巫溪县农光互补光伏发电项目（一期）

35kV 送出线路及升压站改造工程

网络安全防护设备技术规范

重庆三峡水利电力建设有限公司

2026 年 9 月

目　录

1　总则 1

1.1　一般规定 1

1.2　投标方应提供的资料文件 1

1.3　工作范围和进度要求 1

1.4　技术资料 1

1.5　标准和规范 1

2　项目概况 2

3　供货需求一览表 2

4　技术要求 4

4.1　入侵防御装置 4

4.2　终端防护系统 4

4.3　日志审计装置 5

4.4　II型网络安全监测装置 5

4.5　网安管理工作站 6

4.6　工业防火墙 6

4.7　便携式运维网关 7

4.8　电力监控系统专用调试终端 8

4.9　主机加固 8

5　验收及技术培训 9

5.1　验收 9

5.2　技术培训 9

6　技术服务 9

设置格式[作者]: 字体颜色: 自动设置

1　总则

1.1　一般规定

1.1.1　投标方须仔细阅读包括本技术规范在内的招标文件阐述的全部条款。投标方提供的网络安全防护设备应符合招标文件所规定的要求。

1.1.2　本招标文件标准规范提出了对网络安全防护设备技术上的规范和说明。

1.1.3　本招标文件提出的是最低限度的技术要求，并未对一切技术细节作出规定，也未充分引述有关标准和规范的条文，投标方应提供符合本招标标准规范引用标准的最新版本和本招标文件技术要求的全新产品。如果所引用的标准之间不一致或本招标文件所使用的标准与投标方所执行的标准不一致时，按要求较高的标准执行。

1.1.4　如果投标方没有以书面形式对本招标标准规范的条文提出差异，则意味着投标方提供的产品完全符合本招标文件的要求。如有与本招标文件要求不一致的地方，必须逐项在技术差异表中列出。

1.1.5　本招标标准规范将作为订货合同的附件，与合同具有同等的法律效力。本招标标准规范未尽事宜，由合同签约双方在合同谈判时协商确定。

1.1.6　本招标标准规范中涉及有关商务方面的内容，如与招标文件的商务部分有矛盾时，以商务部分为准。

1.1.7　本技术规范中所有款项都为实质性要求，若未响应，作否决处理。

1.2　投标方应提供的资料文件

投标方应按以下内容和顺序提供详实投标资料。如果资质不满足要求、投标资料不详实、严重漏项将导致废标：

1）　投标方应建立了完善的质量保证体系，具备相应的资质及良好售后服务保证体系。

2）　填写技术规范中的项目单位技术差异表。

1.3　工作范围和进度要求

1.3.1　本招标标准规范仅适用于巫溪县农光互补光伏发电项目（一期）网络安全防护设备的设计、制造、试验、包装、供货和服务等技术要求。

1.3.2　交货时间如有延误，卖方应及时将延误交货的原因、后果及采取的补救措施等向买方说明。

1.4　技术资料

设备交付时应提供以下资料：

1）　产品正确完整的中文技术手册及使用说明书。

2）　产品合格证。

3）　装箱清单。

1.5　标准和规范

除招标标准规范和图纸中要求的技术条件外，卖方还将再次确认下表标准的最新版本（以文字形式通知买方），并遵照最新标准要求执行，将最新标准通知买方。

标 准 和 规 范 表

序号	标　准　号	标　准　名　称
1		中华人民共和国电力法
		中华人民共和国网络安全法
2	中华人民共和国国务院令第 115 号	电网调度管理条例
3	国能安全〔2015〕36 号	电力监控系统安全防护总体方案
4	GB/T 36572-2018	电力监控系统网络安全防护导则
5	DL/T 5003-2017	电力系统调度自动化设计规程
6	国能发安全〔2023〕22 号	防止电力生产事故的二十五项重点要求

