

[光伏]

光伏电站II型网络安全监测装置建设与应用

文/江西铜业（铅山）光伏发电有限公司 江 宾

电力监控系统安全防护承受着巨大压力，需要新的网络安全管理技术手段。分析了光伏电站网络安全监测装置建设的相关政策，就目前光伏电站网络安全监测现状及设计要求、应用提出见解，并通过对光伏电站监控系统布置网络安全装置，大大加强了系统网络安全应用和管理手段，确保电站和电网的运行安全。

光伏电站网络安全监测装置建设的必要性

近年来，世界上相继发生了乌克兰大面积停电（2015年）、美国东部互联网服务瘫痪（2016年）和全球爆发勒索病毒（2017年）等事件，电力系统已成为国际网络战的重要攻击目标，电力监控系统安全防护承受着巨大压力，需要新的网络安全管理技术手段。

在我国，随着《网络安全法》的出台，开始启动了网络安全空间的相关工作，在安全法中已要求采取监测、记录网络运行状态和网络安全事件的技术措施。在我国的等级保护制度中，也对第三方审计有明确的要求，需要支持网络设备、安全设备、操作系统和应用程序等多层面联合审计的技术支撑。各电网公司已高度重视网络安全工作，并将网络安全视为大电网安全的重要组成部分，明确要求建立电力监控系统网络安全事件快速反应机制和预防预控机制。

光伏电站网络安全监测装置建设的相关政策依据

《电力监控系统安全防护总体方案》（国能安全〔2015〕36号）中指出：“生产控制大区应当逐步推广内网安全监视功能，实时监测电力监控系统

的计算机、网络及安全设备运行状态，及时发现非法外联、外部入侵等安全事件并告警。”

国家能源局发布的《关于推进电力安全生产领域改革发展的实施意见》（发改能源规〔2017〕1896号）中“三十七条 加强网络安全建设”指出：“组织实施网络安全重大专项工程，加快网络安全实时监测手段建设。”

国家电网公司于2017年12月27日发布的《关于加快推进电力监控系统网络安全管理平台建设的通知》（国家电网调〔2017〕1084号）明确指出：“在变电站、并网电厂电力监控系统的安全Ⅱ区（或Ⅰ区）部署Ⅱ型网络安全监测装置，实现对网络安全事件的监视与管理”。

我国于2017年6月1日起执行主席令53号《中华人民共和国网络安全法》。

因此，在光伏行业部署网络安全监测装置已是必行的措施。

光伏电站网络安全存在的主要问题

- 1) 内部违法违规跨越难以发现。
- 2) 外来人员调试笔记本、移动存储介质随意接入。
- 3) 安全加固无法有效校验。

- 4) 网络安全攻击发现迟缓。
- 5) 调度机构无法对电厂监控系统涉网部分实施动态技术监督。

光伏电站网络安全监测装置建设方案

1. 监控系统目前情况

(1) 监控系统网络架构 (见图1)

