(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 101867566 A
(43)申请公布日 2010.10.20

(21)申请号 201010151782.0
(22)申请日 2010.04.14
(30)优先权数据
61/169,199 2009.04.14 US
12/637,439 2009.12.14 US
(51)Int.Cl.
H04L 29/06(2006.01)

(71)申请人 费舍-柔斯芒特系统股份有限公司
地址 美国德克萨斯州
(72)发明人 李·艾伦·奈策尔
丹·霍尔沃·乌辛
罗伯特·肯特·胡巴
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 康泉 宋志强

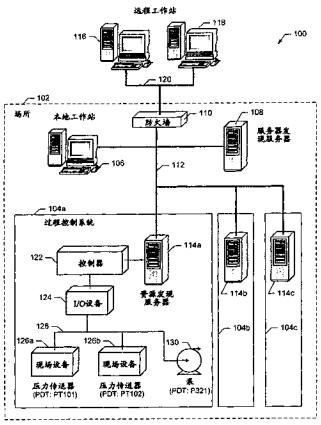
权利要求书 4 页 说明书 18 页 附图 6 页

(54)发明名称

为接口访问控制提供分层的安全防护的方法和设备

(57)摘要

本发明公开了为接口访问控制提供分层的安全防护的示例方法和装置。公开的示例方法包括：在第一服务器上从客户应用接收连接消息以访问至少一个服务器端点；响应于接收该连接消息，如果会话被授权开启，则开启客户应用和至少一个服务器端点之间的会话；从客户应用接收请求以开启对至少一种资源提供读访问、写访问、或订阅访问中的至少一种访问的端点；在确定客户应用被授权通过端点访问至少一种资源之后，开启开放的会话内的端点；从客户应用接收请求以向端点分配所选择的至少一种授权的资源；向端点分配至少一种所选择的资源，并准许客户应用通过端点访问至少一种资源。



CN 101867566 A

1. 一种方法，用于为接口访问控制提供分层的安全防护，所述方法包括：

在第一服务器从客户应用接收连接消息以访问至少一个服务器端点；

响应于接收所述连接消息，在会话被授权开启时，开启所述至少一个服务器端点和所述客户应用之间的所述会话；

从所述客户应用接收请求以开启端点，该端点提供对至少一种资源的读访问、写访问、或订阅访问中的至少一种访问；

在确定所述客户应用被授权通过所述端点访问所述至少一种资源之后，开启开放的会话中的所述端点；

从所述客户应用接收请求以向所述端点分配至少一种所授权的资源的选择；

向所述端点分配至少一种所选择的资源；以及

准许所述客户应用通过所述端点对所述至少一种资源的访问。

2. 如权利要求 1 所述的方法，还包括，如果所述至少一种资源授权被所述客户应用访问，则向所述客户应用提供所述至少一种资源的列表。

3. 如权利要求 2 所述的方法，其中向所述客户应用提供所述至少一种资源的列表是响应于在所述第一服务器从所述客户应用接收发现资源请求消息，以发现与所述至少一个服务器端点相关联的所述至少一种资源。

4. 如权利要求 1 所述的方法，其中所述端点是响应于在所述第一服务器从所述客户应用接收开启端点请求消息而被开启。

5. 如权利要求 1 所述的方法，其中准许所述客户应用对所述至少一种资源的访问包括准许所述客户应用写访问、读访问、或订阅访问中的至少一种访问。

6. 如权利要求 1 所述的方法，其中开启所述端点包括选择所述端点或创建所述端点中的至少一种。

7. 如权利要求 1 所述的方法，还包括：

在所述第一服务器接收所述连接消息之前，在第二服务器从所述客户应用接收发现服务器请求消息，以发现所述第一服务器的所述至少一个服务器端点；

响应于接收所述发现服务器请求消息，确定授权被所述客户应用访问的所述至少一个服务器端点；以及

向所述客户应用提供至少一个所确定的服务器端点。

8. 如权利要求 7 所述的方法，其中确定所述客户应用是否被授权访问所述至少一个服务器端点或所述至少一种资源中的至少一个包括，通过访问控制列表授权所述客户应用，所述访问控制列表使所述客户应用的工作站网络地址、所述客户应用的用户的身份、所述客户应用的工作站的位置、所述客户应用的身份、或所述客户应用所使用的协议中的至少一个有效。

9. 如权利要求 1 所述的方法，还包括：

向至少一种所选择的资源分配一对标识符或一个标识符中的至少一个；

将所述一对标识符或一个标识符中的所述至少一个与所述会话相关联；以及

向所述客户应用传送所述一对标识符或一个标识符中的所述至少一个。

10. 如权利要求 9 所述的方法，其中所述标识符是动态分配的别名标识符，该别名标识符保护由所述标识符标识的所述至少一种资源不被第三方确定。

11. 如权利要求 1 所述的方法，还包括，在一时间段或来自所述客户应用的终止所述会话的终止请求消息中的至少一个之后，终止所述会话。

12. 如权利要求 1 所述的方法，还包括：

通过所述端点从所述客户应用接收信息；以及

通过所述端点将所述信息存储到相应的至少一种所选择的资源。

13. 如权利要求 12 所述的方法，其中所述信息包括执行行动的请求或数据中的至少一种。

14. 如权利要求 1 所述的方法，还包括通过所述端点向所述客户应用发送数据、事件、或警报中的至少一种。

15. 如权利要求 1 所述的方法，其中所述至少一种资源包括数据、警报、或事件中的至少一种。

16. 如权利要求 1 所述的方法，还包括如果所述至少一种资源未授权被所述客户应用访问，则拒绝所述客户应用对可通过所述服务器端点而获得的所述至少一种资源的访问。

17. 一种装置，用于为接口访问控制提供分层的安全防护，所述装置包括：

第一服务器，所述第一服务器编程为：

从客户应用接收连接消息以访问至少一个服务器端点；

响应于接收所述连接消息，在会话被授权开启时，开启所述至少一个服务器端点和所述客户应用之间的所述会话；

从所述客户应用接收请求以开启端点，该端点提供对至少一种资源的读访问、写访问、或订阅访问中的至少一种访问；

在确定所述客户应用被授权通过所述端点访问所述至少一种资源之后，开启开放的会话中的所述端点；

从所述客户应用接收请求以向所述端点分配至少一种所授权的资源的选择；

向所述端点分配至少一种所选择的资源；以及

准许所述客户应用通过所述端点对所述至少一种资源的访问。

18. 如权利要求 17 所述的装置，其中所述第一服务器用来在所述至少一种资源授权被所述客户应用访问时，向所述客户应用提供所述至少一种资源的列表。

19. 如权利要求 18 所述的装置，其中所述第一服务器响应于从所述客户应用接收发现资源请求消息来向所述客户应用提供所述至少一种资源的列表，以发现与所述至少一个服务器端点相关联的所述至少一种资源。

20. 如权利要求 17 所述的装置，其中所述第一服务器响应于在所述第一服务器从所述客户应用接收创建端点请求消息来开启所述端点。

21. 如权利要求 17 所述的装置，其中所述第一服务器用来通过准许所述客户应用写访问、读访问、或订阅访问中的至少一种访问来准许所述客户应用对所述至少一种资源的访问。

22. 如权利要求 17 所述的装置，其中所述第一服务器用来通过选择所述端点或创建所述端点中的至少一种来开启所述端点。

23. 如权利要求 17 所述的装置，其中所述装置还包括第二服务器，用于：

从所述客户应用接收发现服务器请求消息，以发现所述第一服务器的所述至少一个服

务器端点；

响应于接收所述发现服务器请求消息，确定授权被所述客户应用访问的所述至少一个服务器端点；以及

向所述客户应用提供至少一个所确定的服务器端点。

24. 如权利要求 17 所述的装置，其中所述第一服务器用于通过经由访问控制列表授权所述客户应用来确定所述客户应用是否被授权访问所述至少一种资源，所述访问控制列表使所述客户应用的工作站网络地址、所述客户应用的用户的身份、所述客户应用的工作站的位置、所述客户应用的身份、或所述客户应用所使用的协议中的至少一个有效。

25. 如权利要求 17 所述的装置，其中所述第一服务器用来：

向至少一种所选择的资源分配一对标识符或一个标识符中的至少一个；

将所述一对标识符或一个标识符中的所述至少一个与所述会话相关联；以及

向所述客户应用传送所述一对标识符或一个标识符中的所述至少一个。

26. 如权利要求 17 所述的装置，其中所述第一服务器用来在一时间段或来自所述客户应用的终止所述会话的终止请求消息中的至少一个之后，终止所述会话。

27. 如权利要求 17 所述的装置，其中所述第一服务器用来：

通过所述端点从所述客户应用接收信息；以及

通过所述端点将所述信息存储到相应的至少一种所选择的资源。

28. 如权利要求 17 所述的装置，其中所述第一服务器用来通过所述端点向所述客户应用发送数据、事件、或警报中的至少一种。

29. 如权利要求 17 所述的装置，其中如果所述至少一种资源未授权被所述客户应用访问，则所述第一服务器拒绝所述客户应用对可通过所述服务器端点获得的所述至少一种资源的访问。

30. 一种机器可访问介质，该介质存储有指令，所述指令在被执行的时候使得机器：

在第一服务器从客户应用接收连接消息以访问至少一个服务器端点；

响应于接收所述连接消息，在会话被授权开启时开启所述至少一个服务器端点和所述客户应用之间的所述会话；

从所述客户应用接收请求以开启端点，该端点提供对至少一种资源的读访问、写访问、或订阅访问中的至少一种访问；

在确定客户应用被授权通过所述端点访问所述至少一种资源之后，开启开放的会话中的所述端点；

从所述客户应用接收请求以向所述端点分配至少一种所授权的资源的选择；

向所述端点分配至少一种所选择的资源；以及

准许所述客户应用通过所述端点对所述至少一种资源的访问。

31. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器在所述至少一种资源授权被所述客户应用访问时，向所述客户应用提供所述至少一种资源的列表。

32. 如权利要求 31 所述的机器可访问的介质，其中所述指令在被执行的时候使得所述机器响应于从所述客户应用接收发现资源请求消息而向所述客户应用提供所述至少一种资源的列表，以发现与所述至少一个服务器端点相关联的所述至少一种资源。

33. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器响应于从所述客户应用接收开启端点请求消息而开启所述端点。

34. 如权利要求 30 所述的机器可访问的介质，其中所述指令在被执行的时候使得所述机器通过准许所述客户应用写访问、读访问、或订阅访问中的至少一种访问来准许所述客户应用对所述至少一种资源的访问。

35. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器通过选择所述端点或创建所述端点中的至少一种来开启所述端点。

36. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器：

在接收所述连接消息之前，从所述客户应用接收发现服务器请求消息，以发现所述至少一个服务器端点；

响应于接收所述发现服务器请求消息，确定授权被所述客户应用访问的所述至少一个服务器端点；以及

向所述客户应用提供至少一个所确定的服务器端点。

37. 如权利要求 36 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器通过经由访问控制列表授权所述客户应用来确定所述客户应用是否被授权访问所述至少一个服务器端点或所述至少一种资源中的至少一个，所述访问控制列表使所述客户应用的工作站网络地址、所述客户应用的用户的身份、所述客户应用的工作站的位置、所述客户应用的身份、或所述客户应用所使用的协议中的至少一个有效。

38. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器：

向所述至少一种所选择的资源分配一对标识符或一个标识符中的至少一个；

将所述一对标识符或一个标识符中的所述至少一个与所述会话相关联；以及

向所述客户应用传送所述一对标识符或一个标识符中的所述至少一个。

39. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器：

通过所述端点接收来自所述客户应用的信息；以及

通过所述端点将所述信息存储到相应的至少一种所选择的资源。

40. 如权利要求 30 所述的机器可访问介质，其中所述指令在被执行的时候使得所述机器通过所述端点向所述客户应用发送数据、事件、或警报中的至少一种。

为接口访问控制提供分层的安全防护的方法和设备

[0001] 相关申请

[0002] 本申请要求 2009 年 4 月 14 日递交的第 61/169,199 号美国临时申请的利益，该申请通过引用被整体并入。

技术领域

[0003] 本公开一般涉及数据系统，以及，更特别地，涉及为接口访问控制提供分层的安全防护 (layered security) 的方法和设备。

背景技术

[0004] 数据系统如过程控制系统、制造自动化系统和其它工业系统，像在化学、石油或其他过程中使用的那些系统，典型地包括一个或更多集中的过程控制器，这些集中的过程控制器通过模拟、数字或组合的模拟 / 数字总线通信地耦合到至少一个主机、操作员和 / 或用户工作站以及耦合到一个或更多现场设备。这些系统利用访问控制来根据用户身份 (identity) 准许对系统的访问。访问控制技术典型地包括用户认证、加密、和 / 或特定用户访问控制列表。访问控制列表识别哪些系统资源可以被读、写、执行等。此外，访问控制列表可识别用户能够访问 (例如，读、写、和 / 或执行) 系统的哪些资源。这些资源可包括例如数据、警报、事件、和 / 或功能。典型地，根据正在被访问的资源类型，将系统程序、功能、和 / 或过程组织到端点 (endpoint) 中。例如，存在独立的端点来访问警报、事件、和数据的当前值。也存在独立的端点来访问警报、事件和数据的历史值。

