



(12) 发明专利申请

(10) 申请公布号 CN 112667203 A

(43) 申请公布日 2021. 04. 16

(21) 申请号 202011467957.9

(22) 申请日 2020.12.14

(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.

G06F 8/20 (2018.01)

G06Q 10/10 (2012.01)

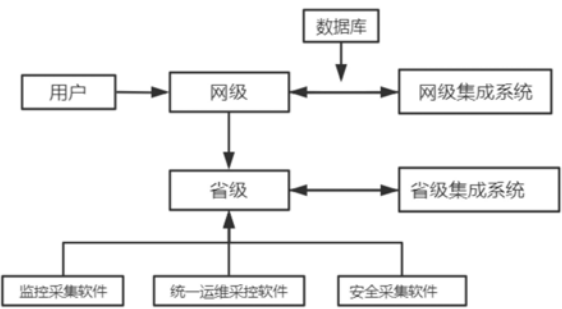
权利要求书1页 说明书6页 附图2页

(54) 发明名称

一种利于运维流程管理的信息安全运行监
测预警系统

(57) 摘要

本发明公开了一种利于运维流程管理的信息安全运行监测预警系统,在用户端的下级连接有网级,网级的下级连接有网级集成系统和省级,省级的下侧连接有省级集成系统,省级下级包括监控采集软件、统一运维采控软件和安全采集软件,它整体技术架构设计从全局出发,充分考虑现有运维模式以及未来运维模式,采用先进的技术架构理念,实现监、管、控于一体的安全运行管理。运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。



1. 一种利于运维流程管理的信息安全运行监测预警系统,包括用户端,其特征在于:所述用户端的下级连接有网级,所述网级的下级连接有网级集成系统和省级,所述省级的下侧连接有省级集成系统,所述省级下级包括监控采集软件、统一运维采控软件和安全采集软件。

2. 根据权利要求1所述的一种利于运维流程管理的信息安全运行监测预警系统,网级包括统一安装运行门户模块(1),其特征在于:所述统一安装运行门户模块(1)的下级连接有运维流程管理模块(2),所述运维流程管理模块(2)的下级连接有网省数据总线安全模块(3),所述网省数据总线安全模块(3)的下级连接有省级平台远程代理模块(4)。

3. 根据权利要求2所述的一种利于运维流程管理的信息安全运行监测预警系统,运维流程管理模块(2)包括运维流程管理(201),其特征在于:所述运维流程管理(201)的下级连接有IT监控(202),所述IT监控(202)的下级连接有IT呼叫(203),所述IT呼叫(203)的下级连接有安全监测预警(204),所述安全监测预警(204)的下级连接有综合安全运行分析(205)。

4. 根据权利要求3所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述运维流程管理(201)是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

5. 根据权利要求3所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述IT监控(202)与IT呼叫(203)采用集中管控和一级部署。

6. 根据权利要求2所述的一种利于运维流程管理的信息安全运行监测预警系统,网省数据总线安全模块(3)包括公共组件(301),其特征在于:所述公共组件(301)的下级连接有配置管理(302),所述配置管理(302)的下级连接有开发框架(303),所述开发框架(303)的下级连接有数据服务(304),所述数据服务(304)的下级连接有作业服务(305),所述作业服务(305)的下级连接有网省数据总线(306)。

7. 根据权利要求6所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述公共组件(301)为解决系统自身的用户、权限、审计和报表服务,以及接入外部安全规则和威胁情报管理。

8. 根据权利要求6所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述配置管理(302)通过模型定义、配置发现、主数据集成、配置校验,配置消费,将配置数据进行统一管理,并统一提供给上层场景应用。

9. 根据权利要求6所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述作业服务(305)通过作业执行与编排,解决自动化执行和命令下达的问题,实现对资源的控制。

10. 根据权利要求6所述的一种利于运维流程管理的信息安全运行监测预警系统,其特征在于:所述数据服务(304)通过数据接入、清洗、存储、计算和消费,解决如日志、性能指标、业务数据等数据的处理,并统一提供给上层场景应用。

