(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111970166 B
(45)授权公告日 2021.11.12

(21)申请号 202010763289.8

(22)申请日 2020.07.31

(65)同一申请的已公布的文献号
申请公布号 CN 111970166 A

(43)申请公布日 2020.11.20

(73)专利权人 南京南瑞继保电气有限公司
地址 211100 江苏省南京市江宁经济技术开发区苏源大道69号
专利权人 南京南瑞继保工程技术有限公司

(72)发明人 黄伟 李忠安 陈丹瑜 冯传水 于哲 笃峻

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 周艳 张颖玲

(51)Int.Cl.
H04L 12/26(2006.01)

(56)对比文件
CN 111092786 A,2020.05.01
CN 102916859 A,2013.02.06
CN 102361346 A,2012.02.22
CN 107679768 A,2018.02.09
CN 109922073 A,2019.06.21
CN 109886475 A,2019.06.14
CN 103152341 A,2013.06.12
WO 2009128905 A1,2009.10.22

审查员 梁丽霞

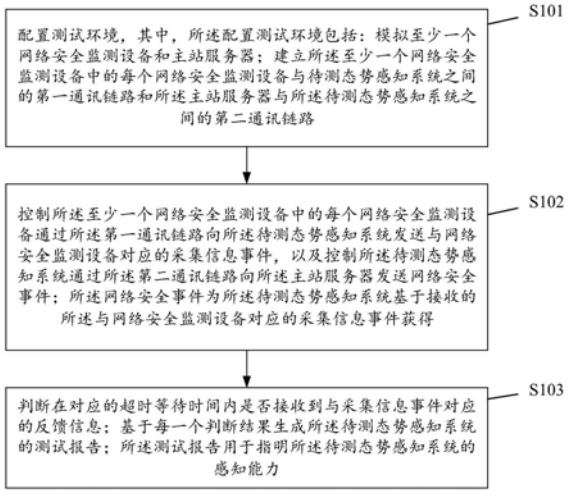
权利要求书3页 说明书17页 附图2页

(54)发明名称

一种测试方法、装置、设备、系统及计算机可读存储介质

(57)摘要

本发明公开一种测试方法、装置、设备、系统及计算机可读存储介质。其中，所述方法包括：配置测试环境，其中，配置测试环境包括：模拟至少一个网络安全监测设备和主站服务器；建立每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和主站服务器与待测态势感知系统之间的第二通讯链路；控制每个网络安全监测设备通过第一通讯链路向待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制待测态势感知系统通过第二通讯链路向主站服务器发送网络安全事件；判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息；基于每一个判断结果生成待测态势感知系统的测试报告。



CN 111970166 B

1.一种测试方法,其特征在于,所述方法包括:

配置测试环境,其中,所述配置测试环境包括:模拟至少一个网络安全监测设备和主站服务器;建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路;

控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;

判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息,其中,所述反馈信息为所述主站服务器按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件后反馈的解析结果;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

2.根据权利要求1所述的方法,其特征在于,所述模拟至少一个网络安全监测设备,包括:

配置至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备,其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;

模拟主站服务器包括:配置第二基本信息,基于所述第二基本信息生成所述主站服务器,其中,所述第二基本信息包括第一通讯地址和第一端口编号;

其中,所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果。

3.根据权利要求2所述的方法,其特征在于,所述建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路,包括:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号,以使所述至少一个网络安全监测设备中的每个网络安全监测设备基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路;

建立所述主站服务器与所述待测态势感知系统之间的第二通讯链路,包括:向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号,以使所述待测态势感知系统基于所述第一通讯地址和第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

4.根据权利要求1所述的方法,其特征在于,所述控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送对应的采集信息事件,包括:

向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令;所述采集信息指令用于指示所述网络安全监测设备生成与所述采集信息指令对应的采集信息事件并通过所述第一通讯链路向所述待测态势感知系统发送所述与采集信息

指令对应的采集信息事件;其中,所述至少一条采集信息指令是基于配置的采集信息项列表生成;所述采集信息项列表包括用于生成每条采集信息指令的各配置参数;

对应的,所述控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件,包括:

控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送每一个与所述采集信息事件对应的网络安全事件。

5.根据权利要求1所述的方法,其特征在于,所述基于每一个判断结果生成所述待测态势感知系统的测试报告,包括:

记录与每一个判断结果对应的测试结果;

基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;

其中,在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息,所述测试结果为通过;在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息,所述测试结果为未通过。

6.根据权利要求4所述的方法,其特征在于,所述方法还包括:

为每一个网络安全监测设备加载与网络安全监测设备对应的采集信息列表;所述采集信息列表为按照设定的态势感知技术规范设置的需要采集网络安全监测设备的各数据所形成。

7.根据权利要求5所述的方法,其特征在于,所述方法还包括:

采用同一标识显示所述测试报告中的相同的测试结果,以及采用不同标识显示所述测试报告中的不相同的测试结果。

8.根据权利要求4所述的方法,其特征在于,所述方法还包括:

记录基于所述采集信息项列表生成的每一条采集信息指令、每一个网络安全监测设备基于每一条采集信息指令生成的每一个采集信息事件,以及所述待测态势感知系统基于每一个采集信息事件生成的每一个网络安全事件;

将每一条记录添加到所述测试报告中的相应位置;其中,所述相应位置是指能够使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系的记录位置。

9.一种测试装置,其特征在于,所述测试装置包括:配置单元、控制单元和判断单元,其中,

所述配置单元,用于配置测试环境,其中,所述配置测试环境包括:模拟至少一个网络安全监测设备和主站服务器;建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路;

所述控制单元,用于控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;

所述判断单元,用于判断在对应的超时等待时间内是否接收到与采集信息事件对应的

反馈信息;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

10.一种计算机可读存储介质,其特征在于,所述可读存储介质上存储有计算机程序;所述计算机程序被处理器执行时实现权利要求1至8任一项所述方法的步骤。

11.一种测试设备,其特征在于,所述测试设备包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,其中,所述处理器用于运行所述计算机程序时,执行权利要求1至8任一项所述方法的步骤。

12.一种测试系统,其特征在于,所述系统包括测试控制模组、监测对象模拟模组和主站模拟模组,其中,所述测试控制模组,用于配置测试环境,其中,所述配置测试环境包括:通过所述监测对象模拟模组模拟至少一个网络安全监测设备和通过所述主站模拟模组模拟主站服务器;

建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路;控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息,其中,所述反馈信息为所述主站服务器按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件后反馈的解析结果;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

