附件 2

厂站端网络安全监测装置
接入与测试规范

河南电力调度控制中心

2019 年 2 月

目录

1　范围

本指南描述了电力监控系统网络安全监测装置（Ⅱ型）（以下简称监测装置）在厂站的部署原则、监测对象接入原则、职责分工、部署流程及各阶段要求等。

本指南适用于监测装置在厂站的现场部署、接入相应调控机构网络安全管理平台（以下简称平台）的调试及验收工作，适用厂站包括 500kV 及以下电压等级变电站和各类并网电厂。

2　装置监测对象接入原则

2.1 总体原则

1）生产控制大区内涉网区域的站控层主机设备、网络设备和安全防护设备（含生产控制大区边界的安全防护设备），均需接入网络安全监测装置。

2）对于因功能不支持而无法实现接入的各类在运设备，应结合技改或大修项目等方式实现设备更换接入。

3）涉网站控层各类设备相应要求如下：

主机设备：凡满足 AGENT 技术条件的主机设备，必须接入监测装置。AGENT 必须经过中国电科院检测，检测结果在中国电力科学研究院有限公司官网（http://www.epri.sgcc.com.cn/）“试验检测—电子公告”中；

网络设备：所涉网络设备及站控层交换机。设备需要满足 SNMP V2c 或 V3 协议，如果不满足，则需要进行版本升级或更换。对于满足 SNMP V2c 或 V3 协议的网络设备但不能完全满足《电力监控系统网络安全监测装置技术规范》时，需由网络设备厂商进行私有 MIB 的开发；

安全防护设备：设备日志应遵循《电力监控系统网络安全监测装置技术规范》，如遇安全防护设备自身日志协议程序版本过于老旧，需要统一由安全防护设备厂商提供满足《电力监控系统网络安全监测装置技术规范》安全防护设备的日志规范的插件。

4）各级厂站宜利用监测装置的本地图形化管理 UI 界面（现场监视功能），实现厂站内部网络安全的就地监视。

5）并网电厂在遵循变电站部署原则的基础上，还需遵循：

并网电厂应将涉网区域的主机设备、网络设备及安全防护设备接入并转发调控机构平台，设备定义即所有与调度数据网有直接或间接网络连接的设备，各类并网电厂涉网区域见 2.4 节；

并网电厂宜将厂站内可接入的主机设备、网络设备及安全防护设备均纳入监视范围，实现全厂就地监视。

2.2 装置监测范围

在变电站、并网电厂部署的监测装置应支持对主机设备（服务器、工作站及装置）、网络设备、安全防护设备等监测对象进行数据采集，此外监测装置还应支持资产配置以外的监

测对象的数据采集。具体如下：

2.2.1 主机设备安全事件采集

主机设备安全事件由可信计算安全模块和主机监测程序（以下简称“AGENT”）产生，并通过网络安全监测装置传输至网络安全管理平台。安全事件包括用户登录信息、操作行为信息、网络连接信息、系统配置信息、权限变更信息、硬件配置信息、硬件状态信息、系统运行信息、外设接入信息、平台核查指令信息。

2.2.2 网络设备安全事件采集

网络安全监测装置通过 SNMP、SNMP trap 和 GB/T 31992 协议实现网络设备安全事件感知，并传输至网络安全管理平台。网络设备安全事件包括：局域网内交换机设备、连接交换机的活跃设备等网络设备拓扑信息。在线时长、CPU 利用率、内存利用率、网口状态、网络连接情况等网络设备运行信息。设备接入、各硬件模块故障等安全事件信息。用户登录、用户退出、用户操作等行为信息。

2.2.3 安全防护设备安全事件采集

通用安全防护设备及电力专用安全防护设备由设备自身实现安全事件感知，并通过网络安全监测装置传输至网络安全管理平台。安全防护设备安全事件包括：设备自身策略的安全事件、配置信息及运行信息、操作信息。

2.3 变电站

根据各类变电站拓扑结构，分智能变电站、常规变电站两种。

2.3.1 智能变电站

智能站监控系统由站控层、间隔层、过程层设备，网络和安全防护设备组成，其中，站控层设备主要包括监控主机、数据通信网关机、数据服务器、综合应用服务器、五防主机、PMU 数据集中器和继电保护等。

智能变电站监控系统如图 1 所示：

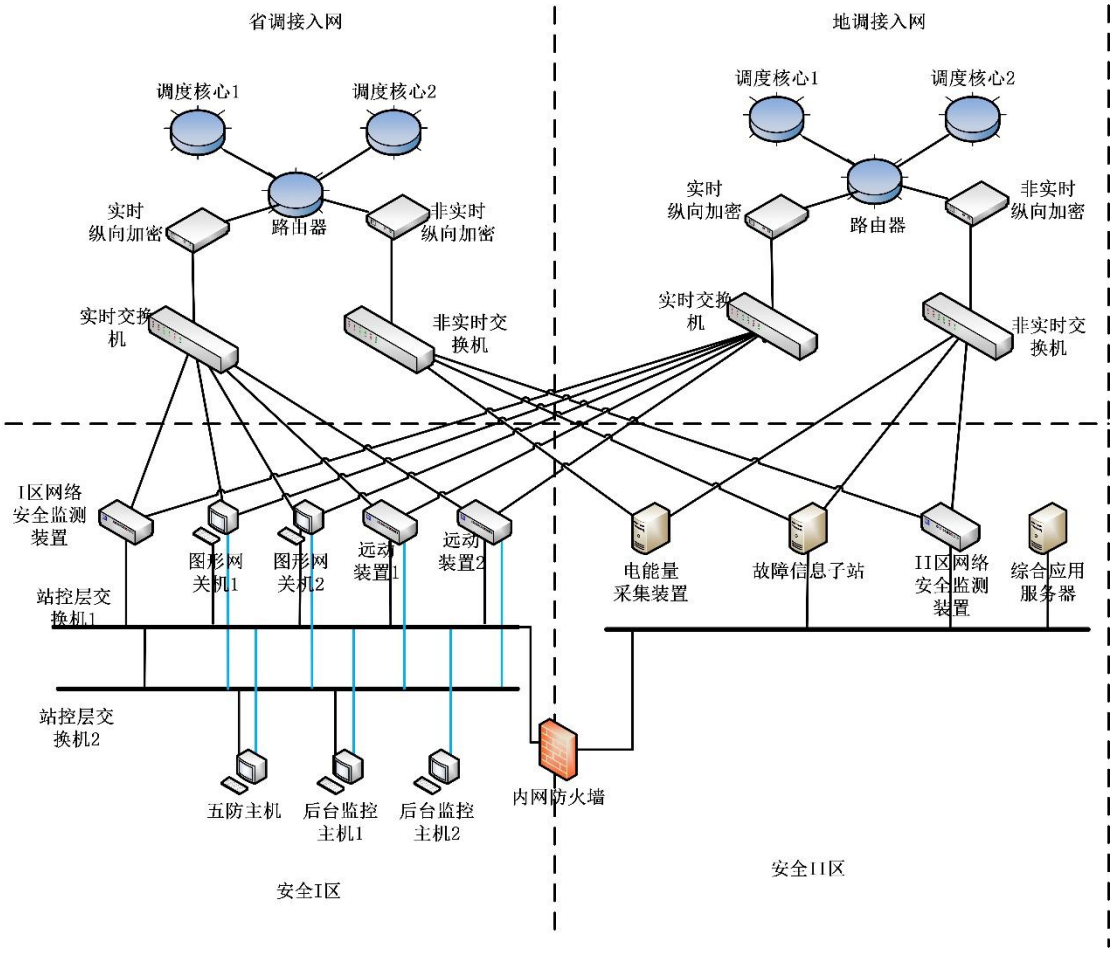

图1　智能变电站监控系统示意图

智能变电站典型监测对象如表 1：

表1 智能变电站典型监测对象表

对象名称	设备类型	备注
远动机	主机设备	包含装置类设备
监控主机	主机设备	
图形网关机	主机设备	
数据服务器	主机设备	
综合应用服务器	主机设备	
五防主机	主机设备	
PMU 数据集中器	主机设备	包含装置类设备
电能量采集装置	主机设备	包含装置类设备
故障录波	主机设备	包含装置类设备
保信子站	主机设备	
Ⅰ区站控层 A 网交换机	网络设备	
Ⅰ区站控层 B 网交换机	网络设备	
安全Ⅰ区与安全Ⅱ区防火墙	安全防护设备	
安全Ⅱ区与安全Ⅲ区正向隔离	安全防护设备	
安全Ⅱ区与安全Ⅲ区反向隔离	安全防护设备	