7	GB/T36047-2018	电力信息系统安全检查规范
8	国家发改委令 2024 第 27 号	电力监控系统安全防护规定

注　上述标准是招标方最低要求。除此标准以外，投标方可以推荐其他标准，但事先必须通过招标方认可，或选择其中较高标准。

2　项目概况

巫溪县农光互补光伏发电项目于 2024 年 8 月建成投运。根据三峡水利调控中心接入的相关要求，电站目前已部署调度数据网纵向加密认证装置及生产控制大区与信息管理大区之间的正、反向隔离装置，基本满足调度数据网通信安全要求。

目前电站电力监控系统在生产控制大区层面仍存在明显的安全防护短板：缺乏入侵检测、恶意代码防护、日志审计等必要的网络安全监测与审计手段，主机系统未按照最新要求进行安全加固，资产台账及网络拓扑管理尚不完善，整体安全防护能力难以有效应对日益严峻的网络安全威胁。

按照《中华人民共和国网络安全法》《电力监控系统安全防护规定》（国家发改委令 2024 年第 27 号）及《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）等法律法规和行业标准要求，电力监控系统应满足等级保护二级及以上安全防护能力要求。电站近期将开展电力监控系统等级保护测评工作，现有防护体系存在较多高风险项，亟需补充完善。

为此，本项目将采购电力监控系统网络安全防护设备，并对现有主机进行安全加固，同步完成资产梳理、标识标签完善、网络拓扑图绘制及安全防护实施方案编制报审等工作。项目实施后，将构建安全防护、监测审计与运行管理的纵深防御体系，全面提升电站电力监控系统网络安全防护水平，满足等保二级测评要求，保障电站安全稳定运行。

3　供货需求一览表

序号	名称	规格	单位	数量	备注
1	入侵防御装置	国产化多核硬件平台和国产操作系统，网络层吞吐量≥10G，IPS 吞吐≥1.5G，并发连接≥350 万，每秒新建连接数≥8 万；标准 1U 机箱，双电源，4TB 硬盘；配置≥8 个千兆电口（支持 3 组 bypass），≥4 个千兆光口，≥2 个扩展插槽，1 个 Console 口，2 个 USB 接口；含两年入侵防御特征库升级服务和硬件维保服务。	台	2	
2	终端防护系统	千兆网口≥6 个，内存≥8GB，硬盘≥1TB。含三年病毒库升级更新	台	1	
3	日志审计装置	千兆电口≥8 个，千兆光口≥4 个，内存≥16G，硬盘≥4T，授权资产数≥45 个，数据平均处理能力≥1500EPS	台	1	
4	II型网络安全监测装置	千兆电口≥8 个，USB 口≥1 个，本地日志审计记录条数≥10000 条	台	2	
5	网安管理工作站	国产网安工作站，国产 CPU、国产安全操作系统；内存≥16GB，存储≥512GB，含 1 套 KVM。	台	2	
6	Agent 探针	含电量采集终端 WFET-3000、故障录波 PCS-996、后台监控机等设备探针	套	9	

设置格式[作者]: 字体颜色: 自动设置

7	国产安全操作系统	银河麒麟/麒麟信安服务器版操作系统	套	4	
8	工业防火墙	国产化 CPU 芯片+国产操作系统，标准 1U 机架式，标配双电源，≥6 个千兆电口，≥2 个扩展槽，≥8G 内存，≥64GmSATA,带风扇；网络吞吐量≥4Gbps，最大并发连接数≥50 万，每秒新建连接数≥3 万，应用吞吐量≥500Mbps ，支持 OPC ,Modbus TCP，Siemens S7 等工控协议的深度报文解析，支持白名单自学习，内置工控威胁漏洞库，基础防火墙等功能。	台	1	
9	电力监控系统专用调试终端	国产化 CPU 芯片，国产化操作系统，CPU 核心数≥8 核，线程数≥8 线程，主频≥2.2GHz，内存≥16GB，硬盘≥512GB，千兆网口≥1 个，USB 口≥2 个	台	1	
10	电力监控系统专用移动存储介质	国产 256GB，读速≥1000MB/S，写速≥800MB/S	个	1	
11	便携式运维网关	便携式设计，采用国产化 CPU 芯片及操作系统，配置 10 寸触摸屏，屏幕分辨率不低于 1280 x 800；配置 4 核心处理器，系统内存≥6GB，硬盘≥1TB；≥2 个网口，≥1 个专用管理口，≥2 个 RS232 串口，≥5 个 USB 接口，≥2 个 HDMI 接口；内置指纹识别模块，LED 告警灯，支持扬声器	台	1	
12	屏柜及配套辅材	2260*800*600，Z42，右门轴	面	1	
13	主机加固	设备安装调试、光伏电站电力监控系统主机加固、网监接入服务（包含业务系统厂家调试）、标识标签完善、网络拓扑图绘制、安全防护实施方案编制报审	项	1	

