



(12) 发明专利

(10) 授权公告号 CN 107077103 B

(45) 授权公告日 2020.10.13

(21) 申请号 201580051534.X

(22) 申请日 2015.09.04

(65) 同一申请的已公布的文献号  
申请公布号 CN 107077103 A

(43) 申请公布日 2017.08.18

(30) 优先权数据  
1458354 2014.09.05 FR

(85) PCT国际申请进入国家阶段日  
2017.03.23

(86) PCT国际申请的申请数据  
PCT/FR2015/052344 2015.09.04

(87) PCT国际申请的公布数据  
W02016/034825 FR 2016.03.10

(73) 专利权人 赛峰电子与防务公司  
地址 法国布洛涅-比扬古  
专利权人 赛峰直升机发动机公司

(72) 发明人 席琳·刘 尼古拉斯·马蒂  
史蒂芬·兰福德

(74) 专利代理机构 北京派特恩知识产权代理有  
限公司 11270  
代理人 王琳 姚开丽

(51) Int.Cl.  
G05B 9/03 (2006.01)

(56) 对比文件  
EP 2595023 A2, 2013.05.22  
US 2008/0205416 A1, 2008.08.28  
JP 2006-229956 A, 2006.08.31  
CN 102421667 A, 2012.04.18  
CN 103930347 A, 2014.07.16  
CN 1203406 A, 1998.12.30  
FR 2986398 A1, 2013.08.02

审查员 艾春艳

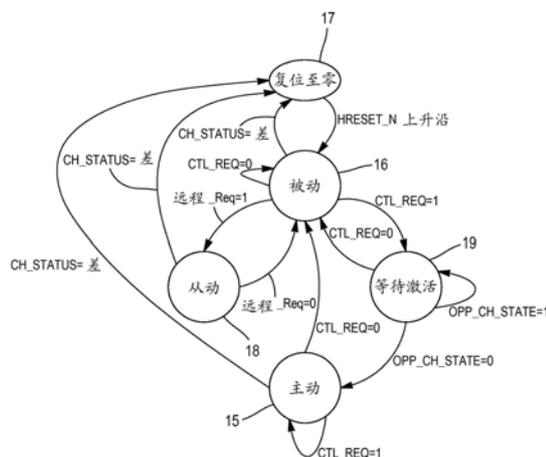
权利要求书3页 说明书10页 附图3页

(54) 发明名称  
双向架构

(57) 摘要

本发明涉及一种由航空器的飞行控制系统的本地处理单元(1,2)执行的切换方法,本地处理单元被配置为控制至少一个本地致动器,连接到至少一个本地传感器上以及通过至少一个链路(3,4)连接到相对处理单元(2,1);相对处理单元被配置为控制至少一个相对致动器,且连接到至少一个相对传感器上;本地处理单元(1,2)进一步被配置为连接到备份通信装置(13,14)上,以在所述本地处理单元(1,2)和相对处理单元(2,1)的链路(3,4)故障的情况下,实现两者之间数据的交换,备份通信装置包括:传感器或致动器阵列(13)和/或用于航空电子设备的安全机载网络(14);所述方法包括以下步骤:向相对处理单元(2,1)发送与至少一个本地传感器有关的采集数据以及与至少一个本地致动器有关的致动器数据,从相对处理单元(2,1)接收与至少一个相对传感器有关的采集数据以及与至少一个相

对致动器有关的致动器数据,接收相对健康数据项以及确定本地健康数据项,根据所接收到的相对健康数据和所确定的本地健康数据,将本地处理单元(1,2)从第一状态切换到选自主动状态(15)、被动状态(16)和从动状态(18)的第二状态。



CN 107077103 B

1. 一种切换方法,由包含至少一个引擎的航空器的飞行控制系统的第一处理单元实施,其中第一处理单元称为本地处理单元,

所述本地处理单元被配置为控制至少一个致动器以控制所述航空器的引擎,其中所述至少一个致动器称为本地致动器,所述本地处理单元能连接到至少一个本地传感器以及通过至少一个链路连接到第二处理单元,其中所述第二处理单元称为相对处理单元;所述相对处理单元被配置为控制至少一个相对致动器,且连接到至少一个相对传感器上;所述本地处理单元进一步被配置为连接到应急通信装置上;所述应急通信装置允许在连接所述本地处理单元和所述相对处理单元的至少一个链路出现故障的情况下,确保所述本地处理单元和所述相对处理单元之间的数据交换,

所述应急通信装置包括:

传感器或致动器的网络;和/或

用于航空电子设备的机载安全网络,

所述方法包括以下步骤:

向所述相对处理单元发送与所述至少一个本地传感器有关的采集数据以及与所述至少一个本地致动器有关的致动器数据,

从所述相对处理单元接收与所述至少一个相对传感器有关的采集数据以及与所述至少一个相对致动器有关的致动器数据,

接收与所述相对处理单元的健康状况有关的健康数据,其中与所述相对处理单元的健康状况有关的健康数据称为相对健康数据,

确定与所述本地处理单元的健康状况有关的健康数据,其中所述与所述本地处理单元的健康状况有关的健康数据称为本地健康数据,

根据所接收的相对健康数据和所确定的本地健康数据,将所述本地处理单元从第一状态切换到第二状态,

发送、接收采集数据以及接收健康数据的步骤通过所述至少一个链路或通过所述应急通信装置来实施,所述状态来自于主动状态、被动状态和从动状态;其中,在所述主动状态中,所述本地处理单元确保对所述航空器的引擎的控制;在所述被动状态中,所述本地处理单元不能确保对所述航空器的引擎的控制;在所述从动状态中,所述本地处理单元将对所述本地致动器的控制交给所述相对处理单元以控制所述航空器的引擎,

其中,所述切换步骤包括:

根据所述本地健康数据,确定与所述本地处理单元的状态有关的状态数据以及与所述本地处理单元确保对引擎的控制的能力有关的所述本地处理单元的健康状态数据,以及

当所述状态数据指示所述本地处理单元处于所述被动状态时,并且当所述健康状态数据指示下列状态:所述本地处理单元能够与所述相对处理单元进行通信,所述本地处理单元不能够确保对引擎的控制且所述本地处理单元能够控制所述本地致动器时,将所述本地处理单元切换到所述从动状态。

2. 根据权利要求1所述的方法,其中,

所述相对处理单元和所述本地处理单元通过第一双向数字链路以及通过第二双向数字链路连接,

且所述相对处理单元通过所述第一双向数字链路和所述第二双向数字链路中的每一

个发送相对健康数据，

接收相对健康数据的步骤包括：通过所述第一双向数字链路接收第一相对健康数据以及通过所述第二双向数字链路接收第二冗余相对健康数据；验证所接收的第一健康数据和第二健康数据的一致性；以及根据所述验证确定所发送的相对健康数据。

3. 根据权利要求2所述的方法，其中，确定所发送的相对健康数据包括：当所接收的第一健康数据和第二健康数据不一致时，执行根据在至少两个连续帧上接收的数据来确定所发送的相对健康数据的整合步骤。

