



变电站二次安防硬件防火墙技术规 范书

深圳供电局有限公司

2026 年 05 月

目 录

1 总则	1
2 工作范围	2
2.1 项目概况	2
2.2 范围和界限	2
2.3 服务范围	2
3 应遵循的主要标准	4
4 使用环境要求	5
5 技术要求	5
5.1 设备技术要求	5
5.2 设备技术参数和性能要求响应表	6
5.3 设备及其附件主要元器件来源	12
6 试验	12
6.1 型式试验	12
6.2 出厂试验	12
6.3 现场交接试验和功能验收	13
7 产品对环境的影响	13
8 技术文件要求	13
9 监造、包装、运输、安装及质量保证	13
9.1 监造	13
9.2 包装	13
9.3 运输	14
9.4 安装使用指导	错误！未定义书签。
9.5 质量保证	14
10 技术差异表	15
11 投标方需说明的其他问题	15

1 总则

1.1 本技术规范书适用于深圳供电局有限公司_____项目采购的变电站二次安防硬件防火墙，它提出了该设备本体及附属设备的功能设计、结构、性能、安装和试验等方面的技术要求。

1.2 本设备技术规范书提出的是最低限度的技术要求。凡本技术规范书中未规定，但在相关设备的行业标准、国家标准或 IEC 标准中有规定的规范条文，投标方应按相应标准的条文进行设备设计、制造、试验。对国家有关安全、环保等强制性标准，必须满足其要求。

1.3 如果投标方没有以书面形式对本技术规范书的条文提出异议，则意味着投标方提供的设备完全符合本技术规范书的要求。如有异议， 不管是多么微小， 都应在报价书中以“对技术规范书的意见和同技术规范书的差异”为标题的专门章节中加以详细描述。

1.4 本技术规范书所使用的标准如遇与投标方所执行的标准不一致时，按较高标准执行。

1.5 本技术规范书经招标、投标双方确认后作为订货合同的技术附件，与合同正文具有同等的法律效力。若本技术规范书涉及有关商务方面内容，如与招标文件的商务部分矛盾时，以商务部分为准。

1.6 本技术规范书未尽事宜，由招标、投标双方协商确定。

1.7 投标方在应标技术规范书中应如实反映应标产品与本技术规范书的技术差异。如果投标方没有提出技术差异，而在执行合同的过程中，招标方发现投标方提供的产品与其应标技术规范书的条文存在差异，招标方有权利要求退货，并将对下一年度的评标工作有不同程度的影响。

1.8 投标方应在应标技术部分按本技术规范书的要求如实详细的填写应标设备的标准配置表，并在应标商务部分按此标准配置进行报价，如发现二者有矛盾之处，将对评标工作有不同程度的影响。

1.9 投标方应充分理解本技术规范书并按本技术规范书的具体条款、格式要求填写应标的技术文件，如发现应标的技术文件条款、格式不符合本技术规范书的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.10 如产品为原装进口设备，代理商应具有本项目出具的制造商授权书。

1.11 标注“★”的条款为关键条款和技术参数，作为评标时的否决项。

2 工作范围

2.1 项目概况

本技术规范书采购的设备适用的工程概况见表 2.1：工程概况一览表。

表 2.1 工程概况一览表 （项目单位填写）

序号	名 称	内 容
1	采购设备或项目名称	
2	项目单位	深圳供电局有限公司
3	项目单位地址	深圳市福田区中心一路 39 号

2.2 范围和界限

1) 本技术规范书适用于所供设备的设计、制造、装配、工厂试验、交付和试验的指导、监督以及试运行工作。

2) 本技术规范书未说明，但又与设计、制造、装配、试验、运输、包装、保管和运行维护有关的技术要求，按条款 3 所规定的有关标准执行。

2.3 服务范围

1) 供货范围一览表

投标方提供的设备及其附件的具体规格、数量见表 2.2：供货范围及设备技术规格一览表。投标方应如实填写“投标方保证”栏。

表 2.2 设备供货范围响应表（项目单位填写）

序号	名 称	单位	项目要求		投标方保证	
			型式、规格	数量	型式、规格	数量
1	万兆防火墙	套	为保证设备稳定性，冗余电源，接口配置：配置千兆电接口 ≥ 20 ，万兆光接口 ≥ 10 ；吞吐量满足业务需求。为保证设备稳定性；交换容量及包转发率满足业务需求，支持 Vxlan 技术。	2		
2	高端万兆防火墙	套	为保证设备稳定性，冗余电源，满足未来扩展需要；接口配置：10G 接口 ≥ 20 个，40GE 接口 ≥ 2 并可支持接口扩展；业务槽位数 ≥ 6 ，支持 50/25G 接口扩展，支持 Vxlan 技术。	1		