注：1、投标方需完成设备的安装调试及联调工作。

2、投标方需提供光伏电站主机设备探针，将主机设备、网络设备及安全设备接入网络安全监测装置，建立网络安全监测预警机制，建立基于内置探针等的网络安全监测手段，实时监视分析电力监控系统网络安全运行状态及可疑行为告警。应提供探针国产化及兼容性证明材料，包括但不限于第三方权威机构出具的检测报告或生产厂家承诺函。

★3、投标方需提供光伏电站电力监控系统后台及故障录波等装置配套探针及现场服务，相关业务系统厂家配合费用应包含在投标总价中。

★4、投标方供货的设备须满足国产自主可控要求并提供相关证明文件，包括但不限于第三方权威机构出具的检测报告或生产厂家承诺函。

★5、投标方供货的设备完全满足本招标文件全部技术参数要求，招标方有权对到货实物开展现场功能核验测试，若实物功能、性能与招标参数不符，视为不满足招标要求，按中标违约处理。

6、投标方需完成光伏电站主机安全加固工作，并出具加固报告。项目实施期间，若存在主机加固异常问题，投标方应负责进行整改。

7、投标方需完成光伏电站电力监控系统资产梳理、标识标签完善工作。

8、投标方需交付最终版网络拓扑图、标准化完整资产台账，台账应明确设备名称、IP 地址、账号密码等情况。

删除[作者]: 设备

9、投标方需交付最终版光伏电站电力监控系统安全防护实施方案编制，并配合招标方报送上级调度机构审核。投标方应完成供货范围涉及的等保测评问题整改。

★10、中标方应在合同签订前提供光伏电站电力监控系统后台厂家（南瑞继保）针对本项目出具的技术支持函。

★11、中标方应在合同签订前提供网络安全防护设备制造商针对本项目出具的授权书或售后服务承诺函。

4 技术要求

4.1 入侵防御装置

1） 采用国产化 CPU 芯片和国产操作系统，网络层吞吐量≥10G，IPS 吞吐≥1.5G，并发连接≥350万，每秒新建连接数≥8 万；标准 1U 机箱，双电源，4TB 硬盘；配置≥8 个千兆电口（支持 3 组 bypass），≥4 个千兆光口，≥2 个扩展插槽，1 个 Console 口，2 个 USB 接口，无液晶屏；含三年入侵防御特征库升级服务和三年硬件维保服务。（提供相关证明文件及）

2） 支持分析识别流量中包括的具体协议类型，包括：ICMP、HTTP、FTP、SNMP、TELNET、SMTP、POP3、IMAP、 NFS、 SMB,、NETBIOS 等, 对 ICMP、 HTTP、 FTP、 SNMP、 TELNET、SMTP、 POP3、IMAP、 NFS、SMB、NETBIOS 流量进行统计;能够对 IPv6 基础协议(ICMPv6)进行识别和统计。（提供 CMA/CNAS 认可检测机构出具的检测报告关键页证明并加盖制造商公章）

