



(12) 发明专利

(10) 授权公告号 CN 101523038 B

(45) 授权公告日 2012. 11. 07

(21) 申请号 200780037760. 8

(51) Int. Cl.

(22) 申请日 2007. 09. 19

F02D 41/22 (2006. 01)

(30) 优先权数据

审查员 孙晶晶

102006048169. 0 2006. 10. 10 DE

(85) PCT申请进入国家阶段日

2009. 04. 09

(86) PCT申请的申请数据

PCT/EP2007/059904 2007. 09. 19

(87) PCT申请的公布数据

W02008/043650 DE 2008. 04. 17

(73) 专利权人 罗伯特·博世有限公司

地址 德国斯图加特

(72) 发明人 B·米勒 V·皮特扎尔

R·格梅利克

(74) 专利代理机构 中国专利代理(香港)有限公司
72001

代理人 曹若 梁冰

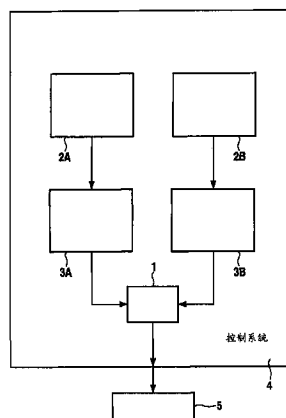
权利要求书 1 页 说明书 7 页 附图 4 页

(54) 发明名称

用于对内燃机的发动机控制系统的功能能力进行监控的方法和装置

(57) 摘要

本发明涉及一种用于对内燃机的发动机控制系统的功能能力进行监控的方法,其中,所述发动机控制系统具有多个执行单元(2A、2B)。在此在比较-运行模式(VM)中在所述系统的多个执行单元(2)上执行力矩监控程序并且将在执行所述监控程序时由所述执行单元(2)输出的信号彼此进行比较以识别故障。



1. 用于对在具有多个执行单元 (2) 的系统上运行的控制系统的功能能力进行监控的方法,

其中,在比较-运行模式 (VM) 中在所述系统的多个执行单元 (2) 上冗余地执行相同的监控任务,并且其中,将在执行监控任务时由这些执行单元 (2) 发出的信号彼此进行比较,以识别故障,其中,所述系统在执行所述监控任务之后切换为执行-运行模式 (PM),在该执行-运行模式 (PM) 中所述执行单元 (2) 执行不同的任务,其中,所述在执行-运行模式 (PM) 中执行的任务实施控制。

2. 按权利要求 1 所述的方法,

其中,所述监控任务由对由发动机产生的力矩进行监控的力矩监控任务构成。

3. 按权利要求 1 所述的方法,

其中,所述控制系统由发动机控制系统构成。

4. 按权利要求 1 所述的方法,

其中,所述监控任务同步地在所述执行单元 (2) 上执行。

5. 按权利要求 1 所述的方法,

其中,所述监控任务异步地在所述执行单元 (2) 上执行。

6. 按权利要求 1 所述的方法,

其中,周期性地执行所述监控任务。

7. 按权利要求 1 所述的方法,

其中,如果由执行单元 (2) 在执行监控任务时发出的信号彼此有偏差,则在执行所述监控任务时识别出故障。

8. 按权利要求 7 所述的方法,

其中,在执行所述监控任务时识别出故障之后切断由所述控制系统 (4) 控制的单元 (5)。

9. 具有多个执行单元的控制系统 (4),

其中,在比较-运行模式 (VM) 中在多个执行单元 (2) 上冗余地执行相同的监控任务并且将在执行监控任务时由所述执行单元 (2) 发出的信号彼此进行比较以识别故障,其中,所述系统在执行所述监控任务之后切换为执行-运行模式 (PM),在该执行-运行模式 (PM) 中所述执行单元 (2) 执行不同的任务,其中,所述在执行-运行模式 (PM) 中执行的任务实施控制。

10. 按权利要求 9 所述的控制系统,

其中,所述监控任务是对由发动机产生的力矩进行监控的力矩监控任务。

11. 按权利要求 9 所述的控制系统,

其中,所述控制系统 (4) 是发动机控制系统。

12. 按权利要求 9 所述的控制系统,

其中,所述执行单元 (2) 由 CPU、协处理器、数字式信号处理器 DSP、浮点计算单元 FPU 构成或者由算术逻辑单元 ALU 构成。

用于对内燃机的发动机控制系统的功能能力进行监控的方法和装置

技术领域

[0001] 本发明涉及一种对控制系统的功能能力进行监控的方法,该控制系统在具有多个执行单元的系统上运行。

背景技术

[0002] 在尤其在汽车技术中或在自动化技术中的嵌入式系统的领域中,有许多应用或者说应用程序,其中在硬件中的故障会引起潜在的对安全来说非常严重的后果。因此为了避免这种后果或者减少其影响,使用对所述的故障进行探测的监控措施。存在一些应用,在这样的应用中需要几乎永久地进行这样的监控。在其它的应用中使用监控功能,所述监控功能定期地比如周期性地或者根据特定的要求检查,数据处理系统或者其它的硬件-部件是否还正确地起作用。