一种利于运维流程管理的信息安全运行监测预警系统

技术领域

[0001] 本发明涉及安全运行监测领域,更具体地说,涉及一种利于运维流程管理的信息安全运行监测预警系统。

背景技术

[0002] 近年来IT服务管理制度、管理手段都得到大大的提升,最新的管理制度、信息运维服务体系设计成果需要在信息安全运行监测预警系统V1.0(运维流程管理)固化以适应业务的发展需要;信息化工作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。

[0003] 完成了调运检基本功能及部分横向协同功能,未完整的体现电网主业“调、运、检、服”的生产运营模式和“网省调度,三线服务”的信息运维服务体系,配置维护数据库是自定义的,不符合国际标准,与其它系统数据交互、数据共享方面存在交互困难以及处理繁琐等缺陷,缺少对IT资产“七”维度信息的功能及接口的完整支撑,未实现运维成本归集功能,服务运维指标管理也有待完善。因此需要对信息安全运行监测预警系统的“调运检”相关流程模块进行功能深化,为支撑资产全生命周期管理帐卡物一致性进行资产“七维度”信息适应性改造、优化与安全运维服务支撑系统横向协同等功能的完善工作,难以全面支撑以应用为视角的全生命周期安全运行管理,而且难以安全运行管理。

发明内容

[0004] 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于运维流程管理的信息安全运行监测预警系统,它整体技术架构设计从全局出发,充分考虑现有运维模式以及未来运维模式,采用先进的技术架构理念,实现监、管、控于一体的安全运行管理。运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0005] 为解决上述问题,本发明采用如下的技术方案:

[0006] 一种利于运维流程管理的信息安全运行监测预警系统,包括用户端,所述用户端的下级连接有网级,所述网级的下级连接有网级集成系统和省级,所述省级的下侧连接有省级集成系统,所述省级下级包括监控采集软件、统一运维采控软件和安全采集软件。

[0007] 进一步的,所述网级包括统一安装运行门户模块,所述统一安装运行门户模块的下级连接有运维流程管理模块,所述运维流程管理模块的下级连接有网省数据总线安全模块,所述网省数据总线安全模块的下级连接有省级平台远程代理模块,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0008] 进一步的,所述运维流程管理模块包括运维流程管理,所述运维流程管理的下级连接有IT监控,所述IT监控的下级连接有IT呼叫,所述IT呼叫的下级连接有安全监测预警,所述安全监测预警的下级连接有综合安全运行分析,在系统技术架构上,同信息安全运行

监测预警系统相同。

[0009] 进一步的,所述运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0010] 进一步的,所述IT监控与IT呼叫将从“分散处理,两级部署”到“集中管控,一级部署”进行转变,方便集中部署。

[0011] 进一步的,所述网省数据总线安全模块包括公共组件,所述公共组件的下级连接有配置管理,所述配置管理的下级连接有开发框架,所述开发框架的下级连接有数据服务,所述数据服务的下级连接有作业服务,所述作业服务的下级连接有网省数据总线,网省数据总线安全模块方便保证数据总线的安全。

