(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 101847278 A
(43)申请公布日 2010.09.29

(21)申请号 201010176720.5

(22)申请日 2010.03.24

(30)优先权数据
12/410,613 2009.03.25 US

(71)申请人 霍尼韦尔国际公司
地址 美国新泽西州

(72)发明人 N·J·格纳 T·P·施米特

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王岳 蒋骏

(51)Int.Cl.
G07C 9/00(2006.01)

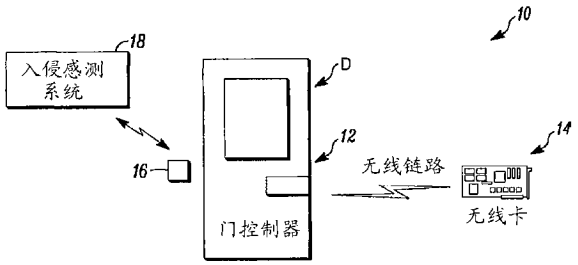
权利要求书 2 页 说明书 4 页 附图 6 页

(54)发明名称

受控区域中调整安全级别和发信号通知警报的系统和方法

(57)摘要

本发明涉及受控区域中调整安全级别和发信号通知警报的系统和方法。一种访问控制系统关于在区域中存在一个或多个个体而对用户的访问数据和信息二者进行响应。可自动确定经授权个体、或非授权个体、或入侵者已被检测到。可响应于寻求访问的个体的等级调整安全级别。



独立门控制器系统

CN 101847278 A

1. 一种系统包括：

至少一个传感器，能够指示接近于其的个体的存在；

访问控制单元，与该传感器相关联；以及

控制电路，耦合到该至少一个传感器和该单元，并且响应于其而调整所选择区域中的安全级别和警报状态。

2. 如权利要求 1 的系统，其中该控制电路可响应于具有第一许可级别的所识别人员的所检测存在，提高区域中的安全级别。

3. 如权利要求 1 的系统，其中该控制电路可响应于具有第一许可级别的所识别人员的所检测存在，降低区域中的安全级别。

4. 如权利要求 1 的系统，其中该访问控制单元对个体进行识别并且响应于经授权个体进入该区域，相关联的警报系统的状态不改变。

5. 如权利要求 1 的系统，其中响应于区域中的第一和第二个体的存在，且在一个个体比另一个体具有更高许可的情况下，降低内部的子区域中的安全级别。

6. 如权利要求 5 的系统，其中对子区域的访问由访问装置限制，该访问装置包括：

至少一个传感器，能够指示接近于其的个体的存在；

访问控制单元，与该传感器相关联；以及

控制电路，耦合到该传感器，并且响应于其而调整该子区域中的安全级别。

7. 如权利要求 1 的系统，其中该控制电路通过改变至少一个所选择区域的安全级别而对区域中的非授权个体的存在进行响应。

8. 如权利要求 1 的系统，其中该控制电路通过改变至少一个所选择区域的安全级别且通过授权访问一些区域及不授权访问其它区域而对区域中的入侵者的存在进行响应。

9. 如权利要求 1 的系统，其中该控制电路通过提高一个或多个所选择区域中的安全级别并改变所选择的警报状态来对所检测的安全和 / 或安全性标记和区域中的至少一个经授权个体的存在进行响应。

10. 一种方法包括：

定义具有第一安全级别的区域；

相对于该区域建立在第一状态下的入侵警报；

经由所选择的传感器，感测授权个体对区域进行访问的标记，并响应于其而允许对该区域的访问；以及

指示在传感器附近的个体的身份和存在并响应于其而保持在第一状态下的入侵警报。

11. 如权利要求 10 的方法，其包括感测在所选择的传感器附近的第一和第二个体的存在，并响应于个体之一比另一个体具有更高的安全级别，通过传感器来临时降低可访问区域中的安全级别。

12. 如权利要求 11 的方法，其中只有在个体的附近继续感测到具有更高安全级别的另一个体时安全级别才降低。

13. 如权利要求 10 的方法，其包括感测在区域中的非授权个体并响应于其而不授权该个体从该区域离开，并启动所选择的入侵警报状态。

14. 如权利要求 10 的方法，其包括感测事故事件并生成所选择的警报状态同时改变相应区域的安全级别。

15. 如权利要求 10 的方法，其包括感测指示区域中的安全和 / 或安全性的条件，并响应于其，改变各个区域的安全级别以便或者包含个体和该条件以使得个体能够离开他们否则可能不被允许离开的地方，或者为了恢复安全和 / 或安全性的某一级别而使得经授权人员能够访问。

受控区域中调整安全级别和发信号通知警报的系统和方法

技术领域

[0001] 本发明涉及区域访问控制(access control)系统和方法。更具体而言,本发明涉及这样的系统和方法,其中区域中的个体被感测和识别并响应于其,安全级别和区域的警报状态可被调整。

