128] 转换条件 1317 在 A 系统高可靠访问信号 1060 发出、B 系统高可靠访问信号 1061 发出、比较结果一致信号 1062 没有发出的条件下成立。

[0129] 转换条件 1310、1311、1314 始终成立，这意味着在向状态 1302、1303、1304 转换后的下一个周期中，向状态 1300 转换。

[0130] 错误检测部 1012 管理 A 系统处理器 1001 和 B 系统处理器 1003 对高可靠 IO 1018 的访问状态，对高可靠 IO 1018 执行访问的处理器在自身处理器的输出与其他系统的处理器的输出不一致的情况下，或其他处理器在一定时间内不对高可靠 IO 1018 进行访问的情况下，转换到状态 1302、1303、1304，在该状态 1302、1303、1304 时发出故障报告信号 1064。

[0131] 高可靠 IO 1018 在故障报告信号 1064 被发出后，识别出发生了故障，并将输出切换到安全状态。这里，所谓安全状态包括继续保持当前输出的情况是安全状态的情况、或与切断了电源的情况相同的状态是安全的情况，随每个执行控制的对象而不同。另外，在发生故障后，错误检测部 1012 使用中断信号 1053、1054 向 A 系统处理器 1001 和 B 系统处理器 1003 报告故障中断。接收到故障中断的处理器迅速中断现状的处理，并执行故障处理。

[0132] 图 7 是表示 A 系统处理器 1001 和 B 系统处理器 1003 正常时的处理动作的时刻图。

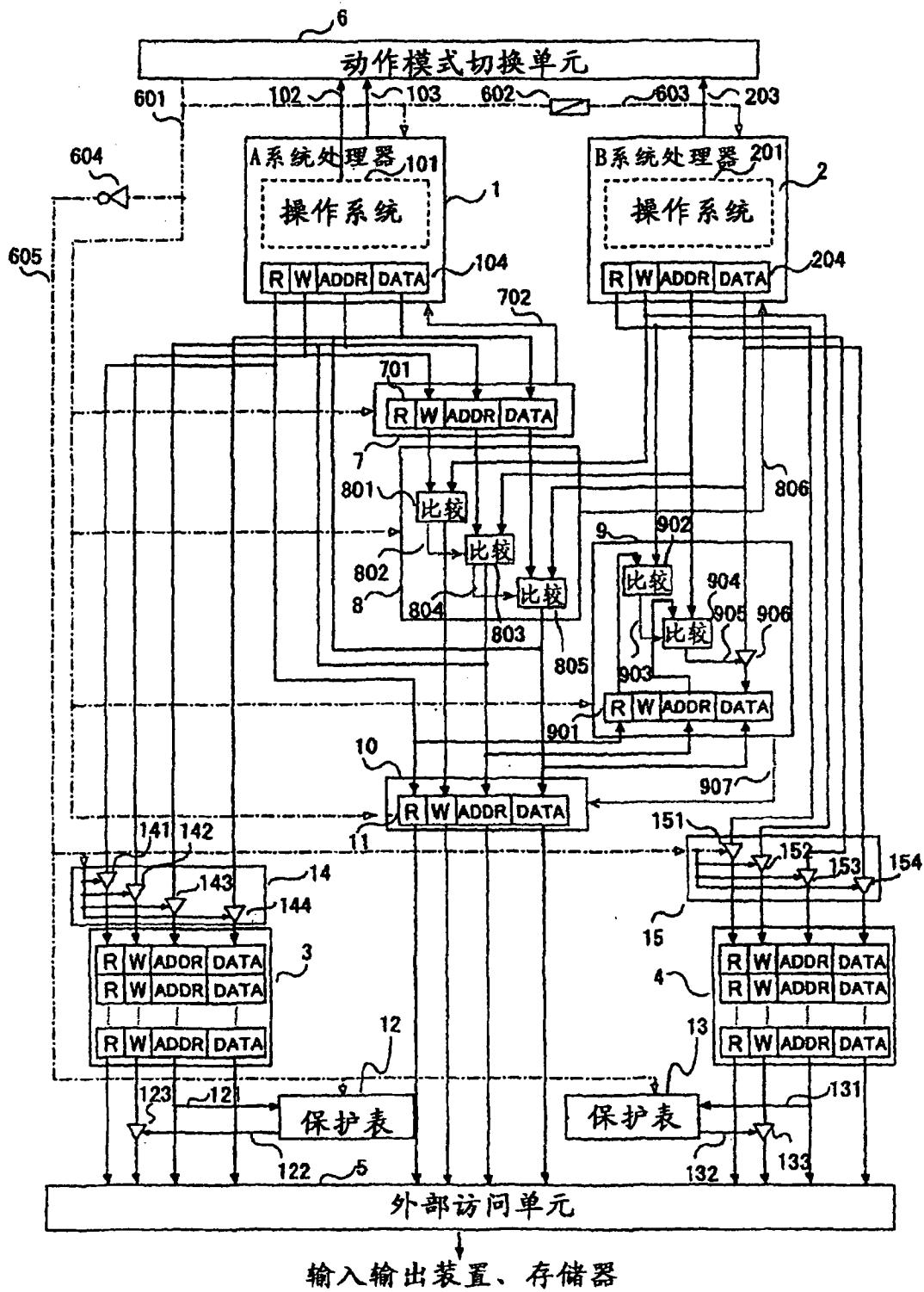
[0133] A 系统处理器 1001 从控制任务 0 开始顺序处理任务，在最后的控制任务 n 的处理结束后，执行用于启动 B 系统处理器高可靠任务的启动任务。该启动任务通过访问中断控制部 1005 内部的 B 系统中断请求寄存器 1997，使 B 系统处理器 1003 发生中断而结束。接下来，A 系统处理器 1001 执行高可靠任务。该高可靠任务对连接到高可靠 IO 1018 上的、要求可靠性的输入输出装置 1019 执行控制。A 系统处理器 1001 周期性地执行从控制任务 0 开始到高可靠任务为止的一连串的处理。

