甘能化（兰州新区）热电有限公司
电力监控系统安全防护评估及等级保护测评技术服务技术规范书

1　总则

1.1 项目概述

为贯彻落实国家信息安全等级保护制度和国家发改委第 27 号令的相关规定，进一步增强电力监控系统安全防护能力，确保电力监控系统安全稳定运行，依据《信息安全技术　网络安全等级保护基本要求》（GB/T 22239-2019）、《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）、《中华人民共和国网络安全法》（2026 年修订版）、《电力监控系统安全防护规定》（2024 年发改委第 27 号令）和《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）、《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）等制度和标准要求，本着提高电力监控系统安全防护水平，落实信息安全等级保护工作，加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统的攻击及侵害，保障电力系统的安全稳定运行，甘能化（兰州新区）热电有限公司（以下简称甲方）组织开展电力监控系统安全防护评估及等级保护测评工作。

1.1.1 目标

甲方电力监控系统安全防护评估及等级保护测评项目的总体目标为：

依据国家和行业信息安全的相关标准，全面了解和掌握公司 NCS 监控系统（三级）、DCS 控制系统（三级）的安全保护状况，找出其与《电力行业信息系统安全等级保护基本要求》对应级别的差距，及时发现系统存在的安全问题，针对等保测评中发现的各种安全风险，提出适宜的安全整改建议，提供整改技术支持；

从风险管理角度，运用科学的方法和手段，系统地分析全厂电力监控系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性地抵御威胁的防护策略和整改措施，为防范和化解信息安全风险、将风险控制在可接受的水平、最大限度地防止由于电力监控系统安全事件引发电力安全事故、全面提升电力监控系统安全防护水平提供科学依据。

1.1.2 要求

甲方信息系统等级保护测评项目的总体要求为：电力监控系统安全防护和信息安全等级保护工作同步开展，两项工作一次完成，即通过一次现场测评（评估），出具两份报告（信

息系统安全等级测评报告和电力监控系统安全防护评估报告）。

1.2 适用范围

本技术规范书适用于电力监控系统安全防护评估及等级保护测评工作，包括技术服务要求和验收要求。

1）本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，但在相关国家标准、电力行业标准中有规定的规范条文，乙方应按相应标准的条文进行服务供应说明。

2）本技术规范书所建议使用的标准如与乙方所执行的标准不一致，乙方应按更严格标准的条文执行或按双方商定的标准执行。

3）本技术规范书经甲乙双方确认后作为实施合同的技术附件，与合同正文具有同等的法律效力。

1.3 测评（评估）依据及原则

1.3.1 测评（评估）依据

本次测评（评估）依据下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，凡是不注日期的引用文件，其最新版本适用于本规范。

- 《信息安全技术 信息系统安全等级保护基本要求》GB/T 22239-2019
- 《信息安全技术 信息系统安全等级保护定级指南》GB/T 22240-2020
- 《信息安全技术 信息系统安全等级保护实施指南》GB/T 25058-2019
- 《信息安全技术 信息系统安全等级保护测评要求》GB/T 28448-2019
- 《信息安全技术 信息系统安全等级保护测评过程指南》GB/T 28449-2019
- 《信息安全技术 信息安全风险评估规范》GB/T 20984-2022
- 《电力行业网络安全等级保护基本要求》DL/T 2614-2023
- 《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）
- 《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）
- 《电力监控系统安全防护规定》（2024 年发改委第 27 号令）

1.3.2 测评（评估）原则

标准性原则：乙方方案的设计与实施应依据国家等级保护和电力行业的相关标准进行；

规范性原则：乙方工作中的过程和文档，具有很好的规范性，以便于项目的跟踪和控制；

整体性原则：项目实施的范围和内容应当整体全面，包括安全涉及的各个层面（网络、

主机、应用、物理、数据、管理制度、管理机构、人员管理、系统建设、系统运维），避免由于遗漏造成评估不准；

可控性原则：实施方法和过程需要在双方认同（认可）的范围之内，项目进度要严格按照项目工作计划执行，保证甲方对于评估工作的可控性；

最小影响原则：项目实施工作应尽可能不影响系统和网络的正常运行，不能对现有网络的运行和业务的正常运行产生明显影响（包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况必须详细描述说明）；