[0003] 图 1 示出了发动机控制领域中一种传统的监控方法的结构。在发动机控制系统中,通过喷射系统将燃料喷入燃烧室中。从安全方面看,这种在发动机控制领域中的示范性的应用结构化三个层面 E1、E2、E3。喷射控制系统的应用程序形成了基础或者说基础层面 E1,该基础层面 E1 包含真正有待执行的功能。所述喷射控制系统表明,应该准确地在何时将多少燃料喷入燃烧室中。在所述喷射控制系统失灵时可能会出现这样的情况,即所述喷射控制系统朝燃烧室中喷射太多燃料或者说持续喷射燃料,使得汽车非常强烈地加速并且可能导致事故。因此,在传统的系统中设置了监控层面 E2,该监控层面监控,所述喷射控制系统在层面 E1 上是否无故障地工作。所述监控层面 E2 由附加的程序或者说附加的软件-代码构成,该软件代码必要时动用额外的传感器。在传统的发动机控制系统中,所述监控层面 E2 通常由连续的力矩监控装置构成,在该力矩监控装置中监控,当前由发动机产生的力矩是否没有超过特定的阈值。在传统的发动机控制系统中,所述喷射控制层面 E1 和监控层面 E2 的程序在相同的硬件上或者说在相同的执行单元上运行。因为在层面 E1 中的喷射控制系统的应用程序以及在层面 E2 中的力矩监控装置的应用程序在相同的执行单元或者说 CPU 上运行,所以执行单元中的硬件故障会导致不仅喷射控制系统而且力矩监控装置同时失灵。因此,出于安全原因,在传统的发动机控制系统中设置另外的安全层面 E3,该安全层面 E3 本身检查,所述监控层面 E2 是否正常工作。所述安全层面 E3 实施所述执行单元与外部的硬件-部件比如 ASIC 之间的问-答-通讯,其中原则上对所述执行单元或者说微型控制器的功能能力尤其对所述监控层面 E2 内部的应用程序的功能进行检查。所述监控层面 E2 的应用程序则实施可信度检查。比如所述监控层面 E2 的监控程序读入油门操纵踏板的角度位置 α 。如果由所述喷射控制层面 E1 的应用程序所表明的燃料量超过特定的、依赖于通过传感器监控的油门操纵踏板位置的阈值,那么所述在层面 E2 上运行的监控程序就发现,在喷射控制系统中出现了故障并且通常出于安全原因促使切断发动机。所述监控层面 E2 比如额外地包括力矩监控程序,该力矩监控程序对在发动机上产生的力矩进行监控并且在超过阈值时使发动机不起作用。为实施所述监控功能,所述监控程序的代码双

重地作为 E2' 来保存。在此用缺省 - 数据或者说检测数据对 E2' 的算法或者说程序进行核对。所述安全层面 E3 的比如在 ASIC 上也就是说在使用者所特有的集成线路上运行的程序将特定的位 - 模式作为问题加载到所述执行单元或者说 CPU 上, 所述执行单元用这个缺省值对所述以副本形式存在的、按层面 E2' 的监控程序进行核对并且在所述使用者所特有的集成线路 ASIC 中将应答 - 位 - 模式发送给所述层面 E3 的安全程序。所述安全程序将这个应答 - 位 - 模式与基准 - 位 - 模式进行比较, 以便确定在 CPU 内部的监控程序是否还在无故障地工作。在使用者所特有的集成线路内部的安全程序在另外的硬件也就是在 ASIC 上运行, 这不同于在执行单元或者说 CPU 上运行的监控程序。因此这种传统的处理方式构成相对于 CPU 内部的硬件故障的一定程度的安全性。

[0004] 不过, 所述传统的如在图 1 中示出的一样的安全方案的缺点在于, 所述用于指令测试的监控程序为了用缺省值或者说测试值进行核对必须以副本的形式存在。因此需要存储空间用于存放所复制的在所述监控层面 E2' 上的程序指令。

[0005] 在所述传统的指令测试中缺省数据或者说测试数据用作用于所复制的监控程序 E2' 的输入数据, 这种传统的指令测试的另一个缺点在于, 没有探测依赖于运算对象的故障。

发明内容

[0006] 因此, 本发明的任务是, 提供一种用于对控制系统的功能能力进行监控的方法, 该方法也可以探测依赖于运算对象的故障。

[0007] 本发明提供一种用于对控制系统的功能能力进行监控的方法, 其中所述控制系统在具有多个执行单元的系统上运行。其中在比较 - 运行模式 VM 中在所述系统的多个执行单元上执行监控程序并且其中将在执行所述监控程序时由这些执行单元输出的信号彼此进行比较, 以识别故障。

