(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107407919 B
(45)授权公告日 2020.08.25

(21)申请号 201680013710.5

(22)申请日 2016.02.26

(65)同一申请的已公布的文献号
申请公布号 CN 107407919 A

(43)申请公布日 2017.11.28

(30)优先权数据
15157511.5 2015.03.04 EP

(85)PCT国际申请进入国家阶段日
2017.09.04

(86)PCT国际申请的申请数据
PCT/EP2016/054097 2016.02.26

(87)PCT国际申请的公布数据
WO2016/139147 EN 2016.09.09

(73)专利权人 ABB股份公司
地址 德国曼海姆

(72)发明人 F·戴 B·马蒂亚斯 H·丁 C·拜纳 Y·韦里哈

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杨忠 李强

(51)Int.Cl.
G05B 19/048(2006.01)
G05B 23/02(2006.01)

(56)对比文件
CN 103249530 A,2013.08.14
CN 101490283 A,2009.07.22
DE 102009051146 A1,2011.04.28

审查员 尚伟昊

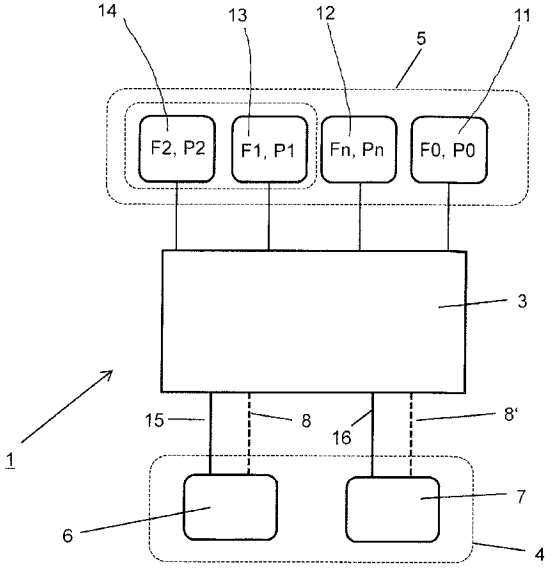
权利要求书3页 说明书13页 附图6页

(54)发明名称

安全控制系统和安全控制系统的运行方法

(57)摘要

一种安全控制系统(1),包括控制单元(3)、安全传感器(4)和机器组件(5),机器组件(5)可在不同的运行模式(F_0,F_N,F_1,F_2)下运行,各运行模式具有机器组件(5)的不同的生产率(P_0,P_N,P_1,P_2),其中控制单元(3)激活机器组件(5)的运行模式(F_0,F_N,F_1,F_2),其中至少一个安全传感器组件(4)具有两个功能性冗余子系统(6,7),对控制单元(3)的输入包括指示所述子系统(6,7)的可用性的信息(8),在控制逻辑(3)可在所有子系统(6,7)都可用的情况下,激活具有正常生产率(P_N)的正常运行模式(F_N),在所有子系统(6,7)都不可用时,激活具有零生产率(P_0)的失效-停止运行模式(F_0),在至少一个子系统(6,7)可用而至少另一个子系统(6,7)不可用时,激活具有小于正常值的非零生产率的失效-运行运行模式(F1,F2)。



CN 107407919 B

1.一种安全控制系统(1),所述安全控制系统(1)包括:

a)控制单元(3),其包括安全控制逻辑;

b)至少一个安全传感器组件(4);

c)至少一个机器组件(5),其可在不同的运行模式(F_0,F_N,F_1,F_2)下运行,其中各运行模式以所述机器组件(5)的不同生产率(P_0,P_N,P_1,P_2)为特征,其中所述至少一个机器组件(5)具有标称生产率;由此

d)所述控制单元(3)从所述至少一个安全传感器组件(4)接收输入且评估所述输入;和

e)作为对所述评估的结果的反应,激活由所述安全控制逻辑确定的所述机器组件(5)的运行模式(F_0,F_N,F_1,F_2),

其特征在于

(1)所述至少一个安全传感器组件(4)具有至少两个功能性冗余子系统(6,7),

(2)对所述控制单元(3)的输入包括指示所述至少两个功能性冗余子系统(6,7)的可用性的信息(8),

(3)所述安全控制逻辑配置成

i.在所述输入指示所有功能性冗余子系统(6,7)都可用的情况下,激活以正常生产率(P_N)为特征的正常运行模式(F_N),

ii.在所述输入指示所有功能性冗余子系统(6,7)都不可用的情况下,激活以零生产率(P_0)为特征的失效-停止运行模式(F_0),

iii.在所述输入指示所述功能性冗余子系统(6,7)中的至少一个至少临时不可用而其至少另一个可用的情况下,激活以小于正常值但高于零的生产率为特征的失效-运行运行模式;且其中,

所述安全控制系统(1)还包括:

- 第一安全区域(Z_1)和第二安全区域(Z_2),由此所述第一安全区域(Z_1)是所述第二安全区域(Z_2)的子集,

且所述至少两个功能性冗余子系统(6,7)包括:第一功能性冗余子系统(D_1,6),其配置为用于检测在所述第一安全区域(Z_1)中的第一危险事件(H_1),和- 第二功能性冗余子系统(D_2,7),其配置为用于检测在所述第二安全区域(Z_2)中的第二危险事件(H_2),

其中第一失效-运行模式(F_1)导致大于零但小于所述正常生产率(P_N)的第一降低的机器生产率(P_1),且第二失效-运行模式(F_2)导致大于零但小于所述标称生产率并高于所述第一降低的机器生产率(P_1)的第二降低的机器生产率(P_2),

其中所述安全控制逻辑在对所述安全控制逻辑的输入指示两个功能性冗余子系统(D_1,6;D_2,7)都可用并指示在所述第二安全区域(Z_2)中有第二危险事件(H_2)而在所述第一安全区域(Z_1)中没有第一危险事件的情况下激活所述第二失效-运行模式(F_2),且其中所述安全控制逻辑在对所述安全控制逻辑的输入指示所述第一功能性冗余子系统(D_1,6)临时不可用而第二功能性冗余子系统(D_2,7)可用并指示在所述第二安全区域(Z_2)中有第二危险事件(H_2)的情况下激活所述第一失效-运行模式(F_1)。

2.根据权利要求1所述的安全控制系统(1),其特征在于,所述安全控制逻辑在对所述安全控制逻辑的输入指示所述第一功能性冗余子系统(D_1,6)可用而所述第二功能性冗余子系统(D_2,7)至少临时不可用并指示在第一安全区域(Z_1)中没有第一危险事件(H_1)的情况

下激活所述第二失效-运行模式(F_2)。

3.根据权利要求1所述的安全控制系统(1),其特征在于,所述安全控制逻辑在对所述安全控制逻辑的输入指示所述第二功能性冗余子系统(D_2,7)至少临时不可用并指示在第一安全区域(Z_1)中有第一危险事件(H_1)的情况下激活所述第一失效-运行模式(F_1)。

4.根据权利要求1所述的安全控制系统(1),其特征在于,所述安全控制逻辑在对所述安全控制逻辑的输入指示所述第一和第二功能性冗余子系统(D_1,6;D_2,7)二者都可用并指示在所述第一和第二安全区域(Z_1,Z_2)二者中有第一和第二危险事件(H_1,H_2)的情况下激活所述第一失效-运行模式(F_1)。

5.根据前述权利要求中的任一项所述的安全控制系统(1),其特征在于,所述机器组件(5)为机器人或自主导引车或离散制造系统或制造基元。

6.根据权利要求1-4中的任一项所述的安全控制系统(1),其特征在于,所述机器组件(5)的生产率为所述机器组件(5)的活动部分的速度。

7.根据权利要求1-4中的任一项所述的安全控制系统(1),其特征在于,所述第一或所述第二功能性冗余子系统(D1,6;D2,7)为接近传感器或挡光板或激光扫描仪或摄像头。

8.根据权利要求1-4中的任一项所述的安全控制系统(1),其特征在于,由临时的通信错误引起功能性冗余子系统的临时的不可用性。

9.根据权利要求8所述的安全控制系统(1),其特征在于,所述临时的通信错误为循环冗余错误或看门狗错误。

10.一种安全控制系统(1)的运行方法,所述安全控制系统(1)包括

- 控制单元(3),其包括安全控制逻辑,

- 至少一个安全传感器组件(4),

- 第一安全区域(Z_1)和第二安全区域(Z_2),由此所述第一安全区域(Z_1)是所述第二安全区域(Z_2)的子集,

- 至少一个机器组件(5),其可在不同的运行模式(F_0,F_N,F_1,F_2)下运行,其中各运行模式以所述机器组件(5)的不同生产率(P_0,P_N,P_1,P_2)为特征,其中所述至少一个机器组件(5)具有标称生产率,且其中,第一失效-运行模式(F_1)导致大于零但小于正常生产率(P_N)的第一降低的机器生产率(P_1),且第二失效-运行模式(F_2)导致大于零但小于所述标称生产率并高于所述第一降低的机器生产率(P_1)的第二降低的机器生产率(P_2),由此

- 所述控制单元(3)从所述至少一个安全传感器组件(4)接收输入和评估所述输入,和

- 作为对所述评估的结果的反应,激活由所述安全控制逻辑确定的所述机器组件(5)的运行模式(F_0,F_N,F_1,F_2),

- 所述至少一个安全传感器组件(4)具有至少两个功能性冗余子系统(6,7),其中,所述至少两个功能性冗余子系统(6,7)包括:第一功能性冗余子系统(D_1,6),其配置为用于检测在所述第一安全区域(Z_1)中的第一危险事件(H_1),和- 第二功能性冗余子系统(D_2,7),其配置为用于检测在所述第二安全区域(Z_2)中的第二危险事件(H_2),

