



(12) 发明专利申请

(10) 申请公布号 CN 112671851 A

(43) 申请公布日 2021. 04. 16

(21) 申请号 202011466799.5

H04L 29/06 (2006.01)

(22) 申请日 2020.12.14

H04L 12/66 (2006.01)

(71) 申请人 南方电网数字电网研究院有限公司

地址 511458 广东省广州市南沙区丰泽东路106号城投大厦1301房(自编1301-12159)

申请人 中国南方电网有限责任公司

(72) 发明人 林志达 张华兵 曹小明 陈华军  
付志博 卢伟开

(74) 专利代理机构 成都玖和知识产权代理事务所(普通合伙) 51238

代理人 胡琳梅

(51) Int. Cl.

H04L 29/08 (2006.01)

H04L 12/40 (2006.01)

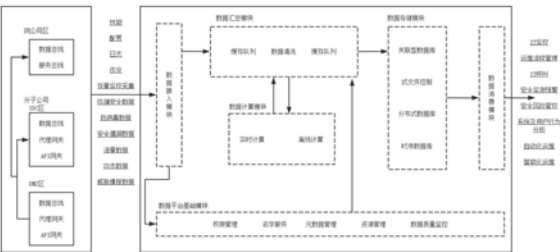
权利要求书2页 说明书5页 附图2页

(54) 发明名称

一种利用远程代理单元的监测预警系统

(57) 摘要

本发明公开了一种利用远程代理单元的监测预警系统,包括有与信息安全运行监测预警系统连接的远程代理单元,平台远程代理系统包括有数据采集模块,数据采集模块输出端分别连接有数据接入模块和数据平台基础模块,数据接入模块输出端连接有数据汇总模块,数据汇总模块输出端连接有数据存储模块;可以通过设置远程代理单元有效降低信息安全运行监测预警系统的数据交互、数据共享的难度,有效提高总部和各分子公司之间的数据交互效率,并且提高信息安全运行监测预警系统数据处理的速度,提高信息安全运行监测预警系统的安全性。



1. 一种利用远程代理单元的监测预警系统, 包括有与信息安全运行监测预警系统连接的远程代理单元, 其特征在于: 所述系统包括有数据采集模块, 所述数据采集模块输出端分别连接有数据接入模块和数据平台基础模块;

所述数据接入模块输出端连接有数据汇总模块, 所述数据汇总模块输出端连接有数据存储模块, 所述数据存储模块连接有数据消费模块; 所述数据平台基础模块包括有权限管理、名字服务、元数据管理、资源管理和数据质量监控;

所述数据采集模块输入端连接有网公司区、分子公司IDC区和DMZ区, 所述网公司区、分子公司IDC区和DMZ区均设有数据总线, 所述网公司区还设有服务总线, 所述分子公司IDC区和DMZ区还设有代理网关和API网关。

2. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述数据汇总模块还连接有数据计算模块, 所述数据计算模块包括有实时计算和离线计算, 所述数据汇总模块包括缓存列队和数据清洗。

3. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述数据存储模块包括有关联型数据库、分布式文件控制、分布式数据库和时序数据库。

4. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述数据消费模块包括有IT监控、运维流程管理、IT呼叫、安全监测预警、安全风险管控、安全综合运营、系统与用户行为分析、自动化运维和智能化运维。

5. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述网公司区与分子公司IDC区之间的数据流连接方法包括如下步骤:

S1. 外围集成系统API注册: 在各省级的API网关上注册各个外围集系统的API, 然后将这些API统一注册到网级运维服务总线中;

S2. 现有监控软件等管理系统数据上报: 在各省级设立数据总线来接收各省级的监控软件等管理系统的数, 并进行数据清洗、协议与格式转换, 然后将其传输到网级数据总线;

S3. IT基础设施与安全设备数据上报: 在各省级设立代理网关, 使用运维采控接入以及安全采集接入方式采集和管理IT基础设施与安全设备。

6. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述子分子公司IDC区和DMZ区之间的数据流连接方法包括如下步骤:

S1. 外围集成系统API注册: IDC的API网关通过内外网交换平台的接入规则实现内外网数据交互, 注册DMZ区的各个外围集成系统的API;

S2. 现有监控软件等管理系统数据上报: IDC的数据总线按照内外网交换平台的接入规则实现内外网数据交互, 接收DMZ区的监控软件等管理系统的数;

S3. IT基础设施与安全设备数据上报: 在DMZ区设立代理网关, 该网关通过运维采控接入以及安全采集接入方式采集和管理DMZ区的IT基础设施与安全设备;

S4. DMZ区的代理网关与IDC的代理网关形成级联关系, 通过IDC的代理网关接入到网公司区。

7. 根据权利要求1所述的一种利用远程代理单元的监测预警系统, 其特征在于: 所述网公司区服务总线的数据消费为: 服务总线可提供给信息安全运行监测预警系统平台上的各类场景应用以及外部其他系统进行调用消费。

8. 根据权利要求1所述的一种利用远程代理单元的监测预警系统,其特征在于:所述网公司区数据总线的数据消费为:数据进入数据总线后,进行一系列的提取、格式化、切分和过滤等清洗操作,根据使用需要对数据进行实时计算或离线计算,然后根据需要将数据存储到结构化存储或分布式存储中,并对外提供API供平台上的各类场景应用以及外部其他系统进行消费。

9. 根据权利要求1所述的一种利用远程代理单元的监测预警系统,其特征在于:所述远程代理单元分别运用在总部及各分子公司服务器区,并与各IT对象的采控接入。

10. 根据权利要求1所述的一种利用远程代理单元的监测预警系统,其特征在于:所述DMZ区部署独立的采控模块,用于负责DMZ区各IT对象的采控接入,所述DMZ区使用内外网数据安全交换平台的接入规则实现内外网数据交互,接入到信息安全运行监测预警系统。

## 一种利用远程代理单元的监测预警系统

### 技术领域

[0001] 本发明涉及信息安全技术领域,更具体地说,涉及一种利用远程代理单元的监测预警系统。

### 背景技术

[0002] 近年来随着科技的不断进步,IT服务管理制度、管理手段都得到大大的提升。信息安全运行监测预警系统将从大建设阶段进入大运维大服务阶段,对运维服务提出了更高的要求和挑战。但是现有的电网用信息安全运行监测预警系统在数据交互、数据共享方面存在交互困难以及处理繁琐等缺陷。需要解决运维持续演进的难题,不断总结运维工程实践经验,降低运维成本,提升IT运维服务水平;实现应用服务的自助化、增值服务的低成本化,并打破现有运维模式,最终达到管理强化、协同融合、数字化转型的最终目标。

### 发明内容

[0003] 针对现有技术中存在的问题,本发明的目的在于提供一种利用远程代理单元的监测预警系统,可以通过设置远程代理单元有效降低信息安全运行监测预警系统的数据交互、数据共享的难度,有效提高总部和各分子公司之间的数据交互效率,并且提高信息安全运行监测预警系统数据处理的速度,提高信息安全运行监测预警系统的安全性。

[0004] 为解决上述问题,本发明采用如下的技术方案。

[0005] 一种利用远程代理单元的监测预警系统,包括有与信息安全运行监测预警系统连接的远程代理单元,所述平台远程代理系统包括有数据采集模块,所述数据采集模块输出端分别连接有数据接入模块和数据平台基础模块;

[0006] 所述数据接入模块输出端连接有数据汇总模块,所述数据汇总模块输出端连接有数据存储模块,所述数据存储模块连接有数据消费模块;所述数据平台基础模块包括有权限管理、名字服务、元数据管理、资源管理和数据质量监控;

[0007] 所述数据采集模块输入端连接有网公司区、分子公司IDC区和DMZ区,所述网公司区、分子公司IDC区和DMZ区均设有数据总线,所述网公司区还设有服务总线,所述分子公司IDC区和DMZ区还设有代理网关和API网关。通过设置远程代理单元有效降低信息安全运行监测预警系统的数据交互、数据共享的难度,有效提高总部和各分子公司之间的数据交互效率,并且提高信息安全运行监测预警系统数据处理的速度,提高信息安全运行监测预警系统的安全性。

