

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 17/60

G06F 17/00 G06F 19/00

[12] 发明专利申请公开说明书

[21] 申请号 99815371.0

[43] 公开日 2002 年 1 月 23 日

[11] 公开号 CN 1332880A

[22] 申请日 1999.8.5 [21] 申请号 99815371.0

[30] 优先权

[32] 1998.11.25 [33] US [31] 09/199,429

[86] 国际申请 PCT/SG99/00066 1999.8.5

[87] 国际公布 WO00/31669 英 2000.6.2

[85] 进入国家阶段日期 2001.7.2

[71] 申请人 ADC 技术国际有限公司

地址 新加坡新加坡

[72] 发明人 林恩诘 沈成宗 林建业 沈荣发

[74] 专利代理机构 柳沈知识产权律师事务所

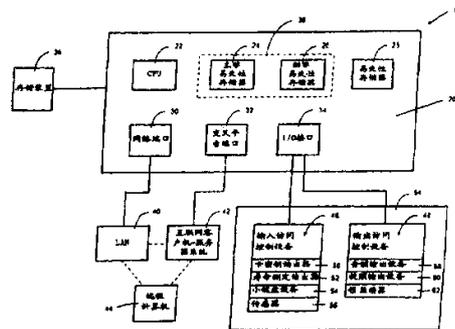
代理人 邵亚丽

权利要求书 4 页 说明书 16 页 附图页数 3 页

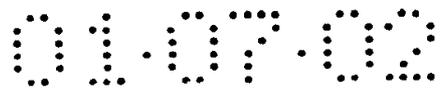
[54] 发明名称 提供交叉平台远程控制和监测设备访问控制器的系统和方法

[57] 摘要

一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法,包括一个 CPU、一个非易失性存储器、网络端口和交叉平台端口中的至少一个、以及一个输入/输出接口。该系统包括一个与接口可操作地链接的输入访问控制设备。该系统还包括一个交叉平台网络和一个通过交叉平台网络与设备访问控制器可操作地链接的远程计算机,由此,交叉平台网络能够不考虑远程计算机的操作系统与设备访问控制器的操作系统之间的兼容性而对设备电子访问控制器进行远程操作。



ISSN 1008-4274



权 利 要 求 书

1. 一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统，该系统包括：

- 5 一个设备电子访问控制器，包括：
- 一个 CPU；
 - 一个非易失性存储器；
 - 网络端口和交叉平台端口中的至少一个；
 - 一个输入/输出接口；
- 10 一个与所述接口可操作地链接的输入访问控制设备，该输入访问控制设备生成用户的识别数据；
- 一个与所述接口可操作地链接的输出访问控制设备；
 - 一个交叉平台网络；和
 - 一个通过所述交叉平台网络与所述设备访问控制器可操作地链接的远程
- 15 计算机，由此，所述交叉平台网络能够不考虑所述远程计算机的操作系统与
所述设备访问控制器的操作系统之间的兼容性而对所述设备电子访问控制器
进行远程操作。

2. 如权利要求 1 所述的系统，其中，所述交叉平台网络包括一个互联网客户机-服务器系统。

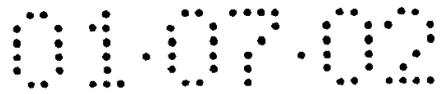
20 3. 如权利要求 1 所述的系统，其中，所述交叉平台网络包括一个局域网。

4. 如权利要求 1 所述的系统，其中，所述 CPU 生成可用于互联网客户机-服务器系统的、由统一资源定位器(URL)识别的信息页数据。

25 5. 如权利要求 1 所述的系统，其中，所述 CPU 至少将所述识别数据、
时间数据和地点数据中的至少一个格式化或使用简单邮件传输协议的电子邮件消息。

6. 如权利要求 1 所述的系统，其中，所述 CPU 运行第一操作系统软件并且所述远程计算机运行第二操作系统软件，所述第一操作系统软件与所述第二操作系统软件不同。

30 7. 如权利要求 1 所述的系统，其中，所述 CPU 运行一个控制器操作系统软件，所述控制器操作系统软件包括一访问控制系统程序模块、一 TCP/IP



程序模块和一互联网服务器程序模块。

8. 如权利要求 1 所述的系统, 其中, 所述 CPU 运行一个控制器操作系统软件, 所述控制器操作系统软件包括一访问控制器系统程序模块、一 TCP/IP 程序模块和一邮件客户机程序模块。

5 9. 如权利要求 1 所述的系统, 其中, 所述输入访问控制设备包括卡密钥读出器、寿命测定读出器和小键盘装置中的至少一个。

10. 如权利要求 1 所述的系统, 其中, 所述输入访问控制设备包括一个传感器。

11. 如权利要求 1 所述的系统, 其中, 所述输出访问控制设备包括音频输出装置、视频输出装置和锁致动器中的至少一个。

12. 一种用于提供交叉平台远程控制和监测设备电子访问控制器的方法, 该方法包括如下步骤:

用所述设备电子访问控制器监控一输入访问控制设备;

15 用所述设备电子访问控制器接收来自输入访问控制设备的第一识别数据;

将储存在所述设备输入访问控制器中的第二识别数据与所述第一识别数据比较;

如果所述第一识别数据与所述第二识别数据相匹配, 则启动所述设备电子访问控制器的输出访问控制设备;

20 响应于所述第一识别数据, 用所述设备访问控制器生成时间数据和地点数据中的至少一个; 并且

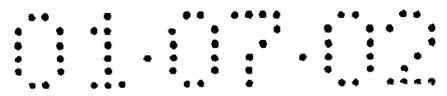
用所述设备电子访问控制器通过交叉平台网络向远程计算机传送所述第一识别数据, 以及所述时间数据和所述地点数据中的至少一个。

25 13. 如权利要求 12 所述的方法, 还包括步骤: 在所述设备电子访问控制器中的非易失性存储器中储存所述第一识别数据, 以及所述时间数据和所述地点数据中的至少一个。

14. 如权利要求 12 所述的方法, 还包括如下步骤:

30 利用经过一交叉平台网络与设备电子访问控制器可操作地链接的远程计算机, 访问来自该控制器的所述第一识别数据、所述第二识别数据、所述时间数据和所述地点数据中的至少一个; 并且

用远程计算机改变所述第一识别数据、所述第二识别数据、所述时间数



据、所述地点数据以及设备电子访问控制器的运行参数中的至少一个。

15. 如权利要求 14 所述的方法，其中，所述的访问和改变设备电子访问控制器的数据的步骤中包括使远程计算机可操作地链接到一互联网客户机-服务器系统。

5 16. 如权利要求 12 所述的方法，还包括如下步骤：

在经过交叉平台网络与所述设备电子访问控制器可操作链接远程计算机的图像设备上，显示对应于所述第一识别数据、所述第二识别数据、所述时间数据、所述地点数据以及设备电子访问控制器的运行参数中的至少一个的图形数据和文本数据中的至少一个；并且