[0008] 按本发明的方法的优点在于, 没有浪费任何用于监控程序的所复制的程序指令的存储空间。

[0009] 在按本发明的方法的一种实施方式中, 所述监控程序由用于对由发动机产生的力矩进行监控的力矩监控程序构成。

[0010] 在按本发明的方法的一种实施方式中, 所述控制系统由发动机控制系统构成。

[0011] 在按本发明的方法的一种实施方式中, 所述监控程序同步地在所述执行单元上执行。

[0012] 在按本发明的方法的一种作为替代方案的实施方式中, 所述监控程序异步地在所述执行单元上执行。

[0013] 在按本发明的方法的一种实施方式中, 所述系统在执行所述监控程序之后切换为执行 - 运行模式, 在该执行 - 运行模式中所述执行单元执行不同的程序。

[0014] 在按本发明的方法的一种实施方式中, 所述在执行 - 运行模式中执行的程序实施控制。

[0015] 在按本发明的方法的一种实施方式中, 周期性地执行所述监控程序。

[0016] 在按本发明的方法的一种实施方式中, 在执行所述监控程序时识别出故障, 如果由执行单元在执行监控程序时发出的信号彼此间有偏差。

[0017] 在按本发明的方法的一种实施方式中,在执行监控程序时识别出故障之后切断由所述控制系统控制的单元。

[0018] 此外,本发明提供一种具有多个执行单元的控制系统,其中在比较-运行模式 VM 中在多个执行单元上执行监控程序,并且将在执行监控程序时由所述执行单元发出的信号彼此进行比较,以识别出故障。

[0019] 在按本发明的控制系统的一种实施方式中,所述监控程序是用于对由发动机产生的力矩进行监控的力矩监控程序。

[0020] 在按本发明的控制系统的一种实施方式中,所述控制系统是发动机控制系统。

[0021] 在按本发明的控制系统的一种实施方式中,所述执行单元由微处理器、协处理器 (Co-Prozessor)、数字式信号-处理器 DSP、浮点计算单元 FPU 或者由算术逻辑单元 ALU 构成。

附图说明

[0022] 下面,在参照用于对那些对本发明来说十分重要的特征进行解释的附图的情况下对按本发明的方法及按本发明的控制系统的优选的实施方式进行说明。其中:

[0023] 图 1 是一张图表,该图表用于表示传统的具有三个层面的安全方案;

[0024] 图 2 是在按本发明的方法中使用的转换和比较单元的框图;

[0025] 图 3 是一张框图,该框图用于表示按本发明的控制系统的一种可能的实施方式;

[0026] 图 4 是用于对按本发明的方法进行解释的流程图;

[0027] 图 5 是用于对按本发明的方法的一种可能的实施方式进行解释的时间流程图。

具体实施方式

[0028] 如可以从图 2 中看出的一样,转换和比较电路 1 在输入侧连接到 $N+1$ 个执行单元 2 上并且从所述执行单元 $2-i$ 上得到逻辑的输入信号 $E_0, E_1, E_2, E_3, \dots, E_N$ 。所述转换和比较单元 1 包括比较逻辑电路 1A 和开关逻辑电路 1B。

[0029] 所述在图 2 中示出的系统可以在至少两种运行模式中运行。在一种用于提高功率的、也称为执行-运行模式 PM 的第一运行模式中,所述执行单元 $1-i$ 或者说核心 (Cores) 平行地处理不同的程序或者说任务。所述执行单元 $2-i$ 可以是用于执行计算指令的任意的执行单元 $2-i$, 比如是处理器、浮点计算单元 FPU、数字式信号处理器 DSP、协处理器 (Co-Prozessor) 或者是算术逻辑计算单元 ALU。可以在执行模式 PM 中通过不同的执行单元 $2-i$ 同步或异步地执行程序的处理。在功率模式中,不进行任何冗余的处理,而是所述执行单元 $2-i$ 平行地执行不同的计算或者说程序。在纯粹的执行-运行模式 PM 中,将所有的输入信号 E_i 转换到或者说引到相应的输出信号 A_i 上。

[0030] 除了超标量的计算系统的使用之外,用于多核的架构的第二原因在于,提高信号处理的安全性,方法是多个执行单元 $2-i$ 冗余地处理相同的程序。在这种也称为安全模式或者说 Safety Mode 或者比较-运行模式 VM 的第二运行模式中,通过所述转换和比较电路 1 对所述执行单元的结果或者说逻辑的输出信号彼此进行比较,从而可以通过在一致性方面的比较来识别出现的故障或者说信号偏差。因此,在纯粹的比较-运行模式 VM 中,将所有输入信号 E_i 引到或者说变换到 (abbilden) 刚好一个唯一的输出信号 A_i 。也可以考虑混

合形式。在可配置的开关逻辑电路 1B 中说明,设置了多少输出接头或者说输出信号 A_i 。此外,在所述开关逻辑电路 1B 中记录,哪些输入信号 E_i 有助于哪一个输出信号 A_i 。由此,在所述开关逻辑电路 1B 中保存了变换函数,该变换函数将输入信号 E_i 分配给不同的输出信号 A_i 。