背景技术

[0002] 已知各种类型的门或区域的访问控制系统。在2008年4月10日公开的、名称为“Decentralized Access Control Framework(分散式访问控制框架)”的美国公开的专利申请No.2008/0086758A1中,公开了一个这样的系统。该'758申请转让给其受让人,并且通过引入结合于此。

[0003] 尽管已知的系统对于它们意图的目的而言是有效的,但仍然存在开放性问题(open issue)。例如,如果非授权持卡者已“随同(piggyback)”进入安全区域,传统的访问控制系统不能检测到,从而它们不能提高区域和子区域中的安全级别。此外,已知的入侵系统能够识别人员是否在安全区域,但它们不能准确识别该人员是否为有效持卡者。当职员工作到很晚时可能发生这种问题,并且当他/她仍在被监控的大楼或区域内时入侵系统被接通。最后,当有效持卡者进入区域时如果入侵系统被设置为解除,则区域内的安全级别被降低。

[0004] 会期望的是解决上述问题以便给所监控区域提供比当前可用的更有效的安全。还会期望的是以使得现有系统能够被升级的方式来做这些。

附图说明

[0005] 图1是体现了本发明的独立访问控制系统的图;

[0006] 图2是体现了本发明的多控制器系统的图;

[0007] 图3是可用于图1或2中的系统的门可安装访问控制单元的框图;

[0008] 图4是例示本发明的细节的所监控区域的图;

[0009] 图5-9例示了例如在图3中控制单元的处理的方面,其体现了本发明。

具体实施方式

[0010] 尽管本发明的实施例可采用许多不同的形式,但其特定实施例示出于图中并将在此按以下理解来详述:即本公开应认为是对本发明原理以及实践该原理的最佳模式的例示,而不意图将本发明限于所例示的特定实施例。

[0011] 在本发明公开的实施例中,识别区域内的持卡者和入侵者(intruder)。所识别的个体可分为授权的、非授权的或未识别出的入侵者。随后可基于(一个或多个)个体的识别和分类进行区域或区的控制。

[0012] 在不同的安全级别和警报状态下当个体进入、离开、和出现在所监控区域中时体现了本发明的方法对个体进行分类。根据于此可以自动建立这样的情形:其中可以指示特

定的警报状态，并且区域的安全级别可自动提高或降低。

[0013] 当已知人员经过一个或多个区域时体现了本发明的系统对其进行识别。通过各种形式的凭证 (credential) 来提供访问，这些包括但不限于，接触式或无线访问卡、或生理特征等等，不限于此。

[0014] 例如，在不离开本发明的精神和范围的情况下，可采用电池辅助无源 (BAP, battery-assisted passive) 访问卡。该访问卡可与区域中的门控制器以及访问点 (access point) 通信。如果访问卡与访问点通信，则认为持卡者在访问点的预定区域内。其他形式的识别装置落在本发明的精神和范围内。

[0015] 在另一个例子中，可采用生理的、或生物的识别装置例如固态照相机，而不离开本发明的精神和范围。该识别装置可与处理区域中的个体的生理数据的视频监视控制器通信。如果区域中的个体的生理数据与已知个体的预记录数据相匹配，则认为持卡者在生理识别装置的预定区域内。

[0016] 另外，可以确定在给定区域内个体的存在，无论他们是否是持卡者。根据本发明可采用运动、或入侵传感器。定位一个或多个入侵传感器以监控与相应的访问点或门控制器相同的区域。因此，可以检测到访问点或门周围的运动。

[0017] 根据本发明的实施例，可以定义由访问点和入侵传感器二者监控的区域和子区域。当入侵传感器检测到区域中的人员时，系统可将该个体归入三种类别中的一个：

[0018] 经授权个体是携带有效凭证（例如卡）的人员，并被允许在该区域中；

[0019] 非授权个体是携带可识别凭证（例如卡）的人员，但是不被允许在该区域中；

[0020] 未识别个体是没有凭证的人员，例如入侵者。

[0021] 根据个体的分类，本发明的实施例可控制警报状态或改变区域或区域组的安全级别。例如，如果经授权人员在该区域中移动，则该区域和它的子区域的安全级别可保持不变。在本发明的一方面中，当有效人员在区域中时，该区域的入侵警报系统不需要被禁用。由经授权人员的移动而生成的任何事件将被分流 (shunt) 并且不发出或传送到公共控制单元或其他控制单元，例如入侵控制器或视频监视控制器。

[0022] 在本发明的另一方面，子区域的（一种或多种）安全级别可以由特定的经授权个体的存在而控制。例如，当主管人员在药箱的特定距离内时药房中药箱的安全级别可降低，该降低可开启药箱或允许学员的访问。随后当主管人员远离药箱时安全级别可自动再次提高。

[0023] 在本发明的另一方面，如果非授权人员进入高安全区域或子区域，则该区域可锁定 (lock down)，例如，非授权人员可“随同”授权人员通过入口且得以访问安全区域。如果发生这种情况，根据本发明，区域的安全级别可自动提高到在安全区域及其子区域中的“锁定”级别。另一方面，如果非授权人员在安全区域中，入侵警报和视频监视控制器的覆盖范围和响应可被改变。

