[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]

G21D 3/04

[12]发明专利申请公开说明书

[21]申请号 99811012.4

[43]公开日 2001年10月17日

[11]公开号 CN 1318199A

[22]申请日 1999.9.17 [21]申请号 99811012.4

[30]优先权

[32]1998.9.18 [33]US [31]60/101,004

[86]国际申请 PCT/US99/21364 1999.9.17

[87]国际公布 WO00/17888 英 2000.3.30

[85]进入国家阶段日期 2001.3.16

[71]申请人 西屋电气有限责任公司

地址 美国宾西法尼亚州

[72]发明人 埃德加·M·布朗

小弗兰克·M·凯斯勒

小理查德·M·曼纳泽

雷蒙德·R·森尼查尔

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

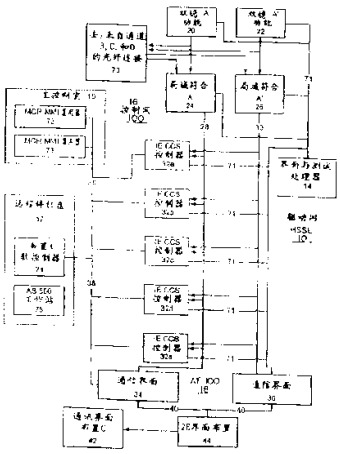
代理人 李德山

权利要求书3页 说明书8页 附图页数1页

[54]发明名称 数字电站保护系统

[57]摘要

一种与核电站的数字电站保护系统配合使用的在需要时激活紧 急反应装置的系统和方法。四个逻辑通道中的每个中的两个冗余双 稳处理器根据来自监测电站运行的电站保护系统的输出确定电站运 行的特定参数是否超出安全限度。各通道内的两个独立的符合处理器将各双稳处理器的输出与另一个逻辑通道的双稳处理器相应的输 出相比较,其结果被提供给一系列部件控制系统处理器以在需要时 激活紧急反应装置。光纤网络将各逻辑通道相互连接,各通道内在 部件控制系统处理器和主控制室之间有光纤网络以便能够向部件控 制处理器发送手动激活信号。



ISSN1008-4274

权　利　要　求　书

1. 一个工程安全特征部件控制系统，它接收来自监测电站运行参数的数字电站保护系统的信号，包括:

多个监测上述电站运行的一个特定参数的逻辑通道，其中上述各逻辑通道包括:

用来接收来自上述数字电站保护系统关于上述特定参数的输入并判定上述电站运行的上述特定参数是否在预定的安全限度以内的双稳处理器;

用来将上述双稳处理器的输出与上述多个通道中的其它通道的双稳处理器的输出相比较的符合处理器; 和

接收来自上述通道和至少另外一个通道的符合处理器的输出并根据所述输出来驱动紧急反应系统的部件的多个部件控制系统处理器; 和

与至少一个双稳处理器、上述符合处理器和上述部件控制系统处理器相连的界面与测试处理器。

2. 权利要求 1 的系统，其中所述多个逻辑通道包括四个逻辑通道。

3. 权利要求 1 的系统，其中所述的至少一个部件控制系统处理器包括各自控制一个预定的紧急反应装置组的多个部件控制系统处理器。

4. 权利要求 3 的系统，其中至少一个所述的部件控制系统处理器是冗余的。

5. 权利要求 1 系统，其中所述各逻辑通道包括:

一个接收输入并执行与第一双稳处理器完全相同功能的第二冗余双稳处理器;

一个接收来自上述第二双稳处理器的输出并将该输出与上述多个逻辑通道中的其它通道的冗余双稳处理器的输出比较的第二符合处理器;