[0031] 所述处理逻辑电路 1A 在每个输出信号 A_i 上确定,所述输入信号以何种形式有助于相应的输出信号。比如,所述输出信号 A_0 由所述输入信号 $E_1, \dots, E_N$ 所产生。对于 $m = 1$ 来说,这简单地相当于一个输入信号的转换。对于 $M = 2$ 来说,将两个输入信号 E_1, E_2 彼此进行比较。这种比较可以同步或者异步地通过所述电路 1 进行。在这种情况下,按位进行这种比较或者作为替代方案仅仅将重要的位彼此进行比较。在 $M \geq 3$ 时存在不同的方案。第一方案在于,将所有信号彼此进行比较并且在存在至少两个不同的数值时探测到故障,该故障可选通过所述转换和比较电路 1 表示出来。另一种方案在于,执行“Kausm”选择(从 m 个中选出 K 个),其中 $K > M/2$ 。这在一种实施方式中通过比较器的设置来实现。在此如果所述输入信号中的一个输入信号被发现与其它的输入信号有偏差,就可选地产生第一故障信号。在第二故障信号不同于所述第一故障信号时,所有三个输入信号彼此间都有偏差。在另一种实施方式中,将所述输入信号值输送给另外的计算单元,该另外的计算单元比如计算一个平均值或者说一个中位值或者说实施一种容错的算法 FTA。在容错的算法中,删除或者说忽略所述输入信号值的极限值,并且将剩余的信号值求平均。在一种实施方式中,将剩余的信号值的整个量求平均。在一种作为替代方案的实施方式中,将剩余的信号值的在硬件中可轻易形成的部分量求平均。在形成平均值时仅仅必须进行加法和除法运算,而 FTM、FTA 或者中位值形成则部分地要求对所述输入信号值进行分类。在一种实施方式中,在出现足够大的信号偏差或者说极限值时可选输出或者说显示故障信号。所提到的将信号处理成信号的不同方案就是比较运算。所述处理逻辑电路 1A 为每个输出信号 A_i 以及由此也为所述输入信号 E_i 确定有待进行的比较运算的精确结构。在所述开关逻辑电路 1B 内部的信息的组合,也就是说每个输出信号或者说每个函数值的在处理逻辑电路 1A 中说明的比较运算的分配函数表示一种运行模式信息并且确定所述运行模式。这个信息通常是多值的并且通过多于一个的逻辑位来表示。对于仅仅设置了两个执行单元 $2-i$ 并且由此仅仅存在一个比较模式这种情况来说,可以将全部信息在所述运行模式中补偿到一个唯一的逻辑位上。

[0032] 通常通过以下方法将系统从所述执行-运行模式 PM 转换为比较-运行模式 VM,即将所述在执行-运行模式 PM 中变换或者说转换成不同的信号输出的执行单元 $2-i$ 在所述比较-运行模式 VM 中变换或者说转换成相同的信号输出。这一点优选通过以下方式来实现,即设置部分量的执行单元 $2-i$,在这些执行单元 $2-i$ 上在所述执行-运行模式 PM 中将所有要在所述部分量中加以考虑的输入信号 E_i 直接转换为相对应的输出信号 A_i ,而在所述比较模式 VM 中的输入信号则全部变换为一个唯一的信号输出或者转换成这个唯一的信号输出。作为替代方案,可以通过改变配对这种方式来实现转换。

[0033] 在所述不同的运行模式之间,可以在通过软件进行控制的情况下动态地在连续的运行过程中进行转换。在一种实施方式中,通过特殊的转换指令或者说转换指示、特殊的指示序列、明确表示出来的指示的执行或者通过所述系统的至少其中一个执行单元 $2-i$ 来访问特定的地址这种方式来触发转换。

[0034] 在所述安全模式 VM 中进行冗余的处理和检查并且在所述功率或者说执行 - 运行模式 PM 中通过单独的程序处理来提高功率,在这两种模式之间的转换通过转换装置 1 进行。在一种实施方式中,为进行转换,通过一个特征标记来标记出程序、应用程序、程序部分或者也标记出程序指令,通过该特征标记可以发现,这些程序指令是否对安全来说十分重要,也就是说是否必须在所述安全运行模式或者说比较 - 运行模式 VM 中进行处理,或者是否可以供所述功率或者说执行 - 运行模式 PM 使用。可以通过在程序指令中的位进行标识。作为替代方案,可以通过特殊的程序指令来标记出紧随其后的序列。

[0035] 在所述安全运行模式或者说 Safety Mode VM 中,在不同的执行单元 2-i 上进行同步处理时所述执行单元 2-i 的结果或者说输出信号的计算持续相同时间。而后所述结果在安全运行模式 VM 中同步处理时同时提供给所述转换装置 1。如果结果一致,那就释放相应的数据。在有信号偏差时,则进行预先给定的故障反应。