[0005] 由于同可连接到互联网和 / 或一个或更多专用网的路由器、服务器、交换机、和 / 或工作站没有物理和 / 或无线连通性，数据系统或过程控制系统可被设计成与外部网络通信隔离。其它数据系统或过程控制系统可有意地包括与互联网和 / 或一个或更多专用网的连通性，以允许远程监视系统监视过程的进展、质量、和 / 或控制操作。此外，数据系统或过程控制系统与外部网络的外部连通性允许控制系统的单个组件接收周期性的和 / 或有计划的更新，如固件更新或修改的控制程序。尽管一个或更多系统的外部连通性可允许外部监视和控制，这样的外部连通性可增加网络入侵对系统的威胁。

发明内容

[0006] 描述了为接口访问控制提供分层的安全防护的示例方法和装置。在一个实施例中，方法包括，在第一服务器上从客户应用接收连接消息以访问至少一个服务器端点，并响应于接收连接消息，如果会话被授权开启 (open)，则开启客户应用和至少一个服务器端点之间的会话。示例方法还包括，从客户应用接收请求以开启提供对至少一种资源的读访问、写访问、或订阅访问中的至少一种访问的端点，在确定客户应用被授权通过端点访问至少一种资源之后，开启开放的会话内的端点，以及从客户应用接收请求以向端点分配所选择的至少一种授权的资源。此外，示例方法包括向端点分配至少一种所选择的资源，并准许客户应用通过端点访问至少一种资源。

[0007] 示例装置包括第一服务器，该第一服务器被编程为从客户应用接收连接消息以访问至少一个服务器端点，以及，响应于接收连接消息，如果会话被授权开启，则开启客户应用和至少一个服务器端点之间的会话。示例装置也可用来接收来自客户应用的请求，以开启提供对至少一种资源的读访问、写访问、或订阅访问中的至少一种访问的端点，并在确定客户应用被授权通过端点访问至少一种资源之后，开启开放的会话内的端点。进一步地，示例装置用来从客户应用接收请求以向端点分配所选择的至少一种授权的资源，向端点分配至少一种所选择的资源，并准许客户应用通过端点访问至少一种资源。

附图说明

[0008] 图 1 为示例过程控制环境的框图。

[0009] 图 2 为图 1 的示例服务器发现服务器和资源发现服务器的功能框图。

[0010] 图 3 为描述图 1 和图 2 的示例服务器发现服务器和资源发现服务器所提供的示例分层的安全防护的图示。

[0011] 图 4A 和 4B 为流程图，描述了可被用来实现图 1、2 和 / 或 3 的示例过程控制环境、示例服务器发现服务器、示例资源发现服务器、和 / 或示例客户应用的示例过程。

[0012] 图 5 是可被用来实现在此描述的方法和装置的示例处理器系统的框图。

具体实施方式

[0013] 尽管以下描述了示例方法和装置，除其他组件，其还包括在硬件上执行的固件和 / 或软件，应当注意到，这样的系统仅仅是示意性的，并不应当被认为是限制。例如，设想任何或所有这些硬件、软件、和固件组件可专门地在硬件、专门地在软件、或在硬件和软件的任何组合中体现。相应地，尽管以下描述了示例方法和装置，本领域的普通技术人员将容易认识到，所提供的实施例不是实现这样的方法和装置的唯一方式。

[0014] 对系统的访问控制典型地是基于用户身份。访问控制技术典型地包括用户认证、加密、和 / 或特定用户访问控制列表。访问控制列表识别哪些系统资源可以被读、写、执行等。此外，访问控制列表可识别用户能够访问（例如读、写、和 / 或执行等）系统的哪些资源，如功能、数据、警报、和 / 或事件。

[0015] 端点提供系统和 / 或服务的一个或更多访问点。客户应用向系统和 / 或服务的端点发送消息，以访问与系统和 / 或服务关联的资源。端点包括地址、绑定单元、和 / 或合同单元。端点的地址是托管服务的应用程序用来通知该服务的位置。例如，地址可包括包含目录名称的统一资源定位符 (URL)，该目录包括与作为端点的那个服务关联的文件的名称和服务。绑定单元指定可用来访问服务的传送机制和 / 或协议。例如，绑定单元可指定 basicHttpBinding 作为用来访问服务的协议。合同单元指示可在服务内部访问的操作和 / 或用来访问资源的参数，该资源可经过端点来访问。

[0016] 端点可通过面向对象的技术、基于表述性状态转移 (representational statetransfer，REST) 的接口、和 / 或服务合同接口来实现。典型地，根据正在被访问的资源类型，将程序、功能、和 / 或过程组织到端点。例如，存在独立的端点来访问警报、事件、或数据的当前值和 / 或警报、事件或数据的历史值。

[0017] 当前，对端点的威胁正在增加。威胁包括病毒、木马、蠕虫、分布式拒绝服务 (DDos)

攻击、和 / 或间谍软件。这些威胁可让未认证的第三方浏览、复制、和 / 或破坏过程控制系统内的数据。系统可被威胁扰乱，该威胁可降低系统所产生的生产能力、效率、和 / 或收益。

[0018] 传统地，使用依赖于被保护的资源的安全机制来保护端点。这些安全机制包括用户认证、授权、和 / 或加密。例如，为保护提供对当前数据值的访问的端点，用户可被认证然后可根据访问控制列表被允许对指定的数据进行读或写。此外，加密可被用来保护正在被访问的数据的机密性。这个典型的方法要求端点支持的所有操作使用相同的安全机制。例如，如果使用认证作为安全机制，则在每一次消息交换中实现认证。类似地，如果使用加密作为安全机制，则对每一次消息传递实现加密。然而，与这些安全机制关联的性能恶化经常导致系统用户和 / 或操作员关闭或以其他方式停用该安全机制，从而，使端点为开放的并容易受到攻击。

[0019] 在此描述的示例方法和装置实现由它们的安全要求来定义和组织的端点。例如，被典型地定义成提供数据访问的端点可被重组成独立的读访问端点、写访问端点、和 / 或订阅访问端点。读、订阅、和 / 或写端点可用来检索和 / 或更新数据、警报、事件等。读端点提供使用一种或更多方法（例如，程序）在服务器内检索（例如，读、获得等）数据、警报、和 / 或事件的客户应用。订阅端点提供使用一种或更多方法（例如轮询 (poll)、召回 (callback) 等）在服务器内周期性地检索数据变化、警报、和 / 或事件的客户应用。写端点提供使用一种或更多方法来改变（例如，写、放入、更新、修改、确认、执行等）服务器内的功能和 / 或事件、警报、数据的值或状态的客户应用。

[0020] 在此描述的示例方法和装置实现了根据安全标准对端点进行访问控制，该安全标准包括请求者的身份和 / 或角色、请求者的位置、请求者所使用的计算机和 / 或工作站的身份、请求工作站和 / 或计算机的网络地址、请求应用的身份和 / 或类型、请求应用用来访问端点的协议、和 / 或端点接收到请求的时间。端点访问控制可认证和 / 或授权请求消息，使得该请求消息可被接收端点处理。此外，端点访问控制授权将列表的内容提供给请求客户应用、操作员、和 / 或用户。这些内容可包括与资源发现端点和 / 或资源发现服务器相关联的资源，该资源发现服务器与资源发现端点相关联。在一些实施例中，端点访问控制可向请求客户应用和 / 或工作站发送安全验证消息，以证实客户应用和 / 或工作站的身份。在其他实施例中，端点访问控制可向第三方计算机（例如，Windows 活动目录服务器）发送安全消息来获得关于请求者的安全信息。

[0021] 在此描述的示例方法和装置通过服务器发现服务器和 / 或一个或更多资源发现服务器提供分层的安全防护。服务器发现服务器定位资源发现服务器。此外，服务器发现服务器维护资源发现服务器列表并可使用访问控制标准来确定哪些请求者访问每个资源发现服务器。服务器发现服务器列出资源发现服务器，请求者（例如，客户、操作员等）可能选择资源发现服务器来访问与资源发现服务器相关联的资源。每个资源发现服务器可通过相应的资源发现端点被访问。服务器发现服务器可向请求者提供资源发现端点，或者，可选择地，服务器发现服务器可向请求者提供每个资源发现服务器里的端点，其中资源发现服务提供资源发现端点。

[0022] 在请求者访问资源发现端点时，资源发现服务器确定哪些资源是请求者可用的，并列出那些资源和 / 或对那些资源的端点。资源发现服务器可使用被用来访问端点的访问控制标准，以确定请求者可访问哪些资源。请求者然后可通过注册来选择可用资源中的一

个或更多，以读、写、订阅、和 / 或执行该资源。资源发现服务器然后通过允许请求者通过读、写、和 / 或订阅端点而访问资源来准许注册者请求，这些读、写、和 / 或订阅端点可被创建、开启、和 / 或与请求者所选择的资源相关联。

[0023] 在此描述的方法和装置限制了通过资源发现端点来访问资源。资源可通过资源发现端点被发现并注册以进行访问。资源发现服务器提供请求者信息，该请求者信息对开启和 / 或创建读、写和 / 或订阅端点并向该读、写、和 / 或订阅端点分配注册资源以访问所注册的资源是必须的。当请求者已经给读和 / 或订阅端点分配了资源后，该请求者可浏览与那种资源相关联的数据。此外，当请求者已经给写端点分配了资源后，请求者可向那种资源写数据，或以其它方式根据通过该写端点可获得的功能修改或执行该资源。在一些实施例中，读、写、和 / 或订阅端点可在请求者选择想要的资源时创建。在其它实施例中，读、写、和 / 或订阅端点可由服务器创建和 / 或预先配置，并由请求者开启。

[0024] 示例方法和装置使得请求者能够使用与资源发现端点相关联的读、写、和 / 或订阅端点，直到请求者终止与资源发现端点的对话。在请求者终止对话后，除了与所选择的资源关联的难以理解的标识符，在会话情境内被创建和 / 或开启的读、写、和 / 或订阅端点也被从会话删除。请求者随后可访问资源发现服务器以创建新的会话来访问资源。

[0025] 在此描述的示例方法和装置利用难以理解的动态分配标识符来为所选择的资源和它们的相关读、写、和 / 或订阅端点起别名。这个别名为每个读端点、写端点、订阅端点、和 / 或通过读、写、和 / 或订阅端点可访问的资源提供了不同的标识符。请求者和 / 或资源发现服务器使用标识符来访问端点，以浏览和 / 或更新与所选择的资源相关联的数据。资源标识符在资源注册的过程中创建，以及端点标识符在端点的开启和 / 或创建的过程中创建。此外，标识符（例如，资源标识符和 / 或端点标识符）不可用来标识会话情境外部的资源和 / 或对应的读、写、和 / 或订阅端点。用来标识资源和 / 或端点的难以理解的标识符使得在操作员和 / 或用户与系统之间的通信过程中，窥伺 (snoop) 和 / 或发觉 (sniff) 应用将数据值与相关资源关联起来更加困难。因此，这些难以理解的标识符使得窥伺和 / 或发觉应用引起安全漏洞更加困难。例如，使用标识符拦截消息的第三方将不能识别正被标识的是哪种资源和 / 或怎样拦截正被传递的数据值。

[0026] 此外，难以理解的标识符安全可通过在一段时间之后刷新难以理解的标识符得到增强。标识符的刷新使得操作员、用户、和 / 或客户应用能够定期更新与资源相关联的难以理解的标识符，以禁止可由窥伺和 / 或发觉应用导致的流量分析。而且，服务器发现端点和 / 或资源发现端点可在与请求者的通信中使用加密，以防止资源和 / 或与每种资源相关联的难以理解的标识符的公开。

[0027] 图 1 为可用来实现在此描述的示例方法和装置的示例过程控制环境 100 的框图。过程控制环境 100 包括具有三个过程控制系统 104a-c 的过程控制场所 (process control plant)102。在其它实施例中，过程控制场所 102 可包括更少的过程控制系统或额外的过程控制系统。此外，过程控制场所 102 包括通过局域网 (LAN)112 通信地耦合到服务器发现服务器 108 的本地工作站 106。在其它实施例中，过程控制场所 102 可包括额外的本地工作站、服务器、和 / 或计算机。

[0028] 示例过程控制场所 102 代表在一个或更多批处理和 / 或批量阶段的过程中可产生一个或更多产品的示例场所。在其它实施例中，过程控制场所 102 可包括发电设施、工业

设施、和/或包括控制和监视系统或信息技术系统的任何其它设施类型。示例本地工作站106可用作场所102的操作员和/或用户接口，并可通过LAN112通信地连接到过程控制系统104a-c中的一个或更多。

