



透明感知和自主决策的城市配电数字孪生系统建设
(低碳高可靠城市配电系统示范工程课题 5 配套)

OS2 省、地级主站基础软硬件

招标技术规范书

广州供电局系统运行部

2025 年 10 月



目 录

1 总则	1
1.1 总体说明	1
1.2 投标须知	1
1.3 工程实施要求	3
1.4 技术应答要求	5
2 应遵循的主要标准	6
3 技术要求	8
3.1 基本要求	8
3.2 硬件配置要求	8
4 验收	24
5 包装、运输、贮存和质量保证	25
6 双方工作安排	26
6.1 招标方职责	26
6.2 投标方职责	27
6.3 项目管理	27
6.4 资料管理	27
6.5 技术（设计）联络会	28
6.6 安装调试	28
6.7 培训	28
6.8 现场服务及售后服务	28
7 订货范围	29
附件一：设备需求一览表	30
附件二：技术差异表	31

1 总则

1.1 总体说明

1) 本技术规范书适用于广东电网有限责任公司广州供电局（以下简称“招标方”）透明感知和自主决策的城市配电数字孪生系统建设（低碳高可靠城市配电系统示范工程课题 5 配套）项目的硬件部分，本技术规范书的最终解释权归广东电网有限责任公司广州供电局；

2) 本技术规范书提出的系统建设目标、需求及技术要求等，可供具备所要求资质参与投标的供应商（简称“投标方”）编写投标文件之用；中标的投标方简称“中标方”，系统的最终用户为广东电网有限责任公司广州供电局电力调度控制中心（以下简称“用户方”）；

3) 本次招标的中标方应提供所中标系统的供货、安装、集成、调试及技术服务，负责在系统中集成招标方采购的第三方硬件和软件产品（如有），并协助相关的建设工作。

4) 双方项目违约的处罚将在合同谈判中明确。

1.2 投标须知

1) 本招标书中提出的仅为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，投标方应提供符合相关标准和本技术规范的产品。本技术规范所使用的标准如与国家、行业、公司以及投标方所执行的标准不一致时，按要求较高的标准执行。

2) 投标方应仔细阅读包括本招标书在内的招标文件的所有条款，并根据招标书中的要求和范围进行技术方案的设计，其提供的产品及技术方案应满足招标文件所规定的所有技术要求及网络安全要求。投标方也可推荐能满足招标文件要求的类似的或更优的产品和方案，但投标方必须详细标明技术差异（附件二）。

未在技术差异表中说明的条款意味着投标方认可其所提供的产品及服务等相应部分完全符合或高于本技术规范相应的要求，投标方中标后除非经过招标方书面同意，否则不得以任何理由提供低于本技术规范要求的相应的产品及服务等。

3) 对于本招标书未提出但应标系统已具有的功能及技术性能指标，投标方可在其技术建议书中加以补充说明，并提供相关技术资料。如果投标方认为本招标书所描述的功能、接口、性能等要求与目标系统要求有所不一致或部分要求不合理，可在响应原要求后给出建议方案。

4) 对于应标系统中尚不具备或未达到相关要求的功能或性能，投标方在应答时须针对该项如实说明。投标方认为相关要求不合理的，应给出充分理由及合理的建议。投标方认为相关要求需要在现有产品基础上进一步实现或完善的，应给出实现相关技术要求的方案和进度计划。

5) 投标方提供的技术应答内容至少应包括技术方案(包括功能实现方案、性能指标等)、软硬件配置、工程计划(包括工程进度计划、技术（设计）联络会、技术培训计划)等。

6) 投标方应在技术建议书中具体说明所建议的技术方案、软硬件配置符合的有关标准(包括国际、国内标准和专用标准)，并附上相应的说明和技术资料。投标建议书中的每个硬件和软件的型号/部件号必须逐一说明。对每个单项产品，投标方必须提供原厂商的正式技术指标说明材料。投标方认为需特殊说明的部分应附有详细的技术资料，否则由于评标理解的不同，产生的后果由投标方负责。

7) 投标方提供的产品必须是标准的，技术上是成熟的，所有产品应是全新的，具有先进结构，并能在中国境内安全使用(包括软件产品必须具有在中国境内的合法使用权)，符合环保要求。

8) 投标方应依据本技术规范的要求及推荐的技术方案提出详细的产品配置和报价清单，招标方现有相关系统（如有）的图形、参数、历史数据、报表的录入和导入由投标方负责，投标方不再收取任何费用。

9) 投标方的报价清单中，如果投标所采用商用软件为开源，应进行标注说明，且不必报价（报价填报应为零）；如果投标方采用开源商用软件进行投标且

进行了报价，所产生后果由投标方负责，且签订物资采购合同（若中标）时本项报价按照“0”处理。

10) 投标方的投标文件应以中文简体编写(原厂商的资料可为英文)，所有的计算、说明和图纸等均应采用国际单位。投标方应保证对本次招标的所有技术说明文件保密，在招标前和招标后不得向其他单位公布招标项目单位的有关材料。

11) 本招标书的解释权属于招标方。未经招标方同意，任何个人和单位对招标书所作的任何修改均无效。在未经双方商定作为订货合同技术附件之前，招标方保留对招标书进行修改的权利，投标方可以提出变更的意见和建议。招投标双方签订合同之后，招标方有权提出和投标方有责任接受因国家、行业、上级主管单位等的规范、标准和规程等发生变化及与相关系统接口要求改变所产生的一些补充要求。具体事项由招投标双方共同商定。

12) 本招标书在内容或技术指标上如果存在错误(包括拼写、印刷错误)，投标方应及时提出并要求招标方澄清，经招标方确认后对错误内容进行修正。

13) 针对本次招标的一切有效的书面通知、修改及补充，都是招标文件不可分割的部分，与招标文件具有同等法律效力。

14) 招标书经招投标双方确认后作为合同的附件，与合同正文具有同等的法律效力。本招标书的未尽事宜，由招投标双方在合同技术谈判时协商确定，或以其它形式补充。

1.3 工程实施要求

投标书应针对如下工程实施要求逐项进行确认和应答。

1) 本项目主要供货范围包括透明感知和自主决策的城市配电数字孪生系统建设（低碳高可靠城市配电系统示范工程课题 5 配套）的硬件部分，投标所采用产品及服务必须完全满足招标规范要求。请投标方确认。

应答：

2) 运杂费、保险费用应包含在设备报价中，中标方应根据项目建设要求分

批次供货，并负责将设备发运至采购方指定的最终用户现场所在地，中标方需保证供货设备的完整性、及时性。中标方应负责所供货设备在正常使用条件下的质保工作。请投标方确认。

应答：

3) 中标方应负责所供设备（包括本项目中标方提供的设备和本项目套用框架招标的设备）的安装（含设备上架）、调试、接线(包括柜内跳线及柜间跳线)，会议及技术培训在内的技术服务，其中安装调试工作包含工厂集成安装调试服务及用户现场安装调试服务，相应费用均应包含在设备报价中。中标方应积极配合项目建设工作，与集成方、施工方积极配合，如因中标方原因或配合不力造成的一切损失，均由中标方负责。请投标方确认。

应答：

4) 中标方应保证所供设备间兼容性良好，保证所供设备与其他软硬件供货商、系统集成商产品兼容性良好；若发生所供设备与其他软硬件供货商产品兼容性不良的情形，应限期内免费调换。若因中标方供货产品影响工期情形，中标方应承担相应责任并赔偿项目单位及软件供货商损失。请投标方确认。

应答：

5) 根据工程建设需要，招标方有权利在招标过程中及招标后调整设备配置要求，投标方不得以停产、缺货、供货周期长等各种原因拒绝招标方合理的技术修改要求。请投标方确认。