4. 根据权利要求1至3中任一项所述的方法，其中，接收相对健康数据包括：验证所接收到的健康数据的完整性。

5. 根据权利要求1至3中任一项所述的方法，其中，确定本地健康数据包括：诊断与所述本地处理单元的硬件和软件有关的健康状况。

6. 根据权利要求1至3中任一项所述的方法，其中，所述切换步骤包括：

确定步骤，其中，所述本地处理单元根据所述本地健康数据和所述相对健康数据确定所述本地处理单元的健康状况比所述相对处理单元的健康状况好，

等待步骤，其中，所述本地处理单元等待所述相对处理单元切换到所述被动状态，

将所述本地处理单元切换到所述主动状态。

7. 一种计算机存储介质，包括：当由处理器执行时，用于执行根据前述任一权利要求所述的切换方法的代码指令。

8. 一种航空器的飞行控制系统的处理单元，所述航空器包含至少一个引擎，所述处理单元被配置为控制称为本地致动器的至少一个致动器，以便控制所述航空器的引擎，

称为本地处理单元的所述处理单元能够连接到至少一个本地传感器上，且通过至少一个链路连接到称为相对处理单元的第二处理单元；所述相对处理单元被配置为控制至少一个相对致动器，且连接到至少一个相对传感器上；所述本地处理单元进一步被配置为连接到应急通信装置上；所述应急通信装置允许在连接所述本地处理单元和所述相对处理单元的所述至少一个链路出现故障的情况下，确保所述本地处理单元和所述相对处理单元之间的数据交换，

所述应急通信装置包括：

传感器或致动器的网络；和/或

用于航空电子设备的机载安全网络，并且

所述处理单元包括：

用于向所述相对处理单元发送与所述至少一个本地传感器有关的采集数据以及与所述至少一个本地致动器有关的致动器数据的装置，

用于从所述相对处理单元接收与所述至少一个相对传感器有关的采集数据以及与所述至少一个相对致动器有关的致动器数据的装置，

用于接收与所述相对处理单元的健康状况有关的健康数据的装置，其中与所述相对处理单元的健康状况有关的健康数据称为相对健康数据，

用于确定与所述本地处理单元的健康状况有关的健康数据的装置，其中与所述本地处理单元的健康状况有关的健康数据称为本地健康数据，

用于根据所接收到的相对健康数据和所确定的本地健康数据将所述本地处理单元从

第一状态切换到第二状态的装置，

所述状态来自于主动状态、被动状态和从动状态；其中，在所述主动状态中，所述本地处理单元确保对所述航空器的引擎的控制；在所述被动状态中，所述本地处理单元不能确保对所述航空器的引擎的控制；在所述从动状态中，所述本地处理单元将对所述本地致动器的控制交给所述相对处理单元以控制所述航空器的引擎，

其中，所述用于根据所接收到的相对健康数据和所确定的本地健康数据将所述本地处理单元从第一状态切换到第二状态的装置还用于：

根据所述本地健康数据，确定与所述本地处理单元的状态有关的状态数据以及与所述本地处理单元确保对引擎的控制的能力有关的所述本地处理单元的健康状态数据，以及

当所述状态数据指示所述本地处理单元处于所述被动状态时，并且当所述健康状态数据指示下列状态：所述本地处理单元能够与所述相对处理单元进行通信，所述本地处理单元不能够确保对引擎的控制且所述本地处理单元能够控制所述本地致动器时，将所述本地处理单元切换到所述从动状态。

9. 一种飞行控制系统，包括根据权利要求8所述的本地处理单元和相对处理单元，进一步包括应急通信装置，所述应急通信装置允许在连接所述本地处理单元和所述相对处理单元的链路出现故障的情况下，确保所述本地处理单元和所述相对处理单元之间的数据交换，

所述应急通信装置包括：

传感器或致动器的网络；和/或

用于航空电子设备的机载安全网络。

10. 根据权利要求9所述的飞行控制系统，其中，所述本地处理单元和所述相对处理单元通过第一双向数字链路以及通过第二双向数字链路连接，所述第二双向数字链路与所述第一双向数字链路冗余，且所述第一双向数字链路和所述第二双向数字链路能同时有效。

11. 根据权利要求10所述的飞行控制系统，其中，所述第一双向数字链路和所述第二双向数字链路是跨通道数据链路CCDL链路。

12. 根据权利要求9所述的飞行控制系统，其中，所述机载安全网络是航空电子全双工交换式以太网AFDX或 $\mu$ AFDX类型的冗余以太网网络。

## 双向架构

### 技术领域

[0001] 本发明涉及航空器的飞行控制系统的领域。

[0002] 更具体地,本发明涉及构成这种系统的双向架构的两个处理单元或计算机间的切换方法。

### 背景技术

[0003] 配备在航空器(例如现有的飞机或直升机)上的机载飞行控制系统执行对所述航空器的引擎的控制功能和调节功能,以确保所述航空器的引擎的正常运行。这些功能对乘客的安全是至关重要的。因此,这样的系统必须可以抵抗故障。

[0004] 为此,现有的飞行控制系统通常包括两个处理单元或计算机,每个处理单元或计算机能够确保引擎的正常运行。从而,这样的系统构成了双向架构,在该双向架构中,每个通道能够在另一个通道故障的情况下,确保上述至关重要的功能的执行。在这两个通道中,通常由具有最佳健康状况(即具有较少故障或故障严重程度最低的)的通道进行引擎的控制。这个通道被称为主动通道。

[0005] 为了执行对引擎的控制和调节功能,每个通道能够控制至少一个致动器。这些致动器可能会出现故障。当所述主动通道的一个或若干个致动器出现故障时,所述主动通道可能不再能够适当地确保对引擎的控制。如果称之为被动通道的另一个通道处于与所述主动通道一样的最坏健康状况时,则所述另一个通道不再能够适当地确保对引擎的控制。从而,这两个通道都不能够适当地确保对引擎的控制,则所述飞行系统的至关重要的功能不再被保证。

[0006] 因此,需要一种使得主动通道即使在主动通道的致动器的至少一个出现故障的情况下也能够为的适当地确保对引擎的控制的方法。

### 发明内容

[0007] 从而,根据第一方面,本发明涉及一种切换方法,由包含至少一个引擎的航空器的飞行控制系统的第一处理单元(称为本地处理单元)实施,

[0008] 所述本地处理单元,被配置为控制至少一个致动器(称为本地致动器)以控制所述航空器的引擎,以及能连接到至少一个本地传感器上且通过至少一个链路连接到第二处理单元(称为相对处理单元)上;所述相对处理单元,被配置为控制至少一个相对致动器,以及连接到至少一个相对传感器上;所述本地处理单元进一步被配置以便连接到应急通信装置上,所述应急通信装置允许在连接所述本地处理单元和所述相对处理单元的所述至少一个链路出现故障的情况下,确保所述本地处理单元和所述相对处理单元之间的数据交换;所述应急通信装置包括:传感器或致动器网络,和/或用于航空电子设备的机载安全网络,

[0009] 所述方法包括以下步骤:

[0010] -向所述相对处理单元发送与所述至少一个本地传感器有关的采集数据,以及与所述至少一个本地致动器有关的致动器数据,

[0011] -接收来自所述相对处理单元的与所述至少一个相对传感器有关的采集数据,以及与所述至少一个相对致动器有关的致动器数据,

[0012] -接收与所述相对处理单元的健康状况有关的健康数据,称为相对健康数据,

[0013] -根据与所述本地处理单元的健康状况有关的健康数据来确定本地健康数据,

[0014] -根据所接收到的相对健康数据和所确定的本地健康数据,将所述本地处理单元从第一状态转换至第二状态,

[0015] 所述用于发送、接收采集数据的步骤以及所述用于接收健康数据的步骤是通过所述至少一个链接或所述应急通信装置来实施;所述状态来自于主动状态、被动状态和从动状态,其中,在所述主动状态中,所述本地处理单元确保对所述航空器的引擎的控制,在所述被动状态中,所述本地处理单元不能确保对所述航空器的引擎的控制,在所述从动状态中,所述本地处理单元将对所述本地致动器的控制交给所述相对处理单元,以对所述航空器的引擎进行控制。