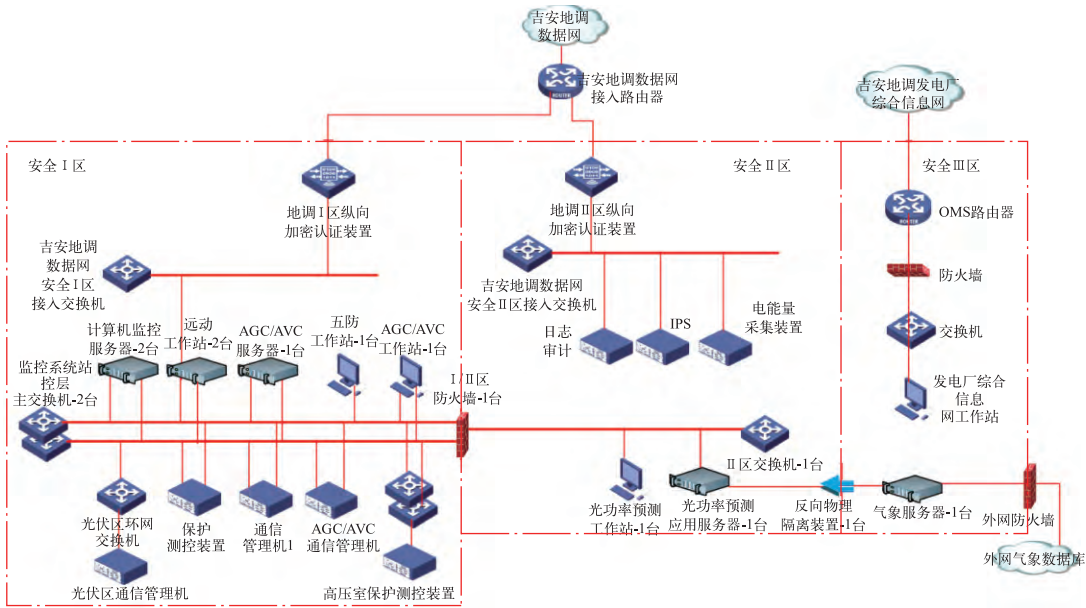


图1 监控系统网络架构

(2) 监控系统安全分区说明

安全 I 区 (控制区) 包含监控系统、五防系统和AGC/AVC系统等。

安全 II 区 (非控制区) 包含电量采集装置、光功率预测系统等。

安全 I 区与安全 II 区之间使用防火墙进行隔离。

安全 III 区 (管理信息大区) 包含气象服务器、OMS等。

安全 II 区与安全 III 区之间采用隔离装置进行隔离。

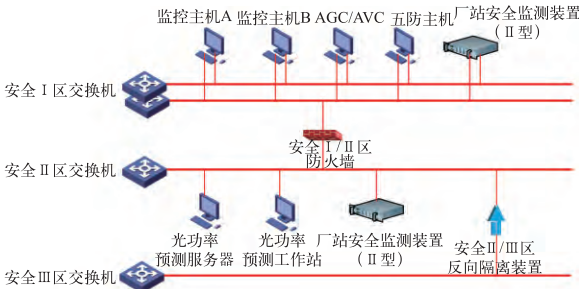


图2 部署结构图

2. 安全监测装置部署方案

(1) 部署方案总体说明

部署两台厂站安全监测装置，分别部署在安全I区 (控制区) 及安全II区 (非控制区)，每台装置负责接入本区域的主机类设备、网络交换设备 (交换机等) 和安全类设备 (防火墙、隔离装置等)。

(2) 部署结构图 (见图2)

(3) 监测装置通信关系

监测装置通信接口关系见表1，监测装置布置图如图3所示。

表1 监测装置通信接口关系

通信区域	通信对象	通信接口	通信方向	通信规约类型
站控层	主机类设备	网口	双向	基于TCP的国网定义私有规约
	网络交换类设备	网口	双向	SNMP V3、SNMP trap
	安全类设备	网口	单向, 从安防设备到安全监测装置	Syslog
主子站	内网安全监管平台	网口	双向	基于IEC104的扩展规约; 基于TCP的国网定义私有规约

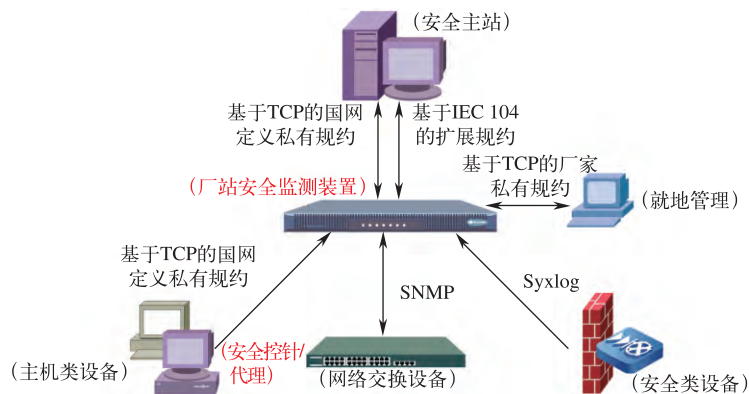


图3 监测装置布置图

(4) 安全监测装置接入设备 (见表2)

表2 安全监测装置接入设备

设备类型	设备名称	设备型号	接入难度评估
主机	后台监控主机A	PRS7000	部署探针后接入
	后台监控主机B	PRS7000	部署探针后接入
	五防操作系统主机	czpnet	部署探针后接入
	AGC/AVC服务器	PRS7000	部署探针后接入
	光功率预测通信管理机	PRS-7910	部署探针后接入
	通信管理机	PRS-7910	部署探针后接入
	远动机主	PRS-7910	部署探针后接入
	远动机备	PRS-7910	部署探针后接入
	光功率预测服务器	PRS7000	部署探针后接入
	光功率预测工作站	Windows7	部署探针后接入
网络设备	站控层交换机1	PRS-7961B	研判是否需升级
	站控层交换机2	PRS-7961B	研判是否需升级
	站控层(高压室)交换机1	PRS-7961B	研判是否需升级
	站控层(高压室)交换机2	PRS-7961B	研判是否需升级
	站控层环网交换机	IES6116-4F*2	研判是否需升级
	Ⅱ区交换机	H3C S3600V2	研判是否需升级
安全设备	I/Ⅱ区隔离防火墙	DPtech-FW1000-MA-AD	研判是否需升级
	Ⅱ/Ⅲ区反向隔离装置	SysKeeper-2000	研判是否需升级

(5) 工程实施步骤

1) 根据现场实际情况进行组网规划：主要用于明确装置具体部署的位置；分配交换机、安防设备的IP地址，用于和装置通信；敷设相应的通信网线

(主要用于装置本身对外通信)。

2) 如果站控层有SNTP对时源，建议采用SNTP对时；否则就采用B码对时，这时需要放B码的对时线。

3) 安装厂站安全监测装置和本地管理单元。

4) 安装配置监控主机和网关机的安全探针软件。

5) 完成交换机接入工作：对于满足国网规范事件报文的交换机设备，配置启动SNMP协议及通信参数；对于不满足规范的，根据现场实际交换机的型号及版本，由业主决定是否升级交换机的程序或者更换交换机。