13.根据权利要求12所述的系统,其特征在于,所述测试控制模组、所述监测对象模拟模组和所述主站模拟模组设置在同一台计算机。

一种测试方法、装置、设备、系统及计算机可读存储介质

技术领域

[0001] 本发明涉及电力监控系统网络安全领域，尤其涉及一种测试方法、装置、设备、系统及计算机可读存储介质。

背景技术

[0002] 目前电网公司对电力监控系统的网络安全要求越来越严格，并且已经逐步建立电力监控系统网络安全态势感知系统，以实现对电网公司各电力监控系统全方位、全天候的网络安全态势感知，以便及时地发现各类网络安全风险以及非法访问事件，从而实现电力监控系统网络安全的态势感知及预警。为了保证接入到电力监控系统中的网络安全态势感知系统的监控能力，国网公司和南网公司提出了对要接入电力监控系统的网络安全态势感知系统进行入网检测，并指定了系列的入网检测规范和要求，然后组织电科院进行网络安全态势感知系统准入测试。应该知道，由于电力监控系统中的设备众多，也即：要接入的网络安全态势感知系统需要监测的对象众多，因而，在实验室很难搭建出一个全面的、数量众多的对象的电力监控系统来满足对网络安全态势感知系统的测试。现有常见的测试方式是利用一台或者少量几台设备搭建的电力监控系统对网络安全态势感知系统进行测试，其可能存在以下缺点：若通过增加电力监控系统中的设备的数量对网络安全态势感知系统进行性能测试，其成本支出将成倍增加；再者而仅用一台或者几台网络设备搭建的电力监控系统又无法实现对较大吞吐量的网络安全态势感知系统的性能进行有效的测试。由于以上原因，亟需一套功能完备，灵活配置各类电力监控系统中的设备，使用简单，操作方面的测试工具来支撑对网络安全态势感知系统的测试。

发明内容

[0003] 有鉴于此，本发明的主要目的在于提供一种测试方法、装置、设备及系统，能够至少解决上述部分问题。

[0004] 为达到上述目的，本发明的技术方案是这样实现的：

[0005] 第一方面，本发明实施例提供一种测试方法，所述方法包括：

[0006] 配置测试环境，其中，所述配置测试环境包括：模拟至少一个网络安全监测设备和主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路；

[0007] 控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件；所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得；

[0008] 判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息；基于

每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

[0009] 在上述方案中,所述模拟至少一个网络安全监测设备,包括:

[0010] 配置至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备,其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;

[0011] 模拟主站服务器包括:配置第二基本信息,基于所述第二基本信息生成所述主站服务器,其中,所述第二基本信息包括第一通讯地址和第一端口编号;

[0012] 其中,所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0013] 在上述方案中,所述建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路,包括:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号,以使所述至少一个网络安全监测设备中的每个网络安全监测设备基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路;

[0014] 建立所述主站服务器与所述待测态势感知系统之间的第二通讯链路,包括:向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号,以使所述待测态势感知系统基于所述第一通讯地址和第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0015] 在上述方案中,所述控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送对应的采集信息事件,包括:

[0016] 向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令;所述采集信息指令用于指示所述网络安全监测设备生成与所述采集信息指令对应的采集信息事件并通过所述第一通讯链路向所述待测态势感知系统发送所述与采集信息指令对应的采集信息事件;其中,所述至少一条采集信息指令是基于配置的采集信息项列表生成;所述采集信息项列表包括用于生成每条采集信息指令的各配置参数;

[0017] 对应的,所述控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件,包括:

[0018] 控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送每一个与所述采集信息事件对应的网络安全事件。

[0019] 在上述方案中,所述基于每一个判断结果生成所述待测态势感知系统的测试报告,包括:

[0020] 记录与每一个判断结果对应的测试结果;

[0021] 基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;

[0022] 其中,在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息,所述测试结果为通过;在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息,所述测试结果为未通过。

[0023] 在上述方案中，所述方法还包括：

[0024] 为每一个网络安全监测设备加载与网络安全监测设备对应的采集信息列表；所述采集信息列表为按照设定的态势感知技术规范设置的需要采集网络安全监测设备的各数据所形成。

[0025] 在上述方案中，所述方法还包括：

[0026] 采用同一标识显示所述测试报告中的相同的测试结果，以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0027] 在上述方案中，所述方法还包括：

[0028] 记录基于所述采集信息项列表生成的每一条采集信息指令、每一个网络安全监测设备基于每一条采集信息指令生成的每一个采集信息事件，以及所述待测态势感知系统基于每一个采集信息事件生成的每一个网络安全事件；

[0029] 将每一条记录添加到所述测试报告中的相应位置；其中，所述相应位置是指能够使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系的记录位置。

[0030] 第二方面，本发明实施例提供一种测试装置，所述测试装置包括：配置单元、控制单元和判断单元，其中，

[0031] 所述配置单元，用于配置测试环境，其中，所述配置测试环境包括：模拟至少一个网络安全监测设备和主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路；

[0032] 所述控制单元，用于控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件；所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得；

[0033] 所述判断单元，用于判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息；基于每一个判断结果生成所述待测态势感知系统的测试报告；所述测试报告用于指明所述待测态势感知系统的感知能力。

[0034] 在上述方案中，所述配置单元，具体用于：配置至少一个第一基本信息，基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备，以及配置第二基本信息，基于所述第二基本信息生成所述主站服务器；其中，所述每个第一基本信息均至少包括：设备名称、互联网协议IP地址以及媒体存取控制MAC地址；所述第二基本信息包括第一通讯地址和第一端口编号；所述网络安全监测设备为电力监控系统中的各电子设备；所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果；所述解析结果为所述反馈信息。

[0035] 在上述方案中，所述配置单元，还具体用于：向所述至少一个网络安全监测设备中的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号，以使所述至少一个网络安全监测设备中的每个网络安全监测设备基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路；以及向所述待

测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号，以使所述待测态势感知系统基于所述第一通讯地址和第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0036] 在上述方案中，所述控制单元，具体用于：向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令；所述采集信息指令用于指示所述网络安全监测设备生成与所述采集信息指令对应的采集信息事件并通过所述第一通讯链路向所述待测态势感知系统发送所述与采集信息指令对应的采集信息事件；其中，所述至少一条采集信息指令是基于配置的采集信息项列表生成；所述采集信息项列表包括用于生成每条采集信息指令的各配置参数；以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送每一个与所述采集信息事件对应的网络安全事件。

[0037] 在上述方案中，所述判断单元，具体用于：记录与每一个判断结果对应的测试结果；基于每一个对应的测试结果生成所述测试报告；所述测试报告以可读文档形式存储；其中，在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息，所述测试结果为通过；在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息，所述测试结果为未通过。