2.3.2 常规变电站

常规站监控系统站控层设备包括监控主机、数据网关机、五防主机、电量采集装置和继电保护等。

常规变电站监控系统如图 2 所示：

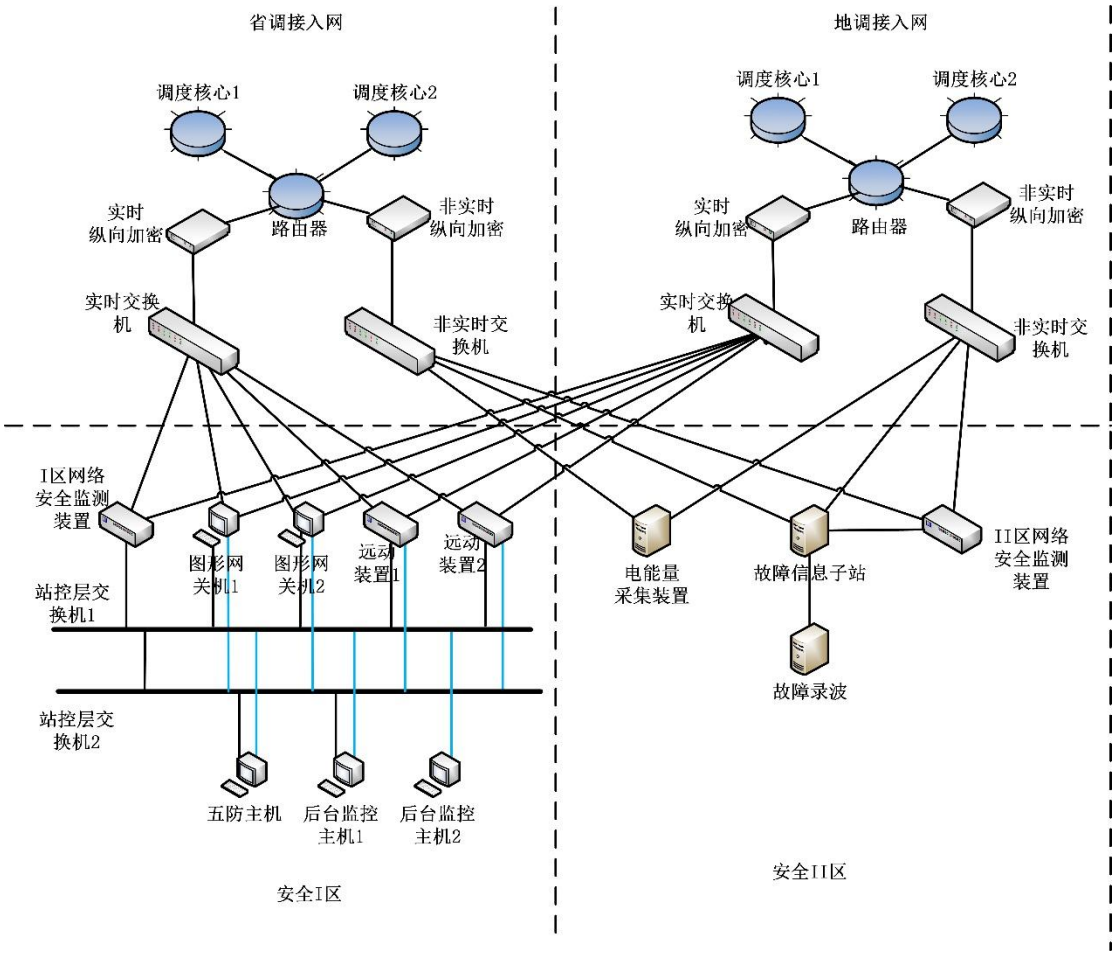

图2　常规变电站监控系统示意图

常规变电站典型监测对象如表 2：

表2 常规变电站典型监测对象表

对象名称	设备类型	备注
远动机	主机设备	包含装置类设备
监控主机	主机设备	
图形网关机	主机设备	
五防主机	主机设备	
PMU 数据集中器	主机设备	包含装置类设备
电能量采集装置	主机设备	包含装置类设备
故障录波	主机设备	包含装置类设备
保信子站	主机设备	
Ⅰ区站控层 A 网交换机	网络设备	
Ⅰ区站控层 B 网交换机	网络设备	

2.4 并网电厂

并网电厂可分为火电厂、水电厂、风电场、光伏电站等主要类型。根据国能安全〔2015〕36 号附件 4：《发电厂监控系统安全防护方案》，列举各类型电厂典型结构及典型监测对象，现场应根据实际情况判断具体监测对象。

原则上并网电厂涉网部分主机设备、网络设备及安全防护设备应接入监测装置并将相关告警信息上传至相关调控机构平台，其他非涉网部分也可接入监测装置，宜利用监测装置的本地图形化管理 UI 界面（现场监视功能），实现电厂内部网络安全的就地监视。

2.4.1 火电厂

火电厂电力监控系统主要包括：火电机组分散控制系统 DCS、电机组辅机控制系统、火电厂厂级信息监控系统、调速系统和自动发电控制功能 AGC、励磁系统和自动电压控制功能 AVC、网控系统、相量测量装置 PMU、自动控制装置、五防系统、继电保护、故障录波、电能量采集装置、电力市场报价终端、管理信息系统 MIS、报价辅助决策系统、检修管理系统、火灾报警系统等。其中，调速系统和自动发电控制功能 AGC、励磁系统和自动电压控制功能 AVC、相量测量装置 PMU、继电保护（管理子站）、故障录波、电能量采集装置、实时调度系统、火电厂监控系统 NCS，应纳入监测范围并将告警信息上传至相关调控机构平台；其余系统可接入装告知实现电厂内部网络安全的就地监视。

火电厂监控系统如图 3 所示：

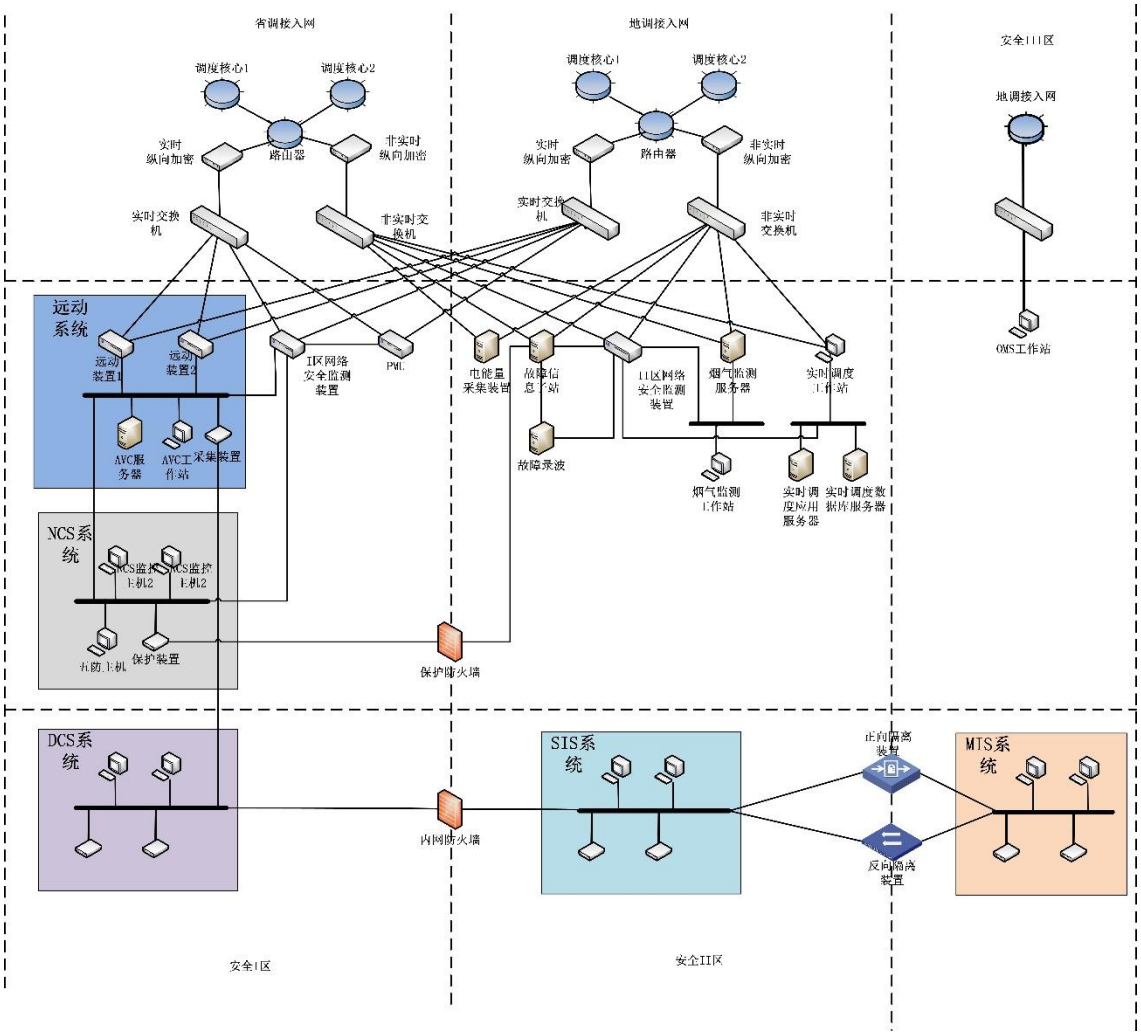

图3　火电厂监控系统示意图

火电厂典型监测对象如表 3：

表3 火电厂典型监测对象表

对象名称	设备类型	备注
远动机	主机设备	包含装置类设备
AVC/AGC 交换机	网络设备	
AVC/AGC 主机	主机设备	
PMU 交换机	网络设备	
PMU 主机	主机设备	包含装置类设备
A 网站控交换机	主机设备	
B 网站控交换机	主机设备	
NSC 监控主机	主机设备	
NSC 交换机	网络设备	
五防主机	主机设备	
烟气监测工作站	主机设备	包含装置类设备
烟气监测服务器	主机设备	包含装置类设备
烟气监测交换机	网络设备	
电能量采集装置	主机设备	包含装置类设备

实时调度数据库服务器	主机设备	
实时调度应用服务器	主机设备	
实时调度工作站	主机设备	
保信子站	主机设备	
保信服务器	主机设备	
故障录波	主机设备	包含装置类设备
保信防火墙	安全防护设备	

2.4.2 风电场

风电场电力监控系统包括：风电场监控系统、自动电压控制 AVC、自动发电控制 AGC、五防系统、继电保护、相量测量装置（PMU）、风功率预测系统、状态监测系统、电能量采集装置、故障录波、风机监控系统等。其中，风电场监控系统、风机监控系统、无功电压控制、发电功率控制、相量测量装置 PMU、继电保护（管理子站）、故障录波、电能量采集装置、风功率预测系统、状态监测系统属于涉网系统，应纳入监测范围并将告警信息上传至相关调控机构平台；其余系统可接入装告知实现电厂内部网络安全的就地监视。

