福海创石化PTA工厂余热发电项目电力监控系统等级保护测评及安全防护评估与整改加固项目技术规范书

发包签核单

一、项目发包说明：

对福海创石化 PTA 厂余热发电项目进行电力监控系统等级保护测评及安全防护评估与整改加固

发包依据：

1、国网漳州供电公司受电工程竣工验收意见：厂站未进行系统定级、备案、等级保护测评和安全评估

2、国网漳州供电公司关于预备役[redacted]余热发电项目接入系统设计评审意见的函第二点第八条根据《信息安全等级保护管理办法》（公通字[2007]43号）规定，翔鹭余热电厂应开列电力监控系统登记保护测评及安全评估费用，等保测评备案[redacted]要求按照国家能源局关于印发《电力行业信息安全等级保护管理办法》的通知（国能安全[2014]318号）十三条执行，到所在地市级以上公安机关办理备案手续，并将相关证明报送漳州地调备案。

发包内容详见：《余热发电项目进行电力系统等级保护测评及安全防护评估技术规格书》

二、承揽商资质要求：

[redacted]公安部及国家能源局认可的电力行业等级保护测评中心实验室或是具有此资质证书的授权单位并提供授权承诺函证明；

②、投标方或授权商应具有连续2年（2018-2019），在国网福建省电力公司实施等保测评的经验并提供相应的合同证明；

③、投标方或授权商应提供专业技术人员的信息安全专业认证证书，投标中部具有等级保护测评资质人员应包含1名高级测

翔鹭石化余热发电厂

电力监控系统等级保护测评及安全防护评估

与整改加固项目技术规范书

2023年[redacted]

1 总则

1.1 引言

为了落实公安部、国家能源局关于电力监控系统安全等级保护的[illegible]

1.2 适用范围

本技术规范适用于电力监控系统等级保护测评及安全防[illegible]

采购，包括技术服务要求和验收要求。

1.2.1 本技术规范提出的是最低限度的技术要求。凡本技术规[illegible]

国家标准、电力行业标准或IEC标准中有规定的规范条文、[illegible]

文进行服务供应说明。

1.2.2 如果投标方没有以书面形式对本技术规范的条文[illegible]

方提供的服务完全符合本技术规范。

1.2.3 本技术规范所建议使用的标准如与投标方所[illegible]

严格标准的条文执行或按双方商定的标准执行。

1.3 标准和规范

[illegible]

规定外，投标方所提供的测评标准均应遵[illegible]

- 《GB/T 25058 信息安全技术 网络安全等级保护实施指南》（正在修订）
- 《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》

项目概况

本项目[illegible]总降变 VII 段母线，数据接入国网漳州电力调控中心。

1.5 项目范围

电力监控系统信息安全等级保护测评与安全防护评估范围如下：

[illegible]

威胁评估、脆弱性评估、

做一步测算后报价，如有

程整项。

理和安全运维管理等十个方面的安全测评；

电力监控系统安全防护评估的主要内容包括：资产评估、

现有安全措施有效性评估等。

注：投标方应到工作现场实际核对工程量（数量）及

遗漏、缺项、计算错误均视为投标方优惠报价，不予调整

2 技术规范

2.1 测评及评估原则

本项目实施方案设计与具体实施应满足以下原则

2.1.1 保密性原则：项目实施方应与招标方签订保密

保密协议，对测评的过程数据和结果

数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害招标方的权益，否则招标方有权追究投标方的责任。

2.1.2 标准性原则：测评及评估方案的设计与实施应依据国家的相关标准进行。

2.1.3 规范性原则：项目实施方案和过程和文档，应具有规范性，便于项目跟踪和控制。

2.1.4 可控性原则：项目的进度应符合进度安排，保证招标方对测评工作的可控性。

2.1.5 整体性原则：测评及评估的范围和内容应系统、全面、规范，满足等级保护和安全防护评估的相关基本要求。

2.1.6 最小影响原则：技术测评及评估工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评及评估应在招标方许可的条件下进行。

包括项目概述、等保测评方案、安全防护评估方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。投标方应详细描述测评及评估人员的组成、资质及各自职责的划分。投标方应配置经验丰富的测评及评估人员进行电力监控系统等级保护测评及安全防护评估工作。