[0016] 这样的方法使得每个处理单元能够具有全局系统的完整图像(所述完整图像包含连接到所述相对处理单元的致动器和传感器),从而即使本地致动器故障,也能够适当地确保对引擎的控制。从而,无法控制所述航空器的引擎的一个处理单元,可为处于主动状态的另一个处理单元提供到所述一个处理单元的致动器的访问,从而即使所述主动处理单元的致动器中的一个或几个出现故障,所述飞行控制系统也能够确保对引擎的控制。进一步,应急通信装置的使用提供避免所述双向系统的全盲以及避免两个处理单元之间的通信被切断的可能性。最后,用于在所述处理单元之间交换信息的网络的使用,提供提高所述处理单元之间的通信装置的冗余级别,以及使得无需对专门用于所述处理单元之间的通信的附加的通信装置进行设置,仍然能够确保所述飞行控制系统的运行安全的可能性。

[0017] 一方面,所述相对处理单元和所述本地处理单元通过第一双向数字链路连接,另一方面,所述相对处理单元和所述本地处理单元通过第二双向数字链路连接,且所述相对处理单元在每个链路上发送相对健康数据。所述根据所述第一方面的方法的接收相对健康数据的步骤可包括以下步骤:通过所述第一链路接收第一相对健康数据以及通过所述第二链路接收第二冗余相对健康数据;所接收的第一健康数据和第二健康数据的一致性;以及根据所述验证步骤确定所述相对健康数据。

[0018] 这使得能够加强所述系统对所述处理单元之间的数据交换的变化的检测能力,从而最大限度地减少了所述飞行控制系统的故障概率。

[0019] 所述用于确定所发送的相对健康数据的步骤可包括:当所述第一和第二接收到的健康数据不一致时,在整合步骤期间,根据在至少两个连续的帧上接收的数据来确定所发送的相对健康数据。

[0020] 当在第一帧上的两个链路所传输的数据不一致,且不允许以安全的方式来确定所发送的健康数据时,这允许在确定所发送的相对健康数据期间错误风险的最小化。

[0021] 为了确保所接收到的数据在传输期间没有损坏,所述用于根据所述第一方面的方法的接收相对健康数据的步骤可包括:用于验证所接收到的健康数据的完整性的步骤。

[0022] 所述用于根据所述第一方面的方法的确定本地健康数据的步骤可包括:用于诊断与所述本地处理单元的硬件和软件有关的健康状况的步骤。

[0023] 这使得能够获取健康数据,以允许对影响所述本地处理单元的确保对引擎的控制

的能力的整个故障进行诊断。

[0024] 根据所述第一方面的方法的切换步骤可包括以下步骤：

[0025] 根据所述本地健康数据，确定与所述本地处理单元的状态有关的状态数据以及与所述本地处理单元确保对引擎的控制的能力有关的所述本地处理单元的健康状态数据，以及

[0026] 当所述状态数据指示所述本地处理单元处于所述被动状态时，并且当所述健康状态数据指示下列状态：所述本地处理单元能够与所述相对处理单元进行通信，所述本地处理单元不能够确保对引擎的控制且所述本地处理单元能够控制所述本地致动器时，将所述本地处理单元切换到所述从动状态。

[0027] 这使得能够确保在切换到所述从动状态之前，所述处理单元不能确保对引擎的控制，所述处理单元无法确保代替另一个处理单元对引擎的控制，以及确保影响所述处理单元的故障不能阻止所述处理单元向所述另一个处理单元提供到所述处理单元的致动器的访问。

[0028] 根据优势和非限制特征，根据所述第一方面的方法的切换步骤包括：

[0029] -确定步骤，其中，所述本地处理单元根据所述本地健康数据和所述相对健康数据来确定所述本地处理单元的健康状况好于所述相对处理单元的健康状况，

[0030] -等待步骤，其中，所述本地处理单元等待所述相对处理单元切换到所述被动状态，

[0031] -切换所述本地处理单元到所述主动状态的步骤。

[0032] 这使得能够避免所述飞行控制系统处于在两个处理单元同时是主动状态且仍将冒险发送矛盾的指令到它们的致动器的情形。

[0033] 根据第二方面，本发明涉及一种计算机程序产品，包括：当所述程序由处理器执行时，用于执行根据所述第一方面的切换方法的代码指令。

[0034] 根据第三方面，本发明涉及一种包含至少一个引擎的航空器的飞行控制系统的处理单元，配置为控制至少一个致动器（称为本地致动器）以便控制所述航空器的引擎，

[0035] 所述处理单元（即所述本地处理单元）能连接到至少一个本地传感器上以及通过至少一个链路连接到第二处理单元（称为相对处理单元）上；所述相对处理单元，配置为控制至少一个相对致动器以及连接到至少一个相对传感器上；所述本地处理单元进一步被配置以便连接到应急切换装置上，所述应急切换装置在连接到所述本地处理单元和所述相对处理单元的所述至少一个链路故障的情况下，使得能够确保所述本地处理单元和所述相对处理单元之间数据交换；所述应急切换装置包括：传感器或致动器网络，和/或用于航空电子设备的机载安全网络，以及，包括：

[0036] -向所述相对处理单元发送与所述至少一个本地传感器有关的采集数据以及与所述至少一个本地致动器有关的致动器数据的装置，

[0037] -接收来自所述相对处理单元的与所述至少一个相对传感器有关的采集数据以及与所述至少一个相对致动器有关的致动器数据的装置，

[0038] -接收与所述相对处理单元的健康状况有关的健康数据（称为相对健康数据）的装置，

[0039] -确定与所述本地处理单元的健康状况有关的健康数据（称为本地健康数据）的装

置，

[0040] 根据所接收到的相对健康数据和所确定的本地健康数据，将所述本地处理单元从第一状态转换至第二状态的装置，

[0041] 所述状态来自于主动状态、被动状态和从动状态，其中，在所述主动状态中，所述本地处理单元确保对所述航空器的引擎的控制，在所述被动状态中，所述本地处理单元不能确保对所述航空器的引擎的控制，在所述从动状态中，所述本地处理单元将对所述本地致动器的控制交给所述相对处理单元，以为了控制所述航空器的引擎。

[0042] 根据第四方面，本发明涉及一种飞行控制系统，包括：根据所述第三方面的两个处理单元；以及进一步包括：应急通信装置，所述应急通信装置允许在连接到所述本地处理单元和所述相对处理单元的所述至少一个链路出现故障的情况下，确保所述本地处理单元和所述相对处理单元之间的数据交换；所述应急切换装置包括：传感器或致动器网络，和/或用于航空电子设备的机载安全网络。

[0043] 这样的计算机程序产品、处理单元以及飞行控制系统具有与根据所述第一方面的方法提到的相同的优点。

[0044] 一方面，两个处理单元可通过第一双向数字链路连接，另一方面，两个处理单元可通过第二双向数字链路连接，所述第二链路与所述第一链路冗余，且所述第一链路和所述第二链路也可同时有效。