3） 支持 MPLS 流量透传，支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。

4） 支持 MTU≥9000byte 的巨型帧 Jumbo Frame。

5） 支持基于 Flood 攻击和恶意扫描的的流量自学习能力，可自定义开始时间、学习时长、查看学习结果，并根据学习结果一键生成 DDOS 防护策略。

6） 支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片、圣诞树攻击、NTP monlist 等。

7） 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；支持基于 FTP、HTTP、HTTPS、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护。

8） 支持拦截流量监听与劫持攻击、错误及弱配置攻击、脆弱性利用攻击、木马攻击、拒绝服务攻击，拦截率不低于攻击事件集的 30%，并能记录入侵拦截入侵的相应攻击行为。（提供 CMA/CNAS 认可检测机构出具的检测报告关键页证明并加盖投标人公章）

9） 支持自定义 TCP、UDP、HTTP/HTTPS 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配。

10） 支持发现并拦截经过躲避处理的攻击行为，如 IP 报文碎片、TCP 报文碎片、协议端口重定位、代码变形，且入侵躲避下降率均不大于 25%。（提供 CMA/CNAS 认可检测机构出具的检测报告关键页证明并加盖投标人公章）

4.2 终端防护系统

1） 2U 机架式设备，采用国产 CPU，国产安全操作系统；内存≥8GB，硬盘≥1TB；千兆网口≥6 个；冗余电源配置。含三年病毒库更新升级。

2） 客户端应支持主动监测恶意代码，具备手动和自动处置查杀的功能；支持特征码检测技术，实

现已知恶意代码的查杀；支持行为判断分析技术，实现未知恶意代码的查杀；支持针对主机系统内核、文件、网络等多点监测，识别病毒、木马、蠕虫等恶意代码的行为；应具备按需配置扫描进程对主机资源占用率的功能；应支持开机自启动功能。

3） 客户端应具备对恶意代码的清楚、隔离、信任以及还原等处置方式；应支持自动处置与手动处置；应具备处理结果以日志方式存储和上报功能，本地日志存储应至少保留 6 个月，日志应包含事件日期时间、恶意代码文件、宿主文件、进程等对象的路径和文件名称、恶意代码名称及处置结果；应支持将恶意代码样本文件加密上报防恶意代码客户端管理模块。

4） 客户端应支持展示客户端软件版本和特征库版本，如有独立查杀引擎版本应支持展示；应支持特征库、客户端软件独立更新，宜支持查杀引擎独立更新；应支持接受管理模块的任务下发、集中配置、恶意代码库更新；应关闭主动更新特征库、策略和软件的功能；应具备卸载授权机制；主机客户端恶意代码查杀引擎应安全可控。

5） 客户端管理模块应能根据业务系统特点制定恶意代码扫描及处置策略，设置主要扫描的文件类型，订制扫描计划并同步分配策略；应能够设置在不影响业务正常运行或者业务空闲的情况下定期进行扫描；应能够设置访问的所有本地或网络位置以及所有支持的通信协议传输信道进行扫描；应支持询问用户后处置或基于预先已设定的策略自动处置；应能够设置对隔离区文件进行删除或还原处置操作；应支持文件、软件或进程的黑白名单设置。

6） 客户端管理功能：应支持接受防恶意代码客户端管理模块的任务下发、集中配置、恶意代码库更新；主机客户端恶意代码查杀引擎应自主可控。

7） 客户端管理模块应支持多级管理模式，支持大型网络管理，各级设置不同管理权限，支持各级管理模块升级管理；应支持通过管理模块对本级所辖的每一个主机客户端的监控、配置、查询、策略下发及更新，扫描结果能够由客户端回传至本级管理模块；应支持分组管理；支持特征库的在线和离线升级更新，应支持增量升级。