[0008] 进一步的,所述数据汇总模块还连接有数据计算模块,所述数据计算模块包括有实时计算和离线计算,所述数据汇总模块包括缓存列队和数据清洗。通过数据计算和数据汇总的相互配合对数具进行科学的处理和反应,有效提高平台远程代理单元的数据处理速度,提高信息安全运行监测预警系统的运维效率。

[0009] 进一步的,所述数据存储模块包括有关联型数据库、分布式文件控制、分布式数据库和时序数据库。

[0010] 进一步的,所述数据消费模块包括有IT监控、运维流程管理、IT呼叫、安全监测预警、安全风险管控、安全综合运营、系统与用户行为分析、自动化运维和智能化运维。数据消费模块对用户和系统的行为进行科学的反应,能够客观的对数据进行描述,有效提高平台远程代理单元数据反应的精准度,促进信息安全运行监测预警系统的运维控制。

[0011] 进一步的,所述网公司区与分子公司IDC区之间的数据流连接方法包括如下步骤:

[0012] S1.外围集成系统API注册:在各省级的API网关上注册各个外围集系统的API,然后将这些API统一注册到网级运维服务总线中;

[0013] S2.现有监控软件等管理系统数据上报:在各省级设立数据总线来接收各省级的监控软件等管理系统的数,并进行数据清洗、协议与格式转换,然后将其传输到网级数据总线;

[0014] S3.IT基础设施与安全设备数据上报:在各省级设立代理网关,使用运维采控接入以及安全采集接入方式采集和管理IT基础设施与安全设备。将各省级的API网关、监控软件、IT设施和安全数据的数据进行采集接入,便于平台远程代理单元的统一处理和综合分析,降低信息安全运行监测预警系统的计算压力。

[0015] 进一步的,所述子公司IDC区和DMZ区之间的数据流连接方法包括如下步骤:

[0016] S1.外围集成系统API注册:IDC的API网关通过内外网交换平台的接入规则实现内外网数据交互,注册DMZ区的各个外围集成系统的API;

[0017] S2.现有监控软件等管理系统数据上报:IDC的数据总线按照内外网交换平台的接入规则实现内外网数据交互,接收DMZ区的监控软件等管理系统的数;

[0018] S3.IT基础设施与安全设备数据上报:在DMZ区设立代理网关,该网关通过运维采控接入以及安全采集接入方式采集和管理DMZ区的IT基础设施与安全设备;

[0019] S4.DMZ区的代理网关与IDC的代理网关形成级联关系,通过IDC的代理网关接入到网公司区。通过DMZ区在IDC和网公司之间作为连接,有效捋顺数据运转衔接,提高数据接入的效率,便于平台远程代理单元的处理。

[0020] 进一步的,所述网公司区服务总线的数据消费为:服务总线可提供给信息安全运行监测预警系统平台上的各类场景应用以及外部其他系统进行调用消费。

[0021] 进一步的,所述网公司区数据总线的数据消费为:数据进入数据总线后,进行一系列的提取、格式化、切分和过滤等清洗操作,根据使用需要对数据进行实时计算或离线计算,然后根据需要存储到结构化存储或分布式存储中,并对外提供API供平台上的各类场景应用以及外部其他系统进行消费。

[0022] 进一步的,所述远程代理单元分别运用在总部及各分子公司服务器区,并与各IT对象的采控接入。远程代理单元通过对数据的多方采控,综合分析,有效提高信息安全运行监测预警系统的稳定性,使全网大运维大服务的工作需求满足全网大运维大服务的工作需求,提高其的运用价值。

[0023] 进一步的,所述DMZ区部署独立的采控模块,用于负责DMZ区各IT对象的采控接入,所述DMZ区使用内外网数据安全交换平台的接入规则实现内外网数据交互,接入到信息安全运行监测预警系统。

[0024] 相比于现有技术,本发明的优点在于:

[0025] (1)本方案通过设置远程代理单元有效降低信息安全运行监测预警系统的数据交

互、数据共享的难度,有效提高总部和各分子公司之间的数据交互效率,并且提高信息安全运行监测预警系统数据处理的速度,提高信息安全运行监测预警系统的安全性。

[0026] (2)通过数据计算和数据汇总的相互配合对数具进行科学的处理和反应,有效提高平台远程代理单元的数据处理速度,提高信息安全运行监测预警系统的运维效率。

[0027] (3)数据消费模块对用户和系统的行为进行科学的反应,能够客观的对数据进行描述,有效提高平台远程代理单元数据反应的精准度,促进信息安全运行监测预警系统的运维控制。

[0028] (4)将各省级的API网关、监控软件、IT设施和安全数据的数据进行采集接入,便于平台远程代理单元的统一处理和综合分析,降低信息安全运行监测预警系统的计算压力。

[0029] (5)通过DMZ区在IDC和网公司之间作为连接,有效捋顺数据运转衔接,提高数据接入的效率,便于平台远程代理单元的处理。

[0030] (6)远程代理单元通过对数据的多方采控,综合分析,有效提高信息安全运行监测预警系统的稳定性,使全网大运维大服务的工作需求满足全网大运维大服务的工作需求,提高其的运用价值。

## 附图说明

[0031] 为了使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明作进一步的详细描述,其中:

[0032] 图1为本发明的平台远程代理单元框架结构示意图;

[0033] 图2为本发明的、分子公司IDC区和DMZ区数据流传输结构示意图;

[0034] 图3为本发明的平台远程代理单元连接结构示意图。

## 具体实施方式

[0035] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述;显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例,基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0036] 在本发明的描述中,需要说明的是,术语“上”、“下”、“内”、“外”、“顶/底端”等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性。

[0037] 在本发明的描述中,需要说明的是,除非另有明确的规定和限定,术语“安装”、“设置有”、“套设/接”、“连接”等,应做广义理解,例如“连接”,可以是固定连接,也可以是可拆卸连接,或一体地连接;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通。对于本领域的普通技术人员而言,可以具体情况理解上述术语在本发明中的具体含义。

[0038] 实施例1:

[0039] 如图所示,一种利用远程代理单元的监测预警系统,包括有与信息安全运行监测

预警系统连接的远程代理单元,平台远程代理系统包括有数据采集模块,数据采集模块输出端分别连接有数据接入模块和数据平台基础模块;数据接入模块输出端连接有数据汇总模块,数据汇总模块输出端连接有数据存储模块,数据存储模块连接有数据消费模块;数据平台基础模块包括有权限管理、名字服务、元数据管理、资源管理和数据质量监控;数据采集模块输入端连接有网公司区、分子公司IDC区和DMZ区,网公司区、分子公司IDC区和DMZ区均设有数据总线,网公司区还设有服务总线,分子公司IDC区和DMZ区还设有代理网关和API网关。通过设置远程代理单元有效降低信息安全运行监测预警系统的数据交互、数据共享的难度,有效提高总部和各分子公司之间的数据交互效率,并且提高信息安全运行监测预警系统数据处理的速度,提高信息安全运行监测预警系统的安全性。

[0040] 请参阅图1,数据汇总模块还连接有数据计算模块,数据计算模块包括有实时计算和离线计算,数据汇总模块包括缓存队列和数据清洗。通过数据计算和数据汇总的相互配合对数具进行科学的处理和反应,有效提高平台远程代理单元的数据处理速度,提高信息安全运行监测预警系统的运维效率。

[0041] 请参阅图1,数据存储模块包括有关联型数据库、分布式文件控制、分布式数据库和时序数据库。

[0042] 请参阅图1,数据消费模块包括有IT监控、运维流程管理、IT呼叫、安全监测预警、安全风险管控、安全综合运营、系统与用户行为分析、自动化运维和智能化运维。数据消费模块对用户和系统的行为进行科学的反应,能够客观的对数据进行描述,有效提高平台远程代理单元数据反应的精准度,促进信息安全运行监测预警系统的运维控制。

