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工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福海创石化（漳州）有限公司低温余热余压回收利用项目接入系统设计评审意见的函第二十五条要求根据

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，投标方须具备等级保护测评资质人员应包含1名高级测评 [illegible]

[illegible]

[illegible]

[illegible]

[illegible] CMMS证书。

[illegible]

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

与整改项目技术规范书

2020 年 09 月

1 总则

1.1 引言

办法》(国能安全[2014]317号)

和《电力行业信息安全等级保护管理办法》(国能安全

全[2014]318号)等制度和标准要

求，进行本次电力监控系统等级保护测评与安全

防护评估。

1.2 适用范围

IEC标准中有规定的规范条文，投标方应按相应标准的条

国家标准、电力行业标准或

文进行服务供应说明。

书面形式对本技术规范的条文提出异议，则招标方认为投标

1.2.2 如果投标方没有以

完全符合本技术规范。

方提供的服务完全符

条文执行或按双方商定的标准执行。

严格标准的条

1.3 标准和规范

- 《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）

项目概况

本项目为翔鹭石化（漳州）有限公司余热电厂……升压站，新增……主变压器……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）……电力监控系统……信息安全防护系统……

（2）完成……等级保护相关……调备案的相关工作。

（3）工程涉及文档整改（安全管理制度不完善或缺失等）。

（4）电力监控系统等级保护测评工作需提交公安部门和国家能源局认可的等级保护测评2.0版本报告，电力监控系统安全防护评估报告。

（5）根据国家等级保护相关标准，电力监控系统属于工业控制系统，安全等级保护测评应包括安全通用要求，测评内容如下：

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、安全建设管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、威胁评估、脆弱性评估、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）及做一步测算后报价，如有遗漏、缺项……不予追加工程款项。

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

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。

实施方案，项目组织协调管理等准备阶段，组建测评及评估项目组，并进行现场实施前的安全教育工作，同时完成检测工具、装备配置等各项准备工作。

2.2.2.2启动阶段

工作周期：1～2个工作日

工作内容：项目组进驻被测单位，收集系统信息资产、被测系统资料等，进行审核，包括确定测评及评估的时间安排、测评及评估范围、测评及评估内容和配合需求等。

整改加固：7个工作日

2.2.2.3现场测评

工作周期：4-5个工作日

工作内容：项目组从管理和技术两个方面入手，开展被测单位测评及评估工作，包括安全区域划分、网络专用、评估管理和制度、基础网络、业务系统、通用服务、主机系统、数据库系统、现有安全措施等。