风电场监控系统如图 4 所示：

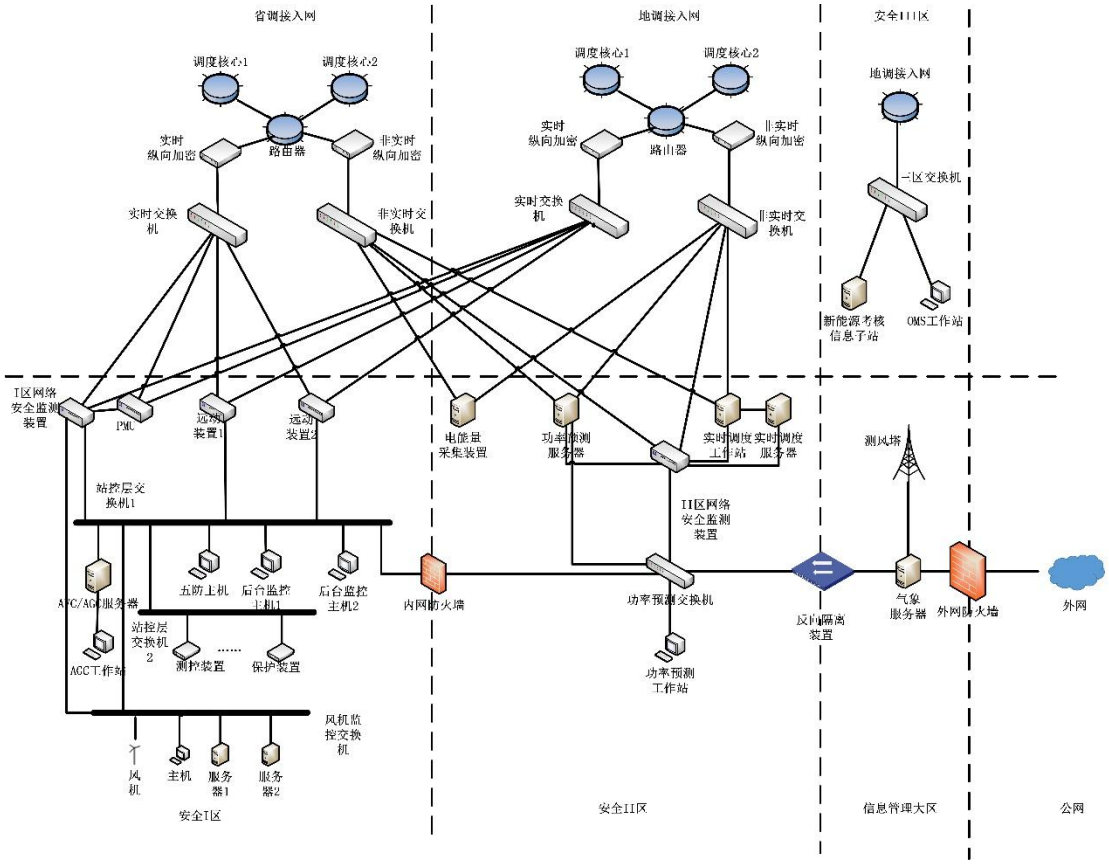

图4　风电场监控系统示意图

风电厂典型监测对象如表 4：

表4 风电厂典型监测对象表

对象名称	设备类型	备注
远动机	主机设备	包含装置类设备

监控主机	主机设备	
监控备机	主机设备	
五防主机	主机设备	
AVC/AGC 交换机	网络设备	
AVC/AGC 主机	主机设备	
PMU 交换机	网络设备	
PMU 主机	主机设备	包含装置类设备
A 网站控交换机	网络设备	
B 网站控交换机	网络设备	
风机监控交换机	网络设备	
风机监控前置服务器	主机设备	
风机监控数据库服务器	主机设备	
风机监控工作站 1	主机设备	
风机监控工作站 2	主机设备	
功率预测交换机	网络设备	
功率预测工作站	主机设备	
功率预测服务器	主机设备	
实时调度服务器	主机设备	
实时调度工作站	主机设备	
电能量采集装置	主机设备、网络设备	包含装置类设备
保信子站	主机设备	
保信服务器	主机设备	
故障录波	主机设备	包含装置类设备
II-III 反向隔离	安全防护设备	
I-II 区防火墙	安全防护设备	

2.4.3 光伏电站

光伏电站监控系统主要包括：光伏站运行监控系统和自动发电控制功能 AGC、自动电压控制功能 AVC、相量测量装置 PMU、五防系统、继电保护、故障录波、光伏功率预测系统、电能量采集装置、管理信息系统、雷电监测系统、气象信息系统、报价辅助决策系统、检修管理系统系统等。其中，自动发电控制功能 AGC、自动电压控制功能 AVC、光伏电站运行监控系统、相量测量装置 PMU、自动控制装置、继电保护（管理子站）、故障录波、电能量采集装置属于涉网系统，应纳入监测范围并将告警信息上传至相关调控机构平台；其余系统可接入装告知实现电厂内部网络安全的就地监视。

光伏电站监控系统如图 5 所示：

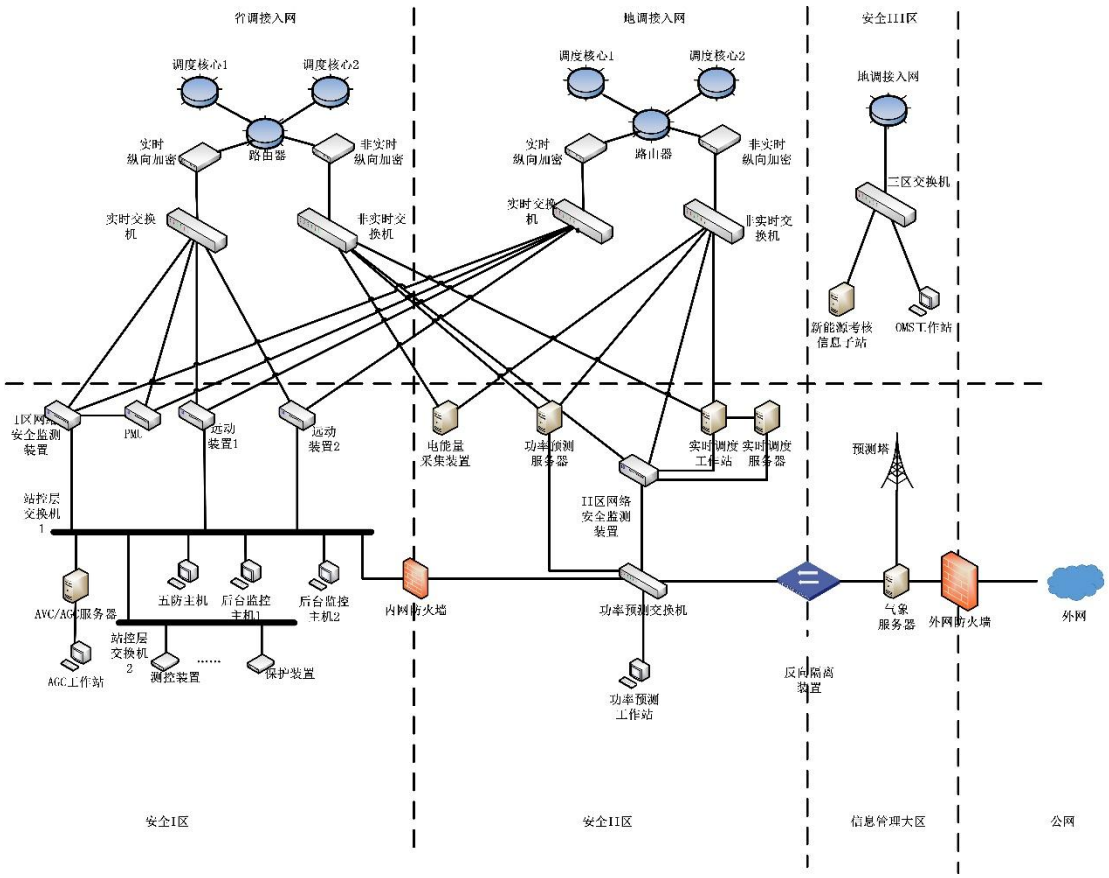

图5　光伏电站监控系统示意图

光伏电站典型监测对象如表 5：

表5 光伏电站典型监测对象表

对象名称	设备类型	备注
远动机	主机设备	包含装置类设备
监控主机	主机设备	
监控备机	主机设备	
五防主机	主机设备	
AVC/AGC 交换机	网络设备	
AVC/AGC 主机	主机设备	
PMU 交换机	网络设备	
PMU 主机	主机设备	包含装置类设备
A 网站控交换机	网络设备	
B 网站控交换机	网络设备	
功率预测交换机	网络设备	
功率预测工作站	主机设备	
功率预测服务器	主机设备	
实时调度服务器	主机设备	
实时调度工作站	主机设备	
电能量采集装置	主机设备、网络设备	包含装置类设备
保信子站	主机设备	
保信服务器	主机设备	

故障录波	主机设备	包含装置类设备
II-III 反向隔离	安全防护设备	
I-II 区防火墙	安全防护设备	

3 职责分工及工作流程

3.1 职责分工

监测装置部署工作一般涉及调控机构、厂站运维检修部门、项目集成厂商等单位，各单位具体职责分工如下：

3.1.1 调控机构

a）负责提供调度主站和监测装置的 IP 地址，以及安全的签名数字证书文件；
b）负责调度主站与厂站两侧纵向加密设备的隧道建立和策略配置；
c）配合项目集成厂商进行平台与监测装置调试及数据上传功能验证；
d）配合开展项目材料附件收集存档；
e）负责监测装置相关信息的云平台录入工作。

3.1.2 厂站运维检修部门

a）负责落实现场施工的各项安全措施；
b）负责监测装置调试结果确认并存档。

3.1.3 项目集成厂商

a）负责开展前期现场设备调研，绘制监测装置部署拓扑图与统计厂站所有设备清单；
b）负责网络安全监测装置的硬件安装、软件调试，以及与调控机构网络安全管理平台的联调；
c） 负责提供、安装和调试监测对象接入监测装置所需且通过中国电科院检测的 AGENT；
d）负责完成设备接入、功能测试、告警消除等工作；
e）负责确保相关监测对象接入监测前后该设备正常运行，并提供必要的技术支持。

3.2 工作流程

厂站网络安全监测装置部署工作大致可分为装置部署准备、装置单体调试、监测对象接入调试、平台接入调试和功能验证五个主要阶段，各阶段包含的具体工作如下：

a）装置部署准备

该阶段主要由项目集成厂商开展现场调研统计相关设备详细信息，协同厂站运维检修部门分析项目实施过程的各类风险点并制定应对措施，联系调控机构进行 IP 地址分配，并编

制项目实施方案。

b）装置单体调试

该阶段主要由项目集成厂商开展装置的上架安装、布线、上电检查和参数配置等工作。

c）监测对象接入调试

该阶段主要由项目集成厂商开展厂站内主机、网络和安全防护等站控层设备的接入装置工作和相应的功能测试。

d）平台接入调试

该阶段主要由项目集成厂商开展和调控机构开展监测装置与调度主站网络安全管理平台的联调测试。

e）功能验证

该阶段主要由项目集成厂商配合调控机构开展主站功能检查和材料收集等工作。

4 装置部署准备

4.1 现场调研

监测装置调试前，应由项目集成厂商配合厂站运维检修部门对现场情况进行详细调研，调研内容包括但不限于以下 3 个方面：

4.1.1 网络拓扑

a）现场调研时，应详细调研厂站监控系统现有网络拓扑，拓扑图上应包含主机设备、网络设备、安全防护设备及其他支持接入的监测对象；

b）对于新投运并网电厂，应将监测装置纳入发电厂安全防护方案中上报相应调控机构审核；对于在运并网电厂，应在现有网络拓扑图基础上，重新绘制监测装置部署后的网络拓扑图，并将更新发电厂安全防护方案报送至相应调控机构。