[0043] 实施例2:

[0044] 如图所示,其中与实施例1中相同或相应的部件采用与实施例1相应的附图标记,为简便起见,下文仅描述与实施例1的区别点。该实施例2与实施例1的不同之处在于:请参阅图2,网公司区与分子公司IDC区之间的数据流连接方法包括如下步骤:

[0045] S1.外围集成系统API注册:在各省级的API网关上注册各个外围集系统的API,然后将这些API统一注册到网级运维服务总线中。

[0046] S2.现有监控软件等管理系统数据上报:在各省级设立数据总线来接收各省级的监控软件等管理系统的数,并进行数据清洗、协议与格式转换,然后将其传输到网级数据总线。

[0047] S3.IT基础设施与安全设备数据上报:在各省级设立代理网关,使用运维采控接入以及安全采集接入方式采集和管理IT基础设施与安全设备。将各省级的API网关、监控软件、IT设施和安全数据的数据进行采集接入,便于平台远程代理单元的统一处理和综合分析,降低信息安全运行监测预警系统的计算压力。

[0048] 实施例3:

[0049] 如图所示,其中与实施例1中相同或相应的部件采用与实施例1相应的附图标记,为简便起见,下文仅描述与实施例1的区别点。该实施例3与实施例1的不同之处在于:请参阅图2,子公司IDC区和DMZ区之间的数据流连接方法包括如下步骤:

[0050] S1.外围集成系统API注册:IDC的API网关通过内外网交换平台的接入规则实现内外网数据交互,注册DMZ区的各个外围集成系统的API。

[0051] S2.现有监控软件等管理系统数据上报:IDC的数据总线按照内外网交换平台的接

入规则实现内外网数据交互,接收DMZ区的监控软件等管理系统的数据。

[0052] S3.IT基础设施与安全设备数据上报:在DMZ区设立代理网关,该网关通过运维采集接入以及安全采集接入方式采集和管理DMZ区的IT基础设施与安全设备;

[0053] S4.DMZ区的代理网关与IDC的代理网关形成级联关系,通过IDC的代理网关接入到网公司区。通过DMZ区在IDC和网公司之间作为连接,有效捋顺数据运转衔接,提高数据接入的效率,便于平台远程代理单元的处理。

[0054] 本说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其它实施例的不同之处,各个实施例之间相同或相似部分互相参见即可。对于实施例公开的装置而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0055] 专业人员还可以进一步意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0056] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块,或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0057] 以上对本发明所提供的一种系统进行了详细介绍。本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想,以上所述,仅为本发明较佳的具体实施方式;但本发明的保护范围并不局限于此。任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,根据本发明的技术方案及其改进构思加以等同替换或改变,都应涵盖在本发明的保护范围内。