应答：

6) 本项目为工程化项目，针对项目建设，投标方应在投标书中详细标注出各投标产品功耗及使用条件，投标方应提供安装、组屏、设备间接线、综合布线、机房环境、基础环境等方面的建议及要求；在中标后应提供的设备运输、搬运、

安装、调试、设备上架、组屏、设备接线方面的工作，并提供详细的施工方案及施工图纸。

应答：

7) 投标方应给出完整的建设团队组织结构和人员配置，投标方应保证最少 5 人的工程技术支持与服务团队专门为本工程项目服务。请投标方确认。

应答：

8) 本项目建设涉及广州电网核心调度业务系统，在项目实施过程中所涉及的所有数据、文档均为保密资料，项目中标方须承诺做好相应保密工作，否则因中标方数据泄密造成的一切后果由中标方承担。请投标方确认。

应答：

1.4 技术应答要求

1) 投标方提供的投标书应分为两册，分别针对商务招标书和技术招标书进行应答。其中商务投标书对商务招标书进行逐项应答，技术投标书对技术招标书进行逐项应答。

2) 投标方提供的技术投标书必须包括技术应答书和技术建议书两部分作为应答。**投标方注意：如果技术建议书内容较多，为了评标方便，应将技术建议书与技术应答书单独成册。**

3) 投标方提供的技术应答书应对技术招标书专用技术规范工程要求进行逐项应答。

4) 投标方提供的技术建议书不应是投标方投标产品的通用产品说明，应充分突出其满足或优于本招标书技术规范的技术方案。

5) 投标方在建议书中,按本招标书中所提的技术及工程要求,对涉及到的主要产品、技术及服务,提供详细的性能参数和技术说明。投标方亦可根据自己的产品技术性能具体情况,在建议书中提出建议,并附详细资料和说明。

6) 技术应答书中应提供所采用的设备清单,按附件一填写。

7) 如果投标方提供的设备与本招标书的要求有差异,应在投标书中以“技术差异表”为标题的专门章节中加以详细描述,并按附件二中指定的格式填写。

8) 投标方应随其投标书一起提供足够详细和清晰的图纸和数据,以便能够与本招标文件中的技术条款进行完整和切实的比较。这些图纸和数据应简要说明系统的设计特点,同时对与招标书要求有异或偏差之处进行准确说明。除非经招标方同意,系统的最终设计应按照这些图纸和数据的所有详细说明进行。

9) 投标书中应按附件一分项列明外购的设备(包括软件),并说明其维修服务的保障能力。

10) 投标文件中若出现相互矛盾或不一致的内容,以有利于招标方的内容为准。

11) 在必要时投标方须在招标方要求下提供应标设备的测试及演示。

2 应遵循的主要标准

除本招标书特别规定外,投标方所提供的设备均应按照国际、国家、行业、公司标准、规范、规定进行设计、制造、检验和安装。所用的标准必须是其最新版本。除非另作特别规定,所有合同设备,包括中标方从他处获得的全部设备或附件,都必须满足最新版本的相关标准,包括在投标时已生效的任何修改和补充。如果投标方选用标书规定以外的标准时,需提交与这种替换标准相当的优于标书规定标准的证明,供招标方确认。

本招标书主要引用或参照了以下标准和规范,投标的设备 and 产品应符合本技术规范及下列标准和规范的要求:

-
- 1) 《中华人民共和国网络安全法》
 - 2) 《中华人民共和国密码法》
 - 3) 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
 - 4) 《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）
 - 5) 《信息安全技术网络安全等级保护安全技术要求》（GB/T 25070-2019）
 - 6) 《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）
 - 7) 《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）
 - 8) 《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101号）
 - 9) 《电力监控系统安全防护规定》（国家发展和改革委员会令 2024 年第 27 号）
 - 10) 《中国南方电网电力监控系统网络安全技术规范》（Q/CSG 120499-2021）
 - 11) 《南方电网一体化电网运行智能系统主站标准化设计指南》（2021 版）
 - 12) 《南方电网电力监控系统网络安全全域防御与纵深防御体系建设工作方案》
 - 13) 《南方电网电力监控系统网络安全纵深防御技术原则》
 - 14) 《南方电网云边融合智能调度运行平台技术系列标准》
 - 15) 《南方电网云边融合智能调度运行平台（CEP）设计指南（2025 版）》
 - 16) 《南方电网公司生产项目准入及预算标准》（2022 年版）

以上所列的主要技术标准和规范，如未能达到国际和国内最新标准时，建设单位应使用符合最近的国际、国内标准，并提供采用的国际、国内标准、规范和所应用的最新版本的有关技术依据资料。

3 技术要求

3.1 基本要求

a) 台式计算机、便携式计算机、一体式计算机、工作站、通用服务器、操作系统、数据库等 7 类产品的采购须严格执行 7 项信息类产品政府采购需求标准，不得低于需求标准要求。CPU 芯片、操作系统和数据库等关键部件需通过安全可靠测评，其安全可靠测评等级不得低于 I 级，详情可从中国信息安全测评中心（www.itsec.gov.cn）和国家保密科技测评中心（www.nsstec.org.cn）网站查询。

b) 各类系统及设备在接口、模型、服务、协议方面兼容主流传统设备。同时应满足电力监控系统网络安全等级测试要求。

c) 系统应落实密码法要求使用商用密码，且所使用的商用密码服务或产品设备应经商用密码认证机构认证合格。

d) 服务器、交换机、工作站等电力监控系统主站设备，其相关部件需满足“全链路自主可控”要求。

e) 各类系统及设备应能提供第三方的检测报告。

3.2 硬件配置要求

3.2.1 总体要求

a) 系统硬件平台的选择应充分考虑生命周期内硬件技术水平发展及电网监控规模需要。整个硬件平台的选择应遵循以下的基本原则：

b) 硬件配置必须符合系统体系结构原理，满足系统性能和功能要求，并且符合实时性、安全性和可靠性原则；

c) 要选择标准化、开放性能好的设备。计算机和网络设备应满足不断优化、平滑升级以及投资保护的需要；

d) 应选用起点高、信誉好的厂家生产的成熟的、高质量的、先进可靠的设备，计算机、存储设备及网络设备能支持异构网络的互联，支持双网或多网运行，支持主流商用数据库；

e) 应具有较好的可扩展性、可维护性和兼容性。系统的硬件设备要选择通用标准且互换性高的产品，具有良好的开放性以及低维护成本；

f) 具有一定的先进性、超前性，但必须根据实用性原则进行优化配置，使系统达到较高的性能价格比。

g) 根据设计水平年系统的功能、性能和容量要求并考虑投运后系统生命周期发展的需要，确定计算机系统的规模并留有一定裕度，系统容量应按照设计的远景年要求配置。在《生产项目准入及预算标准》规定的设备生命周期内无需进行大规模升级改造；

h) 关键设备采用冗余配置方式，设备故障不能相互影响；

i) 所有关键设备（包括服务器、存储设备、路由器、前置交换机、主干交换机、防火墙、硬件隔离装置等）至少配置两路独立供电的电源，任意一路电源故障设备功能应不受影响；

j) 服务器采用 PC 服务器，操作系统应采用安全可靠的 Linux 操作系统。

k) 实际建设中可根据技术发展及行业采购经验，在项目设计、招标中参照本标准设计指南优化设备配置要求。

3.2.2 服务器及工作站

3.2.2.1 全闪融合存储一体机

序号	设备名称	技术要求
1	全闪融合存储一体机	原厂商产品（非 OEM），性能不低于以下要求： 1) 高度≤2U，标准机柜安装，含机架安装套件，带安装导轨等； 2) CPU：X86 或 ARM 架构，其中，X86 架构 CPU：物理核心数≥24 核，原始主频≥2.1GHz，支持超线程；ARM 架构 CPU：物理核心数≥48 核，原始主频≥2.5GHz；满足安全自主可控要求。CPU 为同一品牌型号。所有 CPU 应是同款、同一型号； 3) 内存：当前配置≥256GB DDR4，单条内存≥32GB，最大可配置≥2TB，最大内存插槽总数≥16； 4) 硬盘：（根据实际需求调整配置）：不低于 2 块 960GB SATA SSD 系统盘，12 块 7.68TB NVME SSD 读取密集型企业级硬盘，擦写寿命≥3，DWPD 3 年，

