(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103403668 A
(43)申请公布日 2013.11.20

(21)申请号 201180068801.6
(22)申请日 2011.12.15
(30)优先权数据
12/982,950 2010.12.31 US
(85)PCT申请进入国家阶段日
2013.08.30
(86)PCT申请的申请数据
PCT/US2011/065112 2011.12.15
(87)PCT申请的公布数据
WO2012/091940 EN 2012.07.05
(71)申请人 施耐德电气建筑有限公司
地址 美国马萨诸塞州
(72)发明人 乔恩·L·威廉姆森
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 周靖 郑霞
(51)Int.Cl.
G06F 7/04(2006.01)

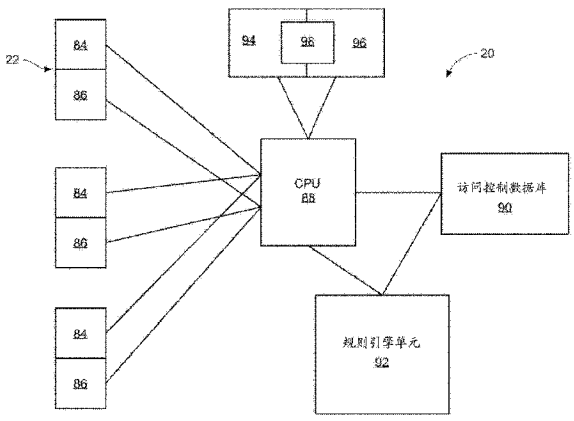
权利要求书3页 说明书9页 附图8页

(54)发明名称

用于访问权限可视化的方法和系统

(57)摘要

本系统和方法利用个人的或团体的状态变化并且按照一系列步骤(规则)确保个人或团体被给予了或曾被给予对安全位置的适当的访问。系统具有至少一个访问控制设备,用于控制物理环境中的人员向至少一个安全区域的流动。系统的访问控制数据库包含关于允许访问至少一个安全区域的标准的信息。规则单元从各种来源收集信息并更新访问控制数据库。系统具有带有集成的可视显示器和文本显示器的接口,所述集成的可视显示器和文本显示器被配置成查看和/或修改用户和团体的访问权限。



CN 103403668 A

1. 一种用于允许访问安全区域的安全系统，所述系统包括：

至少一个访问控制设备，用于控制实际环境中的用户向至少一个安全区域的流动；

访问控制数据库，其包含关于允许访问所述至少一个安全区域的标准的信息；

控制系统，用于接收来自所述至少一个访问控制设备的信息以及将所述信息与所述访问控制数据库相比较以确定是否将授权访问；以及

规则单元，用于从各种来源收集信息并更新所述访问控制数据库。

2. 如权利要求 1 所述的安全系统，还包括被配置成查看和修改对所述至少一个安全区域的访问的接口。

3. 如权利要求 2 所述的安全系统，其中所述接口被配置成接收来自操作员的输入并根据从所述操作员接收到的所述输入更新所述访问控制数据库。

4. 如权利要求 2 所述的安全系统，其中所述接口包括文本显示器。

5. 如权利要求 2 所述的安全系统，其中所述接口包括可视显示器。

6. 如权利要求 3 所述的安全系统，其中所述接口被配置成实时地修改对所述至少一个安全区域的访问。

7. 如权利要求 3 所述的安全系统，其中所述接口被配置成修改在未来的某一时刻对所述至少一个安全区域的访问。

8. 如权利要求 2 所述的安全系统，其中所述接口被配置成实时地查看对所述至少一个安全区域的访问。

9. 如权利要求 2 所述的安全系统，其中所述接口被配置成查看在未来的某一时刻对所述至少一个安全区域的访问。

10. 如权利要求 2 所述的安全系统，其中所述接口被配置成查看在过去的某一时刻对所述至少一个安全区域的访问。

11. 如权利要求 2 所述的安全系统，其中所述接口被配置成按照用户查看对所述至少一个安全区域的访问。

12. 如权利要求 2 所述的安全系统，其中所述接口被配置成按照用户组查看对所述至少一个安全区域的访问。

13. 如权利要求 2 所述的安全系统，其中所述接口被配置成按照所述至少一个安全区域查看对所述至少一个安全区域的访问。

14. 如权利要求 2 所述的安全系统，其中所述接口被配置成按照时间段查看对所述至少一个安全区域的访问。

15. 如权利要求 3 所述的安全系统，其中所述接口被配置成按照用户修改对所述至少一个安全区域的访问。

16. 如权利要求 3 所述的安全系统，其中所述接口被配置成按照所述至少一个安全区域修改对所述至少一个安全区域的访问。

17. 如权利要求 3 所述的安全系统，其中所述接口被配置成按照时间段修改对所述至少一个安全区域的访问。

18. 如权利要求 3 所述的安全系统，其中所述接口被配置成按照用户组修改对所述至少一个安全区域的访问。

19. 如权利要求 1 所述的安全系统，其中所述规则单元包括：

用于从其他数据库收集信息的机构；

用于更新与人员有关的数据库的机构；以及

用于更新所述访问控制数据库的机构。

20. 如权利要求 1 所述的安全系统，其中所述规则单元使用人员数据库和组织数据库来确定所述访问控制数据库中的设置。

21. 如权利要求 20 所述的安全系统，其中所述规则单元使用系统数据库来确定所述访问控制数据库中的设置。

22. 如权利要求 1 所述的安全系统，其中所述规则单元收集信息和更新所述访问控制数据库的周期可以被改变。

23. 一种动态地更新访问权限的方法，所述方法包括：

提供访问控制数据库，所述访问控制数据库包含关于允许通过至少一个访问控制设备访问至少一个安全区域的标准的信息；

从至少一个来源收集与人员有关的信息；

基于所收集的信息更新与人员有关的人员访问数据库；以及

通过包含用于至少一个访问控制设备的标准的规则引擎单元处理来自所述人员访问数据库的信息来更新所述访问控制数据库。

24. 如权利要求 23 所述的动态地更新访问权限的方法，还包括利用被配置成查看和修改对至少一个安全区域的访问的接口显示所述访问控制数据库的内容的步骤。

25. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成接收来自操作员的输入以及根据从所述操作员接收到的所述输入更新所述访问控制数据库。

26. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口包括文本显示器。

27. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口包括可视显示器。

28. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成实时地修改对所述至少一个安全区域的访问。

29. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成修改在未来的某一时刻对所述至少一个安全区域的访问。

30. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成实时地查看对所述至少一个安全区域的访问。

31. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成查看在未来的某一时刻对所述至少一个安全区域的访问。

32. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成查看在过去的某一时刻对所述至少一个安全区域的访问。

33. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成按照用户查看对所述至少一个安全区域的访问。

34. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成按照用户组查看对所述至少一个安全区域的访问。

35. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成按照所

述至少一个安全区域查看对所述至少一个安全区域的访问。

36. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述接口被配置成按照时间段查看对所述至少一个安全区域的访问。

37. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成按照用户修改对所述至少一个安全区域的访问。

38. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成按照所述至少一个安全区域修改对所述至少一个安全区域的访问。

39. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成按照时间段修改对所述至少一个安全区域的访问。

40. 如权利要求 25 所述的动态地更新访问权限的方法，其中所述接口被配置成按照用户组修改对所述至少一个安全区域的访问。

41. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述规则引擎单元使用所述人员访问数据库和组织数据库来确定用于所述至少一个访问控制设备的所述标准。