4.1.2 安装位置

a）监测装置机箱尺寸符合 GB/T19520.12 的规定，采用 1U 整层机箱，宜安装于调度数据网屏柜，可根据现场实际条件选择安装屏柜；

b）对于并网电厂，还应勘察不同监测对象至监测装置的布线距离，如超过 100 米必须部署光电转换器。

4.1.3 监测对象

a）主机设备

统计厂站主机（监控后台主机、图形网关机、综合应用服务器、五防主机、故障录波、保信子站等）的设备数量、操作系统发行版及版本号、位数及硬件架构、所在安全分区、IP 地址和是否能够部署 AGENT。

b）网络设备

统计厂站交换机所在安全分区、交换机名称、厂商及设备型号、设备数量、是否支持 SNMP 协议 V2 以上版本、是否支持固件升级。

c）安全防护设备

统计厂站防火墙、横向隔离装置等安全防护设备名称、所在安全分区、厂商及设备型号、设备数量、是否满足《电力监控系统网络安全监测装置技术规范》中安全防护设备日志规范。

4.2 IP 地址分配

a）调控机构分配监测装置的调度数据网业务 IP 地址，并指定装置证书名称、装置网络及路由配置、主站平台骨干网业务 IP 地址等；

b）厂站运维检修部门根据现场调研情况合理分配监测装置的内网 IP 地址。

4.3 设备清单

a）在汇总现场调研搜集资料的基础上，由项目集成厂商编制《电力监控系统厂站网络安全监测装置设备清单》（附表 1），上报相应调控机构、厂站运维检修部门审核，调控机构审核通过后再与现场做接入调试；

b）提前做好危险源分析，提出安全措施，参考如表 6。

表6 安全措施表

序号	安全措施
1	设备、线缆应有清晰准确的标识，所有进出管孔应用防火材料严密封闭。
2	电力监控系统上工作应使用专用的调试计算机及移动存储介质，调试计算机严禁接入外网。
3	禁止在电力监控系统中安装未经安全认证的软件。
4	禁止在电力监控系统运行环境中进行新设备研发及测试工作。
5	电力监控系统投运前，应删除临时帐号、临时数据，并修改系统默认帐号和默认口令。
6	在电力监控系统上进行板件更换、软件升级、配置修改等工作前，应核对型号、规格及软件版本信息等。
7	需停电检修的电力监控设备，应将设备退出运行、断开外部电源连接、断开网络连接，并做好防静电措施。
8	更换电力监控设备的热插拔部件、内部板卡等配件时，应做好防静电措施。
9	工作过程中需对设备部分参数进行临时修改，应做好修改前后相应记录，工作结束前应恢复被临时修改的参数。
10	电力监控系统的配置文件、业务数据等应定期备份，备份的数据宜定期进行验证。
11	业务数据的导入导出应经业务主管部门（归口管理部门）批准，导出后的数据应妥善保管。
12	电力监控系统帐号的密码应满足口令强度要求。
13	网络与安全设备停运、断网、重启操作前，应确认该设备所承载的业务可停用或已转移。
14	网络与安全设备配置变更工作前，应备份设备配置参数。更改配置时，存在冗余

	设备的，应先在备用设备上修改和调试，经测试无误后，再在其他设备上修改和调试，并核对主备机参数的一致性。工作结束前，应验证网络与安全设备上承载业务运行正常。
15	在安全设备进行工作时，严禁绕过安全设备将两侧网络直连。
16	网络和安防设备配置协议及策略应遵循最小化原则。
17	在主机与存储设备工作前，应备份设备的业务系统软件、业务数据、配置参数等。
18	升级操作系统版本前，应确认其兼容性及对业务系统的影响。
19	主机更换硬件、升级软件、变更配置文件时，存在冗余设备的，应先在备用设备上修改和调试，经测试无误后，再在其他设备上修改和调试，并核对主备机参数的一致性。工作结束前，应验证主机设备上承载的业务系统运行正常。
20	通过控制台或远程终端进行作业时，应输入帐号和密码，禁止使用互信登录、保存密码等方式免密登录。
21	业务系统升级或配置更改前，宜进行功能、性能、安全、兼容等方面的测试及验证。
22	业务系统升级或配置更改前，应备份业务系统软件和配置文件。
23	业务系统升级或配置更改后，应验证业务系统运行正常，方可投入运行。
24	通信网关机更换硬件、升级软件、变更信息点表及配置文件时，应对原软件版本、配置文件及参数、信息点表进行备份。更新完成，检查无误后应重新备份并记录变更信息。
25	通信网关机的通信规约、信息点表、配置文件等升级或变更时，应先在备用设备上修改和调试，经测试无误后，再在另一设备上修改和调试，并核对主备机参数的一致性。
26	工作结束前，应与相关调控机构核对业务正常。

4.4 云平台资料录入

调控机构将待部署的监测装置资料录入云平台，设备属性包含设备名称、所属厂站、运行状态、投运日期等，其中运行状态为“规划”。

5 装置单体调试

5.1 装置上架安装

a）监测装置外壳接地采用黄绿相间多股软铜线，横截面积不小于 2.5㎜²，接入安装所在屏内的接地铜排，满足相关设备接地要求。

b）监测装置应接入直流或交流不同源的双路电源独立供电；

c）现场 PDU 接口不足时可增加 PDU 进行扩充。直流电源电压可支持 110V、220V；交流电源电压 220V。

5.2 装置上电检查

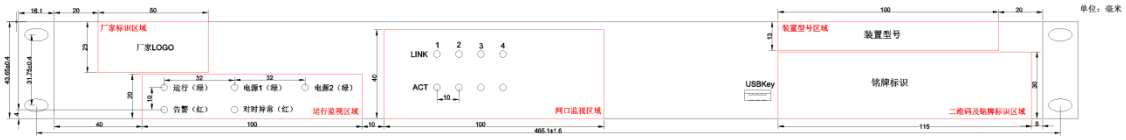

图6　装置前面板示意图

a）接通电源，检查电源是否全部运行正常；

b）监测装置应具备 5 个运行指示灯和若干通道监视灯，运行指示灯定义如表 7。

表7 装置运行指示灯定义表

序号	名称	定义	颜色
1	运行	装置上电后该灯为常亮状态，装置由于硬件或是软件出现异常时导致装置不能工作或部分功能缺失时，处于常灭状态。	绿灯
2	电源 1	装置电源 1 上电后点亮，失电后熄灭。	绿灯
3	电源 2	装置电源 2 上电后点亮，失电后熄灭。	绿灯
4	告警	装置由于硬件、软件或是配置出现异常时会处于常亮状态，正常运行时处于常灭状态，其中通信中断及对时异常时不亮告警灯。	红灯
5	对时异常	对时服务状态异常时会处于常亮状态，对时正常时处于常灭状态。	红灯

5.3 装置网口规划及相关网线敷设

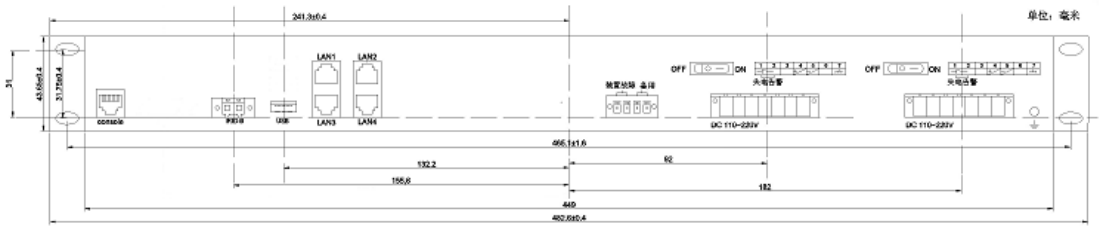

图7　装置后面板示意图

a）现场根据实际业务需要进行网线敷设，其中安全Ⅰ、Ⅱ区网线宜分别用两种颜色予以区分

b）根据技术规范，监测装置后面板有 4 个网口，网口规划参考如表 8。

表8 装置网口规划表

起点	终点
第 1 口（LAN1）	至第一套数据网（如 220 千伏变电站省调接入网）交换机
第 2 口（LAN2）	至第二套数据网（如 220 千伏变电站地调接入网）交换机
第 3 口（LAN3）	至监控系统（Ⅰ或Ⅱ区）A 网主交换机
第 4 口（LAN4）	至监控系统（Ⅰ或Ⅱ区）B 网主交换机或就地监视终端

其中，至数据网交换机及监控系统交换机上联端口各单位自定，禁止监测装置跨接安全区接入。

当现场装置超过 4 个网口，即为 8 个网口时，就地监视终端接在第 8 口（LAN8），其余监测对象依次接在第 5 口（LAN5）至第 7 口（LAN7）。

5.4 装置对时接入

a）监测装置宜同时接入 IRIG-B 码和 NTP 协议对时，其中 IRIG-B 码和 NTP 协议对时源均应为厂站时钟同步装置；

b）根据技术规范，监测装置对时源优先选择 IRIG-B 码对时设备，其次选择 NTP 协议对时；

c）配置 IRIG-B 码对时，应从 IRIG-B 码对时设备引出对时线，接入监测装置的 IRIG-B 码对时模块；

d）配置 NTP 对时，需要在监测装置内配置主时钟主网 IP 地址、主时钟备网 IP 地址、备时钟主网 IP 地址、备时钟备网 IP 地址、NTP 端口号、对时周期以及对时方式，监测装置宜选择站内时间同步装置的 NTP 对时服务。

5.5 软件版本校验

装置开始配置之前，应采用版本校验工具对监测装置的软件版本与通过电科院检测的软件版本进行一致性校验，版本校验工具由“软件版本采集程序”和“软件版本校验工具”组成：

a）“软件版本采集程序”需部署于监测装置内部，完成信息收集和通信；

b）“软件版本校验工具”需部署于专用调试计算机内部，按需校验的装置配置相关参数后，实现对监测装置软件版本的在线收集；

c）校验监测装置文件后，软件版本校验工具会展示各文件的版本一致性校验结果及总体校验结果，应确保结果为“通过”。

5.6 监测装置典型参数配置

a）监测装置参数配置项包括系统参数、通信参数及事件处理参数等；

b）各参数配置和典型参数配置如下：

网卡参数配置：即配置各网口对应的以太网 IP 地址及子网掩码；

路由参数配置：即配置各网口对应的路由目的网段、目的掩码及网关地址，注意应配置精确路由；

NTP 典型参数配置见表 9；

通信典型参数配置见表 10；

事件处理典型参数配置见表 11。

表9 NTP 典型参数配置表

序号	参数项	描述	典型参数
1	主时钟主网 IP 地址	主时钟 A 网 IP 地址	厂站站控层主时钟 A 网 IP 地址
2	主时钟备网 IP 地址	主时钟 B 网 IP 地址	厂站站控层主时钟 B 网 IP 地址