8） ★产品应具备由国家计算机病毒应急处理中心计算机病毒防治产品检验实验室颁发的《网络安全专用产品安全检测证书》，在投标文件中提供证明材料。

4.3 日志审计装置

1） 1U 机架式设备；国产化 CPU 芯片及国产操作系统；内存≥16G，硬盘≥4T；千兆电口≥8 个，千兆光口≥4 个，Console 口≥1 个，USB2.0≥2 个；接口扩展槽≥2 个；冗余电源配置；授权资产数≥45 个，数据平均处理能力≥1500EPS。

2） 应支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集。

3） 应支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。

4） 应支持对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议等。

5） 应具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。

6） 应支持三维关联分析；应支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。

7） 通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。

8） 应支持双因子认证登录，双因子认证令牌支持绑定至具体用户。

4.4 II型网络安全监测装置

1） 采用国产 CPU 芯片及国产操作系统，工业级硬件架构设计，整机无旋转部件。
2） CPU 4 核不低于 1.8GHz，内存不低于 8GB。
3） 硬盘容量不低于 256GB。
4） 8 个自适应网口，1 个 B 码对时接口。
5） 双路交流电源独立供电。
6） 支持 RedHat5、RedHat6、Centos6、Centos5 等系统及国产操作系统采集 agent。
7） 采集信息吞吐量≥2000 条/s。
8） 支持监测对象数量≥500。
9） 对上传事件信息的处理时间≤0.6s，对远程调阅的处理时间≤2.5s。
10） 支持采集信息的本地存储，保存至少半年的采集信息。
11）支持上传事件信息的本地存储，保存至少一年的上传事件信息。
12） 本地日志审计记录条数≥10000 条。
13） 通过 IRIG-B 同步，对时精度≤1ms，通过 SNTP 同步，对时精度≤100ms。
14） 在没有外部时钟源校正时，24 小时守时误差应不超过 1s。
15） 平均故障间隔时间（MTBF）≥30000h。

4.5 网安管理工作站

1） 采用国产处理器（核心数≥8 核，主频≥3.0GHz）；内存≥16GB DDR4；固态硬盘≥512GB。
2） 为满足接入II型网络安全监测装置及站内局域网需要，应配置千兆自适应以太网电口≥1 个；配置 USB 接口≥2 个，其中 USB 接口≥2 个；配置显示输出接口≥1 个。
3） 预装国产安全操作系统（如银河麒麟、麒麟信安、统信、凝思等），并完成安全加固：关闭不必要的端口和服务、禁用高危账户、限制匿名访问等，满足电力监控系统主机安全要求。
4） 支持接入II型网络安全监测装置，接收并展示装置采集的网络安全事件信息，包括用户登录事件、外设接入事件、危险操作事件、状态异常事件等。
5） 支持按事件类型、时间范围、严重等级等条件进行检索和筛选，支持告警实时弹窗提醒。
6） 支持以图表、列表等形式展示网络安全态势信息，包括告警统计、趋势分析、资产状态等。
7） 支持资产信息管理功能，包括设备名称、IP 地址、MAC 地址、操作系统类型。
8） 须完成工作站与II型网络安全监测装置、站内局域网的接入调试，确保工作站可正常接收、展示和管理网络安全监测装置上送的安全事件及告警信息，并将调试结果纳入系统集成验收范围。

4.6 工业防火墙

1） 国产化 CPU 芯片及国产操作系统，标准 1U 机架式，标配双电源，≥6 个千兆电口，≥2 个扩展槽，≥8G 内存，≥64GmSATA,带风扇；网络吞吐量≥4Gbps，最大并发连接数≥50 万，每秒新建连接数≥3 万，应用吞吐量≥500Mbps ，支持 OPC ,Modbus TCP，Siemens S7 等工控协议的深度报文解析，支持白名单自学习，内置工控威胁漏洞库，基础防火墙等功能。（提供相关证明，并加盖产品制造商公章）；
2） 持测试模式、工作模式，透明模式/路由模式，支持静态路由、OSPF 动态路由；
3） 支持 SNAT 和 DNAT，支持多对一正向 NAT，多对多正向 NAT，一 对多反向 NAT，多对多反向 NAT；
4） 支持工控协议的深度解析不少于 30+（包括但不限于 Modbus RTU，Modbus_UDP，Modbus_TCP，OPC DA，OPC UA，Siemens S7，S7-Plus，ENIPTCP，ENIPUDP，ENIPIO，IEC104，DNP3，MMS，Profinet，PNRTDCP，GOOSE，SV，BacNet，Omron Fins，MQTT，CCLINK，GDW273，profinetCBA，SCNet，SONet，EGD，RSSP-I，SINEC-H1，PROFIBUS-DP，MELSEC，Mewtocol，TRDP 等）；可实现协议的指令级解析和控制；