[0134] 另一方面，B 系统处理器 1003 按照从网络 IO 1022 发生的网络中断，依次处理通信任务，在由于 A 系统处理器 1001 执行的启动任务而接收到中断后，执行与 A 系统处理器

相同的高可靠任务。因此,A 系统处理器 1001 和 B 系统处理器 1003 执行同一处理,从而可以保障 2 个处理器的输出一致。B 系统处理器 1003 在高可靠任务的处理结束后,再次按照从网络 IO 1022 发生的网络中断 1066,依次处理通信任务。B 系统处理器 1003 接收到中断并且处理完毕后,对中断控制部 1005 执行访问,清除中断要因。

[0135] 另外,中断控制部 1005 在由于访问 B 系统中断请求寄存器 1007 而发生的中断进入 B 系统处理器 1003 期间,屏蔽优先级低的网络中断 1066,因此,在 B 系统处理器 1003 执行高可靠任务期间,网络中断 1066 不进入,从而不中断处理。

[0136] 如上所述,在执行用于保证可靠性的处理时,利用多个处理器来执行处理,比较多个输出结果,仅在一致的情况下执行输出,从而提高了可靠性,对于不重视可靠性的处理,多个处理器独立动作,从而可以提高处理性能。



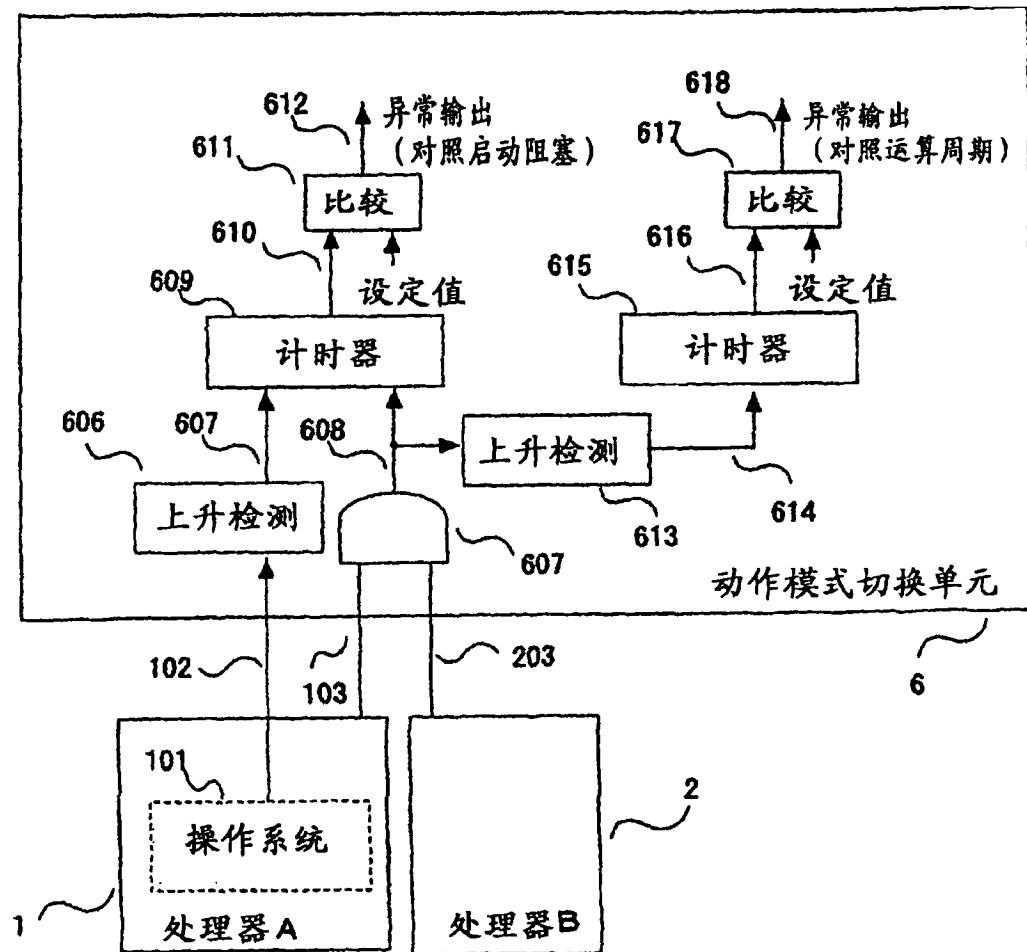
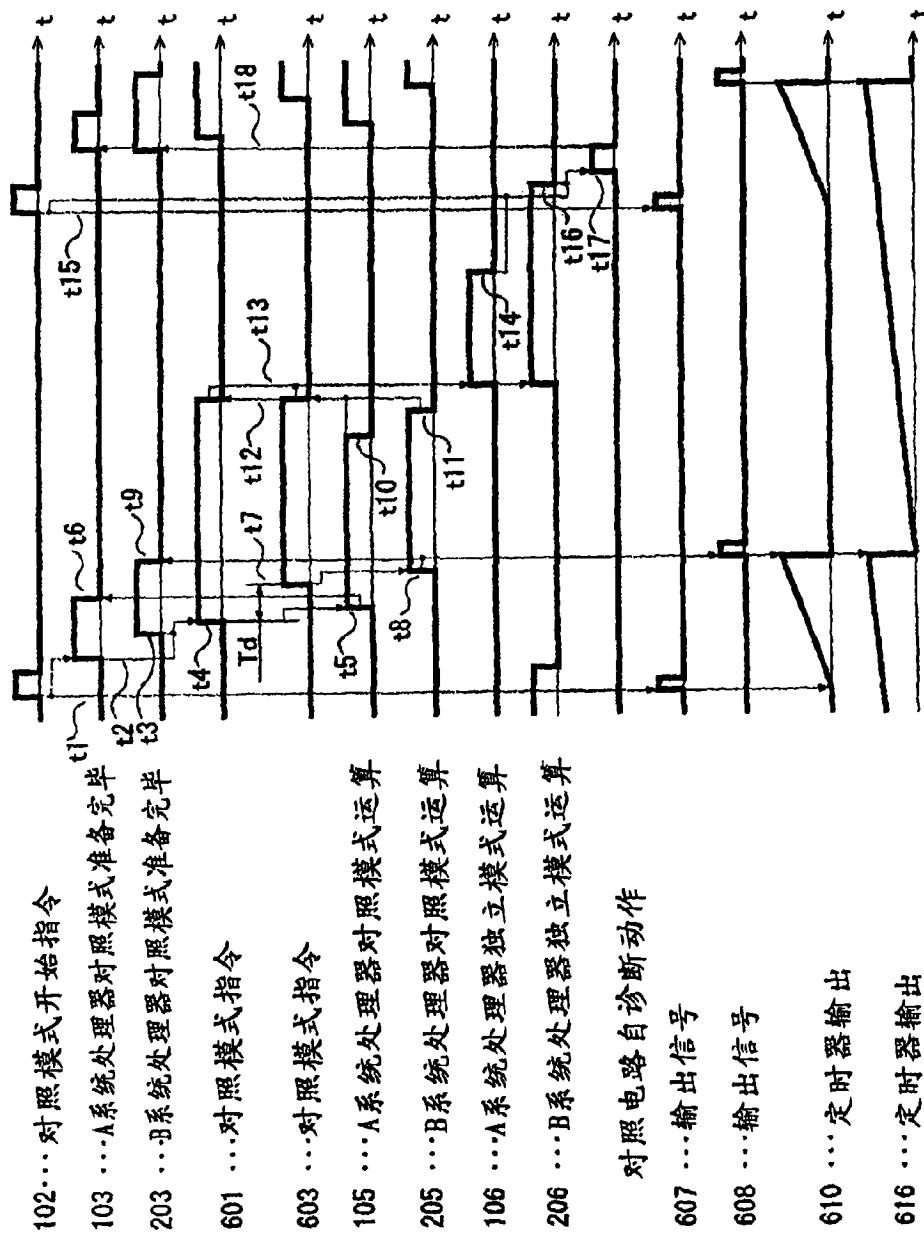