[0038] 在上述方案中，所述测试装置还包括：加载单元，用于：为每一个网络安全监测设备加载与网络安全监测设备对应的采集信息列表；所述采集信息列表为按照设定的态势感知技术规范设置的需要采集网络安全监测设备的各数据所形成。

[0039] 在上述方案中，所述测试装置还包括：显示单元，用于：采用同一标识显示所述测试报告中的相同的测试结果，以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0040] 在上述方案中，所述判断单元，还具体用于：记录基于所述采集信息项列表生成的每一条采集信息指令、每一个网络安全监测设备基于每一条采集信息指令生成的每一个采集信息事件，以及所述待测态势感知系统基于每一个采集信息事件生成的每一个网络安全事件；将每一条记录添加到所述测试报告中的相应位置；其中，所述相应位置是指能够使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系的记录位置。

[0041] 第三方面，本发明实施例提供一种计算机可读存储介质，所述可读存储介质上存储有计算机程序；所述计算机程序被处理器执行时实现上述任一项所述方法的步骤。

[0042] 第四方面，本发明实施例提供一种测试设备，所述测试设备包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，其中，所述处理器用于运行所述计算机程序时，执行上述任一项所述方法的步骤。

[0043] 第五方面，本发明实施例提供一种测试系统，所述系统包括测试控制模组、监测对象模拟模组和主站模拟模组，其中，

[0044] 所述测试控制模组，用于配置测试环境，其中，所述配置测试环境包括：通过所述监测对象模拟模组模拟至少一个网络安全监测设备和通过所述主站模拟模组模拟主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路；控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路

向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

[0045] 在上述方案中,所述测试控制模组,具体用于:配置至少一个第一基本信息,向所述监测对象模拟模组发送所述至少一个第一基本信息;以及配置第二基本信息,向所述主站模拟模组发送所述第二基本信息;

[0046] 所述监测对象模拟模组,用于接收所述测试控制模组发送的所述至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备;

[0047] 所述主站模拟模组,用于接收所述测试控制模组发送的第二基本信息,基于所述第二基本信息生成所述主站服务器;

[0048] 其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;所述第二基本信息包括第一通讯地址和第一端口编号;所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0049] 在上述方案中,所述测试控制模组,还用于:向所述监测对象模拟模组模拟的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编;以及向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号;

[0050] 所述监测对象模拟模组模拟的每个网络安全监测设备,用于接收所述第二通讯地址和所述第二端口编号,并基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路;

[0051] 所述待测态势感知系统,用于接收所述第一通讯地址和所述第二端口编号,并基于所述第一通讯地址和所述第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0052] 在上述方案中,所述测试控制模组,还用于:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令;

[0053] 所述监测对象模拟模组模拟的每个网络安全监测设备,用于接收所述至少一条采集信息指令,并基于每一条采集信息指令生成与采集信息指令对应的采集信息事件,通过所述第一通讯链路向所述待测态势感知系统发送所述采集信息事件;

[0054] 所述待测态势感知系统,用于接收所述采集信息事件,并将所述采集信息事件转换成网络安全事件,通过所述第二通讯链路向所述主站服务器发送所述网络安全事件;

[0055] 所述主站服务器,用于接收所述网络安全事件,按照设定规范解析所述网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0056] 在上述方案中,所述测试控制模组,还用于:记录与每一个判断结果对应的测试结果;基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;其

中，在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息，所述测试结果为通过；在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息，所述测试结果为未通过。

[0057] 在上述方案中，所述系统还包括显示模组，用于采用同一标识显示所述测试报告中的相同的测试结果，以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0058] 在上述方案中，所述测试控制模组、所述监测对象模拟模组和所述主站模拟模组设置在同一台计算机。

[0059] 本发明实施例提供一种测试方法、装置、设备、系统及计算机可读存储介质，其中，所述方法包括：配置测试环境，其中，所述配置测试环境包括：模拟至少一个网络安全监测设备和主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路；控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件；所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得；判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息；基于每一个判断结果生成所述待测态势感知系统的测试报告；所述测试报告用于指明所述待测态势感知系统的感知能力。与现有的测试方法相比，采用本发明提供的测试方法有以下优点：1、在实验室等简单环境中即可部署多种测试系统，大大降低了测试环境搭建的难度、成本及周期；2、可灵活配置不同类型的网络安全监测设备类型，提高了系统的自适应性；3、可支持对多台(比如1000台)网络安全监测设备进行模拟仿真，大大增加了可模拟设备的数量；4、能够实现对待测试态势感知系统的闭环仿真测试，具有极高的实际价值；5、可提供完整全面的测试报告，简化测试人员分析问题的难度；6、实现了快速配置、降低了测试复杂度，节约了劳动成本，提高了测试效率。

附图说明

[0060] 图1为本发明实施例提供的一种测试方法的流程示意图；

[0061] 图2为本发明实施例提供的一种测试系统的结构示意图；

[0062] 图3为本发明实施例提供的一种测试装置的结构示意图；

[0063] 图4为本发明实施例提供的一种测试设备的硬件结构示意图。

具体实施方式

[0064] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对发明的具体技术方案做进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0065] 下面结合附图及具体实施例对本发明作进一步详细的说明。

[0066] 如图1所示，其示出本发明实施例提供的一种测试方法的流程示意图。在图1中，所述方法包括：

[0067] S101：配置测试环境，其中，所述配置测试环境包括：模拟至少一个网络安全监测

设备和主站服务器;建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路;

[0068] S102:控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;

[0069] S103:判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

[0070] 需要说明的是,这里所说的配置测试环境,换句话说,是指搭建用于测试待测试测态势感知系统监控某一电力监控系统中的网络安全监测设备能力的测试系统。更通俗来讲,配置测试环境就是搭建一个电力监控系统与待测试测态势感知系统组成的能够正常运行的系统,以能够测试待测试测态势感知系统的感知能力,其中,所说的感知能力用于描述待测试测态势感知系统对于其监控的电力监控系统的各设备发送的采集信息事件的接收及处理能力。

[0071] 具体来讲,对于步骤S101,要搭建一个正常运行的系统,需要模拟电力监控系统中的至少一个网络安全监测设备和主站服务器,并且建立网络安全监测设备与待测态势感知系统之间的第一通讯链路,以及主站服务器与所述待测态势感知系统之间的第二通讯链路。

[0072] 在一些实施例中,对于步骤S101中的所述模拟至少一个网络安全监测设备,包括:

[0073] 配置至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备,其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;

[0074] 对于步骤S101中的模拟主站服务器包括:配置第二基本信息,基于所述第二基本信息生成所述主站服务器,其中,所述第二基本信息包括第一通讯地址和第一端口编号;

[0075] 其中,所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0076] 需要说明的是,所述网络安全监测设备为电力监控系统中的各电子设备,比如,一般常见有通用主机包含服务器、工作站;嵌入式主机包含嵌入式装置;网络设备包含交换机、路由器;安全设备包含防火墙、纵向加密认证装置、正向隔离装置、反向隔离装置、态势感知采集装置等设备。第一基本信息是模拟一个能够正常运行的网络安全监测设备所需要的数据,至少包括设备名称、互联网协议IP地址以及媒体存取控制MAC地址,还可以包括更多的数据,比如,测试用户名、生产厂家名称等等,具体来讲,第一基本信息包含的数据越多,模拟的网络安全监测设备越符合真实使用的电力监控系统中的设备。

[0077] 这里所说的基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备是指基于每一个第一基本信息均可以生成一个与第一

基本信息匹配的网络安全监测设备，换句话说，第一基本信息与模拟的网络安全监测设备是一一对应的。

[0078] 在实际应用过程中，模拟的主站服务器可以是一个基于IEC-104的传输控制协议(TCP，Transmission Control Protocol)服务器。在进行模拟时，第二基本信息可以包括第一通讯地址和第一端口编号，也就是说，有一个通讯地址、一个端口编号就可以模拟出一个主站服务器了。需要说明的是，设定规范可以是指电力监控系统网络安全监测装置技术规范，此技术规范中规定了解析规则等。

[0079] 在一些实施例中，对于步骤S101中的所述建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路，包括：向所述至少一个网络安全监测设备中的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号，以使所述至少一个网络安全监测设备中的每个网络安全监测设备基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路；

[0080] 以及对于步骤S101中的建立所述主站服务器与所述待测态势感知系统之间的第二通讯链路，包括：向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号，以使所述待测态势感知系统基于所述第一通讯地址和第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0081] 需要说明的是，第一通讯链路是网络安全监测设备与待测态势感知系统之间传输数据的通路，其根据网络安全监测设备遵循的传输协议不同而不同，比如，当网络安全监测设备遵循TCP，则建立的第一通讯链路则是按照TCP传输数据的通路；再如，若网络安全监测设备遵循用户数据包协议(UDP，User Datagram Protocol)，则建立的第一通讯链路则是按照UDP输数据的通路。不论是基于TCP还是基于UDP建立第一通讯链路，其具体建立通讯链路的过程可参考现有技术，在此不再赘述。第二通讯链路是主站服务器与所述待测态势感知系统之间的传输通路，在主站服务器遵循TCP时，按照TCP建立第二通讯链路，具体建立过程在此也不再赘述。

[0082] 在实际应用过程中，在将测试环境配置完成后，就可以开始正常的测试工过程，也即：S102和S103步骤所完成的操作。

[0083] 在一些实施例中，对于S102，可以包括：

[0084] 向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令；所述采集信息指令用于指示所述网络安全监测设备生成与所述采集信息指令对应的采集信息事件并通过所述第一通讯链路向所述待测态势感知系统发送所述与采集信息指令对应的采集信息事件；其中，所述至少一条采集信息指令是基于配置的采集信息项列表生成；所述采集信息项列表包括用于生成每条采集信息指令的各配置参数；

[0085] 对应的，所述控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件，包括：

[0086] 控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送每一个与所述采集信息事件对应的网络安全事件。

[0087] 需要说明的是，采集信息项列表包括用于生成每条采集信息指令的各配置参数，比如，网络安全监测设备的名称、类型、IP、运行参数、运行次数等等。采集信息项列表可以

是一个可扩展标记语言(XML,eXtensible Markup Language)格式文档,其可以由测试人员进行任意配置。

[0088] 应该理解的是,此处所说的任意配置也不是说是没有界限的,换句话说,若测试人员配置一些参数生成的采集信息指令,网络安全监测设备基于这些采集信息指令不能模拟出与采集信息指令对应的采集信息事件时,这样测试肯定失败,这样的配置就是无意义的。因此,在一些实施例中,所述方法还包括:

[0089] 为每一个网络安全监测设备加载与网络安全监测设备对应的采集信息列表;所述采集信息列表为按照设定的态势感知技术规范设置的需要采集网络安全监测设备的各数据所形成。

[0090] 需要说明的是,设定的态势感知技术规范可以是指基于电力监控系统网络安全监测装置技术规范制定的态势感知系统的工作规范,比如规定了采集网络安全监测设备的信息的种类、对采集的信息的处理方式等;与网络安全监测设备对应的采集信息列表中包含的各数据所形成是网络安全监测设备可以完成的一些操作以及一些设备本身所具有的属性,其可以包括采集信息以及信息产生方式,其中,采集信息包含操作信息、配置信息、状态信息、告警信息;信息产生方式包含触发上送或者周期上送。采集信息列表可以采用二进制格式的文件来存储的,可以动态、快捷的修改采集信息列表中的内容,提高了可操作性。采集信息项列表就是根据采集信息列表进行配置的,以保证基于采集信息项列表生成的采集信息指令,能够使网络安全监测设备生成与所述采集信息指令对应的采集信息事件,从而排除因人为配置原因导致的测试失败。

[0091] 这里所说的向每个网络安全监测设备发送至少一条采集信息指令可以是指向一个网络安全监测设备可以发送多条采集信息指令。网络安全监测设备在接收到采集信息指令后,基于采集信息指令的指示生成相应的采集信息事件。所说的采集信息事件可以是指网络安全监测设备完成的某一操作,比如,当采集信息指令为指示网络安全监测设备完成完成登陆成功这一操作,那么网络安全监测设备基于该采集指令完成了登陆成功这一操作后,生成一个登陆成功事件,该登陆成功事件就为采集信息事件。

[0092] 在实际应用过程中,对于S103来讲,所说的对应的超时等待时间可以是在控制网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件后,设定接收到与采集信息事件对应的反馈信息的最大等待时间,比如,所述超时等待时间设置可以为3秒、5秒等。具体来讲,此时在控制网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件后,等待接收到与采集信息事件对应的反馈信息的最大等待时间为3秒,换句话说,若能接收到与采集信息事件对应的反馈信息,接收时间一定在在3秒内;若在3秒内未接收到接收到与采集信息事件对应的反馈信息时,不会再等待接收与采集信息事件对应的反馈信息。

