(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104714439 A
(43)申请公布日 2015.06.17

(21)申请号 201310689383.3

(22)申请日 2013.12.16

(71)申请人 艾默生网络能源－嵌入式计算有限公司
地址 美国亚利桑那州

(72)发明人 罗伯特·查尔斯·图福德 江流
帕希·尤卡·彼得里·韦内尔
马丁·彼得·约翰·科尔内斯

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 严芬 宋志强

(51)Int.Cl.
G05B 19/042(2006.01)

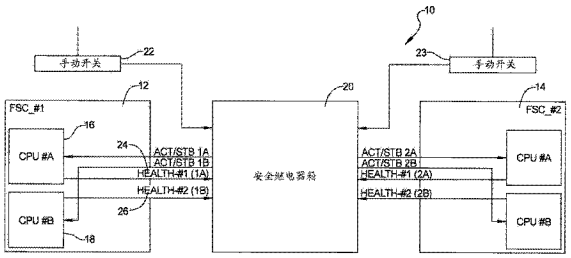
权利要求书2页 说明书6页 附图8页

(54)发明名称

安全继电器箱系统

(57)摘要

公开了一种安全继电器箱系统。一种双冗余计算机安全继电器箱系统包括单独安装至第一和第二印刷电路板的第一和第二故障安全计算系统(FSC)。每个FSC包括被指定为第一CPU和第二CPU的两个计算模块(CPU)。所述第一和第二FSC均连接至安全继电器箱。所述印刷电路板彼此绝缘,以允许在所述印刷电路板之一上维护,而维持另一印刷电路板的FSC的操作。在每个FSC中,从第一和第二CPU的第一和第二印刷电路板生成的健康信号定义多级动态脉冲信号。动态脉冲信号的存在产生被识别为来自第一或第二FSC之一的每一个CPU的第一和第二健康指示信号中的每一个的输出。



CN 104714439 A

1. 一种双冗余计算机安全继电器箱系统，包括：

单独连接至第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统(FSC)；

每个FSC包括被指定为第一CPU和第二CPU的两个计算模块(CPU)；

所述第一和第二FSC均连接至安全继电器箱；并且

所述印刷电路板彼此绝缘，以允许在所述印刷电路板之一上维护，而维持受另一印刷电路板控制的所述FSC的操作。

2. 根据权利要求1所述的双冗余计算机安全继电器箱系统，其中所述第一和第二FSC中的每一个单独连接至印刷电路板(PCB)，所述第一FSC和第二FSC单独连接至第一手动开关或第二手动开关，所述第一手动开关和第二手动开关各自具有限定自动状态的第一开关位置和限定维护状态的第二开关位置。

3. 根据权利要求2所述的双冗余计算机安全继电器箱系统，其中：

所述第一开关位置通过按下所述手动开关以改变至指示操作员的请求的所述第一位置而被手动选择，以允许所述安全继电器箱自动选择哪一个FSC为有效FSC；并且

所述第二开关位置通过按下所述手动开关以改变至指示操作员的请求的所述第二位置而被手动选择，以使受该开关控制的所述FSC转到维护模式，其中所述FSC不被允许在所述维护模式下同时转为有效角色。

4. 根据权利要求1所述的双冗余计算机安全继电器箱系统，其中在每个FSC中，健康信号从所述第一CPU和第二CPU的所述第一和第二印刷电路板生成，每个健康信号定义动态脉冲信号。

5. 根据权利要求4所述的双冗余计算机安全继电器箱系统，其中所述动态脉冲信号的存在产生被识别为第一和第二健康信号中的每一个的输出，所述第一和第二健康信号中的每一个指代来自所述CPU中的每一个的健康指示信号。

6. 根据权利要求5所述的双冗余计算机安全继电器箱系统，其中生效的健康信号指示相关FSC的健康状态，并且失效的健康信号指示相关FSC的不健康状态。

7. 根据权利要求5所述的双冗余计算机安全继电器箱系统，其中所述FSC中的任意一个仅仅在所述FSC中的两个CPU均发出所述健康指示信号时才被指示为健康。

8. 根据权利要求1所述的双冗余计算机安全继电器箱系统，其中所述FSC中首先启动的第一个FSC被指定为有效FSC，并且所述FSC中之后启动的第二个FSC被指定为待机FSC；并且

当所述FSC中的第二个FSC与所述第一个FSC相继通电时，所述安全继电器箱通过向所述待机FSC中的所述CPU模块中的两者返回待机状态信号，来以信号形式向所述待机FSC告知其待机状态。

9. 根据权利要求5所述的双冗余计算机安全继电器箱系统，其中在自动模式下，如果来自所述有效FSC的健康信号中的一个或两个失效，并且来自所述待机FSC的健康信号中的一个或两个未失效，则所述安全继电器箱通过使两个FSC进入所述待机状态而引起故障安全操作，其中不存在有效FSC，并且FSC均不能向外部设备发送安全紧急输出。

10. 一种双冗余计算机安全继电器箱系统，包括：

单独连接至第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统

(FSC)；

每个FSC包括被指定为限定安全继电器模块部分的第一CPU和第二CPU的两个计算模块(CPU)；

具有所述第一和第二FSC的安全继电器箱，所述第一和第二FSC均连接至所述安全继电器箱；并且

在每个FSC中，从所述第一CPU和第二CPU的所述第一和第二印刷电路板生成的健康信号限定多级动态脉冲信号，其中所述动态脉冲信号的存在产生被识别为第一和第二健康指示信号中的每一个的输出，所述第一和第二健康指示信号中的每一个来自所述第一或第二FSC之一的所述CPU中的每一个。

11. 根据权利要求10所述的双冗余计算机安全继电器箱系统，其中所述安全继电器箱连接至用于控制所述第一FSC的第一手动开关，并且所述安全继电器箱连接至用于控制所述第二FSC的第二手动开关，所述第一手动开关和第二手动开关各自具有限定所述FSC的自动状态的第一开关位置和用于限定所述FSC的维护状态的第二开关位置。

12. 根据权利要求11所述的双冗余计算机安全继电器箱系统，其中在从所述第一手动开关和第二手动开关的所述第一开关位置改变为所述第二开关位置或从所述第二开关位置改变为所述第一开关位置之后，所述FSC中的一个被选择为定义“待机”角色的待机FSC，所述待机FSC在所述FSC中的有效FSC发生故障的情况下可用于承担有效角色。

13. 根据权利要求10所述的双冗余计算机安全继电器箱系统，其中所述印刷电路板彼此绝缘，以允许在所述印刷电路板之一上维护，而维持受另一印刷电路板控制的所述FSC的操作。

14. 根据权利要求10所述的双冗余计算机安全继电器箱系统，其中所述安全继电器箱仅在来自所述FSC之一的两个健康指示信号均生效的情况下才选择该FSC为有效FSC，并且两个健康指示信号在所述信号上具有动态波形。

15. 根据权利要求10所述的双冗余计算机安全继电器箱系统，其中在每个FSC中，在所述第一CPU和第二CPU中的每一个生成所述多级动态脉冲健康信号并且将该信号发送至所述安全继电器箱之后，所述安全继电器箱识别来自两个FSC的所有四个健康信号的状态以选择有效FSC，使得经系统初始化后，所述安全继电器箱将所述第一或第二FSC中的使两个健康指示信号均生效的第一FSC选择为指定的有效FSC。