42. 如权利要求 41 所述的动态地更新访问权限的方法，其中所述规则引擎单元使用系统数据库来确定用于所述至少一个访问控制设备的所述标准。

43. 如权利要求 24 所述的动态地更新访问权限的方法，其中所述来源是多个数据库。

44. 如权利要求 43 所述的动态地更新访问权限的方法，其中所述多个数据库选自由培训数据库、项目数据库和人力资源数据库组成的组。

45. 如权利要求 43 所述的动态地更新访问权限的方法，其中所述多个数据库还包括包含身份管理系统（IDMS）数据库的其他数据库。

用于访问权限可视化的方法和系统

发明领域

[0001] 本发明涉及物理安全和访问控制，且更具体地涉及向个人或团体动态地分配权限。

[0002] 发明背景

[0003] 通常通过访问控制系统限制对物理位置的访问。访问控制系统在复杂度上可以从孩童无法触及的门闩到诸如指纹或视网膜读取器的生物测量变化。一些更常见的系统包括感应卡或其他凭证，其中卡或其他凭证被绑定到特定个人。

[0004] 访问控制系统通过将访问权限分配给个人、团体或部门来控制对安全区域的访问。访问权限可以被分配来限制在特定日期和时间内对区域的访问。此外，访问可以按照条件或特权被进一步限制或增加。因此，能够访问整个建筑物的操作员可被限制在特定时间、特权和条件下的特定区域。

[0005] 发明概述

[0006] 已经认识到在访问控制系统中的访问权限的分配是原来一直是静态过程。权限不是从访问控制系统被相互分配，就是基于一种属性（例如部门）被输入或分配给一组访问许可。一旦设置，权限需要定期的人工管理。

[0007] 本发明的一个方面是用于允许访问安全区域的安全系统，该安全系统包括至少一个访问控制设备、访问控制数据库、控制系统、规则单元以及接口；所述至少一个访问控制设备用于控制物理环境中的用户向至少一个安全区域的流动；所述访问控制数据库包含关于允许访问至少一个安全区域的标准的信息；所述控制系统用于接收来自至少一个访问控制设备的信息以及将所述信息与访问控制数据库相比较以确定是否授权允许访问；所述规则单元用于从各种来源收集信息并更新访问控制数据库；以及所述接口被配置为查看和/或修改对至少一个安全区域的访问。

[0008] 在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成接收来自操作员的输入并根据从操作员接收到的输入更新访问控制数据库。在用于允许访问安全区域的安全系统的一个实施方式中，接口包括文本显示器。在用于允许访问安全区域的安全系统的一个实施方式中，接口包括可视显示器。

[0009] 在用于允许访问安全区域的安全系统的另一个实施方式中，接口被配置成实时地修改对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的另一个实施方式中，接口被配置成修改在未来的某一时刻对至少一个安全区域的访问。

[0010] 在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成实时地查看对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成查看在未来的某一时刻对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成查看在过去的某一时刻对至少一个安全区域的访问。

[0011] 在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按用户查看对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，

接口被配置成按用户组查看对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按至少一个安全区域查看对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按时间段查看对至少一个安全区域的访问。

[0012] 在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按用户修改对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按至少一个安全区域修改对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按时间段修改对至少一个安全区域的访问。在用于允许访问安全区域的安全系统的一个实施方式中，接口被配置成按用户组修改对至少一个安全区域的访问。

[0013] 在用于允许访问安全区域的安全系统的一个实施方式中，规则单元包括：用于从其他数据库收集信息的机构；用于更新与人员有关的数据库的机构；以及用于更新访问控制数据库的机构。在用于允许访问安全区域的安全系统的一个实施方式中，规则单元使用人员数据库和组织数据库，用于确定访问控制数据库中的设置。在用于允许访问安全区域的安全系统的一个实施方式中，规则单元使用系统数据库，用于确定访问控制数据库中的设置。在用于允许访问安全区域的安全系统的一个实施方式中，规则单元收集信息和更新访问控制数据库的周期可以被改变。

[0014] 在本发明的另一方面，是动态地更新访问权限的方法，其包括：提供访问控制数据库，该访问控制数据库包含关于允许通过至少一个访问控制设备访问至少一个安全区域的标准的信息；从至少一个来源收集与人员有关的信息；基于收集的信息更新与人员有关的人员访问数据库；通过包含用于至少一个访问控制设备的标准的规则引擎单元处理来自人员访问数据库的信息来更新访问控制数据库；以及利用被配置成查看和修改对至少一个安全区域的访问的接口显示访问控制数据库的内容。

[0015] 在动态地更新访问权限的方法的一个实施方式中，接口被配置成接收来自操作员的输入并根据从操作员接收到的输入更新访问控制数据库。在动态地更新访问权限的方法的一个实施方式中，接口包括文本显示器。在动态地更新访问权限的方法的一个实施方式中，接口包括可视显示器。

[0016] 在动态地更新访问权限的方法的一个实施方式中，接口被配置成实时地修改对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成修改在未来的某一时刻对至少一个安全区域的访问。

[0017] 在动态地更新访问权限的方法的一个实施方式中，接口被配置成实时地查看对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成查看在未来的某一时刻对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成查看在过去的某一时刻对至少一个安全区域的访问。

[0018] 在动态地更新访问权限的方法的一个实施方式中，接口被配置成按用户查看对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按用户组查看对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按至少一个安全区域查看对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按时间段查看对至少一个安全区域的访

问。

[0019] 在动态地更新访问权限的方法的一个实施方式中，接口被配置成按用户修改对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按至少一个安全区域修改对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按时间段修改对至少一个安全区域的访问。在动态地更新访问权限的方法的一个实施方式中，接口被配置成按用户组修改对至少一个安全区域的访问。

[0020] 在动态地更新访问权限的方法的一个实施方式中，规则引擎单元使用人员访问数据库和组织数据库来确定用于至少一个访问控制设备的标准。在动态地更新访问权限的方法的一个实施方式中，规则引擎单元使用系统数据库来确定用于至少一个访问控制设备的标准。在动态地更新访问权限的方法的一个实施方式中，来源是多个数据库。在动态地更新访问权限的方法的一个实施方式中，多个数据库选自由培训数据库、项目数据库和人力资源数据库组成的组。在动态地更新访问权限的方法的一个实施方式中，多个数据库还包括包含身份管理系统（IDMS）数据库的其他数据库。

[0021] 本发明的这些方面并不意味着是唯一的，并且当结合以下描述、所附权利要求以及附图进行阅读时，本发明的其他特征、方面和优点对于本领域的普通技术人员是相当明显的。

[0022] 附图的简要说明

[0023] 本发明的以上及其他目的、特征和优点将从以下对本发明特定实施方式的描述中更加明显地体现，正如附图中所示，同样的参考符号在所有不同的视图中都指同样的部分。附图不必按比例绘制，而是将重点放在说明本发明的原理。

[0024] 图 1 表示建筑物安全系统的绘图显示。

[0025] 图 2 表示工业中心安全系统的绘图显示。

[0026] 图 3 表示用于控制建筑物的物理访问控制系统的本发明的系统的示意图。

[0027] 图 4 表示本发明的规则矩阵的绘图显示。

[0028] 图 5 表示本发明的调整特权的方法的示意图。

[0029] 图 6 表示本发明的交互系统的示意图。

[0030] 图 7 表示本发明的可视显示器。

[0031] 图 8 表示本发明的文本显示器。

[0032] 图 9 表示包括门超控 (door override) 的本发明的可视显示器。

[0033] 图 10 表示包括门超控的本发明的文本显示器。

[0034] 本发明的优选实施方式

[0035] 系统和方法利用个人的或团体的状态发生变化并且按照一系列步骤（规则）确保个人或团体被给予了或曾被给予适当的访问。系统具有至少一个访问控制设备，用于控制物理环境中的用户向至少一个安全区域的流动。系统的访问控制数据库包含关于用于允许访问至少一个安全区域的标准的信息。控制系统接收来自至少一个访问控制设备的信息并将其与访问控制数据库相比较以确定是否授权允许访问。规则单元从各种来源收集信息并更新访问控制数据库。接口被配置成查看和 / 或修改访问权限以及以文本方式和 / 或可视方式显示信息。接口接收来自操作员的输入并更新访问控制数据库。规则引擎单元可以被