		带掉电保护功能； 5) 网卡：提供本机板载网卡，1Gbps 以上；≥3 块双端口 25Gbps 以太网卡，支持 RDMA 协议，满配 25G 多模光模块。 6) 电源和风扇：支持热插拔冗余电源，单电源供电可正常运行，支持热插拔冗余散热风扇，电源和风扇模块要求满配； 7) 支持同时提供块存储、文件存储服务，并为系统技术平台建设的文件服务、对象存储服务等 PaaS 层功能提供底层支撑； 8) 支持高性能网络 RoCE 和标准 NVMe over Fabrics 标准协议，客户端访问存储支持 NVMe over Fabrics 标准协议，存储集群互联支持 NVMe over Fabrics 标准协议。 9) 支持基于卷/RBD 的部署并实现块存储卷（RBD）的在线/离线扩容功能。 10) 可采用多副本机制保证数据可靠性，同一数据的多个副本能够分散到不同的磁盘/节点存储，各副本间保证数据的强一致性，支持多个副本的容错机制，副本数量可基于存储池灵活设置，支持分级的数据保护模式。 11) 支持主流关系型、时序型、文档型数据库、超融合数据库的计算环境与存储环境融合、稳定运行运行，支持实现数据处理时延达到微秒级别性能； 12) 支持多种虚拟化平台、云平台、k8s 的对接，提供 Cinder-iSCSI、Cinder-NVMe-RoCE、CSI-iSCSI、CSI-NVMe-RoCE 工具。 13) 对于硬盘或节点故障，在无人工干预条件下，每 TB 重构速度可控制在 1~5 分钟。 14) 在单客户端单卷场景下，4KB 随机读性能可达到 310 万 IOPS，时延低于 500 微秒（μs）。4KB 随机写性能可以达到 130 万 IOPS，时延低于 500 微秒（μs）。 15) 支持纠删码方式保证数据的可靠性。集群节点或者硬盘故障后的数据重构，在集群中算法保障有一定数量节点或者硬盘故障时，系统可正常使用，数据不丢失。 16) 管理维护简单易用，能够对存储基础架构进行集中的配置，如存储资源池、集群、集群节点、磁盘等资源进行合理的划分和配置，通过配置向导功能，保障存储配置的简易性和准确性。 17) 提供存储集群管理工具，对各个存储节点服务器进行统一的监视和管理。同时支持 CLI 命令行工具，最大化管理效率。提供全闪存储资源告警：容量超阈值告警，系统内节点、磁盘故障告警。 18) 系统管理软件：标配且带无限期使用许可，能提供服务器关键部件（包括但不限于 CPU、内存、硬盘、网卡、HBA 卡、阵列卡、PCI-E 设备、散热、电源、温度等）运行状态和故障状态等监控，并支持与集中管控软件集成（提供集成接口并免费配合集成工作）。 19) 兼容性：兼容并稳定运行主流自主可控 Linux 操作系统近三年内的发布版、提供针对主流操作系统的可稳定运行的驱动程序；支持 64 位操作系统；兼容主流商用数据库软件及主流中间件等近三年内的发布版。 20) 售后服务：设备到货验收合格后，原厂提供 5 年免费上门维修服务，人工、配件、交通等任何费用全免；每天 24 小时、每周 7 天，4 小时到现场的原厂商支持，同时提供五年 5*8 原厂商认证工程师驻场支持保障服务。
--	--	--

3.2.2.2 高性能并行计算一体机

序号	设备名称	技术要求
1	高性能并行计算一体机	1) 规格: $\geq$标准 4U 机架 2) 处理器: $\geq 4*48$ 核 CPU, 主频 2.6GHz 3) 安全等级: 机型满足国产自主可控要求, 其 CPU、AI 处理器使用同一厂家自研芯片, 提供技术白皮书。 4) 内存: 配置内存≥ 2048GB, 单根内存 64GB, 支持 32 个内存插槽 5) 硬盘: 配置≥ 2 块容量 960G SATA SSD 硬盘, 配置≥ 6 块容量 3.84T NVMe SSD 硬盘 6) 存储系统: 配置≥ 1 块磁盘阵列卡, 缓存 4G Cache, 支持 RAID 0/1/5/6/10, 配置掉电保护 7) GPU 计算卡:总显存≥ 512GB, 整机算力不低于 2000TFlops@FP16 和 400TFlops@FP32 提供 8 卡或 8 个 GPU 芯片, 卡间或芯片间互联带宽>200GB/S。 8) 虚拟化: 通过支持物理机、虚拟机和容器多架构下的 GPU 资源动态分配和智能调度, 实现了计算资源的高效利用和精细化管理, 为 AI 计算基础设施提供更加灵活、安全和高性能的虚拟化底座。 a) 架构特性: 单一软件支持物理机、虚拟机(KVM)、纯容器(Docker, 无 K8S)和 K8S (Docker+K8S) 下的 GPU 虚拟化; 支持 VM 和容器同时使用虚拟 GPU 算力; 支持 KVM 虚拟机挂载使用虚拟化之后的虚拟 GPU; 三种架构下产品提供的虚拟化能力一致; 支持英伟达和国产卡混合池化调度 b) 高可用: 支持管理节点多副本, 无单点故障 c) 虚拟化切分: 支持 GPU 双维度申请 vGPU (算力维度和显存维度); 支持 GPU 按照显存大小切分为多个 vGPU 和算力进行切分为多个 vGPU d) 算力资源超分: 支持算力的超分 (2 个或以上算力分配总额超过 100%的任务可以调度到同一张卡运行); 支持内存模拟显存 (2 个或以上显存实际使用总额超过单张卡物理显存的任务可以调度到同一张卡运行) e) 跨机聚合: 支持多台 GPU 节点 (≥ 2) 跨机资源聚合, 为单一容器/虚拟机提供跨服务器节点的多卡 vGPU 资源; 最大可为单一容器/虚拟机提供多达 32 张物理 GPU 卡的虚拟算力聚合 f) 虚拟化切分: 支持 GPU 双维度申请 vGPU (算力维度和显存维度); 支持 GPU 按照显存大小切分为多个 vGPU 和算力进行切分为多个 vGPU 9) 网络接口: 配置≥ 1 张四口 10GE 网卡 (含 10G 多模光模块), ≥ 2 张双口 25GE 网卡 (含 25G 多模光模块), 配置≥ 4 块双口 200GE 光网卡 (含 200G 多模光模块)。 10) 质保服务: 原厂提供 5 年免费上门维修服务, 人工、配件、交通等任何费用全免; 每天 24 小时、每周 7 天, 4 小时到现场的原厂商支持, 提供设备厂商服务承诺函 (其中软件服务由软件原厂家提供, 与服务器同年限免费升级服务)。