其中来自上述第二符合处理器的输出还被提供给至少一个上述部件控制系统处理器，它根据上述两个符合处理器的输出驱动上述紧急反应系统的上述部件。

6. 权利要求 5 的系统，其中所述至少一个部件控制系统处理器包括多个各自控制一组预定的紧急反应装置的部件控制系统处理器。

7. 权利要求 1 系统，还包括用于在上述多个通道中的符合处理器之间传送来自上述双稳处理器的输出的通道间光纤网络。

8. 权利要求 1 系统，还包括经测试网络与上述双稳处理器、上述符合处理器和上述至少一个部件控制系统处理器相连的测试与界面处理器。

9. 权利要求 8 系统，其中上述测试与界面处理器能够测试上述系统或给上述至少一个部件控制系统处理器提供信号以驱动上述紧急反应系统的上述部件。

10. 权利要求 1 系统，还包括将各上述至少一个部件控制系统处理器与被上述电站保护系统保护的电站的主控制室相连的光纤网络。

11. 权利要求 10 系统，还包括与所述光纤网络相连向上述至少一个部件控制系统处理器提供信号以驱动上述紧急反应系统的上述部件的远程控制盘。

12. 一种实现接收来自监测电站运行参数的数字电站保护系统的信号的工程安全特征部件控制系统的方法，该方法包括:

提供多个监测上述电站运行的一个特定参数的冗余逻辑通道，

对各上述逻辑通道内的来自上述电站保护系统关于上述特定参数的输入实施冗余处理，

根据上述处理，对上述电站运行的上述特定参数是否在预定的安全限度之内作出两个独立的判定，

以多个控制器根据上述两个独立的判定和界面与测试处理器的输出控制电站运行和停机。

13. 权利要求 12 的方法，还包括将上述的两个判定分别与上述多个逻辑通道中的其它通道的类似判定进行比较。

14. 权利要求 13 的方法，还包括根据上述比较驱动上述紧急反应系统的部件。

15. 权利要求 14 的方法，其中所述对上述紧急反应系统的部件的驱动还包括提供多个各自控制一组预定的紧急反应装置的部件控制处理器。

16. 权利要求 15 的方法，还包括至少一个冗余部件控制处理器。

17. 权利要求 12 的方法，其中用第一和第二双稳处理器来实现上述的冗余处理，和用第一和第二符合处理器来实现上述的两个独立判定。

18. 权利要求 12 的方法，还包括用光纤网在多个逻辑通道之间相互连接以传送对上述电站运行的上述特定参数是否在预定的安全限度之内作出的上述判定。

19. 权利要求 12 的方法，还包括根据上述判定驱动紧急反应装置的部件。

20. 权利要求 19 的方法，还包括提供与对上述特定参数是否在上述安全限度以内作出的上述判断无关地驱动上述紧急反应装置的上述部件的冗余系统。

01.03.16

说　　明　　书

数字电站保护系统

本申请涉及在 1999 年 9 月 18 日提交的美国临时申请第 60/101,004 号并在其基础上声明优先权。

本申请涉及 1998 年 4 月 30 日提交的美国专利申请序列号 09/069,869，（代理人案卷第 ABB-164, C970270 号）和 1997 年 6 月 6 日提交的美国专利申请序列号 09/076,094，（代理人案卷第 ABB-165, C970330 号）中（共同未决）公开的主要内容，并且也是其部分继续申请。

本发明涉及核电站领域。更具体地，本发明涉及用来监测核电站运行并在电站运行超过已设定的参数的情况下启用紧急安全程序的改进的监测系统。更加具体地，本发明涉及用于数字电站保护系统(DPPS)的改进的工程安全特征(ESF)部件控制系统(CCS)。

为安全起见，核电站包括复杂的监测或“电站保护”系统。这些系统监测核反应堆和整个核电站运行。如果监测到反应堆的任何部分或电站的其它重要功能超过设定的安全参数，电站保护系统能启用紧急安全程序，如关闭反应堆，以防止出现麻烦。

另外，电站保护系统被设计成冗余和自生效的，以便在导致严重问题之前发现出现的任何故障。例如，可以对电站保护系统的一个特定监测功能提供两个或更多冗余系统。该冗余系统监测相同的参数或执行相同的计算。然后比较这些冗余系统的输出以确认所有系统运转正常。冗余系统间的不符表明存在潜在的问题。