保密原则：对项目实施中产生的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害甲方利益的行为，否则甲方有权追究乙方的责任。

1.4 权利和职责

为切实保障本项目的工作质量，确保测评（评估）工作达到预期目标，对甲乙双方技术工作责任约定如下：

1.4.1 甲方责任

1) 负责测评（评估）过程中相关单位和部门的协调。
2) 为乙方提供良好的工作场地和环境。
3) 按工作要求提供相关的资料和信息。
4) 准备应急措施，负责实施过程中的紧急情况的处理。
5) 明确专人全程配合乙方开展现场测评（评估）。

1.4.2 乙方责任

1) 按照甲方工作章程开展工作。
2) 项目内容发生变更及时与甲方代表沟通。
3) 依据国家和行业相关标准开展测评（评估）工作，确保测评工作质量。
4) 按照协议要求提供技术服务和成果。
5) 配合甲方准备应急预案，并参与实施过程中的紧急情况处理。
6) 制定具体测评（评估）实施计划方案。
7) 协助甲方人员完成相关管理制度、安全事故现场处置方案、应急预案等与电力监控系统及信息安全相关的制度建立、修订，并指导完成应急演练工作。
8) 针对发现的问题编制解决方案并提出整改措施，以消除风险。

2 工程环境

2.1 施工地点

甘能化（兰州新区）热电有限公司 2×350MW 超临界抽凝式间接空冷供热机组，同步建设脱硫、脱硝设施，位于甘肃省兰州新区西岔园区西岔镇段家川村淮河大道东段 1688 号，于 2025 年建设完成并投入使用。

2.2 机组概况

全厂现有两台 350MW 超临界机组，均已投入商业运行。

3 电力监控系统简介

公司电力监控系统主要包括以下系统：主机 DCS 监控系统、脱硫 DCS 监控系统、输煤 DCS 监控系统、除灰、除尘 DCS 监控系统、化学 DCS 监控系统、330kV 升压站综合自动化监控系统（NCS）、远动及 AGC/AVC 系统、厂用电气监控系统（ECMS）、电能量采集系统、环保信息子站采集系统、宽频同步相量测量系统（PMU）、稳控装置、快切装置、330kV 系统保护（线路保护、母线保护、发变组保护、继电保护及故障信息子站）、五防系统、励磁调节装置、故障录波装置。

监控系统安全分区表

序号	业务系统及设备	控制区（安全区Ⅰ）	非控制区（安全区Ⅱ）	管理信息大区	备注
1	火电机组分散控制系统 DCS	#1、#2 机组 DCS 脱硫 DCS 输煤 DCS 监控系统、 除灰、除尘 DCS 监控系统、 化学 DCS 监控系统 启动锅炉房 DCS 监控系统			A2
2	火电厂厂级信息监控系统（监控功能）	ECMS 系统 快切装置			A2
3	调速系统和自动发电控制功能 AGC	DEH 远动及 AGC 系统			A1
4	励磁系统和自动电压控制功能 AVC	#1、#2 励磁调节器 远动及 AVC			A1
5	网控系统	330kV 监控系统（NCS）			A1
6	相量测量装置 PMU	PMU			B
7	自动控制装置（PSS、汽门快关等）	励磁调节器 PSS 功能 稳控切机装置			B.A1
8	五防系统	五防操作员站			A2
9	继电保护装置及管理终端	线路保护 母线保护 发变组保护 继电保护及故障信息子站			B B B B B

10	故障录波装置		#1、#2 机组及线路故障录波装置		B
11	电能量采集装置		电能量采集		B.A1
12	脱硫、脱硝信息子站		环保信息子站		A1
13	脱硫、脱硝 CEMS		脱硫 CEMS 脱硝 CEMS		