10 用远程计算机改变所述第一识别数据、所述第二识别数据、所述时间数据、所述地点数据以及设备电子访问控制器的运行参数中的至少一个。

17. 如权利要求 12 所述的方法，还包括如下步骤：

将所述第一识别数据、所述第二识别数据、所述时间数据、所述地点数据格式化使用简单邮件传输协议的电子邮件消息。

15 18. 如权利要求 12 所述的方法，还包括如下步骤：

生成可用于互联网客户机-服务器系统的、由统一资源定位器(URL)识别的信息页。

19. 如权利要求 12 所述的方法，还包括如下步骤：

用第一操作系统操纵设备电子访问控制器；并且

20 用第二操作系统操纵远程计算机，所述第二操作系统与所述第一操作系统不同。

20. 如权利要求 12 所述的方法，其中，接收所述第一识别数据的步骤还包括读出靠近读出器放置的卡密钥的步骤。

25 21. 如权利要求 12 所述的方法，其中，启动输出控制设备的步骤包括步骤：启动锁致动器并且开启所述锁从而允许进出限制区域。

22. 一种用于提供交叉平台远程控制和监测设备电子访问控制器的计算机程序产品，该计算机程序产品包括下列各项：

30 一个计算机可用媒介，具有在其中记载的计算机可读码，所述计算机可读码包括控制器操作系统计算机可读程序码设备，所述控制器操作系统计算机程序码设备还包括：

一个监测设备的输出和输入访问控制数据的访问控制系统计算机可读程

序码模块；

一个 TCP/IP 计算机可读程序码模块；以及

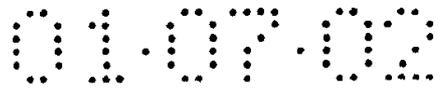
- 5 互联网服务器计算机可读程序码模块和邮件客户机计算机可读程序码模块中的至少一个，由此，所述控制器操作系统计算机可读程序码设备能够不考虑远程计算机的操作系统和所述设备访问控制器的所述控制器操作系统计算机可读码设备之间的兼容性而对设备电子访问控制器的进行远程操作。

23. 如权利要求 22 所述的计算机程序产品，其中，所述控制器操作系统计算机可读码设备包括与所述互联网服务器计算机可读程序码可操作地链接的数据库程序模块。

- 10 24. 如权利要求 22 所述的计算机程序产品，其中，所述控制器操作系统计算机可读程序码设备包括与所述访问控制系统计算机可读程序码模块可操作地链接的卡密钥数据库程序模块。

25. 如权利要求 22 所述的计算机程序产品，其中，所述控制器操作系统计算机可读程序码设备包括 CGI 计算机可读程序码模块。

- 15 26. 如权利要求 22 所述的计算机程序产品，其中，所述访问控制系统计算机可读程序码模块包括多个子模块，所述子模块控制输入访问控制设备和输出访问控制设备中的至少一个。



说明书

提供交叉平台远程控制和监测
设备访问控制器的系统和方法

5

发明背景

发明领域

本发明涉及一种用于提供交叉平台(cross-platform)远程控制和监测设备访问控制器(facility access controller)的系统和方法。对设备访问控制器的监测包括检测状态或监测与设备可操作地链接的报警器。该系统和方法使用与万维网(world wide web)可操作地链接的设备电子访问控制器。该系统和方法能够在具有不同操作系统的设备电子访问控制器之间进行数据传输。该系统和方法还允许使用 web 浏览器的远程站点访问设备电子访问控制器的 web 服务器，从而对设备电子访问控制器进行监测和控制。

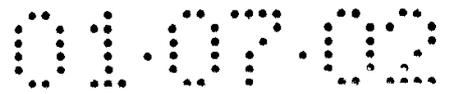
15

背景技术描述

被用于控制和监测人员进出(access)建筑物、房间和限制区域的设备电子访问控制器一般使用某种形式的识别装置来在一个人通过受控或受限制区域之前先验证这个人的身份。这种识别装置一般包括使用特定的编码来识别用户的编码卡或其它类型的承载数据的记录设施。许多设备电子访问控制器被设计成具有内置的能够以数字形式储存唯一识别码的电子处理智能装置，并且能够确定谁可以或不允许进出被控或被限制区域。

这种设备电子访问控制器(facility electronic access controller, FEAC)可以连接到安装有一套特殊应用程序的一台或多台中央计算机。FEAC 和中央计算机通过通信接口链接并且通过预定的特殊协议进行通信/相互作用。一般情况下，在每台中央计算机上安装一套程序，并且将这些程序设计成用特殊的操作系统平台来监控来自 FEAC 的上载处理，也允许将数据下载到 FEAC。通常，一台中央计算机将控制一座建筑物中的若干个 FEAC。

FEAC 一般用于监控一座建筑物、建筑物中的一部分、房间或限制区域中的侵入警报。当警报器被启动时，FEAC 将在建筑物中产生可听到和可见到的显示。监管该设备的警卫将采取适当的行动，对这些显示做出反应。如



果设备或建筑物没有警卫看管，报警信号将被自动地传送到中央计算机。报警信号还可以通过适当的接口被传送到第三方的中央报警监控站。

5 利用常规技术，在多个建筑物中的每台可以被相互互联网的中央计算机中安装应用程序是非常困难的，其中这些联网的计算机以使用户可以通过它们进行一种或多种功能的操作。常常是不同建筑物中的中央计算机具有不同的或不兼容的操作系统。在一个或多个建筑物中具有多台相互互联网的中央计算机的情况下，其中如果一台中央计算机改变其应用程序或操作系统，则要求各台中央计算机逐台做出改变，因而使整个中央计算机网络做出改变。此外，由于各台中央计算机的操作系统版本不同，常规技术不允许在支持不同语言的中央计算机的软件之间相互操作。

10 因此，本领域需要一种用于提供交叉平台远程控制和监测具有不同操作系统的设备电子访问控制器的系统和方法。本领域还需要这样一种用于提供交叉平台远程控制和监测设备电子访问控制器(FEAC)的系统和方法，它们允许单个或多个改变设备的至少一个进出码以及在设备电子访问控制器的中央计算机各自的操作系统中被同时执行的操作参数。

本发明的概述

20 因此，本发明的一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法。本发明的另一个目的是提供一种用于改变设备访问的数据并且对设备电子访问控制器中的可能具有或不具有相似操作系统的多台中央计算机进行控制的系统和方法。

本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备访问控制器的系统和方法，其中，设备电子访问控制器中的每个中央计算机包含 web 服务器。

25 本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，设备电子访问控制器中的每个中央计算机可以通过使用传输控制协议/互联网协议(TCP/IP)和超文本传输协议(HTTP)的工业协议与客户机通信。

30 本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，设备电子访问控制器的客户机可以使用任何类型的 web 服务器程序访问 FEAC，同时，FEAC 的远程计算机或远

程中央计算机能够从和在 web 服务器和/或 FEAC 中监控交易处理行为。这里使用的客户机被定义为一个计算机系统或处理过程，它需要例如服务器的其它计算机系统或处理的服务。服务器是一个对其它(客户机)程序提供某种服务的程序。通常在网络之上，客户机和服务器之间的联接一般是借助于消息传递并且使用某种协议对客户机的请求和服务器的响应进行编码。服务器可以连续运行(象端口监督程序(daemon)那样)，等待请求到达，或者被某个控制许多特定服务器(在 Unix 上的“inet-ed”)的上级端口监督程序调用。在互联网(Internet)上联接有很多服务器，如用于网络文件系统、网络信息服务(NIS)、域名系统(DNS)、文件传输协议(FTP)、新闻、指针(finger)和网络时间协议的服务器。

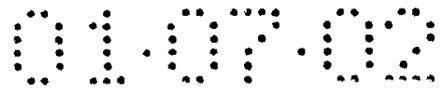
本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备访问控制器的系统和方法，其中，虽然 FEAC 的不同中央计算机使用不同操作系统，但是它们联接在同一个网络上(既可以是局域网也可以是广域网)与 FEAC 的不同中央计算机通信。