[0024] 可替代地，体现了本发明的系统或方法可基于检测到入侵者提高区域或区域组的安全级别。当在区域中检测到运动，且在该区域中没有经授权个体时发生该事件，该安全级别可提高到“锁定”级别，并发出警报。

[0025] 在另一实施例中，可响应于“事故 (distress)”或人员紧急事件的触发而在区域或区中提高安全级别或发出警报。通常响应于意外物理危险或故意暴力而由需要紧急救助

的个体手动触发这些事件。然而这些事件也可由人员工业危害的发生（例如坠落停制装置(fall arresting gear)的激活）而触发。事故事件也可以用本领域技术人员会理解的其他各种方式而触发。

[0026] 在另一实施例中，在区域之间控制安全级别以防止威胁与携带凭证的人员的交互作用。可通过生成已知警报的辅助系统或入侵系统识别该威胁。例如，如果在建筑物的区域中识别出火灾，则控制安全级别使得携带凭证的人员仅可离开该区域并且不得进入。也可控制其他区域的安全级别，这将用可能最快的方法将所有携带凭证的人员集中到安全区域。可发起该自动的安全级别控制的威胁的其他示例可包括武装入侵者、化学溢出物或污染物，不限于此。同样地，也可控制其他区域的安全级别，以便启用针对这些事件紧急响应者(emergencyresponder)所需的访问和基础设施（例如照明、HVAC，等）以便重新建立安全和/或安全性(safety)。

[0027] 图1示出了体现了本发明的独立系统10的的一种形式。在系统10中，无线门控制器安装在门D上以控制对区域（该区域由门D关闭或封闭）的访问。无线卡14可用于使控制器12放开(release)或解锁门D以供拥有卡14的个体的访问。

[0028] 在独立的模式下，如图1中，入侵检测系统18的关联的传感器16可检测到门D附近的一个或多个个体/入侵者的存在。如下所述，传感器16可结合到可无线地或通过有线媒介耦合到系统18的控制器12中。

[0029] 图2示出了多门/区域访问控制系统20。系统20包括门D1承载的无线门控制器22，门D1提供了对各个区域的访问。

[0030] 除响应于无线访问卡24以提供对相应区域的访问外，控制器22还可通过中继器28a、b与控制单元或面板30进行无线通信。应当理解，控制器22可基本上在独立的模式下操作，并且通过门D1提供访问并且向单元30馈给访问相关的数据，或向单元30传送关于卡24的信息，以获得放开门D1的授权，不限于此。

[0031] 控制单元30可包括控制电路32。电路32可部分由可编程处理器32a、由处理器32a执行的相关联的控制软件32b和与控制器22通信的无线接口32c来实现。系统20也可包括通常在36处表示的多个附加控制器，其提供对与控制器22所进行的相比不同的区域的访问。

[0032] 一个或多个入侵传感器（例如运动传感器28）可位于访问控制器22的附近，或配置为控制器22的一部分。传感器（例如传感器28）可耦合到入侵感测系统，例如系统40，其也可与控制面板30通信。耦合到一个或两个系统30、40的火灾警报系统（例如44）可在被监控区域指示了所检测的非授权个体时提供可听/可视警报。

[0033] 图3是示例性控制器40的框图，可与控制器20、22、36相比较。控制器40可包括门可安装外壳42。外壳42可承载控制电路44，其可包括经编程处理器46a和相关连的无线电设备或收发器46b用于通过天线46c进行无线通信。

[0034] 外壳42还可承载短距离电容式运动传感器48a和远距离运动传感器，例如无源红外型传感器48b。个体的其他类型的传感器（例如热传感器、具有相关联的处理以检测运动的固态照相机，不限于此）都在本发明的精神和范围内。此外如上述指出的，这些传感器可以但不必结合到相应的访问控制单元内。

[0035] 来自一个或两个传感器48a、b的输出与来自相关联的无线卡（例如14，或24）的

信息结合在一起可以被电路 44 用于确定相应的门（例如 D 或 D1）是否应被放开，或访问级别是否应被改变，如以上根据本发明所捕述的。这些传感器也可与本地处理或入侵感测系统 40 的处理相结合地用于识别入侵者。在感测到运动、但携带授权凭证的人员没有在该区域中，则该运动将会是由入侵者引起的。

[0036] 应当理解的是控制器 40 仅是例示性的，且其他变型或配置，包括有线控制器，都在本发明的精神和范围内。类似地，用于获得访问的卡的类型的具体细节不是对本发明的限制。例如，RFID 型卡以及光或磁卡都在本发明的精神和范围内。

[0037] 图 4-9 示出了体现了本发明的方法或处理，并且其可由控制器（例如控制器 40）执行。图 4 示出了多个受控区域或区。区域 1,2 表示相对低的安全区域，区域 3,4 表示更高的安全区域。区域 1-4 通过各个入口而被访问，该各个入口提供了经由一个或多个各自的门（例如 D 或 D1）的访问。每个入口具有相关联的访问控制系统（例如单元 22-I）和至少一个本地入侵或运动传感器（例如 28-I,），如以上相对于图 2、3 所述的。

