



(12)发明专利

(10)授权公告号 CN 104618320 B

(45)授权公告日 2019.07.09

(21)申请号 201410615389.0

(51)Int.CI.

(22)申请日 2014.11.05

H04L 29/06(2006.01)

(65)同一申请的已公布的文献号

H04L 29/08(2006.01)

申请公布号 CN 104618320 A

(56)对比文件

(43)申请公布日 2015.05.13

CN 201188626 Y, 2009.01.28,

(30)优先权数据

WO 2013012654 A2, 2013.01.24,

14/072425 2013.11.05 US

WO 2007044832 A2, 2007.04.19,

(73)专利权人 通用电气公司

审查员 李华

地址 美国纽约州

(72)发明人 Y.阿坦纳

(74)专利代理机构 中国专利代理(香港)有限公司 72001

代理人 叶晓勇 刘春元

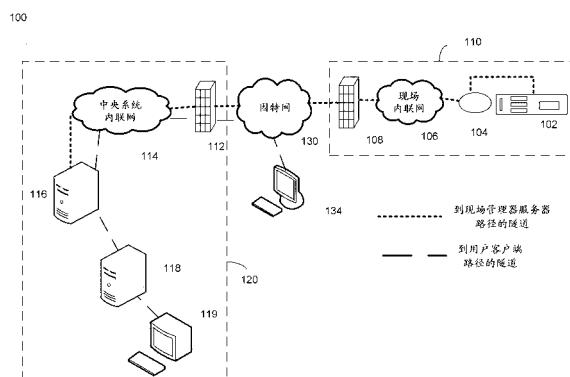
权利要求书2页 说明书8页 附图7页

(54)发明名称

用于安全文件传输的系统和方法

(57)摘要

本公开的实施例能够包括用于安全文件传输的系统和方法。现场监测系统安全文件传输解决方案能够允许由防火墙后面的现场系统通过使用先前开启的连接、经由端口发送异步、并发、并行文件，向中央监测和诊断基础设施来传递操作数据。



1. 一种用于传递数据的方法,包括:
由防火墙后面的现场系统来收集操作数据;
将文件写入传输目录;
调度异步智能传输服务;
建立所述现场系统与中央系统之间的基于安全证书的单向加密链路;
发起用于异步、并发、并行文件上传的命令上传消息;
创建关联出站数据报;
通过预定特定端口来发送所述出站数据报;
由所述中央系统来重构所述出站数据报;
由所述中央系统在对来自所述现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求消息;
由所述现场系统发起用于异步、并发、并行文件下载的下载命令消息;
由所述中央系统创建关联入站数据报;
使用先前开启的连接、通过所述出站单向端口串行地发送入站数据报;以及
由所述现场系统重构所述入站数据报。
2. 如权利要求1所述的方法,还包括由所述中央系统经由对各出站数据报和至少一个完整文件的校验和来对所述出站数据报执行数据传输可靠性。
3. 如权利要求1所述的方法,还包括由所述现场系统对各入站数据报和至少一个完整文件经由校验和来对所述入站数据报执行数据传输可靠性。
4. 如权利要求1所述的方法,其中,发送所述出站数据报包括经由低带宽服务发送所述出站数据报。
5. 如权利要求1所述的方法,其中,收集操作数据包括从与多个传感器进行通信的多个现场控制器来收集所述操作数据。
6. 如权利要求1所述的方法,其中,所述防火墙防止标准双向传输控制协议通信。
7. 如权利要求1所述的方法,还包括使用内插和/或压缩技术来管理所述数据。
8. 如权利要求1所述的方法,还包括确保所述操作数据的质量和时间一致性。
9. 如权利要求1所述的方法,还包括对所述操作数据执行分析和诊断。
10. 一种用于传递数据的系统,包括:
防火墙后面的现场系统,所述现场系统可操作以:
收集操作数据;
将文件写入传输目录;
调度异步智能传输服务;
建立所述现场系统与中央系统之间的基于安全证书的单向加密链路;
发起用于异步、并发、并行文件上传的命令上传消息;
创建关联出站数据报;以及
通过预定特定端口来发送所述出站数据报;以及
所述中央系统可操作以:
至少部分基于所接收出站数据报,来重构所述出站数据报,所述中央系统还可操作以:
在对来自所述现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求

消息；

其中所述现场系统还可操作以：

发起用于异步、并发、并行文件下载的下载命令消息；

其中所述中央系统还可操作以：

创建关联入站数据报；以及

使用先前开启的连接、通过所述出站单向端口串行地发送入站数据报；以及

其中所述现场系统还可操作以：

重构所述入站数据报。

11. 如权利要求10所述的系统，其中，所述中央系统还可操作以：

经由对各出站数据报和完整文件的校验和来对所述出站数据报执行数据传输可靠性。

12. 如权利要求10所述的系统，其中，所述现场系统还可操作以：

经由对各入站数据报和完整文件的校验和来对所述入站数据报执行数据传输可靠性。

13. 如权利要求10所述的系统，其中，所述现场系统还可操作以：

经由低带宽服务来发送所述出站数据报。

14. 如权利要求10所述的系统，其中，所述现场系统还可操作以：

从与多个传感器进行通信的多个现场控制器来收集所述操作数据。

15. 如权利要求10所述的系统，其中，所述防火墙可操作以防止标准双向传输控制协议通信。

16. 如权利要求10所述的系统，其中，所述现场系统还可操作以：

通过使用内插和/或压缩技术来管理所述数据。

17. 如权利要求10所述的系统，其中，所述现场系统还可操作以：

确保所述操作数据的质量和时间一致性。

18. 如权利要求10所述的系统，其中，所述中央系统可操作以：

对所述操作数据执行分析和诊断。

用于安全文件传输的系统和方法

技术领域

[0001] 一般来说,本公开涉及通信安全性,以及具体来说,涉及用于安全文件传输的系统和方法。

背景技术

[0002] 监测和诊断 (M&D) 中心能够为发电站单元以及其它资产提供许多服务。这类服务可包括资产监测、事件跟踪、跳闸事件报告、根本原因分类、强迫断供检测、诊断以及以各种推荐向站点报告。原始操作数据以及后处理数据能够从分析来得出,其可由各种工程组用于性能和可靠性研究、保修支持和工程研发。