3.2.2.3 工作站

序号	设备名称	技术要求
1	工作站	专业机架式工作站。 外形：高度≤2U，标准机柜安装，含机架安装套件，带安装导轨等； CPU：X86 架构，总核数不低于 16 核，原始主频≥2.0GHz； 内存：大于或等于 32GB DDR4； 硬盘：2 块 960GB（或以上）SSD 固态硬盘，SLC 闪存颗粒，读写混合型，擦写寿命：≥3 DWPD 5 年； 阵列卡：至少支持 raid0、1、5 显卡：2 个双屏 3D 显卡（每显卡流处理单元≥768 个,每显卡独立显存≥2GB）或 1 个四屏 3D 显卡（流处理单元≥1536 个,独立显存≥4GB，必须支持三种协议（HDMI、DVI、DP）中任意一种，宜原生支持，可采用转换器）； 网卡：10/100/1000 自适应网口×4； 光驱：DVD ROM； USB 接口：≥4 个； 音频：内置声卡，具备音频输入、输出接口（板载或内置 PCI 方式），配置话筒和小型音箱（具体规格以现场需求为准，在合同签订时确定）； 其它：键盘、鼠标、电源线； 售后服务：设备到货验收合格后，原厂提供 5 年免费上门维修服务，人工、配件、交通等任何费用全免；每天 24 小时、每周 7 天，4 小时到现场的原厂商支持，提供设备厂商服务承诺函（其中软件服务由软件原厂家提供，与服务器同年限免费升级服务）。

3.2.3 网络安全设备

3.2.3.1 纵向加密装置

序号	设备名称	技术要求
1	纵向加密装置	通过国家有关机构认证； 须提供原厂商的专项授权； 具备国家密码管理局颁发的《商用密码产品生产定点单位证书》 具备国家密码管理局颁发的《商用密码产品销售许可证》； 具有公安部计算机信息安全产品质量监督检验中心出具的《检验报告》； 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》； 采用专用服务器硬件和代码可控的安全操作系统； 本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等； 支持设备钥匙、工作参数的备份与恢复。 应通过有关部门组织的电磁兼容性检测； 应支持双机热备功能，在任一设备出现故障时能自动切换；

		应具有可配置自动旁路功能，在紧急故障状态下，用户可以通过配置使得旁路所有安全策略或部分链路的安全策略的功能，使之作为透明桥接设备工作，必要时允许通过网线旁路。在旁路状态下，设备应有明显的警告提示。 采用国家密码管理局批准的电力专用密码算法对传输的数据进行保护，保证数据的真实性、机密性和完整性； 支持 SM2、SM3 等国密算法； 加密认证装置或加密认证网关之间支持基于电力数字证书的认证； 支持透明工作方式与网关工作方式，支持 NAT； 具有基于 IP、传输协议、应用端口号的综合报文过滤与访问控制功能； 加密认证网关支持对电力应用协议的特殊报文进行选择性的加密保护； 符合《IP 加密认证装置技术规范》的技术要求，支持不同厂家设备的互通互联；支持由不同厂家纵向加密认证装置管理中心进行远程监控和管理。 装置必须能够识别、处理网络正常运行所需要的路由协议报文及其他协议报文； 装置必须能够识别、过滤、转发 Trunk 协议的报文，装置本地配置功能必须支持配置 VlanID。 网络接口：4 个 10/100/1000M 网络接口； 热备接口：具备双机热互备接口及相关软件； 外设接口：1 个 RS232 配置接口+1 个 IC 卡读卡器接口； 最大并发加密隧道数：2000 条； 1000M LAN 环境下，加密隧道建立延迟：<1s 明文数据包吞吐量：≥300Mbps 密文数据包吞吐量：≥130 Mbps 数据包转发延迟：< 2ms （50%密文数据包吞吐量） 满负荷数据包丢弃率：0 设备电源：双电源； 装置可安装于 19 英寸标准机柜。 提供现场安装服务，五年原厂免费售后服务（含人工和备件），包括技术支持和系统软硬件保修。
--	--	--

3.2.3.2 正向物理隔离（万兆）

序号	设备名称	技术要求
1	正向物理隔离（万兆）	机架式安装； 采用国产化芯片； 具备电力专用安全防护设备的检测证明； 采用非 INTEL 指令系统（及兼容）的微处理器构筑内外网隔离系统； 嵌入式安全操作系统，去除 TCP/IP 协议栈及其他不需要的系统服务； 本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等； 数据单向传输，1bit 返回信息； 表示层与应用层数据完全单向传输，即从安全区 III 到安全区 I/II 的 TCP 应答

		禁止携带应用数据；从安全接入区到安全 I 区的 TCP 应答禁止携带应用数据； 透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址； 基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制； 支持 NAT； 防止穿透性 TCP、UDP 联接； 配置冗余电源，支持双机热备；支持集群部署； 支持“单进单出”、“双进单出”、“双进双出”等多种连接方式； 万兆状态下数据传输率：≥5Gbps； 网络接口：内网≥4 个 10/100/1000M 网口，4 个万兆 SPF+接口，满配光模块； 外网≥4 个 10/100/1000M 网口，4 个万兆 SPF+接口，满配光模块； 外设接口：1 个管理接口； 数据包转发延迟小于 1ms； 满负荷数据包丢弃率为 0； 平均无故障时间大于 60000 小时（100%负荷）； 质保要求：含 5 年保修和软件升级。
--	--	--

3.2.3.3 反向物理隔离（万兆）

序号	设备名称	技术要求
1	反向物理隔离（万兆）	机架式安装； 采用国产化芯片； 采用非 INTEL 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统； 嵌入式安全操作系统，去除 TCP/IP 协议栈及其他不需要的系统服务； 本身应能够一定程度防御常见的网络攻击，包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等； 具有基于数字证书的数据签名/解签名功能，具有电力加密算法进行数字加密功能； 具有应用数据内容有效性检查功能； 具有纯文本和 E 文本编码检查功能； 实现两个安全区之间的非网络方式的的安全的数据传递； 透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址； 支持 NAT； 基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制； 防止穿透性 UDP 联接； 数据单向传输，1bit 返回信息； 配置冗余电源，支持双机阵列；支持集群部署。 支持“单进单出”、“双进单出”、“双进双出”等多种连接方式； 密文有效网络吞吐率：≥4Gbps； 网络接口：内网≥4 个 10/100/1000M 网口，4 个万兆 SPF+接口，满配光模块； 外网≥4 个 10/100/1000M 网口，4 个万兆 SPF+接口，满配光模块； 外设接口：1 个管理接口；

		数据包转发延迟小于 1ms; 满负荷数据包丢弃率为 0; 平均无故障时间大于 60000 小时（100%负荷）; 质保要求：含 5 年保修和软件升级。
--	--	--

3.2.3.4 正向物理隔离（千兆）

序号	设备名称	技术要求
1	正向物理隔离（千兆）	具有自主知识产权的国产设备； 千兆物理隔离； 机架式安装； 具备电力专用安全防护设备的检测证明； 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》； 采用非 INTEL 指令系统（及兼容）的龙芯微处理器构筑内外网隔离系统； 嵌入式安全操作系统，去除 TCP/IP 协议栈及其他不需要的系统服务； 能抵御除 DoS 以外的已知的网络攻击； 数据单向传输，1bit 返回信息； 透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址； 基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制； 支持 NAT； 防止穿透性 TCP 联接； 具有可定制的应用层解析功能，支持应用层特殊标记识别； 配置冗余电源，支持双机热备； 支持“单进单出”、“双进单出”、“双进双出”等多种连接方式； CPU 主频≥350MHz； 并发联接数≥3000； 数据传输率≥300Mbps； 网络接口：≥1000M 接口 2 个（内网）+≥1000M 接口 2 个（外网）+≥双机热备接口 1 个； 外设接口：≥1 个 RS232 接口 数据包转发延迟小于 10ms(100%负荷)； 满负荷数据包丢弃率为 0； 平均无故障时间大于 60000 小时（100%负荷）； 维护管理方便、安全 质保要求：含五年原厂保修和软件升级。