5） 支持 FTP、MMS、S7、IEC104 等协议文件还原，能够还原协议流量中传输的文件进行审计；
6） 支持 RTP，RTSP，ONVIF，SIP 等视频协议的深度解析；支持 GTP-C，GTP-U 等移动网络通信协议的深度解析；
7） 支持基于 IP 会话限制网络通信建立的连接数/连接速率；支持端口流量异常检测，包括端口流量（报文速率）突变，超过阈值（流量超过预警值），长时间无报文等；）
8） 支持拓扑显示、编辑等功能，支持自定义设备分组，自定义设备类型，设备所属分组，设备标识图片等，并支持保存和导出；
9） 支持通过配置开启自身的安全防护，支持安全区域的 DDOS 攻击防护，包括包括 SYN、UDP、ICMP、PingOfDeath、WinNuke；
10） 为保障产品的可靠性与稳定性，产品制造商须具备软件工程能力成熟度集成模型 CMMI 五级认证证书、ISO28000 供应链安全管理体系认证证书，（提供相关的证书复印件并加盖产品制造商公章）
11）为保证产品网络安全防护能力，制造商须为中国国家信息安全漏洞共享平台（CNVD）用户组（工业控制）成员。（提供相关官网截图证明加盖公章或查询网址证明）

4.7 **便携式运维网关**

1） 采用便携式设计，采用国产化 CPU 芯片及国产操作系统，配置 10 寸触摸屏，屏幕分辨率不低于 1280 x 800；配置 4 核心处理器，系统内存≥6GB，硬盘≥1TB；≥2 个网口，≥1 个专用管理口，≥2 个 RS232 串口，≥5 个 USB 接口，≥2 个 HDMI 接口；内置指纹识别模块，LED 告警灯，支持扬声器；（提供相关证明并加盖制造商公章）
2） 支持网关使用账号密码登录系统，并进行暴力破解保护；支持网关使用账号密码+指纹登录系统；
3） 支持与集中管控系统进行对接；支持将网关中记录的日志向集中管控系统上报，包括文件传输记录、屏幕及图像记录、通信报文记录、风险管控记录、接口使用记录等；
4） 支持运维终端管控，开启运维终端管控后，运维过程中所接入的运维终端需要经过运维网关管理员授权才可执行运维任务；
5） 支持移动介质管控，开启移动介质后，所有接入的网关的移动介质均需要经过运维网关管理员授权才可进行接入；支持便携式运维网关集中管理系统规则拉取设置，支持全部接收、全部拒绝、部分接收；
6） 支持对运维人员进行管理，支持提前录入运维人员信息且支持运维过程中输入的运维人员信息纳入管理；
7） 支持对病毒文件进行离线升级并展示升级记录；支持从便携式运维网关集中管控系统拉取病毒库升级包升级；
8） 支持 Tcp/Udp 端口扫描防御、ARP 扫描防御，并可自定义开启和关闭；
9） 支持 DOS 攻击防御，Syn flood、Udp flood、ICMP flood、ICMP 超长包防御、DNS flood 防御；WinNuke 防御、Smurf 防御、Land 防御、Teardrop 防御（提供功能截图并加盖制造商原厂公章）；
10） 支持将运维任务设置为运维任务模板，便于对新增任务信息的自动填充；支持从工作票 SFTP 服务器同步 E 文件，根据 E 文件内容自动新增任务；
11）支持监控在运维过程中运维电脑的操作情况并保存为 MP4 文件；支持短视频合并；支持操作记录导出 PDF 和视频；支持高危操作在视频播放中的定位和提示（提供功能截图并加盖制造商公章）；
12） 支持免工具直接运维，包括 XDMCP、VNC、RDP、SSH、telnet、FTP 协议的直接运维；
13） 产品应具有中国电力科学研究院有限公司出具的合格型式检测报告（提供检测报告复印件并加盖制造商公章）