2) 投标方应按本技术规范书的要求提供全新的、合格可用的仪器及配件。投标方应向招标方提供必备的备品备件、专用工具和仪器仪表清单见表 2.2， 要求提供的备品备件、专用工具和仪器仪表应是新品，并符合相关技术要求。

3) 投标方所提供的组件或附件如需向第三方外购时，投标方应对其质量向招标方负责，并提供相应出厂和验收报告。

4) 投标方应协助招标方解决设备运行中出现的问题。

5) 如果调试、性能试验、试运行及质保期内技术指标一项或多项不能满足合同技术部分要求，买卖双方共同分析原因，分清责任，如属制造方面的原因，或涉及索赔部分，按商务部分有关条款执行。

6) 设备正常使用后，投标方和招标方（业主）双方应根据相关法律、法规和公司管理制度签署合同设备的验收证明书。该证明书共两份，双方各执一份。

7) 投标方应按招标方要求免费提供必须的人员培训和技术指导，确保招标方正常使用和维护设备。

3 应遵循的主要标准

除本技术规范书特殊规定外,投标方所提供的设备均按规定的标准和规程的最新版本进行设计、制造、试验。如果这些标准内容有矛盾时,应按最高标准的条款执行或按双方商定的标准执行。如果投标方选用本技术规范书规定以外的标准时,则需提交这种替换标准供审查和分析。仅在投标方已证明替换标准相当或优于技术规范书规定的标准,并从招标方处获得书面的认可才能使用。提交供审查的标准应为中文或英文版本。

标准如下:

ISO	《国际标准化组织标准》
IEC	《国际电工委员会标准》
ITU—T G. 652、G. 655	《单模光纤标准》
IEEE	《美国电气电子工程师协会标准》
GA 1089-2013	《电力设施治安风险等级和安全防范要求》
DL	《中华人民共和国电力行业标准》
EIA	《电子工业协会标准》
	《中华人民共和国网络安全法》
GB 50348-2018	《中华人民共和国密码法》
GB17859-1999	《计算机信息系统 安全保护等级划分准则》
GB/T25058-2019	《信息安全技术 网络安全等级保护实施指南》
GB/T25070-2019	《信息安全技术 网络安全等级保护安全设计技术要求》
GB/T 22240-2020	《信息安全技术 网络安全等级保护定级指南》
GB/T22239-2019	《信息安全技术 网络安全等级保护基本要求》
GB/T28448-2019	《信息安全技术 网络安全等级保护测评要求》
DL/T 860	《变电站通信网络和系统》
	《电力二次系统安全防护规定》
Q/CSG 115001-2012	《南方电网调度自动化系统不间断电源配置规范》
	《南方电网公司反事故措施（2018 版）》
电监信息[2012]62 号	电力行业信息系统安全等级保护基本要求

4 使用环境要求

本设备招技术规范书技术文件需要采购的设备，其外部使用条件见表 4.1。投标方应对所提供的设备性能参数在外部条件下进行校验、核对，使所供设备满足实际外部条件要求及全工况运行要求。

2.1 设备使用环境要求相应表（项目单位填写）

万兆防火墙使用环境要求相应表（项目单位填写）

序号	名 称	项目要求值	投标方保证值	备注
1	长期工作环境温度	0℃～45℃		
2	存储温度	-40° C ～ 70° C		
3	长期工作环境相对湿度	5%RH～95%RH，无冷凝		
4	存储相对湿度	5%RH～95%RH，无冷凝		
5	长期工作海拔高度	0m～5000m		
6	存储海拔高度	0m～5000m		

高端万兆防火墙使用环境要求相应表（项目单位填写）

序号	名 称	项目要求值	投标方保证值	备注
1	长期工作环境温度	0℃～45℃		
2	存储温度	-40° C ～ 70° C		
3	长期工作环境相对湿度	5%RH～95%RH，无冷凝		
4	存储相对湿度	5%RH～95%RH，无冷凝		
5	长期工作海拔高度	0m～5000m		
6	存储海拔高度	0m～5000m		