- 对所述控制单元(3)的输入包括指示所述至少两个功能性冗余子系统(6,7)的可用性的信息(8),

其特征在于以下步骤

- 在所述输入指示所有功能性冗余子系统(6,7)可用的情况下激活以正常生产率(P_N)

为特征的正常运行模式(F_N)，

- 在所述输入指示所有功能性冗余子系统(6,7)不可用的情况下激活以零生产率(P_0)为特征的失效-停止运行模式(F_0)，

- 在输入指示所述功能性冗余子系统(6,7)中的至少一个至少临时不可用而其至少另一个可用的情况下激活生产率小于正常值但是大于零的失效-运行运行模式；

- 在对所述安全控制逻辑的输入指示两个功能性冗余子系统(D_1,6;D_2,7)都可用并指示在所述第二安全区域(Z_2)中有第二危险事件(H_2)而在所述第一安全区域(Z_1)中没有第一危险事件的情况下激活所述第二失效-运行模式(F_2)；以及

- 在对所述安全控制逻辑的输入指示所述第一功能性冗余子系统(D_1,6)临时不可用而第二功能性冗余子系统(D_2,7)可用并指示在所述第二安全区域(Z_2)中有第二危险事件(H_2)的情况下激活所述第一失效-运行模式(F_1)。

安全控制系统和安全控制系统的运行方法

技术领域

[0001] 本发明涉及安全控制系统，根据权利要求1的前序，所述系统包括包括安全控制逻辑的控制单元，进一步包括至少一个安全传感器组件，进一步包括至少一个可在不同运行模式下运行的机器组件，其中各运行模式以机器组件的不同生产率为特征，其中控制单元从至少一个安全传感器组件接收输入并评估输入，并且作为对评估的结果反应，激活由安全控制逻辑确定的机器组件的运行模式。

[0002] 本发明也涉及安全控制系统的运行方法，所述系统包括包括安全控制逻辑的控制单元，进一步包括至少一个安全传感器组件，进一步包括至少一个可在不同运行模式下运行的机器组件，其中各运行模式以机器组件的不同生产率为特征，其中控制单元从至少一个安全传感器组件接收输入并评估输入，并且作为对评估的结果的反应，激活由安全控制逻辑确定的机器组件的运行模式。

背景技术

[0003] 一般来说，本发明涉及在离散制造环境或制造现场中的安全控制。用语“机器”旨在包括制造现场的任何单独的机器或子系统，例如机器人、装配机、制造基元或甚至是在制造现场内用来在不同的制造基元或子系统之间自动移动的自主导引车(AGV)。

[0004] 当在制造现场工作或进入制造现场中时，在离散制造中的安全控制具有保护人不受危险的主要目标。基本上，传感器或开关用来通知安全控制装置在特定区域中存在人或他们试图进入这种区域。基于自动制造过程的实际状况，生产线或单独的装置进入使潜在危险降低至或限制在规定的可接受范围内的状态。很多时候，通过停止机器实现这一点，但有时降低运动速度，或限制特定机构(例如工业机器人或机器工具)的移动空间也足以实现这一点。

[0005] 在大多数情况下，实施停止机器，同时使用具有安全停止功能(STO)的驱动器。在工业机器人的情况下，机器人控制器也进行机器人的安全控制，其中通常实施机器人工具位置和速度的监控。也已知使用提供安全速度或位置控制的驱动器。

[0006] 在(潜在的)严重危险的情况下，例如经由紧急停止按钮或对应的传感器装置，触发紧急停止。其使机器进入安全停止状态，这需要专门的确认才能重启机器。

[0007] 用于实现其保护人不受危险的主要目标的安全控制依赖于传感器和开关的正常运行的可用性。

[0008] 但是例如在内部诊断功能检测到电源失效的情况下，传感器和开关可能失效。或在传感器或开关和控制逻辑之间的通信可能有故障。因此当实施安全控制时，控制逻辑需要具有用于处理当传感器或开关不可用的情形(例如在内部停止的情况下，其也可被称为钝化)时的安全概念。

[0009] 另一个原因可能在于在传感器和开关与控制逻辑之间的通信处于有故障的状态。传感器或开关的钝化或换句话说不可用性或在传感器或开关和控制逻辑之间的通信被干扰总结为用语“失效情形”，相对于前面解释的“危险情形”截然不同。

[0010] 控制逻辑还包括在这种失效情形下的预定义反应。

[0011] 在现有技术已知的状态中，对失效情形的反应与对危险情形的反应相同。因此在检测到对安全传感器的通信有故障或传感器组件本身失效的情况下，即使没有检测到危险情形，仍激活对应的紧急功能模式。这是根据停止类别0或1的机器停止与人工复位/重启机器的组合。机器的生产率降低。

[0012] 但是通常，失效情形，例如传感器的不可用性仅仅是临时的，且在某个时间内或多或少地自动被解决。在现有技术的状态中，机器不管怎样被停止，都致使不必要的生产损失。

发明内容

[0013] 因此，本发明的目的是改进安全控制系统和安全控制系统的运行方法，用于控制机器使得在如上所述的失效情形的情况下降低生产损失。

[0014] 根据本发明通过具有权利要求1的特征的安全控制系统实现关于改进安全控制系统的目的。因此根据本发明，至少一个安全传感器组件具有至少两个功能性冗余子系统，且对控制单元的输入包括指示至少两个功能性冗余子系统的可用性的信息，其中控制逻辑配置成在输入指示所有功能性冗余子系统都可用的情况下激活以正常生产率为特征的正常运行模式，并且配置成在输入指示所有功能性冗余子系统都不可用的情况下激活以零生产率为特征的失效-停止运行模式，并配置成在输入指示功能性冗余子系统中的至少一个的至少临时不可用而其至少另一个可用的情况下激活失效-运行运行模式。

[0015] 针对这里在本申请中的安全传感器组件的功能性冗余子系统，另外还使用用语第一和第二安全装置。其可为两个或更多个安全传感器装置，例如观察是较危急安全区域的第一安全区域的接近传感器，和观察是不太危急安全区域的第二或第三或第N安全区域的摄像头，其中第一安全区域是第二或第三或第N安全区域的子集。其也可为具有两个或更多个不同观察区域的一个传感器单元，例如配置成以高分辨率观察靠近机器组件的第一安全区域并以较低分辨率观察进一步远离机器组件而向外延伸的第二或第三或第N安全区域的激光扫描仪或摄像头等。因此用语第一和第二安全装置用来描述传感器或传感器系统，或较复杂的传感器或传感器系统的功能子单元。用语“第二安全装置”旨在意味着功能种类，因此第二安全装置旨在意味着除第一传感器装置之外的一个或两个或三个或N个传感器或感测功能。

[0016] 针对本申请的上下文中的用语“第一或第二失效-运行模式”，此外还使用用语“第一或第二安全功能模式”。

[0017] 换句话说，本发明提供一种安全控制系统，其具有用于检测在第二安全区域中的第二危险情形的第二安全装置，或备选地，其能够实现某个的临时安全状态(例如具有安全受限速度)，通常在某个预定义时间之后必须离开该临时安全状态。在第二安全装置的情形下，控制逻辑与第一和第二安全装置相互作用以检测在一个安全装置中的失效情形并响应于在一个安全装置中的失效情形而切换到另一安全装置或应用失效功能模式中的一个。在第二种情况下，控制逻辑使系统处于某个临时安全状态，通常在某个预定义时间之后必须离开该临时安全状态。

[0018] 根据一个优选实施例，安全控制系统包括具有标称生产率的机器或机器组件，其

进一步包括第一安全区域和第二安全区域,其中第一安全区域为第二安全区域的子集,进一步包括第一功能性冗余子系统,其配置为用于检测在第一安全区域中的第一危险事件,进一步包括第二功能性冗余子系统,其配置为用于检测在第二安全区域中的第二危险事件,其中,第一失效-运行模式导致大于零但小于正常生产率的第一降低的机器生产率,且第二失效-运行模式导致大于零但小于标称生产率且高于第一降低的机器生产率的第二降低的机器生产率,其中控制逻辑在对控制逻辑的输入指示两个功能性冗余子系统都可用并指示在第二安全区域中有第二危险事件而在第一安全区域中没有危险事件的情况下激活第二失效-运行模式,且其中控制逻辑在对控制逻辑的输入指示第一功能性冗余子系统临时不可用而第二功能性冗余子系统可用并指示在第二安全区域中有第二危险事件的情况下激活第一失效-运行模式。

[0019] 根据另一优选实施例,控制逻辑在对控制逻辑的输入指示第一功能性冗余子系统可用和第二冗余子系统至少临时不可用并指示在第一安全区域中没有第一危险事件的情况下激活第二失效-运行模式。

[0020] 根据另一优选实施例,控制逻辑在对控制逻辑的输入指示第二冗余子系统至少临时不可用并指示在第一安全区域中有第一危险事件的情况下激活第一失效-运行模式。

[0021] 根据另一优选实施例,控制逻辑在对控制逻辑的输入指示第一和第二冗余子系统二者都可用并指示在第一和第二安全区域二者中有第一和第二危险事件的情况下激活第一失效-运行模式。

[0022] 根据另一优选实施例,控制逻辑在对控制逻辑的输入指示第二冗余子系统可用和第一冗余子系统临时不可用且在第二安全区域中没有危险事件的情况下激活正常运行模式。