本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，设备电子访问控制器的 web 服务器被设计成使用支持不同语言的超文本标记语言(HTML)标准。

本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，FEAC 的中央计算机按照简单邮件传输协议(SMTP)客户机运行，允许 FEAC 的中央计算机通过互联网电子邮件协议向远程用户发送数据、登录、正常的活动交易处理或安全破坏数据(security breach data)等等。利用这样的系统和方法，基于程序控制的 FEAC 计算机可以传输特定的或被选择的信息。此外，利用这样的系统和方法，通过互联网电子邮件系统可以将特定的或被选择的访问信息或数据发送到在多个地点的多个用户。

本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备访问控制器的系统和方法，其中，FEAC 中使用不同操作系统的中央计算机可以利用标准的电子邮件软件检索/存取信息或数据。

本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，每个 FEAC 的每台中央计算机基本上不用安装相同的识别软件。换句话说，本发明的另一个目的是提供一种用于



提供交叉平台远程控制 and 监测设备电子访问控制器的系统和方法，其中，每个 FEAC 的中央计算机可以使用与相邻的 FEAC 的相邻中央计算机不同的操作系统，并且由远程计算机利用 web 浏览器程序来实现控制。

5 本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备
侵扰报警监管功能的系统和方法，由此，象 web 客户机那样运行的一台或多
台远程计算机能够通过互联网监控用于检测设备或建筑物进入条件
(penetration condition)的警报器。

10 本发明的另一个目的是提供一种用于提供交叉平台远程控制和监测设备
电子访问控制器的系统和方法，其中，实时地给 FEAC 的远程计算机或中央
计算机提供监控限制区域的访问数据。这种限制区域的访问数据包括(但不
限于)实时显示持卡人的识别编码、寿命测定(biometric)扫描的结果、设备名、
位置说明、系统数据库和 FEAC。其它访问数据包括在网页上显示图形图像
和动态的状态信息，以及用 FEAC 的远程计算机或中央计算机的 web 浏览
器检索这些信息。

15 本发明的这些和其它目的通过提供用于提供交叉平台远程控制和监测设
备电子访问控制器的方法来实现，该方法包括如下步骤：用设备电子访问控
制器监控输入访问控制设备；用设备电子访问控制器接收来自输入访问控制
设备的第一识别数据；将储存在设备输入访问控制器中的第二识别数据与第
一识别数据进行比较；如果第一识别数据与第二识别数据相符，启动设备电
20 子访问控制器的输出访问控制设备；由设备访问控制器生成响应第一识别数
据的时间数据和地点数据中的至少一个；通过交叉平台网络由设备电子访问
控制器向远程计算机传输第一识别数据以及时间数据和地点数据中的至少一
个。

25 此外，本发明的这些和其它目的通过用于提供交叉平台远程控制和监测
设备电子访问控制器的系统来实现，该系统包括：设备电子访问控制器，
包括一个 CPU、一个非易失性存储器、网络端口和交叉平台端口中的至
少一个、一个输入/输出接口、一个与接口可操作地链接的输入访问控制设
备、以及一个与接口可操作地链接的输出访问控制设备，其中所述输入访问
30 控制设备生成用户的识别数据；一个交叉平台网络；一台通过交叉平台网络
与设备访问控制器可操作地链接的远程计算机，由此，不论远程计算机的操
作系统与设备访问控制器的操作系统是否兼容，交叉平台都可以远程操纵设

备电子访问控制器。

此外，本发明的这些和其它目的通过一个用于提供交叉平台远程控制和监测设备电子访问控制器的计算机程序产品来实现，该计算机程序产品由下列各项组成：一个具有在其中记载了计算机可读码的计算机可用媒介，该计算机可读码包含一个控制器操作系统计算机可读程序码设备，该控制器操作系统计算机可读程序码设备还包含：一个监控设备的输入和输出访问控制数据的访问控制系统计算机可读程序码模块；一个 TCP/IP 计算机可读程序码模块；至少一个互联网服务器计算机可读程序码模块以及一个邮件客户机计算机可读程序模块。由此，不论远程计算机的操作系统与设备访问控制器的控制器操作系统计算机可读码设备是否兼容，控制器操作系统计算机可读程序码设备都可以远程操纵设备电子访问控制器。

通过在下文中给出的详细描述，本发明更多的适用范围将变得更加清楚。但是，本领域技术人员应当明白，尽管这些详细描述体现了本发明的优选实施例，但这些详细描述仅仅是本发明的举例描述，因为对于本领域技术人员来讲，可以根据这些详细描述在本发明的精神和范围之内对其进行修改和变化。

附图的简要说明

从下文给出的详细描述和仅为了说明而给出的附图中，可以对本发明有更全面的理解，同时，它们并不限制本发明，其中：

图 1 示出了用于提供交叉平台远程控制和监测设备电子访问控制器的系统的框图；

图 2 示出了支持用于提供交叉平台远程控制和监测设备电子访问控制器的系统的软件模块框图；并且

图 3 示出了与交叉平台接口可操作地链接的多个设备电子访问控制器系统。

优选实施例的详细描述

详细参照各个附图，尤其是图 1，示出了用于提供交叉平台远程控制和监测设备电子访问控制器 20 的系统 10。设备电子访问控制器(FEAC)最好包括一个与主非易失性存储器 24 和副非易失性存储器 26 可操作地链接的中央

处理单元 22。与 CPU 22 可操作地链接的还有易失性存储器 28、网络端口 30、交叉平台端口 32 以及输入/输出(I/O)接口 34。CPU 22 还与存储装置 36 可操作地链接。

5 主非易失性存储器 24 最好至少是可擦除的可编程只读存储器 (EPROM)、电可擦除只读存储器(EEPROM)和快闪型存储器(flash type memory)之一。该主非易失性存储器被设计成储存用于设备电子访问控制器 20 的操作系统(OS)和应用码。

10 副非易失性存储器 26 最好至少是电可擦除可编程只读存储器(EEPROM)和快闪型存储器之一。副非易失性存储器 26 被设计成用于储存网页。注意, 如果使用电可擦除非易失性存储器, 则如标号 38 所示, 副非易失性存储器 26 和主非易失性存储器 24 可以使用同一个存储器芯片。易失性存储器 28 最好是随机存取存储器(RAM)。易失性存储器 28 是 CPU 22 所使用的用于其大多数操作的存储器, 这些操作包括跟踪来自 I/O 接口 34 的数据以及为 FEAC 20 提供基本的系统工作区。

15 网络端口 30 最好是 Ethernet™(以太)(已被标准化的用于局域网的访问方法)网络端口, 它至少用非屏蔽双绞线(UTP)或同轴电缆之一连接到局域网(LAN)40。UTP 一般包括象利用电缆的 Ethernet™(已被标准化的用于局域网的访问方法)那样, 用于计算机到计算机通信所使用的线路。以太网定义为同轴电缆局域网, 其中, 利用载波检测多址/冲突引导(carrier sense multiple
20 access/collision direct, CSMA/CD)算法将数据分解到(broke into)数据包, 直到数据包在不与任何其它数据包发生冲突的情况下到达目的地为止。用于局域网的同轴电缆通常是具有多重屏蔽的 50 欧姆同轴电缆。