[0038] 如上所述，访问控制单元 22-I 可以耦合（有线或无线地）到控制单元 30。入侵传感器可耦合到系统 40。传感器 28-I 可包括在各自的访问控制单元 22-i 中或偏离各自的访问控制单元 22-i。本领域技术人员应当理解，可在整个区域 1-4 适当安装多个入侵传感器而不超出本发明的精神和范围。如图 4 中所示，图 5-9 中示出的区域包括访问控制单元和入侵传感器。

[0039] 图 5 示出了当经授权的个体或持卡者存在时区域和它的子区域的安全级别可保持不变。传感器（例如 28-i）与来自相应卡（例如 24）和访问控制单元 22-I 的信息相结合可以使持卡者能进入具有有效的 (active) 入侵警报的区域但不引起警报。

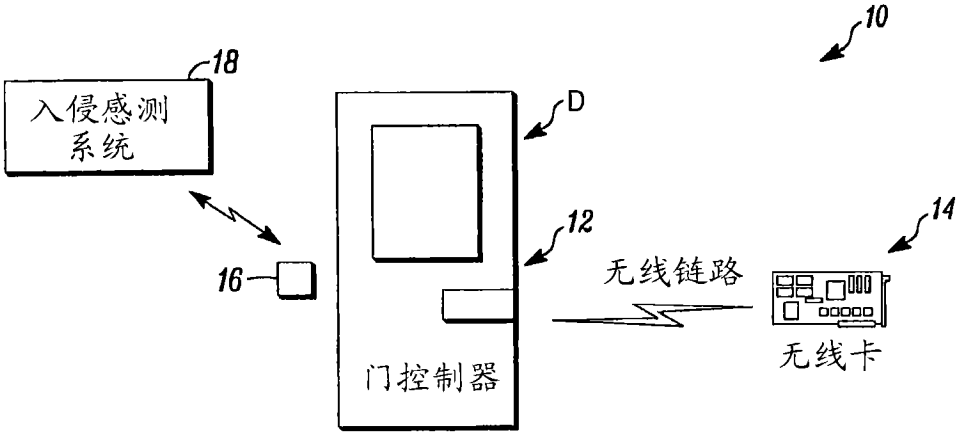
[0040] 图 6 示出了响应于经授权个体的存在而对子区域的安全级别的控制。具有更高安全级别的个体可改变子区域的安全级别从而使得更低安全级别的人员可访问内部的、更高安全区域，但仅在具有高安全级别的人存在时如此。

[0041] 图 7 示出了响应于非授权持卡者进入区域（也许与具有更高安全级别的人员一起）而锁定高安全区域或（一个或多个）子区域。图 8 示出了在检测到入侵者时锁定和提高区域的安全级别。图 9 示出了在入侵者接近更高安全的个体以获得对安全区域的访问的情况下提高区域中的安全或生成警报，且更高安全级别的个体可创建向单元 40 报警的“事故事件”。

[0042] 对基于卡的访问控制单元（例如 22-i）的替代也都在本发明的精神和范围内。这些包括但不限于具有键盘的访问控制单元，或这样的单元，其识别个体的一个或多个生理的或生物的特征，例如指纹、视网膜纹 (retinal print)、脸部特征、语音等等，都没有限制。传感器可包括但不限于视频或其他形式的照相机。