4 项目测评（评估）范围

服务范围	服务内容	
定级备案	系统定级、备案提供咨询服务	
等级测评	第三级	NCS 监控系统
		DCS 控制系统
安全评估	全厂电力监控系统安全防护评估	
培训服务	提供有关电力行业信息安全等级保护和电力监控系统安全防护方面的培训	
咨询服务	围绕信息安全等级测评和电力监控系统防护安全评估，提供安全建设整改方面的咨询服务	
制度、预案完善	协助甲方完善相关制度、预案	

5 项目工作内容

5.1 测评（评估）内容

5.1.1 等级测评

乙方依据相关国家及行业等级保护技术标准对甲方已定级信息系统进行业务现状调研，通过现场测评、整体分析及风险评估工作，全面准确评估业务系统安全保护水平与等级保护相应级别之间的差距，对于发现的问题提出整改建议，最终形成电力监控系统安全防护评估报告和等级测评报告。

测评方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地查看等多种方法。

如需在等级保护测评及电力监控系统安全防护评估实施过程中采用在线测评工具的，安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由乙方推荐，测评软件及工具必须通过国家认可机构的安全检测/认证，且经甲方确认后由乙方提供并在测评中使用。应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应是经过测试、稳定可靠的。

安全测评需要的运行环境（如场地、网络环境等）由甲方提供，乙方应详细描述需要的运行环境的具体要求。

等级测评分安全技术及安全管理两大方面共十个层面的单元测评，以及在此基础上进行的系统整体测评和后续的风险分析。

5.1.2 单元测评

1）物理环境测评：包括位置、访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电磁防护等内容。

2）网络系统测评：包括网络架构、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等内容。

3）主机与数据库测评：包括主机与数据库身份鉴别、主机与数据库访问控制、主机与数据库安全审计、主机与数据库入侵防范、主机恶意代码防范、信息资源安全、资源控制等内容。

4）应用系统测评：包括应用系统身份鉴别、应用系统访问控制、应用系统安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。

5）数据及备份恢复测评：包括数据完整性、数据保密性、备份和恢复等内容。

6）安全管理制度测评：包括管理制度、制定和发布、评标和修订等内容；

7）安全管理机构测评：包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查、资金保障等内容。

8）人员安全管理测评：包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容。

9）系统建设管理测评：包括系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、服务商选择等内容。

10）系统运维管理测评：包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。

5.1.3 整体测评

整体测评是对单元测评中发现的问题进行系统整体测评分析，包括从安全控制点间、层面间、区域间和系统结构等方面进行安全测评。

5.2 电力监控系统安全防护评估

根据国家及电力行业监控系统安全防护评估相关标准，在电力监控系统安全等级保护测评（即以上安全技术与安全管理测评）的基础上，增加如下测评项：资产评估、威胁评估、通用应用评估、现有安全措施有效性评估、终端检测、外设检测等。

5.2.1 资产评估：评估对象包括网络、主机、安全防护措施、应用系统等。根据被测评单位风险评估有关技术要求，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的分析，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被评估单位前期提交的资料，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承载的数据、提供的服务，判定资产重要程度的过程。

5.2.2 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。威胁评估依据《电力监控系统安全防护评估规范》提供的威胁列表，以运行与管理人员访谈的方式进行。如被评估单位能够提供历史信息安全事件统计，也可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。

5.2.3 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，达到发现通用应用安全漏洞的目的。通用应用评估也采用人工审计和漏洞扫描两种方式进行。

5.2.4 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，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。主要包括防火墙、防病毒系统、防病毒网关等现有安全措施。

5.2.5 终端检测：主要为抽查被评估单位办公终端和上网终端是否有驻留木马、蠕虫、恶意软件，是否存在自定义共享文件夹，系统补丁是否及时更新安装，关键工作文件存放是否恰当等情况。主要通过人工查看和工具检测两种方式来进行。

5.2.6 外设检测：主要面向带有硬盘、内存或其他存储设备和简易操作系统的网络打印机、传真机等智能设备。具体工作为判断外设是否未设置管理员口令；是否默认开放了 FTP、TELNET、SNMP、WEB 等服务，导致攻击者可以轻易控制该设备或发送大量请求而进行拒绝服务攻击。具体工作通过人工查看配合工具监测两种方式来进行。