2.2.1 测评及评估方法

测评及评估方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。

实施方案，范围、收集材料、签署保密协议、组建测评及评估委员会并进行培训、

前的安全教育工作，同时完成检测工具、装备配置等各项准备工作。

3.2.2.2 启动阶段

工作周期：1～2 个工作日

[redacted]

测评及评估操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

（2）人员与数据管理

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备（系统）或临时搭建的模拟环境进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统在线应急处置能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评操作。

2.3 进行整改周

2.4 等级保护测评内容

根据国家等级保护 2.0 相关标准，本次项目的安全等级保护测评应包括安全通用要求内容：

安全通用要求测评：包括安全物理环境、安全通信网络、安全区域边界、安全计

全区域边界部分是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等，涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

2.4.1.4 安全计算环境

安全计算环境部分是针对边界内部提出的安全控制要求。主要对象为边界内部的[illegible]和其他设备等，涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

2.4.1.5 安全管理中心

安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

2.4.1.6 安全管理制度

安全管理制度部分是针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

2.4.1.7 安全管理机构

安全管理机构部分是针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

2.4.1.8 安全管理人员

安全管理人员部分是针对人员管理模式提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

2.4.1.9 安全建设管理

安全建设管理部分是针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。

2.4.1.10 安全运维管理

安全运维管理部分是针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理

理。

2.5 安全防护评估内容

根据电力监控系统安全防护评估相关标准，在系统等级保护测评的基础上，增加如下评估项：资产评估、威胁评估、通用应用评估、基础设施安全评估、体系结构安全评估、系统软件安全评估、人员管理评估、安全应急能力评估、现有安全措施的有效性评估等。

2.5.1 资产评估

资产评估对象包括：网络、主机、安全防护措施、应用系统等。根据安全防护评估有关技术要求，资产评估主要考虑两个方面的内容：一是信息系统中所存储、处理、传输的主要信息，二是信息系统所提供的主要服务。通过对每一类信息和服务等级分析，最终确定信息系统的重要性级别。资产评估具体步骤包括：资产数据整理与核实、资产重要程度分析。其中，资产数据整理与核实是根据评估单位提供的资产清单，进行资产数据的真实性的查证与确认。资产重要程度分析是根据资产承载的数据、提供的服务，判定资产重要程度的过程。

2.5.2 威胁评估

威胁评估是对被评估单位业务系统、网络与信息系统面临的威胁进行分析的过程。威胁评估的依据是电力监控系统安全防护评估规范的威胁部分，也可以结合被评估单位的实际情况进行补充。威胁评估的方式是通过调查问卷、人员访谈、现场检查、工具测试等方式进行。被评估单位能够提供历史信息安全事件统计，可以作为威胁评估的补充内容。通过威胁评估，要达到明确被评估单位信息系统面临的主要威胁，以及这些威胁的等级的目的。

2.5.3 通用应用评估

通用应用评估是对信息系统中的数据库服务、Web服务等通用应用进行的安全配置检查，达到发现该类应用存在的安全漏洞的目的。通用应用评估可以采取基于主机漏洞扫描两种方式进行。