许多现有的核电站已经运行了一段时间并使用了电站保护系统，这些保护系统比起现代技术已经是陈旧或过时了。例如，大多数现有的核电站采用的电站保护系统是固态保护系统(“SSPS”)，它使用分立的数字电子电路的庞大网络、机械开关和机电继电器。

这些继电器和开关含有电磁驱动的运动部件以实现电站保护系统的不同部件之间所需的连接。

在一个 SSPS 系统中，可以提供两个冗余逻辑通道以监测核电站运行的一个单独的参数。如果一个通道出故障了，另一个通道还保持着必要的监测功能。

考虑到这样的固态系统的许多部件的服务年限，可以预期当零件开始呈现与正常的产品寿命周期的终结阶段相联的问题时，故障率会增加。例如，工业可靠性模型预计该类型和批号的机电继电器由于触点的粘连和坑蚀或线包松脱造成问题的故障率的上升。

这些故障将明显威胁到电站保护系统的可靠性和被保护的核电站的安全。

另外，用来检查冗余监测系统之间的一致性的 SSPS 中的符合逻辑操作是由通常已经过时的常规电路板来施行的。例如，通常这些电路板使用摩托罗拉高门限逻辑(MHTL)电路。企业报告指出 MHTL 电路对能导致间歇的逻辑水平的老化故障是敏感的。这样，由于不必要的紧急停机的激活和其它紧急响应机制，老化和现有逻辑电路复杂度的增加就会导致系统可靠性下降、故障检修难度增加以及电站使用率下降。

因此，现有技术上存在改进电站保护系统的需要。更具体地，现有技术上存在改进电站保护系统使得应用现有技术可将得高可靠性扩展到整个寿命周期内。

引述的本申请的两个母申请分别公开了一个全数字逻辑电站保护系统(DPPS)和一个数字工程安全特征动作系统(DESFAS)，它们作为核电站中的电站保护系统(DPP)和一个工程安全特征(ESF)之间的界面起作用。这种核电站安全系统具有多个通道，各通道均具有双稳功能并带有局域符合测试系统。这些通道通过控制网，如 AF 100 网将主控制室、远程停机控制盘、界面与测试处理器（ITP 网）之间连接起来。然而希望在这种系统中通过与驱动时过载的 AF 100 网不同的 HSSL 驱动连接或 HSSL 驱动网增加驱动速度。

本发明的目标之一是达到上述需要和其它需要。特别地，本发明的目标之一是提供改进的根据电站保护系统提供的数据运行的紧急反应系统。更具体地，本发明的目标之一是提供改进的紧急反应系统使得提供高可靠性的现有技术在整个扩展的寿命周期内得以应用。再具体地，本发明的总体目标之一是通过与驱动时过载的 AF 100 网不同的 HSSL 驱动网增加驱动速度。

本发明的其它目标、优点和新特性将在接下来的描述中体现出来，或者被熟悉本技术的人通过阅读这些材料或实践本发明所了解。可以通过附带的权利要求所详述的方法获得这些目标和优点。

要获得这些已陈述的和其它的目标，可以以一个工程安全特征部件控制系统举例并描述本发明，该系统从正在监测电站运行参数的数字电站保护系统接收信号。该系统包括两个或更多，最好是四个监测电站特定运行参数的逻辑通道。各逻辑通道包括用来接收来自数字电站保护系统的关于该逻辑通道要监测的特定参数的输入信号并确定这个特定参数是否在预定的安全限度之内的双稳处理器。

各个双稳处理器与符合处理器相联以将该双稳处理器的输出与其它逻辑通道中的双稳处理器的输出相比较。一个或多个部件控制系统处理器接收各符合处理器的输出并根据该输出驱动紧急反应系统的部件。

