[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G05B 19/05 (2006.01)
G05B 15/02 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410032546.1

[45] 授权公告日 2008 年 12 月 24 日

[11] 授权公告号 CN 100445907C

[22] 申请日 2004.4.8

[21] 申请号 200410032546.1

[30] 优先权

[32] 2003. 4. 8 [33] US [31] 10/409，576

[73] 专利权人 费舍－柔斯芒特系统股份有限公司

地址 美国得克萨斯州

[72] 发明人 迈克尔·G·奥特 加里·劳
丹尼斯·史蒂文森
罗伯特·哈夫科斯特
戈弗雷·谢里夫

[56] 参考文献

US5970430A 1999.10.19
CN1098803A 1995.2.15
US6014612A 2000.1.11
US2002/0091451A1 2002.7.11
US2002/0055790A1 2002.5.9
US2002/0052673A1 2002.5.2
CN85109748A 1986.8.27

审查员 经志军

[74] 专利代理机构 北京市柳沈律师事务所

代理人 郭定辉 黄小临

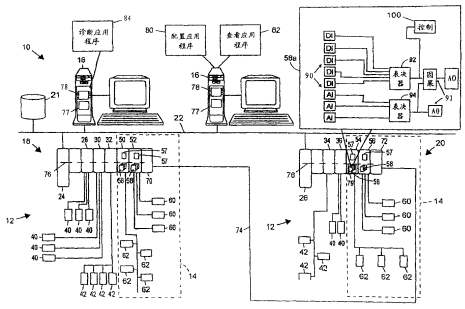
权利要求书 8 页 说明书 20 页 附图 4 页

[54] 发明名称

过程控制系统中包括运行与维护覆盖的表决逻辑块

[57] 摘要

可以被集成到在过程设备或者安全系统中的功能块图示编程环境中的表决功能块，实现表决逻辑并且提供运行与维护覆盖(override)，该运行与维护覆盖可以被设置为覆盖到该表决功能块的各个输入以及覆盖该表决功能块的输出。 该表决功能包括：一个或更多个输入限制单元，其检测特定的冗余输入是否达到了表示过程设备内条件的所指定的限制；覆盖单元，其可以由用户设置以覆盖对于该输入在表决功能中的考虑；表决逻辑实体，其根据有效的或者未禁止输入的值，确定解扣条件是否存在；以及禁止块，其可以用来覆盖该表决逻辑块的输出。 通过通信连接到在过程控制或者安全编程环境内的其他功能块，该表决功能块可以被集成到该过程控制或者安全系统之中。



1. 一种用于具有被通信耦合以控制一个或者更多个现场设备的处理器的过程设备的功能块实体，该功能块实体包括:

计算机可读介质；以及

功能块，存储在该计算机可读介质上，并且用来在该处理器上执行，所述功能块包括:

输入组，每个输入用来接收来自该过程设备内表示过程条件的输入信号;

限制检测单元，与该输入组的每一个相关联，其中每个限制检测单元都产生限制信号，表示相关输入上的输入信号是否满足解扣标准;

输出，用来提供解扣信号;

表决逻辑块，耦合在所述限制检测单元与所述输出之间，该表决逻辑块用来对所述限制信号施加表决逻辑，以当特定数目的所述输入信号满足所述解扣标准时，在所述输出上产生作为已解扣值的解扣信号，并且当特定数目的所述输入信号不满足所述解扣标准时，在所述输出上产生作为正常值的解扣信号；以及

覆盖块，用来防止所述表决逻辑块对于所述输入组中至少一个的使用，或者覆盖由所述表决逻辑块在所述输出上产生的所述解扣信号。

2. 如权利要求 1 所述的功能块实体，其中所述覆盖块为输入禁止块，该输入禁止块防止所述表决逻辑块对于所述输入组中一个的使用。

3. 如权利要求 2 所述的功能块实体，其中所述覆盖块包括覆盖时间参数，该覆盖时间参数指定第一时间量，在所述第一时间量期间将防止所述表决逻辑块对于所述输入组中一个的使用。

4. 如权利要求 3 所述的功能块实体，其中所述覆盖块包括提醒时间参数，该提醒时间参数指定在所述第一时间量到期之前的第二时间量，此时创建提醒信号，表示所述第一时间量的到期的所述提醒信号是即将来临的。

5. 如权利要求 1 所述的功能块实体，其中所述覆盖块包括对于所述输入组的每一个的输入禁止块，其中每一禁止块都可以分别设置，以防止所述表决逻辑块对于所述输入组中不同输入的使用。

6. 如权利要求 1 所述的功能块实体，其中所述覆盖块包含运行覆盖，所述运行覆盖可以被设置来防止所述解扣信号的已解扣值被发送给所述输出。

7. 如权利要求 6 所述的功能块实体，其中所述覆盖块包括定时器，所述定时器跟踪所述运行覆盖的时间，并且在预定时间段之后超时以允许所述解扣信号的已解扣值被发送给所述输出。

8. 如权利要求 6 所述的功能块实体，其中所述覆盖块用来检测何时所述表决逻辑块生成了对于预定的时间量稳定的所述解扣信号的值，并且在检测到所述解扣信号值已经稳定了所述预定时间量之后，允许所述解扣信号的值被发送给所述输出。

9. 如权利要求 6 所述的功能块实体，其中所述覆盖块包括事件检测参数并且使用该事件检测参数以当该事件检测参数指示一事件为存在或者不存在之一时，允许所述解扣信号的已解扣值被发送给所述输出。

10. 如权利要求 1 所述的功能块实体，其中所述覆盖块包括对于所述输入组的每一个的输入禁止块，其中每一输入禁止块都可以被分别设置以防止所述表决逻辑块对于所述输入组中一个输入的使用，所述覆盖块还包括运行禁止块，该运行禁止块可以被设置以通过将所述输出上的已解扣信号设置为正常状态来覆盖所述表决逻辑块。

11. 如权利要求 1 所述的功能块实体，其中所述表决逻辑块包括 N 选 M 表决逻辑方案，其中 N 为被考虑的输入的数目，M 为使所述表决逻辑块检测到存在解扣条件并且将所述解扣信号设置为已解扣值而指示满足所述解扣标准的限制信号的所需数目。

12. 如权利要求 11 所述的功能块实体，其中所述覆盖块为输入禁止块，该输入禁止块防止所述表决逻辑块对于所述输入组中一个输入的使用，并且其中当所述输入组中一个输入被覆盖时，所述表决逻辑方案减少该被考虑的输入的数目 N 但保持限制信号的数目 M 不变。

13. 如权利要求 11 所述的功能块实体，其中所述覆盖块为输入禁止块，该输入禁止块防止所述表决逻辑块对于所述输入组中一个输入的使用，并且其中当所述输入组中一个输入被覆盖时，所述表决逻辑方案减少在表决逻辑方案中该被考虑的输入的数目 N 以及限制信号的数目 M。

14. 如权利要求 11 所述的功能块实体，其中所述输入信号中一个输入信号包括状态参数与值参数，并且其中所述限制检测单元中的一个单元使用该状态参数以确定如何处理所述输入信号之一的所述值参数。

15. 如权利要求 14 所述的功能块实体，其中所述限制检测单元中的一个

单元自动处理具有不良状态参数的所述输入信号之一为满足所述解扣标准的输入信号。

16. 如权利要求 14 所述的功能块实体，其中所述限制检测单元中的一个单元自动处理具有不良状态参数的所述输入信号之一为被禁止的输入信号，以防止所述表决逻辑块对于所述输入信号之一的使用。

17. 如权利要求 1 所述的功能块实体，进一步包括：预限制检测单元，其与所述输入组的每一个相关联，其中每个预限制检测单元都产生预限制信号，表示相关输入上的输入信号是否满足不同于解扣标准的预解扣标准；预解扣输出，用来提供预解扣报警信号；以及预解扣表决逻辑块，在所述预限制检测单元与所述预解扣输出之间耦合，该预解扣表决逻辑块用来对所述预解扣限制信号进一步施加表决逻辑，以当特定数目的所述输入信号满足所述预解扣标准时，产生作为预解扣报警值的预解扣信号。

18. 如权利要求 1 所述的功能块实体，其中所述输入的每一个都用来接收模拟信号作为输入信号。

19. 如权利要求 1 所述的功能块实体，其中所述输入的每一个都用来接收数字信号作为输入信号。

20. 如权利要求 1 所述的功能块实体，其中所述覆盖块用来创建与一操作相关联的事件记录信号，所述操作为防止所述表决逻辑块对于所述输入组中至少一个的使用，或者为覆盖由所述表决逻辑块在所述输出上产生的解扣信号。

21. 如权利要求 1 所述的功能块实体，其中所述限制检测单元之一用来创建事件记录信号，该信号表示所述输入信号之一在满足所述解扣标准的状态与不满足所述解扣标准的状态之间改变，或在不满足所述解扣标准的状态与满足所述解扣标准的状态之间改变。

22.如权利要求 1 所述的功能块实体，其中该输入组为冗余输入。

23. 一种用于具有在过程内互连的多个现场设备的过程设备的控制系统，该控制系统包括：

通信耦合至所述多个现场设备的设备，该设备包括处理器与计算机可读介质；以及

表决块，存储在该计算机可读介质上，并且用来在该处理器上执行，所述表决块包括：

输入组，每个输入用来接收来自该过程设备内表示过程条件的输入信号；

限制检测单元，与该输入组的每一个相关联，其中每个限制检测单元都产生限制信号，表示相关输入上的输入信号是否满足解扣标准；

输出，用来提供解扣信号；

表决逻辑块，耦合在所述限制检测单元与所述输出之间，该表决逻辑块用来对所述限制信号施加表决逻辑，以当特定数目的所述输入信号满足所述解扣标准时，在所述输出上产生作为已解扣值的解扣信号，并且当特定数目的所述输入信号不满足所述解扣标准时，在所述输出上产生作为正常值的解扣信号；以及

覆盖块，用来防止所述表决逻辑块对于所述输入组中至少一个的使用，或者覆盖由所述表决逻辑块在所述输出上产生的所述解扣信号。

24. 如权利要求 23 所述的控制系统，其中所述表决块为功能块。

25. 如权利要求 23 所述的控制系统，其中所述覆盖块为输入禁止块，该输入禁止块防止所述表决逻辑块对于所述输入组中一个的使用。

26. 如权利要求 25 所述的控制系统，其中所述覆盖块包括覆盖时间参数，该覆盖时间参数指定第一时间量，在所述第一时间量期间将防止所述表决逻辑块对于所述输入组中一个的使用。