14） 所选产品应具有国家输配电安全控制设备质量检验检测中心出具的型式检验报告（提供检测报告复印件并加盖制造商原厂公章）

15） 所选产品具备国网电力科学研究院有限公司实验验证中心(PAL)《自动化产品电磁兼容检验合格注册备案证书》、《电力自动化产品型式检验合格注册备案证书》。(提供对应的证书复印件证明，并加盖产品制造商公章)

16） 通过国家网络与信息系统安全产品质量监督检验中心《信息技术产品安全测试证书》认证。(提供对应的证书复印件证明，并加盖产品制造商公章)

17） 所选产品应具有网络安全专用产品安全检测证书，产品类型为运维安全管理产品（增强级）（提供证书与检测报告复印件并加盖制造商原厂公章）

18） 为保障产品的可靠性、稳定性及安全性，产品制造商须具备软件工程能力成熟度集成模型 CMMI 五级认证证书、ISO28000 供应链安全管理体系认证证书，且为中国国家信息安全漏洞共享平台（CNVD）用户组（工业控制）成员（提供对应的证书并加盖产品制造商公章或查询证明）。

4.8 电力监控系统专用调试终端

1） 便携式笔记本电脑屏幕尺寸 14 英寸级或以上。

2） 采用国产处理器，核心数≥8 核，线程数≥8 线程，主频≥2.2GHz。

3） 内存容量≥16GB，类型 DDR4 或以上。

4） 固态硬盘（SSD）容量≥512GB，接口 PCIe NVMe，支持 M.2 规格。

5） 千兆网口≥1 个，USB 接口≥2 个，USB-C≥1 个，HDMI 或 VGA 接口≥1 个。

6） 预装国产桌面操作系统（64 位），支持运行常见办公套件、开发调试工具及网络管理软件。

7） 预装操作系统须进行安全加固：关闭不必要的端口和服务、禁用高危账户、限制匿名访问、启用安全启动机制，对操作系统内核及关键文件进行完整性检查。

8） 具备安全启动机制，对操作系统内核、文件系统进行完整性检查。

9） 应支持电力监控系统常用调试协议，包括 IEC 60870-5-101/104 规约、DL/T 634.5104 远动通信协议、Modbus 等，用于站内综自保护装置、网络安全监测装置等设备的现场调试与联调。

10） 应支持串口通信调试（RS-232/RS-485），配置 USB 转串口适配器或原生串口接口，满足对时装置、规约转换器等设备的现场配置需求。

11）应支持网络抓包与协议分析功能，预装主流网络调试工具（如 Wireshark、Tcpdump 等开源工具或国产等效工具），支持对调度数据网及站内局域网通信报文进行捕获和分析。

4.9 主机加固

根据国能安全[2015]36 号《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》、公通字[2007]43 号《关于印发信息安全等级保护管理办法的通知》、重庆市调〔2018〕40 号《关于印发重庆电网电力监控系统清朗有序安全网络空间创建活动实施方案的通知》等要求，应对电力监控系统主机进行安全加固。