在一个优选实施例中，四个逻辑通道都监测同一个电站运行参数。另外，使用了一系列部件控制系统处理器，各处理器控制预定的一组紧急反应装置。优选地，这些部件控制系统处理器中至少有一个是冗余的。

各逻辑通道优选地包括一个冗余的第二双稳处理器，它与该通道的另一个双稳处理器接收相同的输入并实施完全相同的功能。备有与第二双稳处理器相连第二符合处理器。第二符合处理器接收来自第二双稳处理器的输出并将该输出与来自其它逻辑通道的相应冗余双稳处理器的输出比较。第二符合处理器的输出也被提供给部件

控制系统处理器或控制器，其根据这两个符合处理器的输出驱动紧急反应系统的部件。

本发明的系统还优选地包括用来从各个逻辑通道的双稳处理器向其它逻辑通道的符合处理器传送输出信号的通道间光纤网。第二光纤网被用来连接各部件控制系统处理器和被电站保护系统所保护的电站的主控制室。优选光纤通讯是由于其抗电磁干扰(EMI)和其它形式干扰的能力。

本发明的系统还优选地包括测试与界面处理器，它经测试网与双稳处理器、符合处理器及部件控制系统处理器相连。测试与界面处理器能够测试系统或向一个或多个部件控制系统处理器提供信号来通过驱动网 HSSL 10 驱动紧急反应系统的部件以控制控制网 AF 100。

本发明的系统还可以包括连接在主控制室与部件控制系统处理器之间的光纤网络上的远程停机控制盘。如果主控制室变得不能入内，就能使用这样连接的远程停机控制盘向部件控制系统处理器发送信号以驱动紧急反应系统的部件。

本发明还包括使用工程安全特征部件控制系统的方法，该系统接收来自正在监测电站运行参数的数字电站保护系统的信号。该方法优选地包括下列步骤，提供两个或更多监测电站运行的一个特定参数的冗余逻辑通道，在各逻辑通道内对来自数字电站保护系统的关于该特定参数的输入施行冗余处理，并根据该处理对该电站运行参数是否在预定的安全限度内作出两个独立的判定。

附图作为说明书的一部分并对本发明进行了图示。该图与下面的描述一起说明并解释了本发明的原理。

该图是根据本发明的一个数字电站保护系统("DPPS")的工程安全部件控制系统("ESF-CCS")的框图。

现在将用该图来解释本发明的优选实施例。该图显示了一个单一逻辑通道，它与至少一个另外的同样的冗余通道一起监测核电站

运行的一个特定的参数并当发生被监测的参数变化超出已设定的安全限度的情况时启动紧急反应。

该图显示了在本发明的优选实施例中，驱动网 HSSL 16 具有第一通道，即四通道组中的通道 A。四个通道 A, B, C 和 D 是完全相同的，并监测同一个参数。为简单起见，图中仅显示出通道 A。一些信号和功能可以使用较少的通道。

如图所示通道 A 以一个双稳处理器 20 开始，它接收来自数字电站保护系统(DPPS)（未显示）的传感器的输入以监测核电站运行的一个特定参数。一个被监测参数的例子是反应堆温度。在这种情况下，双稳处理器 20 执行温度变化计算。然后双稳处理器 20 输出一个指示被监测参数是否在可接受的安全限度内的信号。

其它逻辑通道 B, C 和 D 监测同一个参数，最好处于核电站中的不同位置上。双稳处理器 20 的输出经光纤网络 70 提供给其它三个逻辑通道 B, C 和 D。通道 B, C 和 D 上的监测结果也经光纤网络 70 提供给逻辑通道 A。

在核电站保护系统的应用中优选如图所示的 70 和(下面描述的 38)那样的光纤网络，是由于它们对如电磁干扰(EMI)这样的环境因素的抵抗能力。光纤网络也能抵抗其它形式的干扰、交叉通话、信号漏损和类似的情况。