6) 开放安全设备的Syslog接口：对于满足国网规范事件报文的防火墙、正反向隔离设备，将对应的Syslog功能打开，并配置为预先分配好的IP地址；对于不满足规范的，根据现场实际安全设备的型号及版本，由业主决定是否升级程序或者更换交换机。

7) 现场接入和主子站调试：将现场的服务器主机、安防设备和网络设备配置到装置中，核对信号，同时与主站核对信号。

8) 用户验收、培训，投入运行。

3. 部署方案的风险评估及应对措施

新布置网络安全监测装置对已经运行的监控、远动等业务没有交互，基本上都是网络数据监测，因此对运行系统的影响较小，但是由于涉及主机设备的探针布置、参数修改及重启，以及交换机的升级和更换，故需针对可能受影响的设备进行逐一分析并列举应对措施。部署方案的风险识别及应用措施见表3。

表3 部署方案的风险识别及应用措施

序号	风险识别	应对措施
1	本次进站工作涉及范围较宽,涉及设备较多,存在工作范围的风险	1) 明确工作范围,防止走错屏柜和间隔,防止误操作设备 2) 明确工作内容,防止错误操作
2	主机需要布置安全探针并配置参数等,可能需要重启主机等操作	操作前做好备份,对有冗余的主机,先操作其中一台,确保测试完毕无异常后,再操作另外一台
3	站控层交换机升级程序或者更换交换机,修改配置并重启等操作,并且现场站控层通信网络为单网,故会造成主机、网关机和保护、测控等装置短时间的通信中断	需要提前联系调度,做好主站通道数据封锁等防范
4	出站纵向加密涉及修改配置并重启等操作,故可能造成主站通信短时间中断	需要提前联系调度,做好主站通道数据封锁等防范

4. 网络安全监测装置测试方案

(1) 厂站端测试

1) 厂站端监测装置调试完毕,完成资产添加后,在确保测试环境安全的前提下,检查是否可以收到站内被监视对象上传的本地告警。

2) 进行主机、交换机、防火墙及隔离装置的接

入测试,模拟各类安全事件进行告警触发测试,验证各项采集功能运行是否正常。

3) 通过监测装置本地告警监视功能,消除站内告警信息,完善白名单配置。站内告警消除后,再接入主站管理平台。

4) 本地采集信息测试完毕后,联系主站管理平台运维人员进行联调及测试。

(2) 主站端测试

厂站端测试完成后,在确保测试环境安全的前提下,厂站端模拟各类安全事件进行告警触发上传测试,主站端验证各项采集信息是否完整、准确。

主站管理平台针对采集信息测试通过,并无告警信息,可确认监测装置接入工作完成。

(3) 日志测试表(略)

结束语

本文通过对光伏电站监控系统布置网络安全装置,大大加强了系统网络安全应用和管理手段,确保电站和电网的运行安全。EA

(收稿日期:2021-10-27)

(上接第82页)

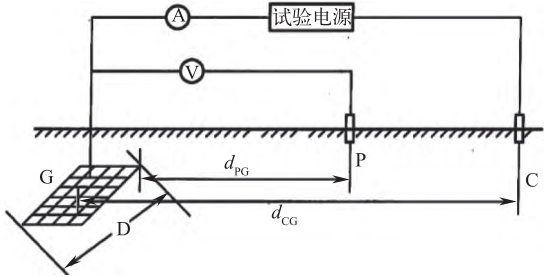


图3 直线法测试阻抗示意图

表2 某变电站大型接地网接地阻抗测量结果(直线法)

测试点	电压极位置/m	注入电流/A	测量电压/V	测量电阻值/ Ω
1	1 000	5	1.790	0.358
2	900	5	1.705	0.341
3	800	5	1.340	0.268
4	700	5	1.315	0.263
5	600	5	1.135	0.227

结果分析:通过测试,接地网接地阻抗远离夹角法测试值为 $0.46\ \Omega$,直线法测试值为 $0.263\ \Omega$,均满足标准及规程小于 $0.5\ \Omega$ 的要求。但是,考虑到变电站的地理位置及根据地质环境判断,远离夹角

法测试值更接近于阻抗真实值(其中,影响远离夹角法的因素有夹角 θ 和接地网对角线 D ,由于是采用GPS定位测量,因此可保证数据的准确性)。

结束语

大型接地网对于电力系统的安全及稳定运行有着极为重要的作用,接地网的性能好坏直接关系到电网、设备及人身安全。我国每年电网运行事故中由于接地网的缺陷或不良引起的事故占比在30%以上。由于电力系统事故造成停电带来的经济损失巨大,因此,定期对大型接地网的安全性进行评估至关重要。大型接地网的安全性指标中,接地阻抗是衡量接地网性能最基本的特性指标,但不是唯一指标。随着电网和计算机技术的发展,对接地网的安全性状态进行评估是接地网全周期管理的重要手段,通过实测和数值分析相结合,可利用接地分析软件(如CDEGS软件),对接地网的安全性状态进行全面分析评估。EA

(收稿日期:2021-10-09)