[0036] 如果所述系统处于执行 - 运行模式 PM 中,那就平行处理所述程序并且没有触发在所述转换和比较电路 1 内部的比较器。

[0037] 在按本发明的用于对在具有多个执行单元 2 的系统上运行的控制系统的功能能力进行监控的方法中,在比较 - 运行模式 VM 中在所述系统的多个或者甚至所有的执行单元上执行至少一个监控程序。将在执行该监控程序时由这些执行单元 2 输出的信号彼此进行比较,以识别故障。在按本发明的控制系统的一种优选的实施方式中,该控制系统具有至少三个执行单元 2。那个和其余的信号之间具有最大的信号偏差的信号比如借助于多数决定被识别为有故障的。所述信号在一种实施方式中是数字的逻辑信号,尤其是二进制的信号。按本发明的控制系统 4 在一种优选的实施方式中是用于控制内燃机的发动机控制系统。在作为替代方案的实施方式中,所述控制系统 4 是用于触发电动机的控制系统。所述监控程序比如由对通过内燃机或电动机产生的力矩进行监控的力矩监控程序构成。在此,所述监控程序可以同步地或异步地在所述执行单元 2 上执行。

[0038] 在按本发明的方法中,用于发动机控制的标准的应用程序在所述执行 - 运行模式 PM 中执行,也就是说所述系统的每个执行单元 2 为提高功率而执行用于控制的程序,而其它的执行单元 2 方面则执行与此不同的应用程序。在层面 E2 上运行的监控程序在按本发明的方法的一种可能的实施方式中周期性地被调用。在按本发明的方法中,所述监控程序在比较 - 运行模式 VM 中在所述系统的多个执行单元 2 上执行。在所述比较 - 运行模式 VM 中,所述系统的多个或者说所有的执行单元 2 执行相同的监控程序,其中将在这过程中产生的输出信号彼此进行比较,以识别故障。在一种可能的实施方式中,在层面 E2 上执行多个监控程序,这些监控程序比如全部周期性地被调用。所有被调用的监控程序在所述比较 - 运行模式 VM 中执行。在一种作为替代方案的实施方式中,所述监控程序根据特定的要求或者说要求指令被调用,并且随后在比较 - 运行模式 VM 中由所述系统的多个或者说至少两个执行单元 2 来执行。所述的用于执行所述监控程序的要求指令可以比如通过中断 (Interrupt) 来触发。

[0039] 在执行所述监控程序之后,所述系统换回到执行 - 运行模式 PM 中,在该执行 - 运行模式 PM 中所述执行单元 2 优选执行第一层面 E1 的不同的程序比如控制程序。

[0040] 在按本发明的方法的一种实施方式中,在所述层面 E2 中执行监控程序时识别出故障,如果由执行单元 2 在所述比较 - 运行模式 VM 中执行监控程序时输出的信号彼此有偏

差。在这种情况下,优选在执行监控程序时识别出故障之后切断由所述控制系统 4 所控制的单元 5 比如发动机。

[0041] 图 3 示出了按本发明的控制系统的一种可能的实施方式的框图。在图 3 所示的实施方式中,按本发明的控制系统 4 具有两个执行单元 2A、2B。所述执行单元 2A、2B 可以是完整的微处理器或者说 CPU,可以是协处理器、数字式信号处理器 DSP、浮点计算单元 FPU 或者可以是算术逻辑单元 ALU。在按本发明的控制系统 4 的其它实施方式中,设置了两个以上的执行单元 2。在图 3 所示的简单的实施方式中,由执行单元 2A、2B 产生的信号相应地中间保存在中间存储器 3A、3B 中。每个执行单元 2 优选在输出端具有自己的中间存储器 3。所述执行单元 2A、2B 的中间存储的结果或者说输出信号被输送给比较单元 1。所述比较单元 4 可以比如由如在图 2 中示出的一样的转换和比较电路 1 构成。所述中间保存的输出信号的比较可以通过相应的比较程序和软件的运行或者以固定布线的方式在硬件中执行。

[0042] 图 4 示出了按本发明的用于对控制系统的功能能力进行监控的方法的一种可能的实施方式的流程图。

[0043] 在第二个层面 E2 中调用监控程序之后,在步骤 S1 中将系统从所述执行-运行模式 PM 切换为比较-运行模式 VM。随后激活所述两个如在图 3 中所示的执行单元 2A、2B 用于在步骤 S2、S3 中执行相同的监控程序,并且执行相同的监控程序比如力矩监控程序。在图 4 所示的实施方式中,所述两个执行单元 2A、2B 在步骤 S2、S3 中异步地计算相应的结果信号,该结果信号在步骤 S4、S5 中被中间保存在相应的中间存储器 3A、3B 中。在一种作为替代方案的实施方式中,所述两个执行单元 2A、2B 在步骤 S2、S3 中彼此同步地计算相应的输出信号或者说结果值。在存在两个结果值或者说输出信号之后,在步骤 S6 中优选通过所述切换和比较电路 1 在这两个输出信号之间进行比较。如果这两个信号彼此有偏差,那就识别出故障并且随后进行相应的故障处理。在一种对安全来说十分重要的应用中,切断由所述控制系统 4 触发的单元 5,比如发动机。在步骤 S6 中的比较要么可以在随后读出所述中间存储器 3A、3B 之后通过相应的借助于软件进行的比较运算来进行,要么在一种作为替代方案的实施方式中通过固定布线的线路来进行比较。