25 交叉平台端口 32 最好是通用异步接收机/发送机(universal asynchronous receiver/transmitter, UART)串行端口。UART 是一个用于串行通信的集成电路, 它包含发送机(由并行到串行的变换器)和接收机(由串行到并行的变换器), 其中发送机和接收机被分别计时。交叉平台端口 32 和网络端口 30 不限于 Ethernet™(已被标准化的用于局域网的访问方法)网络端口和 UART 串行端口。被支持的其它接口类型包括(但并不限于)光纤、无线局域网、并行端口和 ATM(异步传输模式, 它是一种使用被称为单元的固定大小
30 的数据包动态分配带宽的方法)。

网络端口 30 和交叉平台端口被设计成支持传输控制协议/互联网协议

(transmission control protocol over internet protocol, TCP/IP)。TCP 和 IP 是在特定的层次上指定的两个协议，TCP/IP 经常用于查阅基于这些协议的全部 ISO 协议，包括 Telnet、FTP、UDP、RDP、HTTP、SMTP 和 POP3。

5 具体来说，网络端口 30 和交叉平台端口 32 被设计成与在线服务(没有示出)可操作地链接，该在线服务允许对互联网客户机-服务器的分布式信息检索系统或万维网(world wide web, WWW) 42 进行访问。如图 1 所示，FEAC 20 通过交叉平台端口 32 并经过在线服务(服务器没有示出)与互联网客户机服务系统 42 可操作地链接，或者通过网络端口 30 并经过 LAN 40 与互联网客户机服务系统 42 可操作地链接。

10 FEAC 20 与互联网客户机服务器系统 42 可操作地链接，FEAC 20 可以由一个远程控制器或终端 44 远程监测和控制，该远程控制器或终端 44(经过没有示出的在线服务或服务器)与 LAN 40 或互联网客户机服务系统 42 中的至少一个可操作地链接。只要远程计算机 44 与 LAN 40 或互联网客户机服务器系统 42 可操作地链接，远程计算机 44 就可以从任何地理位置监测或控制 FEAC 20。本发明最好被设计成这样，远程计算机 44 通过使用 JAVA™(面向对象的编程语言)和超文本标记语言(HTML)之类语言的 web 浏览器与 FEAC 20 相互作用。但是，本发明不限于这些类型的语言，还可以包括通过互联网或万维网允许交叉平台运行的其它语言。其它语言包括(但并不限于)JAVA 脚本、JAVA BEANS、可扩展的标记语言(XML)、标准化通用标记语言(SGML)、包括 JAVA APPLETs 的 HTML 程序、虚拟现实模型语言(VRML)和其它类似的面向对象编程语言。

25 本发明设计成用于面向对象的语言，允许允许从任何平台远程控制和监测 FEAC。面向对象的语言定义为一种将有关函数和数据分组为可以重复使用的程序块(chunk)的软件开发方法。当处理得当时，面向对象的语言可以减少新项目的开发时间或者减少在 FEAC 中运行的程序的变化。

30 输入/输出(I/O)接口与输入访问设备 46 和输出访问控制设备 48 可操作地链接。优选的输入访问控制设备是卡密钥读出器 50。根据在 FEAC 20 中使用的卡密钥的类型，卡密钥读出器 50 可以采用多种硬件结构。能够访问由 FEAC 20 控制的设备的卡密钥的类型包括(但并不限于)磁条卡、条形码卡、集成电路(IC)电路卡(智能卡)、射频(RF)卡、寿命测定卡、红外线型扫描卡和其它的数据承载设施。本发明不限于仅使用上述各种类型卡之中的一

种类型的卡密钥，还可以包括它们的任意组合。例如，在由卡密钥读出器 50 扫描的卡上出现的卡密钥不但可以使用磁条而且可以使用寿命测定识别指示器。

5 本发明不限于卡密钥型输入访问控制设备 46。其它类型的输入访问控制设备 46 包括(但并不限于)寿命测定读出器(如视网膜扫描、皮肤纹、DNA 扫描、声音识别、重量以及它们的组合等等)、小键盘(keypad)设备 54(它包括用于输入预定码集合的小键盘)和其它的要求用户在被允许进入一个设备之前验证用户身份的读出设备。输入访问控制设备还可以包括检测用户的实际位置和/或者打开和关闭设备进出通道的传感器 56。常用的传感器包括(但并不限于)红外线传感器和其它热传感器、重量传感器、磁性读出开关以及
10 摄像机(比如可以与互联网客户机服务器系统 42 可操作地链接的数字摄像机); 麦克风以及其它检测活生物体存在的传感设备。输入访问控制设备 46 还可以包括配备数字摄像机的计算机，这样视频和音频识别可以由 FEAC 20 认可。

15 输出访问控制设备最好包括(但并不限于)音频输出设备 58 和视频输出设备 60。优选的音频输出设备 58 包括(但并不限于)扬声器、警报器以及其它的活生物体能够听到的报警器类型。视频输出设备 60 包括(但并不限于)闪光灯、彩色灯、视频监视器以及其它的能够被活生物体如人看到的视频输出设备。

20 输出访问控制设备 48 最好包括(但并不限于)允许进出限制区域的锁致动器(actuator)62。常用的锁致动器包括(但并不限于)磁性锁、电致动死门(deadbolts)、液压致动锁、气压致动锁以及其它可以打开通往被封闭的空间或被限制的区域的门或窗户的锁致动器。

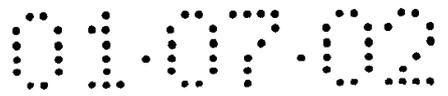
25 输入和输出访问控制设备 46 和 48 可以使用单个设备或单元而不必包括多个设备。换句话说，输入访问控制设备 46 可以仅是一个不使用传感器 56 的卡密钥读出器 50。此外，输出访问控制设备 48 可以仅包括一个不具有音频输出设备 58 或视频输出设备 60 的锁致动器。输入访问控制设备 46 和输出访问控制设备 48 形成了 FEAC 20 的一个子系统 64，它与 FEAC 20 的 I/O 接口 34 可操作地链接。本发明不限于一个 FEAC 子系统 64，而是可以包括
30 控制进出多个限制区域的各个部分的多个子系统 64。最好，FEAC 子系统 64 将提供对于被一个单独 FEAC 20 监控的建筑物中各个房间的访问。

存储装置 36 最好是 FEAC 20 的主非易失性存储器 24 和副非易失性存储器 26 的备份非易失性存储器。存储装置 36 最好是磁带或磁盘存储器装置，它将主非易失性存储器 24 和副非易失性存储器 26 中储存的数据备份。存储装置 36 被设计成对于由输入访问控制和输出访问控制设备 46 和 48 所产生的数据进行备份。具体来说，存储装置 36 被设计成一个辅助的或备份的存储器装置，用于储存每小时/每天的报警报告和/或每小时/每天生物体进出由 FEAC 20 控制的设备的处理记录。存储装置 36 不限于用可擦除的可编程只读存储器(EPROM)、EEPROM、磁泡(bubble)存储器、快闪型可擦除的可编程只读存储器(FEROM)以及其它铁电技术产品。存储装置的其它类型包括(但并不限于) CD ROM、磁带和磁盘存储器。