双稳处理器 20 的输出还被提供给局域符合逻辑处理器 24。优选地，双稳处理器 20 和符合逻辑处理器 24 之间的连接包括冗余 HSSL 数据连接。

符合逻辑处理器 24 会检查了解双稳处理器 20 对被监测的参数是否在已设定的安全范围之内的判定是否与其它逻辑通道 B, C 和 D 的双稳处理器所作的判定一致。符合检查的结果被输出给连线 28。

如图所示，连线 28 连接符合逻辑处理器 24 和一系列部件控制系统("CCS")控制器或处理器 32a 到 32e，它们一起作为以标记 16 表示的控制网 AF 100 的一部分起作用。这些控制器 32 根据符合逻辑处理器 24 的输出在适当的时候驱动紧急反应系统。例如各 CCS

控制器 32a 到 32e 操纵开关齿轮和马达控制中心以控制构成电站的紧急反应系统的真空泵、风扇、缓冲装置、阀门、螺线管以及马达操纵的阀门。这些被 CCS 控制器 32a 到 32e 驱动的部件优选地被分成几组并被分配到不同的机柜以增加对单个故障的抵抗力。

一般地，CCS 控制器 32a 到 32e 各自控制十六个紧急反应系统的部件并提供与相关系统相联的模拟输入。某些 CCS 控制器 32a 到 32e 优选地是冗余的，具有控制单个介入继电器的冗余输出，这增强了系统的可靠性。

通过界面处理器 14 可以与符合处理器 24 配合实现紧急反应系统的外部重置。然后重置信号经连线 28 发送给 CCS 控制器 32。

在连线 28 上的符合处理器 24 的输出还被提供给通讯界面 34，它转而经光纤网络 38 与电站的主控制室 10 相连，因此能向在主控制室里的电站操作者显示或指出通道 A 上的监测结果的一致性。

除了从 A 到 D 四个逻辑通道的提供的冗余，在本实施例的原则下，各通道内部也是冗余的。特别地，提供一个与第一双稳处理器 20 完全相同的第二双稳处理器 22 来重复第一双稳处理器 20 的工作。冗余双稳处理器 22 的输出被提供给第二个逻辑符合处理器 26，同样经 HSSL 光纤网络 70 被传送给其它三个逻辑通道 B, C 和 D。

冗余符合处理器 26 也经光纤网络 70 接收来自各其它逻辑通道 B, C 和 D 中的相应的冗余双稳处理器的输出信号。然后冗余符合处理器 26 将冗余双稳处理器 22 的输出与来自通道 B, C 和 D 的信号相比较。这个比较的结果被输出给 CCS 控制器系列 32a 到 32e。

然后 CCS 控制器 32a 到 32e 将激活需要的紧急反应设备。作为预防措施，只有当两个逻辑符合处理器 24 和 26 都指出两个双稳处理器 20 和 22 都探测到危险条件，并被其它三个逻辑通道 B, C 和 D 中的相应的双稳处理器确认时，控制器 32 才激活一个紧急反应。

连线 30 也将冗余符合处理器 26 的输出连接到通讯界面 36，该界面通过连线 40 连接到通讯界面 34，并最终连接到主控制室 10。举例说明，通讯界面 34 和 36 可以是 AC 160 单元。连线 40 还包括

到 2E 界面布置 44 的光纤连接，它继而又连接到布置 C 的通讯界面。

一系列 CCS 控制器 32a 到 32e 还通过光纤网络 38 连接到主控制室 10 和一个远程停机盘 12。提供了这个连接以便能够从主控制室 10 或在不能进入主控制室 10 的情况下从远程停机盘 12 手动激活由 CCS 控制器 32a 到 32e 控制的紧急反应功能。

可选地，测试处理器 14 的光缆网络 71 可以被配套使用以提供另一个通过 CCS 控制器 32a 到 32e 驱动紧急反应措施的系统。最后，各 CCS 控制器 32a 到 32e 可以在处理器本身上装有用来初始化紧急反应措施的手动工具（未显示）。

