(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 103685296 A
(43)申请公布日 2014.03.26

(21)申请号 201310714365.6

(22)申请日 2013.12.20

(71)申请人 中电长城网际系统应用有限公司
地址 102200 北京市昌平区科技园区超前路37号6号楼四层1108号

(72)发明人 刘恒 廖飞鸣 黄凯峰 陈洪波 黄玉金

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 彭瑞欣 张天舒

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)
G06F 21/50(2013.01)

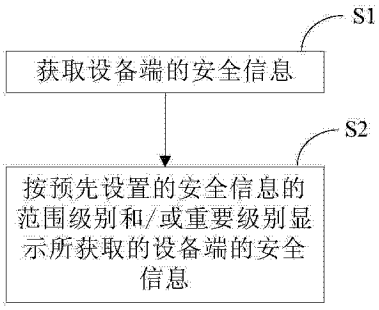
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种安全信息整合显示方法和系统

(57)摘要

本发明提供一种安全信息整合显示方法，该方法包括：S1、获取设备端的安全信息；S2、按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息。相应地，本发明还提供一种安全信息整合显示装置。本发明能够根据需要自定义地整合显示不同级别的安全信息，能够实现整合显示企业安全信息的企业数字地图。与现有技术相比，本发明更加便于对企业内部各设备、网络和文件的安全状况进行监视和管理。



CN 103685296 A

1. 一种安全信息整合显示方法，其特征在于，所述安全信息整合显示方法包括：

S1、获取设备端的安全信息；

S2、按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息。

2. 根据权利要求 1 所述的安全信息整合显示方法，其特征在于，所述安全信息包括：所述设备端的安全防护系统监测到的安全事件信息和/或所述设备端上存储的预设电子文件。

3. 根据权利要求 2 所述的安全信息整合显示方法，其特征在于，所述 S2 之前还包括：

S02、根据预先设定的所述设备端的安全防护系统的身份标识对应的范围级别和/或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和/或重要级别。

4. 根据权利要求 3 所述的安全信息整合显示方法，其特征在于，所述 S02 还包括：根据预先设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别。

5. 根据权利要求 1 至 4 中任意一项所述的安全信息整合显示方法，其特征在于，所述 S2 之后，还包括：

S3、向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

6. 一种安全信息整合显示系统，其特征在于，所述安全信息整合显示系统包括：

设备连接单元，用于获取设备端的安全信息；

显示管理单元，用于按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息。

7. 根据权利要求 6 所述的安全信息整合显示系统，其特征在于，所述安全信息包括：所述设备端的安全防护系统监测到的安全事件信息和/或所述设备端上存储的预设电子文件。

8. 根据权利要求 7 所述的安全信息整合显示系统，其特征在于，所述安全信息整合显示系统还包括：

级别设定单元，用于设定所述设备端的安全防护系统的身份标识对应的范围级别和/或重要级别；

信息处理单元，用于根据所述级别设定单元设定的所述设备端的安全防护系统的身份标识对应的范围级别和/或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和/或重要级别。

9. 根据权利要求 8 所述的安全信息整合显示系统，其特征在于，所述级别设定单元还用于设定所述电子文件的身份标识对应的重要级别；

所述信息处理单元还用于根据所述级别设定单元设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别。

10. 根据权利要求 6 至 9 中任意一项所述的安全信息整合显示系统，其特征在于，所述显示管理单元还用于向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

一种安全信息整合显示方法和系统

技术领域

[0001] 本发明涉及计算机安全技术领域，尤其涉及一种安全信息整合显示方法和系统。

背景技术

[0002] 如今，人们对于网络和计算机的安全防护意识日益增强，公司或企业会引入多种安全防护系统以保证计算机等设备的安全性，这些安全防护系统包括防火墙、入侵检测系统、防病毒软件等。随着安全防护系统的不断增加，对安全防护系统的统一管理也越加困难。现有的安全管理系统大多都是集中显示各个设备上的安全信息，当企业中需要管理的设备数量较多时，终端显示界面上将会显示众多设备的安全信息，因而存在着管理困难、难以对发生安全事件的设备进行快速定位等问题。