3.2.3.5 反向物理隔离（千兆）

序号	设备名称	技术要求
1	反向物理隔离（千兆）	具有自主知识产权的国产设备（千兆型）； 千兆物理隔离； 机架式安装； 具备电力专用安全防护设备的检测证明；

		具备公安部颁发的《计算机信息系统安全专用产品销售许可证》； 反向隔离装置必须通过国家密码管理委员会办公室组织的安全性审查和技术鉴定； 采用非 INTEL 指令系统（及兼容）的 RISC 微处理器构筑内外网隔离系统； 嵌入式安全操作系统，去除 TCP/IP 协议栈及其他不需要的系统服务； 能抵御除 DoS 以外的已知的网络攻击； 具有应用网关功能，实现应用数据的接收与转发； 具有基于数字证书的数据签名/解签名功能，具有电力加密算法进行数字加密功能； 具有应用数据内容有效性检查功能； 具有纯文本编码检查功能； 实现两个安全区之间的非网络方式的的安全的数据传递； 支持 SM2 等国密算法； 透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址； 支持 NAT； 基于 MAC、IP、传输协议、传输端口及通信方向的综合报文过滤与访问控制； 防止穿透性 TCP 联接； 数据单向传输，1bit 返回信息； 配置冗余电源，支持双机热备； 支持“单进单出”、“双进单出”、“双进双出”等多种连接方式； 网络接口：≥10/100M/1000M 接口 2 个（内网）+≥10/100M/1000M 接口 2 个（外网）+≥双机热备接口 1 个； 外设接口：≥1 个 RS232 接口+读写器接口； 数据包吞吐量不低于 200Mbps (100 条安全策略，1024 字节报文长度) 数字签名速率≥300 次/s 数据包转发延迟小于 10ms（100%负荷）； 满负荷数据包丢弃率为 0； 平均无故障时间大于 60000 小时（100%负荷）； 维护管理方便、安全。 质保要求：含五年原厂保修和软件升级。
--	--	--

3.2.3.6 WEB 防火墙

序号	设备名称	技术要求
1	WEB 防火墙	机架式，系统硬件为全内置封闭式结构； 最大支持 8 个千兆接口，要求配备 4 个 GE 口以及 4 个 SFP 接口， 应用层吞吐量≥1Gbps； 时延<50 us； 并发处理能力≥45000； 事务处理能力（TPS）≥25,000； 支持在线部署（支持透明反向代理、传统反向代理）； 支持旁路部署（静态路由牵引、二层回注，增加支持三层回注），支持旁路 HA，支持双臂旁路部署）；

	支持单台设备最大同时保护 5 条链路,本次提供标准配置 1 路 WAF 防护功能; 配置交流冗余双电源; 支持 A/S 部署模式 (链路切换、配置同步); 支持网络接口内置 fail-open, 支持软硬件双 BYPASS 功能; 支持 HTTP 0.9/1.0/1.1; 作为服务器与客户端 (浏览器) 的中间设备, 能够完全解析 HTTP 事务、了解 HTTP 事务的交互流程、并对关键的事务信息进行解码处理, 而无需中断 HTTP 连接; 防护策略模型由基于静态规则的反向 (黑名单) 安全模式及基于智能用户行为识别的动态防护机制 (正向安全模式, 即白名单) 构建; 系统内置规则及自定义规则, 便于管理员根据实际应用灵活地调整具体特征规则; 支持对 HTTP 协议合法性进行验证, 提供 HTTP 协议防护功能。 支持对 SSL (HTTPS) 加密会话进行分析。 可监控双向流量, 对双向数据实时监测和保护; 支持防护: 蠕虫、缓冲区溢出、CGI 信息扫描、目录遍历等攻击。 支持 SQL 注入、XSS 防护, 支持使 HTTP 头域中的 Cookie、Referer、User-Agent、Except 字段过防护策略; 支持 CSRF (跨站请求伪造) 防护; 支持扫描防护; 支持 Cookie 安全机制, 包括加密和签名的防护方法, 支持 Cookie 自学习; 支持盗链防护, 可采用 Referer 和 Cookie 算法; 支持对服务器状态码进行过滤和伪装的安全策略; 支持爬虫防护, 支持盗链防护, 说明所采用的防护算法。 产品提供 URL 访问控制功能, 能够基于多种 HTTP 方法执行访问控制; 能识别上传行为, 并对上传行为的内容做安全检测; 可以根据文件大小、MIME 类型、及文件扩展名, 灵活定义下载限制策略, 限制用户非法获取网站的关键数据 (比如数据库文件, 配置文件等); 对流出数据内容进行安全审查, 对敏感关键字实施过滤, 防止身份证等隐私信息非法泄露; 支持自动监测页面被篡改情况的功能; 支持视觉恢复功能, 即发生网页篡改后, 对外仍显示被篡改前的正常页面; 支持时间管理功能, 可以在不同的时间段设定不同的网页篡改防护策略; 支持 TCP Flood 防护; 支持 HTTP Flood 防护, 检测算法支持 5 种, 包括: etag、http cookies、url cookies、ascii-image、bmp-image; 支持 ARP 攻击防护; 支持基于五元组 (源 IP 地址、目的 IP 地址、源端口、目的源口、协议类型) 及接口的网络层访问控制功能; 支持系统运行日志、WEB 访问日志、安全防护日志等日志类型, 支持日志导出功能, 支持日志服务器 SYSLOG; 安全防护日志类型应包括: 网络层访问控制、URL 访问控制、DDoS 防护、WEB 防护、WEB 防篡改、ARP 防护等;
--	---

		支持安全报表（告警分类统计报表、告警时段统计报表、告警区域分析报表）、访问统计报表（访问时段、访问区域及业务类型）、流量趋势报表、各类排行表等，支持柱状图、饼状图及折线图等多种报表图形；支持报表自动生成及报表下载功能。 《计算机信息系统安全专用产品销售许可证》； 厂家拥有专业安全漏洞研究团队，拥有实时更新的中文安全漏洞库 提供现场安装服务，五年原厂免费售后服务（含人工和备件），包括技术支持和系统软硬件保修。
--	--	---

3.2.3.7 万兆防火墙

序号	设备名称	技术要求
1	万兆防火墙	1) 具有安全认证合格证明材料或者符合《信息安全技术 网络安全专用产品安全技术要求》强制要求的证明材料，证明材料须由《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》相关机构出具。 2) 具备有效期内的国家安全产品销售许可。 3) 基于自主可控芯片的多核 CPU 架构。 4) 采用防火墙专用操作系统。 5) 提供双电源供电，并支持故障告警。设备使用直流或交流电源，合同签订时，由具体合同签订方与投标方协商确定。 6) 配置设备机箱配套支架。 7) CPU、DRAM 颗粒、FLASH、交换转发等采用自主可控的芯片。 8) 电源、PHY、通信等采用自主可控的芯片。 9) 业务口要求：提供万兆光接口数≥ 8个，提供管理接口和 HA 端口。边界防火墙配置 1 个千兆以太网电接口扩展板卡，6 个万兆以太网光接口模块（多模，标准 SFP 接口），2 个万兆以太网光接口模块（单模，标准 SFP 接口）；横向防火墙配置 6 个万兆以太网光接口模块（多模，标准 SFP 接口），2 个万兆以太网光接口模块（单模，标准 SFP 接口）； 10) 数据包吞吐量$\geq 50\text{Gbps}$。 11) 最大并发连接数≥ 1000 万。 12) 每秒新建连接数≥ 30 万。 13) 最大静态路由条数≥ 2000 条。 14) 支持基于源、目的 IP 地址的策略路由能力。 15) 最大访问控制策略条数≥ 10000 条、最大地址集建立数目≥ 30000 条、最大服务集建立数目≥ 30000 条，最大域名对象数目≥ 3000 条。 16) 支持透明模式、路由模式、混合模式。 17) 支持 TCP、UDP 协议，支持 IPv4、IPv6、ICMP、GRE（无需绑定物理接口）、VRRP、OSPF、BGP、RIP、SNMP 等协议，支持 ARP、VLAN Trunk、QinQ 等协议。 18) 支持多条链路的捆绑及链路间的负载均衡。