[0029] 示例过程控制环境100包括通过广域网(WAN)120耦合到过程控制场所102的远程工作站116和118。WAN120可包括公共电话交换网络(PSTN)系统、公共陆地移动网络(PLMN)系统、无线分布系统、有线或电缆分布系统、同轴电缆分布系统、光纤到户(fiber-to-the-home)网络、光纤到路边(fiber-to-the-curb)网络、光纤到基座(fiber-to-the-pedestal)网络、光纤到地下(fiber-to-the-vault)网络、光纤到邻域(fiber-to-the-neighborhood)网络、超高频(UHF)/特高频(VHF)射频系统、卫星或其他地球外系统、蜂窝分布系统、电力线广播系统、和/或这些设备、系统和/或网络的组合和/或混合中的任何类型。

[0030] 此外，过程控制场所102包括防火墙110，以根据一条或更多规则确定是否允许来自远程工作站116和118的通信进入过程控制场所102。示例远程工作站116和118可为不在过程控制场所102内的操作员和/或用户提供对过程控制场所102内的资源的访问。例如，位于美国的过程控制工程师可使用远程工作站116检查位于墨西哥的过程控制场所102内的生产线(例如，资源)的状态。在其它的示例实现中，防火墙可位于每一个过程控制系统104a-c和工作站106、116和/或118之间。

[0031] 示例工作站106、116和/或118可配置成执行与一个或更多信息技术应用、用户交互应用、和/或通信应用相关联的操作。此外，工作站106、116和/或118可包括任何计算设备，该计算设备包括个人计算机、笔记本电脑、服务器、控制器、个人数字助理(PDA)、微型计算机等。

[0032] 示例资源发现服务器114a-c可配置成执行与一个或更多应用、用户交互应用、通信应用、和/或在相关联的过程控制系统104a-c内的一个或更多功能块相关联的操作。例如，资源发现服务器114a-c可配置成执行与过程控制相关的应用和通信应用相关联的操作，其使得资源发现服务器114a-c和各自的控制器(例如，控制器122)能够使用任何通信介质(例如，无线、硬接线等)和协议(例如，HTTP、SOAP等)与其它设备和/或系统通信。在其它实施例里，过程控制系统104a-c中的每一个可包括一个或更多资源发现服务器。

[0033] 每个资源发现服务器114a-c通信地耦合到控制器(例如，控制器122)。示例控制器122可执行一个或更多过程控制程序，所述过程控制程序已经由场所管理者、过程控制工程师、系统工程师、控制系统管理员、和/或负责场所102和/或整个过程控制环境100的运行其它操作员和/或用户配置和/或设计。控制器122可以是例如Emerson Process Management™公司的Fisher-Rosemount Systems有限公司出售的Delta™控制器。然而，可以用任何其它的控制器作为替代。进一步地，尽管图1中只显示了一个控制器122，任何类型或类型组合的额外的控制器可耦合到资源发现服务器114a-c中的每一个。尽管图1被示出的实施例部分地描述了过程控制系统，但在此描述的方法和装置也可应用到测试和测量环境，如实验室测试、审查测试、和/或质量控制分析。

[0034] 控制器122可通过控制总线128和/或I/O设备124耦合到多个现场设备126a-b和130。在过程控制程序的执行期间，控制器122可与现场设备128a-b和130交换信息(例如，命令、配置信息、测量信息、状态信息等)。例如，可向控制器122提供过程控制程序，该

程序在被控制器 122 执行的时候引起控制器 122 向现场设备 126a-b 发送命令，该命令引起现场设备 126a-b 执行特定的操作（例如，执行测量、打开 / 关闭阀门、开启 / 关闭过程泵等）和 / 或通过控制器 122 交流信息（例如，测量数据）。此外，控制器 122 可引起现场设备 126a-b 和 130 获得测量值（例如，压力值、温度值、流量值、电压值、电流值等）、执行算法或计算（例如，积分、求导、加、减等）、控制仪器（例如，打开 / 关闭阀门、熔炉调整、锅炉调整等）、和 / 或执行任何其它功能。

[0035] 服务器发现服务器 108 和资源发现服务器 114a-c 为工作站 106、116 和 / 或 118 提供到被控制器（例如，控制器 122）管理的过程控制资源的分层的访问。服务器发现服务器 108 可包括端点访问控制，其限制对它本身的访问和对它的与资源发现服务器 114a-c 相关联的资源发现端点 114a-c 列表的访问。根据服务器发现服务器 108 实现的端点访问控制的级别，服务器发现服务器 108 为每个用户和 / 或工作站 106、116 和 / 或 118 提供与资源发现服务器 114a-c 相关联的资源发现端点列表。例如，远程工作站 116 的用户和 / 或操作员可能被指定仅能访问过程控制系统 104b 和 / 或访问包括在过程控制系统 104b 内的指定的资源发现服务器（例如，服务器 114b）。结果，当远程工作站 116 的用户和 / 或操作员请求资源发现端点的列表时，服务器发现服务器 108 提供仅包括资源发现服务器 114b 的资源发现端点的列表。可选择地，服务器发现服务器 108 可为每个用户和 / 或工作站 106、116 和 / 或 118 提供资源发现服务器的端点（例如，与资源发现服务器 114a-c 关联的端点）的列表。用户和 / 或工作站 106、116 和 / 或 118 然后可使用这些端点直接从资源发现服务器 114a-c 检索资源发现端点的列表。

[0036] 示例服务器发现服务器 108 可向授权的工作站（例如，工作站 106、116 和 / 或 118）提供与资源发现服务器 114a-c 相关联的资源发现端点的列表。可选择地，示例服务器发现服务器 108 可向授权的工作站（例如，工作站 106、116 和 / 或 118）提供与资源发现服务器 114a-c 相关联的端点的列表。授权的工作站然后可使用端点的列表来检索资源发现端点。一旦工作站 106、116 和 / 或 118 已经接收到所选择的资源发现服务器（例如，资源发现服务器 114a）的资源发现端点，则工作站 106、116 和 / 或 118 然后可使用资源发现端点访问资源发现服务器（例如，服务器 114a）。在一些实施例中，资源发现服务器 114a 可确定工作站 106、116 和 / 或 118 是否被授权访问资源发现端点。在工作站 106、116 和 / 或 118 通过相关资源发现端点访问资源发现服务器 114a 时，资源发现服务器 114a 可实现端点访问控制，以确定授权将被工作站 106、116 和 / 或 118 访问的资源。资源发现服务器 114a 可包括与现场设备 126a-b 和 130 相关联的资源。任何工作站 106、116 和 / 或 118 的用户或操作员可选择授权的资源。

[0037] 当工作站 106、116 和 / 或 118 首次访问资源发现端点时，相关的资源发现服务器 114a 创建一个会话。通过工作站 106、116 和 / 或 118 选择一个或更多由资源发现服务器 114a 提供的资源，工作站 106、116 和 / 或 118 请求资源发现服务器 114a 创建由工作站 106、116 和 / 或 118 用来访问所选择的资源的读、写、和 / 或订约端点。如果工作站 106、116 和 / 或 118 打算读取资源，则工作站 106、116 和 / 或 118 从资源发现服务器 114a 请求读端点。如果工作站 106、116 和 / 或 118 打算更新和 / 或执行（例如，写）资源，则工作站 106、116 和 / 或 118 从资源发现服务器 114a 请求写端点。如果工作站 106、116 和 / 或 118 打算订阅资源，则工作站 106、116 和 / 或 118 从资源发现服务器 114a 请求订阅端点。

[0038] 资源发现服务器 114a 向工作站 106、116 和 / 或 118 提供这些端点，使用别名标识符掩盖端点的身份，并使用别名标识符掩盖即将通过端点访问的每种资源的身份。资源的别名可由工作站 106、116 和 / 或 118 提出，并由资源发现服务器 114a 确认。工作站 106、116 和 / 或 118 可使用端点标识符访问读、写、和 / 或订阅端点，并使用所选择资源的资源标识符浏览和 / 或修改这些资源。如果会话因为包括工作站 106、116 和 / 或 118 请求在内的任何原因即将被关闭，则资源发现服务器 114a 终止会话并删除和 / 或关闭任何开启的读、写、和 / 或订阅端点、与端点相关联的标识符、和 / 或与注册的资源相关联的标识符。在会话已经关闭之后，在工作站 106、116 和 / 或 118 能够再次访问资源发现服务器 114a 之前，工作站 106、116 和 / 或 118 可能被要求建立与资源发现服务器 114a 的新的会话。

[0039] 服务器发现服务器 108 和 / 或资源发现服务器 114a-c 也可实现针对加密、散列标记、和 / 或与工作站 106、116 和 / 或 118 的签名通信的安全协议。与资源标识符一起使用的安全协议进一步保护过程控制场所 102，使出其免于未授权的各方和 / 或实体试图浏览和 / 或修改从资源发现服务器 114a-c 和工作站 106、116 和 / 或 118 传送的过程控制数据。

[0040] 在一个实施例中，本地工作站 106 上的用户和 / 或操作员向服务器发现服务器 108 发送发现服务器请求消息，以定位资源发现服务器，工作站 106 可使用该资源发现服务器获得对泵现场设备 130 的泵速的访问（例如，资源）。服务器发现服务器 108 确定操作员、用户、和 / 或工作站 106 被授权访问的资源发现服务器 114a-c。服务器发现服务器 108 确定工作站 106 可访问资源发现服务器 114a 并提供列表，所述列表包括资源发现服务器 114a 的资源发现端点和 / 或资源发现服务器 114a 内的端点，工作站 106 可访问该端点以检索资源发现服务器 114a 的资源发现端点。

[0041] 工作站 106 然后传送请求消息（例如，连接消息）来开启与资源发现服务器 114a 的会话。工作站 106 将这个消息发送到新获得的资源发现端点的地址，到请求消息的地址字段内的那个服务器 114a。资源发现服务器 114a 接收请求消息并在执行任何端点访问控制以确定会话是否被授权之后开启会话。工作站 106 然后传送一系列消息（例如，发现资源请求消息、开启端点请求消息、和 / 或注册者请求消息）以发现工作站 106、操作员、和 / 或用户被授权访问的资源。资源发现服务器 114a 向工作站 106 提供列表内的资源，包括泵速资源。泵速资源可通过泵的名称“PDT :P321”来识别，或者，可选择地，通过一些其他的名称如泵速参数的名称来识别。

[0042] 一旦工作站 106 选择泵速资源并请求读端点来访问泵速资源，资源发现服务器 114a 创建和 / 或开启读端点，并将泵速与这个新创建和 / 或开启的读端点关联起来。在其他实施例中，资源发现服务器 114a 可将泵速与已经创建和 / 或开启的读端点关联起来。可选择地，工作站 106 可首先请求创建和 / 或开启读端点，然后分别地将泵速参数关联到读端点。可选择地，工作站 106 可首先将泵速参数添加到参数列表中，然后将参数列表添加到读端点。可选择地，如果工作站 106 上的用户和 / 或操作员被授权创建和 / 或开启读和 / 或订阅端点，则可从工作站 106 向资源发现服务器 114a 发送请求，来创建和 / 或开启写和 / 或订阅端点并将泵速与新创建和 / 或开启的读端点关联起来。

[0043] 而且，资源发现服务器 114a 可产生标识符如“1621545”来读取泵速资源并将标识符传送给工作站 106。可选择地，工作站 106 可提供标识符。在另一示例实现中，两个标识符可用于优化目的。例如，当工作站 106 向服务器 114a 发送泵速请求时，工作站 106 可使

用标识符来识别泵速，以及服务器 114a 可使用不同的标识符来向工作站 106 发送值。此外，服务器 114a 可针对读、写、和 / 或订阅要求独立的标识符，或者，可选择地，相同的标识符可用于读、写、和 / 或订阅。在图 1 的实施例中，服务器 114a 使用相同的泵速标识符（例如 1621545）来对泵速进行读和写。可选择地，资源发现服务器 114a 可为新创建和 / 或开启的读端点产生如“36285”的标识符，为新创建和 / 或开启的写端点产生如“88732”的标识符，并将那些标识符传送给工作站 106。

[0044] 工作站 106 上的用户和 / 或操作员可通过向资源发现服务器 114a 发送包括泵速标识符（例如，1621545）和消息中的读端点标识符（例如，36285）的消息来读取泵速资源。资源发现服务器 114a 访问控制器 112 来获得当前的泵速值（如果服务器 114a 还没有储存泵速值），并使用泵速标识符（例如 1621545）在消息中向工作站 106 传送泵速值。此外，工作站 106 上的用户和 / 或操作员可通过产生带有新的泵速、泵速标识符（例如 1621545）和写端点标识符（例如 88732）的消息并向资源发现服务器 114a 传送该消息，来改变泵速。一旦接收到消息，资源发现服务器 114a 向控制器 122 传送新的泵速，来将泵 130 的速度设置成新的指定泵速。工作站 106 上的用户和 / 或操作员然后可关闭与资源发现服务器 114a 的会话。一旦关闭，资源发现服务器 114a 终止会话并删除资源、读端点、写端点、和 / 或订阅端点的标识符。

[0045] 提供示例过程控制系统 104a 来示出系统的一种类型，其中可方便地利用以下被更加详细描述的示例方法和装置。然而，在此描述的示例方法和装置可以，但不限于，方便地用在比图 1 中显示的示例过程控制系统 104a 更加复杂或更不复杂和 / 或不同类型的系统中。而且，读、写、和 / 或订阅端点可使用与检索和 / 或更新数据、事件和警报相关的额外的方法和装置实现，所述方法和装置包括例如轮询和召回机制。