[0003] 因此，需要提出一种方法，能够以自定义的层次或级别的获取并显示企业中各设备的安全信息。

发明内容

[0004] 本发明的目的在于提供一种安全信息整合显示方法和系统，以能够按照预设的安全信息的范围级别和／或重要级别来显示对应的安全信息。

[0005] 为实现上述目的，本发明提供一种安全信息整合显示方法，所述安全信息整合显示方法包括：

[0006] S1、获取设备端的安全信息；

[0007] S2、按预先设置的安全信息的范围级别和／或重要级别显示所获取的设备端的安全信息。

[0008] 优选地，所述安全信息包括：所述设备端的安全防护系统监测到的安全事件信息和／或所述设备端上存储的预设电子文件。

[0009] 优选地，所述 S2 之前还包括：

[0010] S02、根据预先设定的所述设备端的安全防护系统的身份标识对应的范围级别和／或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和／或重要级别。

[0011] 优选地，所述 S02 还包括：根据预先设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别。

[0012] 优选地，所述 S2 之后，还包括：

[0013] S3、向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

[0014] 相应地，本发明还提供一种安全信息整合显示系统，所述安全信息整合显示系统包括：

[0015] 设备连接单元，用于获取设备端的安全信息；

[0016] 显示管理单元，用于按预先设置的安全信息的范围级别和／或重要级别显示所获

取的设备端的安全信息。

[0017] 优选地，所述安全信息包括：所述设备端的安全防护系统监测到的安全事件信息和/或所述设备端上存储的预设电子文件。

[0018] 优选地，所述安全信息整合显示系统还包括：

[0019] 级别设定单元，用于设定所述设备端的安全防护系统的身份标识对应的范围级别和/或重要级别；

[0020] 信息处理单元，用于根据所述级别设定单元设定的所述设备端的安全防护系统的身份标识对应的范围级别和/或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和/或重要级别。

[0021] 优选地，所述级别设定单元还用于设定所述电子文件的身份标识对应的重要级别；

[0022] 信息处理单元还用于根据所述级别设定单元设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别。

[0023] 优选地，所述显示管理单元还用于向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

[0024] 可以看出，本发明通过获取各设备端的安全信息，并预先设定安全信息的范围级别和/或重要级别，能够自定义地根据需要整合显示不同级别的安全信息。与现有技术相比，本发明使得企业安全管理人员能够从总体上直观地了解整个企业的信息安全状况，且更加便于对企业内部各设备、网络和文件的安全状况进行监视和管理，同时，还能够便捷地命令设备端的安全防护系统执行相应操作。

附图说明

[0025] 附图是用来提供对本发明的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本发明，但并不构成对本发明的限制。在附图中：

[0026] 图 1 为本发明所提供的安全信息整合显示方法流程图；

[0027] 图 2 为本发明所提供的安全信息整合显示方法另一流程图；

[0028] 图 3 为本发明所提供的安全信息显示级别划分示例图；

[0029] 图 4 为本发明所提供的安全信息整合显示系统示例图。

[0030] 附图标记说明

[0031] 10- 设备连接单元；20- 显示管理单元；30- 信息处理单元；40- 级别设定单元。

具体实施方式

[0032] 以下结合附图对本发明的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本发明，并不用于限制本发明。

