(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117240600 A
(43)申请公布日 2023.12.15

(21)申请号 202311476911.7

(22)申请日 2023.11.08

(71)申请人 国家工业信息安全发展研究中心
地址 100000 北京市石景山区鲁谷路35号

(72)发明人 于盟 王得福 卢春景 汪慕峰 李敏 郑世涛 刘国良 杨梓涛 张哲宇

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
专利代理师 梁姗

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 41/14(2022.01)
H04L 41/12(2022.01)

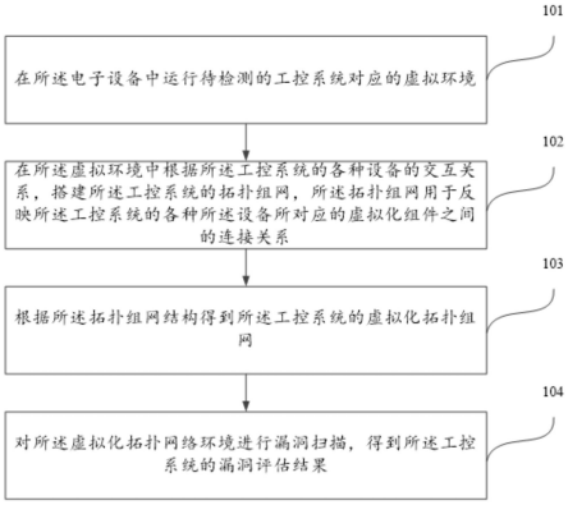
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种工控系统的漏洞检测方法及装置

(57)摘要

本申请提供了一种工控系统的漏洞检测方法及装置,应用于电子设备在电子设备中,包括:运行待检测的工控系统对应的虚拟环境;在虚拟环境中根据工控系统中各种设备的交互关系,搭建工控系统的拓扑结构。根据拓扑结构得到工控系统的虚拟化拓扑组网,对虚拟化拓扑组网进行漏洞扫描,得到工控系统的漏洞评估结果。本申请方案通过在虚拟环境中搭建工控系统的拓扑结构,可以虚拟化整个工控系统,再将工控系统的拓扑结构经过网络配置,实现虚拟化工控系统的真实运行情况,在虚拟环境中,通过漏洞安全评估模块对仿真场景进行漏洞扫描,实现了在工控系统部署前,对工控系统的风险隐患进行安全评估与检测。



CN 117240600 A

1.一种工控系统的漏洞检测方法,其特征在于,所述方法应用于电子设备,所述方法包括:

在所述电子设备中运行待检测的所述工控系统对应的虚拟环境;

在所述虚拟环境中根据所述工控系统中各种设备的交互关系,搭建所述工控系统的拓扑结构,所述拓扑结构用于反映所述工控系统的各种所述设备所对应的虚拟化组件之间的连接关系;

根据所述拓扑结构得到所述工控系统的虚拟化拓扑组网;

对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估结果。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

采集在所述虚拟环境中搭建的所述工控系统中各种所述设备交互的数据,将所述数据进行展示;

对所述工控系统中的各种设备进行监控。

3.根据权利要求1所述的方法,其特征在于,所述在所述电子设备中运行待检测的工控系统对应的虚拟环境之前,所述方法包括:

在所述电子设备上进行虚拟化集群管理;

根据所述虚拟化集群管理创建虚拟机,将所述虚拟机与所述电子设备的云资源池中的多个所述虚拟化组件进行连接;

对多个所述虚拟化组件进行地址配置以及部署所述虚拟机的操作系统;

通过镜像文件,将所述虚拟机以及与所述虚拟机连接的多个所述虚拟化组件,定制为一个或多个虚拟环境的模板,不同所述虚拟环境模板对应不同的工控系统的类型,一个或多个虚拟环境的模板用于得到所述工控系统对应的虚拟环境。

4.根据权利要求1所述的方法,其特征在于,所述电子设备具有云资源池,所述云资源池中存储有一个或多个虚拟化组件,在所述虚拟环境中根据所述工控系统的各种设备的交互关系,搭建所述工控系统的拓扑结构,包括:

响应于用户的第一操作,展示图形化的编辑界面,所述编辑界面上显示有一个或多个所述虚拟化组件的标识;

检测用户在所述编辑界面输入的针对所述一个或多个虚拟化组件中的多个所述虚拟化组件的第一选择操作;

响应于所述第一选择操作,根据被选择的多个所述虚拟化组件生成所述工控系统的所述拓扑结构;

配置构成所述拓扑结构的每个所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网。

5.根据权利要求4所述的方法,其特征在于,所述配置构成所述拓扑结构的每个所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网,包括:

显示构成所述拓扑结构的多个所述虚拟化组件;

检测用户针对所述拓扑结构中任一所述虚拟化组件的配置操作;

响应于所述配置操作,更新任一所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网。

6.根据权利要求4所述的方法,其特征在于,所述配置构成所述拓扑结构的每个所述虚

拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网,所述方法还包括:

通过可视化拓扑组网引擎,将所述拓扑结构转化为所述虚拟化拓扑组网。

7.根据权利要求2所述的方法,其特征在于,所述采集在所述虚拟环境中搭建的工控系统中各种设备交互的数据,将所述数据进行展示,所述数据包括:流量数据、网络数据以及平台数据,所述网络数据至少包括网络静态配置、网络实时状态以及各项性能数据;

所述平台数据包括代理数据、系统资源信息以及网络拓扑信息;

解析数据采集模块采集到的数据;

在所述虚拟环境中展示所述数据。

8.根据权利要求1~7任一项所述的方法,其特征在于,所述对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估报告,包括:

在所述虚拟环境中安装代理或服务,所述代理或所述服务用于访问所述虚拟化拓扑组网的文件和进程;

通过所述代理或服务访问所述虚拟化拓扑组网的文件和进程;

根据所述虚拟化拓扑组网的文件和进程,生成所述漏洞评估结果。

9.一种工控系统的漏洞检测装置,其特征在于,所述装置包括:

运行模块,用于在所述电子设备中运行待检测的工控系统对应的虚拟环境;

构建模块,用于在所述虚拟环境中根据所述工控系统的各种设备的交互关系,搭建所述工控系统的拓扑结构,所述拓扑结构用于反映所述工控系统的各种所述设备的网络结构;

转化模块,将所述拓扑结构转化为虚拟化拓扑组网;

评估模块,用于对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估结果。

10.根据权利要求9所述的装置,其特征在于,所述装置还包括:

监控模块,用于采集在所述虚拟环境中搭建的工控系统中各种设备交互的数据,将所述数据进行展示,对所述工控系统中的各种设备进行监控。

一种工控系统的漏洞检测方法及装置

技术领域

[0001] 本申请涉及工控安全仿真分析技术领域,特别涉及一种工控系统的漏洞检测方法及装置。

背景技术

[0002] 工业控制系统往往涉及一个城市或国家的重要基础设施,比如电力、燃气、自来水等,因此,工业控制系统的安全性非常重要。当工业控制系统的实际规模与安全性需要提升时,如果不经过验证就进行现场升级,未被发现的漏洞与隐患会造成巨大的安全隐患。针对工控系统的安全隐患防御措施,那么对工控操作平台进行漏洞测试尤为重要,它可以及时准确的察觉到信息平台基础架构的安全性问题,保证业务顺利的开展以及高效迅速的发展。