	19) 支持静态网络地址转换(Static NAT), 支持动态网络地址转换(Dynamic NAT), 支持网络地址及端口转换(PAT)。 20) 能够识别常见应用协议并进行应用层处理, 支持对动态端口协议进行识别并控制。 21) 支持对 IP、IP 组、协议及端口进行带宽控制, 支持对最大与最小带宽进行限制, 支持根据 IP 地址限制并发 session 数量。 22) 可将物理防火墙划分为多个完整的虚拟化逻辑防火墙, 可虚拟的防火墙不少于 4 个。 23) 支持对源/目的地址对象、应用等设置并发和新建会话数量; 支持展示被拦截的 IP、地址对象、被拒次数、最近被拒时间等信息。 24) 支持分析失效、冗余、冲突的策略, 支持对策略有效性进行统计, 支持策略的命中统计, 支持策略查询及导出功能 请列明能够查询的功能项, 支持批量修改策略配置信息, 如批量禁用策略、批量删除策略等。 25) 支持 IPV6 功能。 26) 攻击防御: 支持对常见攻击方式进行检测与防御 (DDOS、特殊报文、扫描攻击、特殊控制报文攻击等); 抵抗各种典型的拒绝服务攻击, 包括 SYN FLOOD, UDP FLOOD, ICMP FLOOD, IP 碎片包攻击, 源 IP 地址欺骗攻击; 支持数据包的深度检测; 支持基于源及目的 IP 地址的并发连接数的控制。 27) 访问控制: 支持基于域名的访问控制, 且无需改变主机、终端的域名解析配置; 支持基于 IP 地址的访问控制; 支持基于地理位置的访问控制, 国内地理位置至少精细到省级, 境外地理位置精细到国家级; 支持基于端口的访问控制; 支持基于协议的访问控制; 支持基于时间的访问控制; 支持基于连接的访问控制; 支持默认禁止策略; 支持用户自定义安全策略。 28) 黑名单: 支持黑名单功能, 被列入黑名单的 ip 及 ip 地址段, 禁止所有访问, 支持有效期设置, 并提供黑名单增删 api 接口; 黑名单条数不少于 5000 条; 支持白名单功能, 被列入白名单的 ip 及 ip 地址段, 放行所有访问, 支持有效期设置, 并提供白名单增删 api 接口。 29) 支持 IPSEC VPN。支持对隧道内流量进行监控, 支持多种加密算法。 30) 支持识别并控制各种常见应用, 支持自定义应用特征。 31) 入侵防御: 支持告警和拦截非法、不正常、含攻击行为的报文; 支持手动自定义攻击规则库; 支持在线、离线、手动升级规则库; 至少支持威胁阻断模式、威胁监测模式; 32) 支持黑白名单、恶意 URL 过滤; 内置恶意 URL 库, 并支持在线、离线、手动更新; 支持自定义 URL 和阻断界面内容; 支持 URL 通配符, 可通过通配符阻断某网站二级网站或页面。 33) 支持对数据报文及文件进行病毒查杀, 支持对病毒报文及文件进行查杀、隔离等操作, 可拦截典型木马攻击行为, 支持在线、离线、手动更新规则库。
--	---

		34) 管理方式：支持本地串口管理、远程管理、集中管理、分级管理等；支持多主控台同时管理；支持 HTTPS, SSH 等管理方式；支持设置、查询和修改安全策略；支持鉴别失败管理；支持设备及策略集中管理。 35) 系统管理：支持自身状态监控，支持 snmp 管理，支持流量监测，提供支持设备状态监控、流量监控的北向 api 接口。支持带外网管接口。支持 Trap 协议。支持配置备份、NTP 时间同步等。 36) 用户管理支持对授权管理员的口令鉴别方式；支持管理员权限划分；支持对授权管理员、主机和用户进行身份鉴别。 37) 支持流量日志、事件类日志、操作类日志、运行类日志及用户日志；支持本地日志导出、日志清空、日志查询等；支持 SYSlog 等方式发送至多个日志服务器，提供 syslog 范式化服务；支持设置日志传输参数。 38) 行为审计：支持用户行为审计，支持审计数据查询。 39) 自身安全性：支持配置限定用户登陆的 IP 地址范围；支持 SSH、HTTPS 等加密方式进行远程访问；支持对用户口令进行加密保存；支持用户口令复杂度设置及检查；支持最大登录失败重试次数设置；支持用户登录超时时间设置；支持双因子认证方式；应保证所用的操作系统不存在安全漏洞； 40) 设备应具备开放性、可扩展性，并提供开放接口，其中对外接口包括：允许策略增删改查、特征库版本、运行状态、策略命中情况等信息。支持通过 SYSlog 方式以 UDP 发送日志对接监测系统，并可配合完成联动测试。 41) 应提供 MTBF(Mean Time Between Failure)和 MTTR(Mean Time To Repair)指标，其中 MTBF 不小于 5 万小时，MTTR 不大于 2 小时，业务恢复时间不大于 30 分钟；支持电源和风扇冗余，电源冗余单元应支持热插拔功能；支持软件防护加载、升级失败回滚；支持 trouble-shooting 和性能监控、故障跟踪能力；支持双机备份（双机热备、双机冷备）功能；支持双机配置同步功能；支持主备切换会话保持；支持在关闭防火墙策略时，能够正常路由转发数据包；支持设备状态监测、端口状态监测、链路连通性状态监测，可根据监测的设备状态，实现秒级的高可用切换，保障业务连续性。应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并作出即时故障报告信息。当主防火墙在 WEB 管理页面点击保存配置时，自动实现主、备配置同步。 原厂提供 5 年免费上门维修服务，人工、配件、交通等任何费用全免；每天 24 小时、每周 7 天，4 小时到现场的原厂商支持；提供原厂授权和原厂服务承诺函。
--	--	--

3.2.3.8 配网安全加密网关（万兆）

序号	设备名称	技术要求
----	------	------

1	配网安全加密网关	1) 基本要求 (1)系统架构 具有自主知识产权的国产设备,采用专用服务器硬件和代码可控的安全操作系统。 (2) 功能构成 应能够一定程度防御常见的网络攻击。 (3) 安全性要求 a) 通过国家密码管理局的安全性审查和技术鉴定,获得商用密码产品型号证书。(需提供原件的扫描件并盖原厂公章) b) 取得公安部的销售许可证或由国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会发布认可符合检测资格要求的机构出具的安全认证合格或者安全检测通过证明。(需提供原件的扫描件并盖原厂公章) c) 采用具备商用密码产品型号的密码硬件和代码可控的安全操作系统。 d) 可防御常见的网络攻击,包括 ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack 等。 e) 支持设备密钥、工作参数的备份与恢复。 f) 产品系统及设备核心元器件(CPU、存储)及软件(操作系统、数据库、中间件及应用软件)应采用自主可控及具备持续供应能力的产品。各类自主可控系统及设备在接口、模型、服务、协议方面兼容主流传统设备。同时应满足电力监控系统网络安全等级测试要求。(提供产品硬件及软件相关自主可控证明材料)。 (4) 可靠性要求 a) 应通过有关部门组织的电磁兼容性检测。 b) 平均无故障工作时间应不低于 60000 小时。 c) 应支持双机热备功能,当主机出现故障时自动切换至备机,切换过程中业务不得中断。 d) 对明文配网终端,主站端安全防护设备应配置独立的选择开关,具备手动配置功能。 2)功能要求 (1) 采用国密 SM1、SM2、SM3、SM4 等密码算法对传输的数据进行保护,保证数据的真实性、机密性和完整性。 (2) 支持不同厂家设备的互联互通。 (3) 具备基于电力调度数字证书的认证功能。 (4) 具备与配电终端安全模块\安全芯片建立 VPN 隧道,实现双向身份认证、访问控制和传输数据的加密与解密的功能。 (5) 具备隧道状态、终端在线状态的主动检测功能。 (6) 支持透明工作方式与网关工作方式,支持 NAT。 (7) 具有基于 IP、传输协议、应用端口号的综合报文过滤与访问控制功能。 (8) 具备识别、处理路由协议等报文的功能。 (9) 具备识别、过滤、转发 Trunk 协议报文的功能,且支持 VlanID 标签。 (10) 具备明文、密文的选择功能。
---	----------	--