[0033] 作为本发明的一个方面，提供一种安全信息整合显示方法，如图 1 所示，该方法可以包括：

[0034] S1、获取设备端的安全信息；

[0035] S2、按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息。

[0036] 本发明所提供的方法可以应用于整合显示企业或公司内部多个设备的安全信息。具体地，可以先通过 S1 获取企业或公司内部的各个设备的安全信息，并且，在 S2 中可以将获取的安全信息根据预先设置的安全信息的范围级别进行整合显示；或者，可以根据预先设置的安全信息的重要级别进行整合显示；或者，可以同时根据预先设置的安全信息的范围级别和重要级别进行整合显示。其中，可以根据各安全信息的来源所归属的范围来设定各安全信息的范围级别，可以根据安全信息的内容和性质来判断和定义各安全信息的重要级别。例如，若某一安全信息来源于某一企业的北京分公司的财务部的 PC 机（假设该 PC 机名称为 PC1），则该安全信息的范围级别可以设定为：公司级 / 北京分公司 - 部门级 / 财务部 - 设备级 /PC1；又如，某一普通办公用的 PC 机上的防病毒软件的安全信息的重要级别可以设定为“一般”，而某一涉及商业计划的 PC 机上的防病毒软件的报告的安全信息（如发现严重安全漏洞）的重要级别可以设定为“重要”。可以理解的是，上述仅为本发明所提供的示例，对于安全信息的范围级别和重要级别的设定方法可以根据需要进行设定，本发明对此不作限制。

[0037] 通过上述方法，能够使得在显示时，可以自定义地选择范围级别和 / 或重要级别来显示对应的安全信息，能够便捷地对整个企业内部的安全状况进行监视和管理。

[0038] 更进一步地，本发明上述 S1 中所获取的设备端的安全信息可以包括：所述设备端的安全防护系统监测到的安全事件信息和 / 或所述设备端上预设的电子文件。

[0039] 具体地，可以获取各个设备端的安全防护系统监测到的安全事件信息，以便于获取整个企业内部各设备以及网络的安全状况。其中，设备端的安全防护系统可以但不限于包括：防火墙，入侵检测系统，防病毒软件，数据防泄漏产品等。在获取各安全防护系统监测到的安全事件信息时，可以通过利用各安全防护系统的对外接口采集各安全防护系统的所记录的日志信息来实现。

[0040] 同时，还可以获取设备端上预设的电子文件。具体地，可以在获取设备端的安全信息时，获取预设的记录了企业重要信息的电子文件，以能够监视该些电子文件的安全状况，其中，上述企业电子文件中所记录的重要信息可以但不限于包括：程序源代码、商业计划、人员信息、财务状况等。可以预先保存设备端上相关电子文件的路径或者文件名，在获取该些电子文件时，可以直接到相关路径进行采集，或者检索与预存的文件名匹配的文件并采集该文件来实现。

[0041] 更进一步地，如图 2 所示，在 S2 之前还可以包括：

[0042] S02、根据预先设定的所述设备端的安全防护系统的身份标识对应的范围级别和 / 或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和 / 或重要级别。

[0043] 可以预先设定各个设备端上的安全防护系统所对应的范围级别和 / 或重要级别。具体地，可以预先设定各安全防护系统的身份标识（如名称、ID 等）与范围级别和 / 或重要级别的对应关系，其中，范围级别可以根据安全防护系统的来源归属的层级进行设定，而重要级别则可以根据安全防护系统的性质和检测到的安全事件的威胁等级进行设定，例如，若某一普通办公用的 PC 机上的防病毒软件发现该 PC 机存在漏洞，可以认为该安全事件的威胁较小，其对应的重要等级可以为“一般”，而若某一涉及商业计划的 PC 机上的防病毒软件的报告该 PC 机上存在木马，则可以认为该安全事件的威胁较大，其对应的重要等级可以

为“重要”。在获取安全防护系统监测到的安全事件信息后，可以根据所获取的安全防护系统监测到的安全事件信息中所包括的产生该安全事件信息的安全防护系统的身份标识，确定该安全事件信息来源于哪一个安全防护系统，同时，确定该安全事件信息的范围级别和/或重要级别。

[0044] 更进一步地，上述 S02 中还可以包括：根据预先设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别。