3	备时钟主网 IP 地址	备时钟 A 网 IP 地址	厂站站控层备时钟 A 网 IP 地址
4	备时钟备网 IP 地址	备时钟 B 网 IP 地址	厂站站控层备时钟 B 网 IP 地址
5	端口号	NTP 端口号	123
6	对时周期	NTP 对时周期，单位为 s	30
7	是否采用广播	采用广播/点对点	广播

表10 通信典型参数配置表

序号	参数项	描述	典型参数
1	服务器、工作站数据采集的服务端口	针对采集服务器、工作站信息所开放的 TCP 服务端口	8800
2	安全防护设备数据采集的服务端口	针对采集服务器、工作站的 UDP 服务端口	514
3	网络设备 SNMP TRAP 端口	针对采集网络设备 SNMP TRAP 信息所开发的 UDP 服务端口	162
4	装置服务代理端口	装置自身开启服务代理的 TCP 服务端口	8801
5	平台 IP 地址 1	主站管理平台接收监测装置事件上传/进行服务代理调用的 IP 地址 1	对应平台骨干网业务地址
6	事件上传端口 1	主站管理平台接收监测装置事件上传的 TCP 端口 1	8800
7	平台 IP 地址 1 的权限	针对 IP 地址 1 的权限	读取信息/对监测装置进行参数配置/上传事件/对检测对象进行参数设置、命令控制
8	平台 IP 地址 n	主站管理平台接收监测装置事件上传/进行服务代理调用的 IP 地址 n	对应平台骨干网业务地址
9	事件上传端口 n	主站管理平台接收监测装置事件上传的 TCP 端口 n	8800
10	平台 IP 地址 n 的权限	针对 IP 地址 n 的权限	读取信息/对监测装置进行参数配置/上传事件/对检测对象进行参数设置、命令控制
11	通讯组配置	不同的通讯组上传不同的平台	0 代表默认，应设置 1-15 之间
12	组内优先级配置	同一通讯组内优先级小的优先	优先级为 1-15

表11 事件处理典型参数配置表

序号	参数项	描述	典型参数
1	CPU 利用率上限阈值	CPU 利用率超过上限需要形成告警的阈值	80%

2	内存使用率上限阈值	内存使用率超过上限需要形成告警的阈值	80%
3	网口流量越限阈值	交换机网口流量超过上限需要形成告警的阈值，单位 Kbps	10
4	连续登录失败阈值	连续登录失败多少次形成告警事件上报	5
5	归并事件归并周期	需要归并处理的事件的归并上报周期，单位 s	60
6	磁盘空间使用率上限阈值	磁盘空间使用率超过上限需要形成告警的阈值	80%
7	历史事件上报分界时间参数 t	长时间离线后，监测装置再次上线时，根据此 t 值确定上报哪些未上传事件。单位：分钟	30

6 监测对象接入调试

监测对象主要分为主机设备、网络设备、安全防护设备，分别以部署 AGENT、启用 SNMP 协议、配置 SYSLOG 日志上送等方式来接入，在接入厂站网络安全监测装置后应进行数据采集功能调试。

6.1 主机设备

主机设备接入主要通过在服务器、工作站部署 AGENT 的方法实现节点接入，具体接入步骤如下：

（1）对主机参数及应用数据进行备份；

（2）拷贝 AGENT 程安装文件至主机并安装；

（3）运行注册程序获取机器码；

（4）使用机器码向程序厂商申请 lisence；

（5）使用程序厂商下发的 lisence 激活 AGENT；

（6)配置 AGENT 网络传输参数(包含本机 IP 地址、采集装置 IP 地址、采集装置端口)；

（7）在 AGENT 程序文件夹中导入厂站监测装置证书；

（8）依据主机网络连接状态配置 AGENT 白名单（IP 白名单及端口白名单），并根据业务需求配置关键文件/目录检测配置、开放非法端口检测周期配置等。

（9）运行 AGENT 及其守护进程；

（10）通过网络安全监测装置查看告警和日志，确认 AGENT 部署成功；

（11）配置 AGENT 自启动，并重启主机设备；

（12）确认主机业务运行正常，现场调试人员应利用监测装置的本地图形化管理 UI 界面（现场监视功能），观察告警情况，消除重要及以上告警。

主机设备 AGENT 四类重要配置项及推荐配置参数如下：

IP 白名单配置：

推荐配置主机设备同网段且需业务数据交互的主机地址、广域网通信服务的数据网地址，对于不同网段的地址建议细化。

端口白名单配置：

推荐配置主机设备业务数据交互必须的端口，严禁配置非业务需求的 0-1024 端口及高

危端口。

关键文件/目录检测配置：

推荐配置主机设备的操作系统关键文件夹、业务系统关键文件夹及配置备份文件夹。

开放非法端口检测周期配置：

内网安全规范要求开放非法端口检测周期配置为 5 分钟，即 300 秒。

6.2 网络设备

网络设备接入主要通过在交换机上启用 SNMP 协议（V2c 以上版本）的方法实现节点接入，具体接入步骤如下：

（1）备份交换机相关参数配置；

（2）启用 SNMP 协议，并配置相关的用户表、Trap 等信息；

（3）保存交换机配置，与监测装置测试通讯及功能是否正常。

网络设备接入后，现场调试人员应利用监测装置的本地图形化管理 UI 界面（现场监视功能），观察告警情况，消除重要及以上告警。

6.3 安全防护设备

安全防护设备接入主要通过在安全防护设备上修改 syslog 或通信参数的方法实现节点接入，具体接入步骤如下：

防火墙：

（1）备份防火墙参数配置；

（2）配置 syslog 传输地址为对应监测装置网口地址；

（3）启用符合电力系统通用告警格式的告警传输服务并配置通信参数；

（4）防火墙与网络安全监测装置进行通信测试。

隔离装置：

（1）备份隔离装置参数配置；

（2）修改隔离装置通信策略；

（3）启用符合电力系统通用告警格式的告警传输服务并配置通信参数；

（4）隔离装置与网络安全监测装置进行通信测试。

安全防护设备接入后，现场调试人员应利用监测装置的本地图形化管理 UI 界面（现场监视功能），观察告警情况，消除重要及以上告警。

6.4 装置数据采集功能调试

网络安全监测装置单体调试完毕、监测对象接入完毕后，参照《电力监控系统网络安全监测装置技术规范》附录 A 采集信息规范表，开展监测装置采集监测对象信息的功能调试。

监测装置对主机设备、网络设备、安全防护设备采集功能测试方法见表 12-15。

表12 主机设备采集信息调试表

序号	采集信息内容	信息产生方式	调试及测试方法
1	登录成功	触发	在主机设备登陆成功，检查是否产生相应告警

2	退出登陆	触发	在主机设备退出登陆，检查是否产生相应告警
3	登录失败	触发	在主机设备登陆失败，检查是否产生相应告警
4	操作命令	触发	在主机设备操作命令，检查是否产生相应告警
5	操作回显	触发	在主机设备操作命令，检查是否产生相应告警
6	USB 设备插入	触发	在主机设备插入 USB 设备，检查是否产生相应告警
7	USB 设备拔出	触发	在主机设备拔出 USB 设备，检查是否产生相应告警
8	串口占用	触发	使用调试笔记本占用串口，检查是否产生相应告警
9	串口释放	触发	使用调试笔记本释放串口，检查是否产生相应告警
10	光驱挂载	触发	将光盘放入光驱，检查是否产生相应告警
11	光驱卸载	触发	将光盘从光驱弹出，检查是否产生相应告警
12	异常网络访问事件	触发	网络外联事件在主机设备 telnet 调试笔记本，检查是否产生相应告警
13	存在光驱设备	周期（默认 60 分钟）	若主机设备存在光驱，检查是否周期性产生相应告警
14	开放网络服务/端口	触发	将已经监听的端口从白名单中移除，检查是否产生相应告警
15	网口 UP	触发	将调试笔记本与主机设备使用网线连接，检查是否产生相应告警
16	网口 DOWN	触发	断开调试笔记本与主机设备的网线连接，检查是否产生相应告警
17	关键文件变更	触发	在主机设备修改关键文件，检查是否产生相应告警
18	用户权限变更	触发	在主机设备修改用户权限，检查是否产生相应告警

表13 网络设备采集信息调试表

序号	采集信息内容	信息产生方式	调试及测试方法
1	配置变更	触发	在网络设备修改 MAC 地址绑定关系，检查是否产生相应告警
2	网口状态	周期	在人机界面查看网络设备网口状态，与实际状态进行对比
3	网口 UP	触发	将调试笔记本与主机设备使用网线连接，检查是否产生相应告警
4	网口 DOWN	触发	断开调试笔记本与主机设备的网线连接，检查是否产生相应告警
5	网口流量超过阈值	触发	先将笔记本接入网络设备网口，然后通过 WEB 管理界面增加流量阈值设置，生效后，检查是否产

			生相应告警
6	登录成功	触发	在网络设备 WEB 管理界面登陆成功，检查是否产生相应告警
7	退出登录	触发	在网络设备 WEB 管理界面退出登录，检查是否产生相应告警
8	*登录失败	触发	在网络设备 WEB 管理界面登录失败，检查是否产生相应告警
9	修改用户密码	触发	在网络设备 WEB 管理界面修改用户密码，检查是否产生相应告警
10	用户操作信息	触发	在网络设备 WEB 管理界面进行用户操作，检查是否产生相应告警
11	MAC 地址绑定关系	周期（默认 60 分钟）	对于未绑定 MAC 地址的激活接口，检查是否周期性产生该告警