6 测评（评估）进度

甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评工作时间的总体要求为：本年度 4 月至 12 月。合同签订 7 日内，乙方按照电力监控系统安全防护评估及等级保护测评的工作要求，协助甲方完成被测评系统的等保自查和电力监控系统安全防护自评估工作，并及时提交现场评估实施方案，经同意后 3 个工作日内开展项目现场实施工作。

具体进度如下：

阶段	阶段名称	时间（工作日）
第一阶段	自查自评估、基本情况调研	5
第二阶段	现场实施阶段	10
第三阶段	问题整改阶段	18
第四阶段	复测阶段	5
第五阶段	报告编制阶段	15

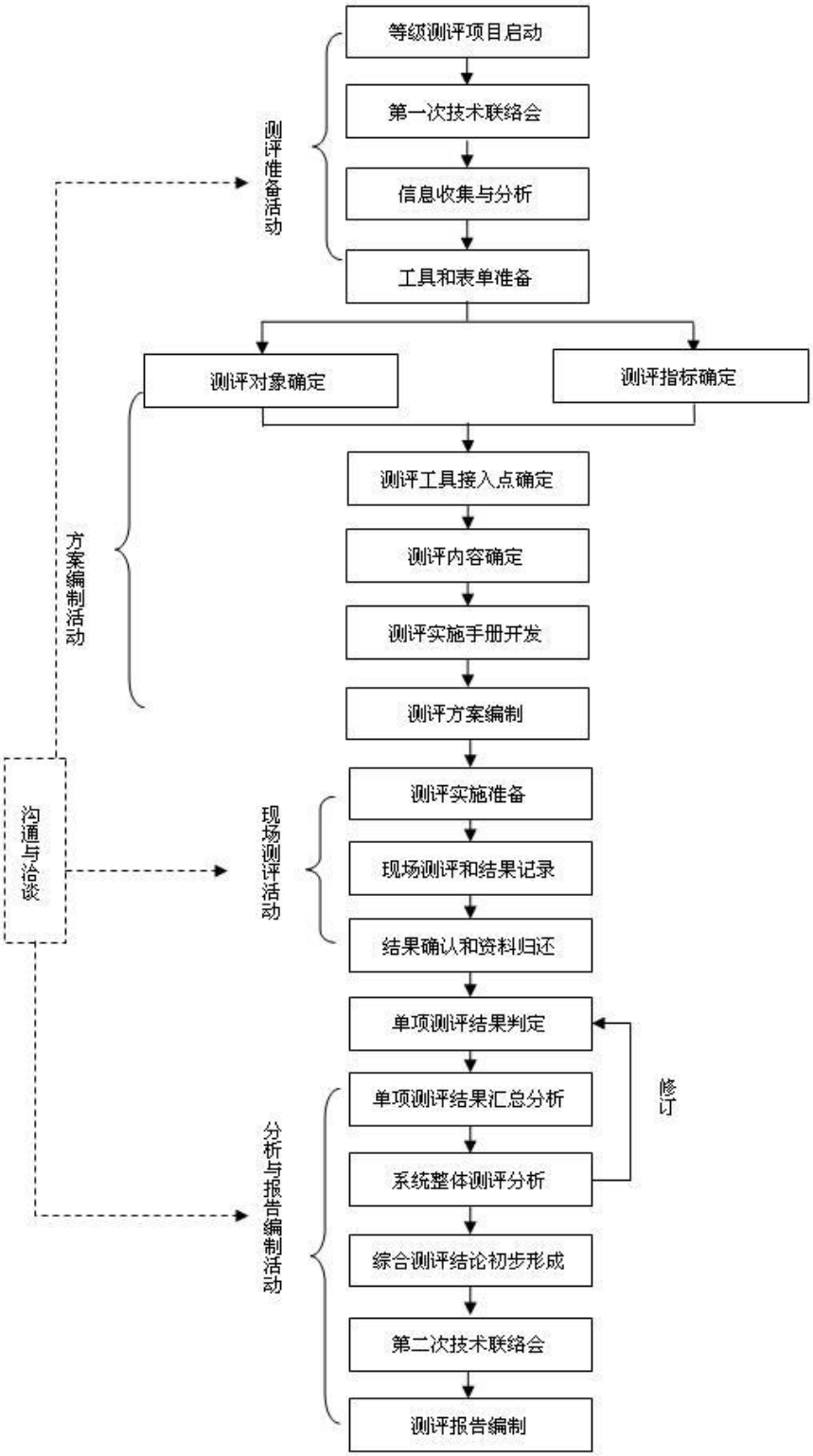
7 测评（评估）实施

乙方对甲方电厂已定级信息系统进行业务现状调研、通过现场测评、整体分析及风险评估工作，全面准确评估业务系统安全保护水平与等级保护相应级别之间的差距，对于发现的问题提出整改建议，最终形成电力监控系统安全防护评估报告和等级测评报告。