[0093] 在一些实施例中,对于S103中的所述基于每一个判断结果生成所述待测态势感知系统的测试报告,包括:

[0094] 记录与每一个判断结果对应的测试结果;

[0095] 基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;

[0096] 其中，在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息，所述测试结果为通过；在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息，所述测试结果为未通过。

[0097] 需要说明的是，这里所说的判断结果包括在对应的超时等待时间内接收到采集信息事件对应的反馈信息，以及在对应的超时等待时间内未接收到采集信息事件对应的反馈信息两种。在这两种判断结果中，在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息，所述测试结果为通过，也即，测试成功；在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息，所述测试结果为未通过，也即，测试失败。这里，将每个测试结果均记录下来，形成一个可读文档，以供测试人员可以很清晰的了解哪个测试有问题，其中，可读文档可以是word、PDF等格式。

[0098] 在一些实施例中，所述方法还包括：

[0099] 采用同一标识显示所述测试报告中的相同的测试结果，以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0100] 需要说明的是，标识可以是任何形式，比如，测试结果为通过时，绿色灯亮；测试结果为未通过时，红色灯亮，这样，测试人员可以很清晰的了解哪个测试项有问题，可以快速定位和排查问题，缩短了故障排查的时间。

[0101] 在一些实施例中，所述方法还包括：

[0102] 记录基于所述采集信息项列表生成的每一条采集信息指令、每一个网络安全监测设备基于每一条采集信息指令生成的每一个采集信息事件，以及所述待测态势感知系统基于每一个采集信息事件生成的每一个网络安全事件；

[0103] 将每一条记录添加到所述测试报告中的相应位置；其中，所述相应位置是指能够使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系的记录位置。

[0104] 需要说明的是，这里是将所有与测试内容相关的均被记入测试报告中，并且按照网络安全监测设备进行分类，使得采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系，以便测试人员很清晰的了解哪个测试环节有问题，以快速定位和排查问题，缩短了故障排查的时间，并且整个记录过程全部自动化，大大节省了测试时间。

[0105] 前述是本发明的测试方法的构思，那么，在实际实现前述的测试方法的过程中，如图2所示，本发明实施例还提供一种测试系统，该测试系统20包括：包括测试控制模组201、监测对象模拟模组202和主站模拟模组203，其中，

[0106] 所述测试控制模组201，用于配置测试环境，其中，所述配置测试环境包括：通过所述监测对象模拟模组202模拟至少一个网络安全监测设备和通过所述主站模拟模组203模拟主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路；控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件；所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采

集信息事件获得;判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

[0107] 需要说明的是,这里出现的与前述相同的名词,其含义相同,在前述已经详细描述,在此不再赘述。测试控制模组201是这个测试系统的核心,所有的控制命令以及配置均是通过测试控制模组201实现,在实际应用中,测试人员可以通过设置在测试控制模组201上的人机交互界面,实现测试控制命令的发送和配置的操作等。

[0108] 在一些实施例中,所述测试控制模组201,具体用于:配置至少一个第一基本信息,向所述监测对象模拟模组202发送所述至少一个第一基本信息;以及配置第二基本信息,向所述主站模拟模组203发送所述第二基本信息;

[0109] 所述监测对象模拟模组202,用于接收所述测试控制模组201发送的所述至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备;

[0110] 所述主站模拟模组203,用于接收所述测试控制模组201发送的第二基本信息,基于所述第二基本信息生成所述主站服务器;

[0111] 其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;所述第二基本信息包括第一通讯地址和第一端口编号;所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0112] 在一些实施例中,所述测试控制模组201,还用于:向所述监测对象模拟模组202模拟的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号;以及向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号;

[0113] 所述监测对象模拟模组模拟的每个网络安全监测设备,用于接收所述第二通讯地址和所述第二端口编号,并基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路;

[0114] 所述待测态势感知系统,用于接收所述第一通讯地址和所述第二端口编号,并基于所述第一通讯地址和所述第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0115] 在一些实施例中,所述测试控制模组201,还用于:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令;

[0116] 所述监测对象模拟模组模拟的每个网络安全监测设备,用于接收所述至少一条采集信息指令,并基于每一条采集信息指令生成与采集信息指令对应的采集信息事件,通过所述第一通讯链路向所述待测态势感知系统发送所述采集信息事件;

[0117] 所述待测态势感知系统,用于接收所述采集信息事件,并将所述采集信息事件转换成网络安全事件,通过所述第二通讯链路向所述主站服务器发送所述网络安全事件;

[0118] 所述主站服务器,用于接收所述网络安全事件,按照设定规范解析所述网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0119] 需要说明的是,这里出现的与前述测试方法中相同的名词其含义相同,在前述已经详细描述,在此不再赘述。

[0120] 在一些实施例中,所述测试控制模组201,还用于:记录与每一个判断结果对应的测试结果;基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;其中,在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息,所述测试结果为通过;在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息,所述测试结果为未通过。

[0121] 在一些实施例中,所述测试系统还包括显示模组,用于采用同一标识显示所述测试报告中的相同的测试结果,以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0122] 需要说明的是,显示模组可以是任何形式的显示元件,比如,映像管(CTR,Cathode Ray Tube)显示器、液晶显示器(LCD,Liquid Crystal Display)、LED显示器等,其形式可以根据实际需要进行选择。

[0123] 在一些实施例中,所述测试控制模组、所述监测对象模拟模组和所述主站模拟模组设置在同一台计算机。

[0124] 需要说明的是,所述测试控制模组、所述监测对象模拟模组和所述主站模拟模组可以设置在同一计算机(PC)上,并且与待测态势感知系统连接到同一交换机上,因所述测试控制模组、所述监测对象模拟模组和所述主站模拟模组是集成在同一个测试系统内,所以配置操作非常简单,也即,使得搭建测试环境的时间大大缩短,又节约了搭建测试环境的成本。

[0125] 为了理解本发明,基于前述的图2中的测试系统,以下采用实施例来说明本发明的测试方法的具体工作原理。

[0126] 以电力监控系统中包含两个网络安全监测设备,一个为名称为server1的服务器和另一个为名称为Fw1防火墙为例。其工作流程具体如下:

[0127] 1)配置测试环境

[0128] 首先,测试人员通过测试控制模组201上人机交互界面的输入元件分别配置server1的第一基本信息和Fw1的第一基本信息,并向监测对象模拟模组202发送server1的第一基本信息和Fw1的第一基本信息,以及配置第二基本信息,并向主站模拟模组203发送所述第二基本信息其中,所述输入元件可以按键、按钮、触摸按键等形式。