[0045] 这样的系统通过其处理单元和其通信装置的冗余性以及通过通信链路的数目的最小化，具有高的抗故障能力，同时减小了自身的体积。

[0046] 所述第一链路和所述第二链路可以是CCDL链路（“跨通道数据链路”）。

[0047] 这样的链路特别地使得所述处理单元能够交换比通过已知系统的离散模拟链路交换的健康信息更复杂的健康信息，同时限制了布线体积。

[0048] 所述用于航空电子设备的机载安全网络例如可以是：AFDX（“航空电子全双工交换式以太网”）类型或 $\mu$ AFDX类型的冗余以太网网络。

## 附图说明

[0049] 通过阅读以下实施例的描述，其他的特征和优点将变得明显。将参考附上的附图给出该描述，其中：

[0050] 图1示意性地示出了根据本发明的实施例的飞行控制系统；

[0051] 图2示意性地示出了根据本发明的实施例的旨在在飞行控制系统的两个处理单元之间建立两个CCDL链路的硬件装置；

[0052] 图3示意性地示出了根据本发明的实施例的飞行控制系统的每个处理单元的CCDL模块的物理隔离；

[0053] 图4示意性地示出了根据本发明的实施例的旨在建立两个CCDL链路的一个处理单元的硬件装置的隔离；

[0054] 图5表示根据本发明的实施例的飞行控制系统中的处理单元的状态图。

## 具体实施方式

[0055] 本发明实施例涉及一种切换方法，所述方法由包括至少一个引擎的航空器的飞行

控制系统(如图1所示)的第一处理单元1(称为本地处理单元)实施。

[0056] 所述飞行控制系统还包括:第二处理单元2(称为相对处理单元)。所述本地处理单元可连接到至少一个本地传感器上,且通过链路3和4中的至少一个连接到所述相对处理单元上,所述相对处理单元连接到至少一个相对传感器上。所述两个处理单元是冗余的,且每一个处理单元可执行用于控制和调节所述航空器的引擎的功能。为此,每个处理单元被配置为控制至少一个致动器,以便控制所述航空器的引擎。所述本地处理单元1可控制的致动器被称之为本地致动器。由所述相对处理单元控制的致动器称之为相对致动器。从而,如图1所示的系统为包含有通道A和通道B的双向架构。

[0057] 所述本地处理单元1和2可以是包含了若干处理器的同一多处理器计算机系统中的一个处理器。为了加强所述飞行控制系统对外部侵略的抵抗,以及避免单独的本地事件使得两个处理单元1和2都不工作,两个通道可以在分开的壳体中彼此相距一定距离地安装。在这样的配置中,所述处理单元不是集成在一个单独的处理器中的执行核心。

[0058] 所述系统还包括:通信装置,所述通信装置使得能够连接两个处理单元以允许用于每个处理单元正常运行的必要数据(例如,关于所述相对处理单元的健康状况的信息)交换。

[0059] 在可选的实施例中,这些通信装置被配置为在所述第一处理单元1和所述第二处理单元2之间建立第一双向数字链路3和第二双向数字链路4。这样的系统不包括两个处理单元之间的任何离散的链路,这能够限制所述系统布线的复杂性,以及所述通信链路中的一个链路出现故障的概率。

[0060] 所述第二链路4与所述第一链路3冗余,以确保在所述第一链路3故障的情况下两个处理单元之间的通信,反之亦然。如此的冗余保证了两个处理单元之间的信息交换的良好安全级别。

[0061] 进一步,所述第一链路和所述第二链路可以同时有效。从而,不同于在所述第一链路故障的情况下仅仅使用冗余的链路的系统,所述飞行控制系统可在正常运行(即所述两个链路均不存在任何故障)期间同时使用所述第一链路3和所述第二链路4,且可通过同时使用所述两个链路来验证在两个处理单元之间交换的数据不存在损坏。

[0062] 所述第一处理单元1和第二处理单元2可使用用于通过两个链路3和4在彼此之间通信的程序,例如,所述过程来自于以太网IEEE 802.3协议,HDLC(高级数据链路控制)协议,SDLC(同步数据链路控制)协议或其他任何具有检测或纠正错误功能的协议。以太网链路可以特别地确保高性能、大的环境鲁棒性、尤其是关于避雷和电磁兼容性(“EMC”),以及通过用于控制数据完整性和用于控制流的机制的应用确保高功能鲁棒性。进一步,所述以太网协议是与航空电子通信技术(例如,AFDX(“航空电子全双工交换式以太网”)或 $\mu$ AFDX、维护技术)相一致的工业标准。

[0063] 所述第一链路和所述第二链路可以是CCDL链路(“跨通道数据链路”)。这样的链路使得能够以小于一百微秒的精度来同步每个应用。作为对如在已知系统中的交换离散数据的代替,这样的链路还允许交换由硬件或软件构建的健康信息、对所述系统有用的信息(采集、状态)、以及操作系统(OS)和应用系统(AS)的功能数据。

[0064] 图2示出了在处理单元A和B之间的CCDL链路。每个处理单元1、2包含有:系统5a、5b,所述系统5a、5b包含有:用于建立所述第一CCDL链路3的第一CCDL模块(CCDLA)6a、6b,以

及用于建立所述第二CCDL链路4的第二CCDL模块(CCDLB) 7a、7b。这样的系统可表现为片上系统(SoC,片上系统),或是由在单独的壳体中或FPGA卡板中实现的微处理器和外围器件构成的系统。每一个CCDL模块通过物理层连接到自身的壳体的输入/输出接口上。例如,这样的层可包括:如图2所示的硬件接口Phy8a、8b、8c、8d以及变压器9a、9b、9c、9d。

[0065] 如图3所示,每一个处理单元的CCDL模块通过放置在所述系统5a、5b上的不同位置且彼此远离而被物理隔离,例如,将每一个CCDL模块放置在片上系统的角落。这使得能够在SEU(“单粒子翻转”)或MBU(“多位翻转”)型改变的情况下降低共同故障的概率。

[0066] 根据第一替换方案,每个系统5a、5b是由单独的电源进行供电的。根据第二替换方案,所述系统包括为整个所述片上系统共有的电源15。如图4所示,每个片上系统可通过两个不同的时钟信号11和12供电。从而,尽管它们不是独立供电的,但是每个处理单元的CCDL模块可以通过独立的时钟供电,其通过防止一个CCDL模块的时钟故障影响另一个CCDL模块,加强了所述片上系统的抗故障能力。

[0067] 每个处理单元的CCDL模块可通过如图2所示的本地实时时钟机制(HTR或RTC,实时时钟) 10a、10b的方式以及同步机制的方式(例如使用同步窗的机制)被同步。从而,在失去同步的情况下,每个处理单元可通过自身的本地时钟运行,然后在接收到有效信号时再次进行同步。所述本地时钟机制可由应用程序来编程,并且其编程被保护以防止SEU(“单粒子翻转”)或MBU(“多位翻转”)型改变。然而,即使在没有同步或时钟丢失的情况下,所述CCDL链路仍可以继续运行。

[0068] 所述系统进一步可包括:应急通信装置,所述应急通信装置使得能够确保在所述第一和第二处理单元之间数据的交换,且所述应急通信装置仅使用在所述第一和第二链路故障的情况下,以便避免所述处理单元之间的通信被切断。