图 2 示出了可在设备电子访问控制器 20 中运行的软件结构 66。设备电子访问控制器 20 最好包括监控几个软件模块的操作系统 68，被操作系统 68 监控的软件模块包括访问控制系统模块 70、卡密钥和系统数据库模块 72、公共网关接口(CGI)程序模块 74、网(web)页数据库模块 76、web 服务器模块 78、邮件客户机模块 80 和使用传输控制协议/互联网协议(TCP/IP)的模块。FEAC 20 的软件结构 66 通过输出访问控制数据 84 和输入访问控制数据 86 使输入和输出访问控制设备 46 和 48 的数据相互作用并进行数据交换。操作系统 68 被设计成允许经过网络端口 30 和/或交叉平台端口 32 与远程计算机进行数据交换。

用于设备电子访问控制器 20 的操作系统监控所有的模块，使它们同时运行。当远程计算机 44 或 LAN 40 通过 web 服务器 78 或电子邮件客户机程序 80 请求信息时，操作系统不停止访问控制系统模块 70 监控和处理来自输入访问控制和输出访问控制设备 46 和 48 的输出访问控制数据 84 和输入访问控制数据 86。操作系统 68 除了管理所有输入/输出访问控制设备 46 和 48 之外，还管理所有程序模块的存储器需要。操作系统 68 除了管理所有的微处理器处理时隙之外，还管理所有的输出访问控制数据 84 和输入访问控制数据 86。

微处理器的时隙被定义为一个允许程序执行的固定时间周期(通常低于秒级(sub-seconds))。当执行多于一个的程序时，操作系统将一秒的时间周期分成若干时隙并且为每个程序指定一个特定的时隙。对于每个计时秒，这种处理通常是重复的。这就允许操作系统在同时执行多个程序。



控制或操作系统 68 最好用 C 语言编程。但是，其它编程语言并非不在本发明的范围之外。其它编程语言包括(但并不限于)C++、Delphi、JAVA™、JavaScript™、Pascal、Perl、visual basic、Ada 和 Eiffel。

5 访问控制系统模块 70 实时地监测所有传感器 56 的状态。基本上来说，访问控制系统模块 70 实时地管理和控制所有的 I/O 功能块以及输出访问控制数据 84 和输入访问控制数据 86。访问控制系统模块 70 根据卡密钥读出器 50、寿命测定(biometry)读出器 52 和小键盘设备 54 中的至少一个运行参数允许对限制区域的进出。FEAC 20 用户的识别信息以数字形式储存在卡密钥和系统数据库 72 中。访问控制系统模块 70 将 FEAC 子系统 64 的所有交易过程和事件随同日期和时间标记一起记录。如果需要的话，访问控制系统模块 70 能够根据基于事件的时间改变警报监测和访问控制特性。访问控制系统模块 70 允许 CGI 程序模块 74 的 CGI 程序通过卡密钥和系统数据库 72 改变访问控制程序的参数。

15 公共网关接口(CGI)模块 74 为数据在 web 服务器程序模块 78 与卡密钥和系统数据库 72 之间的数据流提供了一个标准的接口。CGI 程序模块 74 规定了如何向正在执行的作为 HTTP 请求的一部分的程序传递参数。通常，CGI 程序模块 74 将生成某种将被传回远程计算机 44 的浏览器的 HTML，但是，它也可以要求统一资源定位器(uniform resource locator, URL)进行改道。CGI 程序模块 74 允许根据按请求任选的任何方式返回 HTML(或其它文件形式)。

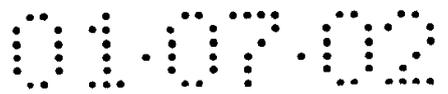
20 本发明的 CGI 程序模块 74 可以是能够接收命令行参数的任何程序。

在优选实施例中，CGI 程序模块 74 包括一套将根据来自远程计算机 44 的 web 服务器请求执行的程序。本发明的 CGI 程序和 CGI 程序模块 74 通常用于从网页上获得数据并且被储存在卡密钥和系统数据库程序模块 72 中。通常，这种数据交易过程包括增加新用户的卡信息、从数据库中删除识别码

25 等等，等等。

CGI 程序模块 74 在改变控制器的操作性能时，或者在从远程计算机 44 接收到用户的请求时，动态地创建网(web)页。这个网页可以显示输入和输出访问控制设备 46 和 48 的交易处理活动或者状态。具体来说，网页由 CGI 程序接口创建并且可以伴有时间/日期标记而显示警报发生。

30 由于访问控制系统模块 70 实时地运行，CGI 程序模块 74 可以生成能够动态更新显示位于由 FEAC 20 控制的设备中的用户位置的图形画面的网页。



由 CGI 程序模块 74 生成的网页可以包含关于用户进出由 FEAC 20 管理的设备的相对位置、日期和时间的图标和状态信息。CGI 程序模块 74 还核实和检查对 FEAC 20 的网络登录和访问权。

5 卡密钥和系统数据库模块 72 包含用户识别以及用户进出记录。卡密钥和系统数据库模块 72 是一套包含进出控制和警报监测程序 70 运行所需要的所有信息的数据库文件。卡密钥和系统数据库模块 72 可以包括(但并不限于)用户和卡密钥信息、进出权、进出时间段、交易处理记录、假日日期以及其它操作系统参数。

10 web 服务器程序模块 78 被设计成生成和服务于包含储存在卡密钥和系统数据库模块 72 中的信息的网页。web 服务器程序模块 78 使用超文本传输协议(HTTP), HTTP 是用于在万维网(WWW)上进行 HTML 文件交换的客户机-服务器 TCP/IP 协议。web 服务器程序模块 78 最好是基于互联网标准 RFC 1945 - 超文本传输协议 - HTTP/1.0 和 RFC 2068 - 超文本传输协议 - HTTP/1.1。web 服务器程序模块 78 通常将响应 URL 信息执行下列功能中的
15 至少一项功能: 检索网页; 执行 CGI 程序; 或从客户机 PC 中检索数据。web 服务器程序模块 78 不限于这些功能并且可以执行任何改进 FEAC 性能所需要的“服务器”类型的功能。伴随 web 服务器程序模块 78 执行的 CGI 程序将通过 web 服务器程序模块 78 将结果传递到客户机 PC 或远程计算机 44。

20 网页数据库程序模块 76 提供如下服务和功能, 如允许登录进入访问控制系统程序模块 70 并且显示存在于卡密钥和系统数据库模块 72 中的过去和当前的交易处理。网页数据库模块 76 允许实时地添加、更新和删除在卡密钥和系统数据库 72 中的卡持有者的识别码、设备名和位置说明。网页数据库程序模块 76 从卡密钥和系统数据库程序模块 72 中检索处理和数据库信息并且允许将数据实时地传输到远程计算机。网页数据库程序模块 76 允许远
25 程计算机 44 发送卡密钥和系统数据库程序模块 72 中被更新的数据库信息。

网页数据库程序模块 76 可以实时地显示输入和输出访问控制设备 46 和 48 的系统状态。这种系统状态显示可以采取远程计算机 44 的图像设备上的带有动态状态信息的图形画面形式。网页数据库程序模块 76 支持 JAVA APPLETs、JAVA 脚本和/或 Virtual basic VB 脚本从而提供来自远程计算机 44
30 的被升级的用户界面。