[0023] 根据另一优选实施例,机器或机器组件为机器人或自主导引车(AGV)或离散制造系统或制造基元。

[0024] 根据另一优选实施例,机器或机器组件的生产率为机器或机器组件的活动部分的速度。

[0025] 根据另一优选实施例,第一或第二冗余子系统为接近传感器或挡光板或激光扫描仪或摄像头。

[0026] 根据另一优选实施例,由临时的通信错误如循环冗余错误 (CRC错误)或看门狗(watchdog)错误致使功能性冗余子系统的临时不可用。

[0027] 因此根据本发明,通过对安全控制引入失效切换(fail-over)的概念实现目的,失效切换在安全装置中存在失效情形的情况下避免不必要的机器停止。失效切换意味着当专门的装置或功能失效时,切换至冗余装置或功能。

[0028] 在根据本发明的分级安全控制系统中,按照第二或第三或(一般情况下)第N不太危急安全区域的顺序给出在危急性方面依次增加的层级,不太危急安全区域由第二安全装置监控,且检测在第二或第三或(一般情况下)第N安全区域中的第二或第三或(一般情况下)第N危险情形,触发不停止机器的第二或第三或(一般情况下)第N安全功能模式,且接着的第一危急安全区域由第一安全装置监控并检测第一危急安全区域中的第一危险情形,触发优选停止机器的第一安全功能模式。因此,根据本发明,分级布置的第一和第二安全装置如同它们是冗余装置一样被使用。

[0029] 当说到安全控制系统对在一个安全装置(即传感器或开关等)中的失效模式的反应时,根据本发明的安全控制系统的优势,控制逻辑在失效模式时不会触发紧急功能模式,而是切换到另一安全装置并应用失效功能模式(而不是严重的紧急功能模式),从两个失效功能模式中选择仍然符合安全要求的不太危急模式。从本发明可以看出,在第二安全装置处于失效情形的情况下,使用第一安全装置而不是第二安全装置,但应用不太危急的第二安全功能模式。这是令人惊讶的发现,因为正常的方式是将较危急的第一安全功能与第一安全装置一起应用。本发明的优势是,比较于应用危急的第一安全功能,通过使用不太危急的第二安全功能,机器的生产率降低地更少,但仍保持高度合理的安全水平。

[0030] 换句话说,典型的危险事件为人进入运行机器可能严重伤害人的限定的区域。传统上,如果检测到这种事件,则机器停止。

[0031] 分级安全控制的概念考虑到这种危险的严重性可不同,使得有时机器可以安全降低的速度运行而不是停止,使得可提高整个机器的生产率。

[0032] 例如,可在工业机器人周围限定“区域1”,其中该区域的违规导致立即停止机器人,但是如果人在该区域外附近,则机器人可以降低的速度运行,使得当人进入“区域1”时机器人能够停止。这是根据本发明的分级控制结构的示例。

[0033] 另一示例可为AGV,如果障碍物或工作人员处于一定的但较大范围内,其可以降低的速度运行,并且当距离变得危急,如在以上示例中的“区域1”时,其停止。

[0034] 以更一般的方式,安全反应还可取决于对人或障碍物的位置、大小和速率的更精确的感测。且安全反应还可停止生产线的某个部分、变速运行生产线的一部分等。

[0035] 第一或第二安全装置可具有第一或第二安全危险检测设备,其例如可以为传感器或开关,它们用来通知安全逻辑(也被称为安全控制装置)在特定区域中存在人或他们试图进入这种区域。例如,在机器(例如机器人或AGV)周围的附近范围的环境可被限定为第一危急安全区域,因为当人进入此第一区域时,存在其受到机器严重伤害的危急的危险。因此,在这种第一危急区域中存在人是根据本发明的危险事件的示例。

[0036] 在机器(例如机器人或AGV)周围的较宽范围的环境被限定为第二不太危急的安全区域。当人在此区域内,这里仍然存在人受到伤害的某种风险,但是其不太可能,且存在到机器的危险部分较大的安全距离和较多反应时间。因此,在这种第二安全区域中人的存在也被认为是根据本发明的危险事件,但是将具有不太严重的后果。

[0037] 第一安全区域通常是第二安全区域的子集。

[0038] 基于自动制造过程的实际状况,在检测到危险事件时,触发生产线或单独的装置,用于执行第一或第二安全功能。这意味着,例如,使它们处于将潜在危险降低至或限制在规定的可接受范围内的状态。很多时候,通过停止机器实现一点,但有时降低运动速度或限制特定机构(例如工业机器人或机器工具)的移动空间也足以实现这一点。

[0039] 第一安全功能意味着例如运动速度的相当急剧的降低或移动空间的限制,并且将在检测到人处于第一安全区域内的情况下被触发。

[0040] 第二安全功能意味着例如运动速度的不太急剧的降低或移动空间的限制,并且将在检测到人处于第二不太危急安全区域内的情况下被触发。

[0041] 根据本发明的另一优选实施例,安全控制逻辑与机器组件相互作用,以在第一安全装置出现失效且第二安全装置没有检测到危险情形的情况下将机器组件触发到正常功

能模式。

[0042] 根据本发明的另一优选实施例，安全控制逻辑与机器相互作用，以在第一安全装置出现失效情形且第二安全装置检测到有危险情形的情况下将机器触发到第一功能模式。

[0043] 根据本发明的另一优选实施例，控制逻辑与机器相互作用，以在第二安全装置出现失效情形且第一安全装置检测到有危险情形的情况下将机器触发到第一安全功能模式。

[0044] 根据本发明的另一优选实施例，控制逻辑与机器相互作用，以在第一和第二安全装置出现失效情形的情况下将机器触发到紧急安全功能模式。

[0045] 根据本发明的另一优选实施例，控制逻辑与第一和第二安全装置相互作用，以检测与第一和第二安全装置的通信错误，其中在一个安全装置中的失效情形是通信错误，例如CRC或循环冗余校验错误或看门狗错误。

[0046] 根据本发明，一种安全控制系统的运行方法，所述系统包括包括安全控制逻辑的控制单元，进一步包括至少一个安全传感器组件，进一步包括可在不同的运行模式下运行的至少一个机器组件，其中各运行模式以机器组件的不同生产率为特征，其中控制单元从至少一个安全传感器组件接收输入并评估输入，并且作为对评估的结果的反应，激活由安全控制逻辑确定的机器组件的运行模式，其中至少一个安全传感器组件具有至少两个功能性冗余子系统，其中对控制单元的输入包括指示至少两个功能性冗余子系统的可用性的信息，其特征在于以下步骤：在输入指示所有功能性冗余子系统都可用的情况下激活以正常生产率为特征的正常运行模式；和在输入指示所有功能性冗余子系统都不可用的情况下激活以零生产率为特征的失效-停止运行模式；以及在输入指示功能性冗余子系统中的至少一个至少临时不可用和其至少另一个可用的情况下激活以小于正常值但大于零的生产率为特征的失效-运行运行模式。

[0047] 因此，关于用于控制机器的安全控制系统的运行方法，所述系统具有：带有控制逻辑的分级安全控制结构；第一安全装置，其用于检测在第一安全区域中的第一危险情形，且响应于检测而触发第一安全功能模式；第二安全装置，其用于检测在第二安全区域中的第二危险情形，并响应于检测而触发第二安全功能模式，本发明教导方法包括以下步骤：

[0048] - 控制逻辑检测在一个安全装置中是否存在失效情形；

[0049] - 如果在一个安全装置中存在失效情形，则控制逻辑切换到另一安全装置或应用失效功能模式之一。

[0050] 根据本发明的另一优选实施例，机器至少可在正常功能模式和紧急功能模式下运行，安全控制系统具有：通信联接到机器的控制逻辑；通信联接到控制逻辑的第一安全装置，控制逻辑使用第一安全装置以检测在第一危急安全区域中的第一危险情形；通信联接到控制逻辑的第二安全装置，控制逻辑与机器相互作用以在没有危险情形时在正常功能模式下运行，具有进一步的步骤：

[0051] - 在第一安全装置被检测到有失效情形的情况下，控制逻辑使用第二安全装置代替第一安全装置，以及在第二安全装置被检测到有失效情形且第一安全装置没有检测到危险情形的情况下，控制逻辑触发第二安全功能模式。

[0052] 根据本发明的另一优选实施例，方法包括进一步的步骤：在第一安全装置被检测到有失效情形并且第二安全装置没有检测到危险情形的情况下，安全控制逻辑触发正常功能模式。

[0053] 根据本发明的另一优选实施例，方法还包括进一步的步骤：在第一安全装置被检测到有失效情形且第二安全装置检测到有危险情形的情况下，控制逻辑触发第一功能模式。

[0054] 根据本发明的另一优选实施例，方法包括进一步的步骤：在第二安全装置被检测到有失效情形且第一安全装置检测到有危险情形的情况下，控制逻辑触发第一安全功能模式。

[0055] 根据本发明的另一优选实施例，方法包括进一步的步骤：在第一和第二安全装置被检测到有失效情形的情况下，控制逻辑触发紧急安全功能模式。

附图说明

[0056] 将参照附图通过对三个实施例的描述来更详细地描述本发明，其中

[0057] 图1是根据本发明的安全控制系统的示范性和示意性图，

[0058] 图2是根据本发明的安全控制系统的另一实施例的示范性和示意性图，

[0059] 图3示出机器人基元的分层安全区域的示例，

[0060] 图4示出AGV的分级安全区域的示例，

[0061] 图5示意性地示出具有基础安全逻辑的安全控制系统的一般情况，

[0062] 图6示出CRC错误的失效切换和恢复方案，

[0063] 图7a-c示出了在不同失效情形下本发明的实施例的示意性图。

具体实施方式

[0064] 图1示出根据本发明的安全控制系统的示范性和示意性图。安全控制系统1包括包括安全控制逻辑的控制单元3。控制单元3经由过程传感器组件4接收来自过程的输入。过程可以是任何技术过程，例如制造基元、机器人或具有若干机器人的机器人系统、或自主导引车(AGV)、或化学处理工厂或化学处理工厂的子系统等。因而用语过程在本发明的背景下也用于描述机器。

