

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评估与整改加固

发包依据：

1、国网漳州供电公司发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漳州翔鹭石化有限公司余热发电

系统回收再利用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，等级保护备案

测评要求按照能源局关于印发《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：

①、为满足电力行业公安部门的有关要求，投标方或授权代理商

必须具有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

电力公司电网获得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，机构内部具有等级保护测评资质人员应包含1名高级测

评师和1名中级测评师；

④ 投标方或授权商应具有在国网福建省电力有限公司范围内

开展等级保护测评的经验；

⑤ 投标方或授权商应具有在国网福建省电力有限公司范围内

开展业务。

4. 投标人应提供近三年内所承担过的类似项目的业绩证明，

业绩证明是指近三年内所承担过的类似项目的合同复印件，

合同复印件应包含但不限于项目名称、项目内容、项目金额、

合同签订日期、合同有效期、

合同编号、合同金额、合同签订日期、合同有效期、

合同金额、合同签订日期、合同有效期、

■

■

■

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

——整改加固报告及整改技术规范书

2018年11月

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防护等级保护测评工作的要求

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护采购，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。凡本技术规范国家标准、电力行业标准或 IEC 标准中有规定的规范条文，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各项要求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

下列标准中的条款通过本规范的引用而成为本规范的一部分。除本技术规范另有规定外，投标方所提供的测评标准均应遵循

➤ 《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》

1.4.1 招标方责任

为切实保证本项目的工作质量，确保测评及评估工作达到预期目标，针对项目实施方双方技术工作责任约定如下：

1.4.1 招标方责任

- 负责测评实施过程中同相关单位和部门的协调。
- 为项目实施方提供良好的工作场地和环境。
- 按工作要求提供相关的资料和信息。
- 准备应急措施，负责实施过程中的紧急情况的处理。

1.4.2 项目实施方责任

- 按照招标方工作章程开展工作。
- 项目内容的变更及时与招标方代表沟通。
- 按照协议要求提供技术服务和成果。
- 确保测评及评估工作质量。
- 能容招标方在应急响应和实施过程中出现的紧急情况处理。
- 负责按时完成所有工作。

同时，双方都必须遵循保密要求。

项目概况

本项目为属翔鹭石化(漳州)有限公司金热电厂,装机容量156MW,设置空冷33台,升压站新增一台220kV主变,原在品字站内的电能变换系统升压后接入220kV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:

(1) 完成电力监控系统内、信息安全管理系统

...

...

理和安全运维管理等十个方面的安全测评;

威胁评估、脆弱性评估、

中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。

做一步测算后报价,'如有
后工程款项。

注: 投标方应到工作现场实际核对工程量(数量)及
遗漏、缺项、计算错误等项为投标方负责,不予追究。

2 技术规范

2.1 测评设计原则

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

陈

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 规范性原则：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 可追溯原则：投标方应详细记录测评过程和文档，应留有规范记录，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。

投标方应提供详细方案、项目实施方案、时间安排、阶段划分、人员安排等，并详细描述测评及评估人员的组成、资质及各自职责。

测评及评估人员进行电力监控系统等级保护测评、配置检查、漏洞扫描、渗透测试和测试三种方法，可细化为文档审查、配置检查、漏洞扫描、渗透测试和测试三种方法。

投标方应提供详细方案、项目实施方案、时间安排、阶段划分、人员安排等，并详细描述测评及评估人员的组成、资质及各自职责。投标方应配置经验丰富的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、漏洞扫描、渗透测试和实地察看等多种方法。

实施方密、范围、收集材料、签署保密协议、做好组建测评及评估项目组并进行培训、测评前的安全教育工作，同时完成检测工具、装备配置等各项准备工作。

2.2.2.2.2 启动阶段

工作周期：1~2 个工作日

工作准备：项目启动前被测单位应收集并准备好资料，网络资料、业务系统资料、信息安全管理规章制度等相应测评所需材料，并召开启动会。就测评及评估事宜进行落实，包括确定测评及评估计划安排、测评及评估范围、测评工

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，在测评及评估前制定应急预案，加强系统在线应急处理能力。

（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。

2.3 进行整改加固

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

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、

算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全

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

安全管理体系的制定是面向整个系统提出的安全管理方面的技术控制。卡毛段应实现集中管理。涉及的的安全控制点包括系统管理、审计管理、主备、日志、灾难恢复管理。以磁盘上的安全控制点包括系统告警、管理、主备、日志、灾难恢复管理。