27. 如权利要求 26 所述的控制系统，其中所述覆盖块包括提醒时间参数，该提醒时间参数指定在所述第一时间量到期之前的第二时间量，此时创建提醒信号，表示所述第一时间量的到期的所述提醒信号是即将来临的。

28. 如权利要求 23 所述的控制系统，其中所述覆盖块包含运行覆盖，所述运行覆盖可以被设置来防止所述解扣信号的已解扣值被发送给所述输出。

29. 如权利要求 28 所述的控制系统，其中所述覆盖块包括定时器，所述定时器跟踪所述运行覆盖的时间，并且在预定时间段之后超时以允许所述解扣信号的已解扣值被发送给所述输出。

30. 如权利要求 28 所述的控制系统，其中所述覆盖块用来检测何时所述表决逻辑块生成了对于预定的时间量稳定的所述解扣信号的值，并且在检测到所述解扣信号值已经稳定了所述预定时间量之后，允许所述解扣信号的值被发送给所述输出。

31. 如权利要求 28 所述的控制系统，其中所述覆盖块包括事件检测参数并且使用该事件检测参数以当该事件检测参数指示一事件为存在或者不存在

之一时，允许所述解扣信号的已解扣值被发送给所述输出。

32. 如权利要求 23 所述的控制系统，其中所述覆盖块包括对于所述输入组的每一个的输入禁止块，其中每一输入禁止块都可以被分别设置以防止所述表决逻辑块对于所述输入组中一个输入的使用，所述覆盖块还包括运行禁止块，该运行禁止块可以被设置以通过将所述输出上的已解扣信号设置为正常状态来覆盖所述表决逻辑块。

33. 如权利要求 23 所述的控制系统，其中所述覆盖块包括对于所述输入组的每一个的输入禁止块，其中每一输入禁止块都可以被分别设置以防止所述表决逻辑块对于所述输入组中一个不同输入的使用，并且其中所述覆盖块还包括运行禁止块，该运行禁止块可以被设置以防止所述解扣信号的已解扣值被发送给所述输出。

34.如权利要求 33 所述的控制系统，其中所述表决逻辑块包括 N 选 M 表决逻辑方案，其中 N 为被考虑的输入的数目，M 为使所述表决逻辑块检测到存在解扣条件并且将所述解扣信号设置为已解扣值而必须指示满足所述解扣标准的限制信号的所需数目。

35. 如权利要求 34 所述的控制系统，其中当所述输入组中一个输入被所述输入禁止块之一覆盖时，所述表决逻辑方案减少被考虑的输入的数目 N 但保持限制信号的数目 M 不变。

36. 如权利要求 34 所述的控制系统，其中当所述输入组中一个输入被所述输入禁止块之一覆盖时，所述表决逻辑方案减少在表决逻辑方案中被考虑的输入的数目 N 以及限制信号的数目 M。

37. 如权利要求 34 所述的控制系统，其中所述输入信号中一个输入信号包括状态参数与值参数，并且其中所述限制检测单元中的一个单元使用该状态参数以确定如何处理所述输入信号之一的所述值参数。

38. 如权利要求 37 所述的控制系统，其中所述限制检测单元中的一个单元自动处理具有不良状态参数的所述输入信号之一为满足所述解扣标准的输入信号。

39. 如权利要求 37 所述的控制系统，其中所述限制检测单元中的一个单元自动处理具有不良状态参数的所述输入信号之一为被禁止的输入信号，以防止所述表决逻辑块对于所述输入信号之一的使用。

40. 如权利要求 34 所述的控制系统，进一步包括：预限制检测单元，其

与所述输入组的每一个相关联，其中每个预限制检测单元都产生预限制信号，表示相关输入上的输入信号是否满足不同于解扣标准的预解扣标准；预解扣输出，用来提供预解扣报警信号；以及预解扣表决逻辑块，在所述预限制检测单元与所述预解扣输出之间耦合，该预解扣表决逻辑块用来对所述预解扣限制信号进一步施加表决逻辑，以当特定数目的所述输入信号满足所述预解扣标准时，产生作为预解扣报警值的预解扣信号。

41. 如权利要求 23 所述的控制系统，其中所述输入的每一个都用来接收模拟信号作为输入信号。

42.如权利要求 23 所述的控制系统，其中该输入组为冗余输入。

43. 如权利要求 23 所述的控制系统，其中所述覆盖块用来创建与一操作相关联的事件记录信号，所述操作为防止所述表决逻辑块对于所述输入组中至少一个的使用，或者为覆盖由所述表决逻辑块在所述输出上产生的解扣信号。44. 如权利要求 43 所述的控制系统，其中所述限制检测单元之一用来创建事件记录信号，该信号表示所述输入信号之一在满足所述解扣标准的状态与不满足所述解扣标准的状态之间改变，或在不满足所述解扣标准的状态与满足所述解扣标准的状态之间改变。

45. 一种用来从过程变量的多个冗余测量来确定在过程中存在解扣条件方法，所述方法包括:

收集表示所述冗余测量的每一个的信号;

确定所收集信号的每一个是否满足解扣标准;

使用表决逻辑方案，以当特定数目的收集信号不满足所述解扣标准时产生作为正常值的解扣信号，以及当特定数目的收集信号满足所述解扣标准时产生作为已解扣值的解扣信号;

从该过程设备内的另一个实体接收禁止信号；以及

在接到所述禁止信号时，防止所述表决逻辑方案对于所收集信号中至少一个的使用，或者防止所述解扣信号被设置到已解扣值。

46. 如权利要求 45 所述的方法，其中接收禁止信号包括：接收与所收集信号之一相关联的输入禁止信号，并且其中防止使用所收集信号中至少一个包括对于预定的时间段防止在所述表决逻辑方案中使用所收集信号中至少一个。

47. 如权利要求 46 所述的方法，其中防止使用所收集信号中至少一个包

括：在所述预定时间段到期之前的预定的时间处生成提醒通知。

48. 如权利要求 45 所述的方法，其中在接到所述禁止信号时防止所述表决逻辑方案对于所收集信号中至少一个的使用或者防止所述解扣信号被设置到已解扣值包括：对于预定的时间段，防止所述解扣信号被设置到已解扣值。

49.如权利要求 45 所述的方法，其中在接到所述禁止信号时防止所述表决逻辑方案对于所收集信号中至少一个的使用或者防止所述解扣信号被设置到已解扣值包括：防止所述解扣信号被设置到已解扣值，直至对于所指定的时间量，所述表决逻辑方案确定所述特定数目的收集信号不满足所述解扣标准。

50.如权利要求 45 所述的方法，其中在接到所述禁止信号时防止所述表决逻辑方案对于所收集信号中至少一个的使用或者防止所述解扣信号被设置到已解扣值包括：防止所述表决逻辑方案对于所收集信号中至少一个的使用，直至检测到一事件为存在或者不存在之一。

51.如权利要求 45 所述的方法，其中在接到所述禁止信号时防止所述表决逻辑方案对于所收集信号中至少一个的使用或者防止所述解扣信号被设置到已解扣值包括：在接到第一禁止信号时，防止所述表决逻辑方案对于所收集信号中至少一个的使用，并且在接到第二禁止信号时，防止所述解扣信号被设置到已解扣值。

52. 如权利要求 45 所述的方法，其中使用表决逻辑方案以产生解扣信号包括：使用包含 N 选 M 表决逻辑的表决逻辑方案，其中 N 为被考虑的所收集信号的数目，M 为产生作为已解扣值的解扣信号而必须满足所述解扣标准的所收集信号的数目。

53. 如权利要求 52 所述的方法，进一步包括：当作为所述禁止信号的结果而使所收集信号之一被覆盖时，减少所述表决逻辑方案考虑的所收集信号的数目 N 但保持必须满足所述解扣标准的所收集信号的特定数目 M 不变。

54. 如权利要求 52 所述的方法，进一步包括：当作为所述禁止信号的结果而使所收集信号之一被覆盖时，减少所述表决逻辑方案考虑的所收集信号的数目 N 以及必须满足所述解扣标准的所收集信号的特定数目 M。

55. 如权利要求 45 所述的方法，其中确定所收集信号的每一个是否满足解扣标准包括：使用与所收集信号的每一个相关联的状态参数，以确定所收集信号是否满足所述解扣标准。

56. 如权利要求 55 所述的方法，其中使用所述状态参数包括：自动处理具有不良状态参数的所收集信号为满足所述解扣标准的所收集信号。

57. 如权利要求 55 所述的方法，其中使用所述状态参数包括：自动防止具有不良状态参数的所收集信号被所述表决逻辑方案使用以产生解扣信号。

58.如权利要求 45 所述的方法，进一步包括：确定所收集信号的每一个是否满足预限制解扣标准；使用另一表决逻辑方案，以当特定数目的收集信号不满足所述预限制解扣标准时产生作为正常值的预解扣报警信号，以及当特定数目的收集信号满足所述预限制解扣标准时产生作为报警值的预解扣报警信号。

59.如权利要求 45 所述的方法，其中收集表示所述冗余测量的每一个的信号包括：收集表示所述冗余测量的每一个的分离的数字信号。

60.如权利要求 45 所述的方法，其中在接到所述禁止信号时防止所述表决逻辑方案对于所收集信号中至少一个的使用或者防止所述解扣信号被设置到已解扣值包括：创建与事件记录信号，所述事件记录信号与使用防止所收集信号中至少一个或者防止所述解扣信号被设置到已解扣值相关联。

61.如权利要求 45 所述的方法，其中确定所收集信号的每一个是否满足解扣标准包括：当所收集信号之一在满足所述解扣标准的状态与不满足所述解扣标准的状态之间改变或在不满足所述解扣标准的状态与满足所述解扣标准的状态之间改变时，创建事件记录信号。

过程控制系统中包括运行与维护覆盖的表决逻辑块

技术领域

一般地，本发明涉及在过程设备（process plant）中所使用的过程控制与安全系统，更具体地说，涉及包含具有带运行与维护覆盖（override）功能的表决逻辑块的系统。