[0003] 现有技术中,每搭建出一个新工控操作平台后,开发人员以及测试人员都需要对其进行漏洞测试,使用漏扫工具对其主机和网页端进行漏洞扫描,生成测试报告。过程操作简单,但是环境搭建需要花费大量时间。

发明内容

[0004] 本申请提供了一种工控系统的漏洞检测方法及装置,通过虚拟仿真手段,在工控系统部署至现场前,通过搭建工控系统的虚拟仿真场景,在场景中对工控系统的漏洞进行扫描检测,从而对工控系统的风险隐患进行安全评估与检测。

[0005] 所述技术方案如下:

第一方面,提供了一种工控系统的漏洞检测方法,所述方法应用于电子设备,包括:在所述电子设备中运行待检测的所述工控系统对应的虚拟环境;

在所述虚拟环境中根据所述工控系统中各种设备的交互关系,搭建所述工控系统的拓扑结构,所述拓扑结构用于反映所述工控系统的各种所述设备所对应的虚拟化组件之间的连接关系;

根据所述拓扑结构得到所述工控系统的虚拟化拓扑组网;

对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估结果。

[0006] 本申请实施例提供了一种工控系统的漏洞检测方法,通过在虚拟环境中搭建工控系统的拓扑组网,可以虚拟化整个工控系统的设备。再将工控系统的拓扑结构经过网络配置,转化为虚拟化拓扑组网,可以实现虚拟化工控系统的真实运行环境。在虚拟环境中,通过漏洞安全评估模块对虚拟化网络拓扑环境进行漏洞扫描,得到工控系统的仿真场景的漏洞评估报告。本申请实施例实现了在工控系统部署至现场前,快速搭建一个虚拟仿真场景,在仿真场景中对工控系统的漏洞进行扫描,从而对工控系统的风险隐患进行安全评估与检测。

[0007] 可选的,所述方法还包括:采集在所述虚拟环境中搭建的所述工控系统中各种所述设备交互的数据,将所述数据进行展示;对所述工控系统中的各种设备进行监控。

[0008] 可选的,在所述电子设备中运行待检测的工控系统对应的虚拟环境之前,所述方法包括:在所述电子设备上进行虚拟化集群管理;

根据所述虚拟化集群管理创建虚拟机,将所述虚拟机与所述电子设备的云资源池中的多个所述虚拟化组件进行连接;

对多个所述虚拟化组件进行地址配置以及部署所述虚拟机的操作系统;

通过镜像文件,将所述虚拟机以及与所述虚拟机连接的多个所述虚拟化组件,定制为一个或多个虚拟环境的模板,不同所述虚拟环境模板对应不同的工控系统的类型,一个或多个虚拟环境的模板用于得到所述工控系统对应的虚拟环境。

[0009] 可选的,所述电子设备具有云资源池,所述云资源池中存储有一个或多个虚拟化组件,在所述虚拟环境中根据所述工控系统的各种设备的交互关系,搭建所述工控系统的拓扑结构,包括:

响应于用户的第一操作,展示图形化的编辑界面,所述编辑界面上显示有一个或多个所述虚拟化组件的标识;

检测用户在所述编辑界面输入的针对所述一个或多个虚拟化组件中的多个所述虚拟化组件的第一选择操作;

响应于所述第一选择操作,根据被选择的多个所述虚拟化组件生成所述工控系统的所述拓扑结构;

配置构成所述拓扑结构的每个所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网。

[0010] 可选的,所述配置构成所述拓扑结构的每个所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网,包括:

显示构成所述拓扑结构的多个所述虚拟化组件;

检测用户针对所述拓扑结构中任一所述虚拟化组件的配置操作;

响应于所述配置操作,更新任一所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网。

[0011] 可选的,所述配置构成所述拓扑结构的每个所述虚拟化组件的网络配置参数和/或存储配置参数,得到所述虚拟化拓扑组网,所述方法还包括:

通过可视化拓扑组网引擎,将所述拓扑结构转化为所述虚拟化拓扑组网。

[0012] 可选的,所述采集在所述虚拟环境中搭建的工控系统中各种设备交互的数据,将所述数据进行展示,所述数据包括:流量数据、网络数据以及平台数据,所述网络数据至少包括网络静态配置、网络实时状态以及各项性能数据;

所述平台数据包括代理数据、系统资源信息以及网络拓扑信息;

解析数据采集模块采集到的数据;

在所述虚拟环境中展示所述数据。

[0013] 可选的,所述对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估报告,包括:

在所述虚拟环境中安装代理或服务,所述代理或所述服务用于访问所述虚拟化拓扑组网的文件和进程;

通过所述代理或服务访问所述虚拟化拓扑组网的文件和进程;

根据所述虚拟化拓扑组网的文件和进程,生成所述漏洞评估结果。

[0014] 第二方面,提供了一种工控系统的漏洞检测装置,包括:运行模块,用于在所述电子设备中运行待检测的工控系统对应的虚拟环境;

构建模块,用于在所述虚拟环境中根据所述工控系统的各种设备的交互关系,搭建所述工控系统的拓扑结构,所述拓扑结构用于反映所述工控系统的各种所述设备的网络结构;

转化模块,将所述拓扑结构转化为虚拟化拓扑组网;

评估模块,用于对所述虚拟化拓扑组网进行漏洞扫描,得到所述工控系统的漏洞评估结果。

[0015] 可选的,所述装置还包括:监控模块,用于采集在所述虚拟环境中搭建的工控系统中各种设备交互的数据,将所述数据进行展示,对所述工控系统中的各种设备进行监控。

[0016] 第三方面,提供了一种计算机设备,包括:存储器和处理器,所述存储器用于存储计算机程序;所述处理器用于在调用所述计算机程序时执行上述的漏洞检测方法。

[0017] 可以理解的是,上述第二方面、第三方面的有益效果可以参见上述第一方面中的相关描述,在此不再赘述。

附图说明

[0018] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0019] 图1是本申请实施例提供的一种工控系统的漏洞检测方法流程图;

图2是本申请实施例提供的一种工控系统安全检测与评估的方案;

图3是本申请实施例提供的一种工控系统的数据采集与监控流程图;

图4是本申请实施例提供的一种仿真环境的快速集成系统;

图5是本申请实施例提供的一种工控系统的漏洞检测与评估方法的流程图;

图6是本申请实施例提供的一种工控系统的漏洞检测装置;

图7是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0020] 为使本申请的目的、技术方案和优点更加清楚,下面将结合附图对本申请实施方式作进一步地详细描述。