如图所示，主控制室 10 可以包括一对用来处理由逻辑通道 A 到 D 向主控制室提供和从主控制室输出的信号的 MCR MMI 复用器 72、73。远程停机盘 12 包括布置 A 软控制器 74 和工作站，优选地为 AS 500 工作站 75。

最后，备有将各个逻辑通道的部件连接到界面与测试处理器 14 的测试总线 71。例如两个双稳处理器 20 和 22 和 CCS 控制器 32a 到 32e 通过总线 71 连接到测试处理器 14。测试处理器 14 也通过总线 71 连接到通讯界面 36。以这种方式，测试处理器可以被用来测试它所连接的逻辑通道的各个部件。

ESF-CCS 柜中提供的维护与测试盘（未显示）和界面与测试处理器 14 一起可以提供与主控制室 10 中的平板显示器相同的控制和测试显示能力。维护与测试盘还能提供测试结果并允许系统的手动测试。

本发明提供了下列好处和优点。首先，向双稳处理器提供传感输入的时刻和 CCS 处理器发出用来初始化用于紧急反应的断路电路的信号的时刻之间的反应时间少于或等于 300 毫秒。信号的复用和数据通讯网络化将成本减至最小，并使得分阶段安装（phased installation）更加简单。控制和监测功能的分离避免了数据通讯的瓶颈，保持了简单的控制系统设计并减少了操作失误的可能性。

通过改进设计提高了系统的可用性。可以使用自动测试功能。系统可以灵活地扩展和升级以适应新需要。比起传统的电站保护系统，本发明的系统需要较少的备件和较少的训练。

在本发明的系统中还有许多冗余系统。有让来自过程传感器的各参数通过的四个独立的通道，它们包括使紧急反应装置断路的初始电路。在各通道内，通讯是冗余的和可转换路径的。为了转换路径，自动和手动激活是经由不同的信号路径完成。

各 ESF-CCS 布置控制一个 ESF 布置且有四个冗余的 ESF-CCS 布置用来操纵四个（或更少）全冗余的 ESF 布置。在存在电站系统水平冗余之处，对冗余 ESF-CCS 布置进行部件安排以保持设计的冗余水平。

将部件分为由分离的 CCS 控制器 32 控制的分离的组也能获得功能的更换，各控制器从具有局域符合处理器和界面与测试处理器的电路中获得输入。用分组来使系统运行部件故障的影响减至最少。分组消除了单个大处理器的多个控制监测功能，并将它们分散成许多较小的处理器，它们限制了处理器故障的影响。