16. 一种双冗余计算机安全继电器箱系统，包括：

单独安装至第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统(FSC)；

每个FSC包括被指定为第一CPU和第二CPU的两个计算模块(CPU)；

所述第一和第二FSC均连接至安全继电器箱；

所述印刷电路板彼此绝缘，以允许在所述印刷电路板之一上维护，而维持另一印刷电路板的所述FSC的操作；并且

在每个FSC中，从所述第一CPU和第二CPU的所述第一和第二印刷电路板生成的健康信号定义多级动态脉冲信号，其中所述动态脉冲信号的存在产生被识别为第一和第二健康指示信号中的每一个的输出，所述第一和第二健康指示信号中的每一个来自所述第一或第二FSC之一的所述CPU中的每一个。

安全继电器箱系统

技术领域

[0001] 本公开涉及用于双冗余计算机系统的安全继电器箱和系统。

背景技术

[0002] 此部分提供与本公开相关的背景信息，该背景信息不必是现有技术。

[0003] 在用于轨道公共运输应用的安全紧急系统中提供有效/待机选择、故障转移以及切换的功能通常被提供为计算机系统内的嵌入功能。双冗余、高可用性的系统为上述功能提供备份，而且也位于计算机系统的体系架构内。商用现成品(COTS)计算机缺少这些特征，因此尚未直接应用于轨道公共运输故障安全应用，从而增加系统的成本和复杂性。产生同时均为有效的信号的双冗余系统会造成安全问题。已知系统还产生固定电压信号或零电压，使得难以确定“被卡住(stuck)”命令信号。

发明内容

[0004] 此部分提供对本公开的一般概括，并且不是本公开的全部范围或本公开的全部特征的全面公开。

[0005] 根据若干个方面，一种双冗余计算机安全继电器箱系统包括单独连接至安全继电器箱上的第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统(FSC)。每个FSC包括被指定为第一CPU和第二CPU的两个计算模块(CPU)。所述第一和第二FSC均连接至安全继电器箱。所述印刷电路板彼此绝缘，以允许在所述安全继电器箱上的所述印刷电路板之一上维护，而维持受另一印刷电路板控制的所述FSC的操作。

[0006] 根据其它方面，一种双冗余计算机安全继电器箱系统包括单独连接至安全继电器箱上的第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统(FSC)。每个FSC包括被指定为限定安全继电器模块部分的第一CPU和第二CPU的两个计算模块(CPU)。所述第一和第二FSC均连接至安全继电器箱。在每个FSC中，从所述第一CPU和第二CPU的所述第一和第二印刷电路板生成的健康信号定义多级动态脉冲信号。动态脉冲信号的存在产生被识别为第一和第二健康指示信号中的每一个的输出，所述第一和第二健康指示信号中的每一个来自所述第一或第二FSC之一的所述CPU中的每一个。

[0007] 根据更多方面，一种双冗余计算机安全继电器箱系统包括单独连接至安全继电器箱上的第一和第二印刷电路板中的每一个的第一和第二故障安全计算系统(FSC)。每个FSC包括被指定为第一CPU和第二CPU的两个计算模块(CPU)。所述第一和第二FSC均连接至安全继电器箱。所述安全继电器箱上的所述印刷电路板彼此绝缘，以允许在所述印刷电路板之一上维护，而维持受另一印刷电路板控制的所述FSC的操作。在每个FSC中，从所述第一CPU和第二CPU的所述第一和第二印刷电路板生成的健康信号定义多级动态脉冲信号。所述动态脉冲信号的存在产生被识别为第一和第二健康指示信号中的每一个的输出，所述第一和第二健康指示信号中的每一个来自所述第一或第二FSC之一的所述CPU中的每一个。

[0008] 根据本文提供的描述，适用的更多领域将变得显而易见的。该发明内容部分中的描述和特定示例旨在仅仅用于图示的目的，而不旨在限制本公开的范围。

附图说明

[0009] 本文所描述的附图仅仅是用于所选择实施例的图示目的，而不是所有可能的实施方式，并且不旨在限制本公开的范围。

[0010] 图 1 是具有两个故障安全计算机的安全继电器箱系统的图；

[0011] 图 2 是利用脉冲信号改变输出条件来进行操作的电路图；

[0012] 图 3 是用于指示 FSC 的健康状态的多级动态脉冲信号的图；

[0013] 图 4 是定义安全继电器箱系统的输入信号和输出信号的图和状态转换表；

[0014] 图 5 是本公开的手动开关的图；

[0015] 图 6 是用于本公开的异步输入 Mealy 状态机；以及

[0016] 图 7A 和图 7B 分别是本公开两个印刷电路板设计的第一电路图和第二电路图。

[0017] 在附图的若干个视图中，对应的附图标记始终指代对应的部分。

具体实施方式

[0018] 现在将参照附图更充分地描述示例实施例。

[0019] 参照图 1，安全继电器箱系统 10 可像以近似 500ms 为周期的故障转移开关一样工作，并且提供两种工作模式：自动模式和手动模式。安全继电器箱系统 10 包括第一和第二故障安全计算系统（或故障安全计算机）FSC12、14（下文被指定为 FSC_#1、FSC_#2），第一和第二故障安全计算系统 FSC12、14 各自包括两个计算模块（CPU）16、18（下文被指定为 CPU#A、CPU#B）。第一和第二 FSC 的 FSC_#1、FSC_#2 连接至故障转移开关或安全继电器箱 20。安全继电器箱系统 10 进一步包括第一和第二手动开关 22、23，这将参照图 5 进行更详细描述。安全继电器箱系统 10 进一步包括位于三个组件 FSC_#1、FSC_#2 和安全继电器箱 20 之间的多个连接器。

[0020] 在 FSC_#1 和 FSC_#2 的每一个中，健康信号将从 CPU#A、CPU#B 的 CPU 板生成。每个健康信号提供故障安全功能。当具有动态脉冲信号时，以健康信号 24、26 标识的输出（在下文中被指定为 health-#1(1A)、health-#1(1B)、health-#2(2A)、health-#2(2B)）指代来自 CPU#A、CPU#B 中每一个的健康指示信号。应注意，健康信号 1A、1B 和 2A、2B 具有含有特定周期的多级动态脉冲。动态多级脉冲的使用排除了当固定电压信号（常用于指示有效信号条件）实际为例如由硬件故障导致的“假安全”状态时出现的情形。如果健康信号生效（是脉冲式的），则该信号指示相关 FSC 的健康状态。如果该健康信号失效（具有与脉冲式健康信号不同的模式脉冲的脉冲式信号、或固定的逻辑电平（非脉冲式）信号），则指示该特定 FSC 的不健康状态。在安全继电器箱系统 10 中，一个 FSC 仅在两个 CPU 模块 CPU#A、CPU#B 均发出健康指示信号时才被判断为健康。每个健康信号 health-#1，health-#2 也可被指定为 health-mn，其中“m”指示特定 FSC 的标识（m=1 或 2），并且“n”指示每个 FSC 中的 CPU 模块的标识（n=A 或 B）。

[0021] 信号也被指定为有效或待机，如有效 / 待机 -mn。有效 / 待机 -mn 信号是从安全继电器箱 20 发回 CPU 模块 CPU#A、CPU#B 的指示信号。有效 / 待机 -mn 信号被提供为具有特

定周期的动态多级脉冲。如果有效 / 待机 -mn 信号生效(是脉冲式的),则相关 FSC 可以以有效模式操作。如果有效 / 待机 -mn 信号失效(具有与脉冲式健康信号不同的模式脉冲的脉冲式信号、或者固定的逻辑电平(非脉冲式)信号),则失效的信号将迫使 FSC 以待机模式工作。针对每个 FSC 中的这两个 CPU 模块 CPU#A、CPU#B 的操作,CPU#A 或 CPU#B 中的每一个将从 FSC 获得其自己的有效 / 待机指示信号。