2.5.4 基础设施安全评估

基础设施评估是对电力监控系统所处的物理安全防护情况，包括防水、防静电、防雷击、防盗窃、防破坏措施实施情况，电子门禁的使用情况等进行评估。

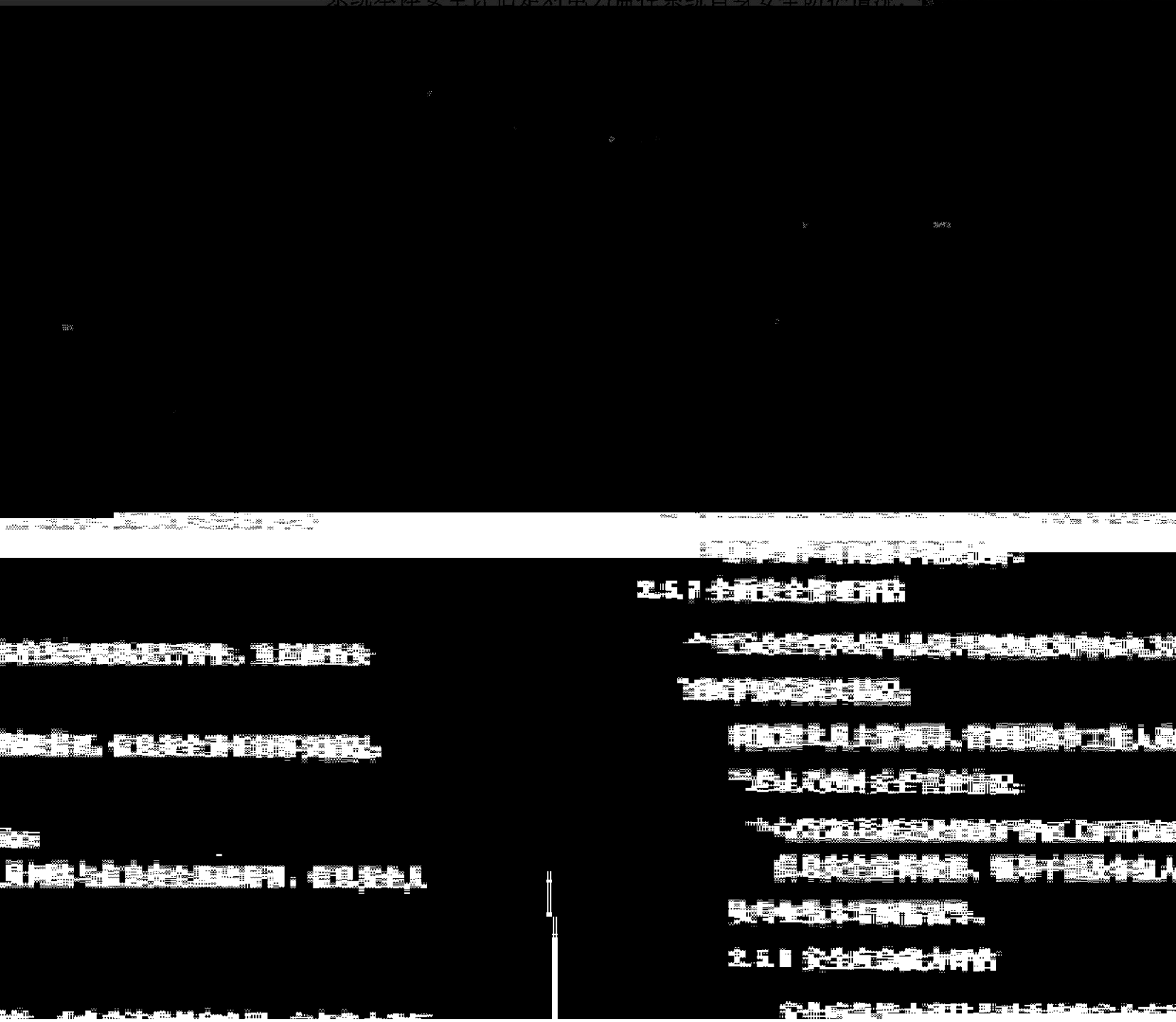
电力监控系统设备及线缆的部署情况，包括服务器、网络设备、安全设备的安装、设备电力供应情况等。

2.5.5 体系结构安全评估

体系结构评估应重点检查 16 字方针“安全分区、网络专用、横向隔离、纵向认证”的落实情况，重点针对网络边界防护措施、横向隔离、纵向认证等关键防护措施的执行情况，安全接入区的设置情况、无线网络防护等。

2.5.6 系统本体安全评估

系统本体安全评估是对电力监控系统自身安全防护情况[illegible]