5 技术要求

5.1 设备技术要求

5.1.1 设备基本要求

设备及全部配件必须为全新的、持久耐用的产品。即使在本技术规范书中没有明确地提出，也应满足作为一个完整产品一般所能满足的全部要求。同时，可根据系统、测试对象性能的要求并随着 IT 技术发展，可提供持续的软件开发和硬件的升级。

5.1.2 设备结构要求

无要求。

5.2 设备技术参数和性能要求响应表

投标方应认真逐项填写所供设备技术参数和性能要求响应表（见表 5.1）中“投标方保证值”栏，不能空格，也不能以“响应”两字代替，不允许改动本表内“投标方保证值”栏之外的数值。如有差异，请填写表 10.1：技术差异表。标注“★”的条款为关键条款，投标方应出具相应技术资料证明达到条款和技术参数的要求，作为评标时的否决项。

表 5.1 技术参数和性能要求响应表（项目单位填写）

万兆防火墙技术参数要求

功能及技术指标	详细技术参数
安全网关硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块。
★安全要求	产品集成部件的芯片基于自主可控芯片，包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
★安全网关接口要求	主机固化：≥1 个配置口（CON），≥1 个 USB 接口，千兆 Combo 接口≥8，≥4 个万兆以太光口。
★安全网关性能要求	整机小包吞吐量（64 字节）≥10G 并发连接数≥400W 新建连接数≥7W 配置 2 个电源
★ NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、等多种 NAT ALG 功能。
★ VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
	支持 IPsec VPN 隧道自动建立，无需流量触发。
	支持 IPsec VPN 智能选路，根据应用和隧道质量调度流量。（提供功能截图）
	可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阈值进行细颗粒度的管控。
攻击防护	实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。
安全策略	支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置。

功能及技术指标	详细技术参数
URL 过滤	<p>设备提供海量预分类的 URL 地址库，支持根据 URL 类别实现 URL 过滤。</p> <p>设备支持管理者自定义新的 URL 地址和 URL 分类。</p>
流量控制	可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。
★ 加密流量检测	支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项。
★ IPv6	<p>实现 IPv6 动态路由协议、IPv6 对象及策略、IPv6 状态防火墙、IPv6 攻击防范、IPv6 GRE/IPSEC VPN、IPv6 日志审计、IPv6 会话热备等功能。</p> <p>支持 IPv6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。</p>
★ 负载均衡	<p>多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式。</p> <p>支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（需提供设备功能界面截图证明）</p>
★虚拟化能力	所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；虚拟防火墙具备 NAT、路由等功能。
设备管理	<p>支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。</p> <p>支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议。</p> <p>支持 BFD 链路检测，支持 BFD 与 HA 联动实现双机快速切换。</p> <p>提供开放 API 接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。</p>
★路由网关包转发率	≥250Mpps
★路由网关端口	固化千兆电口≥12 个，SFP+接口≥6 个。
★路由网关电源系统	冗余交流电源
路由能力	支持静态路由，路由策略，RIP，OSPF，IS-IS，BGP。
路由网关基本功能	★支持 Vxlan 隧道能力，Vxlan 隧道可兼容 BGP4+、OSPFv3 等，通过 Vxlan 相关协议可建立邻居学习路由并正常通讯。

功能及技术指标	详细技术参数
IPv6 技术	支持 IPv6 隧道技术
GR、NSR	增强可靠性，可以实现链路或者设备故障时，业务流量平滑过渡实现不丢包。
★路由网关产品资质	5 年原厂质保，7*24 小时热线支持，5 年原厂软件升级服务，原厂备件服务。
★安全网关产品资质	提供防火墙产品销售许可证。
	5 年原厂质保，7*24 小时热线支持，5 年原厂软件升级服务，原厂备件服务。