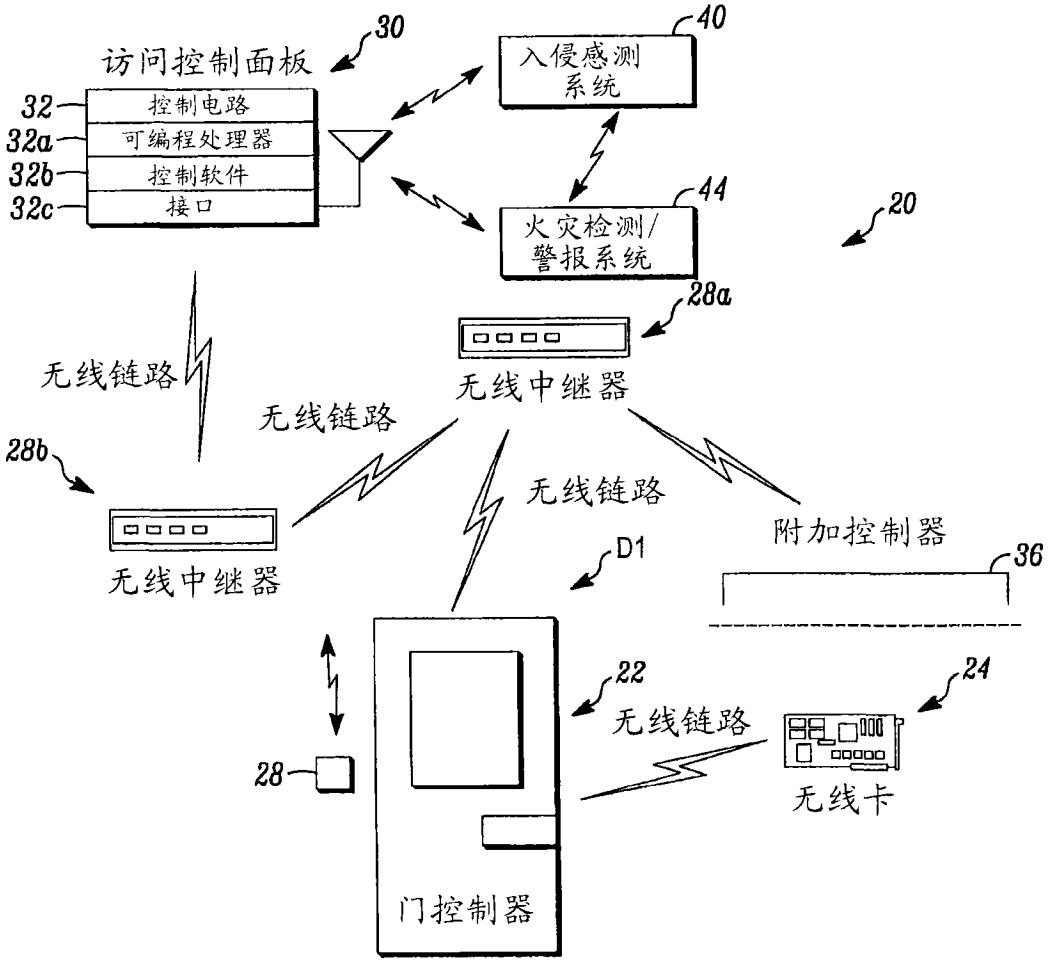
[0043] 因此，本发明的实施例可感测到个体的存在。接着个体可被识别。采用一个或多个传感器而不超出本发明的精神和范围。这些传感器的细节不是对本发明的限制。

[0044] 从前所述，应观察到可实施多种变型和修改而不超出本发明的精神和范围。应当理解的是，针对此处示出的特定装置，不意图限制或不应推断为限制。当然，意图由所附权利要求覆盖落入权利要求的范围内的所有这些修改。