[0021] 应当理解的是,本申请提及的“多个”是指两个或两个以上。在本申请的描述中,除非另有说明,“/”表示或的意思,比如,A/B可以表示A或B;本文中的“和/或”仅仅是一种描述关联对象的关联关系,表示可以存在三种关系,比如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况。另外,为了便于清楚描述本申请的技术方案,采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定,并且“第一”、“第二”等字样也并不限定一定不同。

[0022] 在对本申请实施例进行详细地解释说明之前,先对本申请实施例的应用场景予以说明。

[0023] 针对工控系统的安全隐患防御措施,对工控操作平台进行漏洞测试尤为重要。漏洞扫描可以及时准确的察觉到信息平台基础架构的安全,保证业务顺利的开展。每当搭建出一个工控系统操作平台后,开发人员以及测试人员都需要对其进行漏洞测试,使用漏洞扫描工具对其主机和网页端进行漏洞扫描,生成测试报告,虽说操作简单,但是环境搭建会花费大量时间。对此,为保障工控系统的安全隐患,通过仿真场景的方法,提供一种工控系统的漏洞检测方法,可以实现通过虚拟仿真手段,在新的工控系统部署至现场前,快速搭建一个虚拟仿真场景,在场景中对工控系统进行漏洞检测与分析,以便对工控系统的风险隐患进行安全评估与检测。

[0024] 如图1所示,本申请实施例提供一种工控系统的漏洞检测方法,应用于电子设备,所述方法包括:

步骤101:在电子设备中运行待检测的工控系统对应的虚拟环境。

[0025] 其中,电子设备中具有多个虚拟环境模板,不同虚拟环境模板对应不同的工控系统的类型,根据工控系统的类型,从多个虚拟环境模板中选择一个目标虚拟环境模板来搭建作为待检测工控系统对应的虚拟环境。

[0026] 比如说,用户可以根据工控系统的类型,从电子设备中具有的多个虚拟环境模板中选择一个适用该工控系统的虚拟环境模板。

[0027] 或者用户可以向电子设备输入该工控系统的类型等属性信息,以使得电子设备根据该工控系统的类型从多个虚拟环境模板中选择一个适用该工控系统的虚拟环境模板。或者,用户可以向电子设备输入该工控系统的类型等属性信息,以使得电子设备根据该工控系统的类型在电子设备中部署工控系统对应的虚拟环境。

[0028] 步骤102:在虚拟环境中根据工控系统的各种设备的交互关系,搭建工控系统的拓扑结构。其中,拓扑结构用于反映工控系统的各种设备所对应的虚拟化组件之间的连接关系。

[0029] 举例说明,明确工控系统中的各种设备,以及各种设备的交互关系。对工控系统中的硬件实体资源进行虚拟化资源管理,即基于前端的超文本标记语言技术,通过可视化拓扑组网引擎,利用网格画布,从各种虚拟化组件组成的云资源池中,通过拖拽的方式获取各种虚拟化组件。根据工控系统的实际设备与从云资源池中选择设备对应的虚拟化组件,并根据工控系统的实际运行环境,从云资源池中选择虚拟操作系统组件、虚拟可编程逻辑控制器组件、虚拟交换机组件、虚拟防火墙组件等,与设备对应的虚拟化组件进行连接得到工控系统的拓扑结构。

[0030] 步骤103:根据拓扑结构得到工控系统的虚拟化拓扑组网。

[0031] 举例说明,虚拟化拓扑组网可以通过可视化拓扑组网引擎将工控系统的拓扑结构转化得到,可视化拓扑组网引擎自动配置拓扑结构中的各类虚拟化组件和虚拟机的网络,实现工控系统的仿真场景搭建。

[0032] 步骤104:对虚拟化拓扑组网进行漏洞扫描,得到工控系统的漏洞评估结果。

[0033] 其中,漏洞扫描通过漏洞安全评估模块实现。漏洞安全评估模块在虚拟环境中,在搭建好工控系统的仿真场景后,即获得虚拟化拓扑组网后,漏洞安全评估模块选择仿真场

景,并对仿真场景中的所有虚拟化组件进行漏洞扫描分析,得出漏洞评估报告。

[0034] 在本申请的一个实施例中,如图2所示,图2提供了一种工控系统安全检测与评估的方案。构建工控系统的仿真场景,首先通过虚拟化集群连接管理201,完成生成虚拟环境202,其中,虚拟环境所需要的各类虚拟化组件都是来自资源池203。通过前端的可视化网格搭建拓扑结构,进行网格拓扑搭建场景204,从资源池中获取工控系统中各类设备对应的虚拟化组件,生成可视化拓扑结构,并进行自动化配置,实现仿真场景的搭建。在虚拟环境下,对仿真场景中的所有设备进行监控205。在虚拟环境中,根据监控采集的数据,对仿真场景进行安全检测评估并生成报告206。

[0035] 本申请实施例提供了一种工控系统的漏洞检测方法,通过在虚拟环境中搭建工控系统的拓扑组网,可以虚拟化整个工控系统的设备。再将工控系统的拓扑结构经过网络配置,转化为虚拟化拓扑组网,可以实现虚拟化工控系统的真实运行环境。在虚拟环境中,通过漏洞安全评估模块对虚拟化网络拓扑环境进行漏洞扫描,得到工控系统的仿真场景的漏洞评估报告。本申请实施例实现了在工控系统部署至现场前,快速搭建一个虚拟仿真场景,在仿真场景中对工控系统的漏洞进行扫描,从而对工控系统的风险隐患进行安全评估与检测。

[0036] 在本申请的一个实施例中,工控系统的漏洞检测方法还包括:采集在虚拟环境中搭建的工控系统中各种设备交互的数据,将数据进行展示。对工控系统中的各种设备进行监控。

[0037] 本申请的一个实施例如图3所示,开始搭建仿真环境时,步骤301将资源池形成虚拟化;步骤302将虚拟化组件从云资源池中拖拽出来搭建拓扑结构,即生成可视化拓扑组网;步骤303通过虚拟化组件搭建场景,即配置网络后,可视化拓扑组网形成仿真环境。其中,资源池中的数据采集组件开始对拓扑组网中的虚拟组件以及仿真场景的运行状况进行数据采集,比如可编程逻辑控制器(Programmable Logic Controller,PLC)仿真组件,将采集的数据上传至虚拟化组件,如工程师站、操作员站进行监控。