[0003] 但是,对要求相对安全文件传输的现有发电站的大集合强加新要求。许多站点需要符合北美电力可靠性协会 (NERC) 或者其它监管安全要求和其它通信安全挑战。另外,这些站点的许多具有有限带宽连接以及相对不稳定或者不可靠链路。

[0004] 通常,现场监测位于发电站基础设施中。现场网络通常通过在发电站边缘的防火墙和代理来保护,其可防止入站连接,并且因而增强现场监测是不可路由的。此外,所有标准双向TCP/HTTP通信端口通常通过防火墙来阻塞,以确保系统的安全性。

[0005] 当前通信通常要求基于双向的通信端口方案,并且当前数据传输技术一般不能够充分应对拨号或者低带宽网络拓扑(例如显著等待时间、紧张状态下的带宽管理)。此外,单向通用文件传输解决方案不可用。

[0006] 为了满足新的和不断增长的客户安全要求,需要相对安全文件传输解决方案,以便为现场监测系统与中央监测和诊断基础设施之间的数据的传输来提供安全数据传输。安全文件传输封装需要被部署,以支持具有有限带宽连接和比较不稳定或者不可靠链路的现场监测站点,其能够符合NERC或者其它监管要求和其它通信安全挑战。

发明内容

[0007] 上述需要的部分或全部可通过本公开的某些实施例得到解决。按照一示例实施例,公开一种用于传递数据的方法,其包括:由防火墙后面的现场系统收集操作数据;将输出文件写入传输目录;调度异步智能传输服务;建立现场系统与中央系统之间的基于安全证书的单向加密链路;发起用于异步、并发、并行文件上传的命令上传消息;创建关联出站数据报;通过预定特定端口发送出站数据报;以及由中央系统重构出站数据报。

[0008] 该方法还可由中央系统在对来自现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求消息;由现场系统发起用于异步、并发、并行文件下载的下载命令消息;由中央系统创建关联安全数据报;使用先前开启连接、通过端口串行地发送入站数据报;以及由现场系统重构入站数据报。

[0009] 在另一个实施例中,公开一种用于传递数据的系统。该系统可包括防火墙后面的现场系统。现场系统可以可操作以收集操作数据,将文件写入传输目录,调度异步智能传输服务,建立现场系统与中央系统之间的基于安全证书的单向加密链路,发起用于异步、并

发、并行文件上传的命令上传消息,创建关联出站数据报,并且通过预定特定端口发送出站数据报。中央系统可以操作以至少部分基于所接收出站数据报来重构出站数据报,并且在对来自现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求消息。

[0010] 本文详细描述并且作为要求保护的本公开的一部分来考虑本发明的其它实施例、特征和方面。参照以下详细描述、附图和权利要求书,能够了解其它实施例、特征和方面。

附图说明

- [0011] 现在将参照附图,附图不一定按比例绘制,包括:
- [0012] 图1是按照本公开的一实施例、用于提供现场监测系统与中央监测和诊断基础设施之间的数据的传输的安全数据传输的示例系统架构的示意框图。
- [0013] 技术方案1:一种用于传递数据的方法,包括:
- [0014] 由防火墙后面的现场系统来收集操作数据;
- [0015] 将输出文件写入传输目录;
- [0016] 调度异步智能传输服务;
- [0017] 建立所述现场系统与中央系统之间的基于安全证书的单向加密链路;
- [0018] 发起用于异步、并发、并行文件上传的命令上传消息;
- [0019] 创建关联出站数据报;
- [0020] 通过预定特定端口来发送所述出站数据报;以及
- [0021] 由所述中央系统来重构所述出站数据报。
- [0022] 技术方案2:如技术方案1所述的方法,还包括:
- [0023] 由所述中央系统在对来自所述现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求消息;
- [0024] 由所述现场系统发起用于异步、并发、并行文件下载的下载命令消息;
- [0025] 由所述中央系统创建关联安全数据报;
- [0026] 使用先前开启的连接、通过所述端口串行地发送入站数据报;以及
- [0027] 由所述现场系统重构所述入站数据报。
- [0028] 技术方案3:如技术方案1所述的方法,还包括由所述中央系统经由对各出站数据报和至少一个完整文件的校验和来对所述出站数据报执行数据传输可靠性。
- [0029] 技术方案4:如技术方案2所述的方法,还包括由所述现场系统对各入站数据报和至少一个完整文件经由校验和来对所述入站数据报执行数据传输可靠性。
- [0030] 技术方案5:如技术方案1所述的方法,其中,发送所述出站数据报包括经由低带宽服务发送所述出站数据报。
- [0031] 技术方案6:如技术方案1所述的方法,其中,收集操作数据包括从与多个传感器进行通信的多个现场控制器来收集所述操作数据。
- [0032] 技术方案7:如技术方案1所述的方法,其中,所述防火墙防止标准双向传输控制协议通信。
- [0033] 技术方案8:如技术方案1所述的方法,还包括使用内插和/或压缩技术来管理所述数据。
- [0034] 技术方案9:如技术方案1所述的方法,还包括确保所述操作数据的质量和时间一