[0012] 进一步的,所述公共组件为解决系统自身的用户、权限、审计和报表服务,以及接入外部安全规则和威胁情报管理,方便警示管理。

[0013] 进一步的,所述配置管理通过模型定义、配置发现、主数据集成、配置校验,配置消费,将配置数据进行统一管理,并统一提供给上层场景应用,方便统一管理。

[0014] 进一步的,所述作业服务通过作业执行与编排,解决自动化执行和命令下达的问题,实现对资源的控制,便于资源管理。

[0015] 进一步的,所述数据服务通过数据接入、清洗、存储、计算和消费,解决如日志、性能指标、业务数据等数据的处理,并统一提供给上层场景应用,方便数据处理。

[0016] 相比于现有技术,本发明的优点在于

[0017] (1) 本方案整体技术架构设计从全局出发,充分考虑现有运维模式以及未来运维模式,采用先进的技术架构理念,实现监、管、控于一体的安全运行管理。运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0018] (2) 网级包括统一安装运行门户模块,所述统一安装运行门户模块的下级连接有运维流程管理模块,所述运维流程管理模块的下级连接有网省数据总线安全模块,所述网省数据总线安全模块的下级连接有省级平台远程代理模块,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0019] (3) 运维流程管理模块包括运维流程管理,所述运维流程管理的下级连接有IT监控,所述IT监控的下级连接有IT呼叫,所述IT呼叫的下级连接有安全监测预警,所述安全监测预警的下级连接有综合安全运行分析,在系统技术架构上,同信息安全运行监测预警系统相同。

[0020] (4) 运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0021] (5) IT监控与IT呼叫将从“分散处理,两级部署”到“集中管控,一级部署”进行转变,方便集中部署。

[0022] (6) 网省数据总线安全模块包括公共组件,所述公共组件的下级连接有配置管理,所述配置管理的下级连接有开发框架,所述开发框架的下级连接有数据服务,所述数据服务的下级连接有作业服务,所述作业服务的下级连接有网省数据总线,网省数据总线安全

模块方便保证数据总线的安全。

[0023] (7) 公共组件为解决系统自身的用户、权限、审计和报表服务,以及接入外部安全规则和威胁情报管理,方便警示管理。

[0024] (8) 配置管理通过模型定义、配置发现、主数据集成、配置校验,配置消费,将配置数据进行统一管理,并统一提供给上层场景应用,方便统一管理。

[0025] (9) 作业服务通过作业执行与编排,解决自动化执行和命令下达的问题,实现对资源的控制,便于资源管理。

[0026] (10) 数据服务通过数据接入、清洗、存储、计算和消费,解决如日志、性能指标、业务数据等数据的处理,并统一提供给上层场景应用,方便数据处理。

附图说明

[0027] 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:

[0028] 图1为本发明的信息安全运行监测预警系统架构需求示意图;

[0029] 图2为本发明的网级框架示意图;

[0030] 图3为本发明的运维流程管理模块框架示意图;

[0031] 图4为本发明的网省数据总线安全模块框架示意图。

[0032] 图中标号说明:

[0033] 1、统一安装运行门户模块;2、运维流程管理模块;201、运维流程管理;202、IT监控;203、IT呼叫;204、安全监测预警;205、综合安全运行分析;3、网省数据总线安全模块;301、公共组件;302、配置管理;303、开发框架;304、数据服务;305、作业服务;306、网省数据总线;4、省级平台远程代理模块。

具体实施方式

[0034] 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。

[0035] 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。

[0036] 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。

[0037] 如图所示,本发明的一种利于运维流程管理的信息安全运行监测预警系统,包括

用户端,用户端的下级连接有网级,网级的下级连接有网级集成系统和省级,省级的下侧连接有省级集成系统,省级下级包括监控采集软件、统一运维采控软件和安全采集软件。

[0038] 请参阅图1-2,网级包括统一安装运行门户模块1,统一安装运行门户模块1的下级连接有运维流程管理模块2,运维流程管理模块2的下级连接有网省数据总线安全模块3,网省数据总线安全模块3的下级连接有省级平台远程代理模块4,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0039] 请参阅图3,运维流程管理模块2包括运维流程管理201,运维流程管理201的下级连接有IT监控202,IT监控202的下级连接有IT呼叫203,IT呼叫203的下级连接有安全监测预警204,安全监测预警204的下级连接有综合安全运行分析205,在系统技术架构上,同信息安全运行监测预警系统相同。运维流程管理201是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。IT监控202与IT呼叫203将从“分散处理,两级部署”到“集中管控,一级部署”进行转变,方便集中部署。