[0038] 在本实施例的一种可能实现方式中,以工控系统为火力发电系统为例,搭建火力发电仿真场景,火力发电仿真场景划分为三块区域,分别为:生产管理区、数据分析区、信息管理区。根据火力发电仿真场景,通过底层的云资源池,选择安全仪表系统(Safety Instrumented System,SIS)虚拟组件、管理信息系统(Management Information System,MIS)虚拟组件、Modbus仿真组件、可编程逻辑控制器(Programmable Logic Controller,PLC)仿真组件、操作员站(虚拟主机)、工程师站(虚拟主机)、数据服务器等虚拟组件,作为数据采集监控与管理控制的模块。用户使用可视化拓扑组网引擎对虚拟组件进行拖拽生成仿真环境,通过交换机虚拟组件与防火墙虚拟组件完成网络联通与配置。通过Modbus仿真组件、PLC仿真组件、操作员站(虚拟主机)、工程师站(虚拟主机)进行数据采集,SIS系统虚拟组件进行数据采集的分析,通过MIS系统虚拟组件与前端门户网站等组件,将采集到的数据做展示。

在本申请的一个实施例中,在电子设备中运行待检测的工控系统对应的虚拟环境之前,包括:在电子设备上进行虚拟化集群管理。根据虚拟化集群管理创建虚拟机,将虚拟机与电子设备的云资源池中的多个虚拟化组件进行连接。对多个虚拟化组件进行地址配置以及部署所述虚拟机的操作系统。通过镜像文件,将虚拟机以及与虚拟机连接的多个虚拟

化组件,定制为一个或多个虚拟环境模板,不同虚拟环境模板对应不同的工控系统的类型。

[0039] 其中,虚拟化集群管理是对虚拟化组件进行拖拽。

[0040] 图4提供了一种仿真环境的快速集成系统,基于可视化拓扑组网引擎,在场景快速搭建平台门户网站搭建虚拟环境、工控系统的仿真场景等,并对虚拟环境中的各个虚拟组件进行数据采集和数据监控。

[0041] 具体说明如下:

场景快速搭建平台门户包括用户自服务门户、靶场运营管理门户和靶场运维管理门户,均通过前端页面展现。在前端页面上,基于可视化拓扑组网引擎,可以进行虚拟化集群管理、模板管理、镜像管理、组件资源管理以及监控管理。

[0042] 应用服务及运行引擎,负责定义服务的结构、流程等信息,用于形成完整的服务生命周期管理,具体为:组装原子服务、生成业务服务、将业务服务发布到服务目录、监控服务运行状况。其中,管理员可以通过应用服务及运行引擎监控所有服务实例的整体状况。

[0043] 可视化拓扑组网引擎,是基于前端的超文本标记语言技术实现,具体为一个网格画布,用于编辑网络的拓扑结构,它具有图形化的编辑界面,并且提供由各种通信实体对应的虚拟化组件组成的组件库,如交换机、路由器、可编程逻辑控制器、服务器、工程师站等,用户可以通过简单的拖放操作在网格画布的工作区中快速、方便的配置网络拓扑结构,也可以对网络拓扑结构中各种虚拟化组件的属性进行设置。

[0044] 物理资源层,包含三个方面的内容,即计算机、网络和存储。基于标准化计算、存储和网络构建的场景快速搭建平台系统是动态、高度自动化和软件定义的。用户可以根据需要配置一个适合的、灵活的物理资源系统。本实施例中基于标准X86架构服务器还可以更快地进行部署,更好地进行管理,以满足长期扩展的需要。

[0045] 云资源池基础架构指管理和调度软硬件资源的逻辑组件,它负责构建资源池,生成简单资源供应的技术服务,定义资源运维的操作流程。为了组成资源池,一般将具有相同属性的设备集中安装,相互连接,并通过一定的管理软件来监管和配置。资源池由具有相同属性设备的一组资源组成,用户可以通过云资源池基础架构管理层软件从资源池中申请资源,指定该资源实例的配置,并管理其运行。管理员可以监控每个资源池的资源使用率、健康状况和性能状况。资源管理层将以技术服务的形式对外发布所有的资源操作接口。这一层要屏蔽掉不同虚拟化类别以及物理设备等的差异,使得上层无法感知。

[0046] 数据采集与监控,通常使用采集器对平台的流量数据、网络数据、平台数据进行采集,流量数据以数据包的形式进行采集,将三种数据作为数据源发送给数据监控系统,数据监控系统将数据源进行深层次解析后通过数据接口发送给应用服务及运行引擎后展现到页面中。

[0047] 在本申请的一个实施例中,电子设备具有云资源池,云资源池中存储有一个或多个虚拟化组件,虚拟环境中搭建仿真场景,仿真场景为工控系统的所述拓扑结构,包括:响应于用户的第一操作,展示图形化的编辑界面,编辑界面上显示有一个或多个所述虚拟化组件的标识。检测用户在编辑界面输入的针对一个或多个虚拟化组件中的多个虚拟化组件的第一选择操作。响应于第一选择操作,根据被选择的多个虚拟化组件生成工控系统的拓扑结构,拓扑结构的节点对应一个构成拓扑结构的虚拟化组件,拓扑结构的节点代表工控系统的一个设备。配置构成拓扑结构的每个虚拟化组件的网络配置参数和/或存储配置参

数,得到虚拟化拓扑组网。

[0048] 在本申请的一个实施例中,配置构成拓扑结构的每个虚拟组件的网络参数,得到虚拟化拓扑组网,方法还包括:显示构成拓扑结构的多个虚拟化组件。检测用户在拓扑结构上输入的针对任一虚拟化组件的第二选择操作。响应于第二选择操作,更新任一虚拟化组件的网络配置参数和/或存储配置参数,得到虚拟化拓扑组网。

[0049] 举例说明,在可视化拓扑组网的操作界面上,显示生成的拓扑结构,其中组成拓扑结构的多个虚拟化组件都可以进行操作。作为一种示例,用户对工控系统中的第一设备对应的虚拟化组件进行第二选择操作,该虚拟化组件进行网络参数配置以及存储参数配置。

[0050] 在本申请的一个实施例中,配置构成拓扑结构的每个虚拟化组件的网络配置参数和/或存储配置参数,得到虚拟化拓扑组网,还可以通过可视化拓扑组网引擎实现,可视化拓扑组网引擎可以将拓扑结构转化为虚拟化拓扑组网。

[0051] 在工控系统的拓扑结构在虚拟环境中搭建完成后,可视化拓扑组网引擎可以自动对拓扑结构进行网络配置或存储配置。

[0052] 值得说明的是,配置拓扑结构的网络可以根据搭建的工控系统的拓扑结构,由可视化拓扑组网引擎自动配置。但是由于自动配置存在一定的误差,即配置的不一定完全正确,因此在可视化拓扑组网的操作界面上,用户可以对任一拓扑结构的虚拟化组件进行手动配置。

[0053] 在本申请的一个实施例中,采集在虚拟环境中搭建的工控系统中各种设备交互的数据,将数据进行展示,数据包括:流量数据、网络数据以及平台数据。

[0054] 其中,流量数据的形式为数据包;网络数据至少包括网络静态配置、网络实时状态以及各项性能数据;平台数据包括代理数据、系统资源信息以及网络拓扑信息。将数据发送至监控管理模块,监控管理模块对数据进行解析,将解析后的结果发送至虚拟环境中进行展示。