[0022] 有效 / 待机选择在每个 FSC 中,每个 CPU 模块 CPU#A、CPU#B 生成动态多级脉冲健康信号,并将该信号发送至安全继电器箱 20。安全继电器箱 20 使用所有四个健康信号的状态,以选择有效 FSC。经系统初始化之后,安全继电器箱 20 选择第一 FSC(FSC_#1 或 FSC_#2)作为被指定或有效的 FSC,该第一 FSC 使健康信号 health-#1、health-#2 都生效。安全继电器箱 20 通过在其两个有效 / 待机信号上返回一动态多级脉冲,而以信号形式向有效 FSC 告知其有效状态。在初始化阶段中,通常两个 FSC 同时通电,因此为这两个 FSC 分派不同的初始化周期。通常,具有来自两个 CPU 的生效健康信号的第一 FSC (FSC_#1 或 FSC_#2) 被分派为有效状态。如果 FSC_#1 和 FSC_#2 均为健康的,并且并行操作(在完全相同的时间两个均有效),则 FSC_#1 将被分派为有效状态。因此,如果 FSC_#2 相继 FSC_#1 同步,则其将变为待机 FSC。安全继电器箱 20 通过在有效 / 待机信号上返回静态逻辑 0 至待机 FSC 中的两个 CPU 模块,而以信号形式向待机 FSC 告知其待机状态。

[0023] 安全输入参照图 2 以及再次参照图 1,如之前所述,健康信号来自于每个 FSC 的两个 CPU 板 CPU#A、CPU#B。当存在脉冲信号 28 时,输出 30 被激活。当脉冲信号 28 不存在时,发送到输入 32 的所有 0 或所有 1(与不存在的信号区别开的不健康信号模式)将输出 30 置于未激活状态。输入信号的示例可以是 5V,在 10KHz 的频率下占空比 50%,不过本公开不限于此输入信号或任何特定输入信号。

[0024] 故障转移操作(自动模式),如果来自有效 FSC 的健康信号中的一个或两个失效,并且来自待机 FSC 的两个健康信号均生效,则安全继电器箱 20 引起从旧的有效 FSC 到旧的待机 FSC 的故障转移操作。这通过使到旧的有效 FSC (FSC_#1) 的有效 / 待机信号均失效为并且使到旧的待机且现在新的有效 FSC (FSC_#2) 的有效 / 待机信号均生效而发生。

[0025] 故障安全操作(自动模式) 如果来自有效 FSC 的健康信号中的一个或两个失效,但来自待机 FSC 的一个或两个健康信号未生效,则安全继电器箱 20 通过使到两个 FSC 的有效 / 待机信号均失效而使两个 FSC 进入待机状态来引起故障安全操作。在这种状态下,不存在有效 FSC,并且 FSC 均不能够向外部设备发送安全紧急输出。

[0026] 安全输入参照图 3 并再次参照图 1 和图 2,关于示例性 ACT/STB 信号,安全输出方法如下。当 FSC 需要从安全继电器箱 20 接收信号时,首先 FSC 向安全继电器箱 20 发送脉冲式健康信号。如果位于安全继电器箱 20 中的继电器 34 关闭,则 FSC 接收反馈脉冲式有效 / 待机信号。如果位于安全继电器箱 20 中的继电器 34 打开,则 FSC 不能接收反馈脉冲式有效 / 待机信号。

[0027] 安全内部逻辑参照图 4 并再次参照图 1 至图 3,存在两组输入信号。输入组 A 来自 FSC_#1(A 等于 Health_#1 和 Health_#2),并且输入组 B 来自 FSC_#2(B 等于 Health_#1′ 和 Health_#2′)。这四个输入信号(Health_#1、Health_#2、Health_#1′ 、Health_#2′)控制两个输出信号 :安全信号输出 C 和安全信号输出 D。C 用于指代 FSC_#1,并且 D 用于指代 FSC_#2。这两个输出信号争夺有效状态,因此如果一个获得有效状态,则另一个被禁止输

出有效状态。两个输出 C 和 D 执行“先输入 - 先输出”策略。

[0028] 手动切换操作(手动模式)参照图 5 并再次参照图 1,除了上述自动模式操作之外,操作员可以促使单个 FSC 在有效或待机(维护)状态下工作。安全继电器箱 20 允许操作员通过将 2 静止位置手动开关 22 或 23 改变到维护位置而请求从有效 FSC 到待机 FSC 的切换。然后,针对维护或待机状态所选择的开关将维持在维护静止位置,以防止系统在维护模式时返回至有效状态。手动开关 22 或 23 通常倾向于维持在其最后选择的位置。开关 22、23 可以通过按下开关部分 36 而被复位至自动位置 1,或者通过按下开关部分 38 而被复位至维护位置 2。这种切换操作允许操作员请求如下到 FSC_#1 或 FSC_#2 的切换 :

[0029] 请求切换至 FSC_#1 (假设 FSC_#2 当前有效):

[0030] 1) 通过检查 FSC_#2 为有效 LED 来验证 FSC_#2 当前有效。

[0031] 2) 通过检查 FSC_#1 为健康 LED 来验证 FSC_#1 当前健康。

[0032] 3) 针对 FSC_#2,将开关 23 的开关部分 36 从自动位置改变至维护位置。

[0033] 请求切换至 FSC_#2 (假设 FSC_#1 当前有效):

[0034] 1) 通过检查 FSC_#1 为有效 LED 来验证 FSC_#1 当前有效。

[0035] 2) 通过检查 FSC_#2 为健康 LED 来验证 FSC_#2 当前健康。

[0036] 3) 针对 FSC_#1,将开关 22 的开关部分 36 从自动位置改变至维护位置。

[0037] 安全继电器箱状态机参照图 6,为安全继电器箱系统 10 提供状态机。“输入 A”指示来自 FSC_#1 的两个健康信号。为使输入 A 生效(“1”),来自 FSC_#1 的两个健康信号必须均生效。类似的结论适用于输入 B 和来自 FSC_#2 的两个健康信号。类似地,当状态机使输出 C 生效时,其使到 FSC_#1 的两个有效 / 待机信号均生效,而当其使输出 C 失效时,其使到 FSC_#1 的两个有效 / 待机信号均失效。类似的结论适用于输出 D 和到 FSC_#2 的两个有效 / 待机信号。当输出为“00”时,不存在有效 FSC。当输出为“10”时,FSC_#1 有效。当输出为“01”时,FSC_#2 有效。从来没有两个输出均生效(输出 =“11”)的情况,因此也从来没有两个 FSC 均有效的情况。

[0038] 参照图 7 并且再次参照图 1,安全继电器箱 20 包括安装至背板 44 的第一和第二模块部分 40、42 (下文称为安全继电器模块部分 M#1 和安全继电器模块部分 M#2)。第一和第二安全继电器模块 40、42 之间的连接保证在任何时间安全继电器模块中仅仅不超过一个有效。当一个继电器模块有效时,其 K_NC 触点 46、48 将打开,使电源与另一继电器模块绝缘。