[0046] 图 2 为图 1 的示例资源发现服务器 114a 和示例服务器发现服务器 108 的框图。服务器发现服务器 108 和资源发现服务器 114a 通信地耦合到客户应用 202。示例客户应用 202 可包括任何过程控制应用和 / 或数据系统应用，该数据系统应用可被用来访问信息，该信息中心与提供对当前或历史数据值、事件、和警报的访问的系统的资源相关联。例如，客户应用 202 可以是 DeltaV™ 读 / 写控制应用。

[0047] 客户应用 202 被用来代表操作员、用户、和 / 或自动化用户访问资源。示例客户应用 202 可包括与客户应用 202 的用户相关联的标识信息。客户应用 202 可运行在工作站 106、116 和 / 或 118 的任何一个之上，并可包括标识信息。而且，客户应用 202 可通过图 1 的 WAN120 和 / 或 LAN112 耦合到服务器发现服务器 108 和 / 或资源发现服务器 114a。

[0048] 图 2 的示例客户应用 202 向服务器发现服务器 108 和 / 或资源发现服务器 114a 传送请求消息。该请求消息可包括访问端点以定位过程控制系统 104a 内资源的消息。此外，客户应用 202 可分配特定会话的难以理解的标识符来选择资源、读端点、写端点、和 / 或订阅端点。可选择地，客户应用 202 可为任何资源、读端点、写端点、和 / 或订阅端点从资源发现服务器 114a 接收特定会话的难以理解的标识符分配。可替换地，客户应用 202 和资源发现服务器 114a 可交换各自的特定会话的难以理解的标识符。客户应用 202 存储分配给相应的资源、读端点、写端点、和 / 或订阅端点的标识符。这样，客户应用 202 接收的资源数据与相应的资源标识符关联起来，客户应用可使用该资源标识符识别资源和 / 或与编码的资源数据相关联的端点。而且，客户应用 202 可包括加密解密能力，以从资源发现服务器 114a

接收加密的数据。尽管图 2 显示单个客户应用 202，在其他实施例中，多个客户应用可访问服务器 108 和 114a。

[0049] 为提供安全措施，如对与客户应用 202 的通信的端点访问控制和 / 或加密，示例服务器发现服务器 108 包括安全处理器 204a。此外，为提供安全，如对与客户应用 202 的通信的端点访问控制措施和 / 或加密，示例资源发现服务器 114a 包括安全处理器 204b。示例安全处理器 204a-b 可包括加密处理器和 / 或数字签名产生器，以保护来自未授权的第三方的外发的通信。加密处理器可使用任何类型的加密编码器来将去往客户应用 202 的通信格式化成未授权的用户不可读的格式。数字签名产生器保护通信不受到未授权的第三方的干预。数字签名产生器可使用任何类型的密码安全签名产生器（例如，哈希码），该签名产生器使得能够检测被客户应用 202 和服务器 108 和 / 或 114a 之间的未授权的第三方修改的值。此外，安全处理器 204a-b 可包括其他形式的通信安全，包括认证机制和 / 或访问控制。

[0050] 示例安全控制器 204a-b 可对源自客户应用 202 的加密的、和 / 或签名的通信进行解码。一旦解码该通信，安全处理器 204a-b 将通信传送至各个服务器 108 和 114a 内的预定目的地。此外，安全处理器 204a 可通过标识信息过滤源自客户应用 202 的请求消息，使得只有授权的用户可访问服务器发现服务器 108。可选择地，在一些示例实现中，服务器 108 和 114a 可不包括安全处理器 204a-b。在这些实施例中，与安全处理器 204a-b 相关联的安全功能可被包括在防火墙内（例如，防火墙 110）和 / 或包括在过程控制场所 102 内的其它地方。

[0051] 为管理资源发现服务器的发现，示例服务器发现服务器 108 包括服务器发现端点处理器 206。示例服务器发现端点处理器 206 处理来自客户应用 202 的请求，使得只有授权的请求者可发现资源发现服务器。服务器发现端点处理器 206 接收来自包括示例客户应用 202 的客户应用的请求消息（例如，发现服务器请求消息）以发现资源发现服务器。

[0052] 一旦接收到请求消息，服务器发现端点处理器 206 使用请求消息内的和 / 或与请求消息相关联的信息，来确定使用客户应用 202 的用户和 / 或操作员的身份、和 / 或运行客户应用 202 的工作站的身份、和 / 或与执行端点访问控制相关联的其它信息。例如，服务器发现端点处理器 206 可检查请求消息内的用户标识字段，以确定用户标识值是否对应授权的用户。可选择地，示例服务器发现端点处理器 206 可检查请求消息内的协议类型、工作站标识值、客户应用类型、客户应用序列号、和 / 或客户应用位置。此外，示例服务器发现端点处理器 206 可检查与消息和 / 或客户应用 202 相关的其它信息，以协助消息的授权过程（例如，如果消息从集中式安全计算机被传送）。

[0053] 服务器发现端点处理器 206 可使用访问控制列表来确定哪些资源发现服务器是为客户应用 202 可用的。可选择地，服务器发现端点处理器 206 可实现其他功能来确定与接收到的消息相关联的安全属性。访问控制列表和 / 或其它功能可包括参照资源发现端点的被批准的用户的列表，每个被批准的请求被授权访问该资源发现端点。例如，分配给过程控制系统 104a 的系统操作员和 / 或用户可被授权访问与过程控制系统 104a 相关联的资源发现端点。此外，访问控制列表可包括工作站和 / 或客户应用的列表，该列表参照每个工作站和 / 或客户应用被授权访问的资源发现端点。访问控制列表可由过程控制系统 104a-c 和 / 或过程控制场所 102 的控制器和 / 或管理员预先确定。

[0054] 一旦将请求消息内的标识信息参照到访问控制列表，服务器发现端点处理器 206

向客户应用 202 返回授权的资源发现端点的列表。该资源发现端点的列表可包括资源发现端点的名称、为端点提供访问的系统的名称、和 / 或端点提供的信息类型。此外，根据请求端点列表的客户应用，列表中提供的关于每个资源发现端点的信息量可能被服务器发现端点处理器 206 所限制。这个限制使得第三方和 / 或闯入者对资源发现端点的恶意配置相对困难。恶意配置可包括检查潜在目标（例如，资源发现服务器 114a）的属性，以构造对目标的入侵。例如，如果客户应用 202 根据过程控制场所 102 远程定位，服务器发现端点处理器 206 仅可为列出的每个资源发现端点列表提供参考名称。每个列出的资源发现端点对应于过程控制环境 100 内的资源发现服务器 114a。例如，服务器发现端点处理器 206 可为客户应用 202 提供对应于资源发现服务器 114a-c 的资源发现端点的列表。

[0055] 图 2 的示例服务器发现端点处理器 206 为客户应用提供资源发现端点的列表。服务器发现端点处理器 206 可返回提交请求所必需的信息（例如，连接消息），以在资源发现服务器 114 内开启会话，或者，可选择地，服务器发现端点处理器 206 可返回资源发现端点的身份，使得客户应用 202 能够选择资源发现端点。客户应用 202 一旦选择了一个或更多资源发现端点，服务器发现端点处理器 206 向客户应用 202 传送信息，以开启与每个所选择的资源发现端点的会话。

[0056] 为管理对资源、资源发现端点、读端点、写端点、和 / 或订阅端点的访问，示例资源发现服务器 114a 包括会话控制器 208、资源发现端点处理器 210 和读 / 写 / 订阅端点处理器 212。图 2 仅显示了耦合到客户应用 202 的资源发现服务器 114a。在其它实施例中，客户应用 202 可耦合到资源发现服务器 114b-c，其可包括它们自己的会话控制器 208、资源发现端点处理器 210 和读 / 写 / 订阅端点处理器 212。客户应用 202 从服务器发现端点处理器 206 接收与资源发现端点相关联的信息和 / 或位置。客户应用 202 使用这个信息访问资源发现服务器 114a，以向与资源发现服务器 114a 相关联的资源发现端点发送请求消息（例如，连接消息）。

[0057] 图 2 的示例会话控制器 208 为客户应用 202 管理资源访问会话。会话代表客户应用 202 和资源发现服务器 114a 之间的通信联合的实例。此外，会话控制器 208 可为可访问资源发现服务器 114a 的其它客户应用管理会话。一旦从客户应用 202 接收到连接消息，会话控制器 208 启动一个会话来开启与和服务器 114 相关联的资源发现端点的会话。会话控制器可拒绝来自客户应用 202 的任何其它请求，直到会话控制器 208 开启会话。在会话开启的同时，会话控制器 208 将来自客户应用 202 的每个请求消息路由到资源发现端点处理器 210。

[0058] 如果客户应用 202 从资源发现端点处理器 210 选择资源和 / 或资源端点，并请求创建读、写、和 / 或订阅端点来访问所选择的资源（或向之前创建和 / 或开启的读、写、或订阅端点分配所选择的资源），资源发现端点处理器 210 存储对于所选择的资源和相关的读、写、和 / 或订阅端点的参照。此外，会话控制器 208 可存储对于所选择的资源和它们的相关的读或写端点的参照。

[0059] 读 / 写 / 订阅端点处理器（例如，读 / 写 / 订阅端点处理器 212）可被创建和 / 或用于客户应用 202 创建和 / 或开启的每一个读、写、和 / 或订阅端点。对这些读 / 写 / 订阅端点处理器中的每一个，也可创建和 / 或使用安全处理器和 / 或会话控制器。创建和 / 或使用处理器可包括分派服务器的部分去执行与处理器相关联的功能。可选择地，创建和 / 或

使用处理器可包括激活一个或更多相邻服务器上的处理器，来执行与每个新创建的处理器相关联的功能。通过为不同客户应用的不同会话在资源发现端点处理器 210 之间分离所传送的消息的通信路径，为每个读 / 写 / 订阅端点处理器创建和 / 或使用安全处理器和 / 或会话控制器提供了额外的安全性。此外，分离通信路径为传送至和 / 或来自资源发现端点处理器 210 的消息和传送至和 / 或来自读端点、写端点、和 / 或订阅端点的消息提供了额外的安全性。读 / 写 / 订阅端点处理器 212 可在独立的计算介质而不是安全处理器 204b 和 / 或会话控制器 208 上实现，以提供另一个独立的安全层。可选择地，读 / 写 / 订阅端点处理器 212 可被用来提供对每个读、写、和 / 或订阅端点的访问。

[0060] 对每个读 / 写 / 订阅端点处理器 212，资源发现端点处理器 210 和 / 或会话控制器 208 可将客户应用 202 选择的资源和 / 或那些资源的相关的难以理解的标识符传送至相应的读 / 写 / 订阅端点处理器 212。这些难以理解的标识符可由客户应用 202、由资源发现端点处理器 210 或、可选择地由这二者分配。

[0061] 通过存储标识符参考信息，示例读 / 写 / 订阅端点处理器 212 为每个客户应用 202 管理哪个标识符对应哪种资源。这样，读 / 写 / 订阅端点处理器 212 和客户应用 202 之间的通信可使用标识符作为保护形式，来对抗可能企图监视该通信的未授权的第三方或实体。在一些实施例中，多个客户应用可对于不同的资源使用相同的标识符。类似地，相同的客户可对于通过不同端点可访问的不同的资源使用相同的标识符。可选择地，相同资源的不同的标识符可被相同的客户用来通过不同的端点访问资源。在这些实施例中，资源发现端点处理器 210 管理这些标识符向资源和 / 或向读 / 写 / 订阅端点处理器 212 的分配。读 / 写 / 订阅端点处理器 212 为每个客户应用 202 管理标识符的使用，以访问相关联的资源。

[0062] 示例会话控制器 208 也可为客户应用 202 管理读端点、写端点、和 / 或订阅端点的难以理解的标识符。例如，会话控制器 208 可存储每个读、写、和 / 或订阅端点以及相应的难以理解的标识符，该标识符由资源发现端点处理器 212 分配。

[0063] 而且，示例会话控制器 208 验证并指挥来自客户应用 202 的请求消息。验证确保在请求消息中识别的会话是有效的和 / 或被授权访问预期的处理器 210 和 / 或 212。拟针对服务器 114a 的资源发现端点的有效的请求消息可被会话控制器 208 路由至资源发现端点处理器 210。类似地，拟针对读端点、写端点、和 / 或订阅端点的有效的请求消息可被会话控制器 208 路由至适当的读 / 写 / 订阅端点处理器 212。此外，会话控制器 208 可通过确定在消息内所识别的会话是否有效和 / 或通过确定与读、写、和 / 或订阅端点相关联的难以理解的标识符是否有效，来验证请求消息。拟针对读、写、和 / 或订阅端点的有效的请求消息然后被会话控制器 208 路由至相应的读 / 写 / 订阅端点处理器 212。

[0064] 当客户应用 202 发送消息指示客户应用 202 终止对资源发现服务器 114a 的访问时，图 2 的示例会话控制器 208 终止会话。一旦接收到终止消息，会话控制器 208 删除存储的会话信息，包括资源、读端点、写端点和 / 或相应的标识符。如果客户应用 202 企图从删除的会话访问任何资源和 / 或端点，则客户应用 202 将被要求启动新的会话并为每种资源注册。