邮件客户机程序模块 80 生成到达用户的或系统管理员的电子邮件帐户

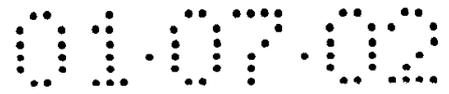
的电子邮件。术语“客户机”被定义为一个要求其它计算机系统或处理过程 (“服务器”)提供服务的计算机系统和处理过程。邮件客户机程序模块通常使用一般通过 ETHERNET™ 在计算机之间传输电子邮件的简单邮件传输协议(SMTP)。SMTP 是一个服务器对服务器协议, 因此其它协议可以用于访问消息。SMTP 对话通常发生在消息传输系统控制的背景之下, 例如, 发送邮件, 但可能与利用 Telnet 连接到正常 SMTP 端口的 SMTP 服务器相互作用。邮件客户机程序模块 80 提供多种电子邮件, 包括(但并不限于)指示系统状态、每小时/每天的报警报告、每小时/每天的交易处理报告和每天的计时交易处理的信息。由邮件客户机程序模块 80 生成的信息可以按照标准文本电子邮件或附属于电子邮件的文本文件的格式来编程。

TCP/IP 程序模块 82 最好是一个 TCP/IP 堆栈。TCP/IP 程序堆栈是一个用于储存按照后进先出(last-in first-out)顺序被访问的项目的数据结构。堆栈操作就是创建一个新堆栈, 将新项目“压入(push)”堆栈顶层并将顶层的项目“弹出(pop)”。通过在 TCP/IP 程序模块中使用 TCP/IP 通讯协议, 不同类型的通讯接口可用于将 FEAC 20 连接到远程计算机 44。具有 TCP/IP 堆栈的 TCP/IP 程序模块 82 允许用于企业内部网访问的标准 LAN 连接; 用于互联网访问的标准 LAN 连接; 以及通过以具有点对点协议(PPP)的串行 RS-232 端口的调制解调器进行的标准数据传输, 所述点对点协议(PPP)用于以拨号进(dial-in)和/或拨号出(dial-out)方式进行互联网访问的。

图 3 示出了本发明优选实施例的框图。在图 3 中, 示出了与互联网客户机服务系统 42 可操作地链接的多个设备电子访问控制器(FEAC) 20。最好, 互联网客户机服务器系统是万维网或因特网。利用本发明的系统, 单独的远程计算机可以从具有远程计算机 44 的单独远程地理位置访问多个 FEAC 20' 和 20''。FEAC 20'和 20''可以具有彼此兼容的操作系统。这是一种在地理上设备或建筑物之间离得非常近的情况。

FEAC 20'形成了具有第一类型的操作系统的子系统 88。FEAC 20''也可以具有彼此相对类似的操作系统, 但它相对于 FEAC 20'的操作系统是不同的。因此, FEAC 20'和 FEAC 20''的操作系统可以是彼此不兼容的, 因此常规的可操作链接是不可能的。

利用本发明, 当本发明的 FEAC 20'和 20''都包含系统硬件 10 和系统软件 66时, 在相对不同的子系统 88 的 FEAC 20'的操作系统和子系统 90 的 FEAC



20''的操作系统之间的交叉平台操作是可能的。这种交叉平台远程控制和监测可以利用与互联网客户机服务器系统 42 可操作地链接的远程计算机 44 来完成。另一方面，由于使用互联网客户机服务器系统 42 的本发明的交叉平台的特性，从子系统 88 的 FEAC 20'控制和监测子系统 90 的 FEAC 20''是可能的。

换句话说，任何 FEAC 系统可以被其中各自的 FEAC 20'或 20''进行内部控制，或者被位于被控制或监测的 FEAC 20'或 20''之外的其它 FEAC 系统 20'或 20''控制。FEAC 20'的子系统 88 和 FEAC 20''的子系统 90 将彼此距离相当远并且可能没有安装相同操作系统的两套设备或建筑物紧密地并行运行。例如，具有 FEAC 20'的子系统 88 可能是在一个地理位置如一个国家的大学，FEAC 20''的子系统 90 可能是在地球对面的另一个国家的具有包含 FEAC 20''的建筑物的大學。

本发明的应用不限于这些例子，还可以包括需要不同的 FEAC 20'或 20''的交叉平台操作的任何其它应用场合。还应注意的是，还可以简单地配备具有可兼容操作系统的 FEAC 20'和 20''，这些操作系统能够使用互联网客户机服务器系统 42，从而免除在子系统 88 和子系统 90 与各个子系统各个 FEAC 20 或 20'之间提供单独电缆的需求。

典型的系统性能：

通过 web 浏览器，远程计算机 44 操纵和监控报警监测条件、报警传感器状态、运行参数、系统数据库以及交易处理文件。远程计算机 44 能够监控交易处理或发送远程命令或将参数变化下载到所选定的 FEAC。

显示建筑物楼层地板或建筑物地面/场地的图形布局图可以在远程计算机 44 的计算机屏幕上显示报警传感器的位置。每个报警器传感器应该被加上含有图标和说明文字的标签。

对于报警监控，每台远程计算机 44 的操纵者能够观察报警传感器的状态，不管是属于情况正常还是报警状态或者甚至是线路故障。在同一图形布局图中，每个传感器的位置应该用图标表示出来。每次侵入报警应该用闪烁的图标和嘟嘟的报警器声音来表示。

除了显示报警传感器位置的图形布局图以外，由操作系统 68 生成的多重网页应该显示不同交易处理行为的当前和历史数据。为用户配置预定安全

检查(security clearance)的特定类型的网页应该是可能的。

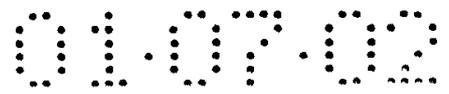
具有较多或较少数据的特定类型的网页可以是基于安全口令和其它类型的登录控制。例如，某些远程计算机 44 可以访问所有 FEAC 功能，允许监控交易处理、数据库进入/编辑/删除以及软件遥控功能。然而，在另一方面，
5 某些具有低层安全检查的远程计算机 44 可能只能访问交易处理和报警监控功能，例如通常由警卫使用的那些功能类型。

所有的警报监控点都应该在当地由当地的配备/解除配备输入装置、或由自动时间段控制或由远程计算机 44 的操作员手动进行配备或解除配备。当从警报控制器接收到报警信号时，远程计算机 44 应该完成下列各项中的
10 至少一项：在警报交易处理查看窗口上显示全部报警说明文字、显示进入报警点发生的准确位置、时间和日期加上能够观察到报警点的布局图名/位置；当对应的布局图正在被激活时，表示特定传感检测器的对应符号应该用闪烁的图标和报警声音来显示；如果同时有多于一个的警报发生，则系统报警计数器应该指示列队中的报警数量；在远程计算机 44 的 SMCCS(PC 扬声器)
15 中，系统将发出嘟嘟的可听见的声音；登录发生报警的报警文字说明、日期和时间；在远程计算机 44 的打印机上生成报警消息的硬拷贝打印输出。

远程计算机 44 的操作员可以以下列方式处理报警条件：如前所述，当警报发生时，远程计算机 44 应该在与警报有关的图上显示一个图标；一旦操作员已被通知到该警报，他/她将通过简单地用鼠标指向并点击远程计算机 4 上的图标关闭警报器，首先关闭警报器声音；然后，操作员简单地将鼠标指向闪烁的报警图标，在对话框中调出与这个特定警报器有关的说明；如
20 果操作员要确认那个警报器，他/她应该点击<确认>图标以证实确认；然后远程计算机 44 应该登录操作员的姓名以及关于具体报警点确认的时间和日期；并且远程计算机 44 应该能够在同一个计算机屏幕上显示多重图形布局
25 图网页以帮助操作员可见而迅速地确定报警传感器的位置。