背景技术

像在化学、石油或其他过程中所使用的过程控制系统一样，一般包括一个或更多个过程控制器，该控制器通信耦合至至少一个主机或者管理员工作站，并且通过模拟、数字或者模拟/数字组合的总线或者线路通信耦合至一个或更多个现场设备。这些现场设备可以是（例如）阀门、阀门定位器、开关与发送器（例如，温度、压力与流速传感器），这些现场设备在过程设备内执行功能，诸如开或关阀门，以及测量过程变量。过程控制器接收由现场设备作出的表示过程量度和/或与现场设备有关的其他信息的信号，使用该信息以实现控制例程，然后生成控制信号，该控制信号通过总线或线路发送给现场设备以控制过程的运行。来自现场设备与控制器的信息一般对由管理员工作站运行的一个或更多个应用程序是可用的，以使管理员能够对该过程执行任意希望的功能，诸如配置该过程，查看该过程的当前状态，修改过程的运行等等。

另外，在许多过程中，提供了分离的安全系统以检测过程设备内有效的安全相关问题，并且在发生可能在工厂内产生或者导致严重危险的问题（诸如有毒化学物溢出、爆炸等等）时自动关闭阀门、切断设备电源、切换工厂内的流向等等。这些安全系统一般具有一个或更多个与标准过程控制控制器的分离的独立控制器，被称为逻辑解算器（solver），其通过安装在过程设备内的分离的总线或者通信线路连接到安全现场设备。逻辑解算器使用安全现场设备以检测与有效事件相关联的过程条件，诸如特定安全开关或者停机阀的位置，过程中的上溢或者下溢，重要的发电机或者控制设备的运行，故障检测设备的运行等等，由此来检测过程设备内的“事件”。当检测到事件时，

安全控制器采取某行动以限制该事件的破坏作用，诸如关闭阀门、关断设备、对工厂的某些部分断电等。一般地，这些行动包括切换安全设备到已解扣（tripped）的或者"安全"运行模式，该模式被设计来防止过程设备内发生严重的或者危险的情况。

在备有安全措施的系统中，一般都使用冗余的输入设备，诸如发送器与开关，以检测系统内的事件，从而提供更高的安全完整性或者过程变量可用性。在这样的系统中，有时需要在停机逻辑中提供表决逻辑功能，以根据冗余输入确定过程条件是可接收的还是危险的。虽然这样的表决逻辑十分简单，即其一般只需确定输入的多数表决以确定是否发生了事件条件，但是这些表决系统没有有效的覆盖。然后，在安全系统与某些过程控制系统中经常希望能够覆盖表决功能的输出，以（例如）防止在过程控制系统启动时停机系统的运行，使维护人员能够在一个或更多个输入设备上进行维护操作，允许所选择的过程条件被暂时旁路等。

虽然在过去，配置或者安全工程师有时使用不同的编程语言手工地将表决逻辑编程到安全系统控制器中，但是不幸的是，该编程步骤非常烦琐、耗时并且错误百出，这种错误可能很严重，因为安全系统不能正常运行可以导致对工厂人员的严重伤害甚或死亡，以及对于工厂内可能成千上万美元的装备与材料的破坏。一般地讲，不容易集成到已知表决逻辑功能中去的一些有用功能包括到表决逻辑系统的所选输入的维护旁路（bypass），启动旁路，启动和/或解扣延迟功能等等。

发明内容

在过程设备内的安全系统使用可以被容易地集成到功能块图示编程环境(function block diagram programming environment)中的一个或更多个表决功能块，以实现由用户指定的表决逻辑以及各种维护覆盖与旁路功能。这样的表决功能块易于创建、使用、测试、调试、编写文档，该表决功能包括：一个或更多个输入限制单元，其检测有关输入是否达到了表示过程设备内条件的所指定的限制；输入旁路单元，其可被用户设置以覆盖对于该输入在表决功能中的考虑；表决逻辑实体，其根据有效输入的值，确定解扣条件是否存在；以及禁止块，在（例如）启动或者其他运行状态的过程中，其可以用来覆盖该表决逻辑块的输出。该表决功能块可以被通信连接到其他功能块，诸如连

接到模拟或者数字输入功能块，模拟或者数字输出功能块，控制功能块，实现因果逻辑的因果功能块等等，以将该表决功能块实现为更大的过程控制或者安全系统的部分。在一种情况中，该表决功能块可以被用来根据由冗余测量或者传感器设备所做的过程变量的多个测量来检测在过程安全系统中事件的存在。

此处所述的表决功能块易于创建，这是因为就其基本形式而言，其只需要配置或者安全工程师提供对于以下指示：所要分析的输入的数目，所要使用的表决逻辑类型，以及所要使用的覆盖或者旁路功能，就可以定义该表决功能块所希望的操作。该表决功能块也易于集成到使用功能块逻辑的控制器或者逻辑解算器中，这是因为通过将该表决功能块的输入与输出互连到该控制策略内的其他功能块或者元件，该表决功能块可以与其他功能块相同的方式集成。结果，此表决功能块也易于编写文档、测试、与调试。另外，此表决功能块可以提供一般不在安全系统中提供的其他功能，诸如提供覆盖或者旁路功能，以在运行时以及维护与启动程序期间使用。

附图说明

图 1 为具有安全系统的示例过程设备的方框图，该安全系统与过程控制系统集成并且使用一个或者更多个可配置表决功能块来在该过程设备内控制系统停机与维护覆盖活动；

图 2 为图 1 的可配置表决功能块之一的方框图；

图 3 为可以由图 2 的表决功能块所使用的有关一个被旁路输入的几个示例表决方案的表；

图 4 为表示当表决功能块输入之一具有不良状态时表决方案退化方式的示例表；

图 5 为表示的可能与图 2 的表决功能块相关联的一组状态的状态图。

具体实施方式

现在参照图 1，过程设备 10 包括与安全系统 14（由虚线表示）集成的过程控制系统 12，其一般作为装备了安全措施的系统（SIS）运行，以监视并覆盖由过程控制系统 12 所提供的控制，以最大化过程设备 10 的可能的安全运行。过程设备 10 也包括一个或更多个主机工作站、计算机或者用户接口 16

（其可能是任意类型的个人计算机、工作站、PDA 等等），其可由工厂人员（诸如过程控制管理员、维护人员、安全工程师等等）访问。在图 1 所示的例子中，显示了两个用户接口 16，其连接到两个分离的过程控制/安全控制结点 18 与 20，并且通过公用通信线路或者总线 22 连接到配置数据库 21。通信网络 22 可以使用任何希望的基于总线的或者基于非总线的硬件，使用任何希望的硬件化的或者无线通信的结构，以及使用任何希望的或者适当的通信协议（诸如以太网协议）来实现。

一般而言，过程设备 10 的每一结点 18 与 20 都包括过程控制系统设备与安全系统设备，这些设备借助总线结构连接在一起，该总线结构可以配置在背板上，在该背板上可以附加不同的设备。在图 1 中，结点 18 显示为包括过程控制器 24（其可能是一对冗余控制器），还有一个或更多个过程控制系统输入/输出（I/O）设备 28、30 与 32，而结点 20 显示为包括过程控制器 26（其可能是一对冗余控制器），还有一个或更多个过程控制系统输入/输出（I/O）设备 34 与 36。过程控制系统 I/O 设备 28、30、32、34 与 36 的每一个都通信连接到一组与过程控制有关的现场设备，在图 1 中显示为现场设备 40 与 42。一般地，过程控制器 24 与 26，I/O 设备 28-36 以及控制器现场设备 40 与 42 就构成了图 1 中的过程控制系统 12。

类似地，结点 18 包括一个或更多个安全逻辑解算器 50、52，而结点 20 包括安全逻辑解算器 54 与 56。安全逻辑解算器 50-56 中的每一个都是具有处理器 57 的 I/O 设备，其执行存储在存储器 79 中的安全逻辑模块 58，并且这些安全逻辑解算器都通信地连接，以向安全系统现场设备 60 与 62 提供控制信号和/或从安全系统现场设备 60 与 62 接收信号。另外，结点 18 与 20 的每一个都包括至少一个消息传播设备（MPD）70 或者 72，其通过环形总线连接 74（图 1 中至显示了部分）相互通信耦合。一般地，安全系统逻辑解算器 50-56，安全系统现场设备 60-62，MPD 70 与 72 以及总线 74 就构成了图 1 中的安全系统 14。

过程控制器 24 与 26 可以是（只是例如）Fisher-Rosemount Systems 公司所销售的 DeltaV™ 控制器或者任何所希望类型的控制器，这些控制器被编程以使用 I/O 设备 28、30 与 32（对于控制器 24），I/O 设备 34 与 36（对于控制器 26）以及现场设备 40 与 42 提供过程控制功能（使用一般被称为控制模块的东西）。具体地说，控制器 34 与 36 的每一个都实现或者管理存储在其中或

者与其以其他方式相关联的一个或更多个过程控制例程，并且与网设备 40 与 42 以及工作站 14 进行通信，从而以希望的方式控制过程 10 或者过程 10 的部分。现场设备 40 与 42 可以是任何希望类型的现场设备，诸如传感器、阀门、发送器、定位器等等，并且可以符合任意希望的开放的、专有的或者其他通信或者编程协议，包括（例如）HART 或者 4-20 ma 协议（如对于现场设备 40 所示），任意的现场总线协议，诸如 FOUNDATION® 现场总线协议（如对于现场设备 42 所示），或者 CAN，Profibus，AS-Interface 协议等。类似地，I/O 设备 28-36 可以是使用任意适当（多个）通信协议的任意已知类型的过程控制 I/O 设备。

图 1 的安全逻辑解算器 50-56 可以是任意希望类型的安全系统控制设备，其包括处理器 57 与存储器，该存储器存储安全逻辑模块 58，该安全逻辑模块适合于在处理器 57 上运行以使用现场设备 60 与 62 提供与安全系统 14 相关联的控制功能。当然，安全现场设备 60 与 62 可以是符合或者使用任意已知或者希望的通信协议（诸如上述）的任意类型的现场设备。具体地说，现场设备 60 与 62 可以是以下类型的、与安全有关的现场设备，此类型可以方便地由分离的、专用的、与安全有关的控制系统来控制。在图 1 所示的过程设备 10 中，安全现场设备 60 被绘制为使用专用的或者点对点通信协议，诸如 HART 或者 4-20 ma 协议，而安全现场设备 62 被描绘为使用总线通信协议，诸如 Fieldbus 协议。安全现场设备 60 可以执行任意希望的功能，诸如停机、关闭开关等等功能。