[0039] 再次参照图 5,2- 位置手动开关 22、23 各自提供两种操作模式之间的选择 :FSC 自动模式和 FSC 强制维护或待机模式。强制维护模式也定义手动开关模式。需注意,FSC 健康信号将使具有最高优先级的 ACT/STB 信号(图 1 所示)失效,无论其是否处于自动有效或维护 / 待机模式。例如,当手动开关 22 处于位置 1 时,安全继电器箱 20 将在正常的自动故障转移模式下工作。当手动开关 22 处于位置 1 时,K_NC 触点 46 断开,并且第二模块部分 42 将从电源线切断。如上所述,安全继电器箱 20 将在强制操作模式下连接 FSC_#1。当手动开关 22 处于位置 2 时,K_NC 触点 48 断开,并且第一模块部分 40 将从电源线切断。如上所述,安全继电器箱 20 将在强制操作模式下连接 FSC_#2。每个安全继电器模块部分中的内部开关(K-NC 和 K_NO)受通过健康指示信号驱动的外部 KA 和 KB 控制。仅仅当 KA 和 KB 均处于连接状态时,K_NC 才改变为断开状态,并且 K_NO 改变为连接状态。否则,K_NO 将维持在安

全断开状态，并且 K_NC 将维持在连接状态，这在图 7 中被示出为默认状态。K_NC 被用作第一和第二 FSC（FSC_#1 和 FSC_#2）之间的互斥机制，以保证在任何时间仅仅一个 FSC 有效。

[0040] 在自动模式下，在两个 FSC 均通电时，因为 FSC 均未通过初始化阶段，因此没有到安全继电器箱 20 的健康指示。两个安全继电器模块部分 M#1 和 M#2 将被供电，但将具有失效状态。因此，K_NO 仍处于打开状态，并且未向 FSC_#1 或 FSC_#2 提供有效指示信号。之后，如果 FSC_#1 首先发出健康指示信号，则此时使 K_NO 实现为连接状态，而使 K_NC 实现为断开状态。此时，FSC_#1 将从安全继电器箱 20 接收有效信号，这是因为 K_NO 被连接为使动态健康信号旁通。此外，因为安全继电器模块部分 M#1 中的 K_NC 处于打开状态，因此供给安全继电器模块部分 M#2 的电源被切断。FSC_#2 此时不能变为有效，无论其健康与否。在这种互斥方式下，安全继电器箱 20 保证在冗余系统中仅仅具有一个有效 FSC。

[0041] 如果之后 FSC_#2 完成其初始化阶段并且向安全继电器箱 20 发送健康指示信号，则 FSC_#2 将没有有效指示，这是因为其安全继电器模块部分 M#2 断电。如果之后 FSC_#1 变为不健康，则安全继电器模块部分 M#1 中的内部开关（K_NO、K_NC）将返回至默认状态，这导致 FSC#1 具有待机指示。此外，安全继电器模块部分 M#1 的 K_NC 将被连接，这接着使安全继电器模块部分 M#2 通电。安全继电器模块部分 M#2 由于其被通电并且具有理想的输入，因此被激活。结果，安全继电器模块部分 M#2 的 K_NO 被实现为连接状态，而其 K_NC 被实现为断开状态，这导致 FSC_#2 具有有效信号。此外，安全继电器模块部分 M#1 的电源将被断开，这保证 FSC_#1 处于待机状态，无论其是否健康。

[0042] 有效 / 待机动态信号的生成为了使安全继电器箱 20 选择 FSC 中的一个有效，必须使来自该 FSC 的两个健康信号均生效，其中这两个健康信号在信号上具有动态波形。为了以信号形式告知 FSC 应变为有效，安全继电器箱 20 仅仅关闭安全继电器模块部分 M#1 或 M#2 之一中的 K_NO 开关，并且将输入的动态健康状态信号作为输出的动态有效 / 待机控制信号发回至 FSC。

[0043] 继续参照图 7，第一和第二模块部分 40、42 中的每一个包括可视化指示单个 PSU16、18 的操作状态的一组 LED50、52。第一和第二模块部分 40、42 中的每一个也可经由连接器 54、56 单独连接至独立的电源。

[0044] 本公开的故障安全安全继电器箱系统提供了若干个优点。因为印刷电路板 40、42 中的各个印刷电路板彼此绝缘，因此可以在印刷电路板之一上执行维护，而另一印刷电路板的 FSC 的故障安全操作将被维持。已知的故障安全系统具有共同安装 / 连接的全部部件，因此维护的执行需要切断整个系统。本公开的故障安全安全继电器箱系统还利用脉冲变化的动态健康信号。当变化的脉冲信号从 FSC 之一中被识别时，FSC 被视为健康的。相反，利用固定电压信号的已知系统可以产生固定的电压，即使在部件处于故障状态时，因此固定电压信号的指示并不总是指示健康的 FSC。另外，作为另一个安全特征，为了使安全继电器箱 20 选择 FSC 之一有效，来自该 FSC 的两个健康信号必须均生效（通过变化的脉冲指示）。

[0045] 提供示例性实施例，使得本公开详尽，并且将范围完全传达给本领域技术人员。阐述了大量具体细节，例如具体组件、装置以及方法的示例，以提供对本公开实施例的详尽理解。无需采用具体细节，示例性实施例可以以多种不同形式来体现，并且示例性实施例不应被解释为限制本公开的范围，这些对于本领域技术人员来说是显然的。在一些示例性实施

例中，并没有具体描述已知的处理、已知的装置结构以及已知的技术。

[0046] 本文中使用的术语仅用于描述特定示例实施例用途，而不旨在作为限制。本文中使用的单数形式“一”、“该”、“此”可以旨在还包括复数形式，除非上下文明确地表示别的含义。术语“包括”、“包含”、“涵盖”和“具有”是包括性的，因此规定所介绍的特征、整体、步骤、操作、元件和／或部件的存在，但是不排除存在或增加一个或多个其它特征、整体、步骤、操作、元件、部件和／或它们的组合。本文中描述的方法步骤、过程和操作不应被解释为必须要求以所介绍或所图示的特定顺序表现，除非特定地被标识为表现的顺序。还应理解，可以采用附加步骤或可替代的步骤。

[0047] 当元件或层被称为“位于另一元件或层上”、“与另一元件或层接合”、“与另一元件或层连接”或者“与另一元件或层联接”，其可以直接位于另一元件或层上、直接与另一元件或层接合、直接与另一元件或层连接或者直接与另一元件或层联接，或者可以存在介于中间的元件或层。相比之下，当元件被称为“直接位于另一元件或层上”、“直接与另一元件或层接合”、“直接与另一元件或层连接”或者“直接与另一元件或层联接”时，可以没有介于中间的元件或层。用来描述元件之间关系的其它词语应当以类似的方式去解释（例如“在……之间”对“直接在……之间”、“与……相邻”对“与……直接相邻”等）。术语“和／或”，当在本文中使用时，包括相关联列出的项目中的一个或多个项目的任一组合和全部组合。

[0048] 虽然在本文中可以使用术语“第一”、“第二”、“第三”等来描述多个元件、组件、区域、层和／或部分，但是这些元件、组件、区域、层和／或部分不应受这些术语限制。这些术语可以仅用来将一个元件、组件、区域、层或部分与另一区域、层或部分区分开。像“第一”、“第二”和其它数字术语这样的术语，当其在本发明中使用时，不指顺序或次序，除非上下文清楚地这样表示。因此，下面介绍的第一元件、第一组件、第一区域、第一层或第一部分可以被称为第二元件、第二组件、第二区域、第二层或第二部分，而不背离示例实施例的教导。

[0049] 为了便于描述，在本文中可以使用像“内”、“外”、“下面”、“下方”、“下”、“上面”、“上”等等这样的与空间有关的术语来描述附图中所示的一个元件或特征与别的元件或特征的关系。空间有关的术语可以旨在涵盖在使用中或在操作中的装置除附图所示的方向以外的不同方向。例如，如果附图中的装置翻转，那么被描述为“位于其它元件或特征下方”或“位于其它元件或特征下面”的元件将朝向“其它元件或特征上方”。因此，示例术语“下面”可以包括上面和下面两个朝向。装置可以朝向别的方向（旋转 90 度或朝向其它方向），相应地解释本发明中使用的与空间有关的描述词。