		(11) 具备设备配置导入和导出功能。 (12) 具备支持网络和本地两种日志存取方式，日志包括事件日志和访问日志。 (13) 支持接入终端加密模块的远程维护。 3)性能要求 (1) 最大并发加密隧道数≥ 100000 条。 (2) 与终端安全防护设备密钥协商并成功建立隧道时间≤ 5 秒（不含网络延时）。 (3) 并发协商并建立 5000 条隧道的的时间≤ 5 秒（不含网络延时）。 (4) 双向数据包吞吐量$\geq 10000\text{Mbps}$。 (5) 转发平均时延≤ 2 毫秒。 4)配置要求 (1) 至少具备 8 个 10/100/1000M 以太网接口；至少具备 4 个万兆光口,满配光模块。 (2) 具备双机热备接口。 (3) 具备 2 个 RS232 配置接口 + 2 个 IC 卡读卡器接口或 USB-KEY 接口。 (4) 具备双电源。 (5) 装置可安装于 19 英寸标准机柜。 5) 安全性要求 (1) 算法安全要求 应使用国家密码管理主管部门批准的非对称密码算法、对称密码算法、杂凑算法和随机数生成算法。算法应选用符合国家密码管理局鉴定要求的密码芯片实现。 (2) 密钥安全要求 使用的密钥分为设备密钥、操作员密钥、会话密钥、通信密钥。纵向加密认证装置应有完善的密钥管理体系，对密钥、配置信息、口令文件等敏感性信息做到安全存储与管理 a)设备密钥 设备密钥为非对称密钥，配置在纵向加密认证装置和装置管理系统，用于设备的认证与会话密钥的协商。 设备密钥由纵向加密认证装置产生，其私钥保存在装置内，公钥经调度数字证书服务系统签名，以数字证书的方式发布。 设备密钥可备份与恢复，但在备份和恢复过程中不能以明文形式出现在非易失性硬件存储器中。 b)操作员密钥 操作员密钥为非对称密钥，配置在操作员卡，用于操作员和纵向加密认证装置的人机卡认证。 操作员密钥由操作员卡产生，其私钥保存在操作员卡内，公钥经调度数字证书服务系统签名，以数字证书的方式发布。 c)会话密钥 会话密钥为对称密钥，用于纵向加密认证装置之间的通信加密，会话密钥由设
--	--	--

	备在建立连接时动态协商产生，存储在装置内存中，拆除连接时失效。 d)通信密钥 通信密钥为对称密钥，用于装置管理系统与设备之间数据通信加密，通信密钥一次一密，通过数字信封随管理报文传输到每个与之连接的设备。 (3)账户安全要求 a)管理员身份鉴别机制 为保证装置的安全访问，防止抵赖和仿冒行为的发生，应使用智能密码钥匙或者 IC 卡作为标识管理员身份信息的硬件介质，与登录口令相结合进行身份鉴别。 无论管理员登录成功或者失败，系统均应记录审计日志。管理员登录成功后提示上次登录成功的时间，管理员登录错误后提示出错次数。当管理员登录出错一定次数后，管理员账户应被锁定，并提供一定的解锁机制解锁账户。 为保证管理员的帐户安全，纵向加密认证装置应限定登录口令的复杂度。登录口令长度不小于 8 个字符,并至少包含以下四类字符中的三类（大写字母、小写字母、数字、键盘上的符号）。 b) 管理员账户要求 管理人员分为三类：系统管理员、安全管理员和审计管理员。三类管理员权力相对独立不能交叉。 系统管理员：完成纵向加密认证装置的初始化操作，负责对软件环境日常运行的管理和维护，对管理员的管理和权限分配，以及对配置的备份和恢复、对装置重启和恢复出厂配置等； 安全管理员：负责设备的网络参数配置、隧道策略配置、参数配置等操作； 审计管理员：负责对系统中的日志进行安全审计。 除系统管理员外，安全管理员和审计管理员均可被删除，为审计唯一性需要，被删除管理员账号不能被再次使用。 (4) 管理安全要求 应支持本地管理终端管理、远程管理系统管理、本地串口调试及远程网络调试等功能。 a) 本地管理终端管理 管理员只有通过管理员卡(智能密码钥匙或 IC 卡)及口令双因子认证通过后才能通过使用本地管理终端管理对纵向加密认证装置进行本地管理维护。 管理报文交互过程应进行加密保护，并能抵御网络一定的重放攻击。 b) 远程管理系统管理 支持被远程管理系统管理，管理报文交互过程应使用双方数字证书进行加密保护。 c) 本地串口调试 本地串口调试时应验证系统用户口令不少于 8 位，应包括数字、英文字母大小写、特殊字符等。 d) 远程网络调试 装置缺省关闭远程网络调试功能，只有通关本地管理终端或远程管理系统打开网络调试功能后才能使用网络对装置进行远程网络调试。 远程网络调试时应验证系统用户口令，系统管理员口令应具有一定的复杂度。
--	--

		(5) 系统安全要求 应对内核做最小化定制处理，裁剪不需要的服务，不对外开放如 tftp、telnet、http、email 等多余服务。 (6) 物理安全要求 应有完备的硬件安全保护机制，防止密钥等敏感信息出现泄漏。 硬件安全防护机制种类厂商可选择性支持，如：机箱锁、一键毁钥、开机箱盖毁钥、密码部件防护罩等。 (7) 数据安全要求 应支持对关键配置信息进行备份和恢复。 配置备份时，使用备份口令对配置信息文件进行对称加密和完整性校验，最后将密文的备份文件从纵向加密认证装置导出。 恢复配置时，纵向加密认证装置使用备份口令，对导入的备份文件进行解密并验证其完整性，验证合法后，将备份文件的内容覆盖原有系统配置。 在开机及运行过程中应对配置文件的完整性自检，避免配置信息被非法篡改。 (8) 运行安全要求 应对系统中的各种事件进行详细的日志记录，并结合日志分析与审计，可以从中发现入侵和破坏行为，及时采取应对措施，起到事前预警和事后追溯的效果，从而更有力地保障系统的安全。 日志的记录要素包括事件发生的日期、时间、主体、客体、类型和结果等。 重要的日志事件通过 syslog 上报至内网监控平台。 装置在开机及运行过程中应对密码运算部件进行开机或周期性自检。
--	--	--

4 验收

1) 主站系统及功能的验收应坚持公平、公正、公开的原则，坚持科学、严谨的工作态度，验收测试应使用专业的测试仪器和测试软件。

2) 主站系统及功能的验收工作按时间顺序分为工厂验收、现场验收、整体考核验收；完成现场验收后，系统投入试运行，试运行时间不得少于 3 个月，试运行期间如有关键设备宕机、重要进程非正常终止、系统崩溃等重大缺陷问题，重新计算试运行时间，重复超过两次则整改后再次现场验收，试运行满足要求后方可开展整体考核验收；只有在前一阶段验收合格通过后，方可进入下一阶段。