致性。

- [0035] 技术方案10:如技术方案1所述的方法,还包括对所述操作数据执行分析和诊断。
- [0036] 技术方案11:一种用于传递数据的系统,包括:
 - [0037] 防火墙后面的现场系统,所述现场系统可操作以:
 - [0038] 收集操作数据;
 - [0039] 将文件写入传输目录;
 - [0040] 调度异步智能传输服务;
 - [0041] 建立所述现场系统与中央系统之间的基于安全证书的单向加密链路;
 - [0042] 发起用于异步、并发、并行文件上传的命令上传消息;
 - [0043] 创建关联出站数据报;以及
 - [0044] 通过预定特定端口来发送所述出站数据报;以及
 - [0045] 所述中央系统可操作以:
 - [0046] 至少部分基于所接收出站数据报,来重构所述出站数据报。
 - [0047] 技术方案12:如技术方案11所述的系统,其中,所述中央系统还可操作以:
 - [0048] 在对来自所述现场系统的前一消息的应答中向开放出站单向端口发送文件下载请求消息;
 - [0049] 其中所述现场系统还可操作以:
 - [0050] 发起用于异步、并发、并行文件下载的下载命令消息;
 - [0051] 其中所述中央系统还可操作以:
 - [0052] 创建关联安全数据报;以及
 - [0053] 使用先前开启的连接、通过所述端口串行地发送入站数据报;以及
 - [0054] 其中所述现场系统还可操作以:
 - [0055] 重构所述入站数据报。
 - [0056] 技术方案13:如技术方案11所述的系统,其中,所述中央系统还可操作以:
 - [0057] 经由对各出站数据报和完整文件的校验和来对所述出站数据报执行数据传输可靠性。
 - [0058] 技术方案14:如技术方案12所述的系统,其中,所述现场系统还可操作以:
 - [0059] 经由对各入站数据报和完整文件的校验和来对所述入站数据报执行数据传输可靠性。
 - [0060] 技术方案15:如技术方案11所述的系统,其中,所述现场系统还可操作以:
 - [0061] 经由低带宽服务来发送所述出站数据报。
 - [0062] 技术方案16:如技术方案11所述的系统,其中,所述现场系统还可操作以:
 - [0063] 从与多个传感器进行通信的多个现场控制器来收集所述操作数据。
 - [0064] 技术方案17:如技术方案11所述的系统,其中,所述防火墙可操作以防止标准双向传输控制协议通信。
 - [0065] 技术方案18:如技术方案11所述的系统,其中,所述现场系统还可操作以:
 - [0066] 通过使用内插和/或压缩技术来管理所述数据。
 - [0067] 技术方案19:如技术方案11所述的系统,其中,所述现场系统还可操作以:
 - [0068] 确保所述操作数据的质量和时间一致性。

- [0069] 技术方案20:如技术方案11所述的系统,其中,所述中央系统可操作以:
- [0070] 对所述操作数据执行分析和诊断。
- [0071] 图2示出按照本公开的一实施例的示例现场监测系统的示意框图。
- [0072] 图3示出按照本公开的一实施例的示例中央监测和诊断基础设施的示意框图。
- [0073] 图4示出按照本公开的一实施例的示例现场监测系统的原理框图。
- [0074] 图5是示出按照本公开的一实施例、现场监测系统与中央监测和诊断基础设施之间的数据的示范安全文件上传的流程图。
- [0075] 图6是示出按照本公开的一实施例、现场监测系统与中央监测和诊断基础设施之间的数据的示范安全文件下载的流程图。
- [0076] 图7是示出对现场监测系统的示范安全远程访问的流程图。

具体实施方式

[0077] 下面将参照附图更全面地描述本公开的示例实施例,附图中示出部分而不是全部实施例。实际上,本公开可通过许多不同形式来实施,而不应当被理解为局限于本文提出的实施例;相反,提供这些实施例,使得本公开将满足适用法律要求。相似标号通篇表示相似元件。

[0078] 为了实现支持具有有限带宽连接或者相对不稳定或者不可靠链路的发电站的现场监测的安全文件传输,开发了组合各种硬件、软件和组网技术的新基础设施。本公开的某些实施例可具有实现从现场监测系统上的资料库的异步、面向服务的提取以及将数据传递给中央存储资料库供分析处理的技术效果。本公开的某些实施例的另一个技术效果可允许中央监测和诊断基础设施中的所指定服务器与现场监测系统之间的文件的异步、并行、同时下载和上传,同时提供安全性、服务的动态保证和可靠性特征。

[0079] 参照附图的图1,示出用于提供现场监测系统110与中央监测和诊断基础设施之间的数据的传输的安全数据传输的示例系统架构100的示意框图。

[0080] 现场监测系统110可通过使用具有各种组网能力的基于Windows™的平台102(通常为高计算服务器)来实现,并且可共存于公司防火墙108后面的发电站站点。现场网络106可通过在发电站边缘的防火墙108和代理104来保护,其防止入站连接,并且因而增强现场监测是不可路由的。此外,所有标准双向TCP/HTTP通信端口可通过防火墙108来阻塞。

[0081] 现场监测安全远程访问解决方案可为监测和诊断用户119、134提供安全和远程访问现场监测系统110并且执行某些管辖或管理任务的能力。通信安全性可通过将HTTPS/TLS协议栈与称作智能代理的定制软件封装相集成来提供。

[0082] 利用中央系统内联网114的用户119或者连接到外部因特网130的远程用户134可建立到远程企业服务器118的连接。远程企业服务器118可建立与企业隧道服务器116的连接。用户119、134然后可建立到现场监测系统110的用户发起远程桌面协议(RDP)会话。通信安全性可使用封装远程访问会话数据的基于TLS/SSL的隧道方法来提供。

[0083] M&D用户119或远程134可请求到现场监测系统110的RDP连接。由于业务端口443是单向(仅开放出站)的,所以代理服务器116可在对来自驻留于现场监测系统110中的服务器上的智能代理102的任何前一消息的应答中发起RDP会话请求消息。智能代理102则可连接到现场监测系统中的RDP模块。

[0084] 参照图2,所示的是按照本公开的一实施例的现场监测(OSM)200的示例。OSM 200可在具有各种组网能力的基于Windows™的平台(通常为高性能服务器)上实现,并且共存于公司防火墙后面的发电站站点。

[0085] 数据收集软件模块210可与单元的操作和动态数据(例如涡轮机的温度、压力、流率、净空(例如两个组件之间的距离)和振动数据)的收集关联。基于网络连通性和原始数据分辨力的各种类型的控制器用来与单元传感器进行接口。控制器的范围可从专有控制器111到标准以太网数据获取系统(EDAS)113。所收集的原始数据然后可经过处理,并且经由数据集线器传递给其它OSM模块。数据集线器可收集大量实时生产信息,并且执行监控自动化连同可靠信息向高级分析应用的传递。这类数据集线器可包括某些专有集线器,例如WSST 115、CIMPLICITY 117和EHISTORIAN 119收集器模块。另外,这些模块能够提供用于数据质量和时间一致性的组合源。

[0086] 存储软件模块220可与数据存储和归档关联。软件平台22能够是专有平台、例如PROFICY HISTORIAN,并且能够提供本地存储时间序列数据以及分析输出所生成的处理数据的能力。它还能够提供使用各种压缩和内插技术来管理数据质量的能力。