[0065] 为管理和 / 或控制对资源和相关端点的访问，图 2 的示例资源发现服务器 114a 包括资源发现端点处理器 210。示例资源发现端点处理器 210 通过会话控制器 208 从客户应用 202 接收请求消息（例如，发现资源请求消息、开启端点请求消息、和 / 或注册请求消息）。

一旦接收到请求消息，资源发现端点处理器 210 可使用该请求消息内的和 / 或与该请求消息相关联的信息，来控制对客户应用 202 可能发现并随后访问的资源的访问。例如，服务器发现端点处理器 206 可检查请求消息内的用户标识字段，以确定客户应用 202 被授权访问哪些资源。可选择地，示例资源发现端点处理器 210 可检查请求消息内的工作站标识值、客户应用类型、客户应用序列号、客户应用地点、和 / 或协议类型。

[0066] 示例资源发现端点处理器 210 可使用访问列表来确定客户应用可访问哪些资源。访问列表可包括授权的用户、工作站和 / 或客户应用的列表，该表中的每一个参照资源列表。在一些示例实现中，资源列表可包括对应一组资源的代码。一旦确定客户应用 202 被授权访问哪些资源，资源发现端点处理器 210 向客户应用 202 提供那个资源列表。列表可包括资源名称、包括在资源内的信息、和 / 或关于资源的编码信息。在一些实施例中，列表可包括组合在一起成为集合的资源。在这些实施例里，客户应用可通过选择集合访问该集合内一些或全部资源。

[0067] 如果被授权，示例资源发现端点处理器 210 向客户应用 202 提供读、写、和 / 或订阅端点，可分配一个或更多所选择的资源给上述端点。此外，资源发现端点处理器 210 将每个所选择的资源添加到读、写、和 / 或订阅端点上，该读、写、和 / 或订阅端点由相应的会话控制器（例如，会话控制器 208）和 / 或共享的读 / 写 / 订阅端点处理器 212 管理。资源发现端点处理器 210 可传送每个所选择的资源，使得读 / 写 / 订阅端点处理器 212 可将每个资源添加到读、写、和 / 或订阅端点上。

[0068] 而且，示例资源发现端点处理器 210 为每个所选择的资源产生标识符并向客户应用 202 传送该标识符。例如，如果客户应用 202 选择油箱资源，资源发现端点处理器 210 可为该油箱资源分配难以理解的标识符“DM45”。资源发现端点处理器 210 向客户应用 202 传送这个标识符 DM45。当提及该油箱资源时，客户应用 202 和资源发现服务器 114a 之间随后的通信可使用标识符 DM45。

[0069] 示例资源发现端点处理器 210 接收注册请求消息和 / 或开启端点请求消息，来创建和 / 或开启一个或更多读、写、和 / 或订阅端点，所选择的资源可被添加到这些端点。资源发现端点处理器 210 确定产生注册请求消息的客户应用 202 是否被授权读、写、和 / 或订阅所选择的资源。通常地，如果给客户应用 202 提供对资源的访问，则该客户应用 202 被允许对该资源的读和 / 或订阅访问。然而，客户应用 202 可能不能对该资源进行写访问。

[0070] 资源发现端点处理器 210 也通过使用资源访问控制来确定客户应用 202 是否被授权写访问。例如，端点访问控制可利用可包括授权用户和 / 或客户应用 202 列表的访问控制列表。如果客户应用 202 被授权写访问，则资源发现端点处理器 210 按照请求，为客户应用 202 选择的资源创建和 / 或开启一个或更多授权的写端点。资源发现端点处理器 210 然后添加所选择的资源，客户应用 202 被授权将其写入新创建和 / 或开启的写端点。

[0071] 为管理读端点、写端点、订阅端点和对过程控制资源的访问，图 2 的示例资源发现服务器 114a 包括读 / 写 / 订阅端点处理器 212。该读 / 写 / 订阅端点处理器 212 通过使用对请求访问资源的消息的端点访问控制，来确定客户应用 202 是否被授权读、写、和 / 或订阅访问。例如，端点访问控制可利用可包括授权用户和 / 客户应用 202 列表的访问控制列表。如果读 / 写 / 订阅端点处理器 212 接收对给定资源的读、写、或订阅请求，则读 / 写 / 订阅端点处理器 212 确认客户应用 202 被授权对那个资源的读、写、和 / 或订阅访问。

[0072] 此外，示例读 / 写 / 订阅端点处理器 212 提供和 / 或准许通过通信路径 214 对资源的访问。例如，所选择的资源可位于图 1 的控制器 122 中。当客户应用 202 传送消息来读、写、和 / 或订阅所选择的资源时，示例读 / 写 / 订阅端点处理器 212 使用消息中难以理解的标识符来访问控制器 122 内的资源。对发送给读端点的消息，读 / 写 / 订阅端点处理器 212 检索想要的资源（例如，值、警报、和 / 或事件）。类似地，对发送给写端点的消息，读 / 写 / 订阅端点处理器 212 向资源（例如，图 1 的控制器 122）写数据。

[0073] 为存储由服务器发现端点处理器 206 使用的端点访问控制信息，资源发现端点处理器 210、和 / 或读 / 写 / 订阅端点处理器 212、图 2 的示例服务器 108 和 114a 被通信地耦合到访问控制数据库 220。在一些实施例中，访问控制数据库 220 可被包括在服务器 108 和 / 或 114a 中。可选择地，示例访问控制数据库 220 可被包括在过程控制系统 104a-c 中和 / 或包括在图 1 的过程控制场所 102 中。而且，访问控制数据库 220 可被包括在过程控制场所 102 的中央访问控制系统中。示例访问控制数据库 220 可由 EEPROM、RAM、ROM、和 / 或任何其他类型的存储器实现。此外，访问控制数据库 220 可由结构化查询语言 (SQL) 服务器和 / 或任何其他数据库技术实现。安全管理员或其他授权用户可访问该访问控制数据库 220，以更新、添加、删除、和 / 或修改访问控制列表中的授权用户和他们的访问级别。

[0074] 尽管图 2 中描述了实现服务器发现服务器 108 和资源发现服务器 114a 的示例方式，图 2 中所示出的接口、数据结构、单元、过程和 / 或设备中的一个或更多可被结合、划分、重组、省略和 / 或以任何其他方式施行。例如，图 2 中示出的安全处理器 204a-b、示例服务器发现端点处理器 206、示例会话控制器 208、示例资源发现端点处理器 210、示例读 / 写 / 订阅端点处理器 212、和 / 或示例访问控制数据库 220 可使用例如由一个或更多计算设备和 / 或计算平台（例如图 5 的示例处理平台 500）执行的机器可访问或可读的指令，来单独实现和 / 或在任何组合中实现。

[0075] 进一步地，示例安全处理器 204a-b、示例服务器发现端点处理器 206、示例会话控制器 208、示例资源发现端点处理器 210、示例读 / 写 / 订阅端点处理器 212、示例访问控制数据库 220 和 / 或，更一般地，服务器发现服务器 108 和 / 或资源发现服务器 114a，可由硬件、软件、固件和 / 或硬件、软件和 / 或固件的任何组合实现。这样，例如，示例安全处理器 204a-b、示例服务器发现端点处理器 206、示例会话控制器 208、示例资源发现端点处理器 210、示例读 / 写 / 订阅端点处理器 212、示例访问控制数据库 220 和 / 或，更一般地，服务器发现服务器 108 和 / 或资源发现服务器 114a 中的任何一个，可由一个或更多电路、可编程处理器、专用集成电路 (ASIC)、可编程逻辑设备 (PLD) 和 / 或现场可编程逻辑设备 (FPLD) 等来实现。

[0076] 图 3 是描述由图 1 和 2 的示例服务器发现服务器 108 和资源发现服务器 114a 提供的示例分层的安全防护的图 300。分层的安全防护图 300 包括访问服务器发现端点 302、资源发现端点 304、读端点 306、写端点 308、和订阅端点 310 的图 2 的客户应用 202。分层的安全防护图 300 描述客户应用 202 访问过程控制系统 104a 中的资源的示例过程。

[0077] 初始时，图 3 的客户应用 202 访问图 1 和 2 的服务器发现服务器 108 的服务器发现端点 302。服务器发现端点 302 包括客户应用 202 可利用的资源发现服务器列表。此外，与服务器发现端点 302 中的服务器的列表相邻的哈希框 (hashedbox) 代表图 2 的安全处理器 204a。资源发现服务器列表可通过将客户应用 202 匹配到该客户应用 202 被授权访问的

资源发现服务器来确定。客户应用 202 可选择列出的服务器中的一个或更多。通过选择列出的服务器，服务器发现端点 302 向客户应用 202 提供针对所选择的服务器的端点。可选择地，服务器发现端点 302 可同时向客户应用 202 提供每个资源发现服务器的资源发现端点 304。

[0078] 下一步，客户应用 202 使用服务器发现端点 302 提供的端点来访问资源发现端点 304。可选择地，在客户应用 202 被初始地配置有端点和 / 或资源发现端点 304 的地址的实施例中，客户应用 304 可在没有首先访问服务器发现端点 302 的情况下，访问资源发现端点 304。资源发现端点 304 包括可被客户应用 202 访问的资源列表。该资源列表可包括资源组和 / 或个体资源。此外，与资源发现端点 304 中的服务器列表相邻的哈希框代表图 2 的安全处理器 204b。在示例实现中，客户应用 202 可从可用资源列表选择一个或更多资源来注册。在这些实施例中，客户应用 202 请求资源发现端点 304 创建和 / 或开启一个或更多读端点 306、一个或更多写端点 308、和 / 或一个或更多订阅端点 310。此外，客户应用指定所选择的资源中的哪一个将被与新创建和 / 或开启的读端点 306、新创建和 / 开启的写端点 308、和 / 或新创建和 / 或开启的订阅端点 310 相关联。客户应用可在端点被创建和 / 或开启时、在端点被创建和 / 或开启之后、和 / 或在端点被创建和 / 或开启的期间指定资源。

[0079] 一旦客户应用 202 创建和 / 或开启读端点 306、写端点 308、和 / 或订阅端点 310，资源发现端点 304 向客户应用 202 提供与每个新创建和 / 或开启的端点 306-310 相关联的难以理解的标识符。此外，一旦选择资源并向读端点 306、写端点 308、和 / 或订阅端点 310 分配该资源，所选择的资源被包括在读端点 306、写端点 308、和 / 或订阅端点 310 中的选择资源列表内。

[0080] 对添加到读端点 306、写端点 308、和 / 或订阅端点 310 的每个资源，对应于该资源的难以理解的标识符或者，可选择地，难以理解的标识符对（例如，一个由客户应用 202 分配以及一个由资源发现端点 304 分配）被资源发现端点 304 传送给客户应用 202。客户应用 202 可以通过经由读端点 306 访问资源数据来读取与所选择的资源相关联的数据（例如，值、警报、和 / 或事件）。类似地，客户应用 202 可通过经由写端点 308 访问资源来向资源写入数据。客户应用 202 也可通过经由订阅端点 310 访问资源来订阅资源数据。

[0081] 图 4A 和 4B 为流程图，描述可被执行来实现图 1、2 和 / 或 3 的示例服务发现服务器 108、示例资源发现服务器 114a-c、示例客户应用 202、和 / 或示例过程控制环境 100 的示例过程。图 4A 和 4B 的示例过程可由处理器、控制器和 / 或其他适当的处理设备来执行。例如，图 4A 和 4B 的示例过程可在编码指令中体现，该编码指令存储在任何可触知的计算机可读的介质中，如闪存、CD、DVD、软盘、ROM、RAM、可编程 ROM(PROM)、电子可编程 ROM(EPROM)、电子可擦除 PROM(EEPROM)、光学存储盘、光学存储设备、磁存储盘、磁存储设备、和 / 或可用来携带或存储以方法、过程或数据结构形式存在的程序编码和 / 或指令的任何其他介质中，该介质可被处理器、通用或专用计算机、或带有处理器的其他机器（例如，以下结合图 5 讨论的示例处理器平台 500）访问。以上介质的组合也包括在计算机可读介质的范围内。

[0082] 过程包括例如引起处理器、通用计算机、专用计算机、或专用处理机器实现一个或更多特定过程的指令。可选择地，图 4A 和 / 或 4B 的示例操作中的一些或全部可使用 ASIC、PLD、FPLD、离散逻辑、硬件、固件等的任何组合来实现。

[0083] 此外，图 4A 和 / 或 4B 的示例操作中的一个或更多可使用一个或更多手动操作或

如任何上述技术的任何组合来实现，例如，固件、软件、离散逻辑和/或硬件的任何组合。进一步地，可利用实现图4A和/或4B的示例操作的任何其他过程。例如，可改变方框(block)的执行顺序，和/或可改变、消除、再分割、或组合所描述的方框中的一个或更多。此外，例如通过独立的处理线程、处理器、设备、离散逻辑、电路等，图4A和/4B中的任何或所有示例操作可顺序执行和/或并列执行。