[0040] 请参阅图4,网省数据总线安全模块3包括公共组件301,公共组件301的下级连接有配置管理302,配置管理302的下级连接有开发框架303,开发框架303的下级连接有数据服务304,数据服务304的下级连接有作业服务305,作业服务305的下级连接有网省数据总线306,网省数据总线安全模块3方便保证数据总线的安全。公共组件301为解决系统自身的用户、权限、审计和报表服务,以及接入外部安全规则和威胁情报管理,方便警示管理。配置管理302通过模型定义、配置发现、主数据集成、配置校验,配置消费,将配置数据进行统一管理,并统一提供给上层场景应用,方便统一管理。作业服务305通过作业执行与编排,解决自动化执行和命令下达的问题,实现对资源的控制,便于资源管理。数据服务304通过数据接入、清洗、存储、计算和消费,解决如日志、性能指标、业务数据等数据的处理,并统一提供给上层场景应用,方便数据处理。

[0041] 请参阅图1-2,使用时,总体设计原则有以下几点:平台+应用模式:全面支撑以系统为视角的全生命周期安全运行管理;建立信息安全运行监测预警系统,运用场景输出模式,对应用功能进行解耦;提供便捷快速服务组合功能,各分子公司可根据实际管理需要实现个性化安全运行应用;

[0042] 安全运行功能全覆盖:构建监、管、控于一体的安全运行管理;

[0043] 功能设计覆盖现有功能;为未来自动化、智能化业务场景预留扩展能力;实现安全规则和策略统一定制;

[0044] 网一级部署:实现全网安全运行统一入口、服务与支持全景展示;建立统一安全运行门户,实现安全运行统一入口;采用一级部署模式,平台及应用均部署在网一级;省级侧部署远程代理服务用于集成各分子公司外围系统数据;构建全网网络安全全景状态视图;

[0045] 先进技术架构:构建一套高可用、高性能安全运行系统;

[0046] 本实施例摒弃传统单体设计模式,采用业界先进微服务设计模式;利用分布式、高可用技术实现平台高可用、高性能;采用开放式标准化的平台接口设计,实现与外围系统的灵活集成。

[0047] 本实施例的信息安全运行监测预警系统,除了平台省级平台远程代理模块4分散部署在网级及各省级用于采控IT监控202和IT呼叫203对象外,其他组件均部署在网级。

[0048] 集中访问入口,所有用户访问信息安全运行监测预警系统将直接访问网级统一安装运行门户模块1。

[0049] SOA设计,系统各组件部署基于SOA设计,各组件均使用高可用设计,并可方便的进行快速扩展。

[0050] 网级本地部署API网关和网省数据总线306两个平台省级平台远程代理模块4,分别用于实现网级其他系统的API到信息安全运行监测预警系统的注册以及其他系统的数据上报。

[0051] 在总部及各分子公司部署平台省级平台远程代理模块4,包括独立的API网关、数据总线、采控接入、安全采集接入,用于负责总部及各分子公司服务器区各IT对象的采控接入。

[0052] 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;使用南网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。

[0053] 将现有IT监控202和IT呼叫203服务管理系统将从“分散处理,两级部署”到“集中管控,一级部署”进行转变,同时根据公司信息运维服务体系设计成果,融入“调、运、检、服”理念的建设思路,对IT服务管理系统中的“调运检”相关流程模块进行功能深化,捋顺运行调度与运维服务的运转衔接;依据公司IT资产全生命周期管理帐卡物一致方案的设计需求,对信息安全运行监测预警系统提出了适应IT资产信息记录的要求;完善与安全运维服务支撑系统的横向协同,使得信息安全运行监测预警系统能够更稳定、更高效地满足全网大运维大服务的工作需求,体现信息安全运行监测预警系统的核心价值,以上便完成该信息安全运行监测预警系统的一系列操作,它整体技术架构设计从全局出发,充分考虑现有运维模式以及未来运维模式,采用先进的技术架构理念,实现监、管、控于一体的安全运行管理。运维流程管理是信息安全运行监测预警系统的其中一个应用,在系统技术架构上,同信息安全运行监测预警系统相同,采用一级部署模式,全面支撑以应用为视角的全生命周期安全运行管理。