[0087] 数据处理模块230可与数据处理以及事件和告警升级关联。基于分析的数据处理可由专有平台来提供,例如CENTRAL CONDITION ASSESSMENT PLATFORM—LOCAL EDITION(CCAP-LE:中央条件评估平台——本地版)231和连续诊断引擎(CDE)规则引擎平台233。告警和事件升级可由动作引擎235来执行,并且可经由电子邮件或者基于万维网的服务来发送通知。

[0088] 传输模块240可与对中央监测和诊断系统的数据传输关联。两种类型的传输机制一般基于特定安全要求、网络拓扑和可用带宽是可用的。第一机制可平衡历史收集器241与收集器服务,以提供实时数据流播传输。第二机制组合由低带宽和智能代理模块243为安全(单向业务/推送)、异步、并发和可靠文件传输所提供的服务。

[0089] 相应地,至少一个技术效果可实现低带宽和智能代理模块,以提供安全、单向业务、异步、并发和可靠文件传输。

[0090] 图3示出按照本公开的一实施例的示例中央监测和诊断基础设施300。

[0091] 中央系统传输模块310可与从现场系统的数据传输关联。两种类型的传输机制一般是可用的。第一机制可平衡历史收集器与收集器服务311,以提供实时数据流播传输。第二机制可提供用于相对安全(单向业务/推送)、异步、并发和可靠文件传输的较低带宽导入服务313。

[0092] 中央存储软件模块320可与最初收集并且从OSM组所传递的时间序列数据的数据存储和归档关联。这个软件平台可提供用于存储时间序列数据以及分析输出所生成的处理数据的能力。存储模块320可提供全企业数据历史服务,其以极高速度来归档和分配大量实时生产信息。它还可提供使用各种压缩和内插技术来管理数据质量的能力。

[0093] 中央存储软件模块320、例如PROFICY HISTORIAN可以可操作以比较历史数据与实时数据的年份,以便允许无数的分析可能性。这种解决方案可提供跨一组并且对长时间期间来比较资产的工具,以便更好地了解设备和过程如何运载与它们应当如何运行。

[0094] 所示模块330的剩余集合是配置数据库、监测和诊断操作可视化工具、分析规则引擎以及分析运行时环境及关联应用编程接口和面向服务的架构的集合。

[0095] 参照图4,所示的是按照本公开的一实施例的示例现场管理器400的原理框图。管理器400可包括一个或多个处理器402、一个或多个存储器404、一个或多个输入/输出(“I/O”)接口406以及一个或多个网络接口408。管理器400可包括未示出的其它装置。

[0096] 一个或多个处理器402可包括一个或多个核心,并且配置成访问和运行一个或多个存储器404中存储的至少部分指令。一个或多个存储器404能够包括一个或多个计算机可读存储介质(“CRSM”)。一个或多个存储器404可包括但不限于随机存取存储器(“RAM”)、闪速RAM、磁介质、光介质等。一个或多个存储器404因为在提供电力的同时来保留信息所以可以是易失性的,或者因为在没有提供电力的情况下保留信息所以是非易失性的。

[0097] 一个或多个I/O接口406也可在管理器400中提供。这些I/O接口406能够允许耦合装置,例如传感器、键盘、鼠标、监视器、打印机、外部存储器等。一个或多个I/O接口406可允许耦合到各种传感器和控制器,其能够提供跨系统的操作数据。

[0098] 一个或多个网络接口408可提供管理器400与另一个装置之间例如以对等方式直接地、经由网络或者通过这两种方式的数据的传递。一个或多个网络接口408可包括但不限于个人区域网络(“PAN”)、有线局域网(“LAN”)、广域网(“WAN”)、无线局域网(“WLAN”)、无线广域网(“WWAN”)等。一个或多个网络接口408可利用声、射频、光或者其它信号在管理器400与其它装置之间交换数据。

[0099] 一个或多个存储器404可存储供一个或多个处理器402运行以执行某些动作或功能的指令或模块。作为说明而不是限制来包括下列模块。此外,虽然模拟描述为存储在存储器404中,但是在一些实现中,这些模块可至少部分存储在外部存储器中,其是管理器400经由网络接口408或I/O接口406可访问的。这些模块可包括操作系统模块410,其配置成管理例如I/O接口406等的硬件资源,并且向处理器402上运行的应用或模块提供各种服务。

[0100] 收集模块414可存储在存储器404中。模块414可配置成从一个或多个输入装置连续获取数据,并且计算各种参数。软件模块414可与单元的操作和动态数据(例如涡轮机的温度、压力、流率、净空(例如两个组件之间的距离)和振动数据)的收集关联。各种类型的控制器(基于网络连通性能力/原始数据分辨力)用来与单元传感器进行接口。控制器的范围能够从某些专有控制器(例如MARK控制器)到标准以太网数据获取系统(EDAS)。所收集的原始数据然后经过处理,并且经由各种数据集线器传递给其它OSM模块。另外,这些模块可提供用于数据质量和时间一致性的组合源。模块414可在数据仓库412中存储数据和所计算估计。

[0101] 处理模块416可配置成存储和归档数据。软件平台可提供用于本地存储时间序列数据以及分析输出所生成的处理数据的能力。它还可提供使用各种压缩和内插技术来管理数据质量的能力。

[0102] 传输模块418可配置成向中央M&D系统传递数据。第一机制可配置用于收集器对收集器服务,其提供实时数据流播传输。第二机制可组合由低带宽智能代理模块为安全(单向业务/推送)、异步、并发和可靠文件传输所提供的服务。

[0103] 以上参照图4所述的管理器400仅作为举例来提供。根据需要,许多其它实施例、系统、方法、设备和组件可用来控制低于临界温度的燃气涡轮机点火温度。

[0104] 图5是示出按照本公开的一实施例、现场监测系统与中央监测和诊断基础设施之间的数据的示范安全文件上传的流程图500。

[0105] 在框510,低带宽导出服务可从归档器模块来提取数据。框510之后接着框520,其中输出文件可写到上传/下载目录。在框530,可调度异步后台智能传输服务。