独立门控制器系统

图 1



有访问控制主机的门控制器系统

图 2

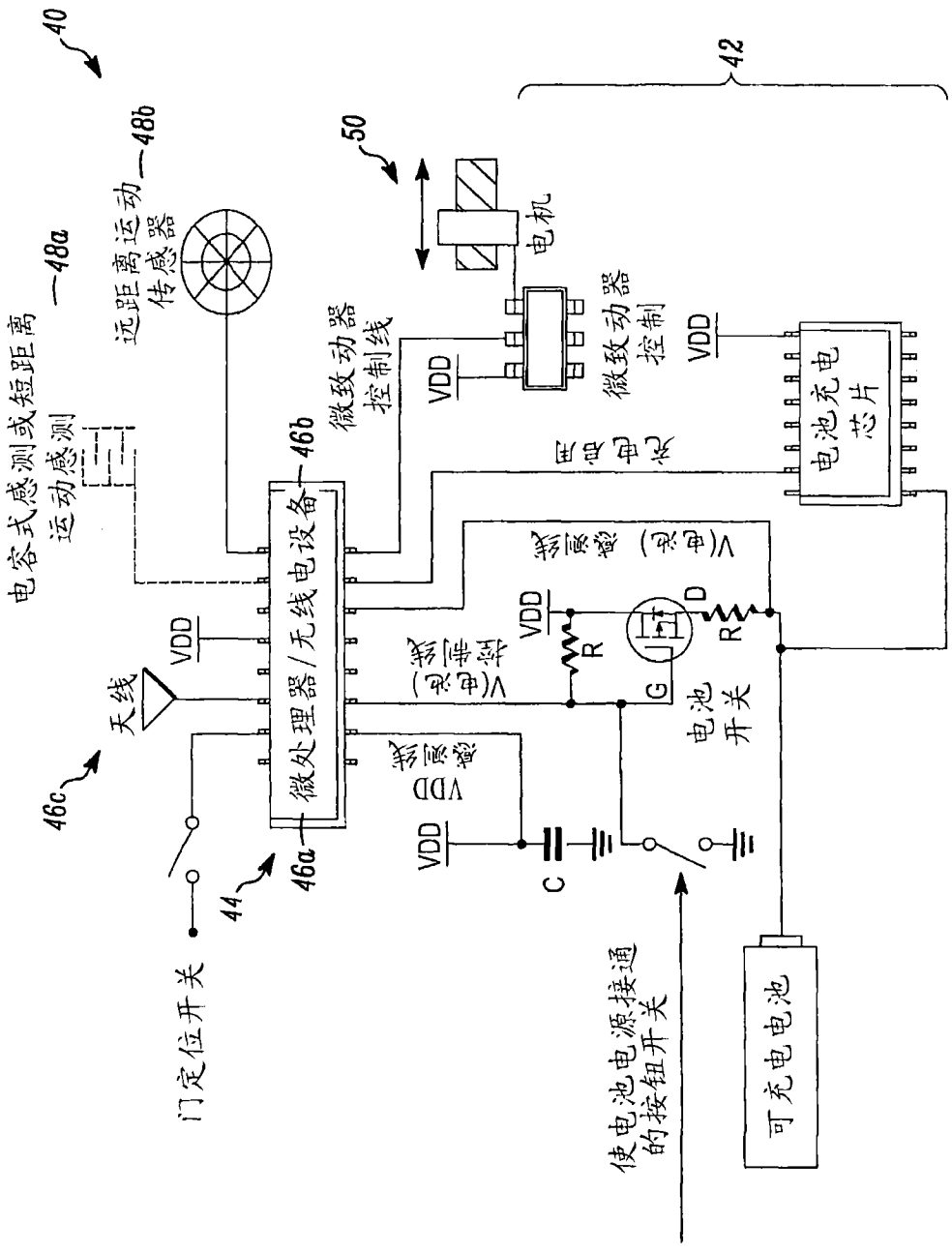

40
42
50
48b
远距离运动传感器
48a
电容式感测或短距离运动感测
电机
微致动器控制线
VDD
微致动器控制
VDD
电池充电芯片
46b
微处理器/无线电设备
天线
VDD
46c
46a
44
门定位开关
VDD
C
R
G
D
R
电池开关
使电池电源接通的按钮开关
可充电电池

图 3

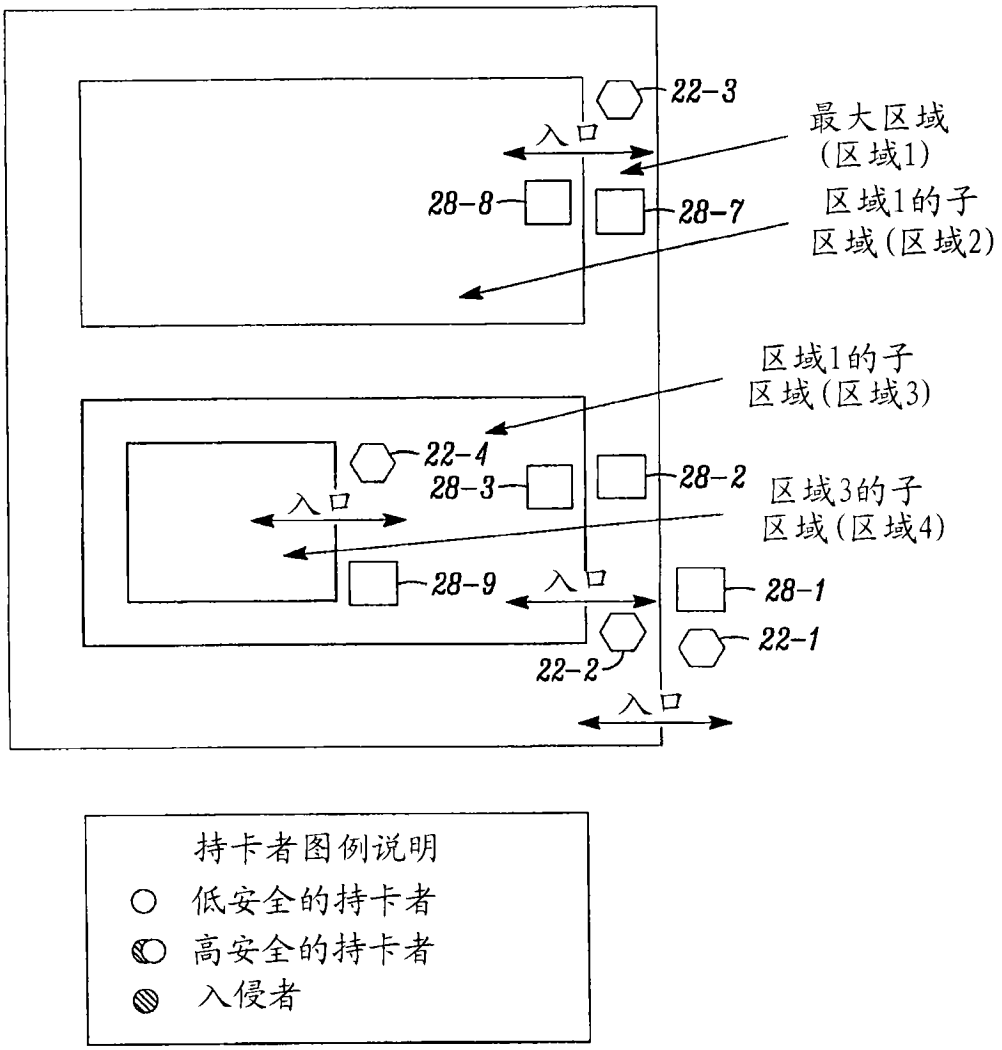

22-3
入口
最大区域
(区域1)
28-8
28-7
区域1的子
区域(区域2)
区域1的子
区域(区域3)
22-4
28-3
28-2
入口
区域3的子
区域(区域4)
28-9
入口
28-1
22-1
22-2
入口
持卡者图例说明
低安全的持卡者
高安全的持卡者
入侵者