[0084] 图4A和4B的示例过程400为图1的示例过程控制环境100中的接口访问控制提供分层的安全防护。此外，示例过程400可为包括制造自动化系统、工业系统等的其他类型的数据系统的接口访问控制提供分层的安全防护。而且，示例过程400可针对每个访问服务器发现服务器(例如，图1的服务器发现服务器108)中的端点的请求来执行。对访问服务器发现服务器108的每个请求，示例过程400可与示例过程400的其他实例串行和/或并行。

[0085] 示例过程400在接收到访问服务器发现服务器108中的端点的发现服务器请求消息时开始(方框402)。请求消息可源自位于远程工作站(例如，远程工作站116和/118)上的客户应用或，可选择地，源自本地工作站(例如，本地工作站106)。示例过程400通过检查与请求消息相关联的特权，确定服务器发现服务器108是否是该消息可访问的或可用的(方框404)。例如，过程400可检查请求消息中的用户标识字段来确定用户标识值是否对应于授权用户。可选择地，示例过程400可检查工作站标识值、客户应用类型、客户应用序列号、客户应用位置、和/或用于传递消息的协议来确定请求消息的发起者是否被授权来访问服务器发现服务器404。

[0086] 如果示例过程400确定请求消息未被授权访问服务器发现服务器108(方框404)，过程400产生和/或传送响应消息给客户应用(406)。响应消息可拒绝访问服务器发现服务器108的请求。一旦产生和传送响应消息(方框406)，示例过程400结束。

[0087] 然而，如果示例过程400确定请求消息被授权访问服务器发现服务器108(方框404)，该请求消息在服务器发现服务器108内被接收(方框408)。示例过程400然后确定哪些资源发现服务器(例如，资源发现服务器114a-c)被授权由与请求消息相关联的客户应用来访问(方框410)。客户应用可用的资源发现服务器可基于请求消息内的和/或与请求消息相关联的标识字段、工作站标识值、客户应用类型、客户应用序列号、客户应用位置、和/或协议。

[0088] 如果示例过程400确定没有授权的资源发现服务器(例如，空的资源发现端点列表)，指示没有可用的资源发现服务器的消息被产生和/或被传送给客户应用(方框414)。一旦传送消息(方框414)，示例过程400结束。

[0089] 然而，如果存在至少一个授权的资源发现服务器(方框412)，示例过程400向客户应用提供批准和/或授权的资源发现端点(例如，资源发现服务器114a-c的资源发现端点)的列表(方框416)。在其他实施例中，可为向客户应用提供资源发现端点列表的每个资源发现服务器提供端点。下一步，客户应用选择列表资源发现端点中的一个或更多(方框418)。在其他实施例中，客户应用可以不选择资源发现端点和/或可以结束示例过程400。

[0090] 当接收到访问所选择的资源发现端点(例如，资源发现服务器114a)的请求消息时，示例过程400继续(方框420)。可选择地，在客户应用被初始地配置有资源发现端点的实施例中，示例过程400可在接收到访问资源发现端点的请求消息(例如，连接消息)时

开始（方框 420）。请求消息由客户应用产生和／或传送。此外，当示例过程 400 接收访问资源发现端点的请求消息，示例过程 400 为客户应用开启会话。在其它实施例中，客户应用可选择多个资源发现端点。在这些实施例中，示例过程 400 可为每个选择的资源发现端点开启会话。此外，对每个选择资源发现端点，示例过程 400 可运行方框 420-446 的独立的实例。

[0091] 一旦接收到访问资源发现端点的请求消息（方框 420），示例过程 400 确定所选择的资源发现端点的哪些资源是客户应用可用的（方框 422）。客户应用可用的资源可基于请求消息内的和／或与请求消息相关联的标识字段、工作站标识值、客户应用类型、客户应用序列号、客户应用位置、和／或协议。此外，可由过程控制场所 102 的操作员、管理员、和／或用户为客户应用预先定义可用的资源。示例过程 400 然后确定是否有与请求消息相关联的可用资源（方框 424）。如果没有可用和／或授权的资源，示例过程 400 可再次提供资源发现端点列表，使得客户应用可选择另一个资源发现端点（方框 416）。此外，示例过程可关闭与客户应用的会话。

[0092] 如果存在至少一个可用的资源（方框 424），示例过程 400 然后向客户应用提供可用资源的列表（方框 426）。下一步，客户应用可请求注册来访问列出的资源之一（方框 428）。可选择地，客户应用可在同一请求中请求注册来访问多于一个的列出的资源。在其它示例实现中，客户应用可选择另一个资源发现端点或结束示例过程 400。

[0093] 一旦选择了资源来注册（方框 428），客户应用向资源发现端点传送针对所选择资源的标识符（方框 430）。该标识符仅为客户应用和包括所选择资源的资源发现端点的资源发现服务器所知。当资源发现端点从客户应用接收标识符时，与该资源发现端点相关联的资源发现服务器存储为会话情境内的资源所传送的标识符。这些标识符对企图访问客户应用（例如，工作站 106、116 和／或 118）和资源发现服务器（例如，资源发现服务器 114a-c）之间的通信的未授权用户是难以理解的。下一步，示例过程 400 确定客户应用是否已经请求了额外的资源（方框 432）。如果客户应用已经请求了其它资源，该客户应用向资源发现端点发送针对该资源的请求（方框 428）。在其它实施例中，一旦客户应用选择了资源（方框 428），示例过程 400 可向客户应用传送针对所选择资源的标识符（方框 430）。然后，一旦接收到标识符，客户应用使用该标识符与资源发现服务器通信。

[0094] 如果客户应用不选择额外的资源来注册（方框 432），示例过程 400 确定客户应用是否已经请求创建和／或开启读、写、和／或订阅端点（方框 434）。如果客户应用不请求创建和／或开启端点，示例过程 400 确定客户应用是否请求向已经创建的端点分配一个或更多资源（方框 442）。

[0095] 然而，如果客户应用请求创建和／或开启读、写、和／或订阅端点（方框 434），客户应用发送请求来创建和／或开启端点。当示例过程 400 接收到请求，示例过程 400 通过根据安全标准确定客户应用是否被授权创建和／或开启端点来处理该请求（方框 436）。安全标准可包括请求者的身份和／或工作职责、请求工作站和／或计算机的网络地址、客户应用的身份和／或类型、客户应用用来访问资源发现端点的协议、和／或端点接收到请求的时间。如果示例过程 400 授权客户应用，示例方法 400 创建和／或开启所请求的端点并向客户应用传送相关标识符（方框 438）。标识符可以是会话专用并可仅为资源发现端点和客户应用所知。

[0096] 下一步，示例过程 400 确定客户应用是否已经请求创建和 / 或开启另一个读、写、和 / 或订阅端点（方框 440）。如果客户应用已经请求额外的端点，示例过程 400 处理该请求（方框 436）。在一些实施例中，客户应用可被授权选择资源并向读端点、写端点、和 / 或订阅端点分配那些资源。在这些情形中，示例过程 400 确定客户应用是否已经请求向所请求的读、写、和 / 或订阅端点分配一个或更多资源（方框 442）。如果客户应用已经请求分配一个或更多资源，示例过程 400 通过授权该请求并向请求开启和 / 或创建的端点分配所选择的资源来处理该请求（方框 444）。示例过程 400 然后通过标识符提供和 / 或准许对所选择资源的访问，直到客户应用请求终止会话（方框 446）。此外，如果客户应用尚未请求分配一个或更多资源（方框 442），示例过程 400 通过标识符提供和 / 或准许对资源的访问（方框 466）。进一步地，客户应用可在会话开启的同时递交额外的请求，如在方框 428、434、和 / 或 442 中所描述的。一旦接收到终止会话的请求，示例过程终止会话和对端点和相关资源的访问（方框 448）。示例过程 400 然后结束。

[0097] 图 5 是可被用来实现在此描述的示例方法和装置的示例处理器系统 500 的框图。例如，与示例处理器系统 500 类似或等同的处理器系统可被用来实现图 1 和 / 或图 2 的示例服务器发现服务器 108、示例资源发现服务器 114a-c、示例客户应用 202、示例安全处理器 204a-b、示例服务器发现端点处理器 206、资源发现端点处理器 210、和 / 或读 / 写 / 订阅端点处理器 212。尽管示例处理器系统 500 在以下被描述成包括多个外围设备、接口、芯片、存储器等，但那些单元中的一个或更多在用来实现示例服务器发现服务器 108、示例资源发现服务器 114a-c、示例客户应用 202、示例安全处理器 204a-b、示例服务器发现端点处理器 206、资源发现端点处理器 210、和 / 或读 / 写 / 订阅端点处理器 212 中的一个或更多的其它示例处理器系统中可被省略。

[0098] 如图 5 中所显示的，处理器系统 500 包括耦合到互连总线 514 的处理器 512。处理器 512 包括寄存器组或寄存器空间 516，其在图 5 中被描述成完全在芯片上，但是可选择地，其可完全或部分不在芯片上，并可通过专用电气连接和 / 或互连总线 514 直接耦合到处理器 512。处理器 512 可以是任何适当的处理器、处理单元或微处理器。尽管图 5 中未显示，系统 500 可以是多处理器系统并且，从而可包括一个或更多额外的处理器，该额外的处理器等同于或类似于处理器 512 并通信地耦合到互连总线 514。

[0099] 图 5 的处理器 512 耦合到芯片组 518，其包括存储器控制器 520 和外围输入输出 (I/O) 控制器 522。众所周知，芯片组典型地提供 I/O 和存储器管理功能以及多个通用和 / 或专用的寄存器、时钟等，该多个通用和 / 或专用的寄存器、时钟等对于耦合到芯片组 518 的一个或多个处理器是可用的或可被其使用。存储器控制器 520 执行使处理器 512（或者多个处理器，如果有多个的话）能够访问系统存储器 524 和大容量存储存储器 (mass storage memory) 525 的功能。

[0100] 系统存储器 524 可包括任何想要类型的易失性和 / 或非 - 易失性存储器，例如静态随机访问存储器 (SRAM)、动态随机访问存储器 (DRAM)、闪存、只读存储器 (ROM) 等。大容量存储存储器 525 可包括任何想要类型的大容量存储设备。例如，如果示例处理器系统 500 被用来实现服务器发现服务器 108 和 / 或资源发现服务器 114a（图 1），则大容量存储存储器 525 可包括硬盘驱动器、光学驱动器、磁带存储设备等。可选择地，如果示例处理器系统 500 被用来实现访问控制数据库 220，则大容量存储存储器 525 可包括固态存储器（例如，

闪存、RAM 存储器等）、磁存储器（例如，硬驱动器）、或适合用于访问控制数据库 220 中的大容量存储的任何其它存储器。

[0101] 外围 I/O 控制器 522 执行使处理器 512 能够通过外围 I/O 总线 532 与外围输入 / 输出 (I/O) 设备 526 和 528 以及网络接口 530 通信的功能。I/O 设备 526 和 528 可以是任何想要类型的 I/O 设备，例如键盘、显示器（例如，液晶显示器 (LCD)、阴极射线管 (CRT) 显示器等）、导航设备（例如，鼠标、跟踪球、电容性触摸板、操纵杆等）等。网络接口可以是使处理器系统 500 能够与另一个处理器系统通信的设备，例如，以太网设备、异步传输模式 (ATM) 设备、802.11 设备、DSL 调制解调器、电缆调制解调器、蜂窝调制解调器等。

[0102] 尽管存储器控制器 520 和 I/O 控制器 522 在图 5 中被描述为芯片组 518 内独立的功能方框，这些方框执行的功能可集成在单个半导体电路中或可使用两个或更多独立的集成电路来实现。

[0103] 以上所描述的示例方法和 / 或装置中的至少一些由运行在计算机处理器上的一个或更多软件和 / 或固件程序来实现。然而，包括但不限于专用集成电路、可编程逻辑阵列和其他硬件设备的专用硬件实现同样可被构造成整体或部分实现在此描述的一些或所有示例方法和 / 或装置。而且，包括但不限于分布式处理或组件 / 对象分布式处理、并行处理、或虚拟机器处理的可选择的软件实现也可被构造成实现在此描述的示例方法和 / 或系统。

[0104] 应当注意到在此描述的示例软件和 / 或固件实现被存储在可触知的存储介质中，如 ：磁介质（例如，磁盘或磁带）；磁 - 光或光学介质如光学盘 ；或固态介质如存储卡或包含一个或更多只读（非易失性）存储器、随机访问存储器、或其它可擦写（易失性）存储器的其它封装。相应地，在此描述的示例软件和 / 或固件可存储在可触知的存储介质中，如以上描述的那些介质或后续的存储媒介。在一定程度上，以上的说明书参照特定的标准和协议描述了示例组件和功能，应理解，本专利的范围并不限于这样的标准和协议。例如，针对互联网和其它分组 - 交换网络传输的每一个标准（例如，传输控制协议 (TCP)/ 互联网协议 (IP)、用户数据报协议 (UDP)/IP、超文本标记语言 (HTML)、超文本传输协议 (HTTP)）代表技术的当前状态的例子。这样的标准被具有相同通用功能的更快或更有效的等同物周期性地取代。具有相同功能的替代标准和协议是本专利所设想的等同物，旨在被包括在附属的权利要求的范围内。