[0050] 已经为了说明和描述目的提供上面对实施例的描述。描述不旨在是详尽的或者限制本公开。特定实施例的单独元件或特征通常不局限于该特定实施例，而是可在适用时互换并且可以在选择的实施例中使用，即便未具体地示出或描述。本发明还可以以多种方式变化。这样的变化不应被视为背离本公开，并且所有这样的修改旨在包含在本公开的范围内。

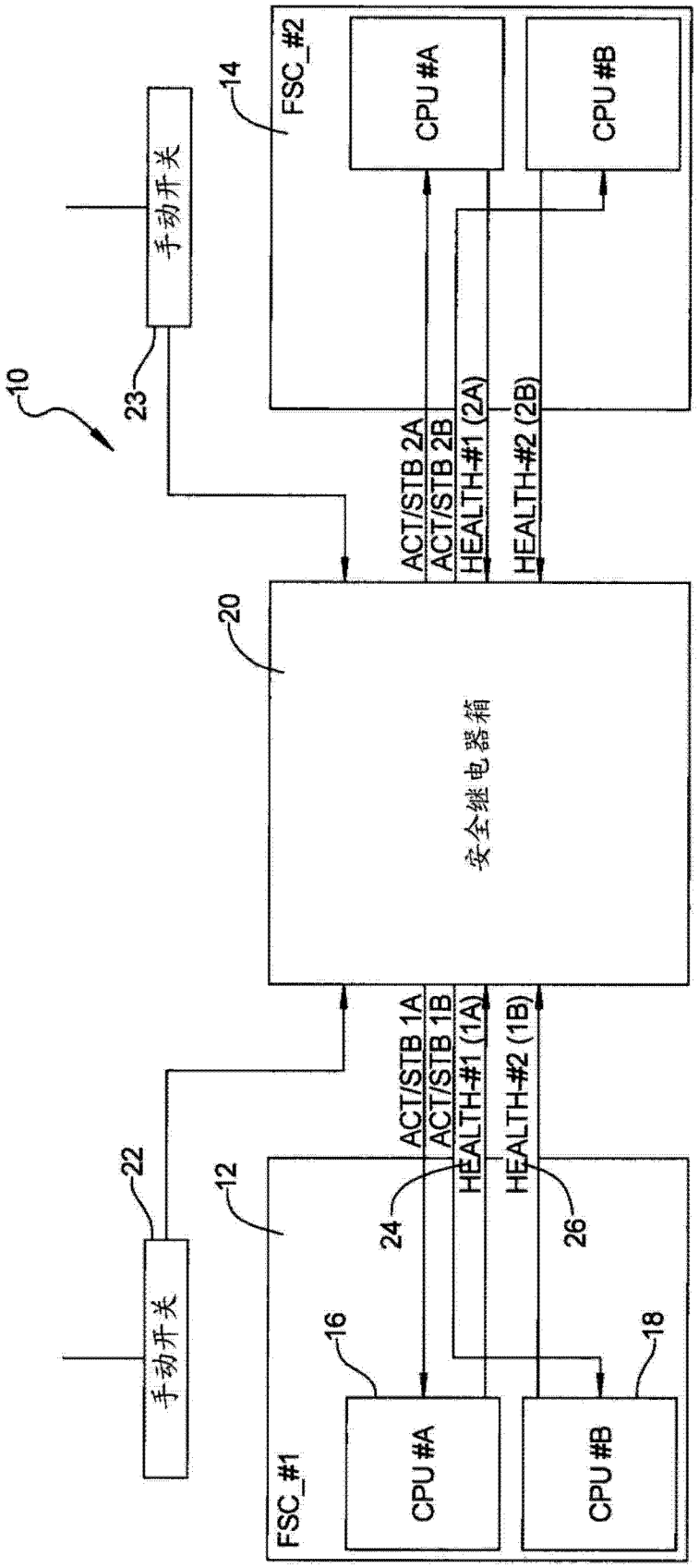

10
23
手动开关
14
FSC_#2
CPU #A
CPU #B
ACT/STB 2A
ACT/STB 2B
HEALTH-#1 (2A)
HEALTH-#2 (2B)
20
安全继电器箱
ACT/STB 1A
ACT/STB 1B
HEALTH-#1 (1A)
HEALTH-#2 (1B)
22
12
24
26
手动开关
16
18
FSC_#1
CPU #A
CPU #B