[0129] 这里,在监测对象模拟模组202接收到server1的第一基本信息和Fw1的第一基本信息后,分别基于server1的第一基本信息模拟出server1、基于Fw1的第一基本信息模拟出Fw1,以模拟的server1和Fw1组成电力监控系统,进而测试待测态势感知系统对于包含两个网络安全监测设备的电力监控系统的感知能力。需要说明的是,此方式因配置方便、灵活,可以根据电力监控系统实际要求模拟网络安全监测设备的数量,大大实现测试环境搭建的便捷性。在主站模拟模组203接收到第二基本信息,模拟出主站服务器。

[0130] 然后,测试人员通过人机交互界面的输入元件启动模拟的server1、Fw1以及主站服务器,也即:分别建立server1、Fw1与待测态势感知系统之间的第一通讯链路,以及建立主站服务器与所述待测态势感知系统之间的第二通讯链路,换句话说,这一步是使模拟的server1、Fw1、主站服务器以及待测态势感知系统形成一个正常运行的系统,以便进行测

试。

[0131] 2)测试

[0132] 首先,测试人员通过测试控制模组201上人机交互界面的输入元件配置采集信息项列表。基于前述的描述,采集信息项列表是基于模拟的各网络安全监测设备的采集信息列表配置的。

[0133] 举例来说,如表1所示的模拟的server1的部分采集信息列表;表2所示的模拟的Fw1的部分采集信息列表,以及基于表1和表2配置的采集信息项列表,如表3所示。

[0134] 表1

[0135]

登录成功	登录失败	退出登录
链路活跃信息	链路跳转信息	操作命令
操作回显	cpu 使用率	内存使用率
硬盘空间使用率	僵尸进程数量 超过阈值	TCP 链接 close_wait 数量超过阈值
开放非法端口	主板温度超过阈值	USB 设备 (非无线网卡)插入
USB 设备 (无线网卡)插入	禁止 USB 主机的 USB 插入	禁止 USB 主机的 USB 拔出
USB 设备拔出	串口占用	串口释放
并口占用	并口释放	光驱加载
异常网络访问	网口 DOWN	网口 UP
风扇故障	电源故障	用户权限变更

[0136] 表2

[0137]

用户登录成功	用户退出	用户登录失败
修改策略	CPU使用率	内存使用率
防火墙电源故障	防火墙风扇故障	防火墙温度异常
网络DOWN/UP	攻击告警	不符合安全策略的访问

[0138] 表3

[0139]

测试项	设备名称	设备类型	设备IP	运行参数	运行次数
登录成功	server1	服务器	198.120.0.100	user:admin	1
攻击告警	Fw1	防火墙	198.120.0.101	user:tester	5

[0140] 然后,测试人员点击测试控制模组201上人机交互界面的输入元件中的运行按钮,开启测试,测试控制模组201分别依次向模拟的server1、Fw1发送基于采集信息项列表生成的各采集信息指令,server1、Fw1在接收到相应的采集信息指令后各自生成与采集信息指令对应的采集信息事件,并将分别将各自的采集信息事件通过第一通讯链路向待测态势感知系统,待测态势感知系统生成与采集信息事件对应的网络安全事件,并向主站服务器发送网络安全事件,主站服务器接收网络安全事件,按照设定规范解析所述网络安全事件并

向测试控制模组201反馈解析结果;所述解析结果为所述反馈信息。若测试控制模组201在对应的超时等待时间内接收到该反馈信息,则该次测试成功;若测试控制模组201在对应的超时等待时间内未接收到该反馈信息,则该次测试失败。

[0141] 举例来说,测试控制模组201向server1发送了一条要server1模拟登陆成功的采集信息指令,server1接收到该指令后,生成登录成功采集信息事件,并上送给待测态势感知系统,待测态势感知系统接收到该登录成功采集信息事件后,基于该登录成功采集信息事件生成登录成功网络安全事件并上送给主站服务器,主站服务器接收到该登录成功网络安全事件按照设定规范进行解析获得解析结果并将所述解析结果反馈给测试控制模组201,以此形成完整的闭环测试。若测试控制模组201在对应的超时等待时间内接收到该解析结果,则表示该次测试成功,也即:测试结果可以记为通过;若测试控制模组201在对应的超时等待时间内未接收到该解析结果,则表示该次测试不成功,也即:测试结果可以记为不通过。

[0142] 3)生成测试报告

[0143] 基于与每一个采集信息事件对应的测试结果生成测试报告,如前述的该测试报告也可以包括所有与测试相关的内容,比如,采集信息指令、网络安全监测设备、采集信息事件、网络安全事件等等。并且将这些与测试相关的内容按照网络安全监测设备添加到所述测试报告中的相应位置,以使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系,从而便于测试人员快速排查问题所在。

[0144] 基于与前述的相同的发明构思,如图3所示,本发明实施例还提供一种测试装置,该测试装置30包括:配置单元301、控制单元302和判断单元303,其中,

[0145] 所述配置单元301,用于配置测试环境,其中,所述配置测试环境包括:模拟至少一个网络安全监测设备和主站服务器;建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路;

[0146] 所述控制单元302,用于控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件,以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件;所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得;

[0147] 所述判断单元303,用于判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息;基于每一个判断结果生成所述待测态势感知系统的测试报告;所述测试报告用于指明所述待测态势感知系统的感知能力。

[0148] 在一些实施例中,所述配置单元301,具体用于:配置至少一个第一基本信息,基于所述至少一个第一基本信息中的每个第一基本信息生成与第一基本信息匹配的网络安全监测设备,以及配置第二基本信息,基于所述第二基本信息生成所述主站服务器;其中,所述每个第一基本信息均至少包括:设备名称、互联网协议IP地址以及媒体存取控制MAC地址;所述第二基本信息包括第一通讯地址和第一端口编号;所述网络安全监测设备为电力监控系统中的各电子设备;所述主站服务器用于按照设定规范解析所述待测态势感知系统发送的每一个网络安全事件并反馈解析结果;所述解析结果为所述反馈信息。

[0149] 在一些实施例中,所述配置单元301,还具体用于:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送所述待测态势感知系统对应的第二通讯地址和第二端口编号,以使所述至少一个网络安全监测设备中的每个网络安全监测设备基于所述第二通讯地址和所述第二端口编号建立与所述待测态势感知系统之间的第一通讯链路;以及向所述待测态势感知系统发送所述主站服务器的第一通讯地址和第一端口编号,以使所述待测态势感知系统基于所述第一通讯地址和第一端口编号建立与所述主站服务器之间的所述第二通讯链路。