集成到系统中或者可以在系统外部。

[0036] 参照图 1，示出了建筑物 30 的安全系统 20 的绘图显示。在该简化表示中，建筑物 30 被示出具有前门 32 和侧门 34。此外，建筑物 30 具有多个房间 36，其中一些房间具有访问控制设备 22。此外，建筑物 30 在前厅 40 和走廊 42 之间具有访问控制设备 22；该门被标记为 38。需要了解的是在工作日期间某些访问控制设备 22 可能利用安全系统 20 被切换到另一种模式：不限制特定位置之间（如大厅 40 和走廊 42 之间，或者可选地为前门 32）的访问。

[0037] 仍然参照图 1，在该实施方式中，每个雇员都有一张打开某些门（例如财务办公室 44、销售办公室 46、实验室 48、前台办公室套房 50 和设施 /IT 套房 52）所需的感应卡。需要了解的是其他位置（例如洗手间 54 和厨房 56）没有访问系统。在传统的系统中，如图 3 中所示的访问控制数据库 90 将列出人员（例如雇员）以及雇员被允许访问的特定门以及时间。表格 1 示出了数据库 90 的一小部分的表示。如果特定雇员的情况改变，例如调换班次或工作，那么安全系统 20 的操作员将进入数据库 90 并调整个人的特权。

[0038]

雇员	后门 第一班次	后门 第二班次	后门 其他时间	实验室 第一班次	实验室 第二班次	实验室 其他时间
A	是	是	是	是	否	是
B	是	否	否	是	否	否
C	是	否	否	是	是	否
D	是	是	否	否	否	否
E	否	是	否	否	是	否
F	否	是	否	否	是	否
G	否	否	是	否	否	是
H	是	否	否	否	否	否

[0039] 表格 1- 用于后门和实验室的访问控制信息

[0040] 参照图 2，示出了工业中心 60 及其相关联的安全系统 58 的绘图显示。图 1 示出了建筑物 30，以及表格 1 示出了只有八个雇员的系统。需要了解的是如图 2 中所示的工业中心 60 将比图 1 中所示的建筑物 30 具有更多的雇员和使用访问控制设备 22 的控制访问点。图 2 中所示的表示出了主办公楼 62，其可能具有许多层和各种套房（包括销售、财务、实验室和计算机室，它们都带有特殊的访问需求）。此外，各实验室可能具有不同的访问需求，或者套房中的各房间可能具有不同的访问需求。同样地，系统可能具有其他项，例如可能具有额外的或不同的需求的贮存库 64 和相关的门 66。同样地，其他设施（例如用于生产的建筑物 68 或爆炸品建筑物 70）可能具有额外的需求。同样地，工业现场 60 可以在墙上或者栅栏上具有不同类型的大门 72 来限制对现场的特定区域的访问。

[0041] 基于与情况和人员相关的变化，这种系统 58 的操作员将无法承受手动更新访问权限。

[0042] 参照图 3，示出了用于控制建筑物或其他物理访问控制系统的安全系统 20 的示意图。安全系统 20 具有多个包括输入机构 84 和访问限制器或输出设备 86 的访问控制设备

22，用于监控和授权准许对位置的访问。为了获得对某一物理位置的访问，用户需要通过输入机构 84 向访问控制设备 22 提供认证。认证可以是各种形式，包括但不限于被放置在感应卡读取器附近的感应卡，所述感应卡读取器是输入机构 84 的一部分。另一种替换形式是按键或刷卡读取器，其中用户输入代码或者刷卡。另外的可替换凭证包括 RFID、读取器和标签。

[0043] 访问控制设备 22，例如感应卡，是一种形式的凭证。凭证通过控制具有、知道或关于这三项中的至少一个限制访问。例如，用户将具有卡。用户将知道 PIN。生物测量是关于用户的。

[0044] 安全系统 20 具有用于控制安全系统 20 的控制器或中央处理单元 88。CPU88 访问包含与访问特权有关的信息的访问控制数据库 90，并且将从访问控制设备 22 的输入机构 84 接收到的信息与存储在访问控制数据库 90 中的信息相比较，以确定访问限制器输出设备 86 是否应被设置成允许访问。访问限制器输出设备 86 可以是电子门闩、机械门闩或者门。安全系统 20 还具有规则引擎单元 92，该规则引擎单元 92 获取与个人或团体有关的信息并修改访问控制数据库 90，如下面进一步详细解释的。

[0045] 仍然参照图 3，安全系统 20 包括用于接收操作员输入的接口设备 94 和用于操作员控制安全系统 20 的图形显示系统 96。在另一个实施方式中，接口设备 94 是键盘和控制点（例如鼠标或跟踪球）。在另一个实施方式中，接口装置 94 和图形显示系统 96 被结合到一个设备（例如触摸屏 98）中。

[0046] 参照图 4，示出了用于规则引擎单元 92 中的规则表 108 的简化表示。在图的左侧，有一个组织数据库 110，其列出了与图 1 中的建筑物 30 相关联的一系列访问控制设备 22。该列表仅是部分列表并且该列表将向下继续且包括每个访问控制设备 22。跨过方块顶部的是包括班次、部门、凭证、雇佣类别和项目的多个标准 112。相关联的方块 114 以是和否（或者可替换地以一和零）进行扩增。因为表格是三维的，所以只显示第一组数字。

[0047] 根据特定的规则，如与图 5 有关的进一步详细解释的，一定数量的“是”或其组合必须适用于用户通过相关联的带有访问控制设备 22 的门 / 大门。

[0048] 仍然参照图 4，在图 4 的右侧示出了第二个表格或数据库，人员数据库 118。第二个表格列出了雇员 120 及其特定状态或标准 112。如果雇员的 120 的状态 112 改变，那么受影响的方块 120 按以下所解释地被改变。例如，如果雇员“B”接收到凭证 9001，代码将变为 1。同样地，如果雇员“C”从项目“苹果”转换到项目“梨”，那么在相应方块中的代码将分别从“1”翻转到“0”和从“0”翻转到“1”。下文解释了用于改变代码的过程。

[0049] 需要了解的是对受控区域的访问可以通过将调度超控应用到区域、门或门的一侧被授权或被拒绝。此信息将与其他全系统信息（如威胁等级信息）一起驻留在系统数据库中。例如，前厅门可以被调度为在工作时间期间不锁，以及后门可被设置为防止在夜间进入建筑物，但允许在任何时候从建筑物出来。因此，系统将包括系统数据库，该系统数据库包括在给定的时间段内的所有访问点及其有关的有效行进方向的列表。

[0050] 需要了解的是以上只是一些潜在标准。其他标准可以包括性别、公民身份、车辆和分类准入。还需要了解的是可以通过各种方法寻址时间和班次。例如，个人、与项目相关联的团体，或者另一个能和班次绑定的团体。与班次有关的访问时间能被安全系统 20 改变，以反映起始时间在例如从上午 7:30 到下午 6:15 内的班次、反映假期或反映另一种情况变

化。此外，术语“班次”可以有两种不同的含义。个人或团体可被分配给一个班次，例如第一班次、第二班次或第三班次。此外，班次可能与访问时间有关，例如个人或团体可以在这些班次中的一个或多个期间和 / 或周末和假期期间获得访问权限。安全系统 20 的操作员可以定义系统以结合上面的两种情况。

[0051] 参照图 5，示出了用于确定访问的方法的示意图。安全系统 20 从如图 1 中所见的建筑物 30 的特定的门的输入机构接收到的授权对特定位置的访问的请求，且如图 4 中所见的方块 152 所表示。安全系统 20 将请求与存储在访问数据库 90 中的授权相比较，且由菱形判断框 154 所表示。如果授权是适当的，则安全系统 20 通过发送通过访问限制器 86 的信号向用户授权访问，如方块 156 所表示。如果授权是不适当的，则安全系统 20 不授权对访问限制器 86 的访问，如方块 158 所表示。