公用背板 76（由贯穿控制器 24、26、I/O 设备 28-36、安全逻辑解算器 50-56 以及 MPD 70、72 的虚线表示）用于每一结点 18 与 20，以将控制器 24 与 26 连接到过程控制 I/O 卡 28、30 与 34，或者 34 与 36，以及连接到安全逻辑解算器 50、52、54，或者 56，以及连接到 MPD 70 或者 72。控制器 24 与 26 还通信耦合至总线 22，并且作为总线 22 的总线仲裁器，以使 I/O 设备 28-36，逻辑解算器 50-56，以及 MPD 70 与 72 的每一个都能通过总线 22 与任意工作站 16 通信。

以下将理解，每一工作站 16 包括处理器 77 与存储器 78，该存储器存储适合于在处理器 78 上运行的一个或更多个配置和/或查看应用程序。配置应用程序 80 与查看应用程序 82 在图 1 中都以放大图显示，其存储在工作站 16 中的一个内，而诊断应用程序 84 被显示为存储在工作站 16 的另一个中。然

而，如果需要，这些以及其他应用程序可以存储在并且执行于不同工作站16上，或者在其他与过程设备10相关联的计算机中。一般而言，配置应用程序80向安全工程师提供配置信息，并且使安全工程师能够配置过程设备10的一些或者所有元件，并且能够在配置数据库21中存储该配置。作为由配置应用程序80所执行的配置活动的部分，安全工程师可以为控制控制器24与26创建控制例程或者扩制模块，可以为任意一个或者所有安全逻辑解算器50-56创建安全逻辑模块58（包括创建并且编程表决功能块，以在安全逻辑解算器50-56甚或控制器24与26中使用），并且可以通过总线22与控制器24与26下载这些不同的控制与安全模块到适当的过程控制器24与26与安全逻辑解算器50-56。类似地，配置应用程序80可以被用来向I/Q设备和现场设备40、42、60和62中的任何一个以创建和下载其他程序和逻辑。相反，查看应用程序82可以向用户（诸如向过程控制管理员，安全管理员等等）提供一个或者更多个显示。如果需要的话，该显示或者在分离的视图中或者在同一视图中包含有关过程控制系统12与安全系统14的状态的信息。例如，查看应用程序82可以是报警显示应用程序，其接收并向管理员显示警报的表示。如果需要的话，此类报警查看应用程序可以采用的在名为“Process Control System Including Alarm Priority Adjustment”(包含警报优先级调整的过程控制系统)的美国专利5768119与名为“Integrated Alarm Display in a Process Control Network”(过程控制网络中集成警报显示)的美国专利09/707580中所公开的形式，这两个专利都转让给了本专利的受让人，此处融入这两个专利作为参考。然后将会理解，这些专利的警报显示或者报警标识可以接收并且在集成的警报显示中显示来自过程控制系统13与安全系统14两者的警报，这是因为来自系统12与14两者的警报都将被送往执行该警报显示应用程序的管理员工作站14，并且将可以被识别为来自不同设备的警报。类似地，管理员可以与过程控制警报同样的方式来处理显示在安全标识内的安全警报。例如，管理员或者用户使用警报显示可以确认安全警报，关闭安全警报等等，该警报显示将通过总线22与背板76使用通信来发送消息给在安全系统14内的适当的过程控制器24、26，以对于该安全警报采取相应的行动。以类似的方式，其他查看应用程序可以显示来自过程控制系统12与安全系统14两者的信息或者数据，这是因为这些系统可以使用同种类型与种类的参数、安全与引用，从而来自系统12与14之一的任何数据都可以被集成到传统上为过程控制系

统所配备的显示或者视图内。

诊断应用程序 84 可以被用来实现在工厂 10 的过程控制系统与安全系统内的诊断或者维护程序。这些诊断应用程序可以执行任意希望类型的诊断或者维护程序，诸如运行过程与阀门测试、启动程序等等，这些诊断应用程序可以提供对在过程设备 10 中所使用的一个或更多个表决功能块（以下描述）的覆盖，以防止安全系统根据来自一个或更多个由诊断程序所影响设备的输入的运行。

在任何情况下，应用程序 80、82 与 84，以及任意其他应用程序都可以发送分离的配置与其他信号给过程控制器 24 与 26 中每一个以及从安全系统逻辑解算器 50-56 中的每一个，并且可以从过程控制器 24 与 26 中每一个以及从安全系统逻辑解算器 50-56 中的每一个接收数据。这些信号可以包括与控制该过程现场设备 40 与 42 的运行参数有关的过程级的消息，并且可以包括与控制有关于安全的现场设备 60 与 62 运行参数有关的安全级消息。虽然安全逻辑解算器 50-56 可被编程来识别过程级消息与安全级消息两者，但是安全逻辑解算器 50-56 能够区别这两种消息类型，并且将不能由过程级配置信号来编程或者影响。在一个例子中，送往过程控制系统设备的编程消息可以包括特定的字段或者地址，这些字段或地址可以由安全系统设备来识别、并且防止这些信号被用来编程安全系统设备。

如果需要的话，安全逻辑解算器 50-56 可以使用与过程控制 I/O 卡 28-36 所使用的硬件与软件设计相比同样或不同的硬件或者软件来设计。对于在过程控制系统 12 中的设备与在安全系统 14 中的设备使用不同技术可以最小化甚至消除共同原因的硬件或者软件故障。另外，安全系统设备，包括逻辑解算器 50-56，可以采用任意希望的隔离与安全技术来降低甚至消除对由此实现的有关于安全的功能进行未授权改动的可能性。例如，安全逻辑解算器 50-56 与配置应用程序 80 可以要求具有特定授权级别的人或者位于特定工作站旁的人对安全逻辑解算器 50-56 内的安全模块进行改动，此时的授权级别或者位置不同于对由控制器 24 与 26 以及 I/O 设备 28-36 所执行的过程控制功能进行改动所需的授权或者访问级别或者位置。在这种情况下，只有那些被在安全软件内所指定的人或者位于被授权用来对安全系统 14 进行改动的工作站旁的人才有改动有关于安全的功能的资格，这就最小化了损害安全系统 14 的运行的可能性。将会理解，为了实现这样的安全，安全逻辑解算器 50-56

内的处理器评估到达的消息，以检查正确形式与安全，并且运行为对在安全逻辑解算器 50-56 内执行的安全级控制模块 58 所进行的改动的守护者。

将会理解，在每一个结点 18 与 20 中使用背板 76 使安全逻辑解算器 50 与 52 以及安全逻辑解算器 54 与 56 能够相互本地地通信，以协调这些设备的每一个所实现的安全功能，以相互通信数据或者进行其他集成功能。在另一方面，MPD 70 与 72 运行来使安全系统 14 的安置在工厂 10 的极不相同位置的部分仍然能够相互通信，以提供在工厂 10 的不同结点处的协调的安全操作。具体地说，MPD 70 与 72 联合总线 74 使与过程设备 10 的不同结点 18 和 20 相关联的安全逻辑解算器能够通信级联在一起，以允许根据所分配的优先级级联过程设备 10 内有关于安全的功能。可替换地，在工厂内不同地点的两个或者更多个有关于安全的功能可以被连锁或者互连，却不必运行到在工厂 10 分离区域或者结点内的单个安全现场设备的专用线路。换而言之，使用 MPD 70 与 72 以及总线 74 使安全工程师能够涉及并配置安全系统 14，该安全系统实质上分布在整个过程设备 10，但是其不同组件被通信互连以使分离的有关于安全的硬件能够如要求地相互通信。该特征还提供了安全系统 14 的可扩展性，即其使附加的安全逻辑计算器在需要其时或者当新的过程控制结点被添加到过程设备 10 时能够被添加到安全系统 14 中。

将会理解，可以使用功能块编程模式对安全逻辑解算器 50-56 进行编程，以对于安全设备 60 与 62 执行控制活动。具体地说，如在逻辑解算器 54 的一个安全控制模块 58a（存储在存储器 79 中）的放大图所示，安全控制模块可以包括一组通信互连的功能块，这些功能块可以被创建并下载到逻辑解算器 54，用来在过程 10 的运行过程中实现。如图 1 所示，控制模块 58a 包括两个输入被通信互连于其他功能块 90 的表决功能块 92 与 94，所述其他功能块 90 可能是（例如）模拟输入（AI）、数字输入（DI）功能块，或者其他被设计来向表决功能块 92 提供信号的功能块。表决功能块 92 与 94 使至少一个输出连接到一个或者更多个其他功能块 91，所述其他功能块 91 可能是（例如）模拟输出（AI）、数字输出（DI）功能块，实现因果逻辑的因果功能块，可以接收来自表决功能块 92 与 94 的、用来控制安全设备 60 与 62 等等运行的输出信号的控制与诊断功能块。当然，可以用任意希望的方式对安全控制模块 58a 进行编程，以包括任意类型的功能块以及一个或更多个以任意希望的或者有用的方式配置的表决功能块，以执行任意希望的功能。

虽然图 1 的安全控制模块 58a 的放大图包括了具有 5 个数字输入的数字表决功能块 92 以及具有 3 个模拟输入的模拟表决功能块 84，但将会理解，可以为不同逻辑解算器 50-56 的每一个创建并在其中使用任意数目的不同的安全逻辑模块 58，并且这些模块的每一个都可以包括具有以任意希望的方式通信互连到其他功能块的任意希望数目的输入的任意数目的表决功能块。类似地，如果用在（例如）Fieldbus 网络，则可以是任意现场总线类型功能块的表决功能块 92 与 94，或者任意连接于此的其他功能块都可以位于并实现在其他设备中，诸如在现场设备 62 中。如果用在安全系统之外，则表决功能块 92 与 94 可以实现在过程控制器 24、36，I/O 设备 28-36，现场设备 42 等等之中。将会理解，表决功能块 92 与 94 一般接收由在安全系统 14 内的冗余传感器或者发送器提供的冗余输入，并且对这些输入施加表决方案以确定根据所有这些输入，是否存在安全系统解扣条件。

图 2 为显示图 1 的示例表决功能块 94 的组件的方框图，该功能块为模拟表决功能块，这是因为其处理通过（例如）模拟输入（AI）功能块 90 传送的模拟输入信号。一般地，表决功能块 94 包括 3 个输入，标记为 IN1、IN2、IN3，其适用于接收来自（例如）过程设备 10 内冗余传感器或者其他冗余部件（例如来自图 1 的现场设备 60 与 62）的模拟输入信号。输入 N1、IN2、IN3 的每一个都被提供给解扣限制检查块 95a、95b 或者 95c 之一，并提供给预限制检查块 96a、96b、或 96c。解扣限制检查块 95 将传送到那里的输入与预定限制比较，以确定该输入信号是否已经到达与解扣条件相关联的值。类似地，预限制检查块 96 将传送到那里的输入与预定预限制比较，以确定该输入信号是否已经达到与指示解扣条件虽然还未存在但接近存在的警报或者警告相关联的值（可以是高值、低值或者在预定范围内的值）。实际上，预限制检查块 96 使得可以创建警报或者事件信号，表示危险或者由于其他原因而不希望的条件接近存在，即使还未存在。