本发明还提供了一种允许进行交叉平台远程控制和监测设备电子访问控制器的系统和方法。本发明还提供了用于根据设备访问的数据进行变化并且控制设备电子访问控制器的多台可能具有或可能不具有相似操作系统的中央计算机的系统和方法。

30 本发明还提供了用于交叉平台远程控制和监测设备访问控制器的系统和方法，其中，每个设备电子访问控制器的中央计算机包括 web 服务器。



用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法允许设备电子访问控制器的每台中央计算机通过使用传输控制协议/互联网协议(TCP/IP)和超文本传输协议(HTTP)的工业协议与客户机进行通讯。

5 用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法允许设备电子访问控制器的客户机用远程计算机或 FEAC 的远程中央计算机，利用任何 web 浏览器访问 FEAC。该系统允许从和在 web 浏览器和/或 FEAC 中监控对限制区域的交易处理/活动行为。

10 本发明还提供了用于提供交叉平台远程控制和监测设备入侵报警监控功能的系统和方法，由此，按照 web 客户机那样运行的一台或多台远程计算机可以通过互联网监测用于检测设备或建筑物进入条件的报警器。

本发明还提供了用于提供交叉平台远程控制和监测设备访问控制器的系统和方法，其中，FEAC 的不同的中央计算机运行不同的操作系统，但是它们被连接在同一个网络(或者是局域网或者是广域网)上，与 FEAC 的不同中央计算机通信。

15 本发明还提供了用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，设备电子访问控制器的 web 服务器被设计成使用支持不同语言的超文本标记语言(HTML)标准。

20 用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法(其中，FEAC 的中央计算机象简单的邮件传输协议(SMTP)客户机那样工作)允许 FEAC 的中央计算机通过互联网电子邮件协议向远程用户发送数据、登录、正常活动行为交易处理或者安全破坏数据等等。用这种系统和方法，基于程序控制的 FEAC 的计算机能够发送特定的或选定的信息。此外，利用这种系统和方法，通过互联网电子邮件系统，特定的或选定的访问信息或数据可以被发送到多个地点的多个用户。

25 本发明还提供了用于交叉平台远程控制和监测设备访问控制器的系统和方法，其中，FEAC 中按照不同操作系统运行的中央计算机可以用标准电子邮件软件检索/访问信息或数据。

30 本发明还提供了用于提供交叉平台远程控制和监测设备电子访问控制器的系统和方法，其中，基本上免除了在每个 FEAC 中的每个中央计算机中安装同样的软件的需要。

本发明使用了用于提供交叉平台远程控制和监测设备电子访问控制器的

系统和方法，其中，监测限制区域的访问数据实时地提供给远程计算机或 FEAC 的中央计算机。这种限制区域的访问数据包括(但并不限于)实时地显示持卡人的识别码、寿命测定扫描的结果、设备名、地点说明、系统数据库以及 FEAC。其它访问数据包括(但并不限于)在网页上显示图形图像和动态状态信息，以及用远程计算机或 FEAC 的中央计算机的 web 浏览器检索这

5 些信息。

虽然本发明是如本文所描述的，但是，很明显，同一种事物可以有多种方式的变化。这些变化不应该认为是偏离本发明的精神和范围，同时，所有这些对于本领域技术人员来说是显而易见的修改应该包括在后面的权利要求