[0052] 安全系统 20 除了授权访问，还通过从各种资源（如图 6 中所见的培训数据库 180、项目数据库 182 和人力资源数据库 184）获得信息来更新访问数据库 90（如图 1 所见）。信息的获得由图 6 中的方块 170 表示。利用来自如上所述的各种来源的被更新的信息，安全系统 20 更新图 4 中所示的人员（雇员）数据库 118，如方块 172 所表示。

[0053] 随着人员（雇员）数据库 118 被更新，系统在规则引擎单元 92 中运行规则，以确保访问控制数据库 90 是最新的，所述规则引擎单元 92 从组织数据库 110 和人员数据库 118 获取信息。该步骤由图 5 中的方块 174 表示。该步骤也结合了将来自系统数据库的信息作为最终检查（未示出）。

[0054] 参照图 6，示出了显示各种设备的交互的示意图。规则引擎单元 92 从各项（例如数据库）提取信息。数据库包括培训数据库 180、项目数据库 182、人力资源数据库 184 和其他数据库。例如，另一种数据库可以是身份管理系统（IDMS）。身份管理系统和其他数据库不仅可以包括正面特征（如证书），也可以包括与系统（例如性犯罪记录）相关的反面特征。

[0055] 作为实例，雇员 John 被从一个部门调到另一个部门。安全系统 20 将通过规则引擎单元 92 获取该信息，所述规则引擎单元 92 从人力资源数据库 184 获得信息，如图 5 中的方块 170 所表示。人员数据库 118 被更新以改变如图 4 中所见的相应的方块 122，且该过程如图 5 中的方块 172 所表示。然后，系统 20 运行从组织数据库 110 和人员数据库 118 获得信息的规则，以确保访问控制数据库 90 是最新的。这种部门的改变可能不会影响访问控制数据库 90 中的任何东西，或者它可能改变单个设置，例如用于一个访问点的第三班次，或者它可能改变多个设置。

[0056] 同样地，如果雇员 Joe 收到某一培训证书，那么系统 20 从培训数据库 180 获得信息将确保访问控制数据库 90 是最新的。

[0057] 尽管以上实例与单个雇员相关，但是所述改变可以是对团体或项目的改变。在这种情况下，组织数据库 110 将被改变。例如，如果生产调度要求通常在周末或不同班次不被允许进入的雇员要处于特定的实验室中，那么安全系统 20 将获取生产信息并通过修改各种雇员对各种位置的访问权限或雇员群对各种位置的访问权限的一组规则处理所述生产信息。

[0058] 尽管班次被显示为组织数据库 110 中的标准 112，但是班次可以是与如表格 1 中所示的访问点有关的标准和限制因素。

[0059] 如以上所指出的，组织数据库 110 和人员数据库 118 的方块用“1”和“0”表示是

和否。访问控制数据库 90 通过乍一看可能不明显的规则引擎单元 92 确定。例如，如果雇员“A”具有用于第一班次、前台办公室、GS、苹果、梨和开销的“1”，那么规则可以允许其访问图 1 中所见的前台办公室 50，对于所有的班次，则可能仅允许其在第一班次期间访问实验室 48，以及不允许其访问销售办公室 46 或设施 /IT 套房 52。在一种标准中的变化可能取决于操作员所建立的规则。

[0060] 尽管需要了解的是系统 20 将以规则的间隔（例如每晚）从各种来源获得数据，但是系统 20 可以按不同的周期进行调整。此外，操作员可以手动地请求系统 20 运行更新；例如，一个班的新实习生在工厂或大型跨国公司完成课程。还需要了解的是系统可以基于需要增加特殊的访问权限，例如医疗问题可能导致通过系统 20 自动增加访问权限，以允许某些有资格的人员访问他们通常不被授权访问的位置。

[0061] 需要了解的是个人凭证的动态变化速度依赖于环境。例如，在一些系统中，一个人可以没有变化地工作数月或数年。相反，在教育机构中的系统将有与学生有关的变化，当学生注册新的课程或潜在地放弃或改变章节时，这些变化将相当规律地发生。同样地，雇员从一个项目调换到另一个项目的情形在大工业中心每周或每天都可能有变化。

[0062] 需要了解的是用于整个设施的门超控的全局调度将是有利的。根据目标区域，门超控可以在一个方向或两个方向上起作用。包括门超控和威胁等级设置的系统的设置将取代其他设置，从而使公共区域的强制性关闭和管理更加有效，因此，进一步促进了进入和离开设施的大量雇员和访问者的管理。

[0063] 需要了解的是某些设施将可能更需要非常迅速地改变大量用户组的访问，例如在威胁等级改变的过程中。该信息可以表示通过因特网获得的来自另一个数据库的数据，所述数据可以用于规则引擎单元 92 中。类似地，如果警报在设施的一个区域内发出，根据警报的性质，可能的优势是使所有访问权限临时受限，或相反地放宽访问权限以允许“访问者”（例如第一响应者）进入。根据警报的性质，这可以在设施的区域内或整个设施中实现。

[0064] 需要了解的是可以报告个人和 / 或一组个人的当前和过去的访问权限，以及预测个人和 / 或一组个人在未来的某一时刻的访问权限的访问控制系统可以导致管理访问控制系统的更有效的系统以及甚至可以提高区域内的整体安全。

[0065] 通过具有集成接口来可视地查看和 / 或修改访问权限来获得效率，所述集成接口被整体链接到以文本方式查看和 / 或修改大量个人用户组以及多个用户组的访问权限的接口。

[0066] 区域的安全性的潜在增长源自系统实时地以及在过去和在未来的设定时间处准确地考虑各种用户的访问权限的能力。如下文更详细讨论的，该系统可以有助于在事件发生后的侦破分析；它可以使安全系统对增加的威胁等级或紧急情况反应灵活；以及它可以允许组织通过预测当前用户的访问权限以及控制在未来某一设定时间内的临时访问者的访问权限为即将来临的事件计划安全需要。

[0067] 需要了解的是无论环境如何，将在某些情况下，访问者将需要出现在设施中且将需要对设施内的各个区域的受限的且可能可修改的访问。系统的动态性质的益处是通过经由交互地图显示选择区域，或通过调用列表或表格中的名字以及按照安全区域、按照时间段、按照用户或按照团体来修改访问权限，来预先安排访问者对设施的某些指定区域的访问的能力。

[0068] 如前所述，访问控制系统通常服务于许多用户和许多区域，并且许多都具有基于各种因素的不同的访问规则。此外，不同的时间安排通常应用于不同的用户(例如，史密斯博士在第二个班次工作)，和／或不同的位置(例如，体育馆仅在上午六点到晚上十一点开放)。此外，将存在其他的全系统因素，例如假期安排或威胁等级，这可能适合许多或所有的用户，但是带有不同的效果。

[0069] 需要了解的是系统必须管理复杂的组合。系统利用接口(集成的可视显示器和文本显示器)实现该目的，该接口可以基于时间段、位置和用户(作为个人或作为团体的一员)来查看和／或修改(添加／移除／改变)访问权限。接口可以以地图的形式显示安全区域的可视表示，与图 7 和图 9 中所示的平面图非常类似；或者它可以文字方式显示信息、以表格或列表显示信息，这可以通过键入用户名、团体名、位置或日期／时间来访问。参见图 8 和图 10。然后，如果适当，可以显示并且可以处理与无论使用哪种搜索方法相关联的剩余信息。