解扣限制检查块 95 与预限制检查块 96 的输出（其可能是例如当达到了块 95 与 96 中的限制或者预限制时设置为高值的数字信号）的每一个都传送到一组输入旁路禁止块 98a、98b、98c 之一。这些输入旁路禁止块 98 在各个输入 IN1、IN2、IN3 上进行输入禁止，从而可以禁止这些输入的一个或者更多个，即不在表决功能块 94 中被用来决定解扣条件是否存在或者预解扣报警条件是否存在。每个输入旁路禁止块 98 都向解扣表决逻辑块 100a 提供相关

联的解扣限制条件的输出，并且向预解扣限制条件向解扣表决逻辑块 100b 提供相关联的解扣限制条件的输出。表决逻辑块 100a 与 100b 执行下面将详细描述的表决逻辑，以确定根据其输入是否存在解扣条件或者预解扣条件。

解扣表决逻辑块 100a 与预解扣表决逻辑块 100b 分别提供解扣信号与预解扣报警信号（当确定存在这些条件时）给启动禁止块 102，在希望禁止表决逻辑块 94 的操作的（例如）启动或者其他运行或者运行时程序的过程中，启动禁止块 102 可能禁止表决逻辑块 94 提供任何解扣信号或者预解扣报警信号输入。启动禁止块 102 生成作为解扣表决逻辑块 100a 与启动禁止块的运行的结果所确定的解扣输出信号（标记为 Out），并且还生成作为预解扣表决逻辑块 100b 与启动禁止块 102 的运行的结果所确定的 Pre_out 信号。Out 信号可以被用来驱动图 1 的安全系统 14 内停机程序的运行，而 Pre_out 信号可以被用来提供警报，以表示在过程设备 10 内解扣条件接近存在的现实情况。当然，如果需要，Out 与 Pre_out 信号可以用于其他目的。

表决功能块 94 可以包括一组参数，其中一些参数在图 2 中显示在使用它们的块的上面或者下面，这些参数是在（例如）配置表决功能块 94 时设置的，以影响或者指定表决功能块 94 的运行。具体地说，解扣限制（Trip_Lim）与预解扣限制(Pre_Trip_Lim)参数用来设置或者建立用于解扣限制块 95 的解扣限制以及设置用于预解扣限制块 96 的预解扣限制。解扣限制和/或预解扣限制参数可以对各个不同的块 95 与 96 相同，或者可以对块 95 与 96 的每一个分别设置。类似地，解扣滞后(Trip_Hys)与预解扣滞后(Pre_Trip_Hys)参数可以用来设置块 95 与 96 必须在连续解扣之间穿过的滞后。即一旦块 95 与 96 之一检测到输入信号之一高于（或者低于）限制，则（对于块 95）类型滞后的滞后值与（对于块 96）预解扣滞后的滞后值确定在关闭解扣信号（或者预解扣信号）之前或者在使第二解扣信号（或者预解扣信号）能够由该块设置之前，输入信号必须穿过低于（或者高于）该限制多少。

表决功能块 94 还具有名为 Trip_Type 的内部解扣类型配置参数，该参数限定与表决功能块 94 的输入和/或输出相关联的正常的与已解扣状态值。例如，当表决功能块 94 被配置为“断电解扣”（其可以是缺省值）时，输出的正常运行值为 1 而解扣状态值为 0。相反，当表决功能块 94 被配置为“通电解扣”时，正常运行值为 0 而解扣状态值为 1。此初始确定在解扣限制检查块 95a、95b、95c 上以及在预解扣限制检查块 96a、96b、96c 上作出，其分

别对应于输入 IN1、IN2、IN3。检测类型（Detec_Type）参数可以用来确定与解扣限制的比较是大于（高限制）比较或者是小于（低限制）比较。该比较发生在适当的解扣限制检查块 95 与预限制检查块 96 之上，以确定输入信号是否已经达到了预定的限制。

将会理解，解扣限制检查块 95 输入的每一个都将指示相应的输入 IN1、IN2 和/或 IN3 是否指示了解扣。如上所述，维护覆盖或者旁路可以由输入旁路禁止块 98 对于各自输入 IN1、IN2、IN3 的每一个施加，以防止这些输入被用于施加了表决逻辑块 100 的表决逻辑。当（例如）在发送器或者其他向表决功能块 94 提供输入信号的现场设备上进行维护时，希望有此旁路功能。当使用根据多个输入确定解扣输出的表决逻辑时，不总是需要维护旁路，这是因为对解扣的单一伪表决（其可能由于在提供该输入的传感器上的维护活动而产生）不一定会导致解扣。然而，此旁路功能是人们所希望的，以防止在维护活动过程中的伪解扣，并且在某些表决逻辑中可能需要该功能，诸如在两选一表决逻辑方案中，存在来自冗余传感器的即使单一的解扣信号也将导致解扣。

当输入旁路禁止块 98 的一个使输入被旁路时，表决逻辑块 100a 与 100b 将不会使用被旁路的输入来生成解扣信号或者预解扣报警信号，即使该输入值超过了由解扣限制或者预解扣限制参数所指定的限制。为了使能旁路，可以首先使能旁路允许（Bypass_Permit）参数，以首先控制是否允许对输入的旁路。一般而言，如果 Bypass_Permit 参数被设置或者被使能，则允许旁路输入，而如果 Bypass_Permit 参数未被设置或者未被使能，则不允许旁路输入。虽然单一的 Bypass_Permit 参数可以适用于所有旁路禁止块 98，但是可以为每个输入旁路禁止块 98a、98b、98c 设置分离的旁路允许。

如果 Bypass_Permit 参数被设置或者被使能，则可以使用 BYPASSx 参数来使旁路禁止块 98 的一个或更多个进行动作以禁止使用输入 IN1、IN2 或 IN3 中相关的一个。参数 BYPASSx 中的 x 表示输入 IN1、IN2 或 IN3 中的哪一个将被废止。如果需要，在任意特定时间都可以禁止多于一个的输入，或者可以配置表决功能块 94 以允许一次只能禁止一个输入。可以以任意希望的方式设置或者发出 Bypass_Permit 与 BYPASSx 参数，诸如通过在管理员或者维护画面上的管理员显示按钮，物理的按键开关，对安全模块的分立的输入，通过配置、控制、显示或者诊断应用程序，或者任意其他方式。当然，如果在

表决功能块 94 的任何特定实现中不需要使用旁路允许，则在配置表决功能块 94 时可以设置 Bypass_Permit 参数的缺省值为使能。

旁路超时（Bypass_Timeout）参数可以用来设置在对于块 98 中一个设置旁路之后，该旁路将自动截止的时间量。在这种情况下，输入旁路禁止块 98 的每一个都可包括作为一组定时器 110 之一的旁路定时器，该旁路定时器被设置为 Bypass_Timeout 参数值，并且在该旁路开始处倒计时。在这种情况下，输入旁路禁止块 98 可以禁止使用相关输入，直至关闭 BYPASSx，或者直至旁路定时器达到零。将会理解，旁路定时器被用来确保在预定的时间量滞后移除旁路。

如果需要，输入旁路禁止块 98 也可以被配置来提供提醒警报给用户，诸如管理员、安全工程师、技师等等，以提醒或者通知用户面临旁路超时。如果旁路被配置为消失或者在旁路超时时被废止，则通过设置提醒时间（REMINDER_TIME）参数为某非零值，可以向用户或者其他管理员预先发送超时通知。在这种情况下，如果旁路定时器非零但小于提醒时间参数并且任一被旁路的输入表决解扣，则可以启动提醒报警，以向用户发出警报，来指示在即将来临的旁路定时器截止时可能发生停机。如果没有被旁路的输入表决解扣，则不需要启动警报，但其仍然可以被启动。然而，将会理解，即使当旁路超时警报有效时，也不一定面临解扣，这是因为可能没有足够的其他输入表决解扣，从而不能使解扣表决逻辑块 100a 生成解扣信号。

在一个实施例中，只有当第一旁路超时时，才重新开始旁路定时器。然而，旁路定时器可以是可写参数，从而在将要发生超时的通知之后，可以使用管理员显示按钮增加该旁路定时器，以延长旁路时间，例如当仍然正在向表决功能块 94 提供被旁路的输入的现场设备上维护程序时。可替换地，旁路超时通知可以只为指示的目的，例如，在当旁路定时器超时时不废止旁路的情况下。在这种情况下，当旁路定时器超时时，即使提醒时间参数被设置为零，也可以将提醒警报设置为有效。然而，如果提醒时间参数非零，则在超时之前（如果输入表决解扣）仍然会发生提醒。提醒警报与旁路警报可以时确认或者非确认警报。

由表决逻辑块 100a 与 100b 进行的表决逻辑最后被配置为“N 选 M”逻辑功能。根据此功能，在总共 N 个输入中，必须有 M 个输入表决解扣。例如，表决功能块 94 可以被配置为 3 选 2（2oo3）表决器，这意味着在表决逻辑块

100a 输出被设置为解扣状态值之前，三个输入中必须有两个达到解扣限制，以及在预解扣表决逻辑块 100b 输出被设置为预解扣警报值之前，三个输入中必须有两个达到预解扣限制。“N 选 M”功能中的 N 值从未被禁止的输入数目确定，而 M 值根据被称为解扣数目（NUM_TO_TRIP）的该块内部参数确定，其缺省值在配置时可以设置为等于或者小于 N 的任意希望值。常见的表决方案包括（例如）3 选 2（2oo3），2 选 1（1oo2），2 选 2（2oo2）等等。然而，可以使用任意其他表决逻辑。由于块 94 的其他功能，表决功能块 94 也可以用于单一发送器应用，诸如在 1 选 1（1oo1）表决功能逻辑的情况中。

一般而言，1oo2 或者 1oo1 表决方案将需要维护旁路功能，这是因为废止即使一个发送器从而在维护活动过程中在表决功能块 94 对于该发送器的输入上引起检测到的解扣条件，也必将导致表决逻辑块 100a 设置解扣条件。然而，被配置需要多个解扣表决的表决功能块也可以得益于旁路功能，以求得在维护程序过程中更加可以预测的行为。