表14 安全设备（防火墙）采集信息调试表

序号	采集信息内容	信息产生方式	调试及测试方法
1	登录成功	触发	在防火墙 WEB 管理界面登陆成功，检查是否产生相应告警
2	退出登录	触发	在防火墙 WEB 管理界面退出登陆，检查是否产生相应告警
3	登录失败	触发	在防火墙 WEB 管理界面登陆失败，检查是否产生相应告警
4	修改策略	触发	在防火墙 WEB 管理界面修改策略，检查是否产生相应告警
5	CPU 利用率	周期（默认 1 分钟）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
6	内存利用率	周期（默认 1 分钟）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
7	电源故障	触发	切断防火墙备用电源，检查是否产生相应告警
8	风扇故障	触发	当发生风扇故障时，防火墙应产生相应告警
9	温度异常	触发	将防火墙温度阈值设置为 0，检查是否产生温度异常告警
10	网口 DOWN	触发	将调试笔记本与防火墙使用网线连接，检查是否产生相应告警
11	网口 UP	触发	断开调试笔记本与防火墙的网线连接，检查是否产生相应告警
12	不符合安全策略的访问	触发	增加禁止调试笔记本 ICMP 的规则，然后使用调试笔记本进行 PING 测试，检查是否产生相应告警
13	攻击告警	触发	打开调试笔记本接口的 PingofDeath 监测，然后在调试笔记本上使用“ping192.168.2.202-1900”进行测试，检查是否产生相应告警

表15 安全设备（横向隔离装置）采集信息调试表

序号	采集信息内容	信息产生方式	调试及测试方法
1	用户登录	触发	在隔离设备管理界面登陆成功，检查是否产生相应告警
2	修改配置	触发	在隔离设备管理界面修改配置，检查是否产生相应告警
3	CPU 利用率	周期（默认 1 分钟）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
4	内存利用率	周期（默认 1 分钟）	将装置内存利用率越限阈值设置为 0，检查是否周期产生内存利用率越限阈值告警
5	不符合安全策略的访问	触发	使用调试笔记本 telnet 不在安全策略中的端口，检查是否产生相应告警

7 平台接入调试

各类厂站的监测装置应接入两套调度数据网接入网所属相应调控机构平台，如 220 千伏变电站应接入省调平台及地调平台、双地网新能源厂站双平面应接入地调平台；

平台接入调试期间，现场调试人员应利用监测装置的本地图形化管理 UI 界面，观察告警情况（需要提供相应的截图作为附件），确认无重要及以上等级告警后通知调控机构人员进行监测装置的级联调试；调控机构人员应在平台将该监测装置置“挂牌”状态，通过过滤告警信息，观察告警情况，确认无重要及以上告警后通知调控机构人员将该监测装置取消检修。

若级联阶段发现平台上仍能收到无效告警信息，应及时通知现场集成商进行断开数据网通讯，并提供信息说明。

7.1 厂站纵向加密认证装置配置

厂站纵向加密认证装置需增加一条至主站采集服务器加密卡地址的隧道，其策略配置如表 16。

表16 厂站纵向加密认证装置配置表

序号	描述	策略协议	源起始 IP	源终止 IP	源起始端口	源终止端口	目的起始 IP	目的终止 IP	目的起始端口	目的终止端口	隧道对端 IP
1	厂站监测装置管控	密通 TCP	厂站网络安全监测装置地址	厂站网络安全监测装置地址	8801	8801	主站采集服务器加密卡地址	主站采集服务器加密卡地址	1025	65535	主站采集服务器加密卡地址/主站端非实
2	网络安全事件上传	密通 TCP	厂站网络安全监测装	厂站网络安全监测装	1025	65535	主站采集服务器加密	主站采集服务器加密	8800	8800	

			置地址	置地址			卡地址	卡地址			时加密
3	业务探测	密通 ICMP	厂站网络安全监测装置地址	厂站网络安全监测装置地址	0	0	主站采集服务器加密卡地址	主站采集服务器加密卡地址	0	0	加地址

7.2 主站采集服务器加密卡配置

主站采集服务器加密卡需增加一条至厂站纵向设备地址的隧道，其策略配置如表 17。

表17 主站采集服务器加密卡配置表

序号	描述	策略协议	源起始IP	源终止IP	源起始端口	源终止端口	目的起始IP	目的终止IP	目的起始端口	目的终止端口	隧道对端IP
1	厂站监测装置管控	密通 TCP	主站采集服务器加密卡地址	主站采集服务器加密卡地址	8800	8800	厂站网络安全监测装置地址	厂站网络安全监测装置地址	1025	65535	厂站端加密机地址
2	网络安全事件上传	密通 TCP	主站采集服务器加密卡地址	主站采集服务器加密卡地址	1025	65535	厂站网络安全监测装置地址	厂站网络安全监测装置地址	8801	8801	
3	业务探测	密通 ICMP	主站采集服务器加密卡地址	主站采集服务器加密卡地址	0	0	厂站网络安全监测装置地址	厂站网络安全监测装置地址	0	0	

7.3 装置的双向身份认证

监测装置与平台间通信需通过数字证书实现双向的身份认证：

a)现场调试人员导出装置证书请求，发送给相应负有监控及现场维护责任的调控机构。如 220 千伏变电站监测装置证书应发送给地调签发；

b）调控机构人员使用调度数字证书系统录入装置证书请求，审核签发生成装置公钥证书，并将装置公钥证书、平台网关机证书发送给现场调试人员；

c）调控机构人员将装置公钥证书导入平台；

d）现场调试人员将装置公钥证书、平台网关机证书导入到监测装置中。

7.4 装置数据上传功能调试

a）网络安全监测装置单体调试完毕、监测对象接入完毕、接入网络安全管理平台后，根据《电力监控系统网络安全监测装置技术规范》附录 B 上传信息规范表，开展厂站网络安全监测功能与网络安全管理平台联调测试。

b）监测装置对主机设备、网络设备、安全防护设备、监测装置自身上传功能测试方法

见表 18-22。

表18 主机设备上传信息调试表

序号	验收项目	级别	验收标准或要求
1	USB 设备（无线网卡）	紧急（1）	插入 USB 设备（无线网卡）到主机，通过平台能够查看到 USB 插入事件记录
2	网络外联事件	紧急（1）	使用笔记本电脑 SSH 远程连接主机，该笔记本电脑 IP 不在变电站网段中，装置人机界面记录及主站端管理平台告警均正确
3	USB 设备（非无线网卡类）插入	重要（2）	插入 USB 设备到主机类设备，装置人机界面记录及主站端管理平台告警均正确
4	串口占用	重要（2）	使用调试笔记本占用串口，检查是否产生相应告警
5	并口占用	重要（2）	使用调试笔记本占用并口，检查是否产生相应告警
6	光驱挂载	重要（2）	将光盘放入光驱，检查是否产生相应告警
7	登录失败超过阈值	重要（2）	主机类设备输入错误登录密码达到规定次数，装置人机界面记录及主站端管理平台告警均正确
8	关键文件变更	重要（2）	在主机设备修改关键文件，检查是否产生相应告警
9	用户权限变更	重要（2）	在主机设备修改用户权限，检查是否产生相应告警
10	危险操作	重要（2）	在主机上执行主机探针上设定的危险指令，检查是否产生相应告警
11	设备离线	重要（2）	断开监测装置与主机设备的网线连接，检查是否产生相应告警
12	存在光驱告警	重要（2）	若主机设备存在光驱，检查是否周期性产生相应告警
13	开放网络服务/端口	重要（2）	将已经监听的端口从白名单中移除，检查是否产生相应告警
14	网口 UP	重要（2）	将调试笔记本与主机设备使用网线连接，检查是否产生相应告警
15	网口 DOWN	重要（2）	断开调试笔记本与主机设备的网线连接，检查是否产生相应告警
16	串口释放	一般（4）	使用调试笔记本释放串口，检查是否产生相应告警
17	并口释放	一般（4）	使用调试笔记本释放并口，检查是否产生相应告警
18	USB 设备拔出	一般（4）	拔出 USB 设备，装置人机界面记录及主站端管理平台告警均正确

19	光驱卸载	一般（4）	将光盘从光驱弹出，检查是否产生相应告警
20	登录成功	一般（4）	在主机设备登陆成功，检查是否产生相应告警
21	设备上线	一般（4）	将监测装置与主机设备使用网线连接，检查是否产生相应告警
22	退出登录	一般（4）	在主机设备退出登陆，检查是否产生相应告警

表19 网络设备上传信息调试表

序号	上传信息	级别	调试及测试方法
1	交换机离线	重要（2）	断开监测装置与网络设备的网线连接，检查是否产生相应告警
2	MAC 绑定关系	重要（2）	对于未绑定 MAC 地址的激活接口，检查是否周期性产生该告警。
3	网口 UP	重要（2）	将调试笔记本与网络设备使用网线连接，检查是否产生相应告警
4	网口 DOWN	重要（2）	断开调试笔记本与网络设备的网线连接，检查是否产生相应告警
5	网口流量超过阈值	重要（2）	先将笔记本接入网络设备网口，然后通过 WEB 管理界面增加流量阈值设置，生效后，检查是否产生相应告警
6	配置变更	一般（4）	在网络设备修改 MAC 地址绑定关系，检查是否产生相应告警
7	交换机上线	一般（4）	将监测装置与网络设备使用网线连接，检查是否产生相应告警
*8	登录成功	一般（4）	在网络设备 WEB 管理界面登陆成功，检查是否产生相应告警
9	退出登录	一般（4）	在网络设备 WEB 管理界面退出登录，检查是否产生相应告警
10	登录失败	一般（4）	在网络设备 WEB 管理界面登录失败，检查是否产生相应告警
11	修改用户密码	一般（4）	在网络设备 WEB 管理界面修改用户密码，检查是否产生相应告警
12	用户操作信息	一般（4）	在网络设备 WEB 管理界面进行用户操作，检查是否产生相应告警

表20 安全设备（防火墙）上传信息调试表

序号	上传信息	级别	调试及测试方法
1	攻击告警	紧急（1）	主机发送命令： ping -l length（length 略高于防火墙设定值）到防火墙，装置人机界面记录及主站端管理平台告警均正确
2	不符合安全策略访	重要（2）	使用防火墙策略 IP 范围外的电脑进行访问

	问		业务，装置人机界面记录及主站端管理平台告警均正确
3	防火墙离线	重要（2）	断开监测装置与防火墙使用网线连接，检查是否产生相应告警
4	CPU 利用率超过阈值	重要（2）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
5	内存使用率超过阈值	重要（2）	将装置内存越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
6	登录成功	一般（4）	在防火墙 WEB 管理界面登陆成功，检查是否产生相应告警
7	退出登录	一般（4）	在防火墙 WEB 管理界面退出登陆，检查是否产生相应告警
8	登录失败	一般（4）	在防火墙 WEB 管理界面登陆失败，检查是否产生相应告警
9	防火墙上线	一般（4）	将监测装置与防火墙使用网线连接，检查是否产生相应告警
10	修改策略	一般（4）	修改防火墙策略，装置人机界面记录及主站端管理平台告警均正确
11	网口 UP	重要（2）	将调试笔记本与防火墙使用网线连接，检查是否产生相应告警
12	网口 DOWN	一般（4）	断开调试笔记本与防火墙的网线连接，检查是否产生相应告警
13	电源故障	一般（4）	防火墙单电源运行，装置人机界面记录及主站端管理平台告警均正确