[0070] 例如，参照图 1，建筑物 30 的地图可以是交互的。系统操作员可以通过使用用于接收操作员输入的接口设备 94 和用于操作员控制安全系统 20 的图形显示系统 96 来选择房间 48。接口设备 94 可以是键盘和控制点(例如鼠标或跟踪球)。接口设备 94 可以具有结合到设备(例如触摸屏 98)中的图形显示系统 96。然后，操作员可以选择日期和／或时间来查看房间 48 的细节，且随后能够访问房间 48 的用户和／或团体的列表将出现在房间中。用户可以被拖入和／或拖出房间且也可以这种方式将成员移除和／或加入团体。此外，通过选择个人用户，用户的配置可以被修改。因此，个人可以被添加到团体、从系统整个地被移除(被终止)或者可以被给予不同的许可等级，所有这些都实时地进行。在前面的实例(修改团体和／或用户配置)中，系统可以启动用于编辑配置的单独界面。这还可以应用于实时地修改许可等级。接口被配置成使得基于从操作员接收到的输入更新访问控制数据库。访问控制设备可以包含规则引擎单元或者规则引擎单元可以在访问控制设备的外部。

[0071] 在另一个实例中，可以使用以上讨论的接口从列表中选择用户，且然后操作员可以选择日期和／或时间来查看，并且房间、建筑物和／或设施的地图将表现为可视显示器。参见图 7 和图 9。图 9 还示出了包括威胁等级信息和门超控的系统信息。地图可被标记上可视元素，例如颜色、纹理、动画，以帮助快速评定。例如，可以在用户能够“被允许访问”的所有区域内标记为绿色，且可以在用户会“被拒绝访问”的所有区域内标记为红色。同样地，地图可以被调用并输入用户名，则在给定的天、周内，用户能够访问的时间和日期可以被列在建筑物或者设施内的建筑物内的每个房间中，等等。

[0072] 系统的另一个功能是在不同的时间段内查看以及如果合适的话修改访问控制系统中的信息的能力。换句话说，系统将保留历史信息，是可实时访问的，且预测在某些参数内的未来访问权限。对用户和／或团体的访问控制权限的修改将仅用于当前和未来时间。

[0073] 当使用历史信息时，系统可以及时回到事件的特定位置和时间，并且向操作员报告已经在那个时间段访问指定区域的所有用户。当实时地使用系统时，许多因素可以通过使用已经讨论过的任何接口被容易地修改。如前所述，系统也将基于来自操作员的输入进行更新。当以预测形式使用系统时，系统可以通过导入在查询时存在的数据来模拟时间(明天、下周、下月等)。作为预测系统，可以假定某些因素，例如威胁等级、电力中断、下雪天以及病假时间。其他因素将是已知的，例如假期和门超控。但是，如果需要更精确地预测某一

未来日期，所有的因素都可以由操作员参数化或改变。系统可被用于预测性地安排会议、计划旅游、定期维护或其他特殊事件，例如球类游戏、玩耍、假期和停工。

[0074] 尽管本文已经对本发明的原理进行了描述，但本领域的技术人员应该理解该描述仅以实例进行，而不作为对本发明的范围的限制。除本文示出和描述的示例性实施方式之外，在本发明的范围内还可以设想其它实施方式。认为本领域的技术人员之一做出的修改和替代属于本发明的范围。