旁路输入 IN1、IN2 或者 IN3 之一可以以两种方式之一影响表决逻辑块 100a 与 100b。这可以使确定解扣条件（或者预解扣警报条件）所需的输入数目减 1，或者使该输入数目保持同样。例如，当表决逻辑块 100a 被配置为 2oo3 表决逻辑块并且输入 IN1、IN2 或者 IN3 之一被旁路时，表决方案变为 1oo2 表决方案，意味着表决解扣所需的输入数目（与可能输入的数目一道）减 1。可选地，当所选输入被旁路时，2oo3 表决方案可以变为 2oo2 表决方案，意味着表决解扣所需的输入数目（与可能输入的数目一道）保持不变（即使可能输入的数目减 1）。旁路选项参数可以用来指定当输入被旁路时解扣所需的实际数目是否减 1。图 3 显示此选项对几种不同表决方案的影响。图 3 的第一列表示没有禁止输入的所配置的表决逻辑方案，图 3 的第二列表示当单一输入被禁止时使用原来配置的解扣数目 M 的表决逻辑，图 3 的第三列表示当单一输入被禁止时解扣数目 M 减 1 的表决逻辑。当然，其他输入禁止可以造成从图 3 第二与第三列所指示的值类似的改变。不论何种情况，解扣表决逻辑块 100a（以及预解扣表决逻辑块 100b）一般不会将解扣所需的实际输入数目降到小于 1，并且当表决解扣的可能输入降低到零时将禁止解扣，诸如在 1oo1 表决方案中。

输入旁路禁止块 98 的缺省行为可以被设置为一次只允许旁路一个输入。该功能可以通过写检验来实现，其将防止第二输入被旁路。可选地，可以同

时旁路多个输入。如果需要，BYPASSx 参数可以具有附加的写检验，其需要在 BYPASSx 能够被设置之前旁路允许 BYPASS_PERMIT 参数为真或者被设置。

在解扣表决逻辑块 100a 上根据所选择的 N 选 M 表决方案进行表决之后，可以使用解扣延迟开时间（trip-delay-on time）参数 TRIP_DELAY_ON，从而在 OUT 信号变为解扣的状态值之前，所决出的解扣条件必须在一可配置的时间段上有效。类似地，可以使用解扣延迟关时间（trip-delay-off time）参数 TRIP_DELAY_OFF（其缺省值可以设置为零秒），以延迟当清除解扣表决条件（即当解扣表决逻辑块 100a 根据其输入确定解扣条件不存在时）时 OUT 信号返回正常状态值的时间。当然，解扣延迟开时间参数与解扣延迟关时间参数可以具有不同的以及任意希望的值，并且可以用于由解扣表决逻辑块 100a 生成的 Out 信号与由预解扣表决逻辑块 100b 生成的 Out 信号的一个或者两个。如果需要，可以独立的为解扣表决逻辑块 100a 与预解扣表决逻辑块 100b 配置解扣延迟开时间参数与解扣延迟关时间参数，并且这些参数可以由定时器 110 之一跟踪。

如上所述，启动禁止块 102 提供了启动或者其他运行覆盖功能。可能（例如）需要覆盖表决功能块 94 的输出，以迫使 Out 信号在启动或者其他暂时运行情况过程中的短暂时间段内处于正常状态。此启动禁止功能可以被用来（例如）失活由表决功能块 94 生成的常设（standing）解扣命令，这是因为该过程或者其有关部分处于停机状态，由此允许过程启动程序进行到被提供给表决功能块 94 输入的过程值不再处于指示应该开始解扣的值的点。

在一个实施例中，启动禁止块 102 可以包括缺省行为，从而在接到可能通过设置 Startup 参数来指示的启动指示时，在由启动延迟（STARTUP_DELAY）参数限定的可配置时间段内，启动禁止块 102 迫使 Out 信号以及（如果需要）Pre_out 信号在正常状态值。启动禁止块 102 可以包括启动倒计时定时器作为定时器 110 之一，该定时器被设置为由启动延迟参数指定的值，并且在通过启动参数接到启动指示时，该定时器开始倒计时。当该倒计时定时器超时时，解扣表决逻辑块 100a 与预解扣表决逻辑块 100b 恢复正常解扣检测。可以配置启动禁止块 102 使得当启动定时器倒计时时启动参数的随后设置将不影响启动时间。可选地，可能允许启动参数的每一新设置都重启启动定时器，从而可以避免等待超时的解扣。

与输入旁路禁止块98类似，启动禁止块102可以具有提醒功能，其可以通过（例如）设置旁路参数来启动。该提醒功能以与其运行输入旁路（维护旁路）基本相同的方式运行启动旁路。由此，当启动定时器大于零但小于可配置的提醒时间（REMINDER_TIME）参数（其可在配置时设置）并且有足够的解扣表决时，提醒警报条件变为有效，表示该旁路将到期，基于输入IN1、IN2与IN3的值，这可能导致停机。

如果需要，当输入稳定后，即当在一可配置的时间段内一直没有足够的解扣表决时，启动定时器可以另外或者可替换地自动到期。该稳定时间可以由稳定定时器跟踪，该定时器可以是定时器110之一，并且该定时器可以检测何时表决逻辑块100a对于所指定的时间段稳定在（例如）非解扣或者正常值。在这种情况下，当启动定时器倒计时时，只要当没有足够的解扣表决时稳定定时器就可以正计时，并且只要当解扣表决达到或者超过解扣所需的数目时就可以重置。如果稳定定时器达到所配置的稳定时间值，则启动定时器重置为零，并且恢复正常解扣检测功能。当然，在启动时间段结束时稳定定时器不重置，但在启动开始时以及在启动禁止期的任意时刻当具有足够的解扣表决时，该定时器被重置。

可替换地，启动旁路时间不一定基于固定时间段或者基于到表决功能块94的输入IN1、IN2与IN3，但可以基于事件的发生或者未发生。在这种情况下，当启动重置参数被设置或者变为被设置的或者真时，启动旁路结束，这可以在检测到事件时发生。以这种方式，可以将启动旁路与不定时长事件的存在或者不存在相联系。

如果需要，输入IN1、IN2和/或IN3的状态可以被用来影响表决功能块94的行为，并且可以使用状态选项参数来设置该状态行为。将会理解，在许多系统中，诸如在HART与Fieldbus系统中，发送器或者其他现场设备将与过程变量信号或者过程值一道发送状态信号，其中该状态信号指示发送器自身的状态。这些状态信号可以指示该发送器处于正常或者良好状态，或者处于非正常状态，诸如不良或者其他不受欢迎的状态，所述非正常状态可能使由该发送器所发送的过程变量值为可疑的。由此，提供给表决功能块94的IN1、IN2与IN3输入的输入信号的状态可以被确定并且被用来影响表决方案或者这些输入将在表决方案中的使用方式。

如果需要，可以设置块100所使用的表决方案使得当有其他发送器指示

正在测量的过程变量的有效值时，一个故障发送器（即具有不良状态的一个输入）将不会自动启动解扣。当考虑输入信号的状态时，一个选择是总是使用输入 IN1、IN2 或 IN3 的值，而不管输入的状态。以这种方式，硬件故障不一定引起停机，并且允许用于修理的时间。另一个选择是将输入上的不良状态作为该输入好像被旁路地处理，这就以与上述针对输入旁路禁止块 98 所述的同样方式防止了该输入表决解扣。第三个选择是如果该输入的状态为不良，则自动将该输入当作解扣表决。这可以被配置为缺省选项，其对于 1ooX 表决方案提供了最高级别的安全。图 4 显示对于上述的每个选择当单一输入具有不良状态时几个常见表决方案退化的方式。例如，如图 4 第一行第一列所示，当总是使用输入值时，2oo3 表决方案实际上退化为 2oo3（如果来自不良发送器的信号值为非解扣值）或者 1oo2（如果来自不良发送器的信号值为解扣值）。相反地，如图 4 第一行第二列所示，当根本不使用输入值时，2oo3 表决方案退化为 2oo2 表决方案(或者根据所选择的旁路功能可以退化为 1oo2 表决方案)。类似地，如图 4 第一行第三列所示，如果把不良发送器的信号值当作解扣表决而不管该信号实际值如何指示，则 2oo3 表决方案实际上退化为 1oo2 表决方案。

当然，对表决功能块 94 的输入的状态的使用可在解扣表决逻辑块 100a 与预解扣表决逻辑块 100b 的每一个中做同样或者不同处理。如果需要，除非所有未旁路输入都具有不良状态，Out 信号与 Pre_Out 信号的状态可以被设置为良好，在所有未旁路输入都具有不良状态的情况下，Out 信号与 Pre_Out 信号的状态可以被设置为不良。如果需要，当任一未旁路输入具有不良状态时，表决功能块 94 可以设置表示不良输入的报警条件参数。

图 5 绘出显示表决功能块 94 从已解扣状态(此时 Out 信号设置为已解扣状态）到未解扣或者正常状态（此时 Out 信号设置为正常状态）、或者相反的可能循环通过的不同状态的状态图 130。状态图 130 包括五个状态，定义为已解扣状态 132、已表决正常与延迟状态 134、已表决解扣与延迟状态 136、解扣禁止状态 138 以及正常状态 140。状态图 130 中状态之间的箭头或者线条表示状态 132-140 之间可能的状态转换。图 5 中的实线表示当所测量的过程值在解扣限制上下移动时所期望的常见状态转换。图 5 中的虚线表示不常见状态转换。

当无论何时启动旁路有效或者当因为或者由于一个或者更多个输入被旁

路或者一个或更多个输入具有不良状态并且处理不良状态使得该输入不被用于表决而没有足够的输入参加表决方案进而不可能解扣时，表决功能块 94 从任一其他状态进入解扣禁止状态 138。当禁止条件消失时，根据延迟参数（解扣延迟开时间参数与解扣延迟关时间参数）的设置以及到表决功能块 94 的输入，表决功能块 94 可以从解扣禁止状态 138 进入任意其他状态。

将会从状态图 130 理解，当到表决功能块 94 的输入所处的值使得用于图 2 解扣表决逻辑块 100a 中的表决方案指示不存在解扣条件时，表决功能块 94 一般将处于正常状态 140。当然，解扣表决逻辑块 100a 可以使用所有的输入，并且可以以上述的任意方式来使用被禁止的输入以决定解扣条件不存在。当解扣表决逻辑块 100a 检测到解扣条件时，如果没有设置解扣延迟开时间，表决功能块 94 可以直接进入已解扣状态 132， 或者如果解扣延迟开时间被设置为某非零值，表决功能块 94 可以进入已表决解扣与延迟状态 136。