[0045] 在预先设定在获取安全信息的步骤中所要获取的电子文件时，可以同时设定该电子文件对应的重要级别，电子文件的重要级别可以根据电子文件的内容进行设定，例如，若某一电子文件记录的为某一部门的人员信息，则该电子文件的重要级别可以设定为“重要”；若某一电子文件记录的为某一分公司的财务信息，则该电子文件的重要级别可以设定为“非常重要”。可以理解的是，上述仅为本发明所提供的示例，对于电子文件的重要级别的设定方法可以根据需要进行设定，本发明对此不作限制。

[0046] 具体地，可以预先设定电子文件的身份标识（如电子文件的名称、ID、保存路径等）与重要级别的对应关系，在获取了电子文件后，可以根据电子文件身份标识确定该电子文件的显示级别。

[0047] 通过上述方法，能够获取企业中各设备端的安全防护系统监测到的安全事件信息以及预设的电子文件，同时，能够确定所获取的安全事件信息以及电子文件的显示级别。图 3 为本发明所提供的范围级别划分示例图，如图 3 所示，可以将所获取的安全信息的级别分为文件级、设备级、部门级和公司级，其中，安全防护系统监测到的安全事件信息的级别可以为公司级、或部门级、或设备级，而电子文件（包括重要文件和事件报告）也可以设定对应范围级别，例如可以设定为文件级。同时，安全信息的范围级别可以形成为层级归属关系，以便于在显示时能够整体显示某一范围层级内安全信息。

[0048] 例如，对于北京分公司研发部内的设备上的安全防护系统监测到的安全事件信息的范围级别可以为：公司级/北京分公司-部门级/研发部-设备级/设备名称，而对于北京分公司研发部内的设备上的预设的电子文件的范围级别可以为：公司级/北京分公司-部门级/研发部-设备级/设备名称-文件级/文件名称。在显示时，可以选择显示公司级别的安全信息，以查看北京分公司或上海分公司内部整体的安全信息，或者，可以选择具体某一部门的安全信息进行查看，例如，可以选择部门级别中北京分公司研发部以查看该部门整体的安全信息，或者，可以选择设备级查看某一设备上的安全防护系统监测到的安全事件信息或该设备上的电子文件，或者可以选择文件级来具体查看具体的电子文件。上述各范围级别在显示时可以逐级递进，例如，在显示设备级的安全信息时可以向下进一步显示文件级的安全信息，或者向上返回显示部门级的安全信息。此外，在显示某一范围级别的安全信息时，还可以同时显示安全信息的重要级别。可见，如图 3 所示，通过本发明能够实现企业安全信息数字地图显示系统，能够便捷地对企业内部的安全信息进行监视和管理。

[0049] 可以理解的是，上述仅为本发明所提供的应用示例，本发明的应用范围不限于此。

[0050] 更进一步地，如图 2 所示，上述方法中在 S2 之后，还可以包括：

[0051] S3、向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

[0052] 在整合显示了所获取的安全信息之后，还可以对设备端的安全防护系统发送操作命令，使安全防护系统执行相应操作。具体地，可以通过各安全防护系统的对外接口向各安全防护系统发送相关操作命令。通过上述方法，不仅能够集中显示所获取的安全信息，还能根据所获取的安全信息控制安全防护系统执行相关操作。例如，若某一 PC 机的防病毒软件报告了某一文件存在危险，则可以命令该防病毒软件删除该文件。

[0053] 上述为对本发明所提供的方法进行的描述，可以看出，本发明通过获取各设备端的安全信息，并预先设定安全信息的范围级别和 / 或重要级别，能够自定义地根据需要整合显示不同级别的安全信息。与现有技术相比，更加便于对企业内部各设备、网络和文件的安全状况进行监视和管理，同时，还能够便捷地命令设备端的安全防护系统执行相应操作。

[0054] 作为本发明的另一方面，提供一种安全信息整合显示系统，如图 4 所示，该安全信息整合系统可以包括 ：

[0055] 设备连接单元 10，用于获取设备端的安全信息 ；

[0056] 显示管理单元 20，用于将所述设备连接单元 10 所获取的设备端的安全信息按预先设置的范围级别和 / 或重要级别进行显示。

[0057] 更进一步地，上述设备连接单元 10 所获取设备端的安全信息可以包括 ：所述设备端的安全防护系统监测到的安全事件信息和 / 或所述设备端上存储的预设电子文件。