况等；

网络与信息安全应急预案的制定、修订情况，包括应急预案是否健全，是否具有针对性和可操作性等；

应急技术支撑队伍建设、应急演练的执行情况；

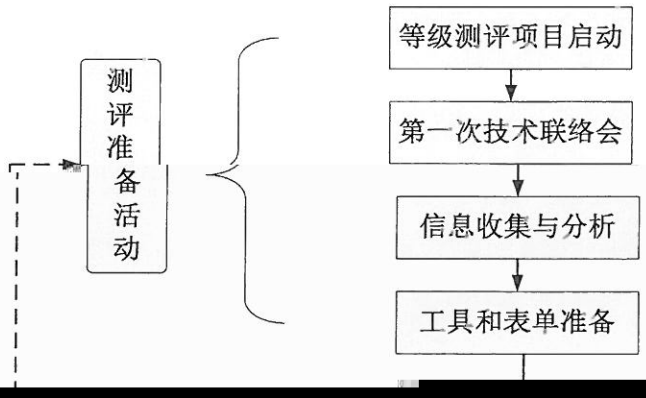
重大网络安全事件处置情况。

2.5.3 现有安全措施有效性评估

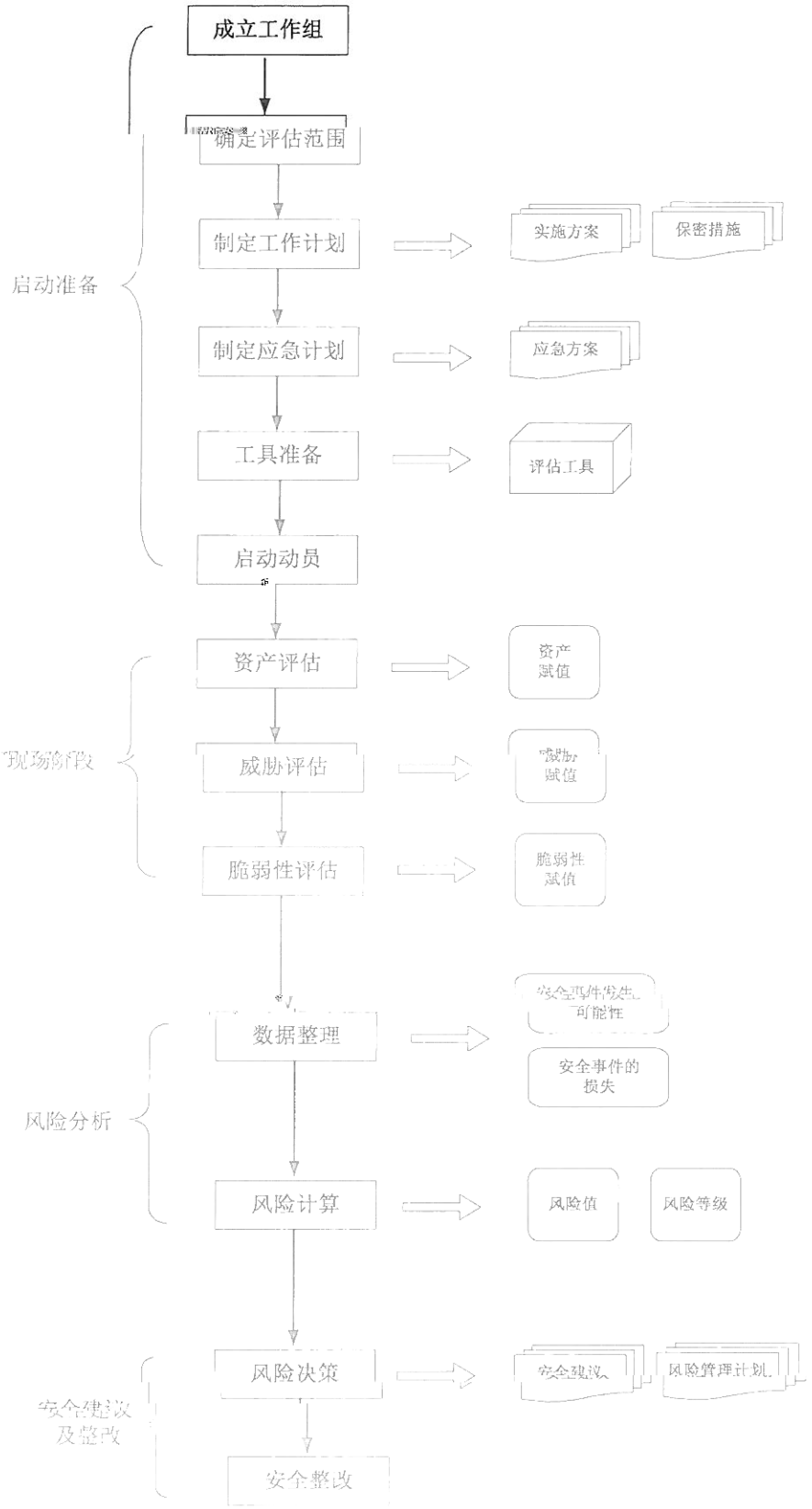
现有安全措施有效性评估是对信息系统中部署的主要安全防护措施进行的审计，[illegible]达到确定这些安全措施的管理和使用情况是否存在重大漏洞和缺陷，明确现有安全措施的有效性程度的目的。现有安全措施的评估主要采用人工检查和访谈的方式进行。[illegible]主要包括防火墙、防病毒系统、入侵检测防御装置、防病毒网关、单向隔离装置、纵向认证装置等现有安全措施。