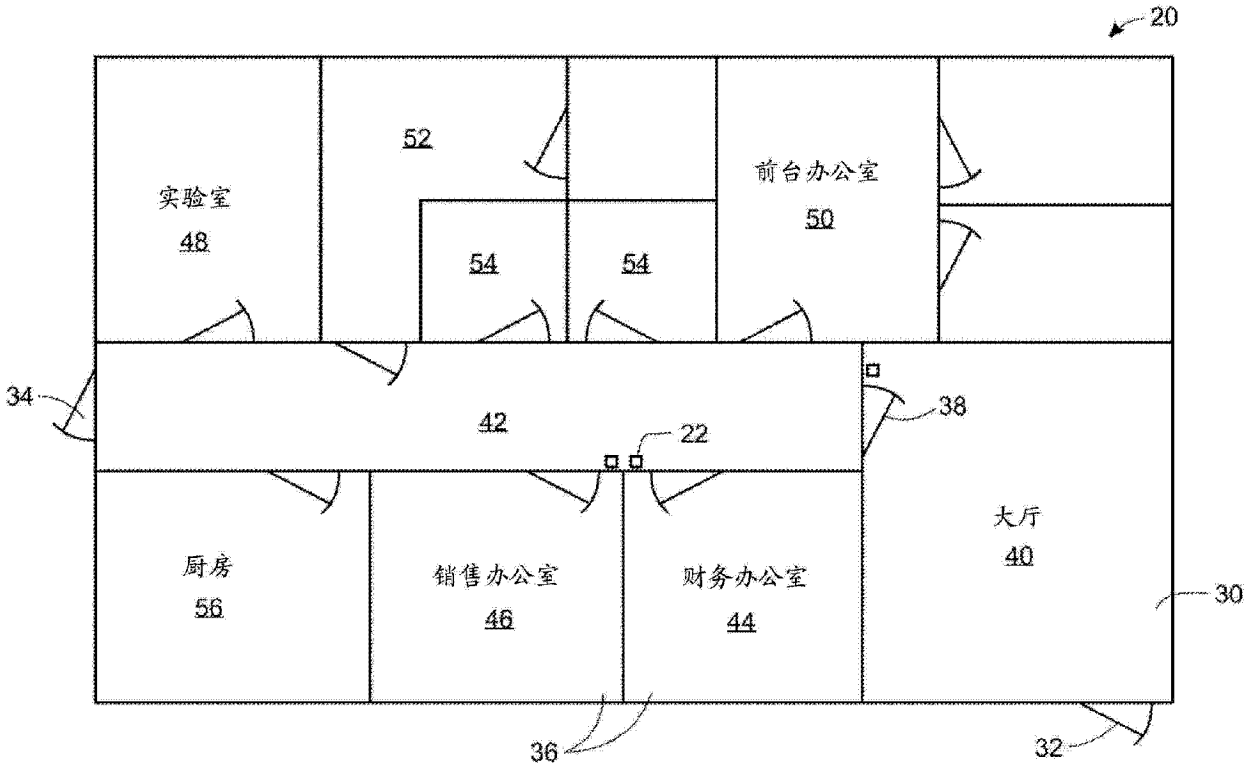

20
实验室
48
52
54
54
前台办公室
50
34
42
22
38
厨房
56
销售办公室
46
财务办公室
44
大厅
40
30
36
32

图 1

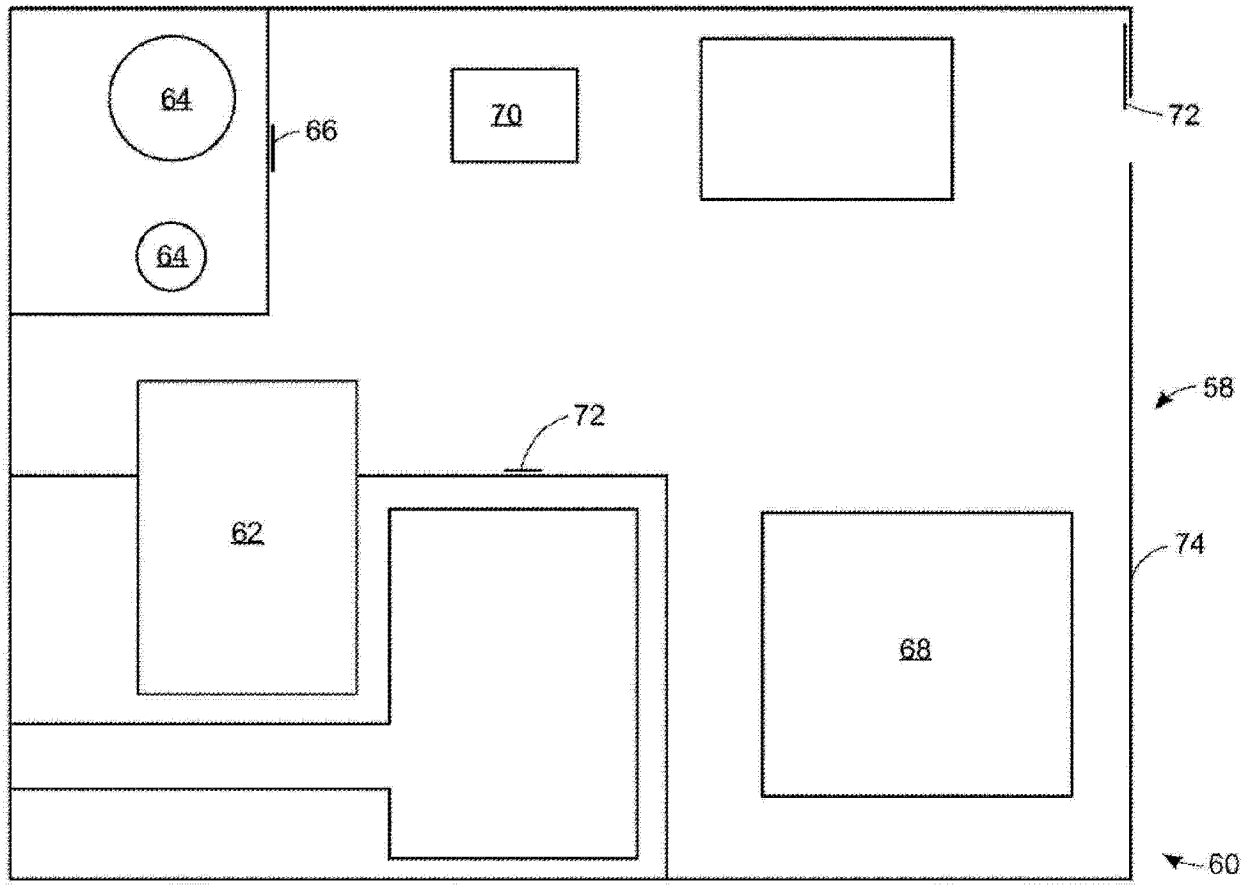


图 2

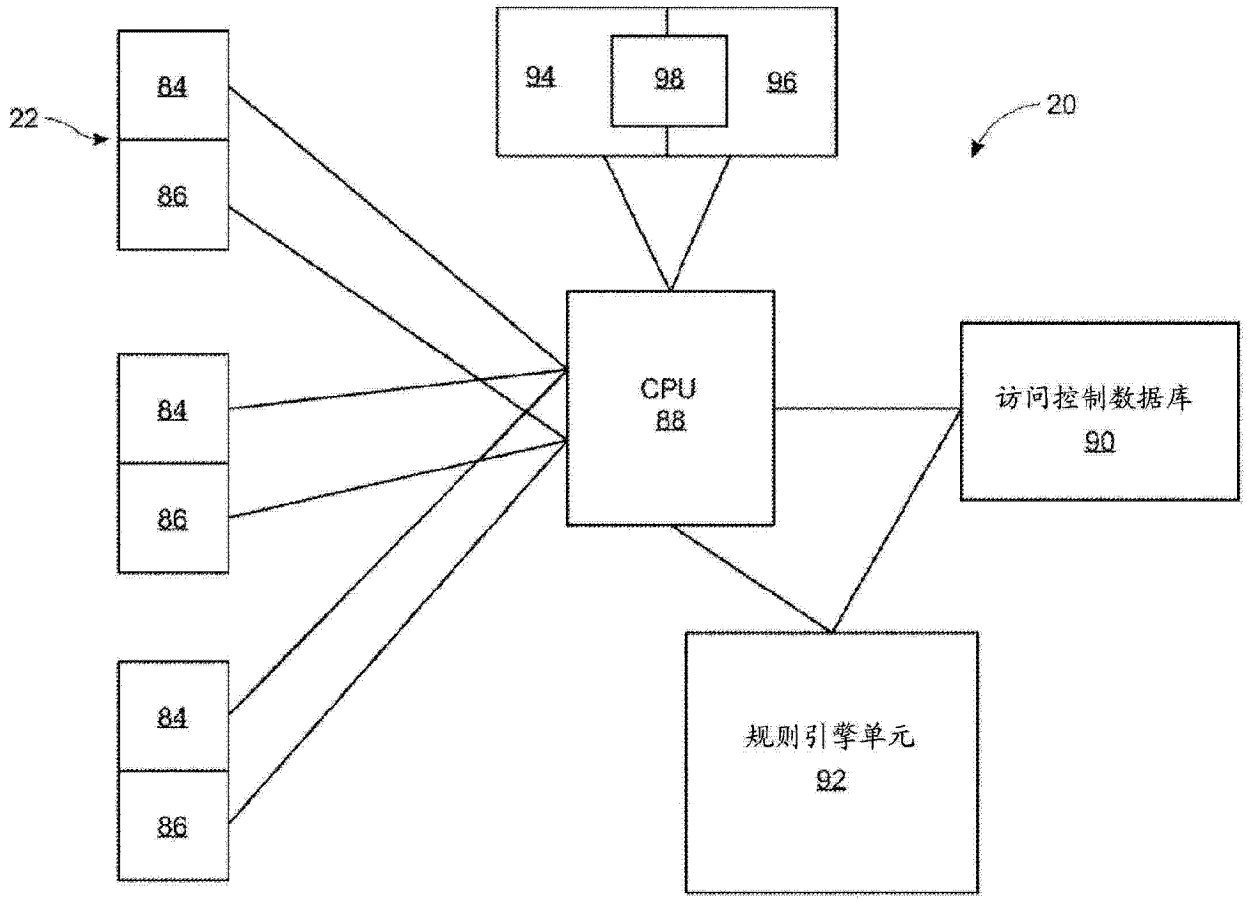


图 3

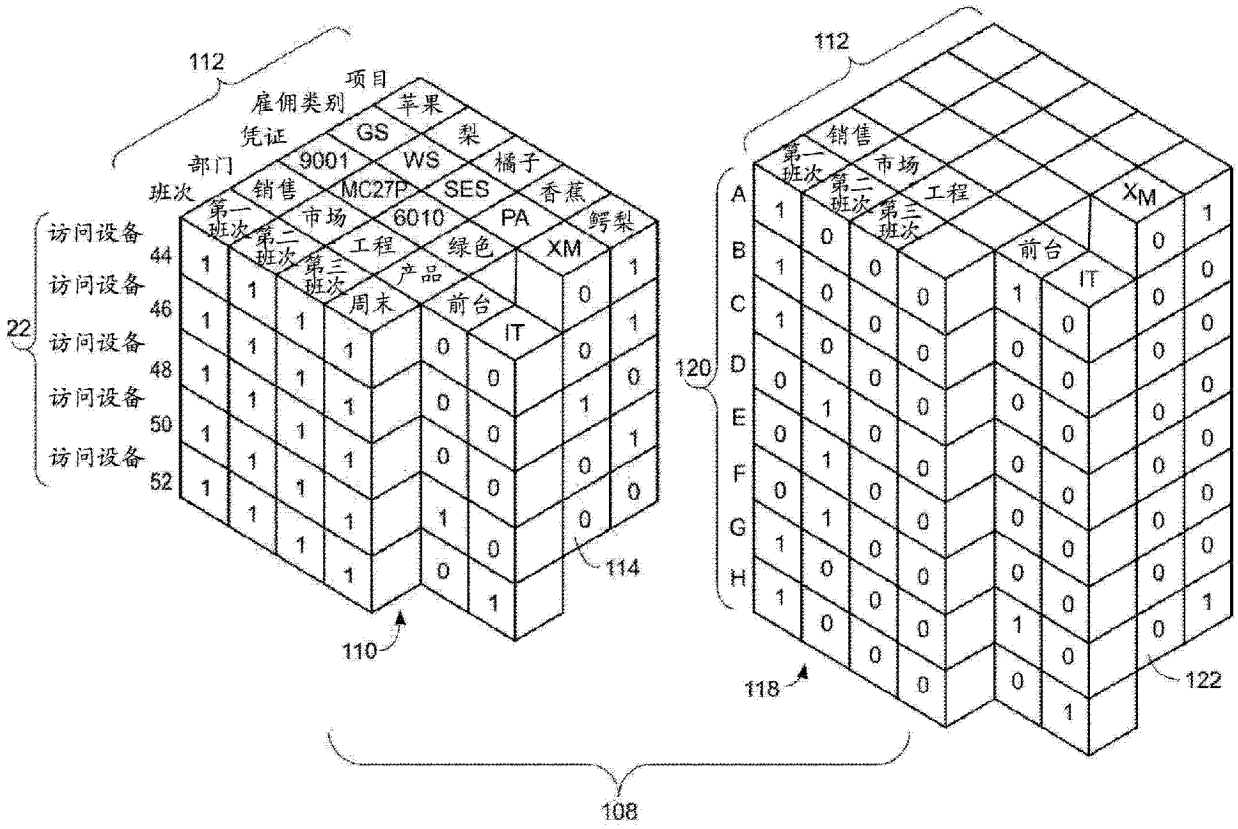

112
项目
雇佣类别
苹果
凭证
GS
梨