[0069] 在如图1所示的第一实施例中,这些应急通信装置可包括:传感器或致动器的网络13。作为一个示例,所述传感器或致动器的网络可以是智能传感器或致动器(智能-传感器,智能-致动器)的网络。然后,每个处理单元可通过RS-485类型的总线连接到所述网络13,以允许不再以模拟方式而是以数字方式进行信息的发送。

[0070] 在如图1所示的第二实施例中,这些应急通信装置包括:用于航空电子设备14的机载安全网络。作为一个示例,这样的机载安全网络可以是冗余以太网,例如AFDX(“航空电子全双工交换式以太网”)或 $\mu$ AFDX。这样的网络提供了用于共享资源、用于分离流、以及用于航空认证所需的确定性和可用性的装置。

[0071] 在所述处理单元之间发送的所述数字信号可能扰动敏感,用于控制在两个远程处理单元之间发送的数据的完整性和一致性的机制可以被设置到位。

[0072] 从而,每个处理单元可包括:用于验证所接收到的数据的完整性的装置。

[0073] 为了验证所接收到的数据的完整性,每个接收到的帧的不同字段可以被验证,特别地,在以太网链路的情况下,与目的地址有关的字段、与源地址有关的字段、与帧的类型有关的字段、与帧的长度有关的字段、与MAC数据和填充数据有关的字段可以被验证。如果所述帧的长度与所述帧的长度字段中指定的长度不一致,或如果相应字节不是整数,则所述帧可被认为是无效的。如果根据接收到的所述帧计算的冗余控制(CRC,“循环冗余校验”)由于错误(例如发送期间的干扰)而与所述接收的CRC不对应,则所述帧也可被认为是无效的。

[0074] 进一步,当所述本地处理单元和所述相对处理单元通过两个双向链路连接时,则每个处理单元可包括:用于在所述第一链路和所述第二链路上数据的发送之后,在所发送的帧没有故障或损坏的情况下,验证传递相同信息的两个链路上所接收到的数据的一致性,以及用于确定实际发送的数据的装置。当在两个链路上所接收到的数据不一致时,所述处理单元应用一个整合步骤,在该步骤期间,根据在至少两个连续的帧,或可选地在至少三个连续的帧上接收到的数据来确定实际发送的数据。如此的整合也可以通过延长对两个连续以太网数据包的接收进行分离的时段来实现,例如通过将所述时段的长度设置为大于电磁扰动的持续时长来实现。这可以通过增加一个参数(“帧间间隔”)来实现,该参数设置在所发射的数据包之间的时段。例如,这种实现方式能够以冗余的方式避免发送的两个以太网数据包被损坏。

[0075] 所述飞行控制系统中的每个处理单元可以处于以下状态中的一种,如图5的状态图所示:

[0076] ■主动状态(“ACTIVE(主动)”)15,其中,所述处理单元确保对所述航空器的引擎的控制,

[0077] ■被动状态(“PASSIVE(被动)”)16,其中,所述处理单元不能确保对所述航空器的引擎的控制,但执行其他的功能(例如,诊断功能),以及可选地可以与所述控制系统的另一个处理单元进行通信。

[0078] ■复位状态(“RESET(复位)”)17,其中,所述处理单元是不活动的,且不执行任何功能,

[0079] ■从动状态(“SLAVE(从动)”)18,其中,所述处理单元将对自身的致动器(用于控制所述航空器的引擎)的控制交给另一个处理单元。

[0080] 为了使每个处理单元具有对包括连接到所述相对处理单元的所述致动器和传感器的全局系统的完整概览,以便在本地致动器故障的情况下能够正确地确保对所述引擎的控制,由所述本地处理单元实施的切换方法包括以下步骤:

[0081] -向所述相对处理单元发送与所述至少一个本地传感器有关的采集数据、以及与所述至少一个本地致动器有关的致动器数据,

[0082] -从所述相对处理单元接收与所述至少一个相对传感器有关的采集数据、以及与所述至少一个相对致动器有关的致动器数据。

[0083] 作为传感器情况下的一个示例,与传感器有关的采集数据可以是包含由所述传感器测量的温度的温度。

[0084] 进一步,为了允许所述本地处理单元1从上述描述的四种状态中改变状态,所述切换方法包括以下步骤:

[0085] -接收与所述相对处理单元2的健康状况有关的健康数据(称之为相对健康数据),例如状态,

[0086] -确定与所述本地处理单元1的健康状况有关的健康数据,称之为本地健康数据,

[0087] -根据所接收到的相对健康数据和所确定的本地健康数据,将所述本地处理单元1从第一状态切换到第二状态,所述第一状态和所述第二状态来自于上述描述的主动状态、被动状态、复位状态和从动状态。

[0088] 所述用于发送、接收采集数据以及接收健康数据的步骤是通过连接两个处理单元

的链路3、4或在所述链路3、4故障的情况下通过应急通信装置13、14来实施。

[0089] 所接收到的相对健康数据可能会遭受扰动,所述用于接收相对健康数据的步骤可包括:用于验证所接收到的数据的完整性的步骤。

[0090] 此外,用于验证一致性的机制也可以被应用,所述相对健康数据可以在所述双向链路上以冗余的方式发送。所述用于接收相对健康数据的步骤包括以下步骤:通过所述第一链路接收第一相对健康数据以及通过所述第二链路接收第二冗余相对健康数据,验证接收到的第一和第二健康数据的一致性,以及根据所述验证步骤确定所发送的相对健康数据。或者,在验证所述第一链路上接收到的所述第一相对健康数据和所述第二链路上接收到的所述第二相对健康数据的一致性之前,它们可能要经受完整性的验证。

[0091] 在所述两个链路上接收到的数据不一致的情况下,所述本地处理单元可以忽略这个健康数据,并等待新的相对健康数据的传输。在两个或多个连续的传输期间,在两个链路上接收到不一致的数据的情况下,如果在第一传输期间接收到的数据与后续传输期间接收到的数据一致,所述本地处理单元可以适当地保留所接收的指示所述相对处理单元的最坏健康状况的数据作为相对健康数据。否则,只要没有一致地接收到新的健康数据,则保持一致的方式最后接收到的健康数据。

[0092] 为了确定本地或相对健康数据,相关处理单元对与自身的硬件元件和软件元件有关的健康状况做出诊断。这样的诊断可以根据从不同的监测装置或从若干寄存器中获得的信息来建立。作为一个示例,寄存器使得能够获取所述处理单元的硬件的健康状况,另一个寄存器使得能够获取所述处理单元的软件的健康状况。

[0093] 从而,所确定的本地健康数据或由所述相对处理单元发送的数据使得能够选择一个通道以及建立全系统诊断。特别地,它们可以是诊断CCDL数据,操作系统或应用程序的状态的数据,硬件的诊断数据(尤其是传感器或致动器的诊断数据)、由软件产生的功能诊断数据。

[0094] 所述本地处理单元可以根据本地或相对健康数据确定指示相应的本地或相对处理单元处于的状态的状态数据(主动、被动、从动或复位),以及与所述本地或相对处理单元的确保对所述引擎的控制的能力有关的健康状态的数据。

[0095] 根据一实施例,每个处理单元可以具有以下四种状态中的一种状态:

[0096] ■ 状态“GOOD(良好)”,其中,所述处理单元没有任何故障,

[0097] ■ 状态“ACCEPTABLE(可接受)”,其中,所述处理单元具有一些故障,然而,这些故障将不会阻止其正确地确保对引擎的控制,例如,CCDL链路变压器的损坏,或来自于一个CCDL链路的时钟信号的丢失。

[0098] ■ 状态“SLAVE(从动)”,其中,所述处理单元具有太严重的故障使得其不能够正确地确保对所述引擎的控制,例如处理器故障;但是所述本地处理单元没有会阻止其控制自身的致动器或阻止其与所述相对处理单元进行通信的材料故障。

[0099] ■ 状态“BAD(差)”,其中,所述处理单元不能够正确地确保对所述引擎的控制,以及所述本地处理单元具有至少一个硬件故障,所述至少一个硬件故障阻止所述处理单元控制自身的致动器,例如影响整个所述处理单元电源或时钟故障或两个CCDL链路的故障。

[0100] 所述本地处理单元定期执行上述用于接收相对健康数据和用于确定本地健康数据的步骤。为了确定所述本地处理单元是否应该改变状态,所述本地处理单元根据所述本

地健康数据确定指示自身状态的本地状态数据以及指示自身健康状态的本地状态数据。而且,所述本地处理单元根据所述相对健康数据确定指示所述相对处理单元的状态的相对状态数据以及指示所述相对处理单元的健康状态的相对状态数据。

[0101] 然后,所述本地处理单元将由所述本地状态数据指示的所述本地处理单元的健康状况与由所述相对状态数据指示的所述相对处理单元的健康状况进行比较。

[0102] 如果所述本地处理单元处于主动状态,并且所述本地处理单元的健康状况仍然比另一个处理单元的健康状况好 (CTL\_REQ=1),所述处理单元保持在主动状态,且继续确保对引擎的控制。

[0103] 作为一个示例,在以下情况下,所述本地处理单元的健康状况比所述相对处理单元的健康状况好:

[0104] -所述本地处理单元具有GOOD状态,且所述相对处理单元具有ACCEPTABLE、SLAVE和BAD状态之一,

[0105] -所述本地处理单元具有ACCEPTABLE状态,且所述相对处理单元具有SLAVE状态或BAD状态。

[0106] 如果所述本地处理单元处于主动状态,且所述本地处理单元的健康状况变得不如另一个处理单元的健康状况好 (CTL\_REQ=0),则所述本地处理单元将切换到被动状态,并且停止确保对所述引擎的控制,然后由所述相对处理单元确保对所述引擎的控制。

[0107] 作为一个示例,在以下情况下,所述本地处理单元的健康状况不如所述相对处理单元的健康状况好:

[0108] -所述本地处理单元具有ACCEPTABLE状态,且所述相对处理单元具有GOOD状态,或

[0109] -所述本地处理单元具有SLAVE状态,且所述相对处理单元具有GOOD状态或ACCEPTABLE状态,或

[0110] -所述本地处理单元具有BAD状态,且所述相对处理单元具有GOOD状态或ACCEPTABLE状态。

[0111] 如果所述本地处理单元处于被动状态,且所述本地处理单元的健康状况仍然没有所述相对处理单元的健康状况好 (CTL\_REQ=0),则所述处理单元仍然在被动状态。

[0112] 如果所述本地处理单元处于被动状态,且所述本地处理单元的健康状况变得比所述相对处理单元的健康状况好 (CTL\_REQ=1),则所述本地处理单元切换到主动状态,以便替代所述相对处理单元来确保对所述引擎的控制。从被动状态到主动状态的切换可以经过等待状态19,在等待状态,所述本地处理单元在进入所述主动状态之前,等待所述相对处理单元进入所述被动状态 (OPP\_CH\_STATE=0),以便接管对所述引擎的控制。这使得能够避免所述飞行控制系统处于两个处理单元同时是主动状态且仍将冒险发送矛盾的命令到它们的致动器的情况。只要所述相对处理单元是主动状态 (OPP\_CH\_STATE=1),则所述处理单元仍可处于这样的等待状态19。如果在所述本地处理单元进入主动状态之前,所述相对处理单元的健康状况再次变得比所述本地处理单元的健康状况好 (CTL\_REQ=0),则所述本地处理单元甚至可能从等待状态返回到被动状态。

[0113] 如果所述本地处理单元处于被动状态,且所述本地状态数据指示所述处理单元具有“SLAVE”健康状态 (Remote\_Req=1 (远程\_Req=1)),则所述本地处理单元可以切换到上述描述的所述从动状态。根据替代方案,也可通过从所述相对处理单元接收用于请求访问

所述本地处理单元的致动器的信号,来调节到所述从动状态的切换。当所述本地状态数据仅仅指示所述处理单元具有“SLAVE”的健康状态 (Remote\_Req=0) 时,所述处理单元可以从所述从动状态返回到所述被动状态。

[0114] 如果所述本地状态数据指示“BAD”健康状态时,所述本地处理单元不管自身当前的状态如何都切换到所述复位状态。一旦所述复位被成功地执行 (HRESET\_N上升沿),所述处理单元可再次进入到所述被动状态。

[0115] 在所述本地处理单元和所述相对处理单元具有相同的健康数据 (GOOD或ACCEPTABLE) 的情况下,根据第一替代方案,每个处理单元保持在其当前状态 (主动或被动)。根据第二替代方案,可以将对引擎的控制提供给默认处理单元,例如所述第一处理单元1。在这种情况下,如果所述默认处理单元已经处于主动状态,则两个处理单元保持在其当前状态;否则,如果所述默认处理单元之前处于被动状态,则从所述被动状态切换到所述主动状态,反之亦然。

[0116] 如果一个处理单元恢复先前已经丧失的功能,则所述处理单元可以从ACCEPTABLE状态切换到GOOD状态,但一个处于SLAVE或BAD状态的处理单元除非被复位否则不能再次切换到ACCEPTABLE或GOOD状态。

[0117] 从而,所述控制系统的所述被动通道可以切换到使得所述被动通道的致动器可用于处于更好的健康状况的主动通道的状态,使得即使存在影响所述主动通道控制自己的致动器的能力的故障,所述飞行控制系统也可以继续确保对引擎的控制。