[0065] 过程或机器具有由安全传感器组件4监视的某些安全危急区域。下面将在图2、3、4和7a-c的背景下更详细地解释这一点。

[0066] 控制单元3从安全传感器组件4接收包含信息的信号，并评估所接收的输入。为此，控制单元3包括至少一个输入/输出单元(I/O单元)。安全控制逻辑布置成用于评估在输入处接收到的信息并生成给过程或机器(这里在图1中示意性地表示为机器组件5)的包含相应输出信息的相应输出信号。机器装置5或机器或过程可在不同的运行模式下运行。例如，如果机器组件为AGV，则不同的运行模式可以是不同的速度，其范围为：零或停止、慢速、稍快的速度、正常速度。如果机器组件是具有至少一个机器人手臂的机器人，同样如此。在这里，不同的运行模式也可以是一个或多个机器人手臂的移动速度或甚至是一个或多个机器人手臂所覆盖的范围，其范围为从静止，仅经由一小节段、较大节段到完整的运行区域。各运行模式与机器或机器组件或过程的某个生产率相关联。因此，例如，如果机器人静止不动，则生产率为零。如果其只是缓慢移动，则生产率会很低。如果其以正常速度移动，则生产率正常。

[0067] 以上以机器人或AGV给出的示例仅用于示范性的示例。要理解，对于所有种类的过

程，包括但不限于用多种其他类型的机器或化学生产过程的制造过程，可以以相当的方式限定具有指定的不同生产率的不同运行模式。

[0068] 在图1中，上述解释的内容以概要的方式示出为机器组件5，运行模式示意性地指示为具有标号11的功能块或子系统F_0，具有标号12的功能块或子系统F_N，具有标号13的功能块或子系统F_1，具有标号14的功能块或子系统F_2。各功能块或子系统被指定规定的生产率。功能块或子系统F_0以生产率P_0为特征，功能块或子系统F_N以生产率P_N为特征，功能块或子系统F_1以生产率P_1为特征，功能块或子系统F_2以生产率P_2为特征。生产率P_N为正常的生产率。生产率P_0为零生产率，相当于系统停止。生产率P_1低于正常生产率P_N，但大于零。生产率P_2大于P_1，但小于正常生产率P_N。

[0069] 安全传感器组件4具有两个功能性冗余子系统6、7。其甚至可不止两个。安全传感器组件4的功能是监视在过程中或在机器或机器组件5附近的安全区域。监视意味着具有功能性冗余子系统6、7的安全传感器组件4检测在安全区域中的潜在危险的事件H_1、H_2。危险事件可以是例如在鞣革AGV的路径中的障碍物或人机器人或机器人系统的在一个或多个机器人手臂到达的范围内的运行区域内。功能冗余意味着两个子系统6、7可以冗余地用于这种危险事件的安全监视或检测。这可能例如意味着在机器5周围存在两个安全区域，一个危急安全区域和一个不太危急区域。危急安全区域例如特征在于，如果障碍物在该区域内，则对于机器存在高的潜在威胁，或者对于潜在地位于该区域内的人存在高的潜在安全风险。

[0070] 因此，功能性冗余子系统可例如是各自监视不同安全区域的两个子系统。这可以通过一个对于不同区域具有两个或更多个监视模式的传感器或通过两个不同的传感器(一个用于第一区域，一个用于另一区域)来实现。

[0071] 功能性冗余子系统6、7中的各个使用第一信号输入线路15、16将关于在其监视区域内存在或不存在危险事件的信息发送到控制单元3。并且另外，各功能性冗余子系统6、7使用可用性指示输入线路8、8'将关于其可用性的信息发送到控制单元3。传感器组件4的功能性冗余子系统的可用性可由于子系统6、7本身的故障或由于在子系统6、7和控制单元3之间的干扰通信而受到限制或缺乏。

[0072] 缺乏安全传感器子系统的可用性是潜在的安全风险。因此，在传统的安全控制系统中，一旦不再给出安全传感器组件或安全传感器子系统的可用性，在机器组件中相关的功能块或子系统将被设置为紧急停止(意味着零生产率)。在大量情况下，这不是必需的，因为相应的安全传感器或安全传感器子系统的可用性在短时间之后自动恢复。

[0073] 因此，在示于图1中的的根据本发明的安全控制系统1中，控制逻辑3配置成在输入指示所有功能性冗余子系统6、7都可用的情况下激活以正常生产率P_N为特征的正常运行模式F_N，并且配置成在输入8指示所有功能性冗余子系统6、7都不可用的情况下激活以零生产率P_0为特征的失效-停止运行模式F_0，并且进一步配置成在输入8指示功能性冗余子系统6、7中的至少一个临时不可用和其至少另一个可用的情况下激活以小于正常值但高于零的生产率为特征的失效-运行运行模式F_1、F_2。因此只有在所有子系统都不可用的情况下，才激活零生产率的停止模式。在一个子系统临时不可用的情况下，只要冗余子系统中的至少一个可用，则机器组件将设置成仅生产率降低而不为零的状态，这在很大程度上增加了安全受控制的机器组件5的整体可用性。

[0074] 现在观察图2，这示出根据本发明的安全控制系统1'的另一实施例的示范性和示

意性图。图2示意性地示出用于控制机器2的安全控制系统1'。机器2可以是机器人、AGV或在离散制造系统或制造基元中使用的任何其它机器。与机器2相关的是限定了第一危急安全区域Z_1和第二不太危急安全区域Z_2。第一安全区域Z_1比第二安全区域Z_2更靠近机器2。第一危急安全区域Z_1是第二不太危急安全区Z_2的子集。

[0075] 安全控制系统1进一步包括包括安全逻辑并通信链接到机器2的控制单元3。进一步存在第一安全装置D_1(参考标号6),其与安全逻辑3通信链接。其具有配置为用于检测在第一安全区域Z_1中的危险事件H_1的第一危险检测设备。进一步存在第二安全装置D_2 (参考标号7),其与安全逻辑3通信链接。其具有配置为用于检测在第二安全区域Z_2中的危险事件H_2的第二危险检测设备。具有危险检测设备的安全装置6、7可以是已知用于此目的的任何种类的传感器,例如接近传感器、挡光板、激光扫描仪等。安全装置6、7是更为一般和抽象的用语"安全传感器组件4的功能冗余传感器子系统6、7"所表示的示例,这里在图2中,第一和第二个危险检测设备6、7一起形成一种虚拟安全传感器组件4。

[0076] 机器2进一步包括具有第一安全功能设备的第一促动器系统,该第一安全功能设备配置成由安全逻辑3触发用于执行第一安全功能。

[0077] 机器2进一步包括具有第二安全功能设备的第二促动器系统,该第二安全功能设备配置成由安全逻辑3触发用于执行第二安全功能。

[0078] 第一和第二促动器系统可以是例如用于机器人轴的驱动器或用于驱动AGV的驱动器等。那么在该示例中的安全功能将是例如不同的驱动速度,紧急功能在该示例中将是驱动器的停止。

[0079] 控制单元3进一步具有输入评估设备10,其配置成确定第一和第二安全装置6、7的功能状况和/或可用性。控制单元3进一步具有激活设备9,其配置为用于在第一和第二安全装置6、7运行和可用的情况下,在检测到在第一安全区域Z_1中有危险事件时,触发或激活用于执行第一安全功能的第一促动器系统,在检测到在第二安全区域Z_2中有危险事件时,触发或激活用于执行第二安全功能的第二促动器系统。输入评估设备10和激活设备9可例如实施为I/O装置和作为在存储器中存储的控制运行程序的部分的相关联的程序例程,控制运行程序在作为控制单元3和其控制逻辑的一部分的微信计算机内并由微型计算机执行。

[0080] 激活设备9配置为用于在确定第一安全装置6出故障和/或不可用以及第二安全装置7运行和可用时并且在检测到在第二安全区域Z_2中有危险事件时,触发或激活用于执行第一安全功能F_1的第一促动器系统。

[0081] 激活设备9进一步配置为用于在输入评估设备10确定第二安全装置7出故障和/或不可用和确定第一安全装置6运行和可用的情况下,只要第一安全设备或危险检测设备6在第一安全区域Z_1中未检测到有危险,就触发或激活用于执行第二安全功能F_2的第二促动器系统。

[0082] 激活设备9进一步配置为用于在输入评估设备10确定第二安全装置7出故障和/或不可用和第一安全装置6运行和可用的情况下,如果第一危险检测设备或第一安全装置6在第一安全区域Z_1中未检测到有危险,就触发或激活用于执行第二安全功能F_2的第二促动系统。

[0083] 激活设备9进一步配置为用于在输入评估设备10确定第一和第二安全装置6、7出故障和/或不可用的情况下,对机器2进行逻辑触发,以用于过渡到安全状态(即,例如紧急