[0106] 在框540,智能代理可建立OSM与关联中央文件传输服务之间的安全(基于证书的)单向(使用组网端口443)TLS/SSL加密链路。

[0107] 在步骤、框中,智能代理可发起用于异步、并发、并行文件上传的命令上传消息。框560接着框550,其中智能代理可创建关联HTTPS数据块,并且可在框570通过预先选择端口(这个示例中的端口443)串行地发送数据报。数据传输可靠性经由校验和(对于各数据块和完整文件)以及通过基础传输协议栈所提供的重传和容错机制来执行。框580接着框570,其中HTTPS数据报可通过代理服务器服务来重构,并且呈现给低带宽导入服务。

[0108] 图6是示出按照本公开的一实施例、现场监测系统与中央监测和诊断基础设施之间的数据的示范安全文件下载的流程图600。

[0109] 在框610,代理服务器在对来自智能代理的任何前一消息的应答中发起文件下载请求消息,因为预先选择业务端口(端口443)可以是单向的(仅开放出站)。框610之后接着框620,其中智能代理可发起用于异步、并发、并行文件下载的下载命令消息。在框630,代理服务器创建关联HTTPS数据块,并且在框640使用智能代理先前所开启的连接、通过端口(端口443)串行地发送数据报。数据传输可靠性由代理服务器经由校验和(对于各数据块和完整文件)以及通过基础传输协议栈所提供的重传和容错机制来执行。最后,在框650,HTTPS数据报通过智能代理服务来重构,并且呈现给低带宽导出服务。

[0110] 图7是示出对现场监测系统的示范安全远程访问的流程图700。通信安全性使用封装远程访问会话数据的基于TLS/SSL的隧道方法来提供。

[0111] 在框710,用户可请求到现场监测系统的远程桌面协议(RDP)连接。在框720,代理服务器可在对来自智能代理的任何前一消息的应答中发起RDP会话请求消息,因为业务端口443是单向的(仅开放出站)。

[0112] 在框730,智能代理连接到现场监测系统上的RDP服务器。框740接着框730,其中智能代理在代理服务器开启TLS/SSL隧道。在框750,数据使用验证加密库来加密,以及在框760,智能代理完成认证过程。最后在框770,可建立连接。可通过连接现场监测系统RDP服务器、智能代理、代理服务器和终端用户计算装置之间的中间连接,来建立端对端RDP连接。

[0113] 以上所述和所示的操作和过程可在各种实现根据需要按照任何适当顺序来实行或执行。另外,在某些实现中,操作的至少一部分可并行执行。此外,在某些实现中,可执行少于或多于所述的操作。

[0114] 本书面描述使用示例来公开包括最佳模式的本公开的某些实施例,并且还使本领域的技术人员能够实施本公开的某些实施例,包括制作和使用任何装置或系统,以及执行任何结合方法。本公开的某些实施例的专利范围通过权利要求书来定义,并且可包括本领域的技术人员想到的其它示例。如果这类其它示例具有与权利要求的文字语言完全相同的结构单元,或者如果它们包括具有与权利要求的文字语言的非实质差异的等效结构单元,则预计它们落入权利要求的范围之内。

[0115] 附图标记说明

图 1		图 4	
100	示例系统架构	400	示例现场管理器
102	基于 Windows™的平台/智能代理	402	处理器
104	代理	404	存储器
106	现场网络	406	I/O 接口
108	公司防火墙	408	网络接口
110	现场监测系统	410	操作系统模块
114	中央系统内联网	412	数据仓库
116	企业隧道服务器	414	收集模块
118	远程企业服务器	416	处理模块
119	用户	418	传输模块
130	因特网	图 5	
134	用户	510	框
图 2		520	框
111	控制器	530	框
113	以太网数据获取系统(EDAS)	540	框
115	WSSTt 集线器	550	框
117	Cimplicity 集线器	560	框
119	Ehistorian 收集器	570	框
210	软件模块	580	框
220	存储软件模块	图 6	
230	数据处理模块	610	框
231	中央条件评估平台——本地版(CCAP-LE)	620	框
233	CDE 规则引擎平台	630	框
240	传输模块	640	框
241	历史收集器	650	框
243	智能代理模块	图 7	
图 3		710	框
300	示例中央监测和诊断基础设施	720	框
310	中央系统传输模块	730	框
311	收集器服务	740	框
313	低带宽导入服务	750	框
320	中央存储软件模块	760	框
330	所示模块	770	框
		780	框