[0044] 图 5 示出了用于对按本发明的方法的一种可能的实施方式进行解释的时间流程图。在该实施方式中,所述监控程序在层面 E2 中周期性地被调用,并且在所述比较-运行模式 VM 中通过多个执行单元 2 同时执行。在执行所述监控程序之后,系统返回到所述执行-运行模式 PM 中并且在层面 E1 中执行真正的控制程序。

[0045] 在按本发明的控制系统 4 的一种作为替代方案的实施方式中,所述控制系统 4 始终在执行-运行模式 PM 中工作,其中用至少两个执行单元 2 异步地计算所述监控程序。在此将由执行单元在这过程中输出的结果或者说输出信号彼此进行比较,以识别故障。当然,在该实施方式中,必须相应地中间保存所述结果并且随后将所述结果彼此比较两次,也就是一次在第一执行单元 2A 上进行比较并且一次在第二执行单元 2B 上进行比较,以便对所述两个执行单元 2 的可能的硬件故障加以考虑。因此,这种实施方式比一种在所述比较-运行模式 VM 中执行监控程序的实施方式更加麻烦。

[0046] 按本发明的方法也允许探测依赖于运算对象的故障。除此以外,按本发明的方法与传统的在图 1 中示出的安全方案相比也明显地节省了存储空间。

[0047] 在按本发明的控制系统 4 的一种可能的实施方式中,该控制系统 4 具有至少三个

执行单元 2, 其中借助于多数决定在出现信号偏差时可以确定, 哪个执行单元 2 可能在有故障的情况下工作。这个执行单元 2 随后优选进行自测, 以便确定这个执行单元 2 是否实际上已失灵。在一种实施方式中, 如果所述自测表明所述执行单元 2 实际上已失灵, 就使所述执行单元 2 不起作用。在这种实施方式中, 系统由此甚至在容错的情况下进行工作。

[0048] 为防止在两个核心或者说执行单元 2 中出现比如因制造误差而产生的永久故障, 在按本发明的方法的一种可能的实施方式中, 所述执行单元 2 分别进行自测。

[0049] 在按本发明的方法的一种可能的实施方式中, 在层面 E2 中在所述比较 - 运行模式 VM 中执行监控程序, 其中为进一步保险起见额外地设置了安全层面 E3, 该安全层面 E3 继续执行用于对所述监控程序的功能能力进行监控的指令测试。一种所述的实施方式在对安全来说特别关键的应用中是可能的。