[0055] 作为一种示例,如图4所示,数据采集设备与物理资源层连接,即计算机设备。在物理资源层中的虚拟环境、云资源池、工控系统的仿真场景中的各类虚拟组件将运行的数据发送至数据采集设备,例如,构建工控系统的仿真环境使用的虚拟组件数量、运行的虚拟组件数量、仿真场景占用所使用的虚拟机内存、创建时间、使用时间等。数据采集设备将采集的数据进行储存,并发送至虚拟环境中的监控管理模块进行解析,并在可视化拓扑组网引擎的基础上进行展示。

[0056] 在本申请的一个实施例中,对虚拟化拓扑组网进行漏洞扫描,得到工控系统的漏洞评估报告,包括:在虚拟环境中安装代理或服务,代理或服务用于访问虚拟化拓扑组网的文件和进程。根据虚拟化拓扑组网的文件和进程,生成评估报告。

[0057] 图5为本申请实施例提供的一种工控系统的漏洞检测与评估方法的流程图,场景快速搭建平台508通过前端页面的形式展现,页面中包含搭建仿真场景、进行监控管理以及漏洞检测所需要使用的七个模块:虚拟化连接模块501、模板管理模块502、镜像管理模块503、组件资源模块504、场景管理模块505、监控管理模块506以及漏洞安全评估模块507。

[0058] 步骤1:通过连接虚拟环境平台的地址调用应用程序编程接口(Application Programming Interface,API)进行数据对接,使虚拟环境平台能够与虚拟环境进行数据通信,用户可以通过虚拟化连接模块501以拖拽的方式,新增多个虚拟环境,指定开启某个虚

拟环境即可对其进行操作。

[0059] 步骤2:用户模板管理模块502在虚拟环境下进行手动新建虚拟机,对虚拟机部署指定操作系统,在操作系统中配置好环境变量并且部署刚需软件,将此虚拟机定制成模板以供用户使用;镜像管理模块503用于根据已有镜像库做支撑,可以免去下载和编辑源文件,以及上传和配置安装开发工具(比如,Cloud-init),从而在镜像管理模块503中一键获取刷新镜像资源,支持镜像扩展及基本启停操作;组件资源模块504用于结合不同工控系统的真实场景,将工控系统中的各种通信实体虚拟化,形成虚拟化组件,并且提供由各种通信实体对应的虚拟化组件组成的组件库。

[0060] 步骤3:搭建工控系统的拓扑结构,配置网络形成仿真场景。场景管理模块505对计算资源、存储资源和网络资源进行有效管控,可根据实际需求灵活组建不同业务场景,最大限度优化实体资源使用效率,实现从简单到复杂的多场景快速迭代。

[0061] 步骤4:通过监控管理模块506对每个创建的仿真场景进行监控,包括仿真场景使用的组件数量、运行组件数量、占用所使用的虚拟机内存、创建时间、使用时间等,并进行展示。其中,超级管理员还可以进入用户的拓扑结构图对其进行控制。

[0062] 步骤5:在场景快速搭建平台通过前端页面,通过漏洞安全评估模块507对虚拟环境和前端进行漏洞扫描,生成漏洞检测报告,以及给出相应的修改指导方案,供研发人员进行修改调整。

[0063] 图6为本申请实施例提供的一种工控系统的漏洞检测装置60,包括:运行模块601,用于在电子设备中运行待检测的工控系统对应的虚拟环境。构建模块602,用于在虚拟环境中根据工控系统的各种设备的交互关系,搭建工控系统的拓扑结构,拓扑结构用于反映工控系统的各种设备的网络结构。转化模块603,将拓扑结构转化为虚拟化拓扑组网。评估模块604,用于对虚拟化拓扑组网进行漏洞扫描,得到工控系统的漏洞评估结果。

[0064] 在本申请的一个实施例中,提供了一种工控系统的漏洞检测装置,包括:监控模块605,用于采集在虚拟环境中搭建的工控系统中各种设备交互的数据,将数据进行展示,对工控系统中的各种设备进行监控。

[0065] 图7为本申请实施例提供的一种计算机设备的结构示意图。如图7所示,计算机设备701包括:处理器7011、存储器7012以及存储在存储器7012中并可在处理器7011上运行的计算机程序7013,处理器7011执行计算机程序7013时实现上述实施例中的同步数据方法中的步骤。

[0066] 计算机设备701可以是一个通用计算机设备或一个专用计算机设备。在具体实现中,计算机设备701可以是台式机、便携式电脑、网络服务器、掌上电脑、移动手机、平板电脑、无线终端设备、通信设备或嵌入式设备,本申请实施例不限定计算机设备701的类型。本领域技术人员可以理解,图7仅仅是计算机设备701的举例,并不构成对计算机设备701的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件,比如还可以包括输入输出设备、网络接入设备等。

[0067] 处理器7011可以是中央处理单元(Central Processing Unit,CPU),处理器7011还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、

分立硬件组件等。通用处理器可以是微处理器或者也可以是任何常规的处理器。

[0068] 存储器7012在一些实施例中可以是计算机设备701的内部存储单元,比如计算机设备701的硬盘或内存。存储器7012在另一些实施例中也可以是计算机设备701的外部存储设备,比如计算机设备701上配备的插接式硬盘、智能存储卡(Smart Media Card,SMC)、安全数字(Secure Digital,SD)卡、闪存卡(Flash Card)等。进一步地,存储器7012还可以既包括计算机设备701的内部存储单元也包括外部存储设备。存储器7012用于存储操作系统、应用程序、引导装载程序(Boot Loader)、数据以及其他程序等。存储器7012还可以用于暂时地存储已经输出或者将要输出的数据。

[0069] 本申请实施例还提供了一种计算机可读存储介质,该计算机可读存储介质存储有计算机程序,该计算机程序被处理器执行时可实现上述各个方法实施例中的步骤。

[0070] 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实现上述方法实施例中的全部或部分流程,可以通过计算机程序来指令相关的硬件来完成,该计算机程序可存储于一计算机可读存储介质中,该计算机程序在被处理器执行时,可实现上述各个方法实施例的步骤。其中,该计算机程序包括计算机程序代码,该计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。该计算机可读介质至少可以包括:能够将计算机程序代码携带到拍照装置/终端设备的任何实体或装置、记录介质、计算机存储器、ROM(Read-Only Memory,只读存储器)、RAM(Random Access Memory,随机存取存储器)、CD-ROM(Compact Disc Read-Only Memory,只读光盘)、磁带、软盘和光数据存储设备等。本申请提到的计算机可读存储介质可以为非易失性存储介质,换句话说,可以是非瞬时性存储介质。

[0071] 本申请实施例还提供了一种芯片,芯片包括处理器,处理器与通信接口耦合,处理器用于运行计算机程序或指令,以实现如上述实施例的数据同步方法,通信接口用于与芯片之外的其它模块进行通信。