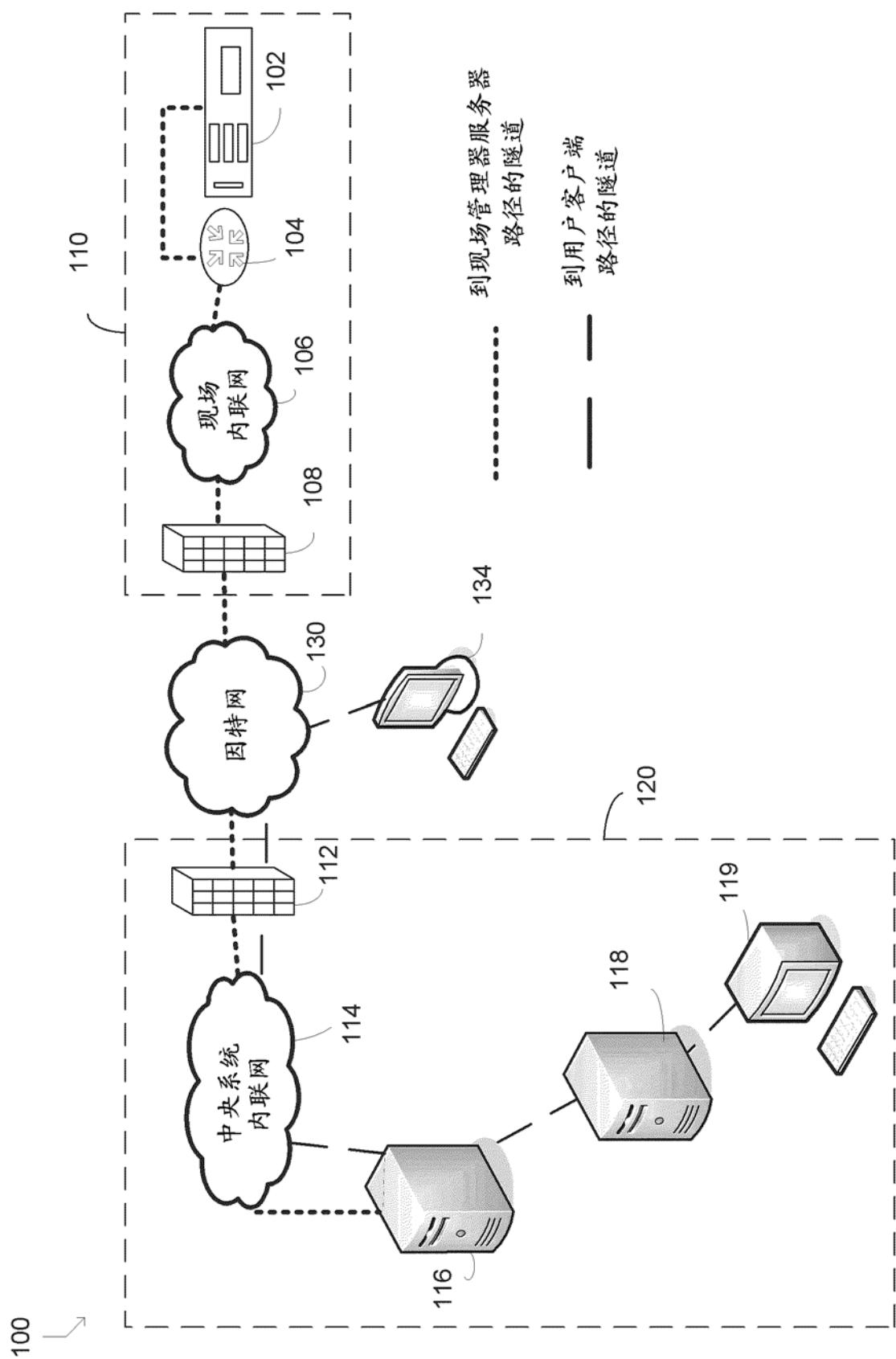
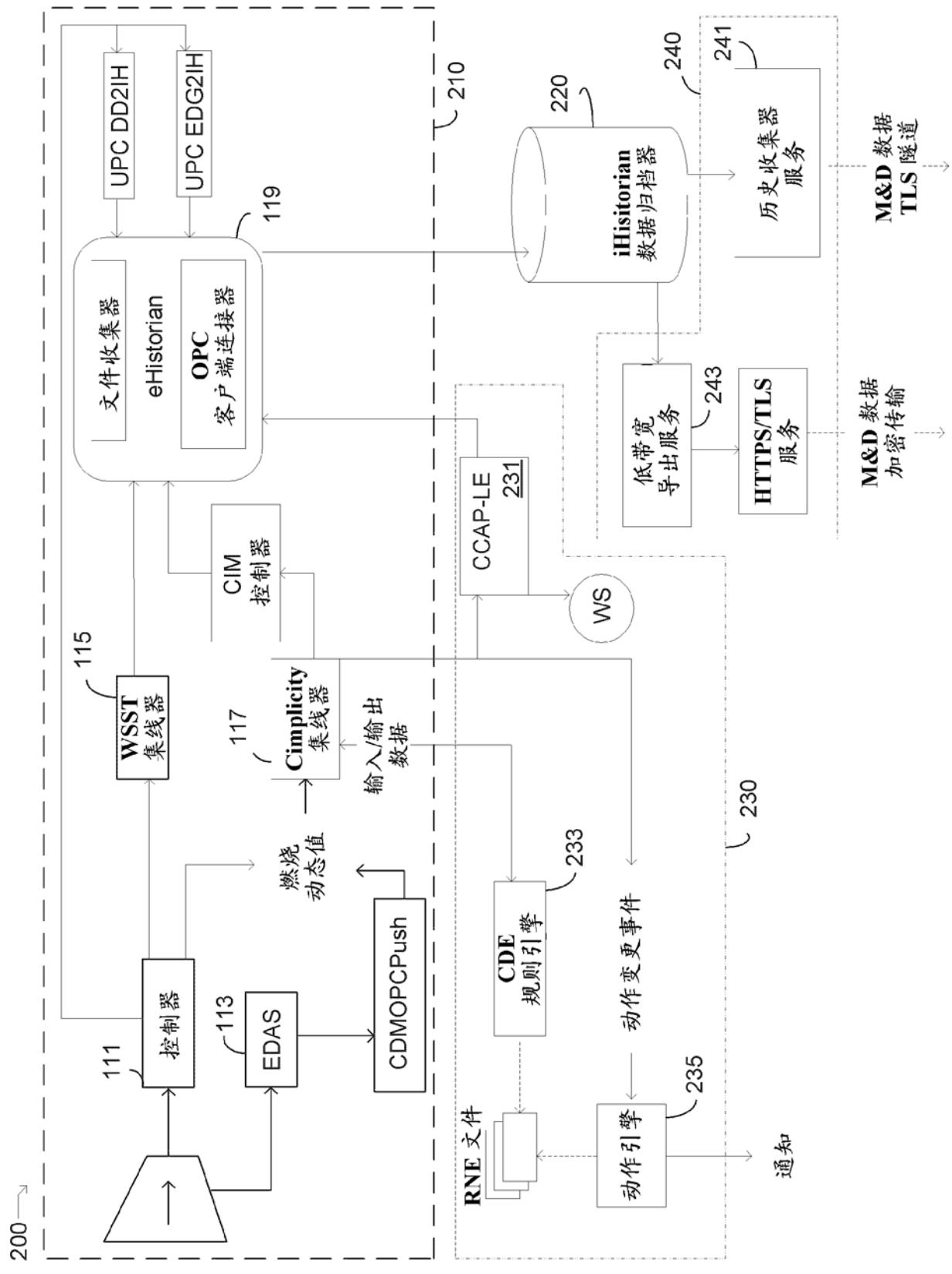