部门
9001
WS
橘子
班次
销售
MC27P
SES
香蕉
第一班次
市场
6010
PA
鳄梨
第二班次
工程
绿色
XM
第三班次
产品
周末
前台
IT
访问设备
44
46
48
50
52
22
110
114
112
A
B
C
D
E
F
G
H
120
118
122
108

图 4

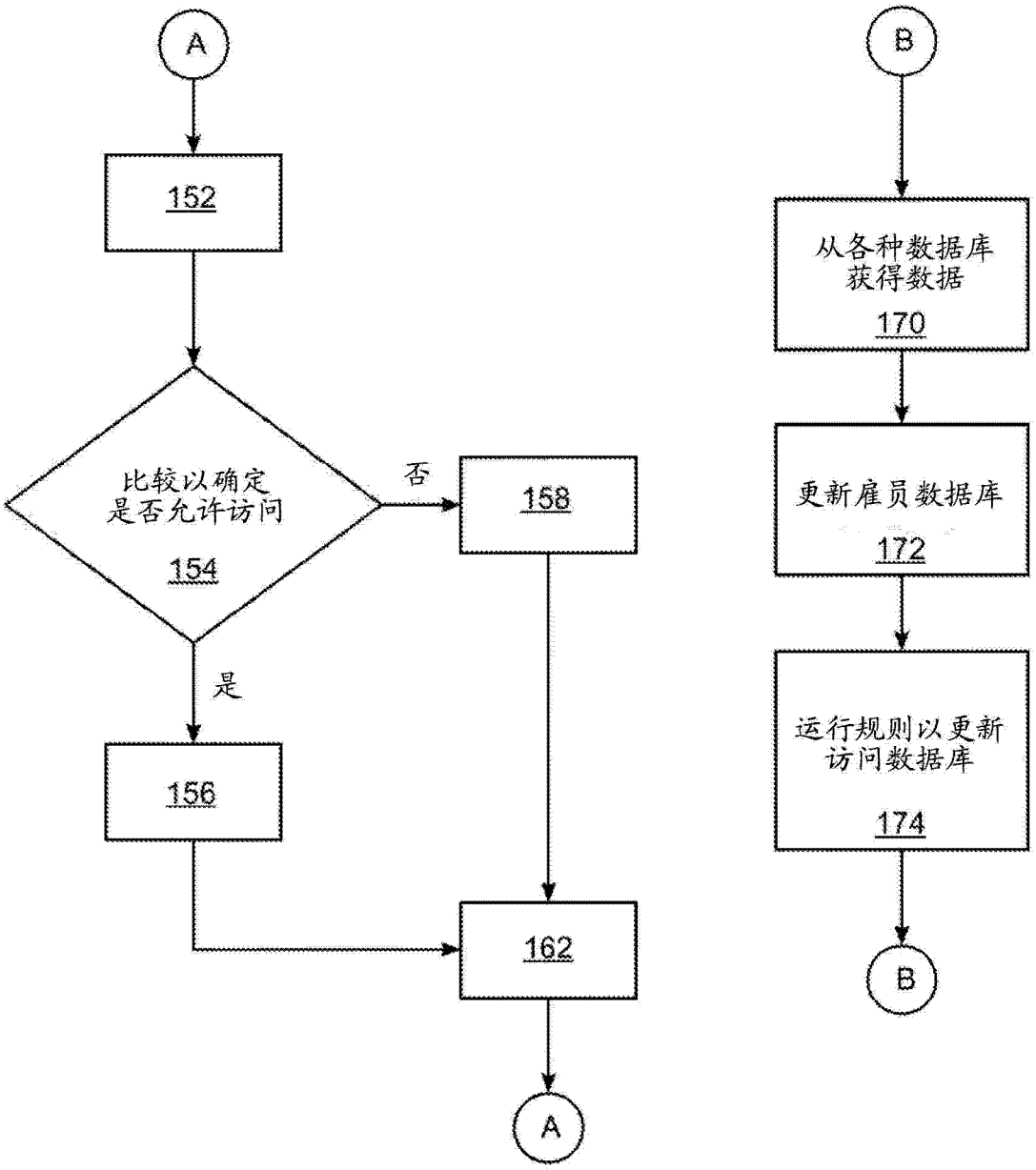

A
152
比较以确定
是否允许访问
154
否
158
是
156
162
A
B
从各种数据库
获得数据
170
更新雇员数据库
172
运行规则以更新
访问数据库
174
B