10 书的范围内。

说明书附图

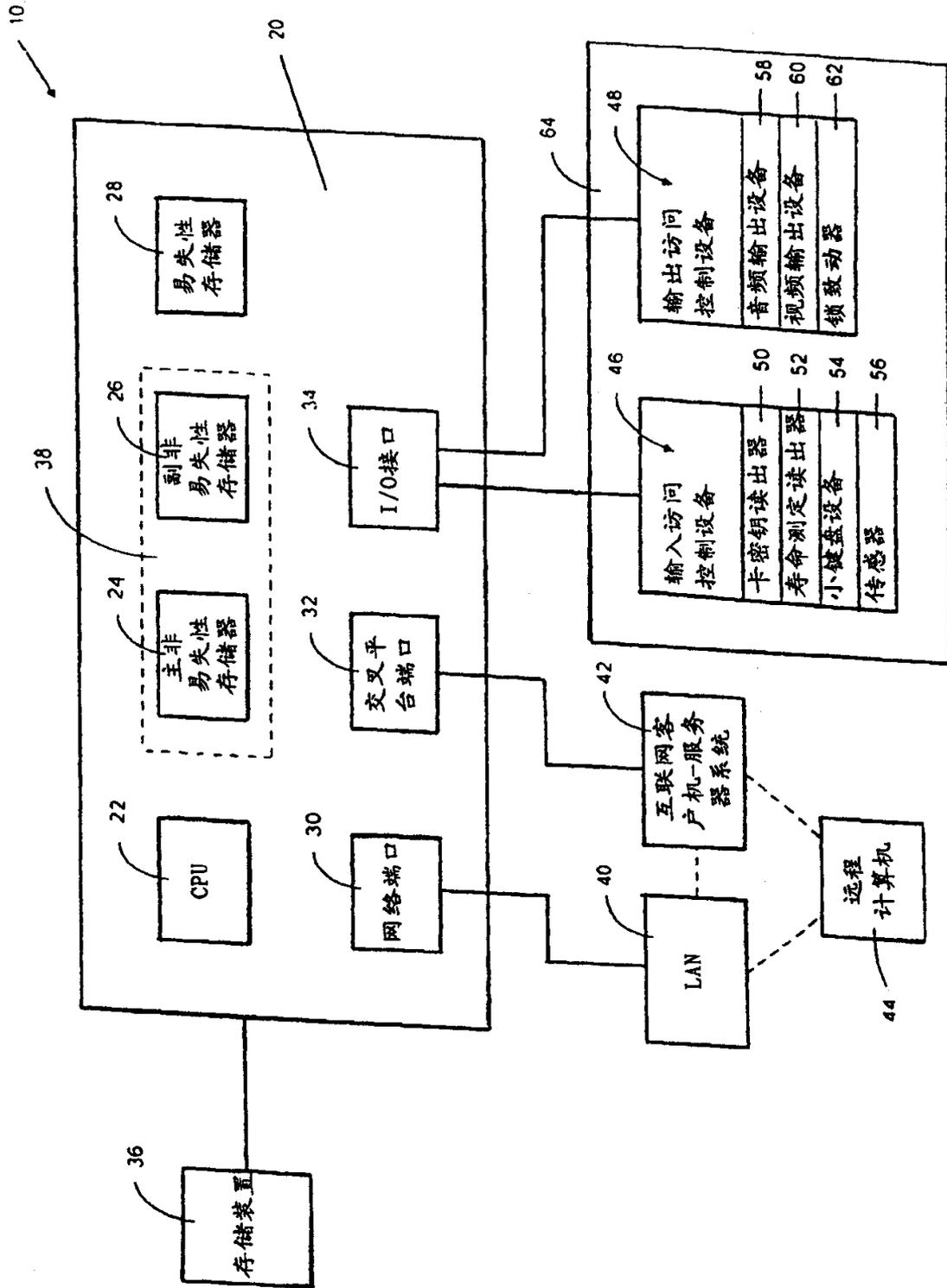


图 1

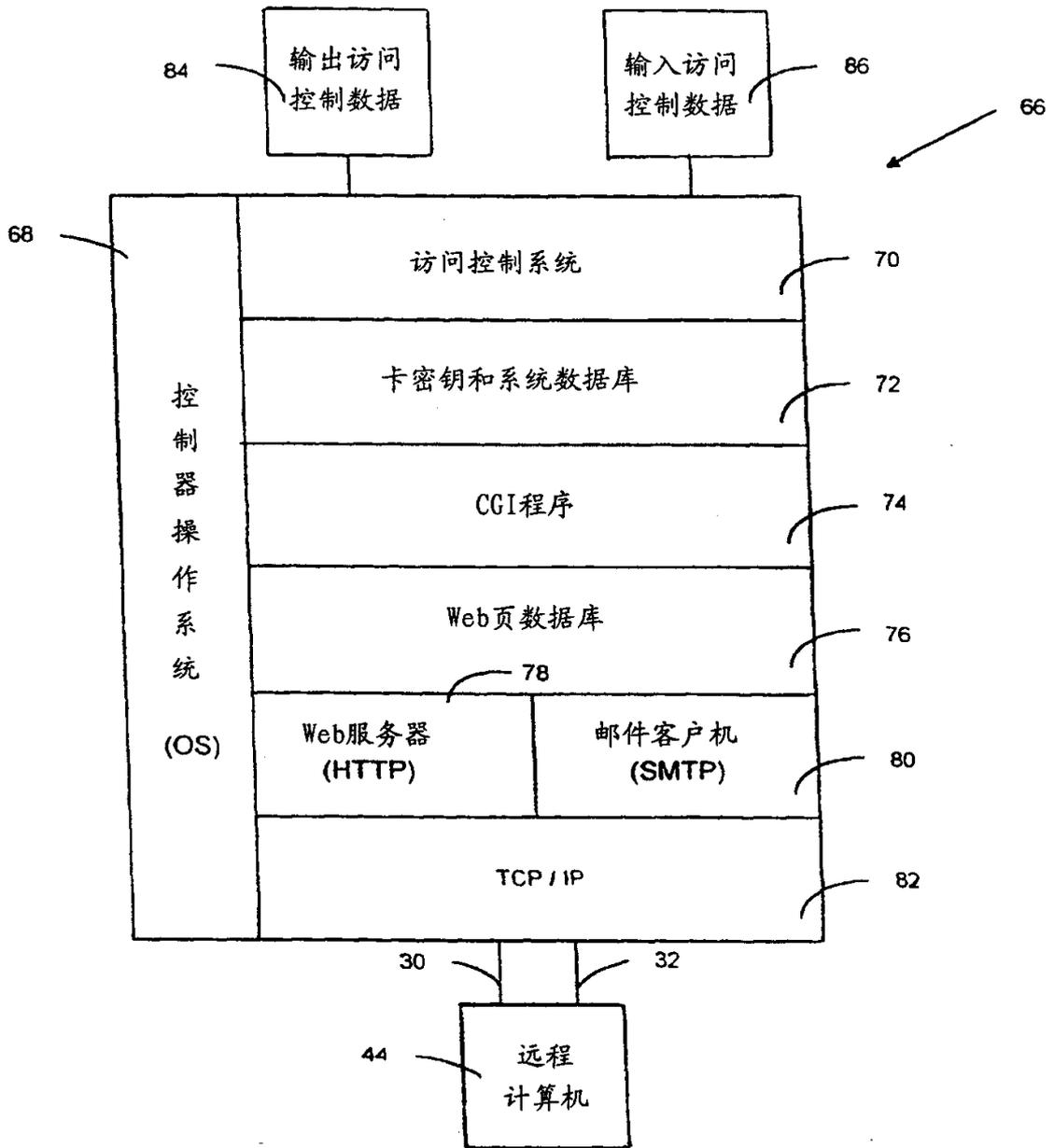


图 2

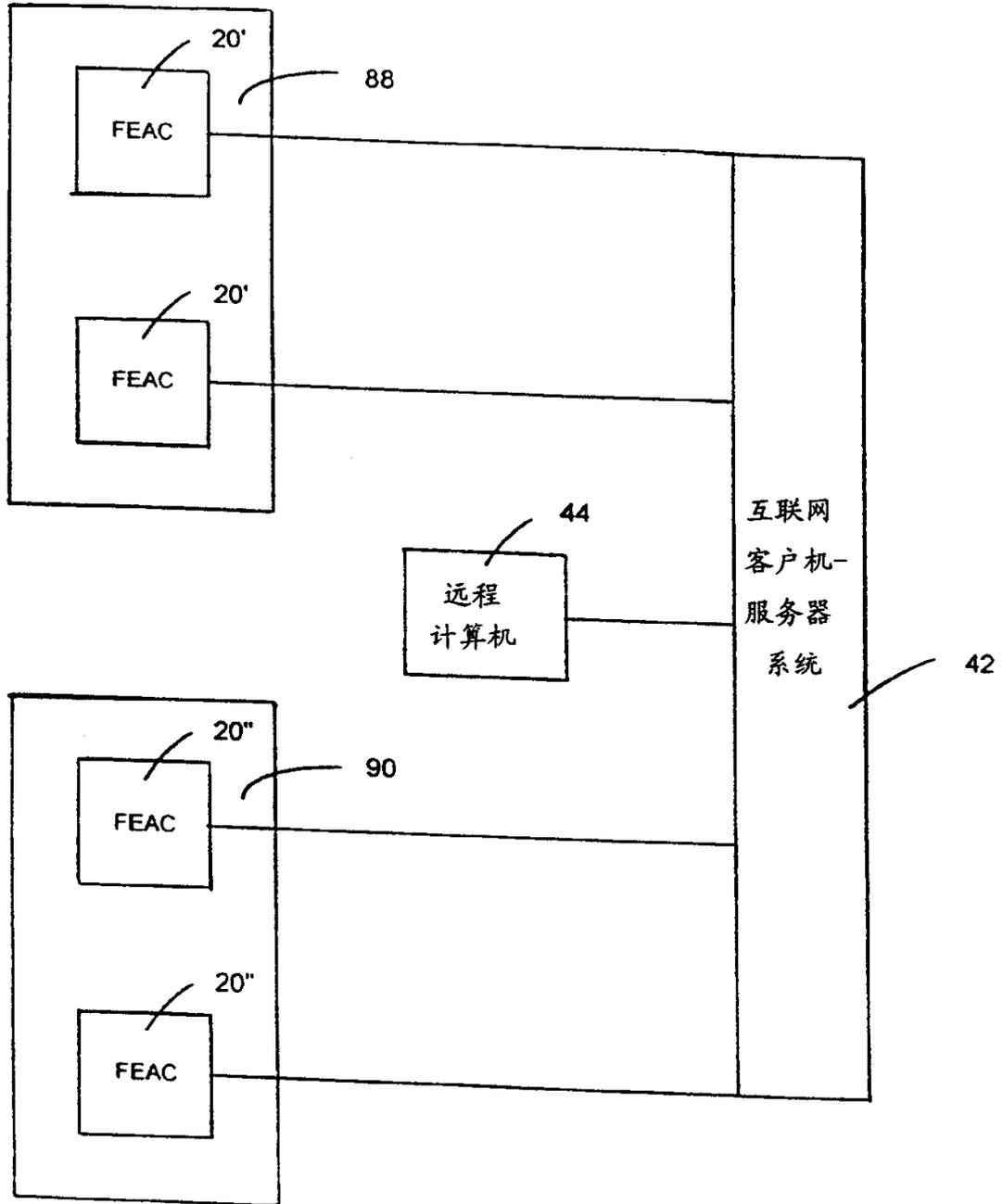


图 3