[0058] 更进一步地，该安全信息整合显示系统还可以包括 ：信息处理单元 30 和级别设定单元 40，其中，级别设定单元 40 用于设定所述设备端的安全防护系统的身份标识对应的范围级别和 / 或重要级别 ；信息处理单元 30 用于根据级别设定单元 40 设定的所述设备端的安全防护系统的身份标识对应的范围级别和 / 或重要级别，确定所述设备端的安全防护系统监测到的安全事件信息的范围级别和 / 或重要级别。具体地，可以在级别设定单元 40 设定设备端的安全防护系统的身份标识与范围级别和 / 或重要级别的对应关系表。

[0059] 更进一步地，级别设定单元 40 还用于设定所述电子文件的身份标识对应的重要级别 ；信息处理单元 30 还可以用于根据级别设定单元 40 设定的所述电子文件的身份标识对应的重要级别，确定所述设备端上预设的电子文件的重要级别。具体地，可以在级别设定单元 40 设定电子文件的身份标识与重要级别的对应关系表。

[0060] 更进一步地，显示管理单元 20 还可以用于向所述设备端的安全防护系统发送操作命令，以使所述设备端的安全防护系统执行相应操作。

[0061] 具体地，显示管理单元 20 向设备端的安全防护系统发送的操作命令可以通过信息处理单元 30 和设备连接单元 10 传递至设备端的安全防护系统。

[0062] 可以理解的是，以上实施方式仅仅是为了说明本发明的原理而采用的示例性实施方式，然而本发明并不局限于此。对于本领域内的普通技术人员而言，在不脱离本发明的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本发明的保护范围。

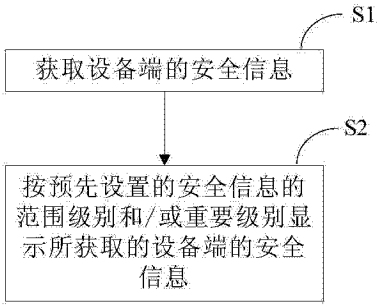

S1
获取设备端的安全信息
S2
按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息

图 1

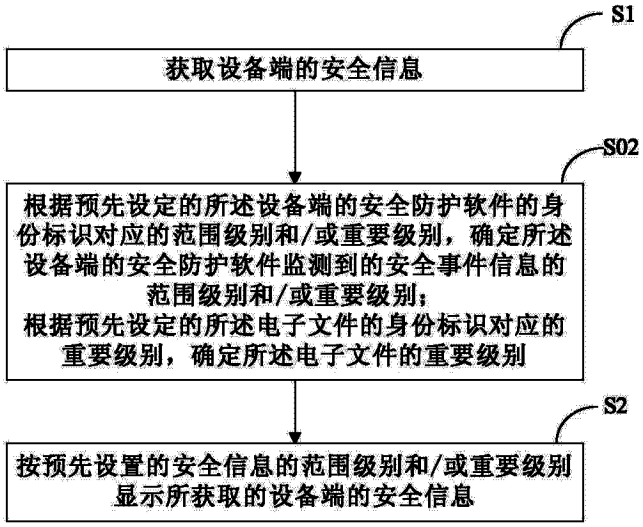

S1
获取设备端的安全信息
S02
根据预先设定的所述设备端的安全防护软件的身份标识对应的范围级别和/或重要级别，确定所述设备端的安全防护软件监测到的安全事件信息的范围级别和/或重要级别；
根据预先设定的所述电子文件的身份标识对应的重要级别，确定所述电子文件的重要级别
S2
按预先设置的安全信息的范围级别和/或重要级别显示所获取的设备端的安全信息