停止)。

[0084] 以下,将解释如在根据本发明的安全控制系统中应用的分层安全控制的概念。

[0085] 典型的危险事件是人进入其中运行机器可能严重伤害人的限定区域。传统上,如果检测到这种事件,机器停止。然而,这种危险的严重性可不同,使得有时候机器可以降低的速度运行而不是停止,使得显著提高机器的整体生产率。

[0086] 例如,参见图2或图3,可以在机器2或机器组件5(例如工业机器人)周围限定第一危急安全区域Z_1,其中该区域的违规导致机器人立即停止,但是如果人是在该区域Z_1外附近范围,机器人可以降低的速度运行,使得当人进入区域Z_1时机器人能够停止。

[0087] 另一个示例可以是AGV,参见图4,如果障碍物或工作人处于一定但较大的范围Z_2内,则其可以较低的速度运行,并且当距离变得危急(如在图4中示出的在上述示例中的区域Z_1)时,其停止。

[0088] 以更一般的方式,安全反应也可取决于对人或障碍物的位置、尺寸和速率的更精确的感测。且安全反应也可以是停止生产线的某个部分、变速运行生产线的部分等。

[0089] 所有这些都导致了分层安全控制方案,其在提高生产率同时确保相同的安全水平方面是有益的。

[0090] 以简化和一般的方式,我们假设以下情况:

[0091] D_1=安全装置1

[0092] H_1=要由D_1检测的局部化的危险事件,

[0093] F_1=(安全)功能1(例如安全停止)

[0094] P_1=以F_1运行时的生产率

[0095] D_2=安全装置2

[0096] H_2=要由D_2检测的不太局部化的危险事件,

[0097] F_2=(安全)功能2(例如降低的速度)

[0098] P_2=以F_2运行时的生产率

[0099] 以及

[0100] $100\% = P_N > P_2 > P_1 > P_0 = 0$

[0101] 且

[0102] H_1是H_2的子集

[0103] 这意味着H_1与H_2是同一种类,并且H_1被H_2覆盖,但是H_1更局部化或更详细。

[0104] 在机器人示例图3或图2中,D_1是保护机器人的工作空间的局部传感器,且D_2是观察附近范围的传感器。并且对于AGV示例,D_1可以是在感测前面的前方区域的局部传感器(例如,激光扫描仪),且D_2是观察工作基元的远程摄像头。

[0105] 安全控制逻辑将是:

[0106] If H_1 then

[0107] F_1 // 生产率 P_1

[0108] Else

[0109] If H_2 then F_2// 生产率 P_2

[0110] End If 。

[0111] 图5示出该具有对应的基础安全逻辑的一般情况,其中任何检测到或隐含的安全

装置故障导致紧急停止。对应的安全控制实施可遵循以下规则：

[0112]

状况 D_1	检测到 H_1	状况 D_2	检测到 H_2	F_X	P_X	注释
OK	假	OK	假	-	P_0	无安全反应
OK	假	OK	真	F_2	P_2	例如，降低速度
OK	真	OK	真	F_1	P_1	例如，减速或停止
OK	真	OK	假	F_E	P_0	紧急停止，与“H_1是H_2的子集”矛盾
NOK	任一	OK	任一	F_E	P_0	紧急停止
OK	任一	NOK	任一	F_E	P_0	紧急停止
OK	任一	NOK	任一	F_E	P_0	紧急停止

。

[0113] NOK意味着安全装置由于任何原因(包括临时通信错误)而导致的故障或不可用性。

[0114] 在下文中，将解释如在根据本发明的安全控制系统中应用的失效切换的概念。

[0115] 一般来说，失效切换意味着在专用装置或功能失效时切换到冗余设备或功能。

[0116] 如上所述，在由于D_1的故障或其它原因(例如，通讯错误)不能检测到H_1的情况下，其会致使紧急停止F_e的激活，以P_0运行机器。

[0117] 在F_e之后，系统必须进行错误诊断和恢复，并且必须重新启动。此过程的平均时间段为T_e。

[0118] 但在装置临时不可用的情况下，因而如果装置的功能在可接受的时间段之后恢复，而无需人工修复和重新启动系统，则可尝试通过使用冗余装置或功能来渡过该时间段。

[0119] 假设H_1间接地由H_2覆盖，因而H_1是H_2的子集。那么通过使用D_2作为D_1的失效切换装置而改变逻辑是可行的，如下所示：

[0120] If (D_1 is OK) then

[0121] If H_1 then

[0122] F_1 // 生产率 P_1

[0123] Else

[0124] If H_2then

[0125] F_2 // 生产率 P_2

[0126] End If

[0127] Else

[0128] If H_2 then

[0129] F_1 // 生产率 P_1

[0130] End IF。

[0131] 在这种情况下，如果没有检测到安全区域违规，机器将以100％运行。因此，如果D_1不工作，则通过(H_2隐含F_1)切换为(H_2隐含F_1)而使安全控制保持原样，如果没有安全区域违

规，则以100％运行，或在H_2时至少以P_1运行。生产率低于D_1工作时的生产率，如果D1不工作，则与经常停止机器时的生产率相比较高。

[0132] 在D_2至少临时不可用的情况下，则情形略有不同：H_2仅部分被H_1覆盖，并且D_1不能用作失效切换装置来检测H_2。然而，我们可结合H_1则F_1而使用F_2作为失效切换功能用于(D_2 is NOK)，从而一旦D_2为NOK，激活F_2，且在H_1被D_1检测到时激活F_1。由于H_1为H_2的子集，所以H_2被该失效切换策略充分地考虑。

[0133] 所产生的安全控制实施方式遵循以下规则：

[0134]

状况 D_1	检测到 H_1	状况 D_2	检测到 H_2	F_X	P_X	注释
OK	假	OK	假	-	P_N	无安全反应
OK	假	OK	真	F_2	P_2	例如，降低速度
OK	真	OK	真	F_1	P_1	例如，减速或停止
OK	真	OK	假	F_E	P_0	与 H_1 是 H_2 的子集矛盾
NOK	任一	OK	假	-	P_0	失效切换至 (D_2,H_2->F_1)
NOK	任一	OK	真	F_1	P_1	失效切换至 (D_2,H_2->F_1)
OK	假	NOK	任一	F_2	P_2	失效切换至 (D_2NOK)->F_1)
OK	真	NOK	任一	F_1	P_1	以 H_1 是 H_2 的子集考虑 H_2
NOK	任一	NOK	任一	F_E	P_0	紧急停止

。

[0135] 在下文中，描述了其中失效情形是CRC(循环冗余校验)错误的样本情况。

[0136] 在样本情况中，假设安全装置D_1经由PROFINET(使用PROFIsafe协议)远程连接，可能会出现临时通信错误如CRC或看门狗错误，这在当前的实践中导致系统的紧急停止。在下文中，描述了失效切换概念可如何应用于这种情况中。

[0137] 实际上，失效切换只是保持机器运行直到部分失效恢复的临时解决方案。通常，如果安全装置失效，则需要人工干预以恢复失效，例如，更换装置并重新启动安全控制。但在某些情况下，失效只是临时的。

[0138] 在该情况中，仔细观察CRC错误，CRC错误是至安全装置的通信的临时失效的典型示例。CRC错误可由安全控制器检测。根据本发明之前的现有技术的状态，如果在安全协议实施方案中没有实施另外的措施来覆盖该情形，偶尔出现的单次CRC错误将致使紧急停止。

[0139] 但在大多数情况下，CRC错误在短时间段后消失，并且再次建立与装置的稳定通信。在这种情形下，当应用上述的失效切换概念时，系统不必由于单个CRC错误而停止，因为存在冗余安全装置，并且当下一电报变为有效时可以通过切换回正常的安全功能而本身自动恢复(见图6)。

[0140] 在限定的时间间隔内的多个CRC错误被解释为严重失效，在这种情况下，机器必须停止(也参见图6)。检测CRC错误累积的常用时间间隔目前为100小时。

[0141] 可以通过检验校验和来检测CRC错误。因此，安全控制器记录通信失效，且如果CRC错误重复出现，则将其解释为对应的安全装置的故障。

[0142] 在安全装置本身失效的情况下，不幸无法自动恢复。安全控制必须被重新启动。

[0143] 在下文中，描述了其中失效为看门狗错误的样本情况。

[0144] 临时通信错误的另一典型示例是看门狗错误。这些错误每分钟都可能发生甚至更频繁，这取决于所使用的参数。看门狗时间限定在安全功能响应时间和可用性之间的折衷。看门狗时间设置的越小，越接近黑色通道(black channel)的性能，由于突然的黑色通道性能缺陷，人可能必须停止机器的概率越高。

[0145] 在进行本发明之前实践的现有技术的当前状态中，看门狗错误的出现频率没有限制。但是，与CRC故障相似，如果在应用程序级别上没有做任何事情以处理该错误的话，机器随时可能停止。

[0146] 根据本发明的看门狗错误的失效切换的概念对于在自动存储处理系统中的自主导引车(AGV)特别有利。这种AGV很多时候通过无线网络连接并从中央位置进行控制。

[0147] 在由于干扰或阻挡的墙壁削弱数据传递等导致无线连接突然太慢的情况下，则因为经由无线连接的通信太慢，AGV控制系统就会与中央站失去通信，并标记看门狗错误。在看门狗错误的情况下，可以启动计时器而不是停止AGV。如果在例如3秒钟内通信不恢复和运行，则停止AGV。否则，其使用局部安全传感器例如激光扫描仪作为失效切换装置。

[0148] 在这种情况中，局部传感器为D_1，相当于第一安全装置6，其检测车辆紧靠的前方中障碍物或人的存在，并且触发受控停止。此外，与第二安全装置7相当的D_2观察较大的区域并经由无线通信连接到局部AGV控制器。如果D_2临时不可用，局部AGV可以切换到降低的速度，并在可接受的时间段内依靠局部传感器。