测评及评估方法有顾问访谈、日志审计、人工查看、漏洞扫描等。

现场工作结束后，测评及评估工作组对现场测评情况进行初步整理汇总，向被测单位领导和系统管理员等汇报现场阶段工作情况。

2.2.2.4结论分析报告编制阶段

工作周期：3～4周

工作内容：项目组对检测情况和采集的数据进行分类统计、风险计算、综合分析与评估，编写被测单位系统《等级保护测评报告》及《监控系统安全风险评估报告》。

2.2.2.5整改技术支持阶段

工作周期：根据整改进度而定

工作内容：项目组针对现场测评及评估发现的问题，出具整改建议后，向被测单位提供整改技术咨询支持。

2.2.3风险控制

测评及评估工作本身也会引入安全风险，必须加强测评及评估过程中的风险控制

测评及评估操作必须遵守现场运行管理制度，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）测评机构选择

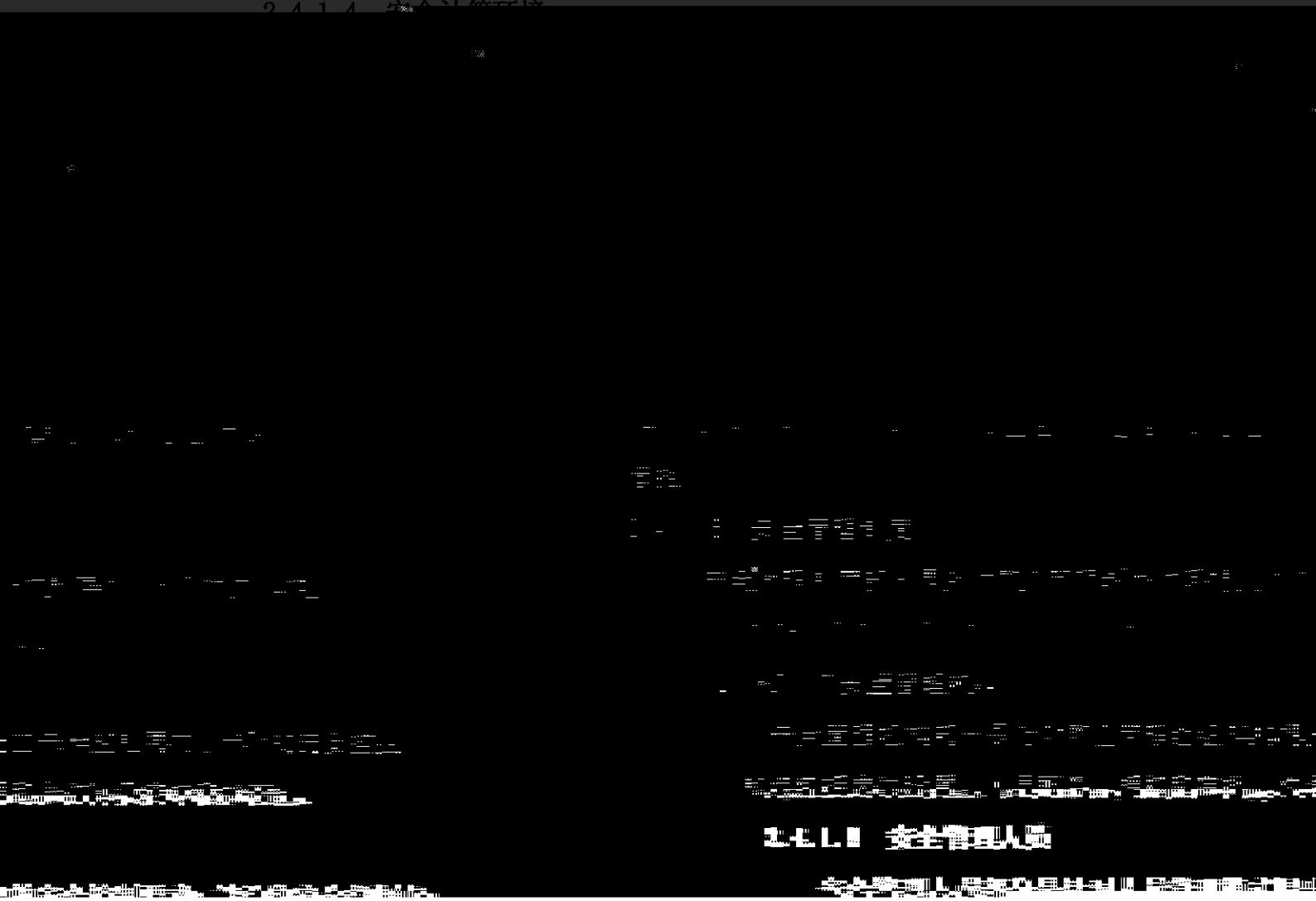
[redacted]

线系统运行。

[redacted]

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



理。

2.5 安全防护评估内容

有效性评估等。

2.5.1 资产评估

2.5.2 威胁评估

2.5.3 通用应用评估

2.5.5 体系结构安全评估

体系结构评估应重点检查"安全分区、网络专用、横向隔离、纵向认证"的落实情况，重点包括网络边界防护措施（横向隔离、纵向认证等关键防护措施）的部署情况、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，包括软、硬件