2.6 测评及评估流程

根据国家等级保护相关规范，电力监控系统安全等级保护测评流程分为[illegible]


测评准备活动
等级测评项目启动
第一次技术联络会
信息收集与分析
工具和表单准备

范，进行分类和启动准备阶段，现场数据采集评估阶段，风险计算和分析阶段，以及总结阶段。



3、 项目服务商要求

3.1. 服务团队技术要求

投标方应仔细阅读本技术规范书所列的各项规范，所提供的安全服务应满足本技术规范书提出的要求。投标方也可以推荐满足本技术规范的其他方案，但必须对其在二次技术规范中所与本技术规范书之间所存在的差异部以详细说明。若无说明，则视为对投标方标书的充分理解。

投标方及投标产品应满足以下要求：

① 为满足电力行业和公安部门的要求，投标方或授权商应属于公安部及国家能源局认可的电力行业等级保护测评中心实验室或是具有合格资质证书的测评机构并提供授权承诺函证明；

② 投标方或授权商应具有连续2年（2018-2019）为国网系统省公司及以上单位提供等保测评的经验并提供相应的合同证明；

③ 投标方或授权商应提供专业技术人员的资质证书，具有高级等保测评师证书，有等级保护测评资质人员应包含1名高级测评师和1名CISP认证测评师；

④ 投标方或授权商须具有中国信息安全认证中心颁发的《信息安全风险评估服务资质》二级及以上；

⑤ 投标方或授权商须具有中国合格评定国家认可委员会颁发的CNAS证书。

3.2 驻场服务人员要求

投标方应与招标方签订保密协议，对检测和加固过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害招标方的权益，否则招标方有权追究投标方的责任。

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

测评选择备用设备（系统）或临时搭建的模拟环境进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统在线应急处置能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评。

4 工程管理

4.1 项目验收

验收应按照招标方确认的验收测试大纲进行，全过程必须由招标方在场见证。

- 等级保护测评及安全防护评估项目应编制等级保护测评及安全防护评估报告，该项目将产生一定数量的文档。
- 投标方应对所有正式交付件的综合质量负责，指定各交付件的相关责人，明确相关职责。
- 投标方应提交验收流程、验收方法和验收依据。
- 投标方应提供交付件归档办法和方式。
- 投标方应提供详细的验收测试大纲或计划，大纲中应明确规定验收须满足的要求。大纲必须经招标方确认后方可生效。
- 验收报告需双方代表签字认可。

4.2 项目文档

4.2.1 投标方提供的资料应使用国际单位制（SI），语言为中文。

4.2.2 资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整。如所供资料不能达到要求时，投标方应免费给予补充。

4.2.3 投标方资料的提交必须按合约规定的时间节点要求。

4.2.4 投标方完成项目后应提供以下文档：

表 3-1 投标方完成项目提供文档列表

序号	文档名称	提交时间	备注
1	《测评方案》	签署合同后1周	电子版
2	《系统自查指南》	签署合同后1周	电子版
3	《系统安全等级保护测评报告》	现场测评后1周	正式版
4	《电力监控系统安全防护评估报告》		

4.3 质量保证

投标方在项目方案设计、实施、验收的各个阶段，应符合国家和行业规定运行的要求。

投标方出具的相关报告应得到行业主管单位认定。

4.4 保密要求

投标方承担被测评及评估单位敏感信息的保密义务。

要复制双方提供的保密资料时，应经过书面申请，

并将数据内容记录成表，签字确认。

未经双方书面同意，不得向第三方透露项目实施及双方的商业信息等，包括但不限于的任何内容。

项目结束后，双方必须互相确认测评过程中提供的相关资料，