[0072] 本申请实施例还提供了一种通信装置,包括:通信接口以及至少一个处理器,至少一个处理器与通信接口连接,至少一个处理器与存储器耦合,至少一个处理器用于运行存储器中存储的指令以执行上述实施例的数据同步方法,通信接口用于与通信装置之外的其它模块进行通信。

[0073] 应当理解的是,实现上述实施例的全部或部分步骤可以通过软件、硬件、固件或者其任意结合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机指令。该计算机指令可以存储在上述计算机可读存储介质中。

[0074] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述或记载的部分,可以参见其它实施例的相关描述。

[0075] 本领域普通技术人员可以意识到,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、或者计算机软件和电子硬件的结合来实现。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申请的范围。

[0076] 在本申请所提供的实施例中,应该理解到,所揭露的装置/计算机设备和方法,可以通过其它的方式实现。例如,以上所描述的装置/计算机设备实施例仅仅是示意性的,例如,模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口,装置或单元的间接耦合或通讯连接,可以是电性,机械或其它的形式。

[0077] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0078] 以上实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围,均应包含在本申请的保护范围之内。

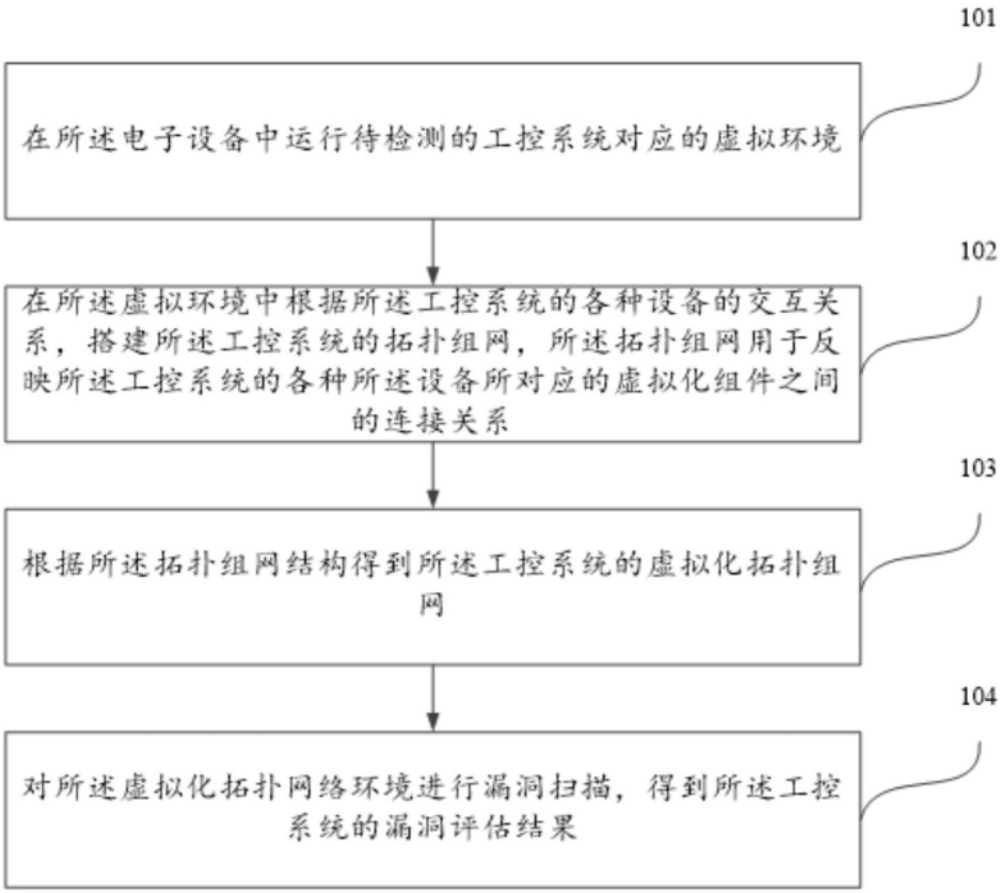

101
在所述电子设备中运行待检测的工控系统对应的虚拟环境
102
在所述虚拟环境中根据所述工控系统的各种设备的交互关系，搭建所述工控系统的拓扑组网，所述拓扑组网用于反映所述工控系统的各种所述设备所对应的虚拟化组件之间的连接关系
103
根据所述拓扑组网结构得到所述工控系统的虚拟化拓扑组网
104
对所述虚拟化拓扑网络环境进行漏洞扫描，得到所述工控系统的漏洞评估结果