[0150] 在一些实施例中,所述控制单元302,具体用于:向所述至少一个网络安全监测设备中的每个网络安全监测设备发送至少一条采集信息指令;所述采集信息指令用于指示所述网络安全监测设备生成与所述采集信息指令对应的采集信息事件并通过所述第一通讯链路向所述待测态势感知系统发送所述与采集信息指令对应的采集信息事件;其中,所述至少一条采集信息指令是基于配置的采集信息项列表生成;所述采集信息项列表包括用于生成每条采集信息指令的各配置参数;以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送每一个与所述采集信息事件对应的网络安全事件。

[0151] 在一些实施例中,所述判断单元303,具体用于:记录与每一个判断结果对应的测试结果;基于每一个对应的测试结果生成所述测试报告;所述测试报告以可读文档形式存储;其中,在所述判断结果为在对应的超时等待时间内接收到采集信息事件对应的反馈信息,所述测试结果为通过;在所述判断结果为在对应的超时等待时间内未接收到采集信息事件对应的反馈信息,所述测试结果为未通过。

[0152] 在一些实施例中,所述测试装置还包括:加载单元,用于:为每一个网络安全监测设备加载与网络安全监测设备对应的采集信息列表;所述采集信息列表为按照设定的态势感知技术规范设置的需要采集网络安全监测设备的各数据所形成。

[0153] 在一些实施例中,所述测试装置还包括:显示单元,用于:采用同一标识显示所述测试报告中的相同的测试结果,以及采用不同标识显示所述测试报告中的不相同的测试结果。

[0154] 在一些实施例中,所述判断单元303,还具体用于:记录基于所述采集信息项列表生成的每一条采集信息指令、每一个网络安全监测设备基于每一条采集信息指令生成的每一个采集信息事件,以及所述待测态势感知系统基于每一个采集信息事件生成的每一个网络安全事件;将每一条记录添加到所述测试报告中的相应位置;其中,所述相应位置是指能够使采集信息指令、网络安全监测设备、采集信息事件、网络安全事件形成一一映射关系的记录位置。

[0155] 需要说明的是,上述各实施例所述的测试装置与前述的测试方法是同一发明构思,因此,上述各实施例所述的测试装置中出现的各名词的含义与前述相同,在此不再赘述。

[0156] 本发明实施例还提供一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序处理器被处理器执行时实现上述方法实施例的步骤,而前述的存储介质包括:移动存储设备、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0157] 本发明实施例还提供一种测试设备,包括:处理器和用于存储能够在处理器上运

行的计算机程序的存储器，其中，所述处理器用于运行所述计算机程序时，执行存储在存储器中的上述方法实施例的步骤。

[0158] 图4为本发明实施例测试设备的一种硬件结构示意图，该测试设备40包括：至少一个处理器401、存储器402，可选的，测试设备40还可进一步包括至少一个通信接口403，测试设备40中的各个组件通过总线系统404耦合在一起，可理解，总线系统404用于实现这些组件之间的连接通信。总线系统404除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图4中将各种总线都标为总线系统404。

[0159] 可以理解，存储器402可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(ROM，Read Only Memory)、可编程只读存储器(PROM，Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM，Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM，Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM，ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM，Compact Disc Read-Only Memory)；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM，Random Access Memory)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(SRAM，Static Random Access Memory)、同步静态随机存取存储器(SSRAM，Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM，Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM，Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM，Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM，SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM，Direct Rambus Random Access Memory)。本发明实施例描述的存储器402旨在包括但不限于这些和任意其它适合类型的存储器。

[0160] 本发明实施例中的存储器402用于存储各种类型的数据以支持测试设备40的操作。这些数据的示例包括：用于在测试设备40上操作的任何计算机程序，如控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件等，实现本发明实施例方法的程序可以包含在存储器402中。

[0161] 上述本发明实施例揭示的方法可以应用于处理器401中，或者由处理器401实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器(DSP，Digital Signal Processor)，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。处理器可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成前述方法的步骤。

[0162] 在示例性实施例中，测试设备40可以被一个或多个应用专用集成电路(ASIC，Application Specific Integrated Circuit)、DSP、可编程逻辑器件(PLD，Programmable Logic Device)、复杂可编程逻辑器件(CPLD，Complex Programmable Logic Device)、现场可编程门阵列(FPGA，Field-Programmable Gate Array)、通用处理器、控制器、微控制器(MCU，Micro Controller Unit)、微处理器(Microprocessor)、或其他电子元件实现，用于执行上述方法。

[0163] 在本发明所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元，即可以位于一个地方，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全部单元来实现本实施例方案的目的。另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0164] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