[0149] 当然，以装置或功能的失效切换具体实施安全控制必须考虑会影响达到的安全等级的所有方面。

[0150] 图7a-c示出在不同失效情形中本发明的实施例的示意性图，作为根据本发明的控制系统的优选实施例的示例。

[0151] 类似于在图1中所示的安全控制系统，图7a以示意性和示范性的方式示出了安全控制系统1。图7a-c示出根据本发明的安全控制系统的运行方法。图7a示出其中两个安全传感器子系统6、7都可用并且运行的情形。

[0152] 在第一安全传感器子系统6，D_1检测到在区域Z_1(较危急的安全区域)中的危险情形H_1的情况下，则在控制单元3中的安全逻辑激活机器组件5(相应的促动器)进入具有大大降低的生产率P_1的第一运行模式F_1，F_1和P_1如上述所限定和解释。

[0153] 在第二安全传感器子系统7，D_2检测到在区域Z_2(区域Z_2包括Z1，因为Z1是Z_2的子单元，Z_2为不太危急的安全区域)中的危险情形H_2的情况下，则在控制单元中的安全逻辑3激活机器组件5(相应的促动器)进入具有降低不大的生产率P_2第二运行模式F_2，F_2和P_2如上述所限定和解释。

[0154] 图7b示出其中安全传感器子系统6不可用(以虚线表示)但是安全传感器子系统7可用的情形。在这种情况中，应用D_1到D_2的失效切换，以及从F_2到F_1的失效切换。这意味着，在第二安全传感器子系统7，D_2检测到危险事件的情况下，在控制单元3中的安全逻辑激活机器组件5(相应的促动器)进入具有大大降低的生产率P_1的第一运行模式F_1。这是一种为了

安全起见的切换切换，更为严格的安全功能F_1被应用于由子系统D_2检测到的危险情形，子系统D_2观察不太危急的安全区Z_2。但是由于Z_2包括Z_1，可能由D_2检测到的危险情形已发生在安全区域Z_1中，且因此在安全控制的意义上激活更为严格的安全功能F_1是有用的。因此作为失效切换，组合子系统1.2-2.3.1或7-F_1就位。

[0155] 图7c示出其中安全传感器子系统7，D_2不可用(以虚线表示)但安全传感器子系统6，D_1可用的情形。在D_2不可用的情况下，装置功能没有明确的失效切换。相反，对于H_2的安全功能被看作一般的失效切换功能，即，如果(D_2NOK)则触发F_2。换句话说，如果D_2为NOK，则触发F_2，即使D_1未检测到危险情形，出于安全和预防的原因，减低速度并使生产率从P_0降低到P_2。如果另外D_1检测到在Z_1区域中的危险情形，则触发F_1，进一步降低速度和进一步降低生产率至P_1。

[0156] 附图标记列表

[0157] 1安全控制系统

[0158] 1’安全控制系统

[0159] 3控制单元

[0160] 4安全传感器组件

[0161] 5机器组件

[0162] 6第一安全传感器子系统D_1

[0163] 7第二安全传感器子系统D_2

[0164] 8指示子系统可用性的信息

[0165] 8’指示子系统可用性的信息

[0166] 9激活设备

[0167] 10输入评估设备

[0168] 11功能块/功能子系统

[0169] 12功能块/功能子系统

[0170] 13功能块/功能子系统

[0171] 14功能块/功能子系统

[0172] 15第一信号输入线路

[0173] 16第二信号输入线路

[0174] Z_1第一危急安全区域

[0175] Z_2第二不太危急安全区域。

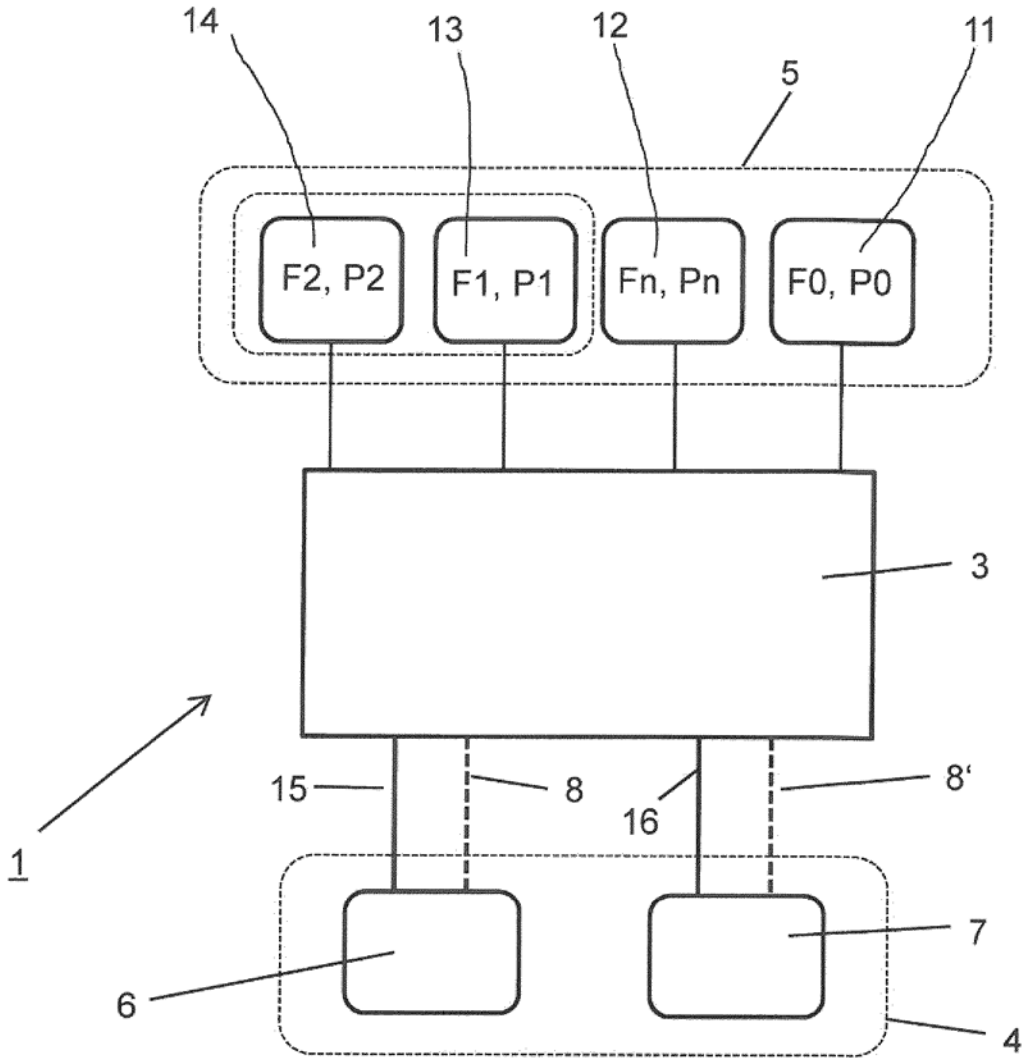


图 1

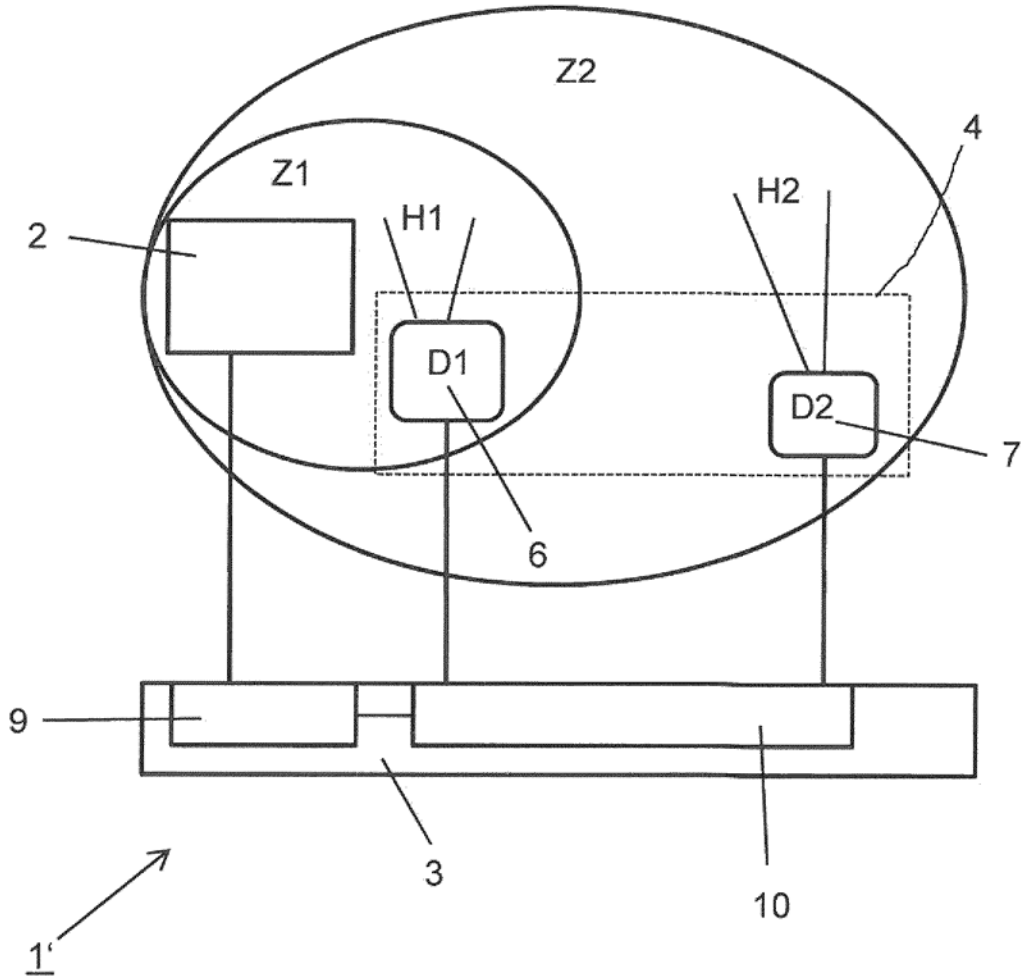
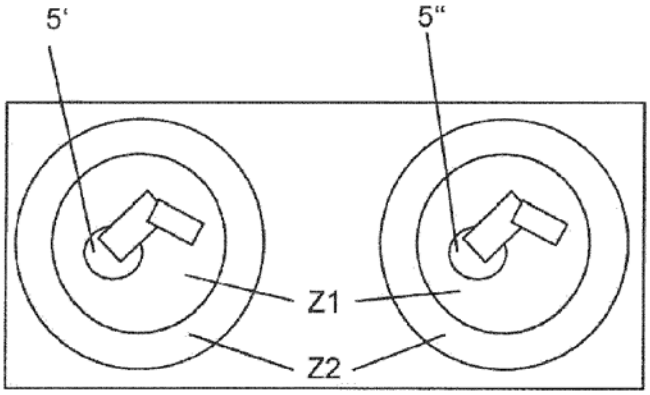