图 2



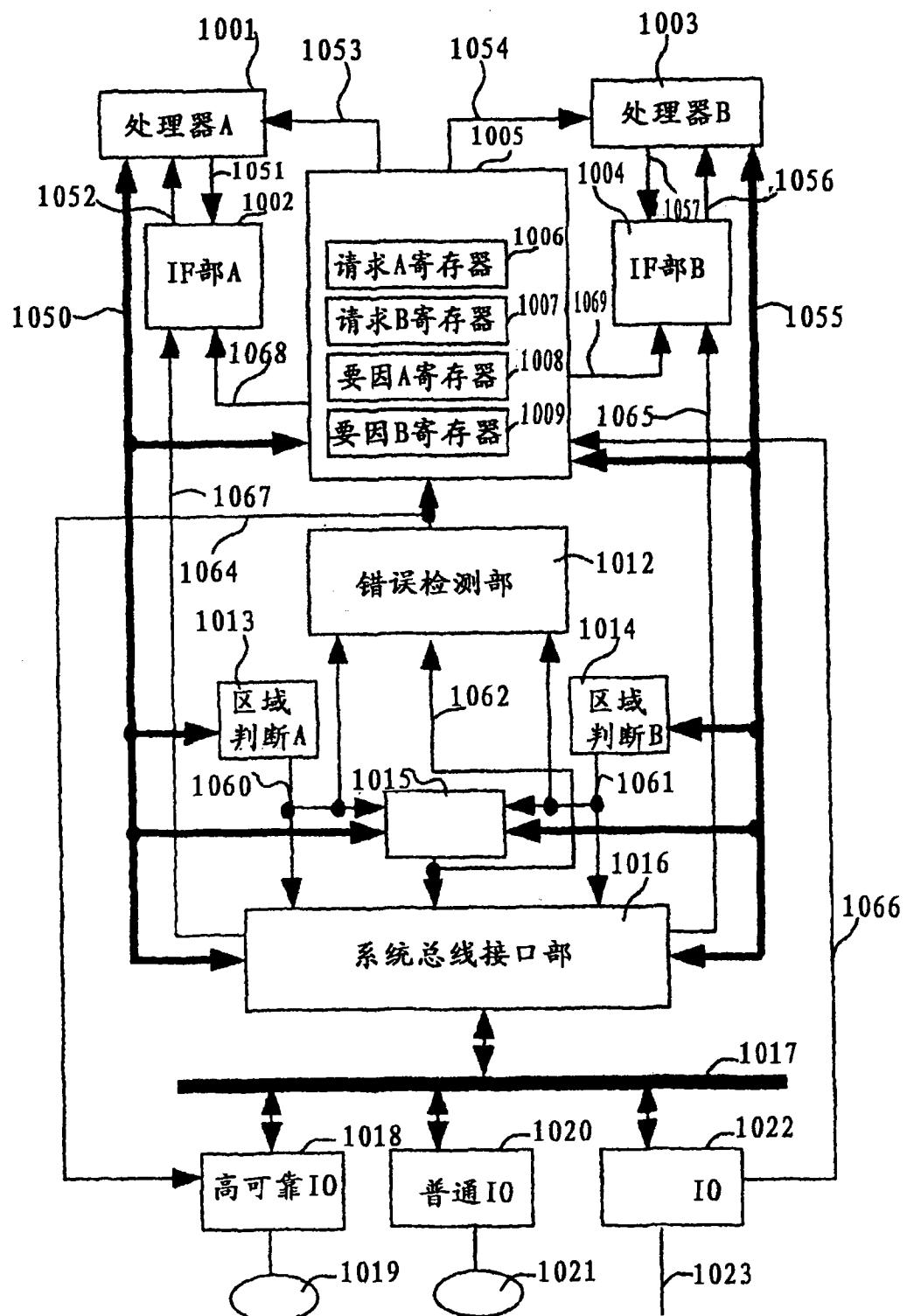


图 4