表21 安全设备（横向隔离装置）上传信息调试表

序号	上传信息	级别	调试及测试方法
1	不符合安全策略的访问	重要（2）	在正/反向隔离装置配置接收端口为 6666，协议为 UDP，目的 IP 为 192.169.0.2，使用隔离装置测试软件进行如下测试： 1. 向 192.169.0.2 的端口 7777 发送 UDP 包； 2. 向 192.169.0.1 的端口 6666 发送 UDP 包； 3. 向 192.169.0.2 的端口 6666 发送 UDP 包； 装置人机界面记录及主站端管理平台告警均正确。
2	隔离装置离线	重要（2）	断开监测装置与隔离设备的网线连接，检查是否产生相应告警
3	CPU 利用率超过阈值	重要（2）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
4	内存使用率超过阈	重要（2）	将装置内存利用率越限阈值设置为 0，检查

	值		是否周期产生内存利用率越限阈值告警
5	隔离装置上线	一般（4）	将监测装置与隔离设备的网线连接，检查是否产生相应告警
6	修改策略	重要（2）	修改策略 1.修改协议 2.修改 IP 3.修改端口，装置人机界面记录及主站端管理平台告警均正确

表22 监测装置上传信息调试表

序号	验收项目	级别	验收标准或要求
1	USB 设备（无线网卡）	紧急（1）	插入 USB 设备（无线网卡）到装置，通过平台能够查看到 USB 插入事件记录
2	网络外联事件	紧急（1）	使用笔记本电脑远程连接装置，该笔记本电脑 IP 不在变电站网段中，通过管理平台能够查看到网络外联事件记录
3	系统登录失败超过阈值	重要（2）	在后台输入错误登录信息，通过管理平台能够查看登录失败事件
4	危险操作	重要（2）	在监测装置上执行监测装置设定的危险指令，检查是否产生相应告警
5	开放非法端口	重要（2）	将已经监听的端口从白名单中移除，检查是否产生相应告警
6	网口 UP	重要（2）	监测装置网口接入设备，通过平台能够查看网口 UP 信息记录
7	网口 DOWN	重要（2）	监测装置网口网线拔出，通过平台能够查看网口 DOWN 信息记录
8	CPU 利用率超过阈值	重要（2）	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警
9	内存使用率超过阈值	重要（2）	将装置内存利用率越限阈值设置为 0，检查是否周期产生内存利用率越限阈值告警
10	磁盘空间使用率超过阈值	重要（2）	将装置磁盘空间使用率越限阈值设置为 0，检查是否周期产生磁盘空间利用率越限阈值告警
11	装置异常告警	重要（2）	模拟装置故障，装置断电，通过管理平台能够查看到设备离线事件记录
12	对时异常	重要（2）	模拟对时异常，将装置对时源去除，通过平台能够查看对时异常事件记录
13	本地管理界面登录失败被锁定	重要（2）	在本地客户端错误登录信息，通过管理平台能够查看登录失败事件
14	验签错误	重要（2）	在本地界面导入错误的证书，通过管理平台能够查看登录失败事件
15	USB 设备（非无线网卡类）插入	重要（2）	插入 USB 设备到装置，通过管理平台能够查看到 USB 插入事件记录
16	系统登录成功	一般（4）	登录监测装置后台，通过管理平台能够查看登录信息

17	系统退出登录	一般（4）	退出监测装置后台，通过管理平台能够查看退出信息
18	USB 设备拔出	一般（4）	拔出 USB 设备，通过管理平台能够看到告警信息
19	本地管理界面登录成功	一般（4）	通过客户端登陆监测装置，通过管理平台能够查看登录信息
20	本地管理界面退出登录	一般（4）	通过客户端退出用户登陆，通过管理平台能够查看登录信息
21	配置变更	一般（4）	在监测装置上修改自身内部信息，通过管理平台能够查看登录信息

8 功能验证

8.1 主站功能检查

平台需要对厂站侧接入的监测装置进行相应的验收测试，以保障现场实施功能的竣工验收的完整性。具体包括如下 7 个方面：

a）通过平台对装置状态的查询，实现资产在线测试；

b）通过平台查询装置上报告的告警信息，实现装置告警事件上传测试；

c）通过平台对监测装置采集信息调阅和上传事件调阅，实现对装置的远程信息调阅测试；

d）通过平台查看及修改监测装置的资产信息、网卡配置、路由配置、NTP 配置、通信配置（是否双平面上送）、事件处理等配置，实现对装置的远程配置管理测试；

e）通过平台远程升级装置的版本，实现对装置远程升级的测试；

f）通过平台远程配置装置的网络连接白名单、服务端口白名单和危险操作命令清单，实现对监控对象的配置管理测试。

g）通过平台远程查看监测装置对监测对象的基线核查项，实现主站对厂站监测对象的基线核查和漏洞扫描。

8.2 厂站现场验收

监测装置上述调试流程完成后，工程参与单位应配合厂站运维检修部门完成如下现场竣工工作：

a）按施工工艺标准再次检查施工现场，完成标识牌张贴和屏柜防火封堵等扫尾工作；

b）做好装置和其他改动过配置的设备配置备份；

c）按保管规则妥善保管好 U-key；

d）办理工作票等安全组织措施的终结手续。

8.3 填写验收卡

监测装置上述调试流程完成后，工程参与单位应配合厂站运维检修部门，按附表 2《电力监控系统厂站网络安全监测装置部署验收卡》进行现场验收各工作，并将验收卡报调控机构备案。

8.4 云平台资料补充

工程参与单位配合调控机构，将监测装置资料（如厂商及设备型号等）补充录入云平台，并将运行状态由“规划”改为“投运”。

厂站网络安全监测装置部署“五提醒”

- **对时。**需保证厂站监测装置时间与主站平台、与监测对象时间相差 30 秒之内。
- **证书。**需保证厂站监测装置所需证书、厂站主机设备 AGENT 所需证书、主站平台所需证书正确。
- **端口。**需保证厂站监测装置与监测对象、与主站平台通信所需端口正常通信。
- **白名单。**需保证监测对象白名单设置符合正常业务需求且包括自身采集事件上传通信需求，无高危服务或端口。
- **告警。**需保证监测装置无重要及以上告警后再接入主站平台，现场调试人员应利用监测装置的本地图形化管理 UI 界面（现场监视功能），观察告警情况。装置接入主站调试期间，调控机构人员应在平台将该监测装置置“挂牌”状态，完成接入后取消。

附表 1：电力监控系统厂站网络安全监测装置部署设备清单

设备大类	设备名称	探针厂商	IP 地址	操作系统版本或软件版本	能否接入监测装置	不能接入原因（仅不能接入设备填写）	计划接入时间（仅不能接入设备填写）
主机设备							
网络设备							
安全防护设备							
现场工作负责人：							

附表 2：电力监控系统厂站网络安全监测装置部署验收卡

1、设备及功能检查

序号	验收项目	验收标准或要求	验收情况	备注
1	装置接口检查	电源接线、网线等连接应牢固、可靠、无松动，接线正确	□通过 □未通过	
		电缆标牌制作美观，标识齐全、清晰	□通过 □未通过	
		通讯网络接头制作工艺符合要求	□通过 □未通过	
		通讯网线标牌正确、清晰	□通过 □未通过	
2	装置接地检查	装置外壳可靠接地，接地线和接地点符合规范要求。	□通过 □未通过	
		电缆屏蔽层可靠接地	□通过 □未通过	
3	电源回路检查	电源空开与主机实际接入要求一致	□通过 □未通过	
		双电源应接自不同的直流电源设备	□通过 □未通过	
		电源空开级差符合要求	□通过 □未通过	
		双电源切换检查	□通过 □未通过	
4	设备功能性要求检查	网络拓扑	□通过 □未通过	
		104 仿真测试功能	□通过 □未通过	

		主站事件信息或触发信息过滤功能（可设置）	□通过 □未通过	
		装置外设接入调试软件人机交互功能检查（要求汉化版本）	□通过 □未通过	
		软件版本核对	□通过 □未通过	
		同步时钟对时情况（具备 SNTP 对时）	□通过 □未通过	
5	AGENT 程序部署情况	监控系统服务器或工作站	□通过 □未通过	
		站控层交换机	□通过 □未通过	
		防火墙	□通过 □未通过	
结论：□通过 □未通过			**现场工作负责人:**	

2、网络安全监测装置自身监测功能测试

序号	验收项目	验收标准或要求	验收情况	备注
1	USB **设备（无线网卡）**	插入 USB 设备（无线网卡）到装置，通过平台能够查看到 USB 插入事件记录	□通过 □未通过	触发方式
2	**网络外联事件**	使用笔记本电脑远程连接装置，该笔记本电脑 IP 不在变电站网段中，通过管理平台能够查看到网络外联事件记录	□通过 □未通过	触发方式
3	**系统登录失败超过阈值**	在后台输入错误登录信息，通过管理平台能够查看登录失败事件	□通过 □未通过	触发方式
4	**危险操作**	在监测装置上执行监测装置设定的危险指令，检查是否产生相应告警	□通过 □未通过	触发方式
5	**开放非法端口**	将已经监听的端口从白名单中移除，检查是否产生相应告警	□通过 □未通过	触发方式

6	**网口** UP	监测装置网口接入设备，通过平台能够查看网口 UP 信息记录	□通过 □未通过	触发方式
7	**网口** DOWN	监测装置网口网线拔出，通过平台能够查看网口 DOWN 信息记录	□通过 □未通过	触发方式
8	CPU **利用率超过阈值**	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警	□通过 □未通过	触发方式
9	**内存使用率超过阈值**	将装置内存利用率越限阈值设置为 0，检查是否周期产生内存利用率越限阈值告警	□通过 □未通过	触发方式
10	**磁盘空间使用率超过阈值**	将装置磁盘空间使用率越限阈值设置为 0，检查是否周期产生磁盘空间利用率越限阈值告警	□通过 □未通过	触发方式
11	**装置异常告警**	模拟装置故障，装置断电，通过管理平台能够查看到设备离线事件记录	□通过 □未通过	触发方式
12	**对时异常**	模拟对时异常，将装置对时源去除，通过平台能够查看对时异常事件记录	□通过 □未通过	触发方式
13	**本地管理界面登录失败被锁定**	在本地客户端错误登录信息，通过管理平台能够查看登录失败事件	□通过 □未通过	触发方式
14	**验签错误**	在本地界面导入错误的证书，通过管理平台能够查看登录失败事件	□通过 □未通过	触发方式
15	USB **设备（非无线网卡类）插入**	插入 USB 设备到装置，通过管理平台能够查看到 USB 插入事件记录	□通过 □未通过	触发方式
16	**系统登录成功**	登录监测装置后台，通过管理平台能够查看登录信息	□通过 □未通过	触发方式
17	**系统退出登录**	退出监测装置后台，通过管理平台能够查看退出信息	□通过 □未通过	触发方式