[0105] 此外，尽管这个专利公开了包括在硬件上执行的固件或软件的示例装置和方法，应当注意到，这样的系统仅仅是示意性的，并不应当被作为限定。例如，设想这些硬件和软件组件中的任何或所有可以完全包含在硬件中、完全包含在软件中、完全包含在固件中或在硬件、固件和 / 或软件的一些组合中。相应地，尽管以上的说明书描述了示例方法、系统、和机器可访问的介质，但所述实施例不是实现这样的系统、方法和机器可访问的介质的唯一方式。因而，尽管在此已经描述了某些示例方法、系统、和机器可访问的介质，本专利的覆盖范围并不局限于此。相反，本专利覆盖真正地或根据等同原则清楚地落入所附权利要求范围内的所有方法、系统、和机器可访问的介质。

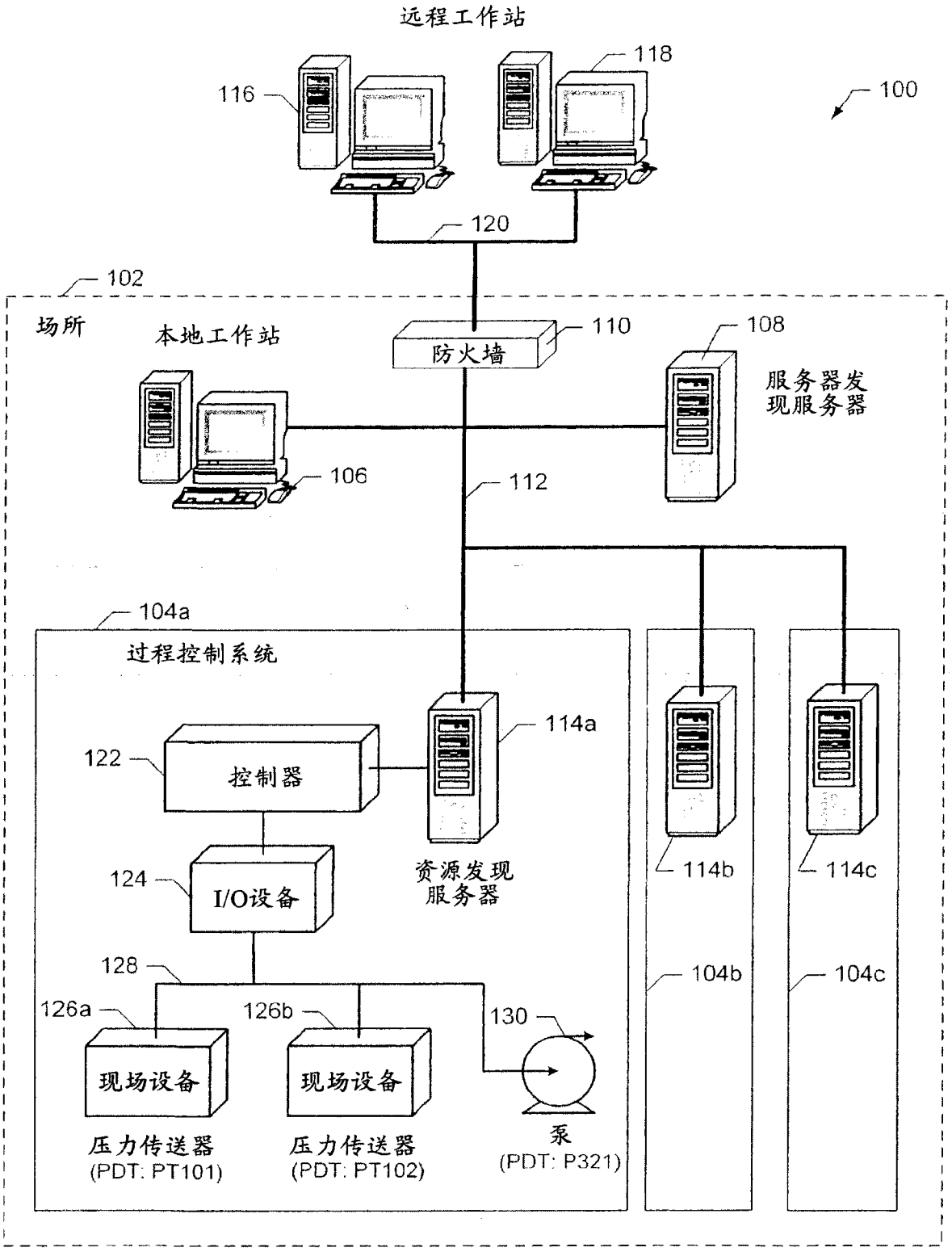

远程工作站
116
118
100
120
102
场所
本地工作站
防火墙
110
108
服务器发现服务器
106
112
104a
过程控制系统
122
控制器
114a
资源发现服务器
124
I/O设备
114b
114c
128
104b
104c
126a
126b
130
现场设备
现场设备
压力传送器
(PDT: PT101)
压力传送器
(PDT: PT102)
泵
(PDT: P321)

图 1

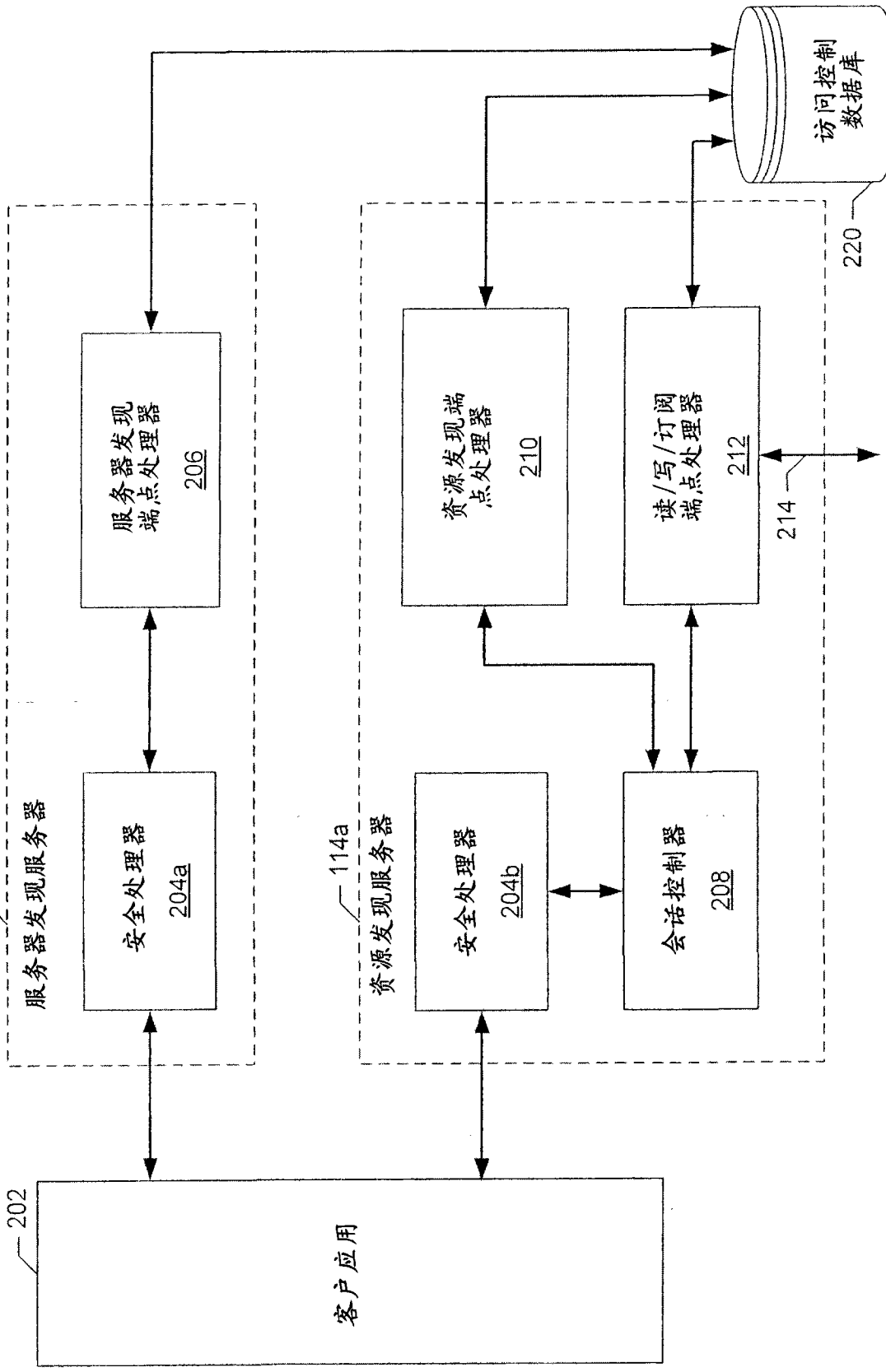

访问控制数据库
220
服务器发现端点处理器 206
资源发现端点处理器 210
读/写/订阅端点处理器 212
214
108
服务器发现服务器
安全处理器 204a
114a
资源发现服务器
安全处理器 204b
会话控制器 208
202
客户应用

图 2

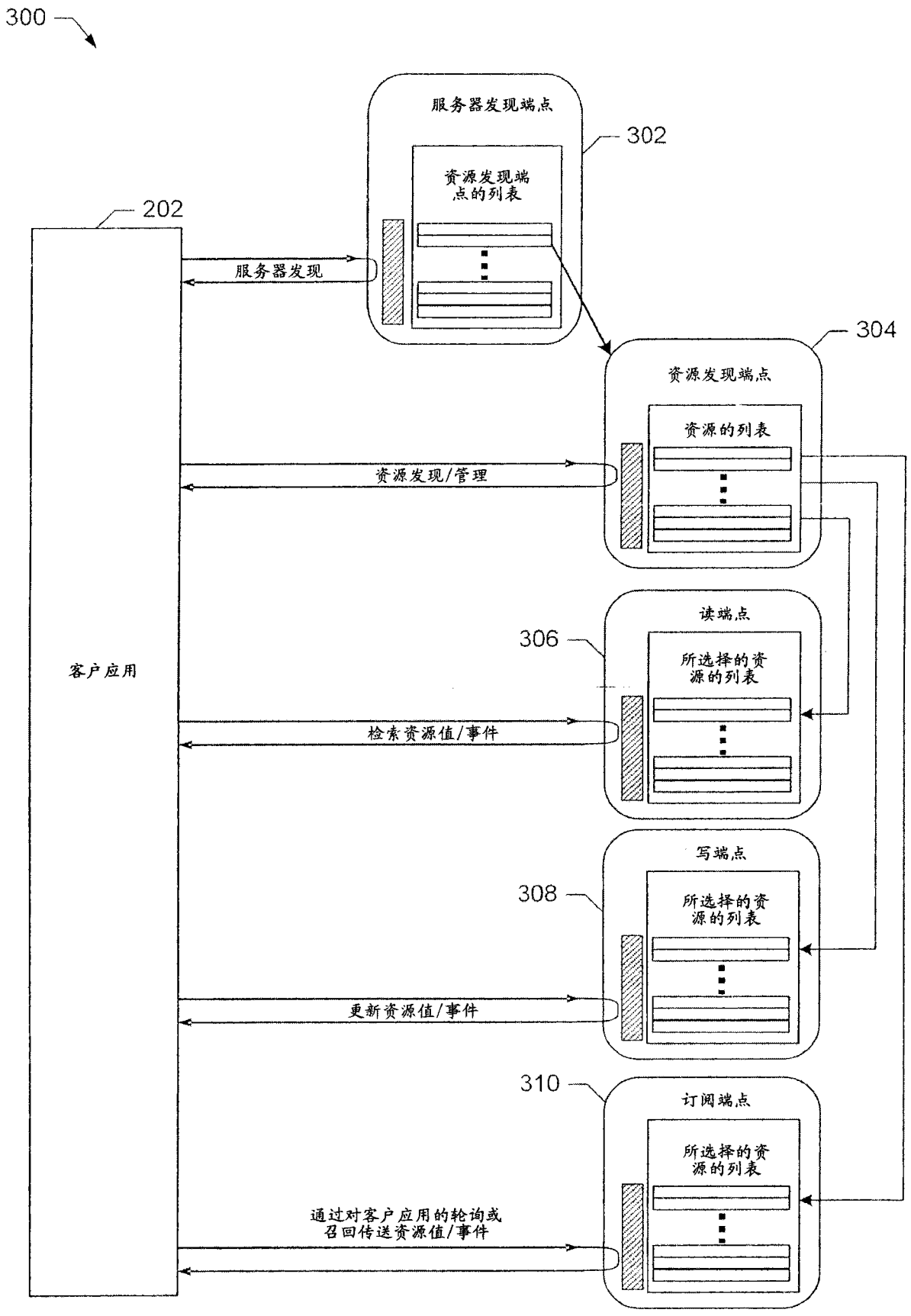

300
服务器发现端点
302
资源发现端点的列表
202
服务器发现
304
资源发现端点
资源的列表
资源发现/管理
读端点
306
所选择的资源的列表
客户应用
检索资源值/事件
写端点
308
所选择的资源的列表
更新资源值/事件
310
订阅端点
所选择的资源的列表
通过对客户应用的轮询或召回传送资源值/事件