高端万兆防火墙技术参数要求

功能及技术指标	详细技术参数
★ 安全网关硬件架构	采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块。
★ 安全要求	产品集成部件的芯片基于自主可控芯片，包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
★ 安全网关存储	支持硬盘≥1T
★安全网关扩展性	支持 40G 接口扩展，或已有 40GE 接口≥2
★ 安全网关接口要求	配置千兆电接口≥8，万兆光接口≥12
★ 安全网关性能要求	整机小包吞吐量（64 字节）≥30G
	并发连接数≥1200W
	SSL 代理吞吐量≥7Gbps
	新建连接数≥40W/s
升级服务	支持防火墙、链路负载均衡、入侵防御、防病毒等功能。
部署模式	实现路由模式、透明（网桥）模式、混合模式。
★隧道能力	支持 NAT64 功能，支持 IPv4 to IPv6 隧道功能
路由实现	实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。
★NAT 功能	实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP 等多种 NAT ALG 功能。
	★NAT64 条数≥50000 条
	NAT 地址池支持动态探测和可用地址分配
★ VPN	实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。
	支持 IPSec VPN 隧道自动建立，无需流量触发。
	支持 IPSec VPN 智能选路，根据隧道质量调度流量。

功能及技术指标	详细技术参数
	可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阈值进行细颗粒度的管控。
攻击防护	实现安全区域划分, 访问控制列表, 配置对象及策略, 动态包过滤, 黑名单, MAC 和 IP 绑定功能, 基于 MAC 的访问控制列表, 802.1q VLAN 透传等功能。
安全策略	支持一体化安全策略, 能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置。
	支持将基于端口的安全策略转换为基于应用的安全策略, 分析设备策略风险, 及冗余策略, 提供安全策略优化建议。
	支持 BFD 链路检测, 支持 BFD 与 HA 联动实现双机快速切换。
	支持策略冗余分析, 冲突策略分析以及命中率统计。
	支持策略风险调优, 支持安全策略优化分析, 支持策略数冗余及命中分析, 支持基于应用风险的策略调优, 可根据流量、应用、风险类型等细粒度展示, 并给出总体安全评分, 便于用户更好的管理安全策略。
应用识别	支持至少 5000 条以上的应用识别, 且提示风险类型及风险级别, 便于用户根据实际情况进行上网行为管理。
★URL 过滤	设备提供海量预分类的 URL 地址库, 支持根据 URL 类别实现 URL 过滤。
	设备支持管理者自定义新的 URL 地址和 URL 分类。
	支持超过 8000 种特征的攻击检测和防御。
防病毒	可基于病毒特征进行检测, 实现病毒库手动和自动升级, 实现病毒日志和报表; 支持基于文件协议、邮件协议 (SMTP/POP3/imap)、共享协议 (NFS/SMB) 的病毒功能。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息, 支持用户编辑告警内容。
流量控制	可支持基于应用层协议设置流控策略, 包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式, 支持父子带宽策略。
加密流量检测	支持 HTTPS 加密流量的安全检测, 支持 TCP 代理和 SSL 代理, 且代理策略中可同时配置多类过滤条件, 具体包括: 源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项。
IPv6	实现 IPv6 动态路由协议、IPv6 对象及策略、IPv6 状态防火墙、IPv6 攻击防范、IPv6 GRE/IPSEC VPN、IPv6 日志审计、IPv6 会话热备等功能。
	支持 IPv6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。

功能及技术指标	详细技术参数
★负载均衡	多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式。
	支持智能 DNS 解析功能，引导访问用户从最优路径的线路接入应用系统。
	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
DDoS 防护	能够防范 DOS/DDOS 攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范，还包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击的检测防御。
	支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略。
★虚拟化能力	所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；虚拟防火墙具备 NAT、路由等功能。
设备管理	支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。
	为了保证整个网络的可靠稳定，要求本次采购的安全设备支持 A/S，A/A 方式部署，支持配置同步和会话同步。
	提供开放 API 接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。
★路由网关体系架构	为保障接口扩容，支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位。
	要求支持主控冗余。
★路由网关交换容量	交换容量 $\geq 70\text{Tbps}$ ，需提供产品截图。
★路由网关包转发率	包转发率 $\geq 12000\text{Mpps}$ ，需提供产品截图。
路由网关要求	集成部件须基于自主可控，包括但不限于 CPU、操作系统。
路由网关单槽位最大处理能力	$\geq 50\text{ Gbps}$
★路由网关接口形态	整机框业务槽位数 ≥ 6 ，支持 50/25G 接口扩展。 实配 ≥ 8 个 SFP+业务接口。
★路由网关电源系统	实配冗余电源。
路由网关基本功能	★支持 PPP、MP、HDLC、ETHERNET 等链路层协议。