3) 对于主站系统整体升级工程的验收工作，招标方组织开展工厂验收、现场验收和整体考核验收工作；对于主站系统功能加装、改造工程的验收工作，招

标方组织开展现场验收工作，工厂验收和整体考核验收可根据实际情况确定是否开展。

4) 各阶段验收的基本原则如下：

- a) 中标方在各验收阶段所提供的系统说明书及各功能使用手册等完整的技术文档必须为按系统实际情况所编制的版本，各阶段验收大纲的功能测试项目的测试步骤应按使用手册对应的叙述编制，以验证使用手册的正确性；如该项测试步骤不能正确执行，则视为该项测试不通过。
- b) 若各阶段验收测试结果证明某一设备、软件功能或性能不合格，中标方必须更换不合格的设备或修改不合格的软件，对于第三方提供的设备或软件，同样适用。设备更换或软件修改完成后，与该设备及软件关联的功能及性能测试项目必须重新测试。
- c) 主站系统各阶段验收的功能及性能测试宜在人机界面上进行，尽量避免使用命令行方式。
- d) 各验收阶段的验收测试时间应根据验收大纲的测试项目核定，各阶段验收测试时间均不得少于 5 个工作日。
- e) 主站系统在各阶段验收的资料核查应按照《南方电网一体化电网运行智能系统技术规范第 8 部分：验收 第 1 篇：电网运行监控主站系统及功能验收规范》的具体要求执行。

5) 主站系统在各阶段验收的各项性能指标和功能要求均应严格遵循项目合同技术条件书及历次技术（设计）联络会议纪要的所有技术方面的条款和合同执行过程中产生的技术澄清文件（以下合称项目技术文件），不足部分应执行当前最新行业标准、国家标准或国际标准。

5 包装、运输、贮存和质量保证

- 1) 设备制造完成并通过试验后应及时包装，否则应得到切实的保护，确保

其不受污损。

2) 所有部件经妥善包装或装箱后,在运输过程中尚应采取其它防护措施,以免散失损坏或被盗。

3) 在包装箱外应标明需方的订货号、发货号。

4) 各种包装应能确保各零部件在运输过程中不致遭到损坏、丢失、变形、受潮和腐蚀。

5) 包装箱上应有明显的包装储运图示标志。

6) 整体产品或分别运输的部件都要适合运输和装载的要求。

7) 随产品提供的技术资料应完整无缺。

8) 中标方应保证制造过程中的所有工艺、材料等(包括中标方的外购件在内)均应符合本技术文件的规定。若需方根据运行经验指定中标方提供某种外购零部件,中标方应积极配合。

9) 中标方应将设备发运至采购方指定的最终用户现场。

10) 质保期间,因制造质量问题而发生损坏,或不能正常工作时,中标方应免费为需方修理或更换零件。

6 双方工作安排

6.1 招标方职责

1) 负责对本技术文件进行解释。

2) 保留对本技术文件增删、修改的权利。

3) 有权对中标方的技术建议书的内容进行取舍。

4) 授予合同前,有权要求中标方提供产品功能演示,以验证中标方投标产品满足功能要求。

5) 协助中标方开展现场相关工作。

-
- 6) 确认中标方提供的相关资料 and 文件。
 - 7) 负责提供现场安装的条件及必要的支持。
 - 8) 协助现场设备布置。
 - 9) 组织现场验收。

6.2 投标方职责

投标方职责包括但不限于：

- 1) 提供项目实施所需的设备（包括软硬件），包括设备的采购运输、现场安装调试、验收测试、技术支持和售后服务等相关工作内容。
- 2) 提供设备自合同结算后 5 年免费维护服务。中标方应积极配合处理现场故障。
- 3) 在现场验收前，中标方应负责提供本项目实施相关最新版本的软件，并在合同结算后的 5 年免费维护期内免费负责这些软件版本的更新。
- 4) 负责承担现场验收相关事宜及验收费用。

6.3 项目管理

合同签定后，中标方应指定负责本工程的项目经理，负责协调中标方在工程全过程的各项工作。

6.4 资料管理

中标方应提供项目完整的文档资料。文档应包含设计、运行、维护和测试、培训资料以及本规范书中要求的所有文档资料。

投标方应对其所提供的全部文档的准确性和完整性负责。所有由投标方采购供货的第三方设备的技术手册的准确性由投标方负责。

系统提供的所有文档必须与实际系统相一致。文档内容的任何不一致均将被视为不符合技术规范要求。包括但不限于以下技术文档：

-
- a) 系统使用操作手册。
 - b) 系统结构和配置说明。
 - c) 维护和检修手册。

6.5技术（设计）联络会

1) 为便于合同的执行、审查和系统设计方案的确定，中标方与招标方根据需要举行技术（设计）联络会，除按合同规定举行的技术（设计）联络会外，双方可以根据需要约定对方举行额外的技术（设计）联络会。

2) 每次技术（设计）联络会招投标双方均签署会议纪要，纪要将视为合同的组成部分。

6.6安装调试

1) 投标方在招标方的监督下负责现场系统的安装调试。

2) 凡是本项目所需的设备/软件，无论是否由投标方提供，投标方均有义务在招标方及第三方设备/软件提供方的指导、配合下进行整体调试。

6.7培训

1) 投标方负责对招标方技术人员及运行、维护人员进行培训。

2) 由投标方负责提供培训，招标方选派人员参加，培训费用包含在设备报价中。

6.8现场服务及售后服务

1) 中标方应派代表到现场负责安装、调试和运行，并负责解决合同设备制造及性能等方面的有关问题，详细解答合同范围内需方提出的问题。

2) 在产品质保期内有制造质量的设备，由中标方负责修理或更换。对非中

标方责任造成的设备损坏，中标方有优先提供配件和修理的义务。

3) 对招标方选购的与本合同设备有关的配套设备，中标方有提供技术配合的义务，并不由此而增加任何费用。

4) 售后服务要求

a) 自合同结算之日起 5 年，中标方应免费提供系统软件升级、技术服务，优惠提供有关扩建工程的软件扩容服务；

b) 提供 7×24 小时的技术支持服务，制定相对固定的技术负责人及联络电话等；

c) 在用户发现软件故障时，中标方必须在用户提出维护要求的 2 小时内作出响应，24 小时内提交故障分析报告和解决方案，48 小时内故障得以解决；

d) 对于用户提出的软件性能提高、功能增加等改进要求，如属“技术文件”或“合同”的范畴，中标方应在 2 周内予以解决；如属“技术文件”或“合同”以外的功能开发，也应提供优惠服务。

7 订货范围

序号	名称	配置	单位	数量
1	I 区全闪融合存储一体机	详见 3 技术要求	台	3
2	I 区纵向加密装置	详见 3 技术要求	台	4
3	I 区/安全接入区物理隔离装置（万兆正向）	详见 3 技术要求	台	4
4	I 区/安全接入区物理隔离装置（万兆反向）	详见 3 技术要求	台	4
5	配网安全加密网关（万兆）	详见 3 技术要求	台	4
6	I 区/III 区物理隔离装置（千兆正向）	详见 3 技术要求	台	2
7	I 区/III 区物理隔离装置（千兆反向）	详见 3 技术要求	台	2
8	II 区/III 区物理隔离装置（千兆正向）	详见 3 技术要求	台	2
9	II 区/III 区物理隔离装置（千兆反向）	详见 3 技术要求	台	2
10	II 区纵向加密装置	详见 3 技术要求	台	2
11	III 区全闪融合存储一体机	详见 3 技术要求	台	3
12	III 区 Web 防火墙	详见 3 技术要求	台	1
13	工作站	详见 3 技术要求	台	4
14	高性能并行计算一体机	详见 3 技术要求	台	2

附件一：设备需求一览表

设备需求表

序号	名 称	规格（品牌、型号及主要技术参数等）	单位	数量
1				
2				
3				
4				
5				
.....				
	合 计			

说明：

投标厂商需根据招标要求作出详细投标方案，报来投标产品型号规格、技术性能参数、产品使用说明书等资料，如有差异或更好建议配置，需作专门说明。

附件二：技术差异表

投标人要将投标文件和招标文件的差异之处汇集成表。

序号	招标文件		投标文件	
	条目	简要内容	条目	简要内容

投标授权代表（签字）_____

年 月 日