图 1



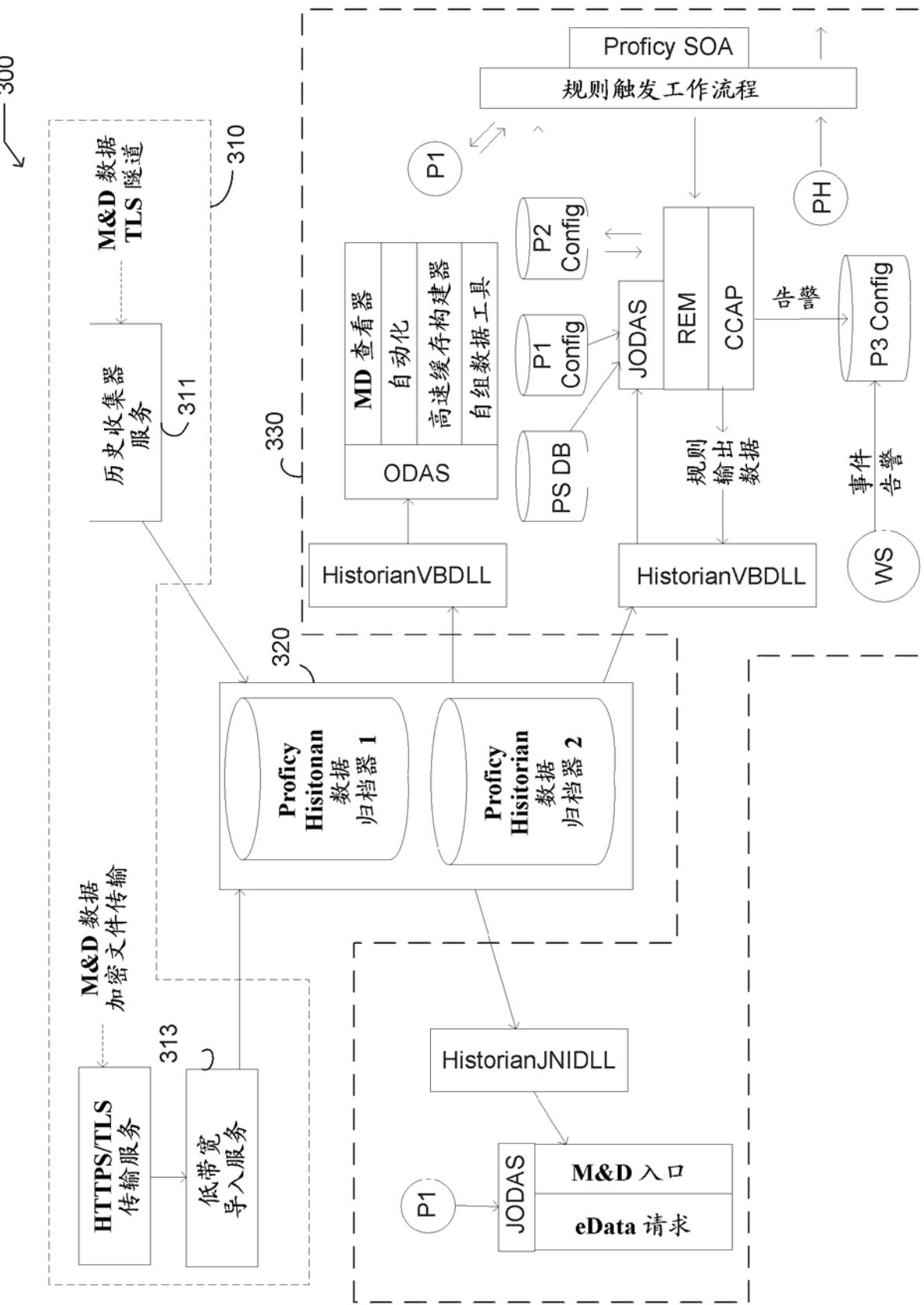


图 3

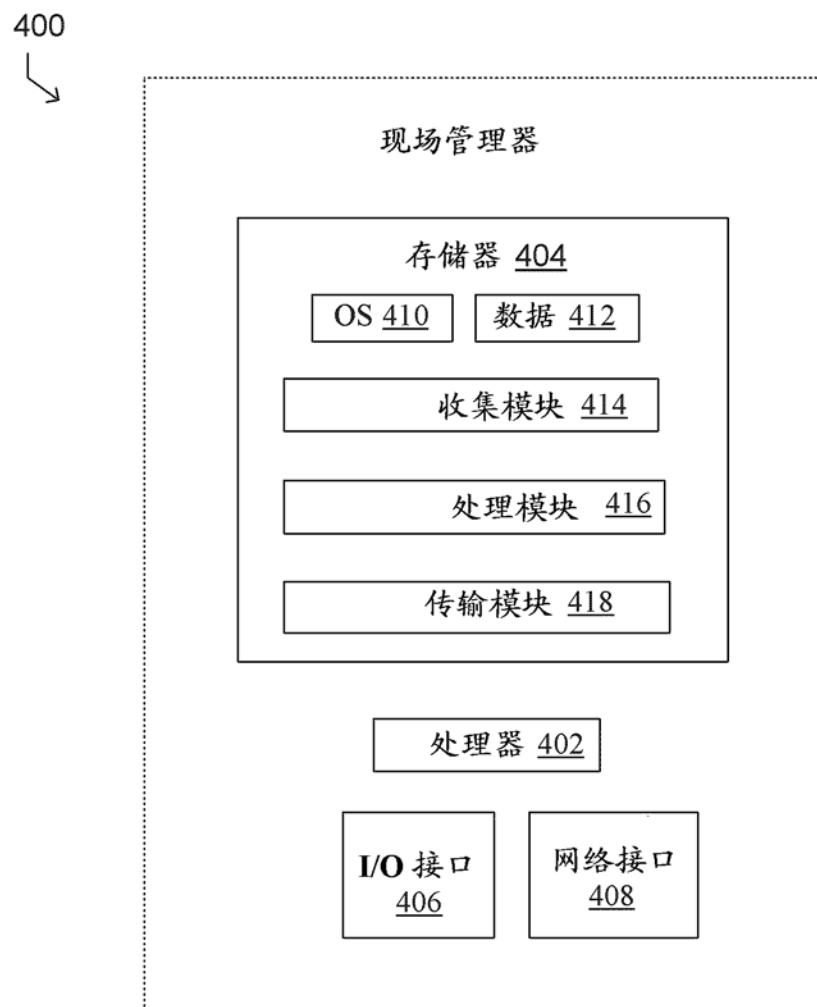


图 4