Z2
Z1
H1
H2
4
2
D1
D2
7
6
9
3
10
1‘

图 2


5‘
5“
Z1
Z2

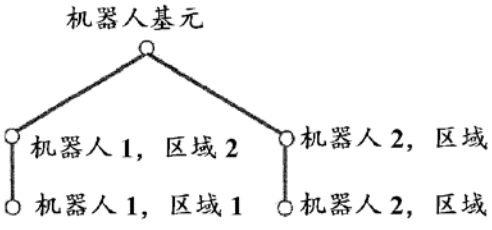

机器人基元
机器人 1，区域 2
机器人 2，区域
机器人 1，区域 1
机器人 2，区域

图 3

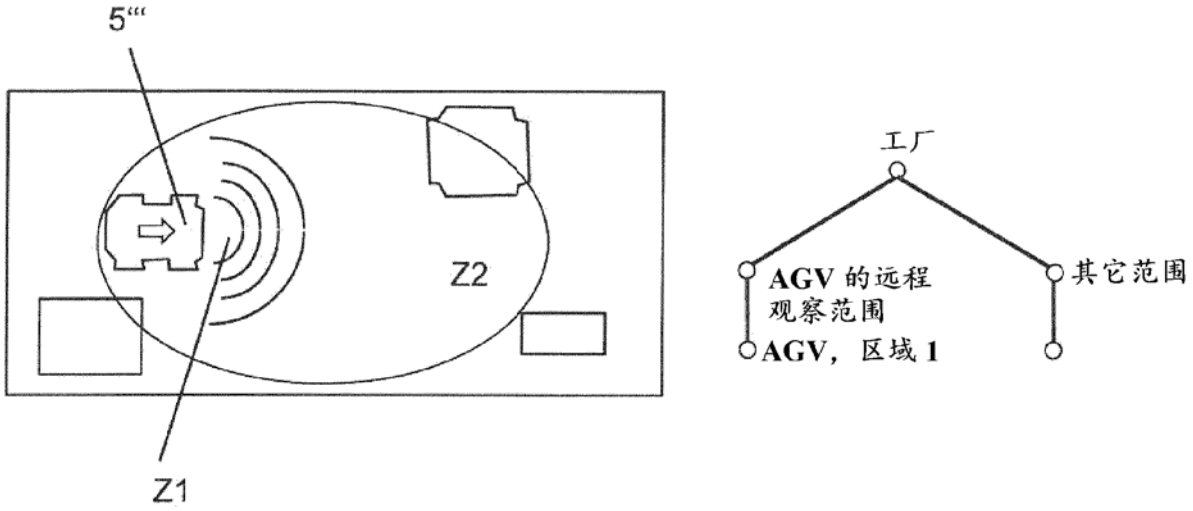

5‴
Z2
Z1
工厂
AGV 的远程
观察范围
AGV，区域 1
其它范围

图 4

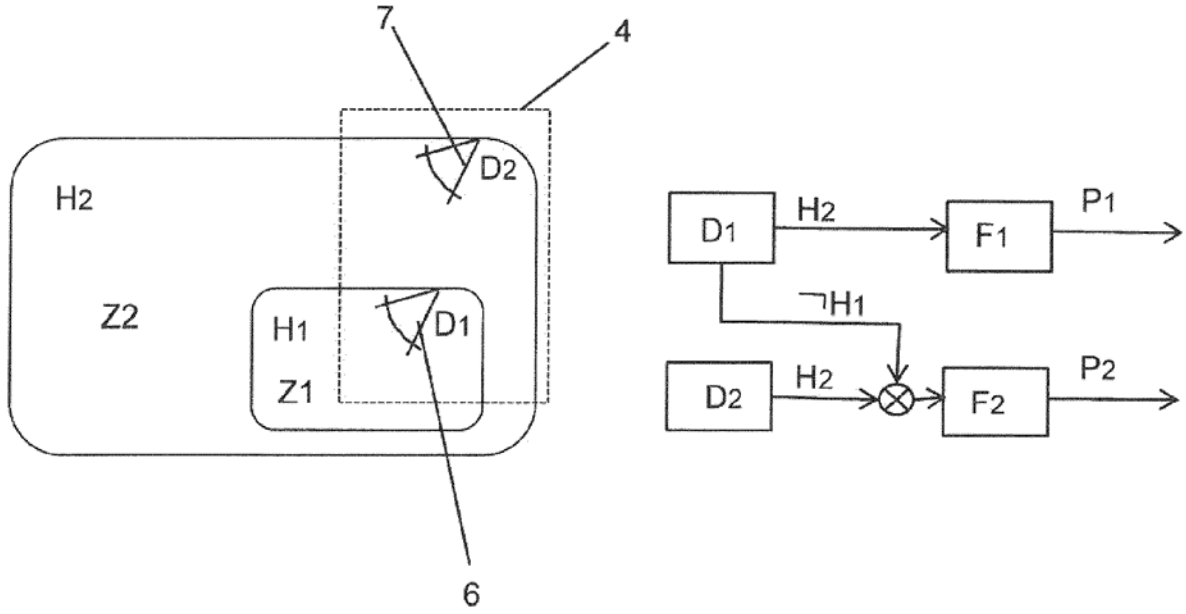

7
4
H2
D2
Z2
H1
D1
Z1
6
D1
H2
F1
P1
H1
D2
H2
F2
P2

图 5

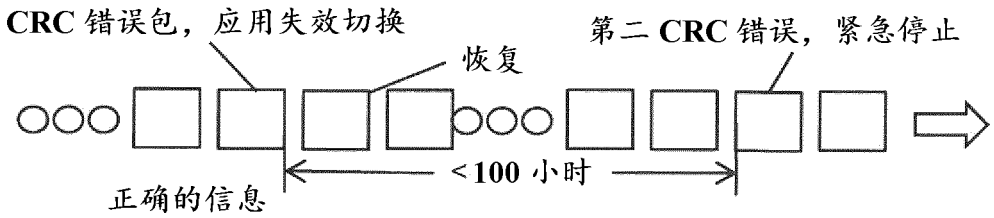

CRC 错误包，应用失效切换
恢复
第二 CRC 错误，紧急停止
<100 小时