图 3

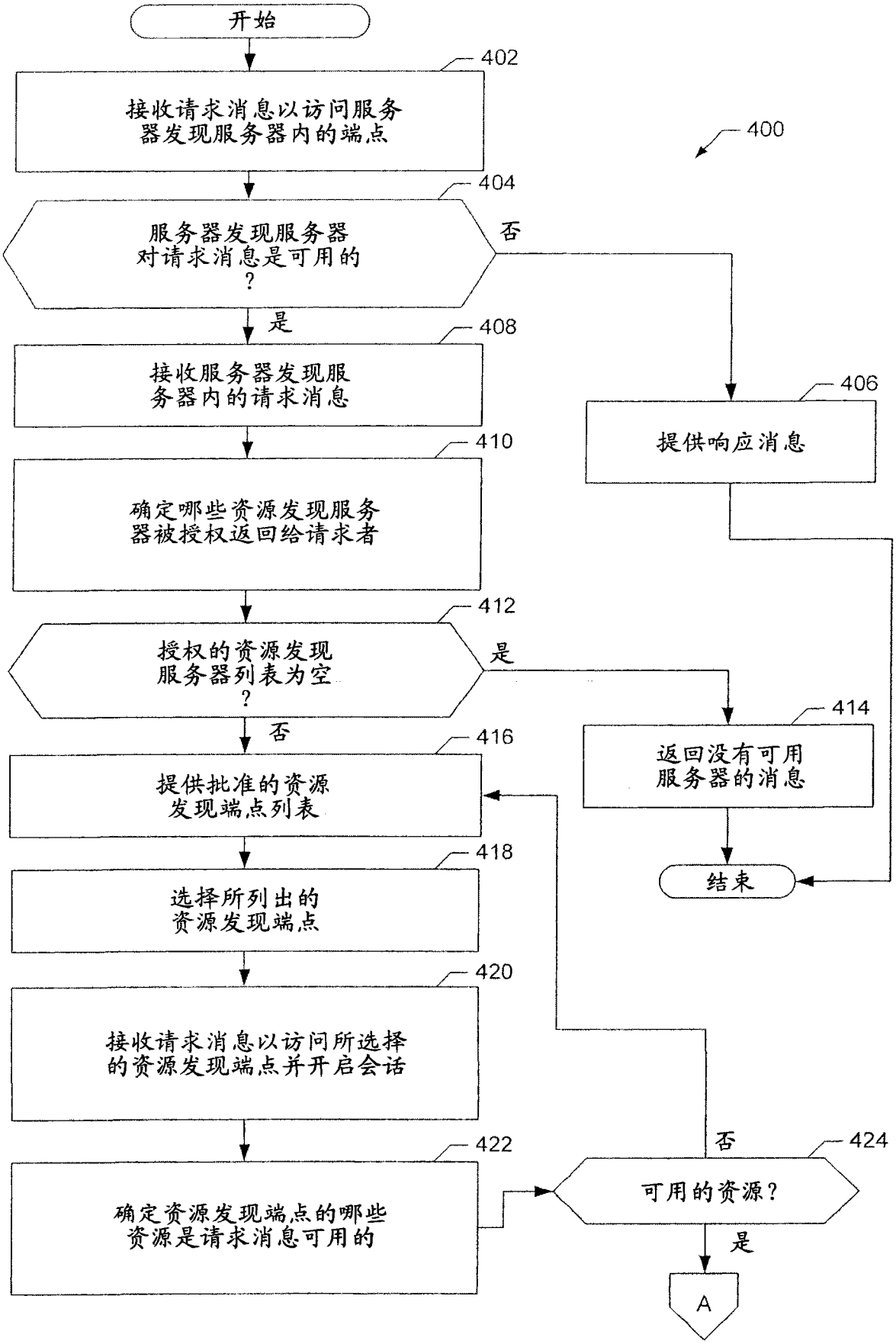

开始
402
接收请求消息以访问服务器发现服务器内的端点
400
404
服务器发现服务器对请求消息是可用的？
否
是
408
接收服务器发现服务器内的请求消息
406
提供响应消息
410
确定哪些资源发现服务器被授权返回给请求者
412
授权的资源发现服务器列表为空？
是
414
返回没有可用服务器的消息
否
416
提供批准的资源发现端点列表
418
选择所列出的资源发现端点
结束
420
接收请求消息以访问所选择的资源发现端点并开启会话
422
确定资源发现端点的哪些资源是请求消息可用的
否
424
可用的资源？
是
A

图 4A

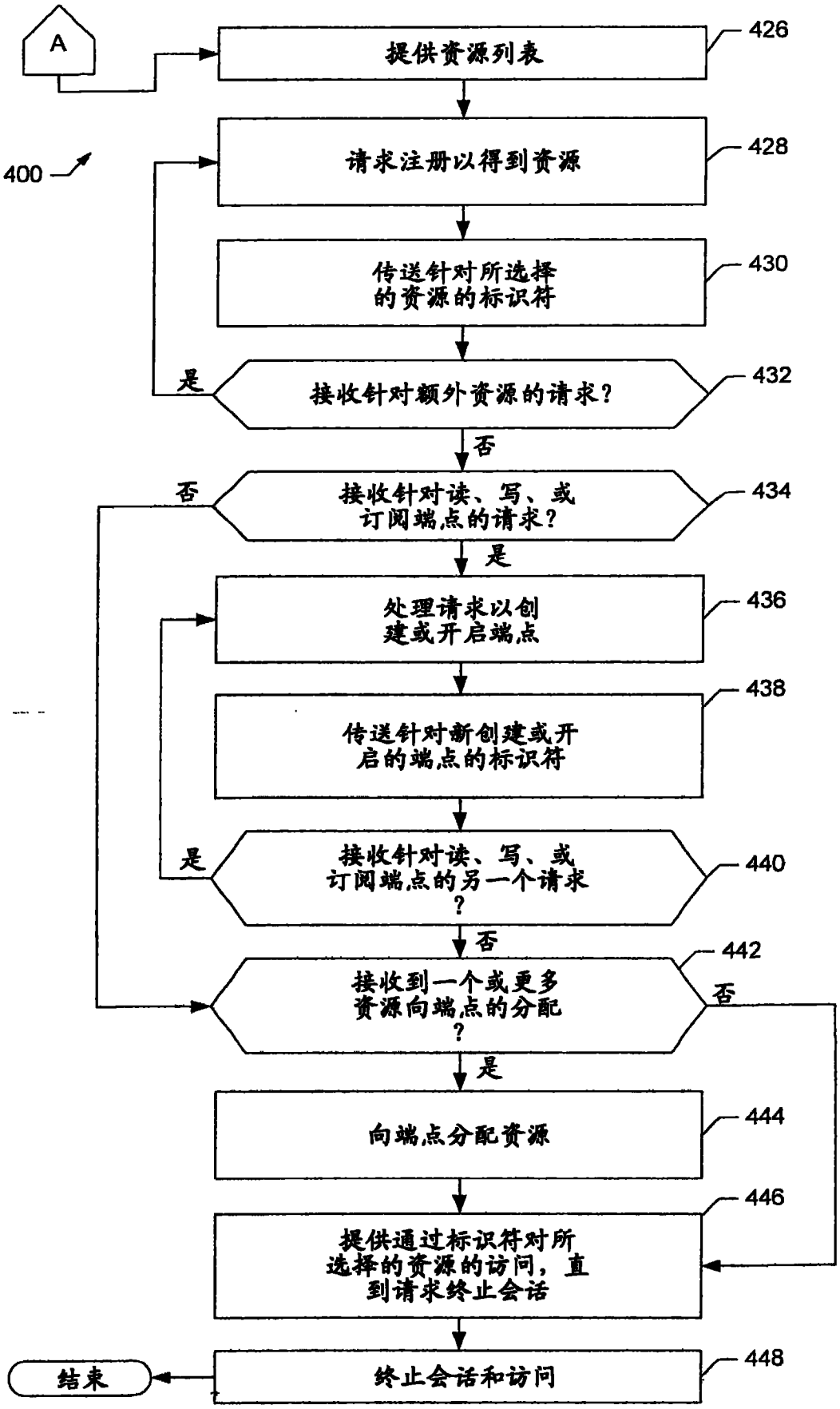

A
提供资源列表
426
400
请求注册以得到资源
428
传送针对所选择的资源的标识符
430
是
接收针对额外资源的请求？
432
否
否
接收针对读、写、或订阅端点的请求？
434
是
处理请求以创建或开启端点
436
传送针对新创建或开启的端点的标识符
438
是
接收针对读、写、或订阅端点的另一个请求？
440
否
接收到一个或更多资源向端点的分配？
442
否
是
向端点分配资源
444
提供通过标识符对所选择的资源的访问，直到请求终止会话
446
结束
终止会话和访问
448

图 4B

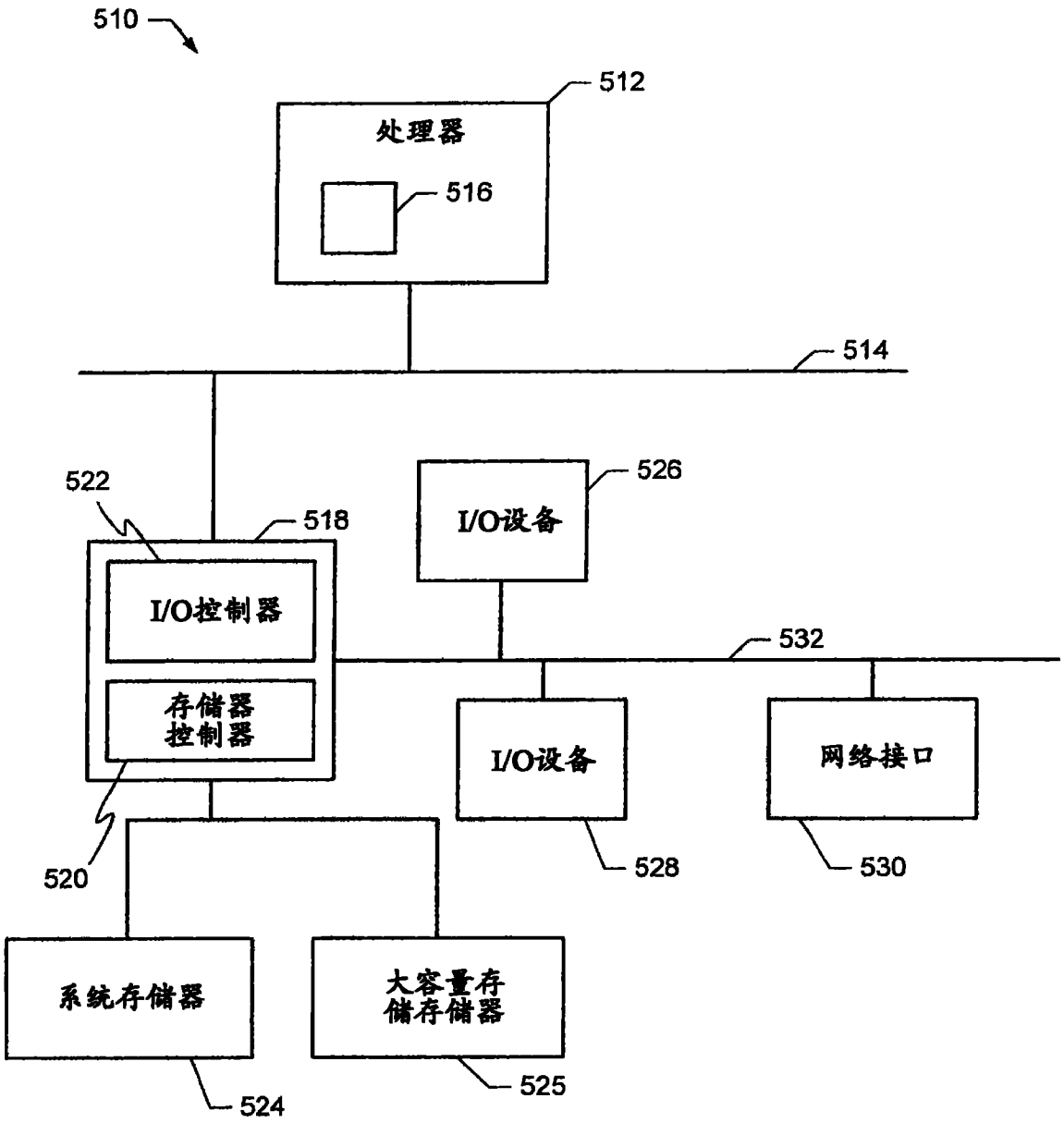

510
512
处理器
516
514
522
518
526
I/O设备
I/O控制器
532
存储器
控制器
I/O设备
网络接口
520
528
530
系统存储器
大容量存
储存储器
524
525

图 5