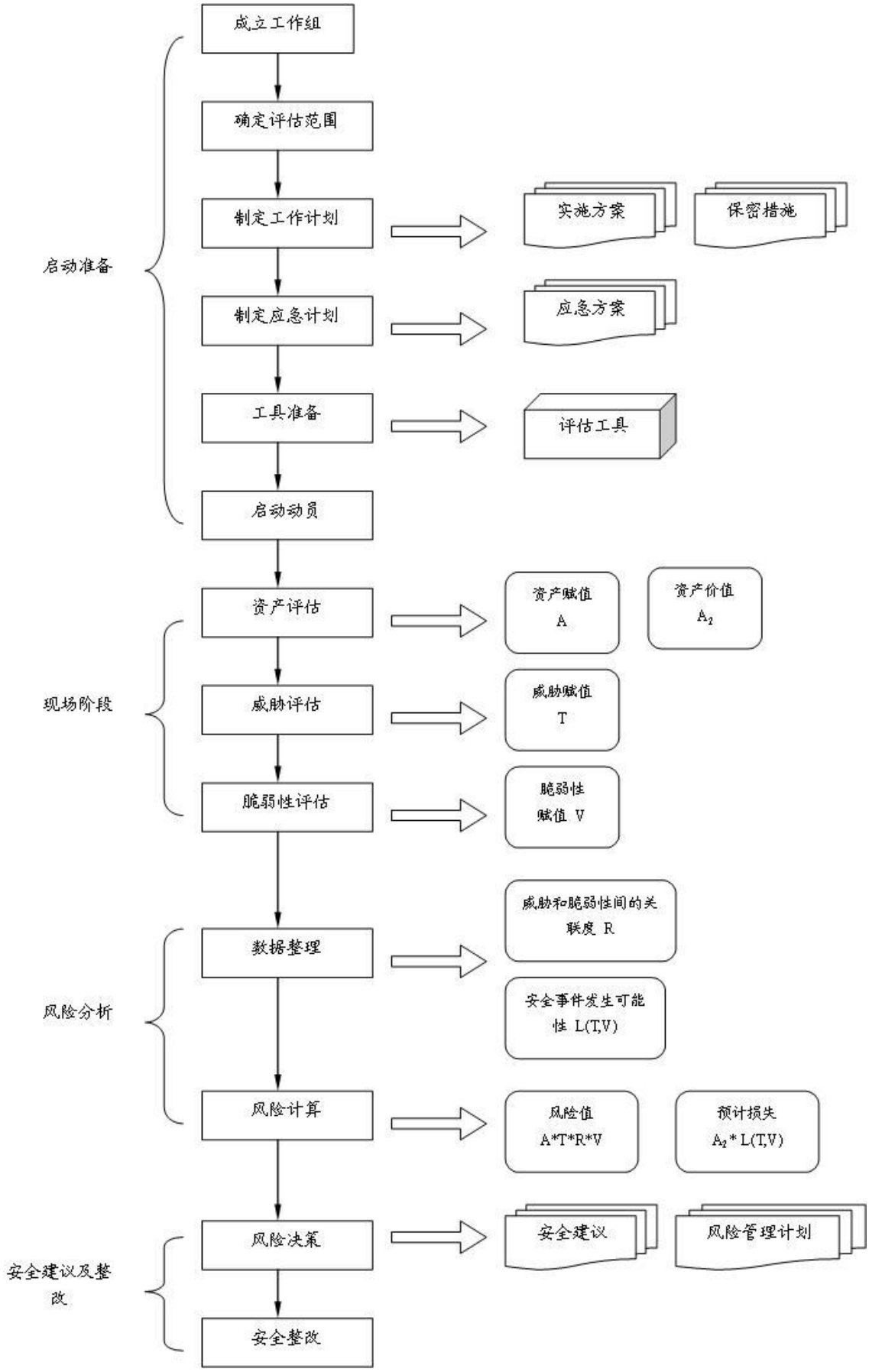
7.1 测评（评估）流程

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，提供整改建议书，配合甲方根据测评范围进行整改实施，整改完成后由乙方针对整改问题进行复测。

电力监控系统的安全等级保护测评流程如下图所示：



电力监控系统安全防护评估工作基本流程将依照《电力监控系统安全防护评估规范》进行，分为前期交流和启动准备阶段、现场数据采集和评估阶段、风险计算和分析阶段，以及总结阶段。


成立工作组
确定评估范围
制定工作计划
制定应急计划
工具准备
启动动员
启动准备
实施方案
保密措施
应急方案
评估工具
资产评估
威胁评估
脆弱性评估
现场阶段
资产赋值
A
资产价值
A_2
威胁赋值
T
脆弱性
赋值 V
数据整理
风险计算
风险分析
威胁和脆弱性间的关联度 R
安全事件发生可能性 L(T,V)
风险值
A*T*R*V
预计损失
A_2 * L(T,V)
风险决策
安全整改
安全建议及整改
安全建议
风险管理计划

7.2 质量控制

测评准备活动过程中，与甲方保持良好沟通，详细了解甲方的要求。对测评组人员进行保密性和规范性的培训。填写好的调查表分别由负责相应工作的测评人员检查后，再由项目组长审核并做好查漏补缺工作，最后交由监督组评标。

方案编制活动过程中，项目组长负责组织完成测评对象、测评指标、测评方法的确定并制定测评方案，组织测评组内部进行评标，对方案编制过程进行说明，对有效性、适用性进行论证，确保所有测评人员了解测评工作整体流程和各自承担的任务。内部评标通过后，交由监督组进行评标。新的测评指导书开发需经过测试验证并进行评标以保证其正确性。