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。

2.4.1.7.1 女生管理机构

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点包括岗位设置、人员配备、授权和审批、沟通和合作以

2.4.1.8 安全管理人员

安全管理人員部分針對人員管理模式提出的安全控制
包括人員選聘、人員離崗、安全意識教育和培訓以及外聘

安全建设管理产品是为针对安全建设过程提出
包括定级和备案、安全主体策划、安全主体策划
发、工程实施、测试验收、系统交付、等级测

2.4.1.6 安全运维管理

安全管理部分是针对安全运维过程

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、系统运行安全评估、安全管理责任评估、安全应急预案评估、现有安全措施有效性评估等。

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等级别。资产评估具体步骤包括:资产数据整理与分类、资产重要程度分析。其中资产数据整理与分类是根据法律法规标准程序对资产承载的数据、资料,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。威胁评估应依据《电力监控系统安全防护规定》及相关标准,结合被评估单位资产数据整理与分类结果,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面临的威胁等级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,及时发现通用应用安全漏洞缺陷,并采用两种方式进行。

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环境中的物理安全、网络安全、电磁兼容、防火、防静电、防雷击、防窃密、防破坏等安全措施实施情况,电子门禁的使用情况等等进行评估。

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。通信线缆和电源线的铺设情况。

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，安全接入区部署设置情况、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，包括的、可修改的系统软、

2.5.7 全面安全管理评估

“六统一”安全管理原则，从管理、技术、制度等方面，对电力监控系统安全防护工作进行全面评估。

中电联《电力监控系统安全防护规定》、《电力监控系统安全防护管理办法》等文件。

“六统一”安全管理原则，从管理、技术、制度等方面，对电力监控系统安全防护工作进行全面评估。

2.5.8 安全应急响应能力评估

评估电力监控系统安全防护工作应急响应能力，包括应急响应组织、应急响应流程、应急响应资源等。

2.5.9

“六统一”安全管理原则，从管理、技术、制度等方面，对电力监控系统安全防护工作进行全面评估。

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。

2.5.9 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,旨在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等的目的。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。

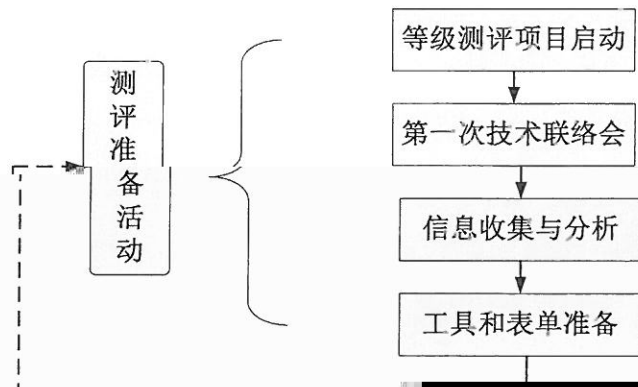
主要包括防火墙、防病毒系统、入侵检测防御装置、防病毒网关、邮件隔离装置、双向认证装置等现有安全措施。