图 4

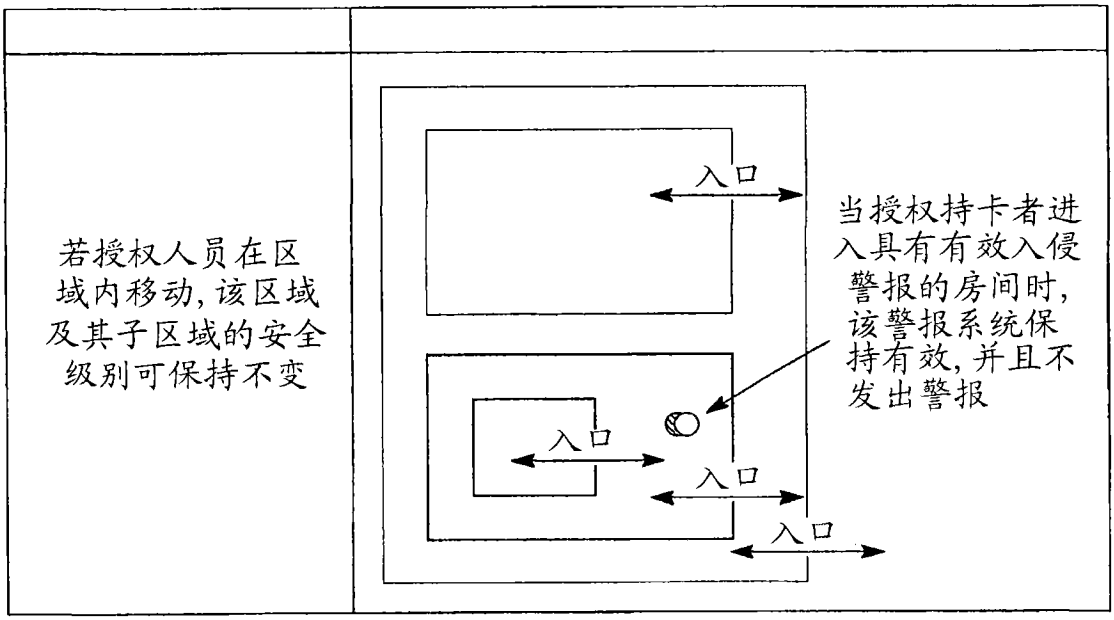

若授权人员在区域内移动，该区域及其子区域的安全级别可保持不变
入口
当授权持卡者进入具有有效入侵警报的房间时，该警报系统保持有效，并且不发出警报
入口
入口
入口

图 5

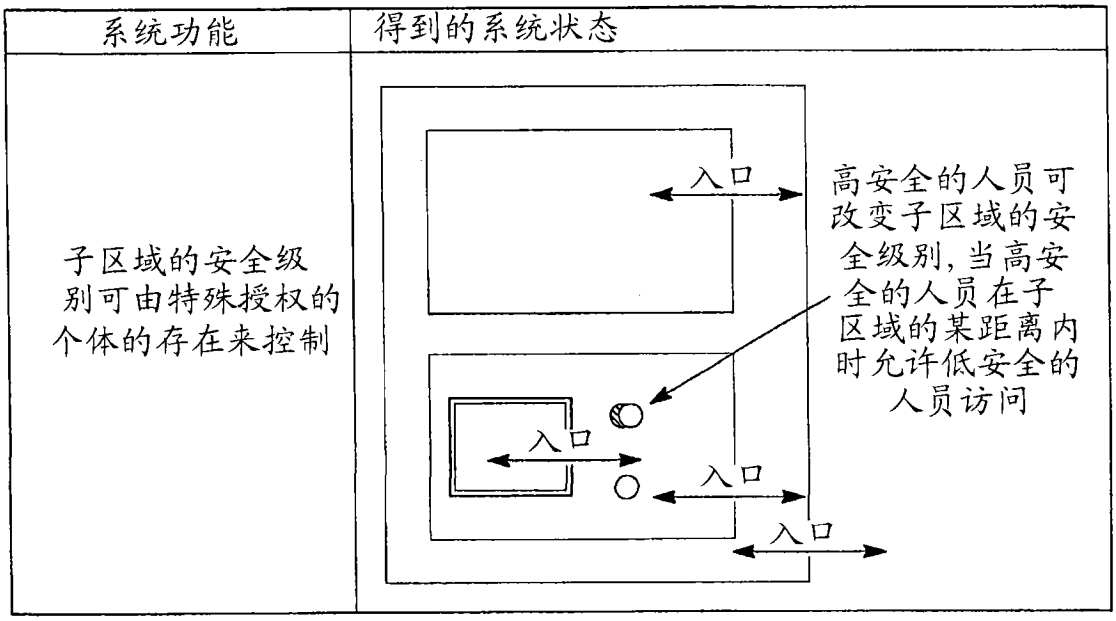

系统功能
得到的系统状态
子区域的安全级别可由特殊授权的个体的存在来控制
入口
高安全的人员可改变子区域的安全级别，当高安全的人员在子区域的某距离内时允许低安全的人员访问
入口
入口
入口