来进行。

2.5.7 全面安全管理评估

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。

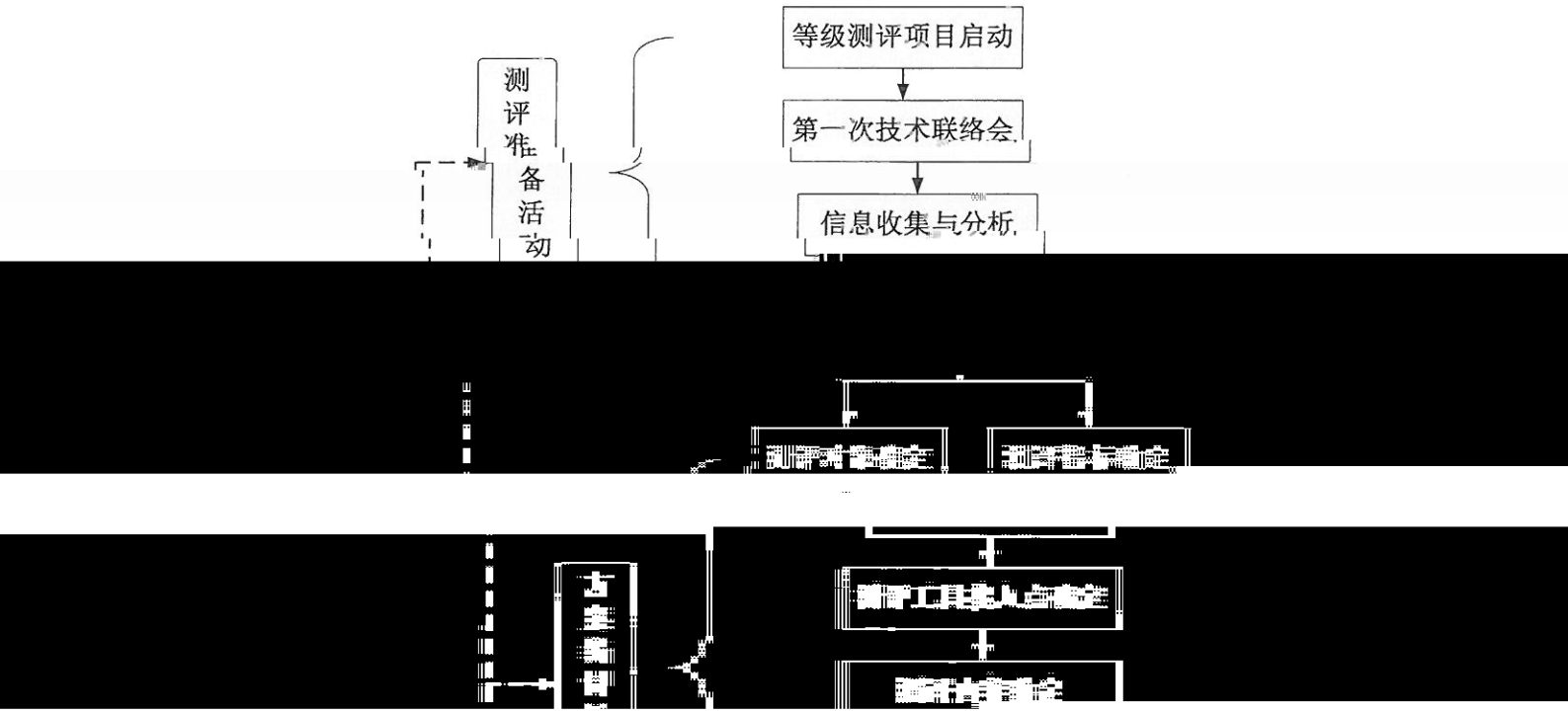
2.5.9 现有安全措施有效性评估

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，[illegible]措施的有效性[illegible]方式进行。[illegible]隔离装置[illegible]向认证装置等现有安全措施。