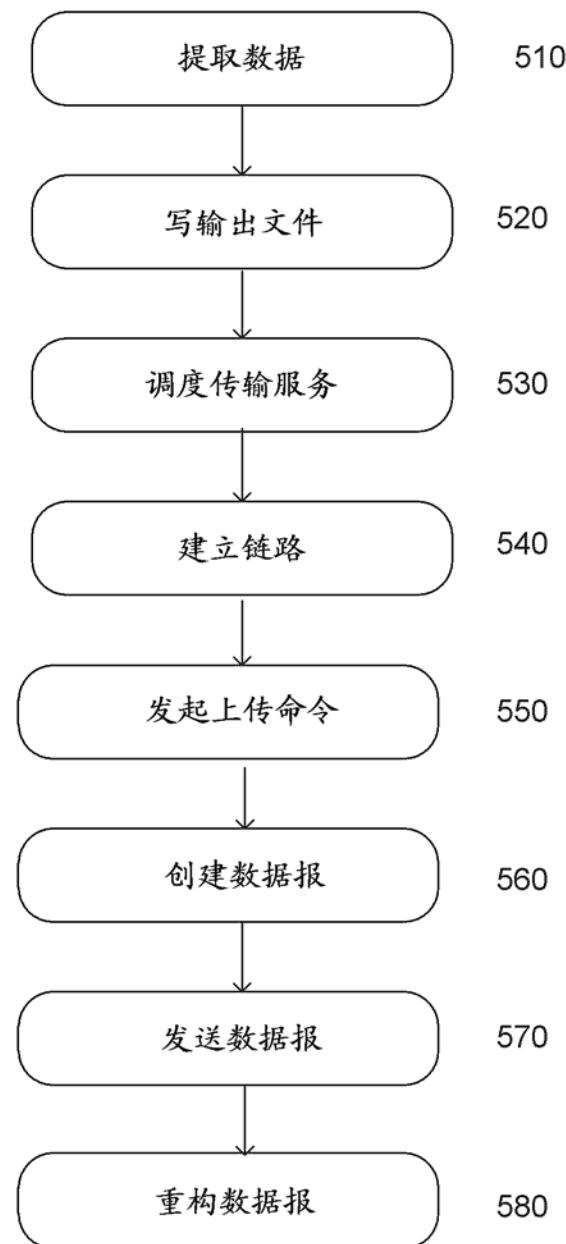


图 5

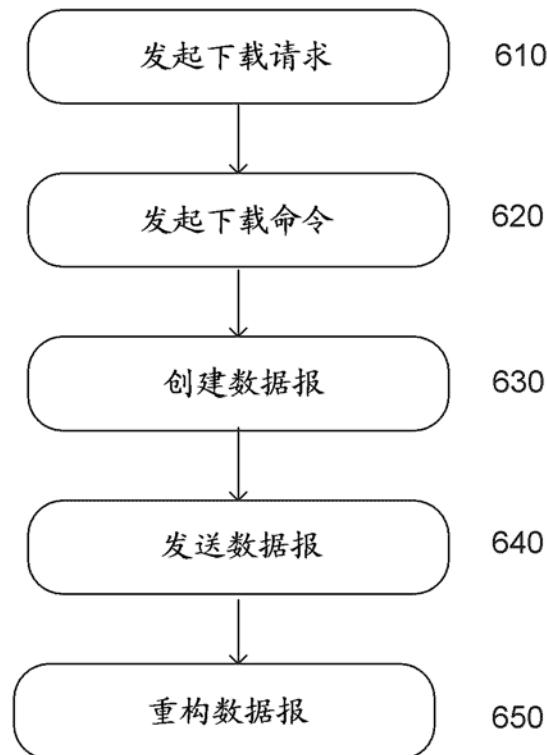


图 6

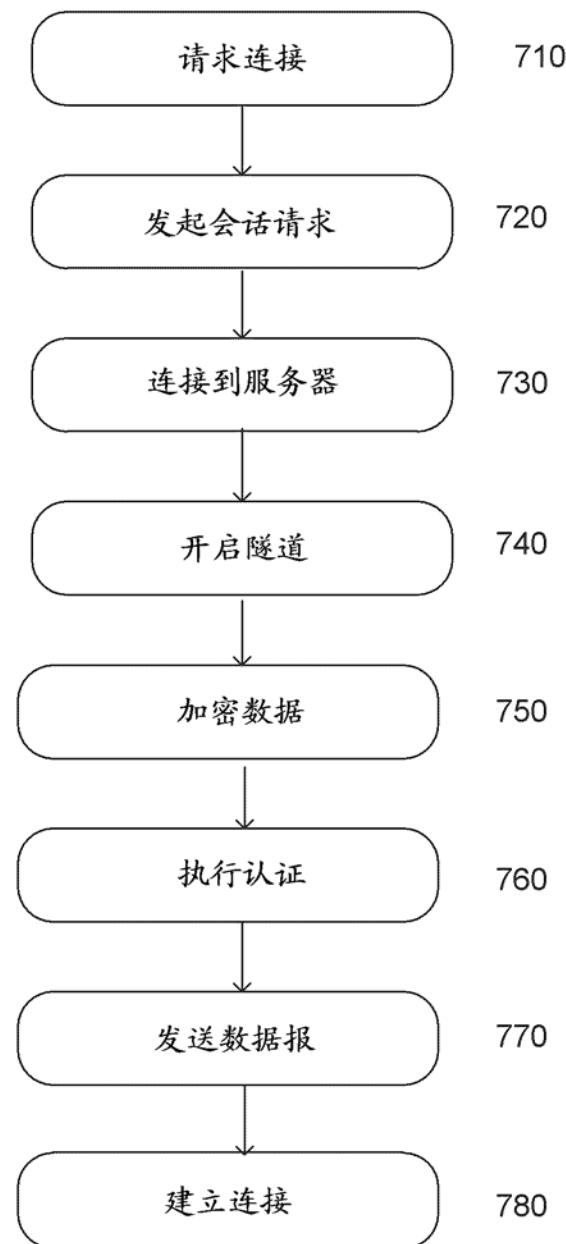


图 7