图 2

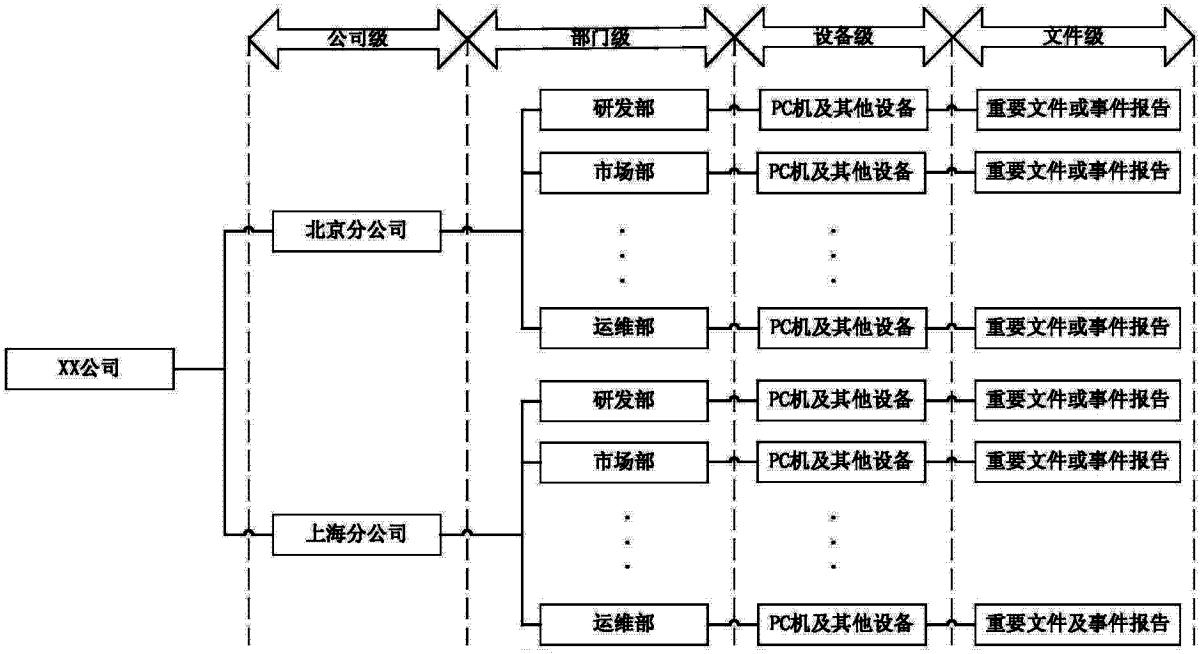

公司级
部门级
设备级
文件级
XX公司
北京分公司
上海分公司
研发部
市场部
运维部
研发部
市场部
运维部
PC机及其他设备
PC机及其他设备
PC机及其他设备
PC机及其他设备
PC机及其他设备
PC机及其他设备
重要文件或事件报告
重要文件或事件报告
重要文件或事件报告
重要文件或事件报告
重要文件或事件报告
重要文件及事件报告

图 3

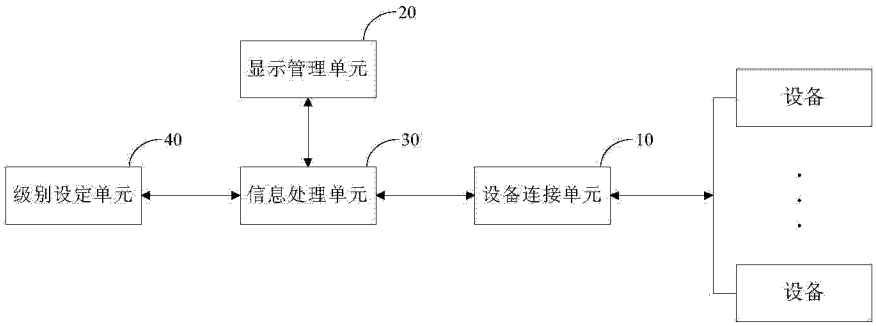


图 4