[0054] 应当认识到,本发明的实施例可以由计算机硬件、硬件和软件的组合、或者通过存储在非暂时性计算机可读存储器中的计算机指令来实现或实施。所述方法可以使用标准编程技术-包括配置有计算机程序的非暂时性计算机可读存储介质在计算机程序中实现,其中如此配置的存储介质使得计算机以特定和预定义的方式操作——根据在具体实施例中描述的方法和附图。每个程序可以以高级过程或面向对象的编程语言来实现以与计算机系统通信。然而,若需要,该程序可以以汇编或机器语言实现。在任何情况下,该语言可以是编译或解释的语言。此外,为此目的该程序能够在编程的专用集成电路上运行。

[0055] 此外,可按任何合适的顺序来执行本文描述的过程的操作,除非本文另外指示或以其他方式明显地与上下文矛盾。本文描述的过程(或变型和/或其组合)可在配置有可执行指令的一个或多个计算机系统的控制下执行,并且可作为共同地在一个或多个处理器上执行的代码(例如,可执行指令、一个或多个计算机程序或一个或多个应用)、由硬件或其组合来实现。所述计算机程序包括可由一个或多个处理器执行的多个指令。

[0056] 进一步,所述方法可以在可操作地连接至合适的任何类型的计算平台中实现,包括但不限于个人电脑、迷你计算机、主框架、工作站、网络或分布式计算环境、单独的或集成

的计算机平台、或者与带电粒子工具或其它成像装置通信等等。本发明的各方面可以以存储在非暂时性存储介质或设备上的机器可读代码来实现,无论是可移动的还是集成至计算平台,如硬盘、光学读取和/或写入存储介质、RAM、ROM等,使得其可由可编程计算机读取,当存储介质或设备由计算机读取时可用于配置和操作计算机以执行在此所描述的过程。此外,机器可读代码,或其部分可以通过有线或无线网络传输。当此类媒体包括结合微处理器或其他数据处理器实现上文所述步骤的指令或程序时,本文所述的发明包括这些和其他不同类型的非暂时性计算机可读存储介质。当根据本发明所述的方法和技术编程时,本发明还包括计算机本身。

[0057] 计算机程序能够应用于输入数据以执行本文所述的功能,从而转换输入数据以生成存储至非易失性存储器的输出数据。输出信息还可以应用于一个或多个输出设备如显示器。在本发明优选的实施例中,转换的数据表示物理和有形的对象,包括显示器上产生的物理和有形对象的特定视觉描绘。