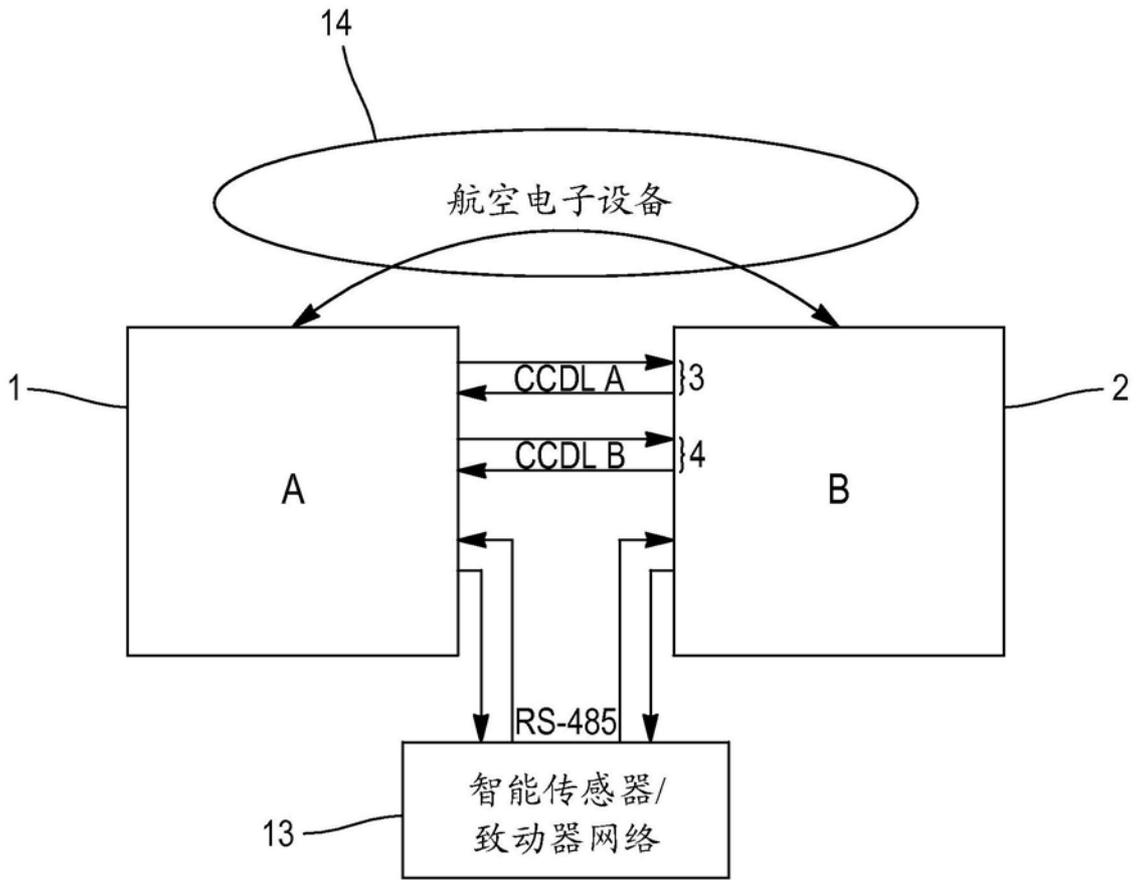


图1

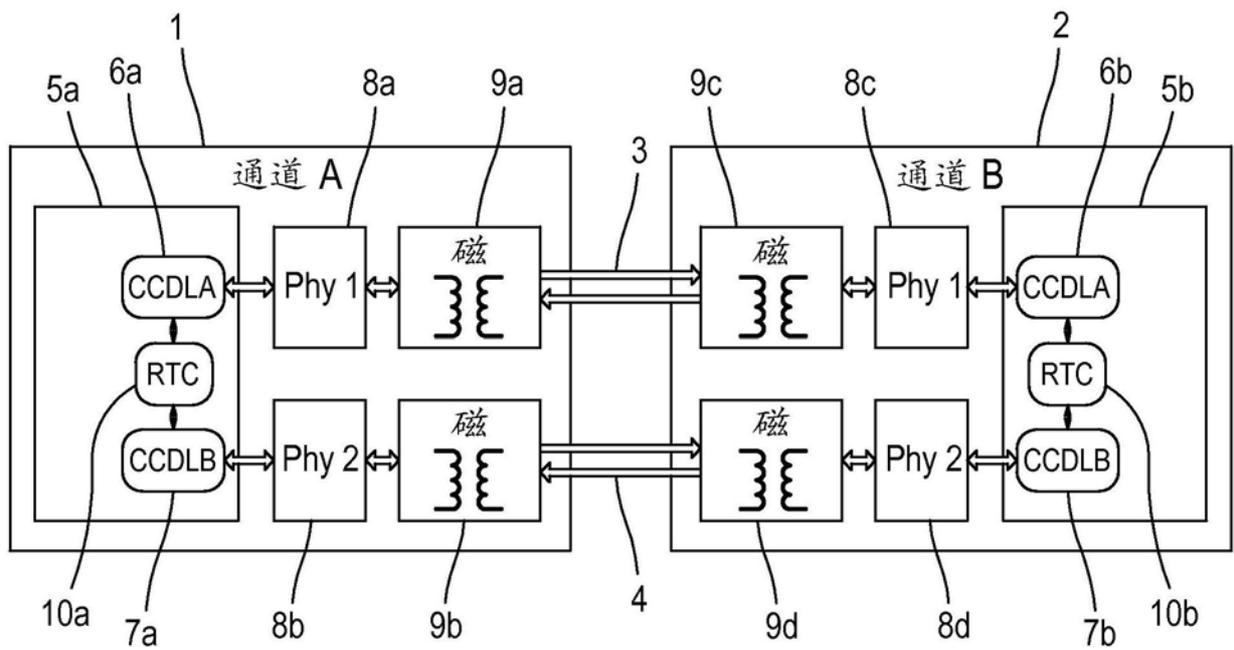


图2

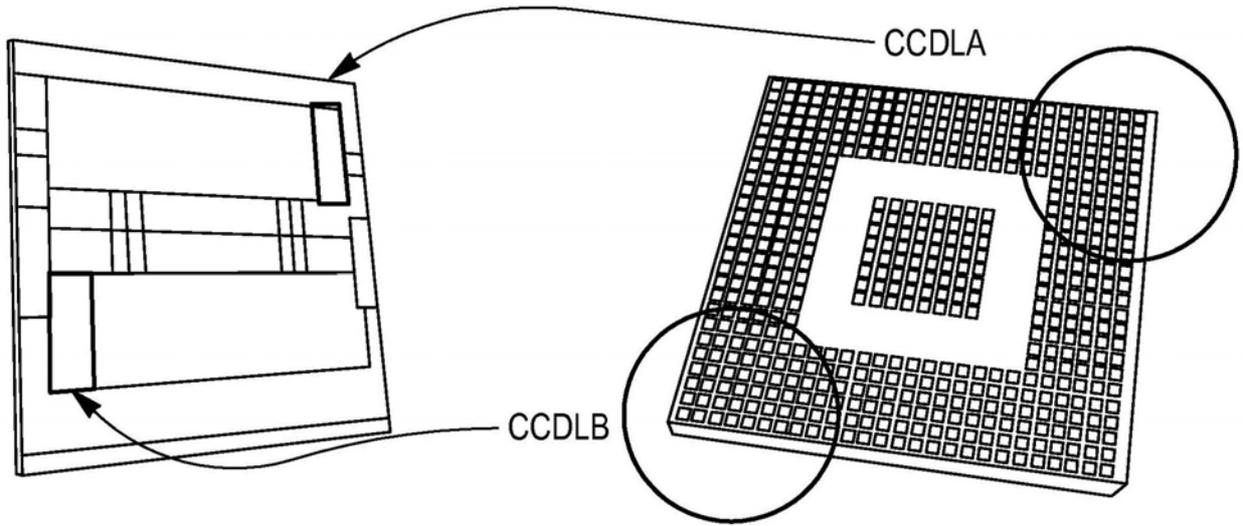