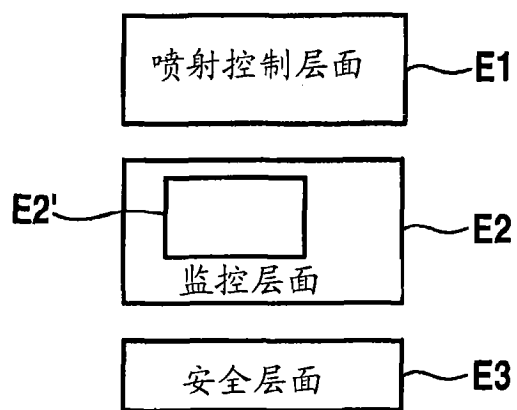


图 1

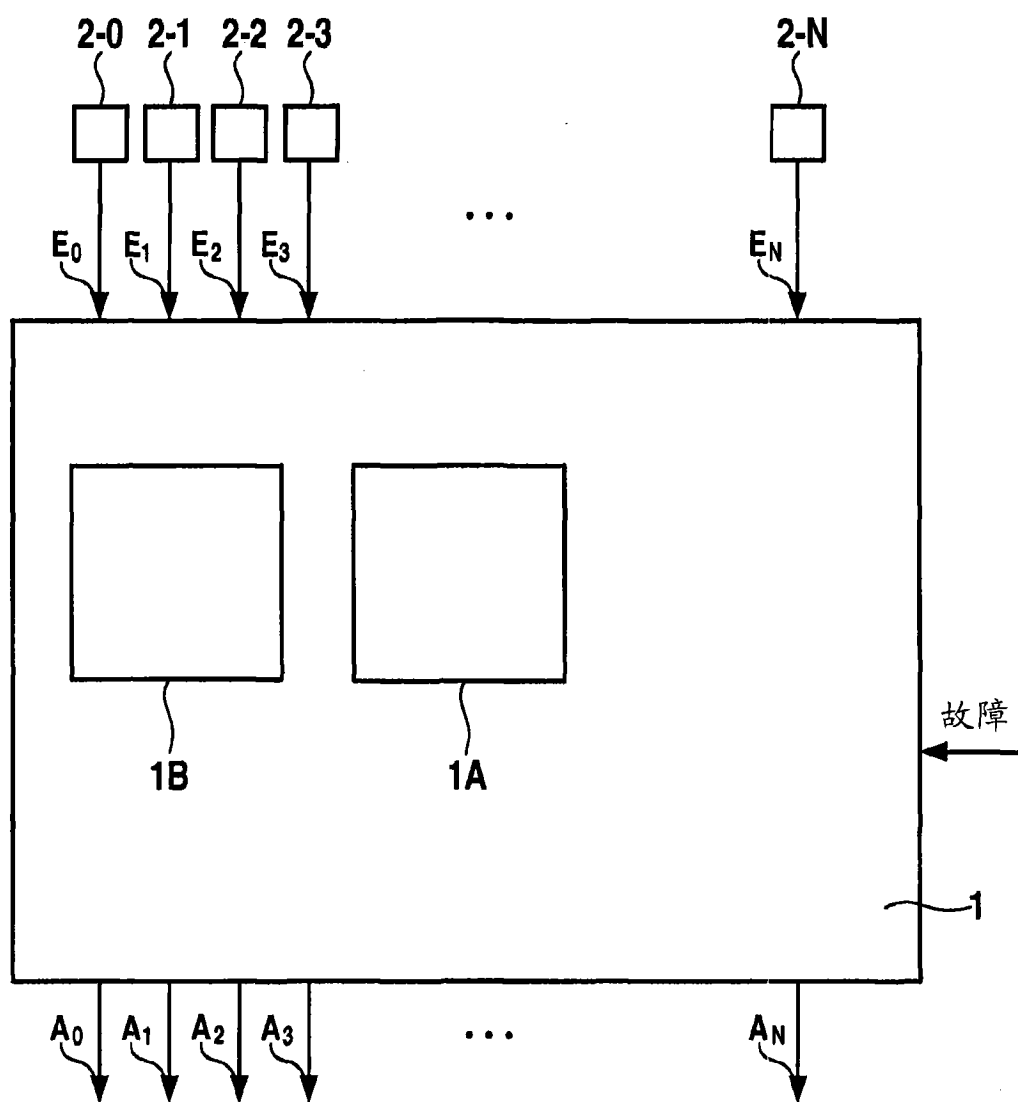


图 2

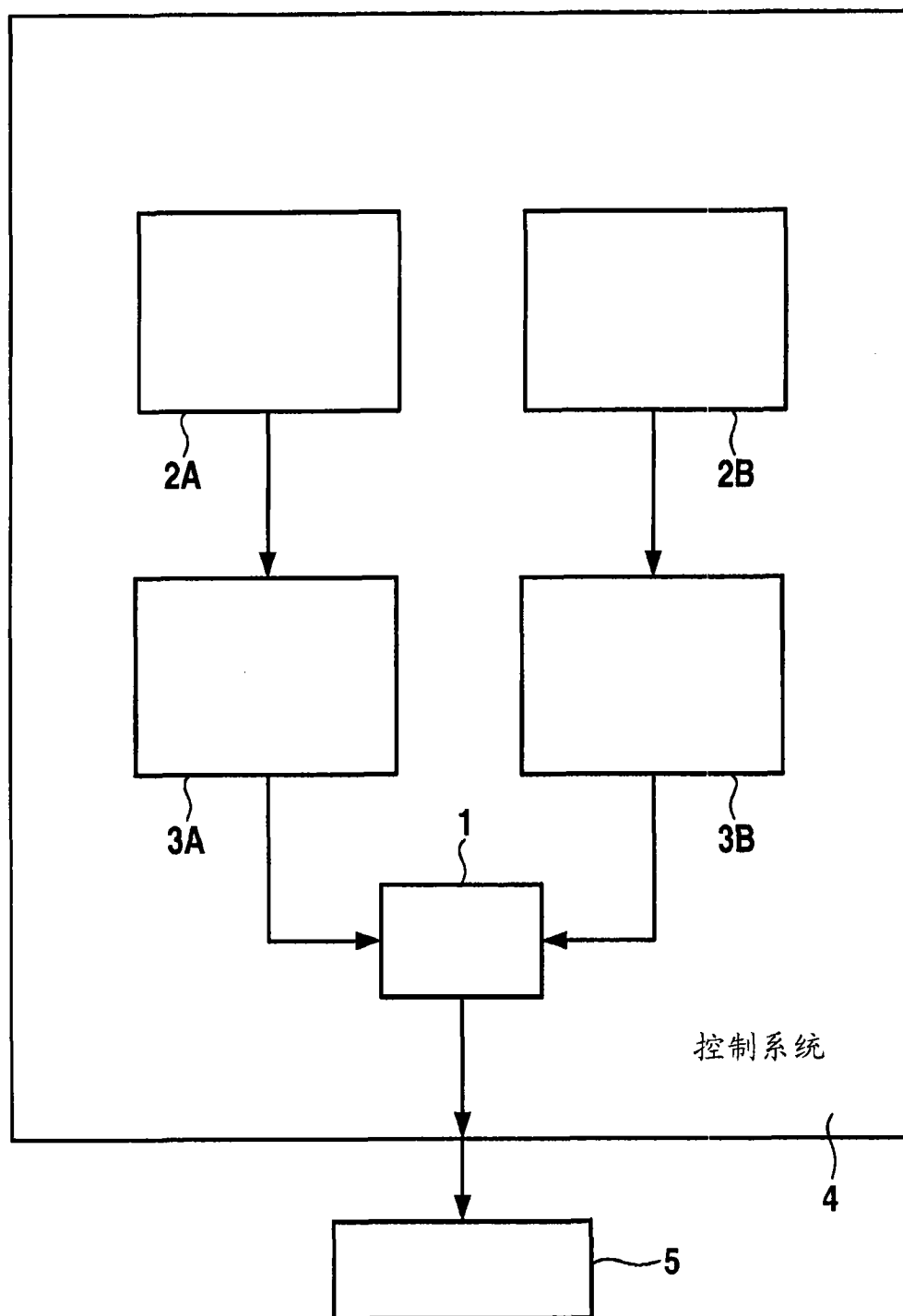