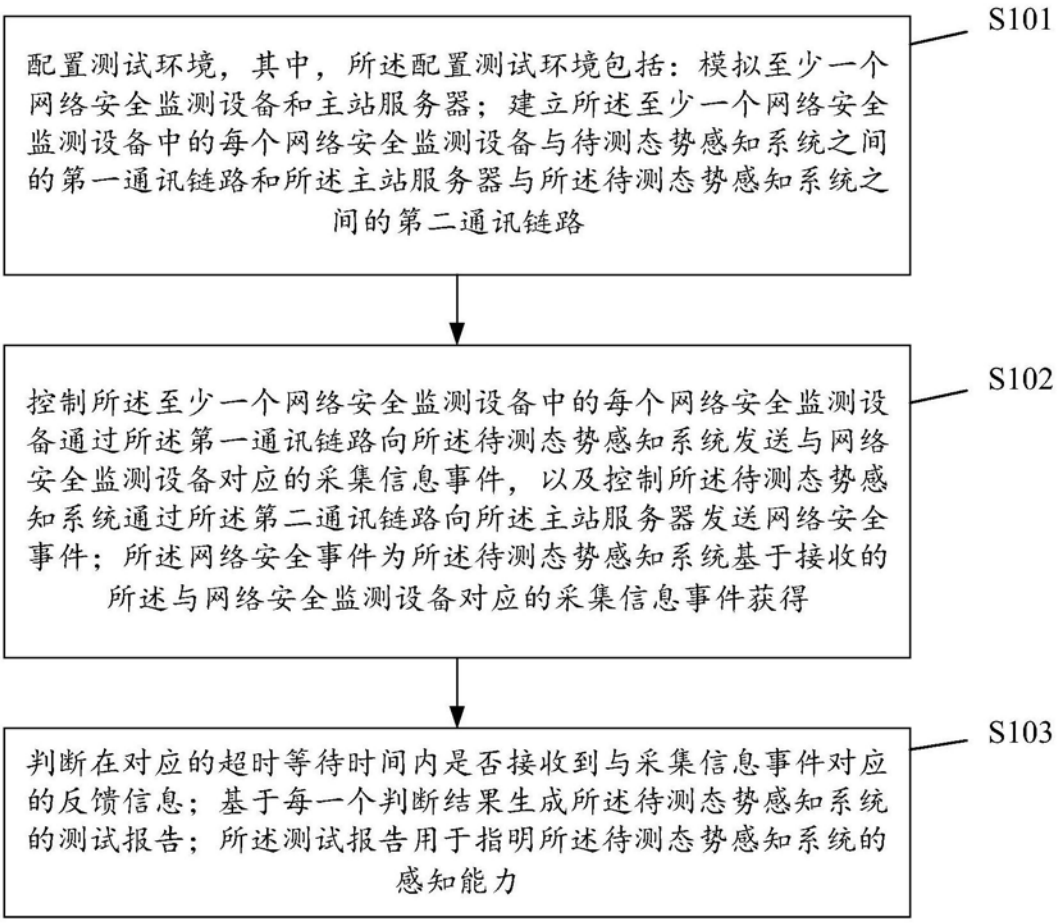

S101
配置测试环境，其中，所述配置测试环境包括：模拟至少一个网络安全监测设备和主站服务器；建立所述至少一个网络安全监测设备中的每个网络安全监测设备与待测态势感知系统之间的第一通讯链路和所述主站服务器与所述待测态势感知系统之间的第二通讯链路
S102
控制所述至少一个网络安全监测设备中的每个网络安全监测设备通过所述第一通讯链路向所述待测态势感知系统发送与网络安全监测设备对应的采集信息事件，以及控制所述待测态势感知系统通过所述第二通讯链路向所述主站服务器发送网络安全事件；所述网络安全事件为所述待测态势感知系统基于接收的所述与网络安全监测设备对应的采集信息事件获得
S103
判断在对应的超时等待时间内是否接收到与采集信息事件对应的反馈信息；基于每一个判断结果生成所述待测态势感知系统的测试报告；所述测试报告用于指明所述待测态势感知系统的感知能力

图1

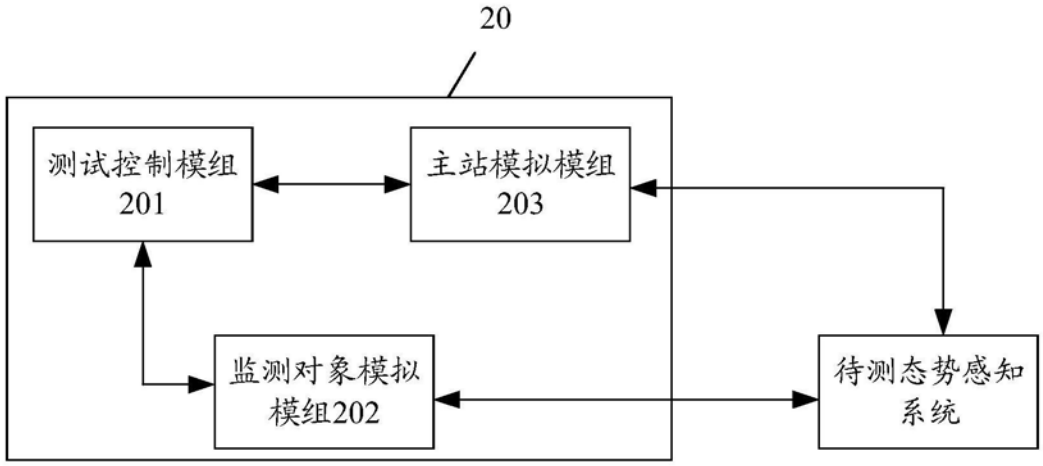

20
测试控制模组
201
主站模拟模组
203
监测对象模拟
模组202
待测态势感知
系统

图2

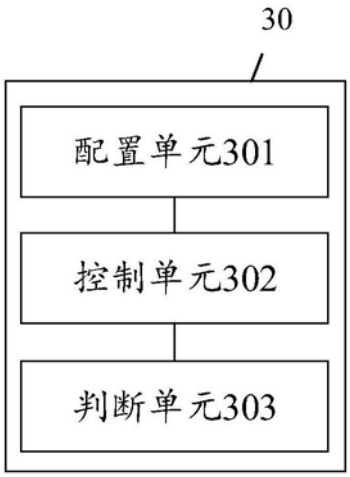


图3

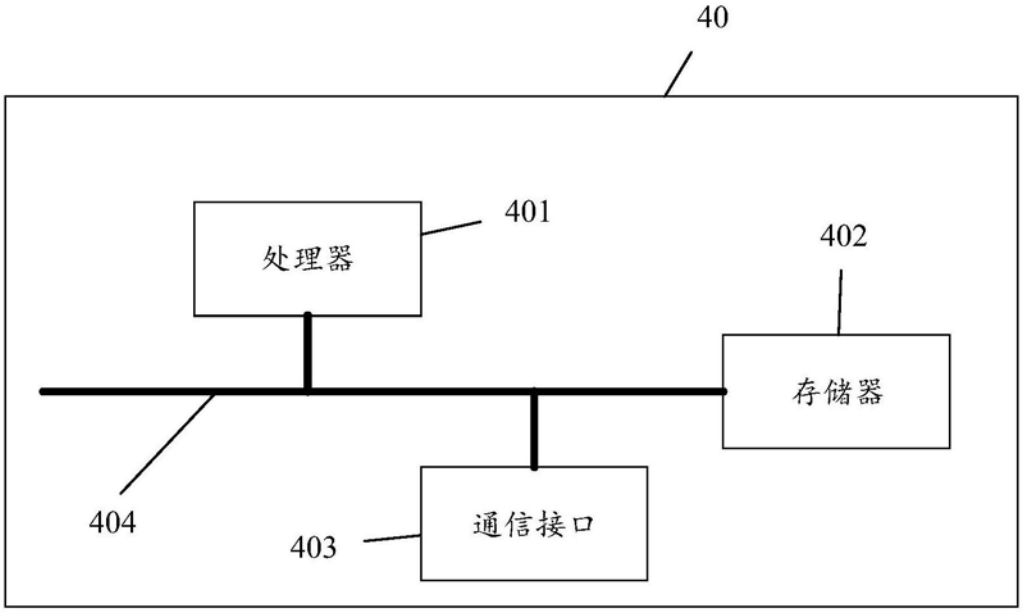


图4