图1

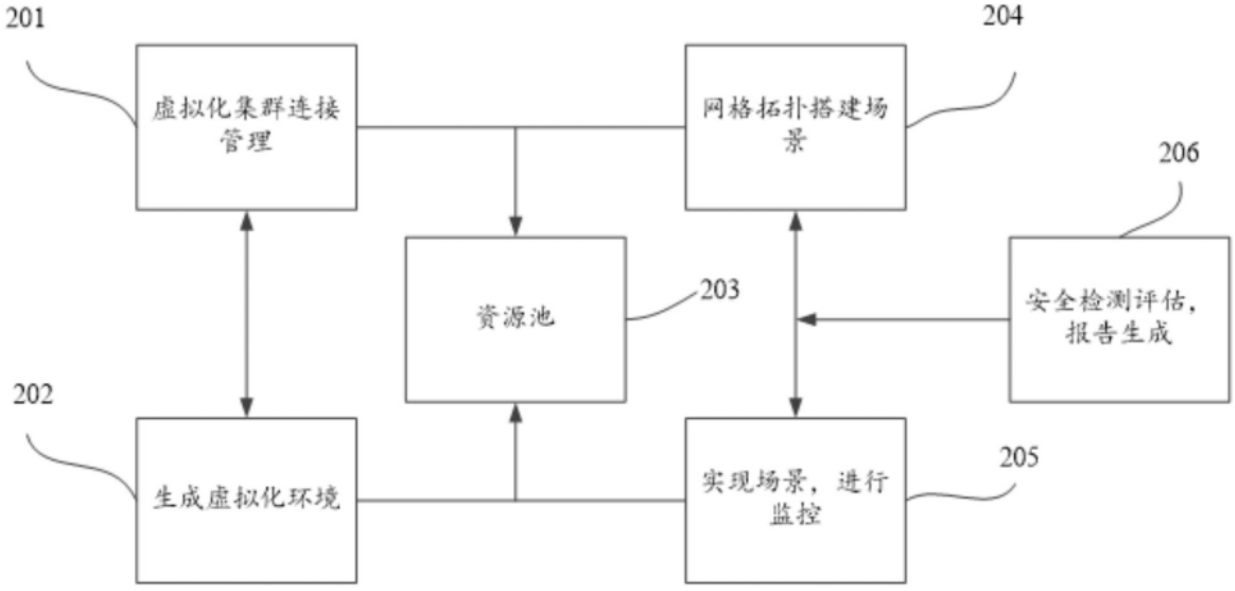

201
虚拟化集群连接管理
204
网格拓扑搭建场景
206
资源池
203
安全检测评估，报告生成
202
生成虚拟化环境
205
实现场景，进行监控

图2

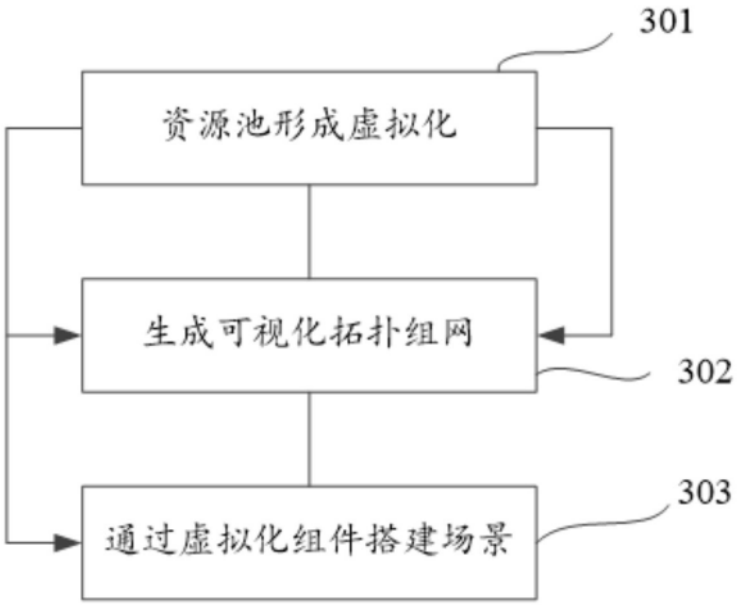

301
资源池形成虚拟化
生成可视化拓扑组网
302
通过虚拟化组件搭建场景
303

图3

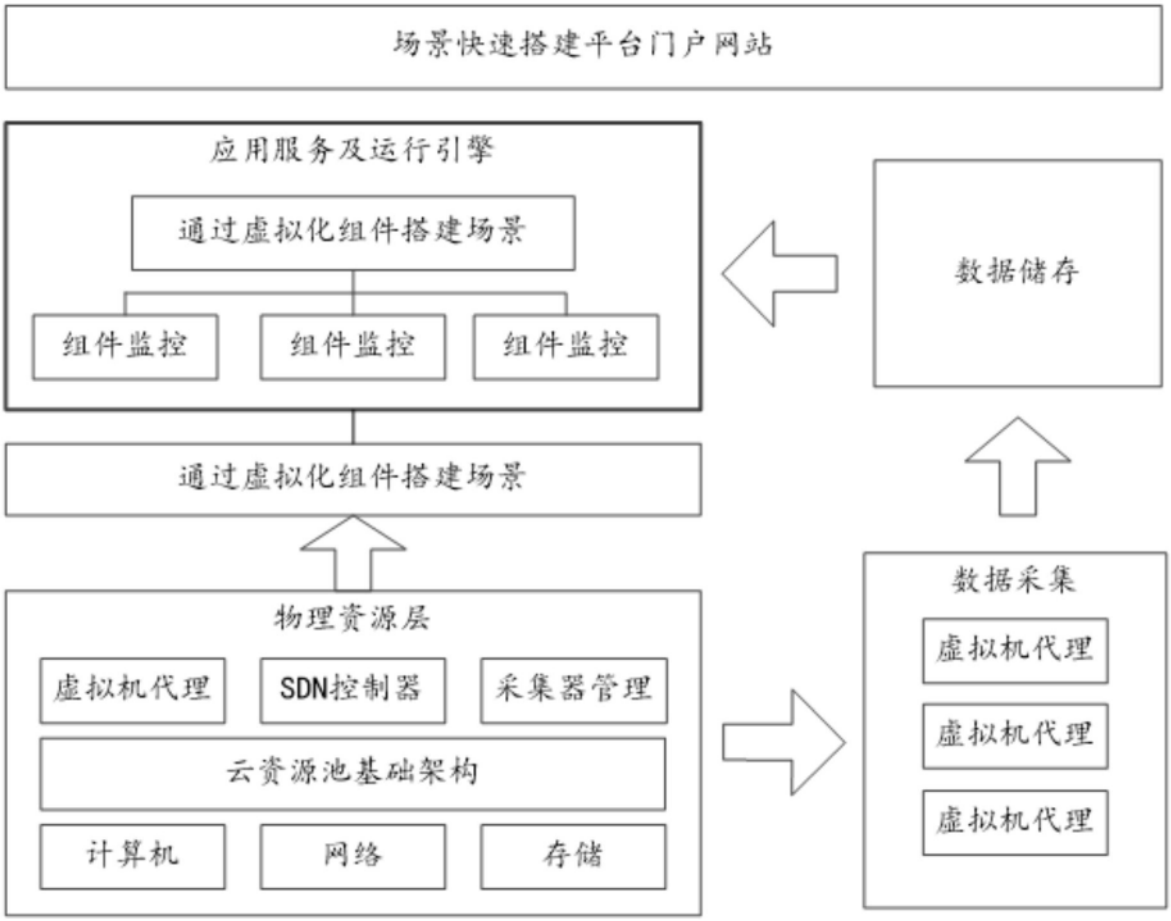

场景快速搭建平台门户网站
应用服务及运行引擎
通过虚拟化组件搭建场景
组件监控
组件监控
组件监控
数据储存
通过虚拟化组件搭建场景
物理资源层
虚拟机代理
SDN控制器
采集器管理
云资源池基础架构
计算机
网络
存储
数据采集
虚拟机代理
虚拟机代理
虚拟机代理