图 1

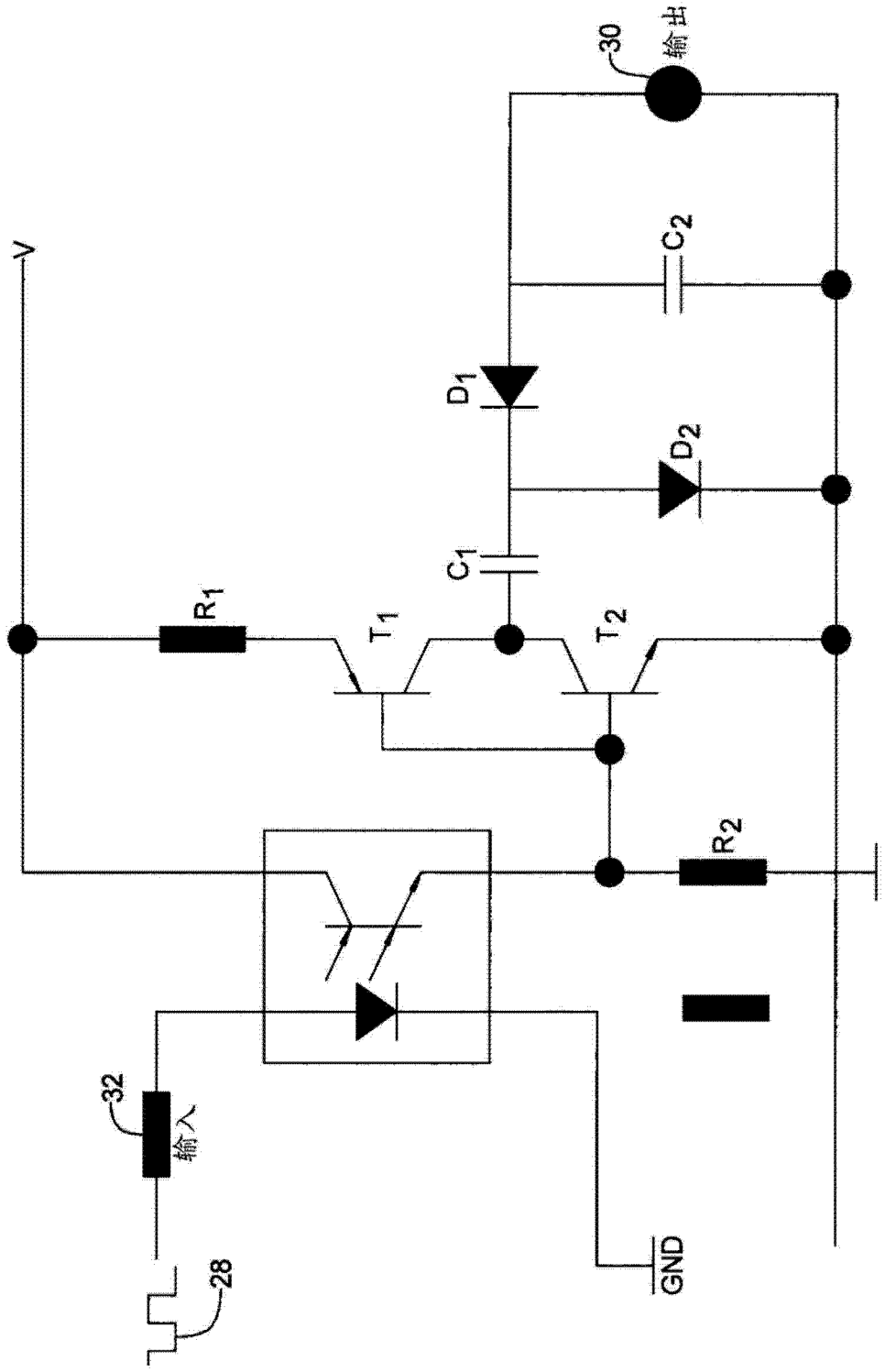


图 2

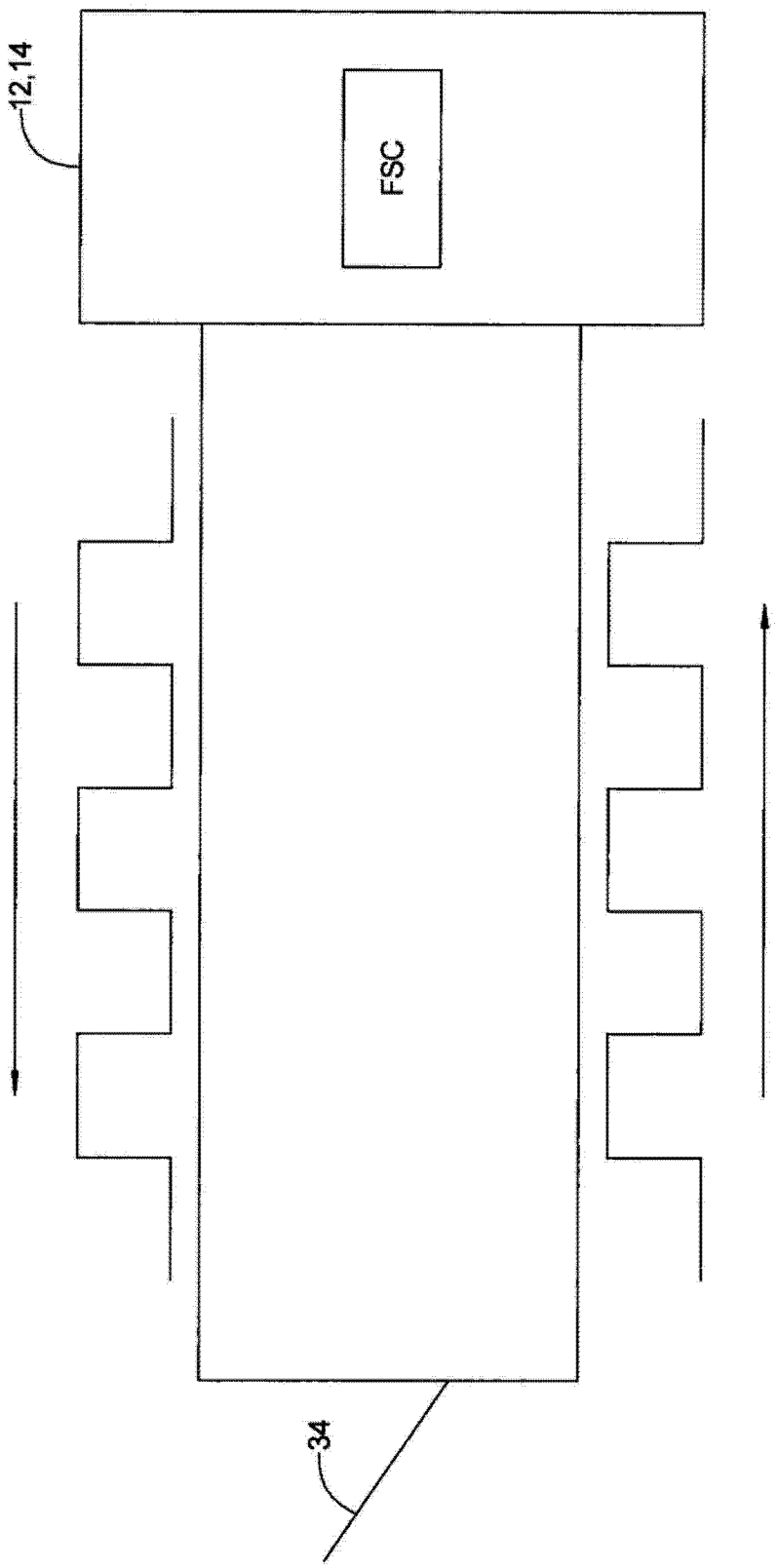
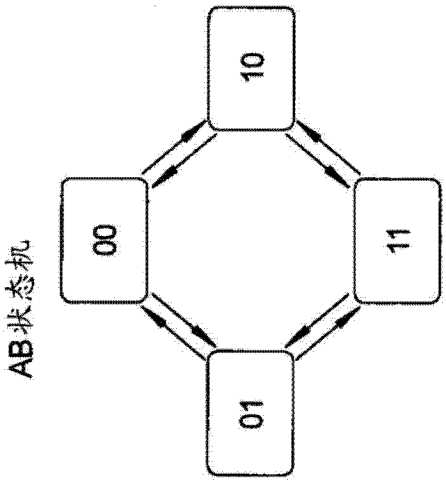
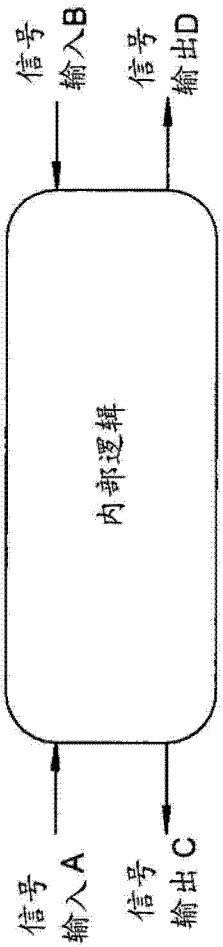


图 3





信号输入	状态转换表							
AB	00—01	01—11	11—10	10—11	11—01	01—00	00—10	10—00
C	0	0	1	1	0	0	1	0
D	1	1	0	0	1	0	0	0