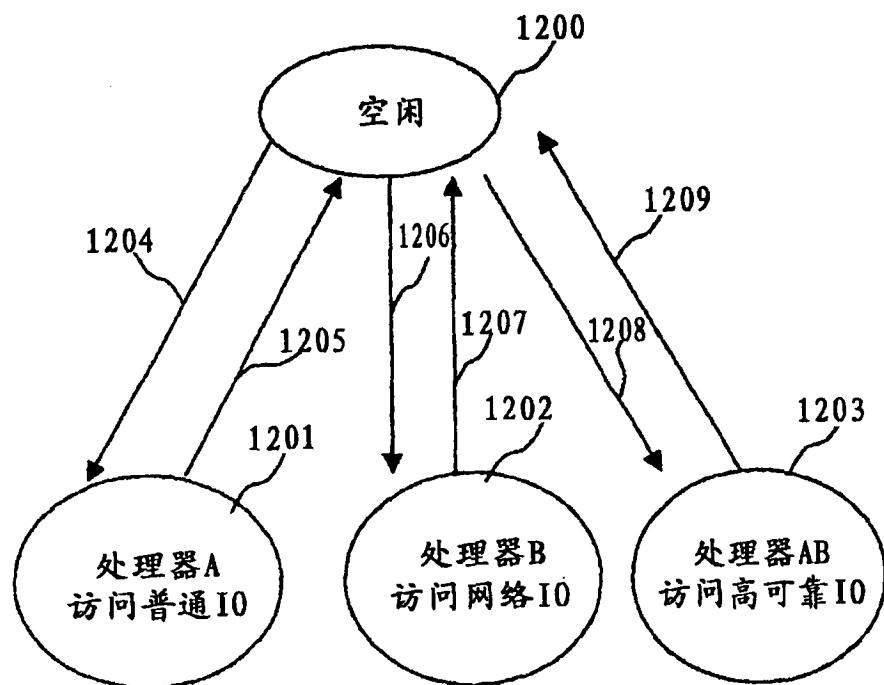


图 5

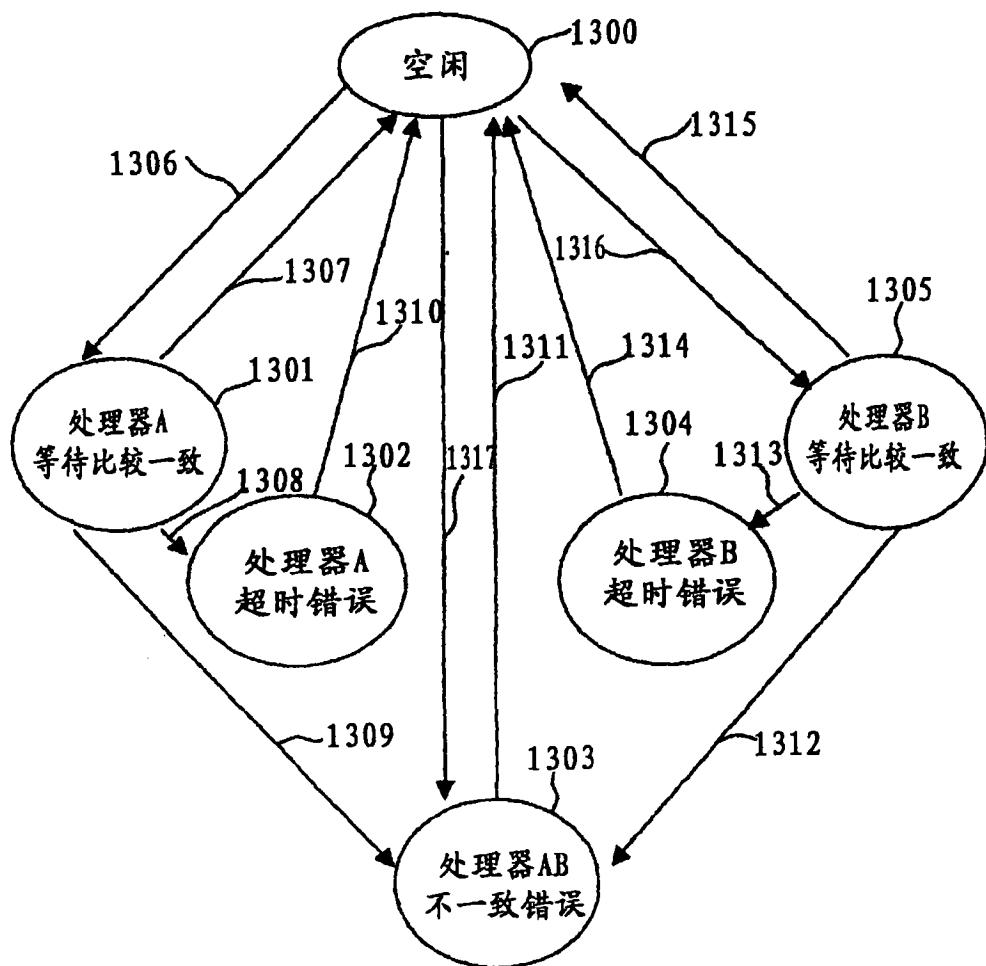