主机加固后接入调度数据网各系统不得出现异常告警、异常访问等，否则加固方应承担所有责任以及向上级主管部门说明情况，并解决出现的问题。

主机加固后出具上级认可的加固报告。

主要内如下：

1） 卸载无关软件，按最小安装原则，卸载与生产业务工作无关的软件，尤其是具有自动监听端口或对外发送垃圾网络报文行为的无关软件。

2） 关闭未用端口，综合采用删除驱动，物理封闭等措施关闭主机 USB 接口，光驱设备等硬件接口，关闭计算机中未用的网络接口和串口。

3） 关闭主机不必要的网络服务，主机仅安装和开启必要的服务，禁止与监控系统无关的服务开启，

禁用或关闭 E-MAIL.WEB.FTP.TELNET.DHCP.SNMP V3 以下版本 SMB 等通用网络服务或功能。

4） 无效程序行为，消除业务系统或功能设计缺陷，取消无价值的程序行为。

5） 关闭私有监听口，关闭业务系统不使用的私有网络监听端口。

6） 删除默认路由，添加主机路由。合理设置主机路由，按业务需求配置明细路由，避免使用默认路由。

7） 停用与业务无关的进程。逐一检查持续运行或周期运行的进程，及时消除用于调试、测试等与正常运行无关的进程。

8） 关闭程序自动更新。关闭输入法、防病毒等应用软件的互联网更新服务。

9） 消除弱口令。操作系统账号应按实名制要求建立，并采用复杂口令。

5 验收及技术培训

5.1 验收

1） 现场验收

现场验收在系统安装调试及高中风险漏洞修复完成后开始，现场验收除对功能及安全漏洞风险作进一步的测试外，还要对系统的稳定性进行测试。验收合格后，由双方人员签字，随后进入质保期。

2） 验收标准

系统将是由招标方与中标人双方共同进行验收，主要分以下几个方面分阶段进行：

（1）设备单项验收包括对设备名称、规格、型号、数量、外观、包装、完整性、技术资料等进行验收。

（2）设备自检验收自检结果符合合同及技术规范规定。

（3）系统集成验收：验收安装调试是否完成，调度数据网是否连通，网络安全防护系统是否连通等。

（4）网络安全验收：按照二级系统要求提交系统漏洞扫描和渗透测试等网络安全测试报告，需无高中安全漏洞风险。

5.2 技术培训

对招标方指定人员进行现场使用培训及维护培训，使招标方指定人员在实际的工作中能够分辨出系统中存在的问题，提高对网络及安全设备使用及维护能力。要求投标方提供相应的培训资料。

培训内容：

介绍系统的接线和安装等要求。掌握系统设备面板显示灯的意义。熟悉设备的启动和关机。了解设备的安全操作规范、条例。对一般性故障进行诊断、定位、排除和恢复的方法。

掌握故障报警、事故报警的处理方法等。

6 技术服务

1） 软件产品、硬件产品质量保证期自工程完工验收合格之日起至少 2 年。质保期内服务：质保期内免费提供质保服务，包括软件、硬件、系统日常维护、故障维修、设备更换等相关服务。

2） 合同签订后，投标方应指定负责本工程的项目经理，负责协调投标方在工程全过程的各项工作，如工程进度、设备包装运输、现场安装、调试验收等。

3） 随设备发货向招标方提供 1 份。开箱资料应包括运行使用说明书、装配图和安装说明书及其他满足安装、调试、生产运行所需要的资料。

4） 设备在现场安装时，投标方应派技术人员到现场进行柜内设备安装和调试，负责解决设备在安装调试、试运行中发现的制造及性能等方面的有关问题，同时负责与其他设备的接口及现场的验收等。

5） 在质保期内，因制造问题而发生损坏，或不能进行正常工作时，投标方应免费为招标方更换部件（质保期按照招标文件的有关规定）。

6） 质保期内，如设备在使用中发生问题，投标方应在接到通知后 1 小时内答复，如客户要求或系统出现严重故障或重大安全漏洞时，须 5 小时内到达现场处置。

7） 附　录　A 技术偏差表

技 术 偏 差 表

投标方名称：_____

序号	项目	招标技术文件要求	差异	备　注