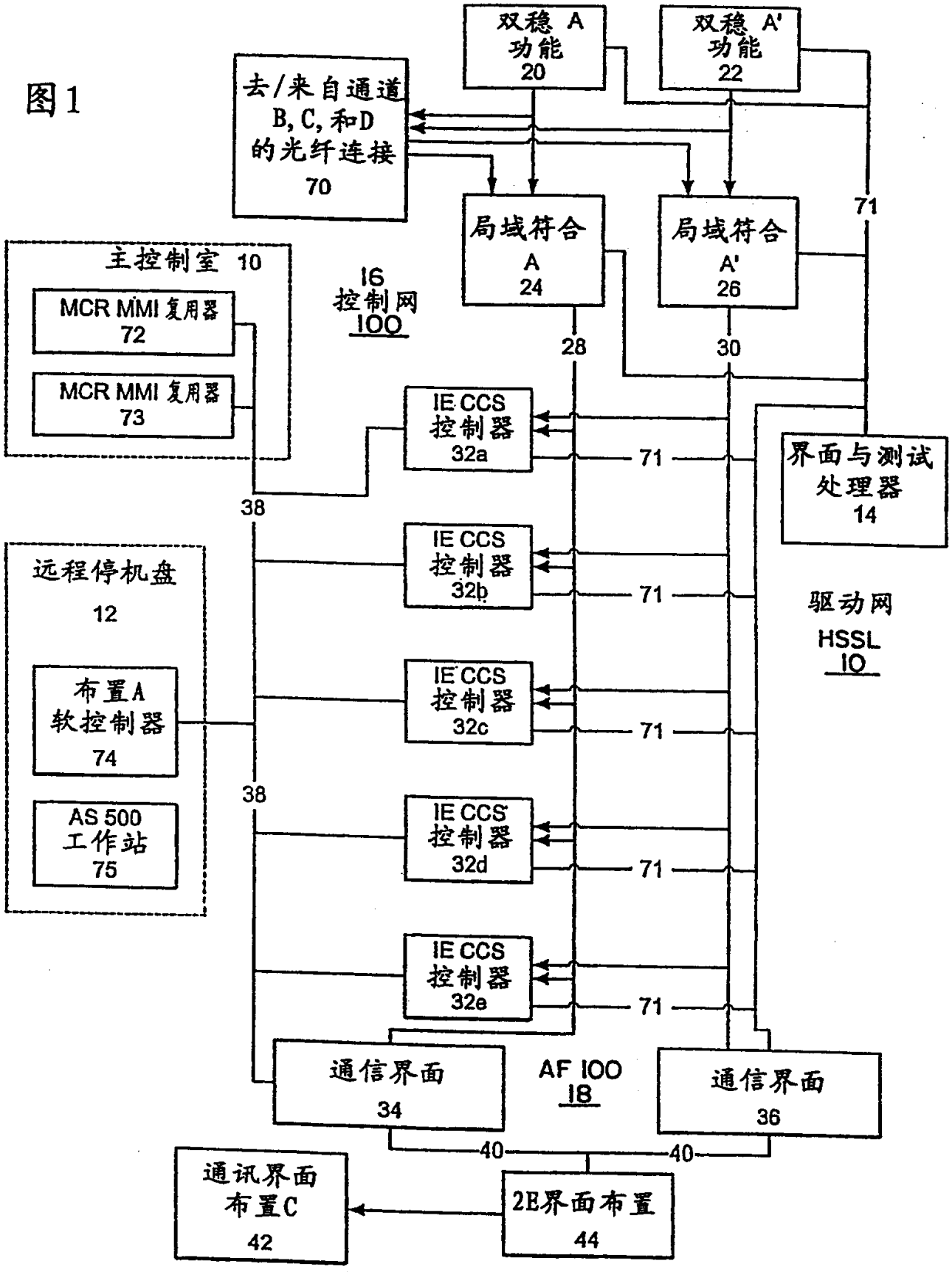
还有多种驱动。主要的断路路径是驱动数据连线 28。从主控制室 10 的手动备用断路则经由通讯网络 38。备用手动断路路径是测试网络 71。

前面的描述仅仅是为了说明和描述本发明，并不打算穷尽本发明或局限本发明于任何公开的实现形式。在上面说明的知识范围内还可能有许多修改和变化。

为了最好地解释本发明的原则和它的实际应用而选择和描述了优选实施例。前面的描述致力于允许其他熟悉本技术的人在各种实施例中最好地利用本发明并有各种适合于经周密考虑的应用的修改。这里打算用下列权利要求定义本发明的范围。

说 明 书 附 图

图1


双稳 A
功能
20
双稳 A'
功能
22
去/来自通道
B, C, 和D
的光纤连接
70
71
局域符合
A
24
局域符合
A'
26
主控制室 10
MCR MMI 复用器
72
MCR MMI 复用器
73
16
控制网
100
28
30
IE CCS
控制器
32a
71
界面与测试
处理器
14
38
IE CCS
控制器
32b
71
远程停机盘
12
驱动网
HSSL
10
布置A
软控制器
74
IE CCS
控制器
32c
71
AS 500
工作站
75
38
IE CCS
控制器
32d
71
IE CCS
控制器
32e
71
通信界面
34
AF 100
18
通信界面
36
40
40
通讯界面
布置C
42
2E界面布置
44