图 6

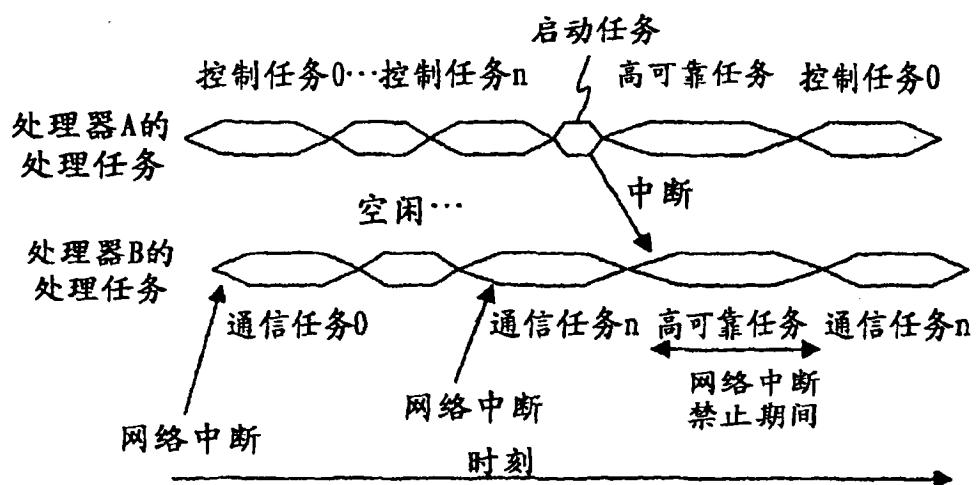


图 7