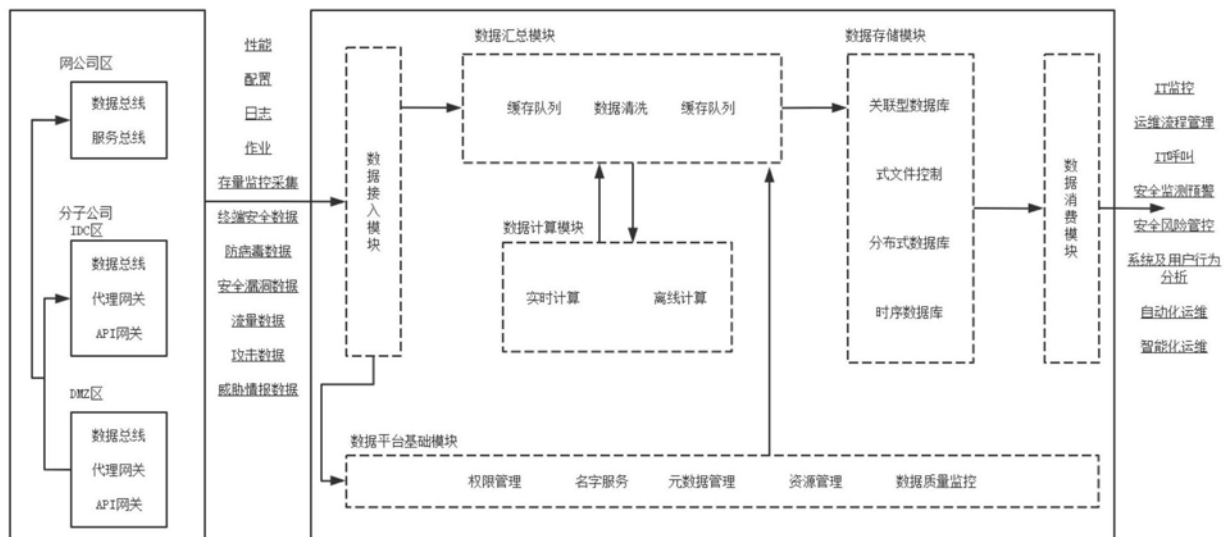


图1

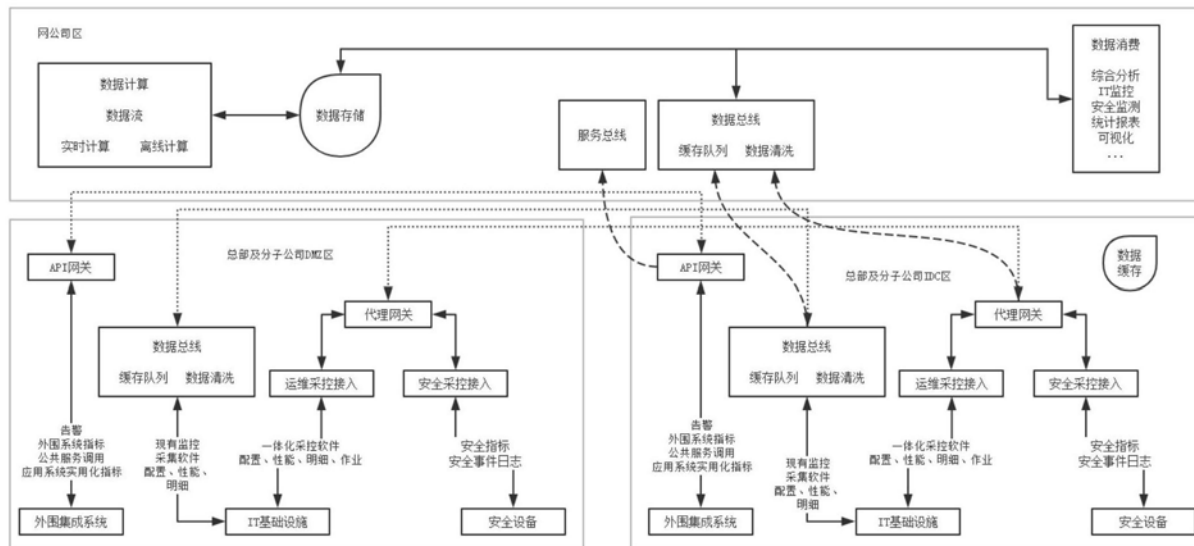


图2

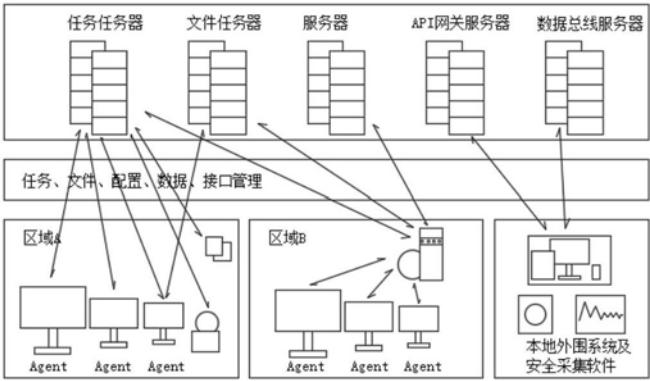


图3