18	USB 设备拔出	拔出 USB 设备，通过管理平台能够看到告警信息	□通过 □未通过	触发方式
19	本地管理界面登录成功	通过客户端登陆监测装置，通过管理平台能够查看登录信息	□通过 □未通过	触发方式
20	本地管理界面退出登录	通过客户端退出用户登陆，通过管理平台能够查看登录信息	□通过 □未通过	触发方式
21	配置变更	在监测装置上修改自身内部信息，通过管理平台能够查看登录信息	□通过 □未通过	触发方式
结论：□通过 □未通过		现场工作负责人:		

3、主机类监测功能测试

序号	验收项目	验收标准或要求	验收情况	备注
1	USB 设备（无线网卡）	插入 USB 设备（无线网卡）到主机，通过平台能够查看到 USB 插入事件记录	□通过 □未通过	触发方式
2	网络外联事件	使用笔记本电脑 SSH 远程连接主机，该笔记本电脑 IP 不在变电站网段中，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
3	USB 设备（非无线网卡类）插入	插入 USB 设备到主机类设备，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
4	串口占用	使用调试笔记本占用串口，检查是否产生相应告警	□通过 □未通过	触发方式
5	并口占用	使用调试笔记本占用并口，检查是否产生相应告警	□通过 □未通过	触发方式
6	光驱挂载	将光盘放入光驱，检查是否产生相应告警	□通过 □未通过	触发方式
7	登录失败超过阈值	主机类设备输入错误登录密码达到规定次数，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式

8	**关键文件变更**	在主机设备修改关键文件，检查是否产生相应告警	□通过 □未通过	触发方式
9	**用户权限变更**	在主机设备修改用户权限，检查是否产生相应告警	□通过 □未通过	触发方式
10	**危险操作**	在主机上执行主机探针上设定的危险指令，检查是否产生相应告警	□通过 □未通过	触发方式
11	**设备离线**	断开监测装置与主机设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
12	**存在光驱告警**	若主机设备存在光驱，检查是否周期性产生相应告警	□通过 □未通过	触发方式
13	**开放网络服务/端口**	将已经监听的端口从白名单中移除，检查是否产生相应告警	□通过 □未通过	触发方式
14	**网口** UP	将调试笔记本与主机设备使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
15	**网口** DOWN	断开调试笔记本与主机设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
16	**串口释放**	使用调试笔记本释放串口，检查是否产生相应告警	□通过 □未通过	触发方式
17	**并口释放**	使用调试笔记本释放并口，检查是否产生相应告警	□通过 □未通过	触发方式
18	USB **设备拔出**	拔出 USB 设备，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
19	**光驱卸载**	将光盘从光驱弹出，检查是否产生相应告警	□通过 □未通过	触发方式
20	**登录成功**	在主机设备登陆成功，检查是否产生相应告警	□通过 □未通过	触发方式
21	**设备上线**	将监测装置与主机设备使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式

22	**退出登录**	在主机设备退出登陆，检查是否产生相应告警	□通过 □未通过	触发方式
结论：□通过 □未通过		**现场工作负责人:**		

4、网络设备监测功能测试

序号	测试内容	验收标准或要求	验收情况	备注
1	**交换机离线**	断开监测装置与网络设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
2	MAC 绑定关系	对于未绑定 MAC 地址的激活接口，检查是否周期性产生该告警。	□通过 □未通过	触发方式
3	**网口** UP	将调试笔记本与网络设备使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
4	**网口** DOWN	断开调试笔记本与网络设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
5	**网口流量超过阈值**	先将笔记本接入网络设备网口，然后通过 WEB 管理界面增加流量阈值设置，生效后，检查是否产生相应告警	□通过 □未通过	触发方式
6	**配置变更**	在网络设备修改 MAC 地址绑定关系，检查是否产生相应告警	□通过 □未通过	触发方式
7	**交换机上线**	将监测装置与网络设备使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
8	**登录成功**	在网络设备 WEB 管理界面登陆成功，检查是否产生相应告警	□通过 □未通过	触发方式
9	**退出登录**	在网络设备 WEB 管理界面退出登录，检查是否产生相应告警	□通过 □未通过	触发方式
10	**登录失败**	在网络设备 WEB 管理界面登录失败，检查是否产生相应告警	□通过 □未通过	触发方式
11	**修改用户密码**	在网络设备 WEB 管理界面修改用户密码，检查是否产生相应告警	□通过 □未通过	触发方式

12	**用户操作信息**	在网络设备 WEB 管理界面进行用户操作，检查是否产生相应告警	□通过 □未通过	触发方式
结论：□通过 □未通过		**现场工作负责人:**		

5、防火墙监测功能测试

序号	测试内容	验收标准或要求	验收情况	备注
1	**攻击告警**	主机发送命令： ping -l length（length 略高于防火墙设定值）到防火墙，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
2	**不符合安全策略访问**	使用防火墙策略 IP 范围外的电脑进行访问业务，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
3	**防火墙离线**	断开监测装置与防火墙使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
4	CPU **利用率超过阈值**	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警	□通过 □未通过	触发方式
5	**内存使用率超过阈值**	将装置内存越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警	□通过 □未通过	触发方式
6	**登录成功**	在防火墙 WEB 管理界面登陆成功，检查是否产生相应告警	□通过 □未通过	触发方式
7	**退出登录**	在防火墙 WEB 管理界面退出登陆，检查是否产生相应告警	□通过 □未通过	触发方式
8	**登录失败**	在防火墙 WEB 管理界面登陆失败，检查是否产生相应告警	□通过 □未通过	触发方式
9	**防火墙上线**	将监测装置与防火墙使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
10	**修改策略**	修改防火墙策略，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
11	网口 UP	将调试笔记本与防火墙使用网线连接，检查是否产生相应告警	□通过 □未通过	触发方式

12	网口 DOWN	断开调试笔记本与防火墙的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
13	电源故障	防火墙单电源运行，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
结论：□通过 □未通过		**现场工作负责人:**		

6、隔离装置监测功能测试

序号	测试内容	验收标准或要求	验收情况	备注
1	不符合安全策略的访问	在正/反向隔离装置配置接收端口为 6666，协议为 UDP，目的 IP 为 192.169.0.2，使用隔离装置测试软件进行如下测试： 4. 向 192.169.0.2 的端口 7777 发送 UDP 包； 5. 向 192.169.0.1 的端口 6666 发送 UDP 包； 6. 向 192.169.0.2 的端口 6666 发送 UDP 包； 装置人机界面记录及主站端管理平台告警均正确。	□通过 □未通过	触发方式
3	**隔离装置离线**	断开监测装置与隔离设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
4	CPU **利用率超过阈值**	将装置 CPU 利用率越限阈值设置为 0，检查是否周期产生 CPU 利用率越限阈值告警	□通过 □未通过	触发方式
5	**内存使用率超过阈值**	将装置内存利用率越限阈值设置为 0，检查是否周期产生内存利用率越限阈值告警	□通过 □未通过	触发方式
6	**隔离装置上线**	将监测装置与隔离设备的网线连接，检查是否产生相应告警	□通过 □未通过	触发方式
7	修改策略	修改策略 1.修改协议 2.修改 IP 3.修改端口，装置人机界面记录及主站端管理平台告警均正确	□通过 □未通过	触发方式
结论：□通过 □未通过		**现场工作负责人:**		

7、装置接入平台功能检查

序号	测试内容	测试项	验收标准或要求	验收情况	备注

*1	平台资产在线测试	装置状态查询	［北京科东］ 安全监视—平台监视—厂站装置监视，显示装置在线状态，即正常。	□通过 □未通过	
*2	装置告警事件上传测试	告警信息显示	［北京科东］安全监视—告警监视，查看装置上报告警信息，即正常	□通过 □未通过	
*3	远程信息调阅测试	采集信息调阅	［北京科东］ 厂站管理—采集信息—选择装置—点击查询，返回查询成功，并有信息显示，即正常。	□通过 □未通过	
*4		上传事件调阅	［北京科东］ 厂站管理—上传事件—选择装置—点击查询，返回查询成功，并有告警事件信息，即正常。	□通过 □未通过	
*5	远程配置管理测试	资产配置	［北京科东］ 厂站管理—配置管理—资产配置—选择装置，可添加、删除、编辑及查看装置的资产，即正常。	□通过 □未通过	
6		网卡配置	［北京科东］ 厂站管理—配置管理—网卡配置—选择装置，可添加、删除、编辑及查看装置的网卡配置，即正常。	□通过 □未通过	
7		路由配置	［北京科东］ 厂站管理—配置管理—路由配置—选择装置，可添加、删除、编辑及查看装置的路由配置，即正常。	□通过 □未通过	
8		NTP 配置	［北京科东］ 厂站管理—配置管理—NTP 配置—选择装置，可编辑及查看装置的 NTP 配置，即正常。	□通过 □未通过	
9		通信配置	［北京科东］ 厂站管理—配置管理—通信配置—选择装置，可编辑及查看装置的通信配置，即正常。	□通过 □未通过	

*10		事件处理配置	［北京科东］ 厂站管理—配置管理—通信配置—选择装置，可修改 CPU 利用率上限阈值、内存使用率上限阈值、网口流量越限阈值、连续登录失败阈值、磁盘空间使用率上限阈值，即正常。	□通过 □未通过	
11	远程升级测试	远程升级	［北京科东］ 厂站管理—软件升级，上传正确装置版本，升级成功，即正常。	□通过 □未通过	
*12	监控对象配置管理	网络连接白名单	［北京科东］ 厂站管理—监测对象，可修改装置自身-网络连接白名单修改成功，即正常	□通过 □未通过	
*13		服务端口白名单	［北京科东］厂站管理—监测对象，可修改装置自身的服务端口白名单修改成功，即正常	□通过 □未通过	
14		危险操作命令清单	［北京科东］ 厂站管理—监测对象，可修改装置自身的危险操作命令清单修改成功，即正常	□通过 □未通过	
结论：□通过 □未通过			**现场工作负责人:**		