表决功能块 94 将在已表决解扣与延迟状态 136 保持解扣延迟开时间参数所设置的延迟期，该参数可以由用户、配置工程师等等设置。当解扣延迟开时间段超时（并且没有被用户重置）并且仍然存在解扣条件时，表决功能块 94 将进入已解扣状态 132，并设置 Out 信号为已解扣值。然而，如果在已表决解扣与延迟状态 136 期间解扣条件消失，则表决功能块 94 将返回正常状态 140 而不影响 Out 信号。

当处于已解扣状态 132 时，表决功能块 94 设置 Out 信号为已解扣状态，并且将其保持在该状态，直至表决功能块 94 进入解扣禁止状态 138 或者正常状态 140。如果因为（例如）到表决功能块 94 的一个或更多个输入变化了，由此使解扣表决逻辑检测到表决不解扣条件，从而已解扣条件消失，则如果解扣延迟关时间段未设置，表决功能块 94 将直接进入正常状态 140，或者如果解扣延迟关时间段被设置为某非零值，表决功能块 94 将进入已表决正常与延迟状态 134。表决功能块 94 将保持在已表决正常与延迟状态 134，直至第一个解扣延迟关定时器超时（此时表决功能块 94 将进入正常状态 140），发生了解扣禁止条件（此时表决功能块 94 将进入解扣禁止状态 138），或者根据输入的变化重新出现已表决解扣条件（此时表决功能块 94 将重新进入已解扣状态 132）。

虽然图 5 的状态图 130 显示了一种表决功能块 94 可以在正常运行状态与已解扣状态之间以及相反地转换的运行方式，将会理解，如果需要，表决功

能块 94 可以被设计来使用比这些状态少或者多或者两者的某种组合的状态。另外，将会理解，虽然状态机 130 具体描述为被用来控制 Out 信号，即解扣信号的状态，但是类似的状态机可以被用来描述 Pre_Out 信号从正常状态到已报警或者已设置状态以及相反的运行。

另外，如果需要，表决功能块 94 可以提供指示表决功能块 94 所处于的解扣与预解扣状态的一个或更多个状态变量或者信号。对于这些信号，典型的状态值可以是“正常”以及不常见的“已解扣”。然而，如图 5 的状态图 130 中所示，当解扣延迟开或者解扣延迟关参数被设置为非零值并且发生正常与已解扣状态之间的转换时，解扣状态以及(如果需要)预解扣状态可以采用“延迟”值。类似地，当表决功能块 94 处于解扣禁止状态 138 时，解扣与预解扣信号（Out 与 Pre_Out）可以具有“已禁止”状态。

如果需要，可以配置过程控制系统 12 以根据与表决功能块 94 相关联的信号与参数在事件日志中捕获或者存储关于何时输入被旁路或者何时旁路被移除的信息。在许多情况下，因为旁路参数直接被写入表决功能块 94，所以这些事件可以被自行记录。在某些情况下，旁路与旁路允许是从物理按键开关布线的，并且可能需要特殊的写检验/事件日志。在实践中，旁路允许可以对一组表决功能块或者对逐个的表决功能块进行。当使用旁路超时时，可以使用特殊的事件日志以捕获该块已经移除了旁路的实际情况。当然，表决功能块 94 可以生成任何希望的事件记录（通过创建事件记录信号），以发送到并存储在（例如）图 1 的配置或者历史数据库 21。这些事件记录或者事件记录信号可以包括(例如)每个设置的记录或者旁路允许参数的变化、BYPASSx 参数、旁路超时（一般由限制检查块 95 创建）、覆盖与启动超时（一般由启动禁止块 102 创建），以及与可由（例如）表决逻辑块 100 或者解扣限制检查块 95 创建的表决解扣（或者表决预解扣）的特定输入相关联的状态变化的记录。在一般在安全系统发生停机之后发生的事件序列调查时，这些事件记录对于用户是有价值的。

可以看出，如此处所描述地使用表决功能块 94 使得易于创建具有已知形式的功能块，并且由此，一旦创建就只需以适当的配置参数设置编程以提供正确操作。在功能块编程环境内表决功能块的实现是容易的，这是因为可以创建表决功能块并且以任意已知或者希望的方式将其连接到其他功能块。类似地，表决功能块的调试也变得比以其他编程语言创建的表决逻辑容易，这

是因为表决功能块一般只需在其如何在编程环境下连接以及发送给它的配置参数的环境下调试。更进一步地，表决功能块的文档编写是容易的，这是因为其一般是典型功能块，其标准文档只需按提供给它的各个参数设置进行修改。

虽然此处详细描述了为模拟表决功能块的表决功能块94，但是应该理解数字数字表决功能块可以类似方式运行。然而，在数字表决功能块（其处理数字输入信号）中，限制检查块或者检测单元95将只运行来检测数字信号值为逻辑1或者逻辑0，其中这些状态中的一个被定义为达到解扣条件而另一个为未达到解扣条件。另外，在数字表决功能块中可能不需要或者不可能有预限制检查块或者检测单元96，这是因为数字输入信号一般只采用两种状态之一，并且不能与这两种状态之间的其他限制比较。然而，如果需要，解扣限制检查块95的输出可以提供给第二表决逻辑块（其使用比解扣表决逻辑块100a所使用的表决方案更宽松的表决方案），以确定预解扣警报。另外，虽然此处表决功能块92与94被描述为分别包括5个与3个输入，但是也可以使用任意其他数目的输出。

虽然图1显示表决功能块92与94接收来自AI、DI或者其他功能块的输入，但表决输入可以来自任意其他类型的功能块或者可以被生成为过程设备10内其他类型的信号。更进一步地，虽然表决功能块92与94的输出被显示为连接到诸如AO、DO、或其他如因果功能块或者控制例程的功能块的输出功能块，但是这些输出可以连接到任意其他希望类型的功能块，诸如定序（sequencer）功能块、准备（staging）功能块等等，甚或直接连接到过程设备10中其他应用程序或者编程环境。类似地，虽然此处描述的逻辑是使用功能块编程模式实现的，但是同样的逻辑也可以在其他类型的编程环境中提供，并且仍然可以被当作如此处所使用的功能块。更进一步地，虽然此处描述的表决功能块被描述为用于过程设备或者过程控制环境的安全系统，但是这些或者类似的功能块可以用于标准过程控制环境或者用于不同于安全系统用途的其他希望的用途。

虽然此处使用状态机图描述表决功能块，但是这些图只是用来描述表决逻辑与旁路功能的。将会理解不必使用状态机，并且如果使用了，也可以任意形式实现，诸如通过硬件或者以任意编程语言编写的软件。为了称为这样的状态机，诸如软件程序、例程、对象等等元件只需使功能块在此处解释或

者定义的或者如功能块的输出所表示的状态之间转换，由此使该输出从正常到已解扣状态或者相反地状态。

在实现时，此处所述的任意元件，包括禁止块、表决逻辑块、状态机、信号连接等等，都可以被实现于存储在诸如磁盘、激光或者光学盘或者其他存储介质的任何计算机可读存储器或者计算机或者处理器的RAM或者ROM等等中的软件。此处所述的信号与信号线可以采用任何形式，包括实际线路、数据寄存器、存储位置等等。该软件可以采用任何形式，包括在通用计算机或者处理器上执行的应用软件或者烧入（例如）特定用途专用集成电路（ASIC）、EPROM、EEPROM或者任意其他固件设备的硬编码的软件。类似地，可以使用任意已知或者希望的发送方法，包括（例如）在计算机可读盘或者其他可传送计算机存储机制或者通过诸如电话线、因特网、万维网、任意其他局域网或者广域网等等（其发送被看作与通过可传送存储介质提供这些软件相同或者可以互换）的通信信道，将该软件发送给用户、过程设备、管理员工作站、控制器、逻辑解算器或者任意其他计算设备。另外，可以不用调制或者加密来直接提供该软件，或者可以在通过通信信道发送此软件之前使用任意适当的调制载波和/或加密技术将该软件调制和/或加密。

当然，此处所述的表决功能块可以使用任意外部过程通知通信协议（除Fieldbus协议或者DeltaV协议之外）来实现，并且可以用来与任意类型的功能块通信，包括与由Fieldbus协议特别指定或者支持的任意不同功能块类似或者相同的任意功能块。另外，虽然此处一个实施例中表决功能块被描述为Fieldbus“功能块”，但是应该注意此处对“功能块”这个词的使用不局限于Fieldbus协议所指定的功能块，而是包括任意任意其他类型的块、程序、硬件、固件等等，即与任意类型的控制系统和/或通信协议相关联的实体，所述控制系统和/或通信协议可以用来实现某些过程控制例程功能或者具有预先定义的、用来的向其他这种功能块提供信息或者数据的设置或者协议。由此，虽然在面向对象编程环境中，功能块一般采用对象的形式，但也不一定如此，其可以是用来在过程设备或者控制环境中使用任意希望的编程结构或者模式来执行特定控制（包括输入与输出）功能的任意其他逻辑单元。

由此，虽然针对只是用于说明目的而不是用来限制本发明的特定例子描述了本发明，但是对于本领域技术人员来说，显然可以对所公开的实施例进行加减而不脱离本发明的原理与范围。