图 3

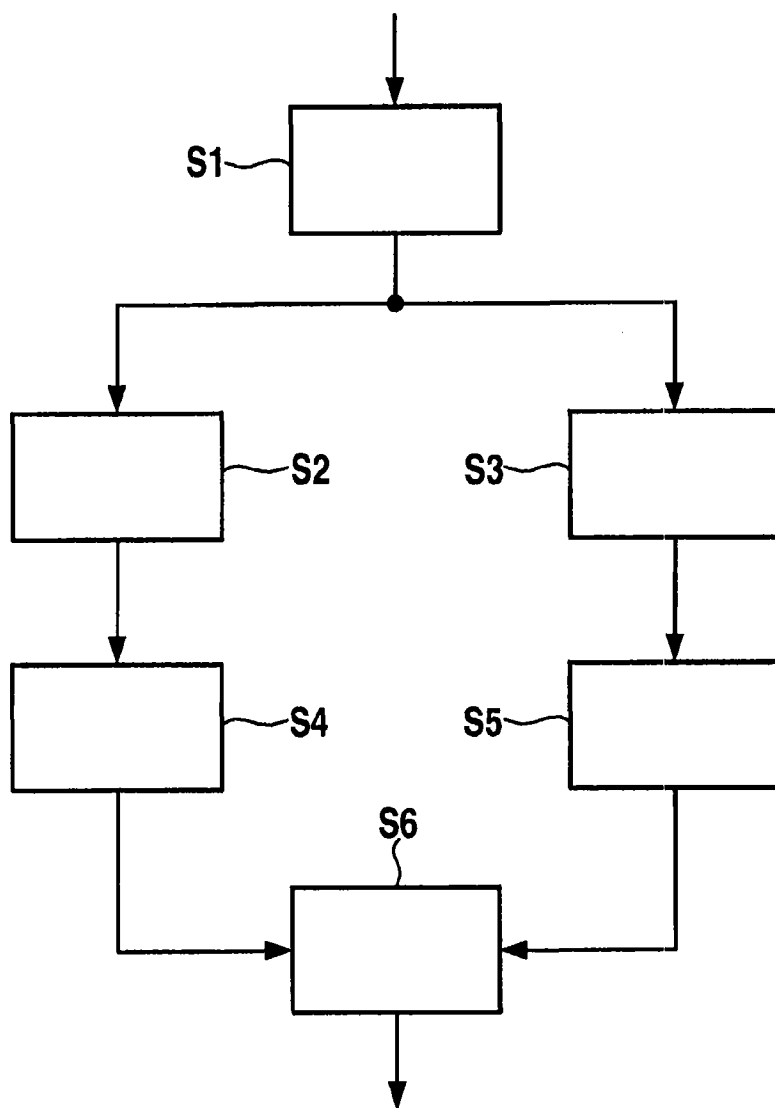


图 4

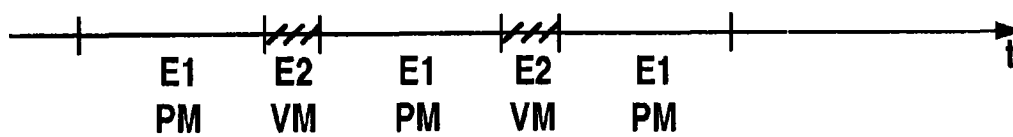


图 5