[0058] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

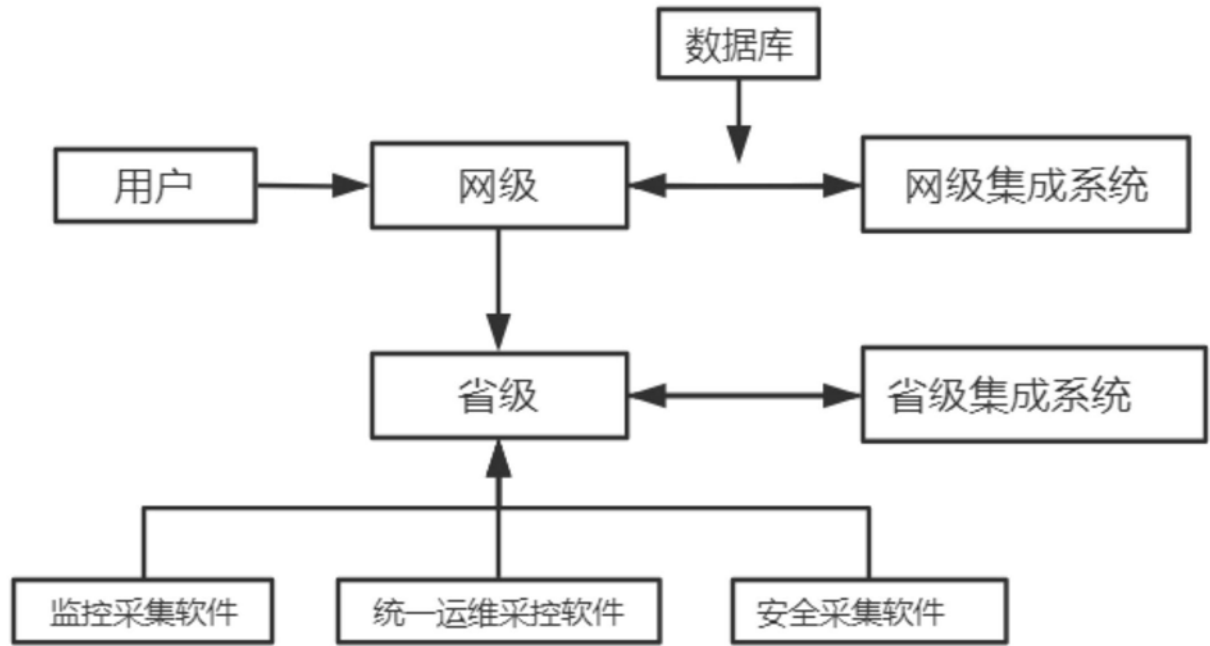


图1

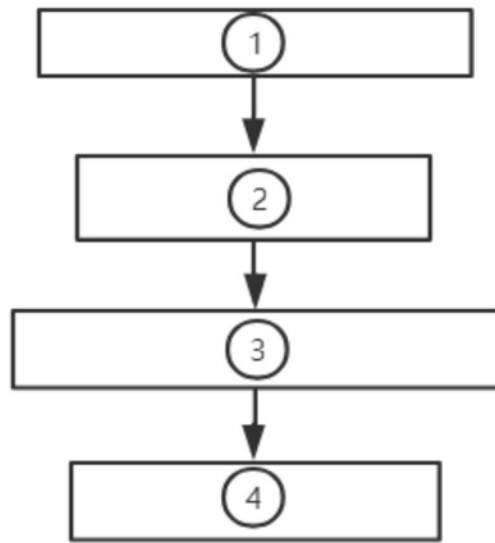


图2

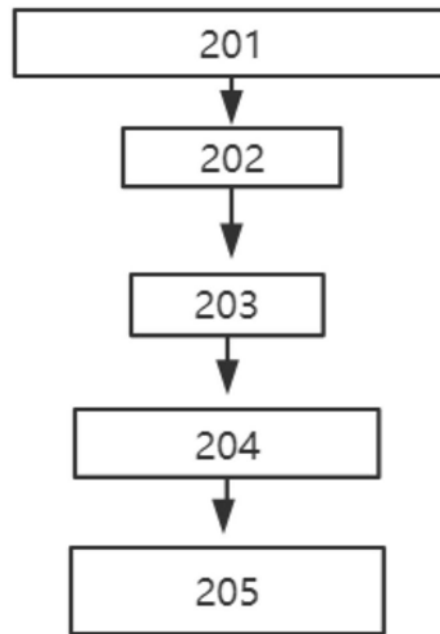


图3

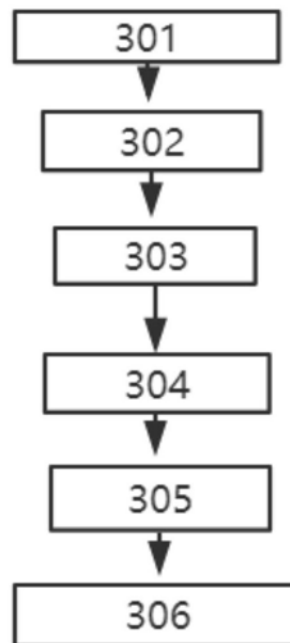


图4