图3

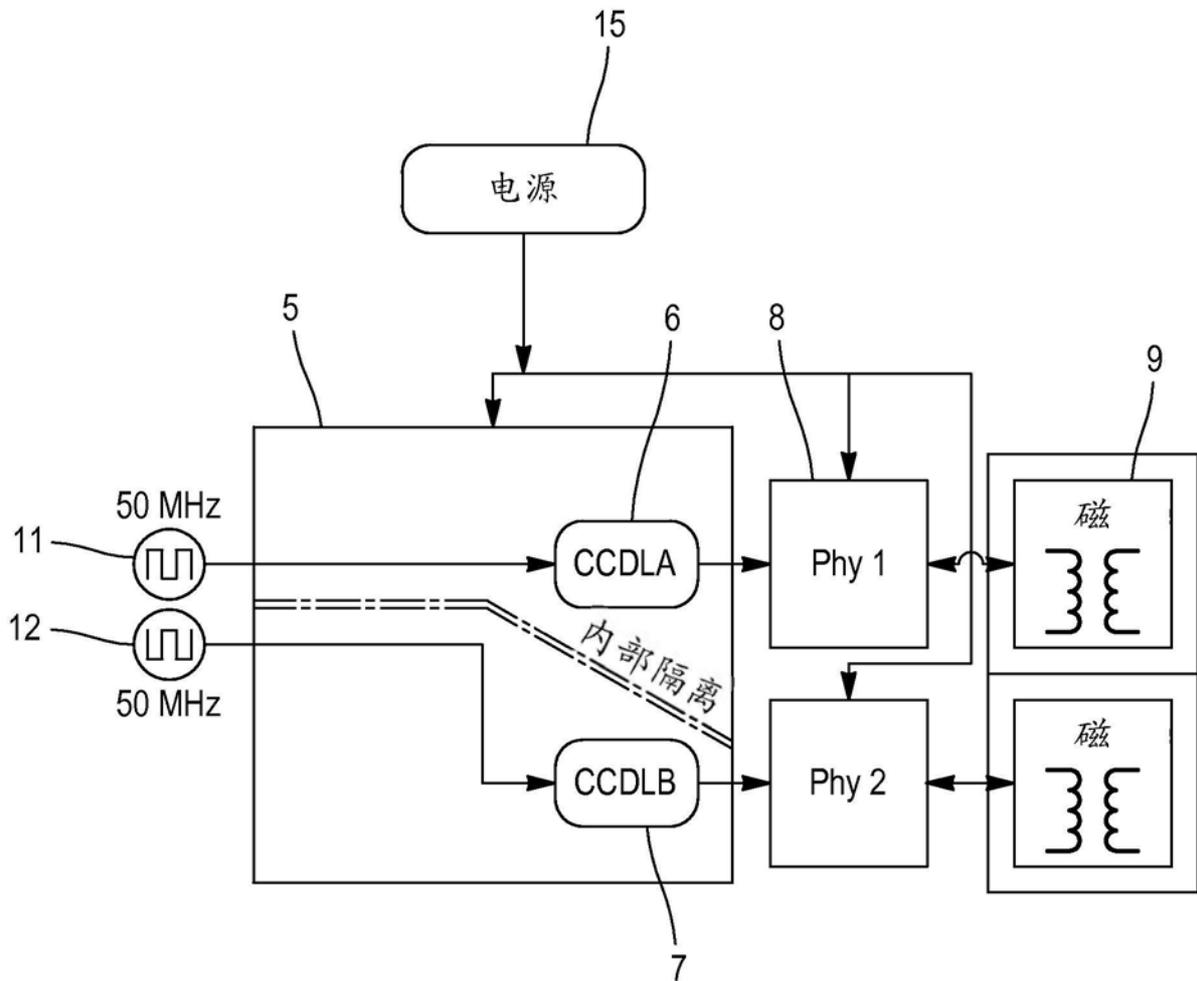


图4

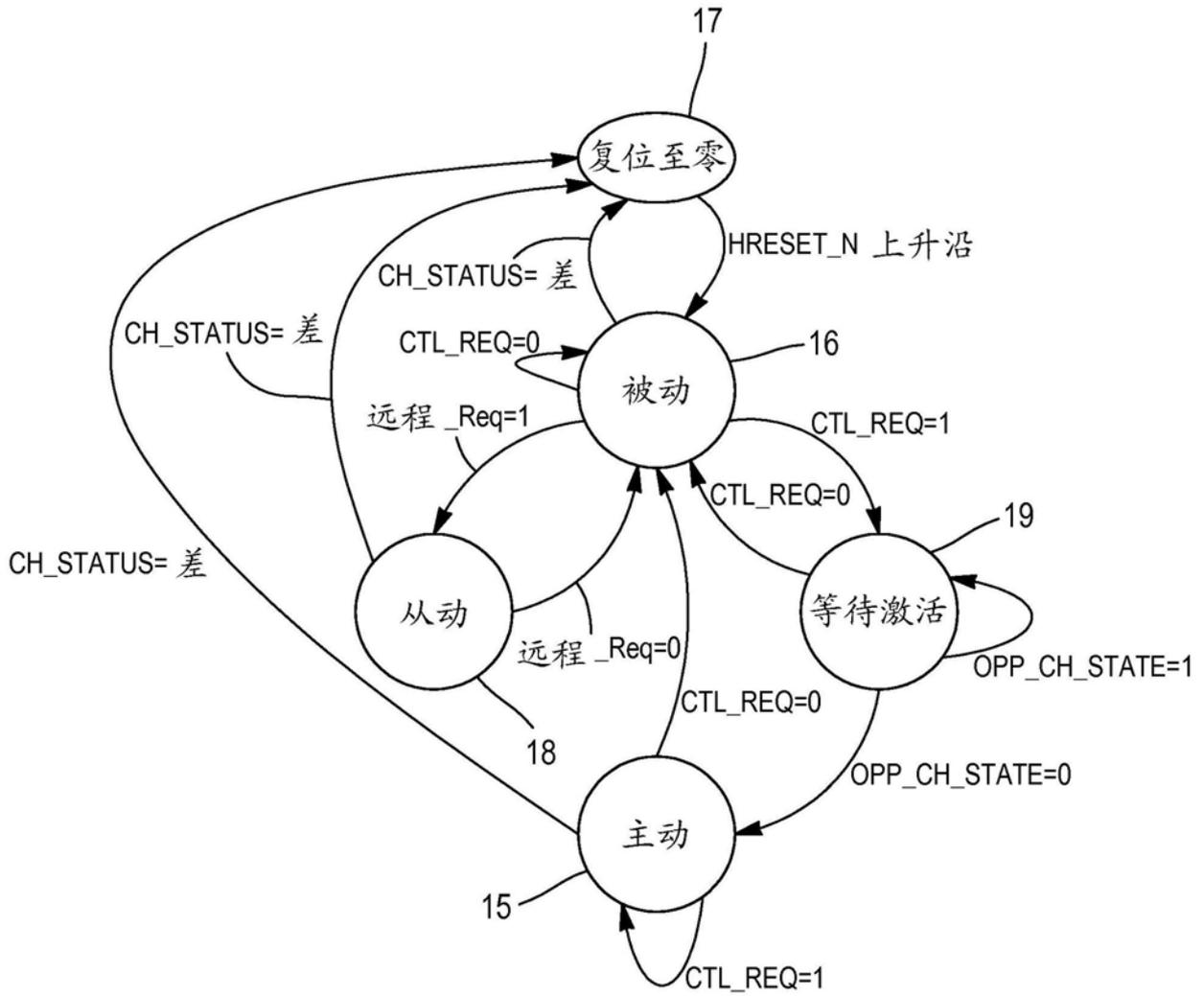


图5