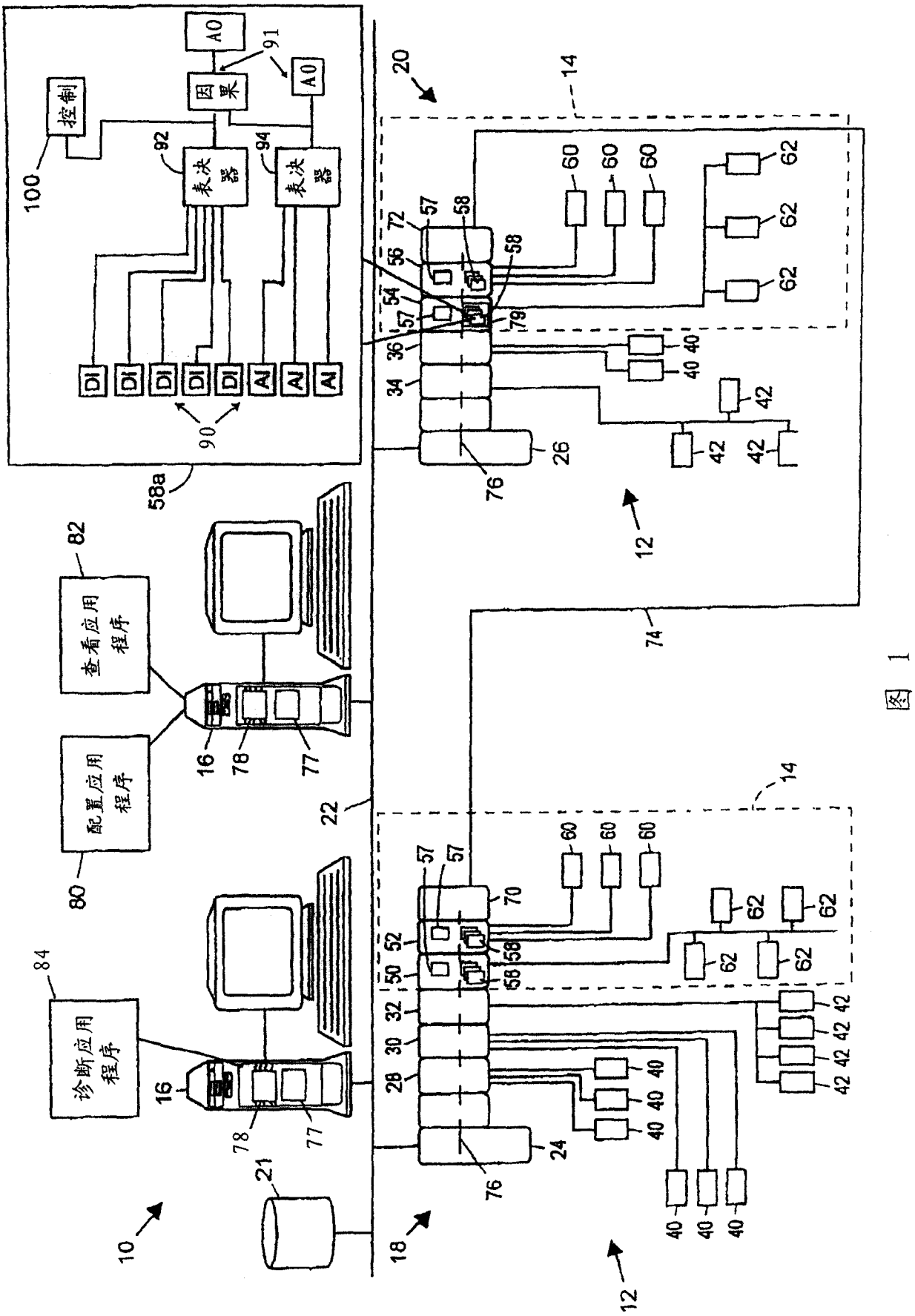

AO
因果
控制
表决器
DI
AI
查看应用程序
配置应用程序
诊断应用程序
10
12
14
16
18
20
21
22
24
26
28
30
32
34
36
40
42
50
52
54
56
57
58
60
62
70
72
74
76
77
78
79
80
82
84
90
91
92
94
100

图 1

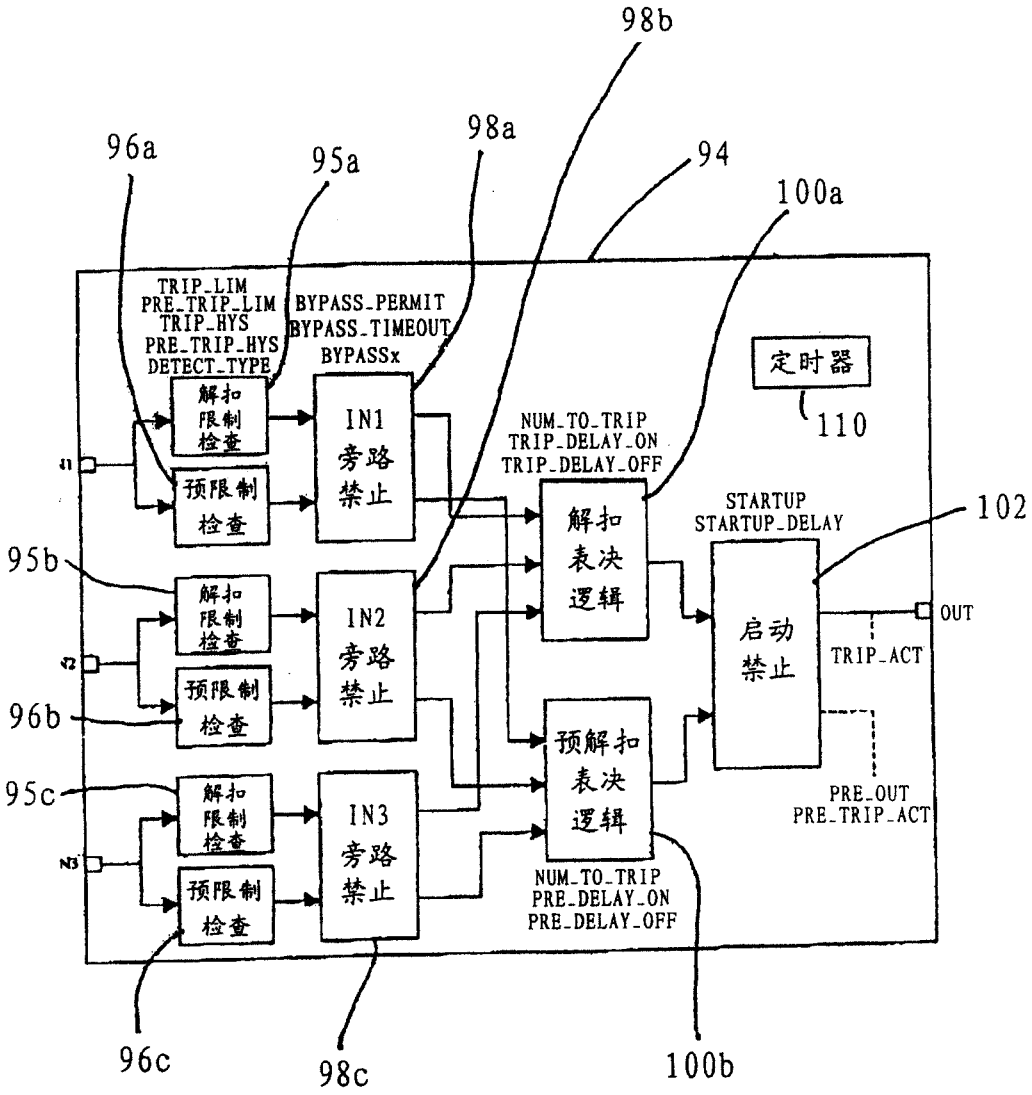

98b
96a
95a
98a
94
100a
TRIP_LIM
PRE_TRIP_LIM
TRIP_HYS
PRE_TRIP_HYS
DETECT_TYPE
BYPASS_PERMIT
BYPASS_TIMEOUT
BYPASSx
定时器
110
解扣限制检查
预限制检查
IN1旁路禁止
NUM_TO_TRIP
TRIP_DELAY_ON
TRIP_DELAY_OFF
解扣表决逻辑
STARTUP
STARTUP_DELAY
102
95b
IN2旁路禁止
启动禁止
OUT
TRIP_ACT
96b
95c
预解扣表决逻辑
PRE_OUT
PRE_TRIP_ACT
IN3旁路禁止
NUM_TO_TRIP
PRE_DELAY_ON
PRE_DELAY_OFF
96c
98c
100b

图 2

所配置的表决方案	一个输入被旁路 (使用所配置的NUM_TO_TRIP)	一个输入被旁路 (减少NUM_TO_TRIP)
2oo3	2oo2	1oo2
2oo2	解扣禁止	1oo1
1oo2	1oo1	1oo1
1oo1	解扣禁止	解扣禁止
2oo4	2oo3	1oo3
6oo8	6oo7	5oo7

图 3

所配置的 表决方案	总是使用值	如果不良则不表决	如果不良则表决解扣
2oo3	2oo3 or 1oo2	2oo2	1oo2
2oo2	2oo2 or 1oo1	解扣禁止	1oo1
1oo2	1oo2 或已解扣	1oo1	已解扣
1oo1	1oo1 或已解扣	解扣禁止	已解扣

图 4

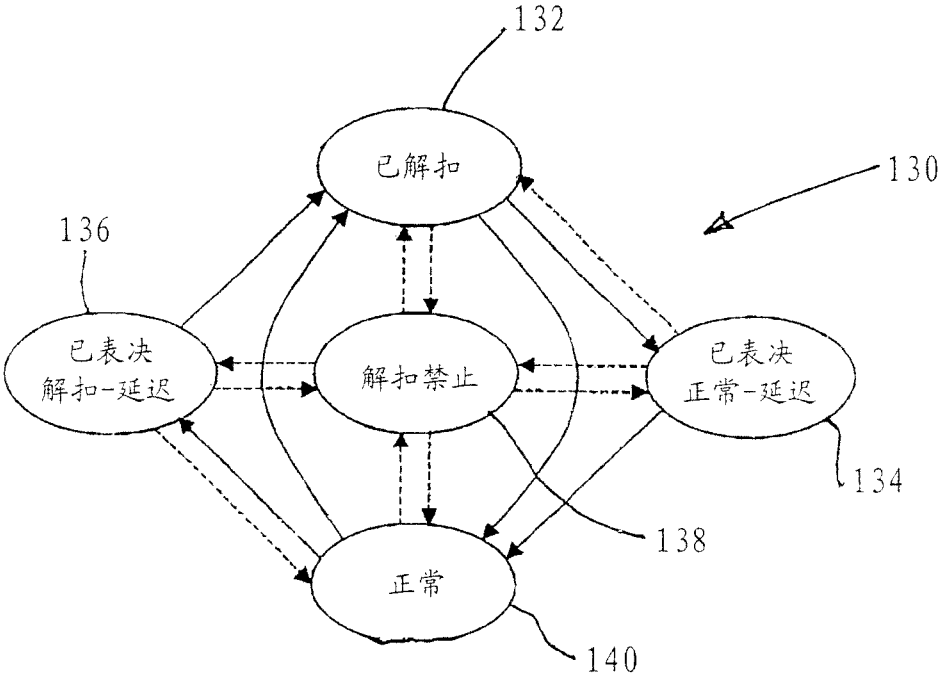


图 5