图 6

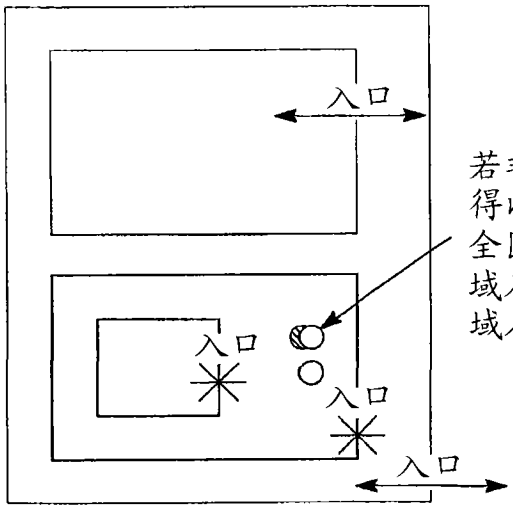
系统功能	得到的系统状态
若非授权持卡者进入高安全区域或子区域，该区域被锁定	

图 7

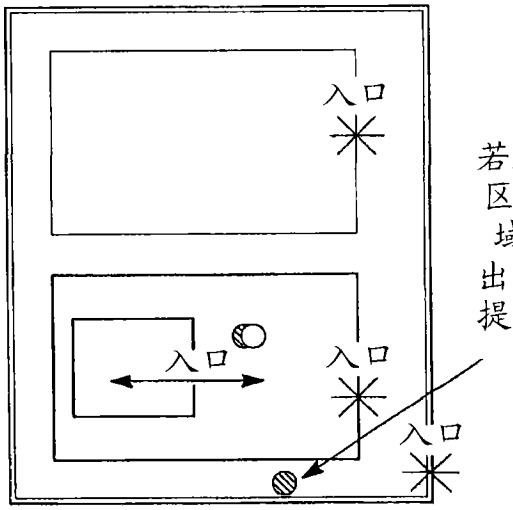
系统功能	得到的系统状态
检测到入侵者时，区域或区域组可提高安全级别	

图 8

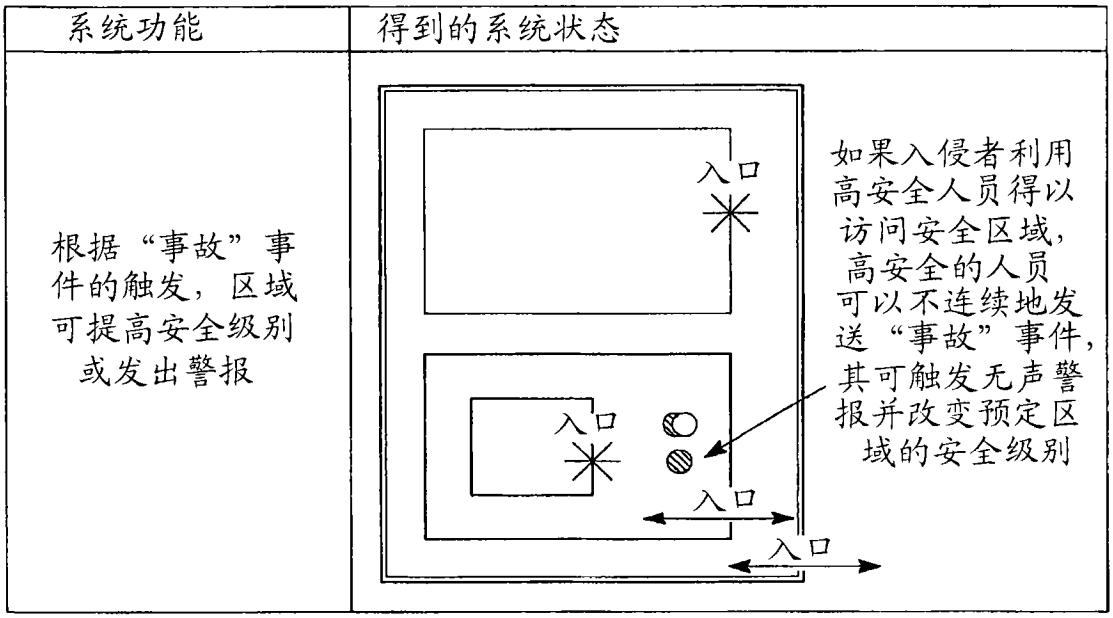

系统功能
得到的系统状态
根据“事故”事件的触发，区域可提高安全级别或发出警报
入口
入口
入口
入口
如果入侵者利用高安全人员得以访问安全区域，高安全的人员可以不连续地发送“事故”事件，其可触发无声警报并改变预定区域的安全级别

图 9