功能及技术指标	详细技术参数
	★支持 Vxlan 隧道能力, Vxlan 隧道可兼容 BGP4+、OSPFv3 等, 通过 Vxlan 相关协议可建立邻居学习路由并正常通讯。
	支持链路聚合 (Link aggregation), 支持动态聚合、手工聚合、跨板聚合。
	支持不同速率物理接口链路捆绑功能。
	支持 IPv4 静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略。
	支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+。
路由网关接口类型	支持 FE、GE、10GE (LAN/WAN) 等接口, 需提供产品截图。
★GRE	随板支持 GRE 功能。
★Netstream	随板支持 Netstream 功能。
★NAT	随板支持 NAT 功能。
组播 VPN (MVPN)	支持分布式 NG-MVPN 功能。
QOS	支持优先级 Mark/Remark、CAR (Committed Access Rate)、GTS 等功能。
	为简化 ACL 配置, 设备需支持全局 ACL 功能。
	支持 FIFO、PQ、WFQ、LLQ 等各种队列调度机制, 支持拥塞避免算法: Tail-Drop、RED、WRED, 支持层次化 Qos (H-Qos)。
SDN	设备支持通过 Netconf (RFC 6241) 协议下发配置。
	设备支持 YANG 功能 (RFC 6020)。
	为实现报文最优路径转发, 设备需支持 MPLS Segment Routing 功能, MPLS 隧道通过 SR-LSP 进行转发 (OSPF 通告 SID)。
	为实现按服务类型选择隧道路径, 设备需支持 CBTS 功能 (YD/T 1391.1)。
	★设备支持 EVPN 和 VxLAN 功能, 并提供第三方测试报告。
★可靠性	支持 VRRP、MPLS TE FRR、IP FRR (IS-IS/OSPF/LDP 等)
	为减小设备或线路故障对业务的影响、提高网络的可用性, 需支持 BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route/RIPng/OSPFV3/BGP4+/ISISv6。
	支持热补丁功能, 可在线进行补丁升级。
	为提高设备软件稳定性及可靠性, 主备倒换时业务不中断, 需要支持 NSR 功能, 具体协议包括 VRRP、IPv6 VRRP、IPV4 PIM、IPv6 PIM、OSPF、OSPFV3、ISIS、ISISv6、BGP、BGP4+。
	为提高设备硬件稳定性及可靠性, 板卡、子卡支持热插拔功能。
	为检测设备之间的双向时延、抖动、丢包进行统计等信息, 设备

功能及技术指标	详细技术参数
	需支持 Y.1731 检测网络质量。
	支持 OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+ 的 MD5 认证功能，支持 Keychain 功能。
维护特性	设备需支持 TCL 语言功能，能够解析执行 TCL 语言脚本。
★路由网关产品资质	提供工信部入网许可证复印件，要求设备入网时间>1 年。
	5 年原厂质保，7*24 小时热线支持，5 年原厂软件升级服务，原厂备件服务。
★安全网关产品资质	具备信息产业信息安全测评中心出具的防火墙 EAL4+级资质。
	5 年原厂质保，7*24 小时热线支持，5 年原厂软件升级服务，原厂备件服务。

5.3 设备及其附件主要元器件来源

投标方应按表 5.2 如实填写主要元器件来源。

表 5.2 设备及其附件主要元器件来源一览表 （投标方填写）

序号	元器件名称	型号	厂家或供应商名称	产地	备注

6 试验

根据相关国标和行标等有关标准及其补充说明进行各项试验,有关条款的特殊要求和补充应在试验期间遵守并执行。

6.1 型式试验

型式试验是为了验证所设计和制造的设备的性能是否能够达到相应产品标准的要求,投标方应提供有相应资质的第三方检测机构出具的产品型式试验报告,型式试验的项目内容如下:

无

6.2 出厂试验

出厂试验是为了发现产品所用材料和制造中的缺陷,它不应损伤产品的性能和可靠性。出厂试验应在整体组装后进行,应该对每台成品进行检验,以确保每台产品与已经通过型式试验的产品相一致。出厂试验的项目内容如下:

无

6.3 现场交接试验和功能验收

本技术规范书采购设备应进行现场交接试验和功能验收,并派专人进行现场设备验收与设备交付实施工作。交接试验和功能验收是为了确认设备经过运输、储存和/或调整等过程后是否存在损坏、各个单元的兼容性、装配是否正确。本技术规范书采购现场交接试验和设备功能验收应按表 5.1 要求执行。

7 产品对环境的影响

制造厂应该提供有关设备对环境影响所需要的材料。任何已知的化学危险和环境危害应在手册或使用说明中明确。

制造厂应该对有关设备的不同材料的使用寿命和拆除的程序给予必要的指导,对再循环使用的可能性给予简要说明。

8 技术文件要求

在设备到货时,投标方应按招标方要求提供满足本次采购设备、调试、使用、维护所需要的相关技术文件纸质版至少 2 套,电子版资料 1 套。投标方提供的所有资料均应为中文版或中英文对照版。投标方提供本次采购设备所需的软件应为原装正版软件。具体要求提供资料如下:

- a. 出厂试验报告;
- b. 具备由国家认可的第三方出具的校验证证书;
- c. 产品合格证;
- d. 产品安装说明书和产品使用手册(包括:软件和硬件安装使用说明、系统功能说明、调试方法、维护项目、培训教程等等)。
- e. 其它相关图纸资料、测试数据、软件密钥等等;

9 监造、包装、运输、安装及质量保证

9.1 监造

本技术规范书采购设备无监造要求。

9.2 包装

1) 要严格按照制造厂给出的说明书对设备进行包装、运输和储存。制造厂应在交货前的适当时间提供设备的运输和储存说明书。

2) 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。其包装也应符合铁路、公路和海运部门的有关规定。

3) 包装箱上应有明显的包装储运图示标志， 并应标明招标方的订货号和发货号。

4) 设备的包装应能保证设备各零部件在运输过程中不致遭到脏污、损坏、变形、丢失及受潮。对于其中的绝缘部件及由有机绝缘材料制成的绝缘件应特别加以保护，以免损坏和受潮。对于外露的接触表面，应有预防腐蚀的措施。所有运输措施均应经过验证。凡有运输损坏，应由制造厂负责赔偿。

9.3 运输

1) 设备单独运输的零部件应有标志，便于用户安装装配。

2) 整体产品或分别运输的部件，都要适合于运输及装卸的要求。

3) 制造厂应提供按全部解体检修用的备品备件和装用机具，随同产品发运。

4) 随同运输的产品应附有装箱清单，产品所需提供的技术资料应完整无缺。

9.4 质量保证

1) 全部设备必须是全新的， 持久耐用的，应满足作为一个完整产品所能满足的全部要求。投标方应保证设备在规定的使用条件下运行、预期使用寿命应不少于 12 年。

2) 投标方应对其整组设备在到货后提供不少于 5 年的“三包”质量保证。之后如发生产品损坏，投标方应及时为本组装置提供维修部件，并按最近的投标价提供。

3) 订购的新型产品除应满足本标准外，投标方还应提供该产品的鉴定证书。

4) 投标方应保证制造过程中的所有工艺、材料试验等（包括投标方的外购件在内）均应符合本标准的规定。若招标方根据运行经验指定投标方提供某种外购零部件，投标方应积极配合。

5) 附属及配套设备必须满足有关行业标准的要求，并提供试验报告和产品合格证。

6) 投标方应有遵守本标准中各条款和工作项目的 ISO9000-GB/T19000 质量保证体系，该质量保证体系已经通过国家认证并在正常运转。

7) 对仪器设备在质保期内出现的故障，投标方人员在接到通知后应在 2 个工作日内派技术人员到现场检查处理，并立刻提出处理意见，免费进行维修。

8) 对于质保期已过的仪器设备，厂家将负责终身维修。对于一般的故障，处理时间 15 个工作日内。对于严重的故障，将根据情况安排维修时间的长短。

10 技术差异表

投标方应将所供设备与本招技术规范书技术文件有差异之处,无论优于或劣于本招技术规范书技术文件要求,均汇集至表 10.1。

表 10.1 技术差异表 (投标方填写)

序 号	招 标 文 件		投 标 文 件	
	条 目	简 要 内 容	条 目	简 要 内 容

投标方: _____ 盖章:

11 投标方需说明的其他问题

如有需说明的其他问题,投标方应通过书面形式提交,并加盖公章。