图 5

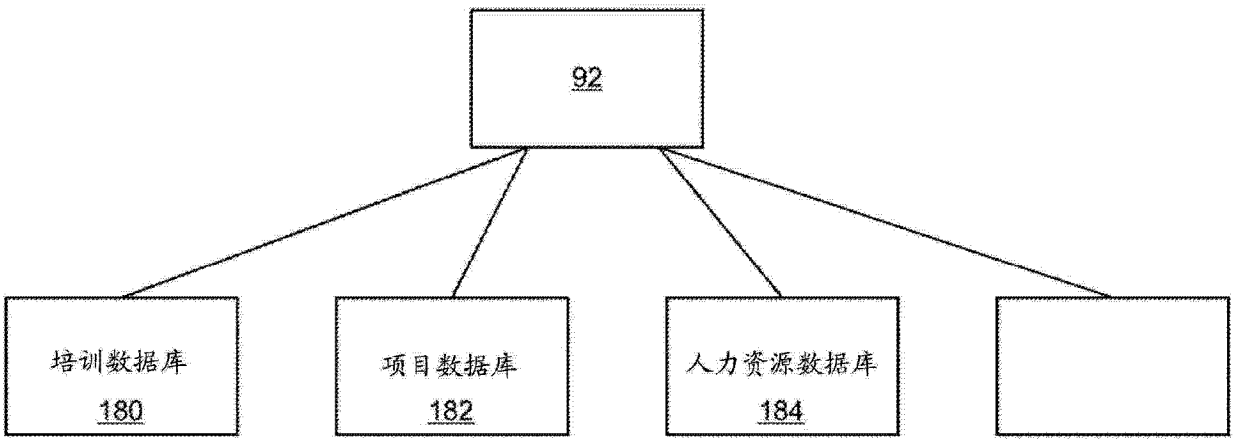

92
培训数据库
180
项目数据库
182
人力资源数据库
184

图 6

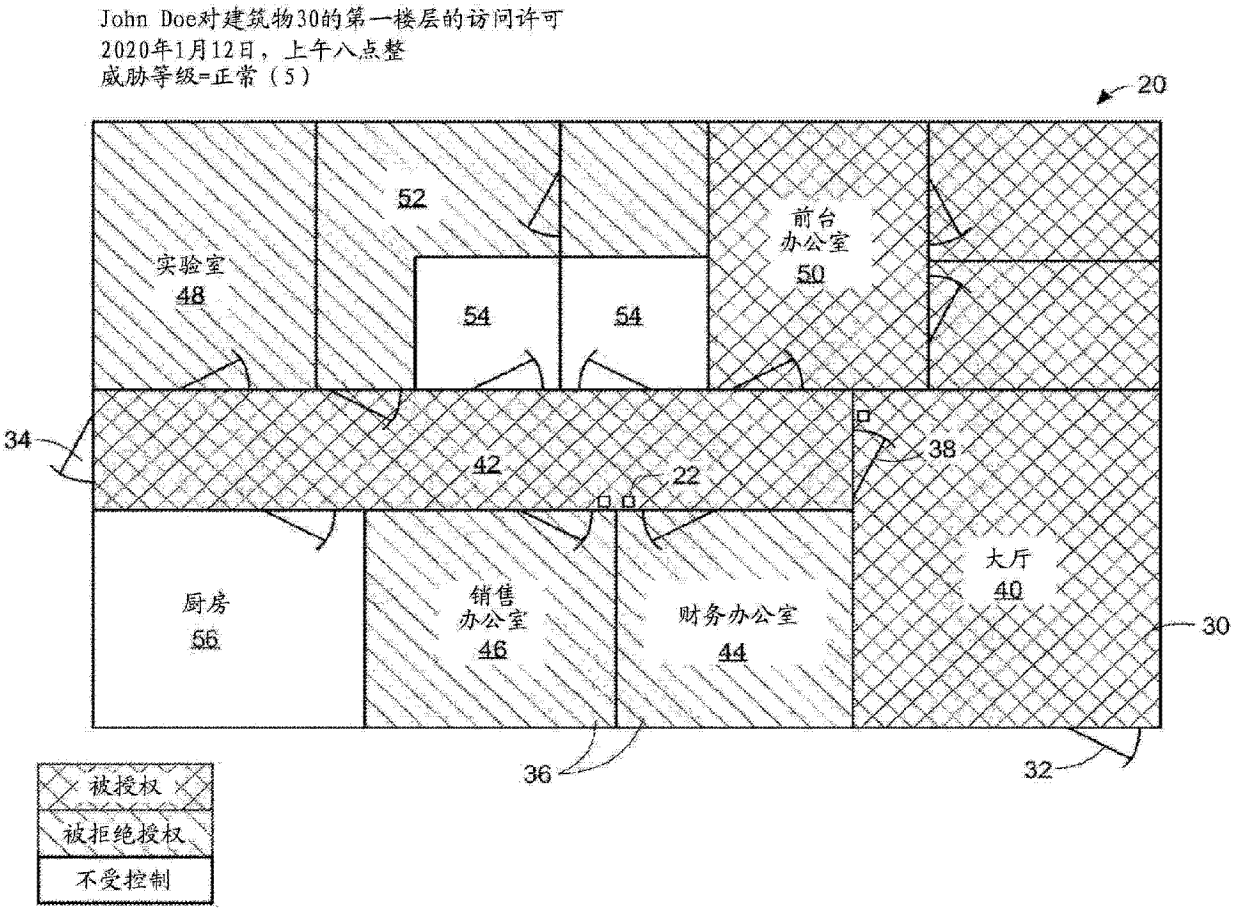

John Doe对建筑物30的第一楼层的访问许可
2020年1月12日，上午八点整
威胁等级=正常（5）
20
52
实验室
48
54
54
前台
办公室
50
34
42
22
38
厨房
56
销售
办公室
46
财务办公室
44
大厅
40
30
36
32
被授权
被拒绝授权
不受控制

图 7 图形实施方式

John Doe对建筑物30的第一楼层的访问许可
2020年1月12日，上午八点整
威胁等级=正常（5）

被授权:
- 大厅
- 前台办公室套房

被拒绝授权:
- 销售办公室
- 财务办公室
- 实验室

图 8 文本实施方式

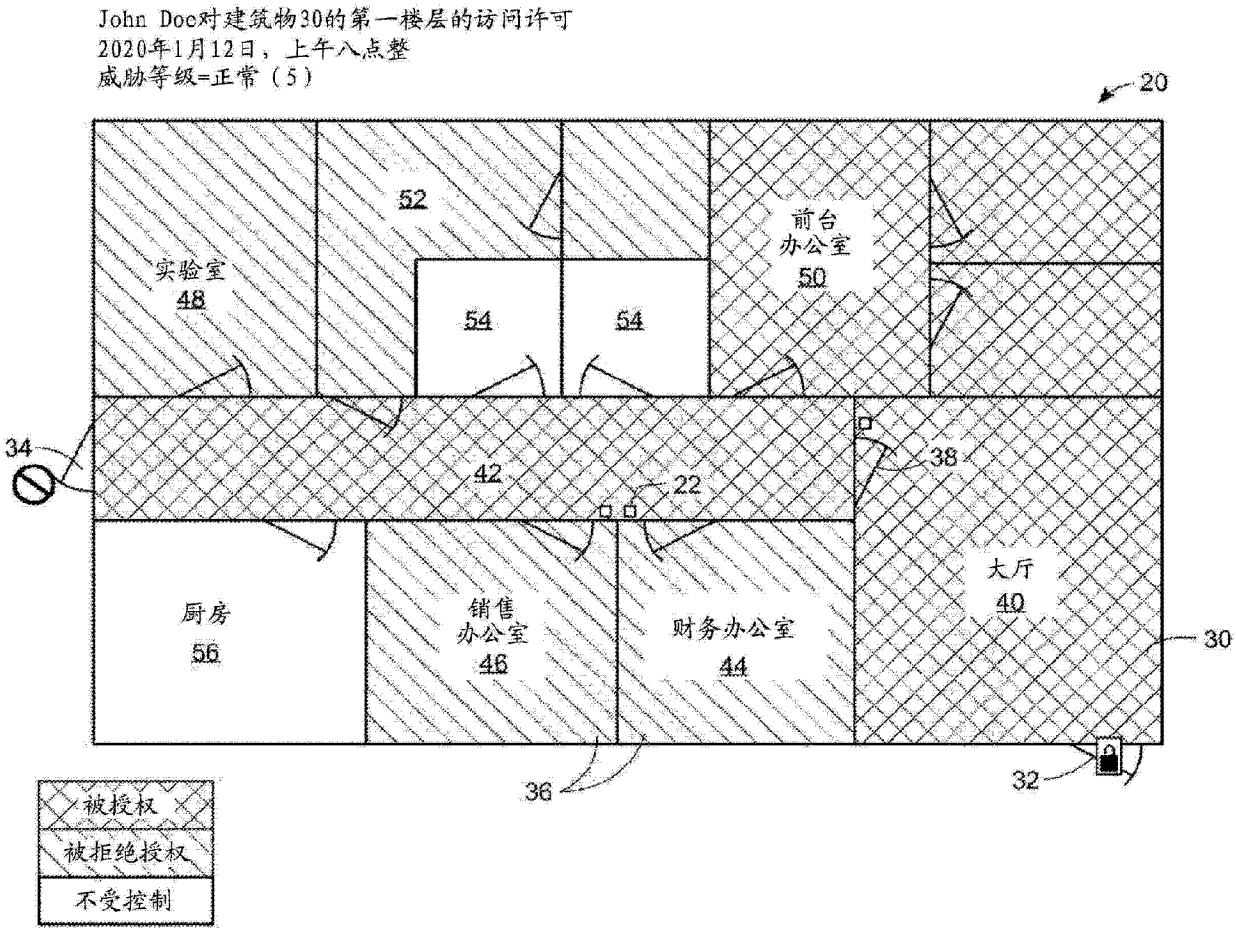


图 9 带有门超控的图形实施方式

John Doe对建筑物30的第一楼层的访问许可
2020年1月12日，上午八点整
威胁等级=正常（5）

被授权:
- 大厅
- 前台办公室套房

被拒绝授权:
- 销售办公室
- 财务办公室
- 实验室

超控（调度解锁）:
- 门32

超控（调度读取器被禁用）:
- 门34外侧

图 10 带有门超控的文本实施方式