正确的信息

图 6

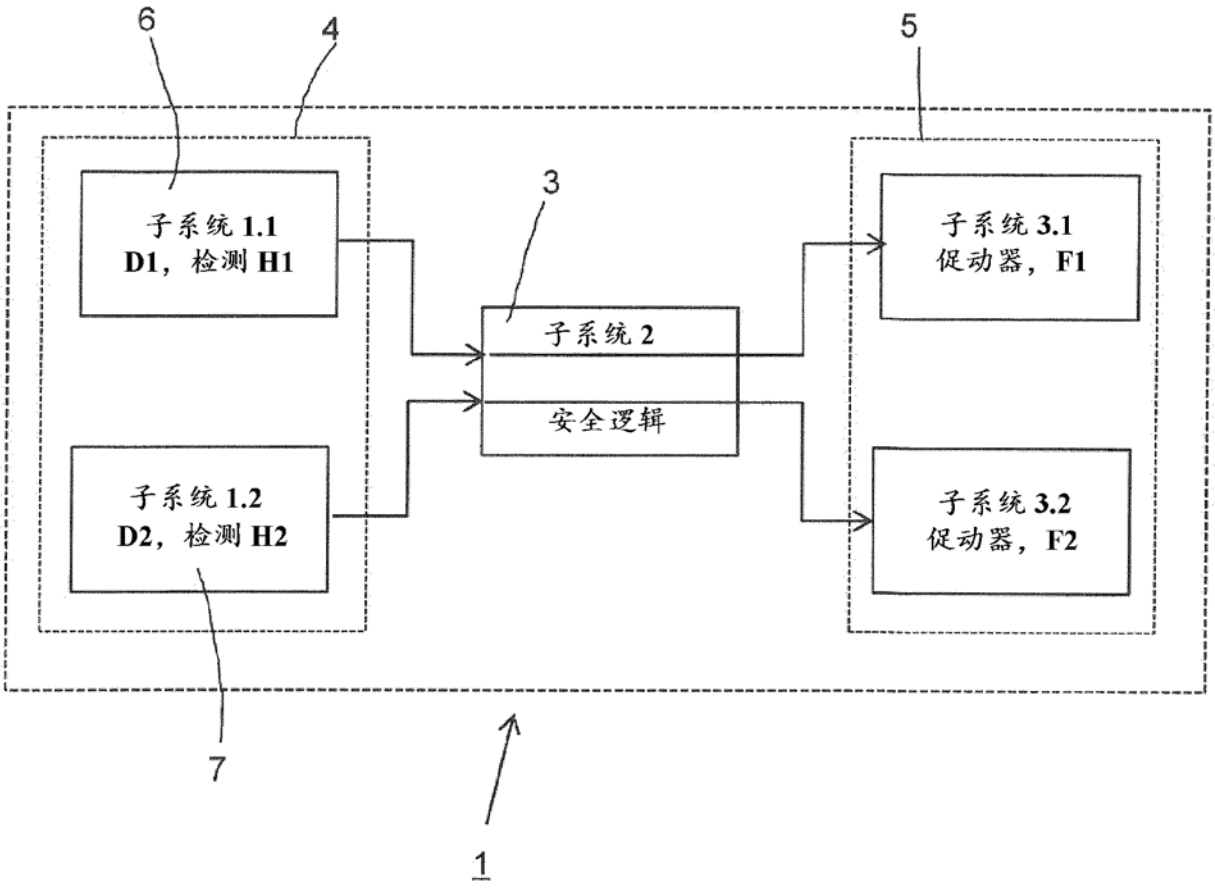

6
4
5
3
子系统 1.1
D1，检测 H1
子系统 2
安全逻辑
子系统 3.1
促动器，F1
子系统 1.2
D2，检测 H2
子系统 3.2
促动器，F2
7
1

图 7a

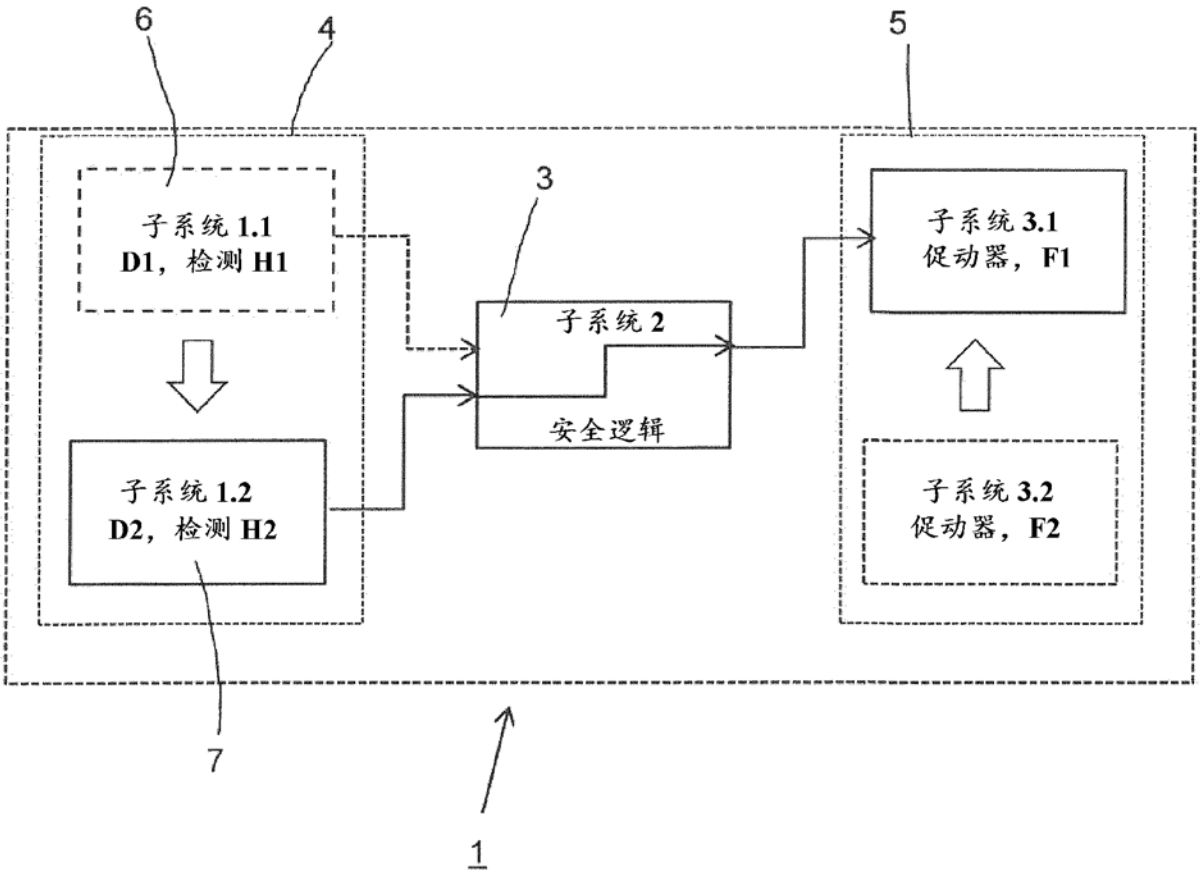

6
4
5
3
子系统 1.1
D1，检测 H1
子系统 2
子系统 3.1
促动器，F1
安全逻辑
子系统 1.2
D2，检测 H2
子系统 3.2
促动器，F2
7
1

图 7b

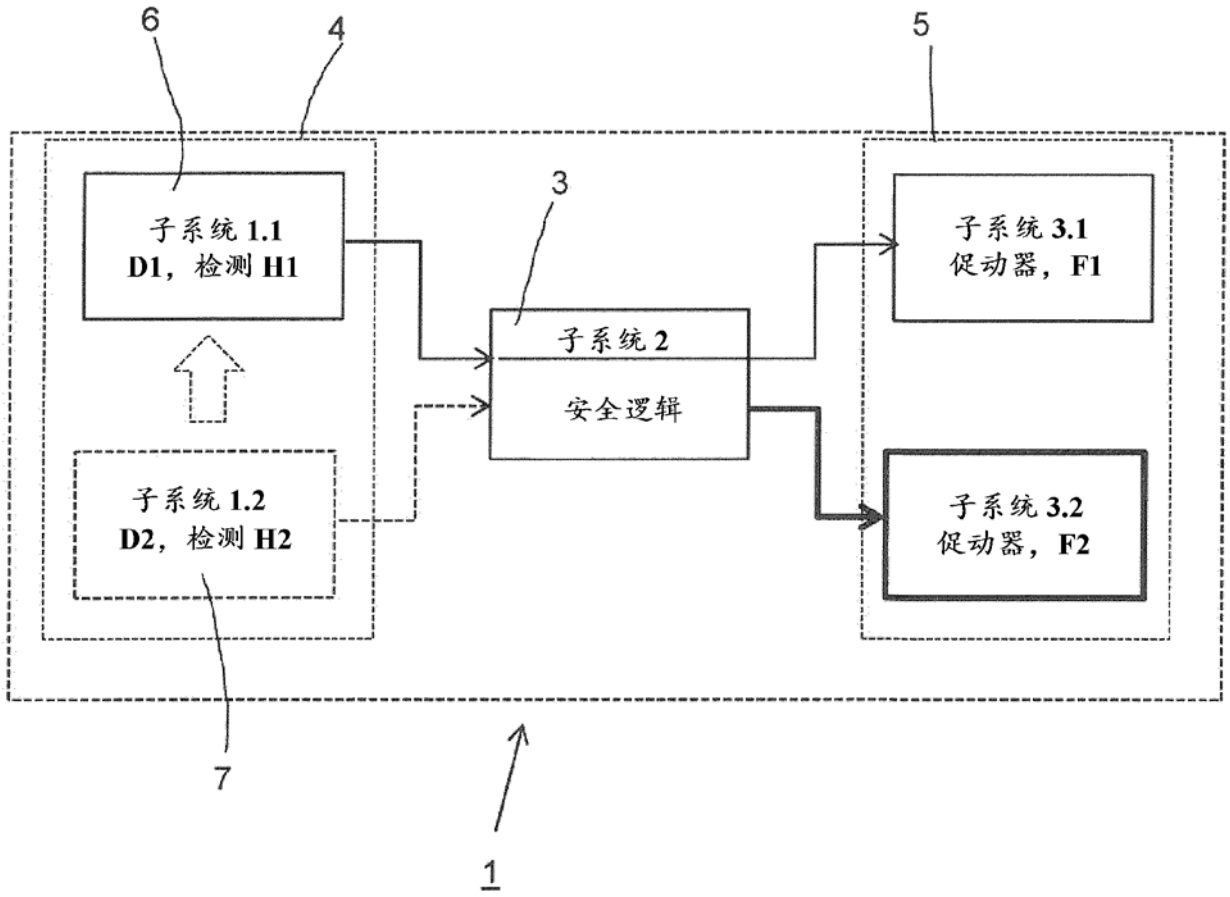

6
4
5
3
子系统 1.1
D1，检测 H1
子系统 2
安全逻辑
子系统 3.1
促动器，F1
子系统 1.2
D2，检测 H2
子系统 3.2
促动器，F2
7
1

图 7c