图 4

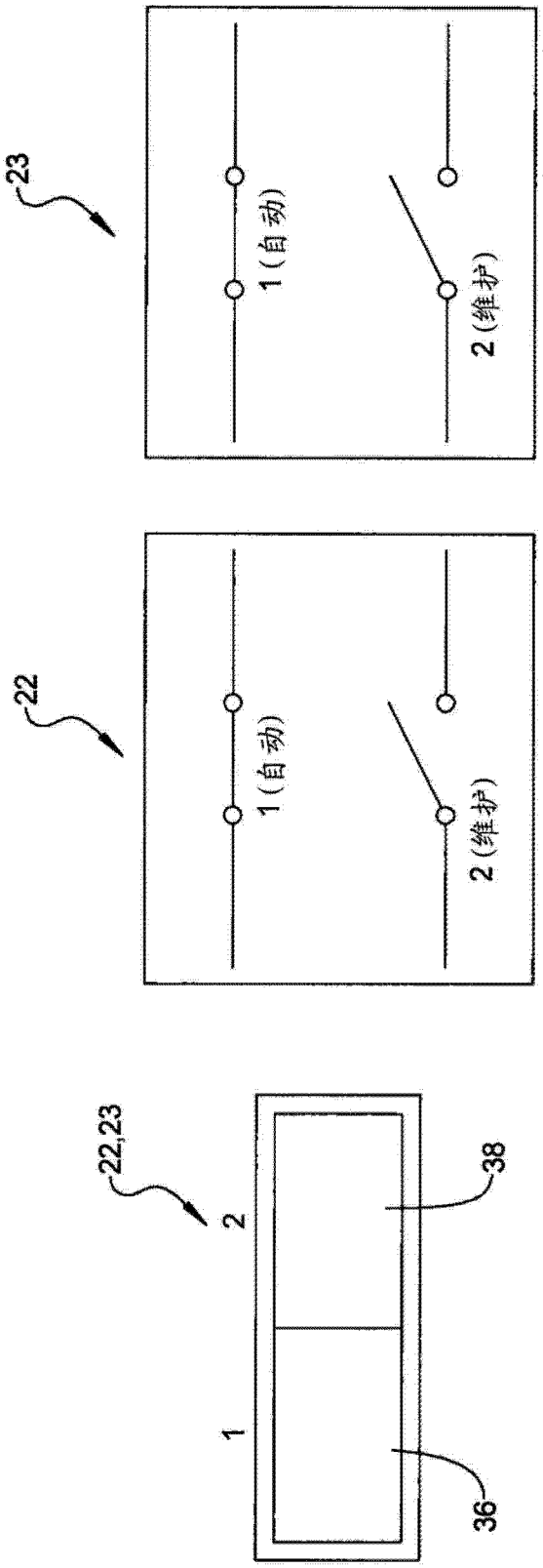


图 5

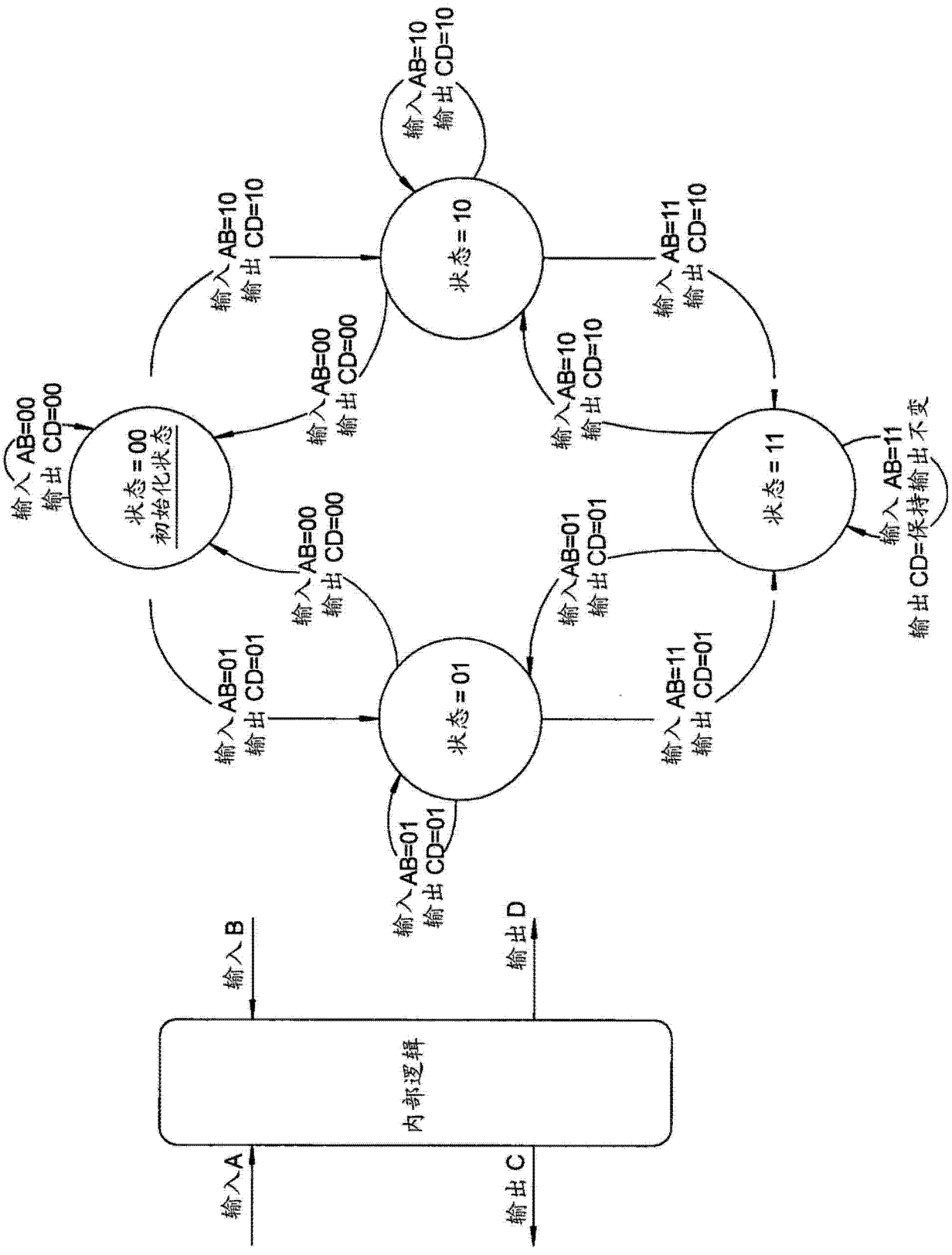

状态 = 00
初始化状态
状态 = 10
状态 = 01
状态 = 11
输入 AB=00
输出 CD=00
输入 AB=10
输出 CD=10
输入 AB=01
输出 CD=01
输入 AB=11
输出 CD=10
输出 CD=保持输出不变
内部逻辑
输入 A
输入 B
输出 C
输出 D