图4

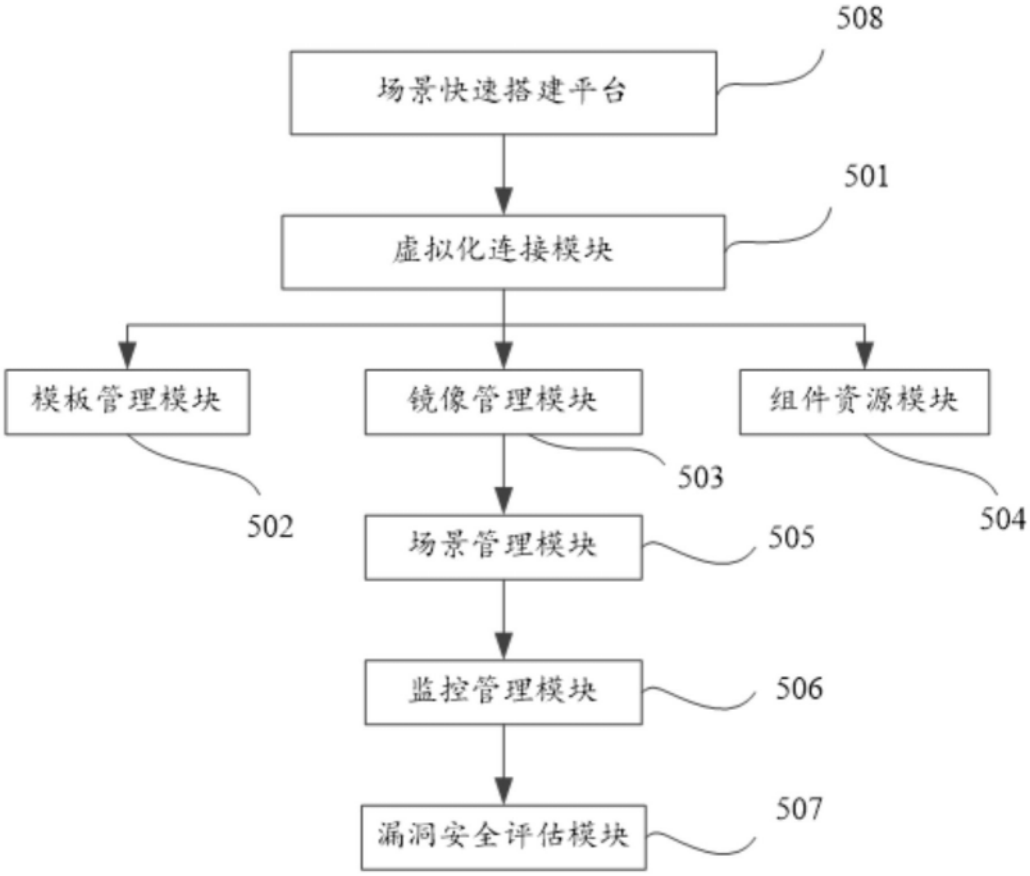

508
场景快速搭建平台
501
虚拟化连接模块
模板管理模块
镜像管理模块
组件资源模块
502
503
504
场景管理模块
505
监控管理模块
506
漏洞安全评估模块
507

图5

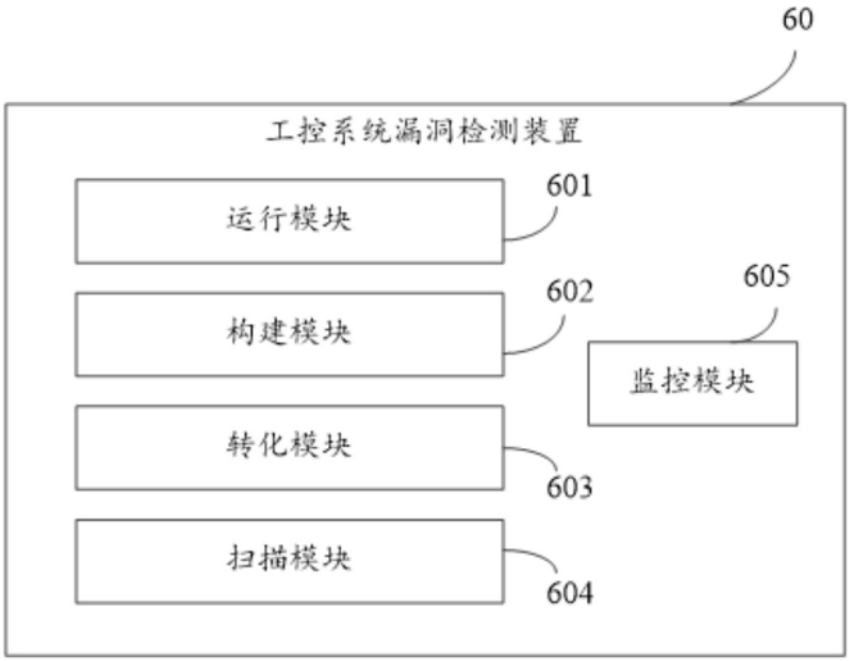

60
工控系统漏洞检测装置
运行模块
601
构建模块
602
605
监控模块
转化模块
603
扫描模块
604

图6

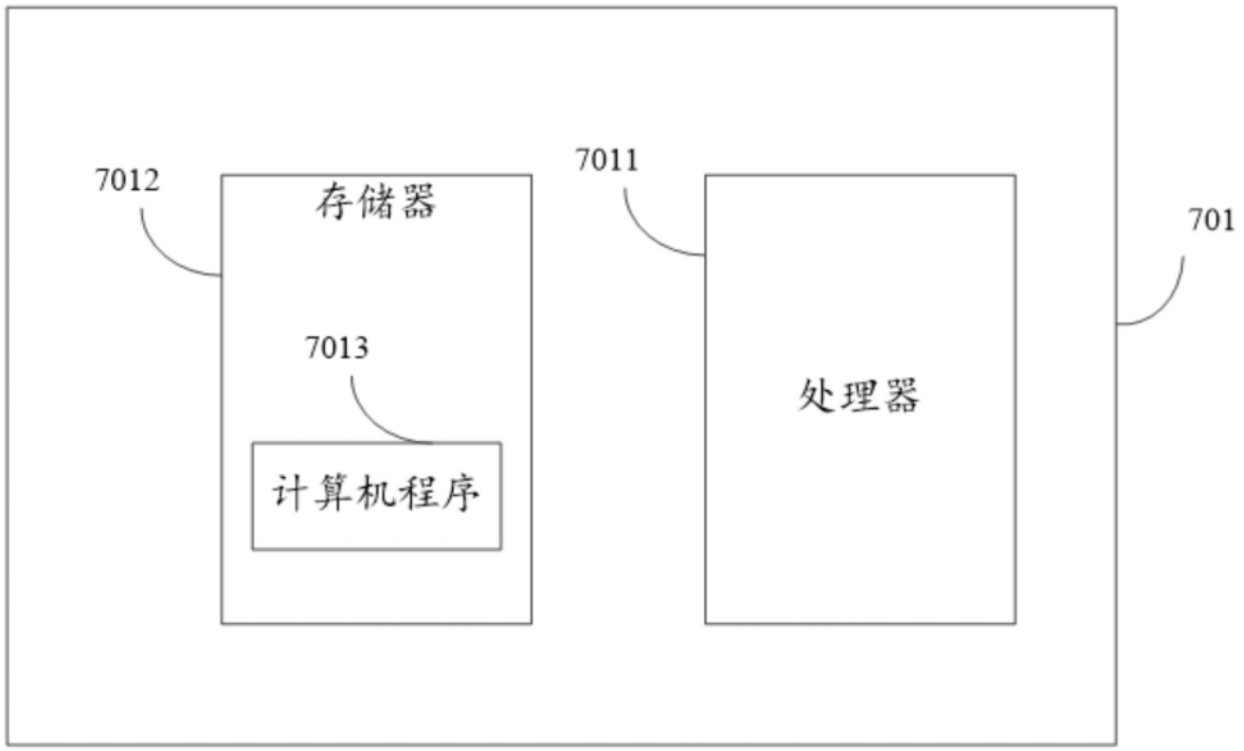


图7