2.6 测评及评估流程

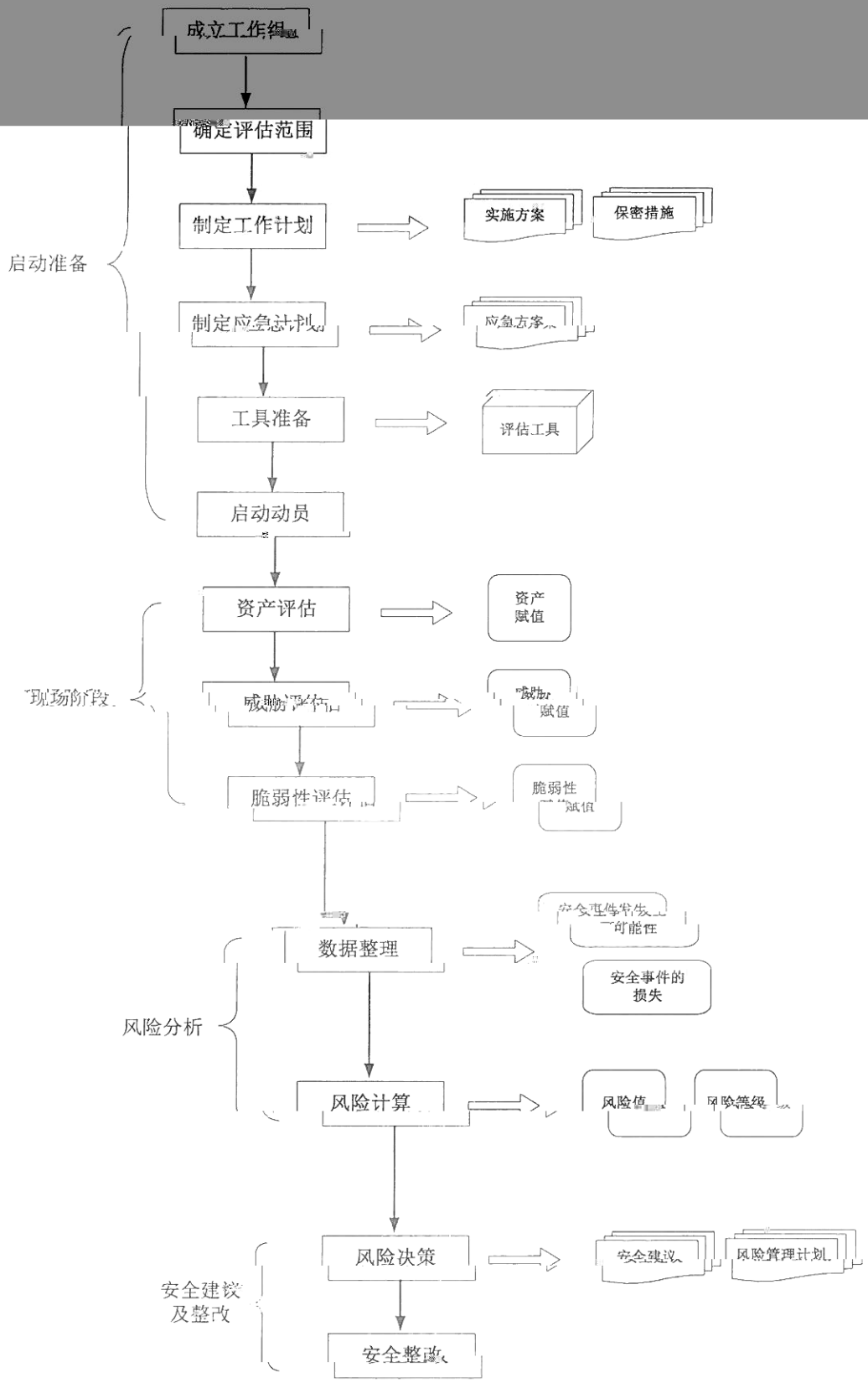
根据国家等级保护相关标准，电力监控系统安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，提供整改建议，配合招标方根据测评范围进行整改方案实施。

电力监控系统的安全等级保护测评流程如下图所示：



测评报告编制

范进行，分前期商洽和启动准备阶段、现场数据采集和评估阶段、二风险计算和分析阶段、以及总结阶段。



3、 项目服务商要求

8.1 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，所提供的产品和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，但必须对其在技术规范书中提出与本技术规范之间所存在的差异做详细说明。若无说明，则对投标方将按响应方理解。

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 3 年（2016-2018）在国网福建省电力公司实验等

[redacted]

靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

[redacted]

线系统运行。

（4）制定应急预案

[redacted]

能力。

（5）关键业务系统风险控制

[redacted]

4　工程管理

4.1　项目验收

[redacted]

[redacted]

人，明确相关职责。

[redacted]

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》	[illegible]	[illegible]
4	《电力监控系统安全防护评估报告》	现场测评后4周	[illegible]

4.3 质量保证

投标方在项目方案设计、实施、验收的各个阶 [illegible] [redacted]

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 [illegible] 的任何内容。

项目结束后，双方必须互相确认测评过程中 [illegible]