图 6

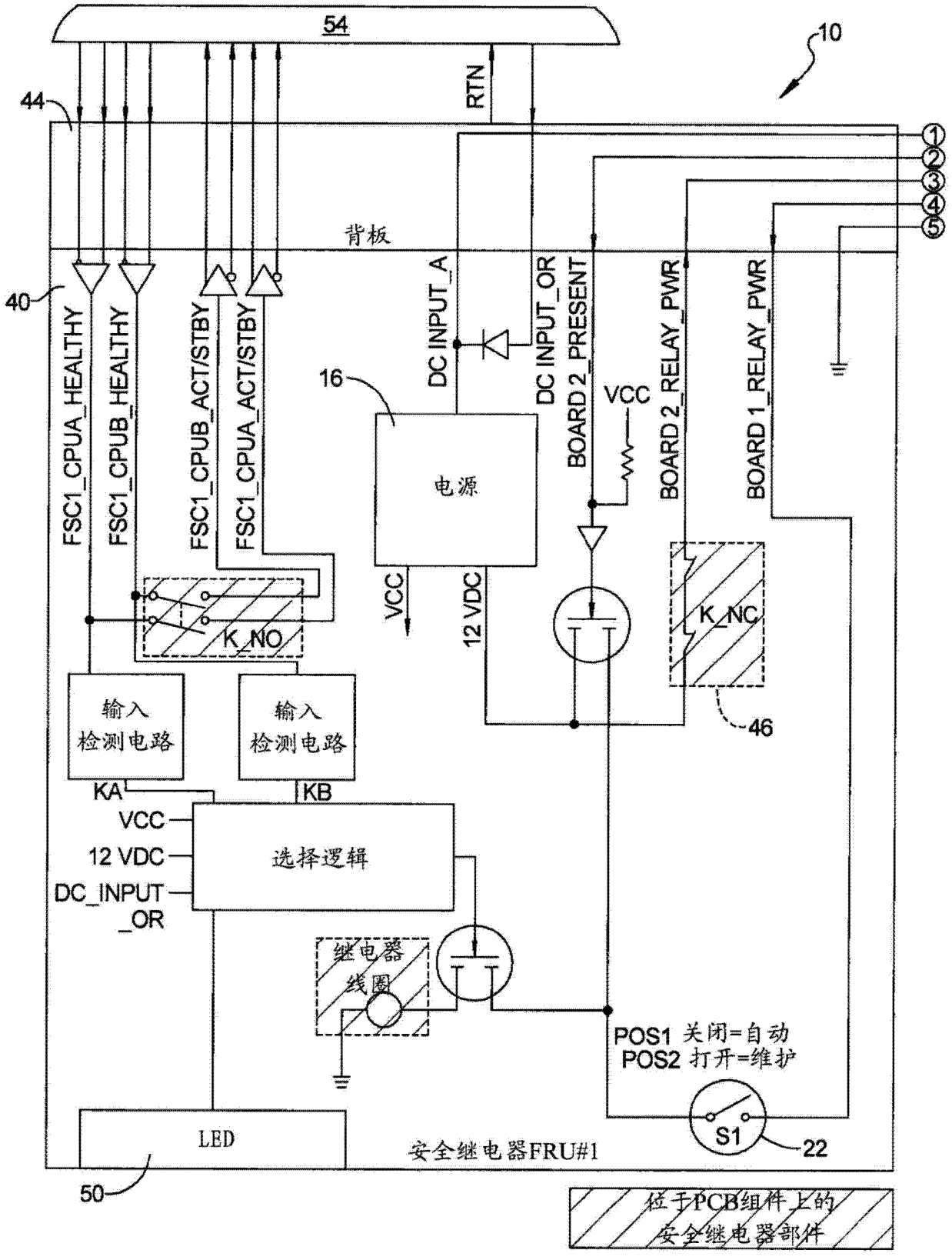

54
10
44
RTN
背板
1
2
3
4
5
40
FSC1_CPUA_HEALTHY
FSC1_CPUB_HEALTHY
FSC1_CPUB_ACT/STBY
FSC1_CPUA_ACT/STBY
DC INPUT_A
DC INPUT_OR
BOARD 2_PRESENT
BOARD 2_RELAY_PWR
BOARD 1_RELAY_PWR
16
电源
VCC
12 VDC
K_NO
K_NC
46
输入
检测电路
输入
检测电路
KA
KB
VCC
12 VDC
DC_INPUT
_OR
选择逻辑
继电器
线圈
POS1 关闭=自动
POS2 打开=维护
S1
22
LED
50
安全继电器FRU#1
位于PCB组件上的
安全继电器部件

图 7A

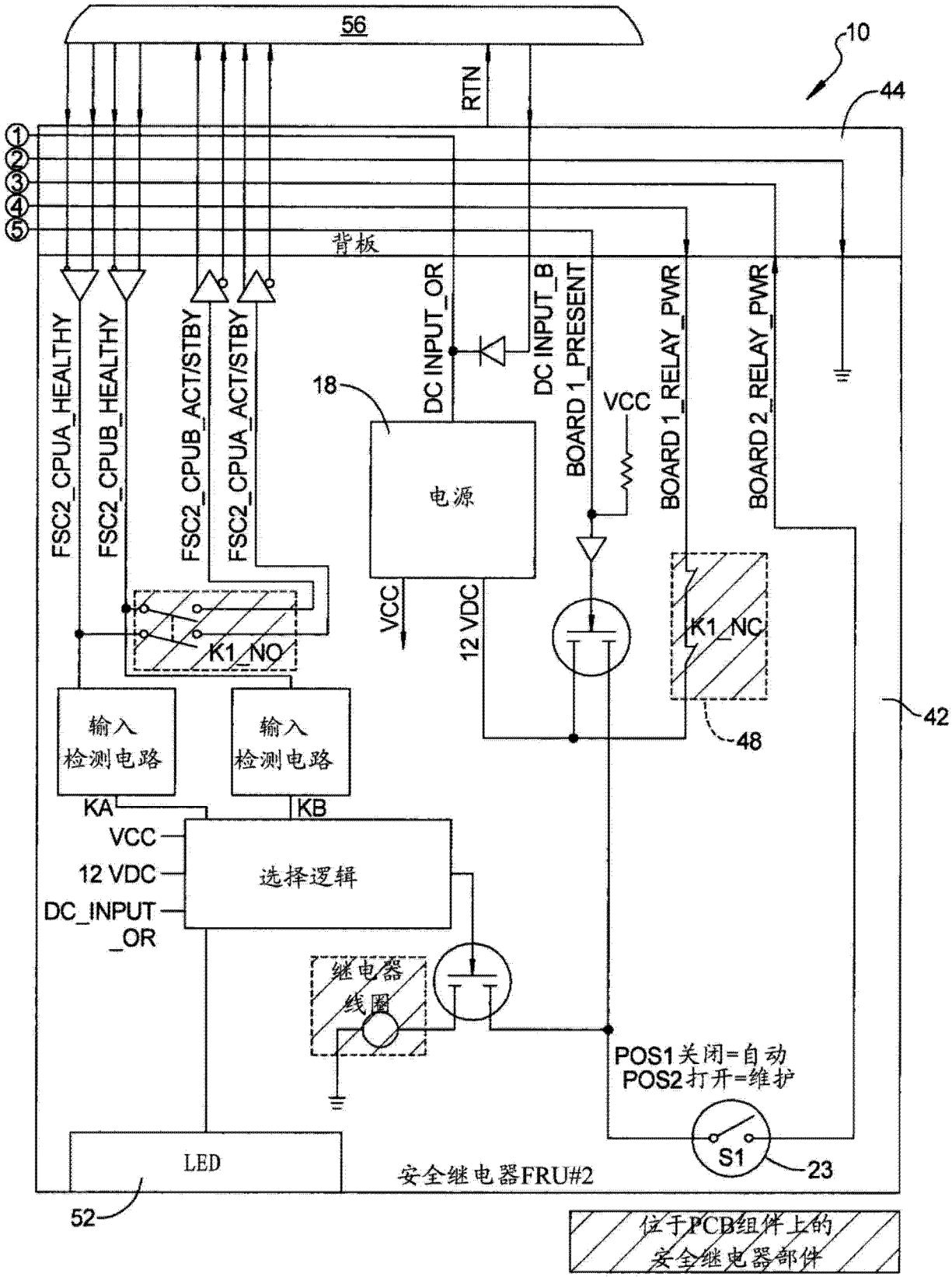

56
RTN
10
44
背板
FSC2_CPUA_HEALTHY
FSC2_CPUB_HEALTHY
FSC2_CPUB_ACT/STBY
FSC2_CPUA_ACT/STBY
DC INPUT_OR
DC INPUT_B
BOARD 1_PRESENT
BOARD 1_RELAY_PWR
BOARD 2_RELAY_PWR
18
电源
VCC
12 VDC
K1_NO
K1_NC
输入
检测电路
输入
检测电路
KA
KB
VCC
12 VDC
DC_INPUT
_OR
选择逻辑
继电器
线圈
42
48
POS1关闭=自动
POS2打开=维护
S1
23
LED
52
安全继电器FRU#2
位于PCB组件上的
安全继电器部件

图 7B