2.6 测评及评估流程

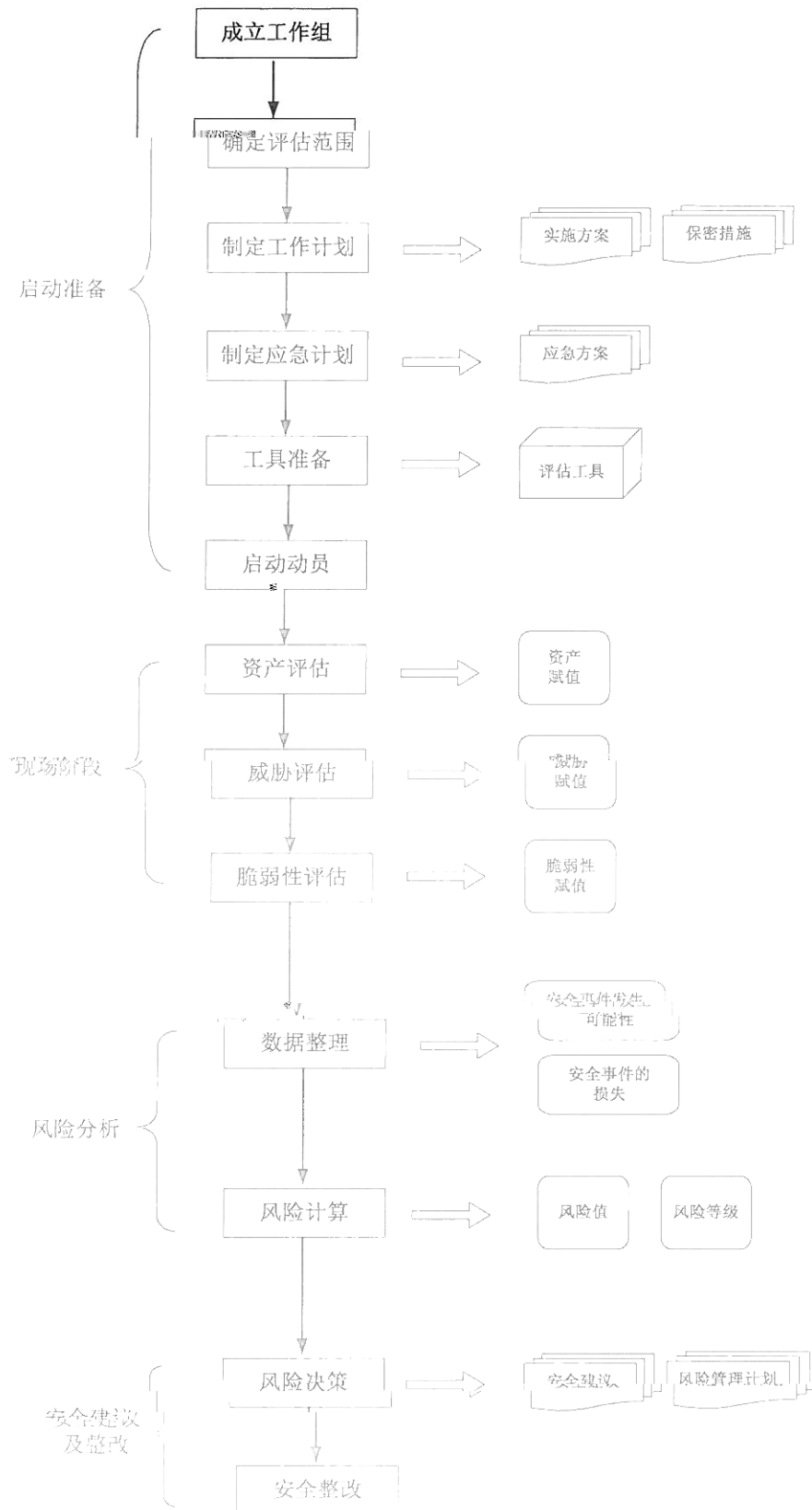
根据国家标准《信息安全等级保护基本要求》,信息安全等级保护测评流程分为

91-2005-01-01 发布 2005-01-01 实施

25



评估过程, 分为前期准备和启动准备阶段, 现场数据收集和评估阶段, 以及风险分析和总结阶段。



3. 项目服务商要求

3.1.1 明确团队技术要求

投标方应仔细阅读本技术规范书所列的各项规范，所提供的字全型设备亦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，但必须对其布、工、材料、规范与所出本技术规范存在的所有差异加以详细证明。若无法证明，则按对投标方所标为标的方面理解。

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质量监督检验检疫总局认可的电力行业等级保护测评中心实验室或是具有网络等级保护测评资质单位并提供授权承诺函证明；
- ② 投标方或授权商应具有自2018年7月1日至2021年12月31日期间等级保护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至少两名具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；
- ④ 投标方或授权商须具有中国信息安全认证中心颁发的《信息安全业务资质》二级及以上；
- ⑤ 投标方或授权商须具有国家合格评定委员会颁发的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

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。

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攻防评估项目目标超出等级保护测评及安全攻防评估项
目报告，该项目将产生完整等级保护项目。

➤ 投标方应对所有正式交付件的最终质量负责，指派各交付件的报告美
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等级保护测试大纲或计划，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、

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 投标方资料的编写应满足招标文件中规定的要求。

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	《电力监控系统网络安全风险评估报告》	现场测评后 1 周	正式版

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，应严格按照国家、行业、地方标准及合同要求，保证系统安全稳定运行的要求。

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

投标方承担被测系统及评估单位敏感信息的保密责任，不得向第三方泄露。在项目实施过程中，如需使用被测系统的数据，应事先书面申请，在得到甲方书面同意后，方可使用，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所涉及双方的商业秘密及安全、技术等任何内容。

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，相互承担保密责任。