现场测评活动过程中，测评前各人员需确定自己的工作流程、检查内容和检查方法，交由项目组长审核，确保现场测评能顺利进行。测评前召开的准备会议上，须与甲方充分交流，做好相应变更修改，以便测评能得到甲方全力配合，测评工作不偏离预期目标。现场测评过程中严格规范工作流程，避免风险。测评记录需填写全面、清晰，变更和作废等操作需标明版本和原因，每次现场测评结束后需由项目组长进行审查。

报告编制活动过程中，测评结论需依据现场测评证据，对于单元测评结果和最终的测评结论，需进行论证并提供相应证据。对于测评过程中较模糊的项，需与甲方进一步沟通获取信息，确保测评过程公正、严谨。

7.3 风险管理

定期收集项目完成情况的数据，并将实际完成情况数据与计划进度进行比较，一旦发现实际进程晚于计划进程，立即采取纠正措施，分析项目变更的原因，评估项目变更对进度计划的影响。

积极保持与测评委托单位的良好关系，通过甲方主要联系人传达信息。定期向甲方提交项目报告，汇报项目进程，及时收集反馈信息。对于测评工作过程中产生的问题和意见分歧，及时开会协商解决。

告知甲方测评可能对信息系统运行带来的影响。与甲方商定测评时间，避开业务高峰期。测评人员不得直接对被测信息系统相关设备进行操作，对于检查工作，由甲方相应人员进行操作演示或现场陪同。入场前确认系统已备份。可以模拟的操作需在模拟环境中测试或进行预演操作。

在开展电厂等保测评（评估）工作中也会引入安全风险，必须加强实施过程中的风险控制。等保测评（评估）实施前，双方应充分讨论并明确测评对系统可能带来的风险和隐患，确定测评对象、测评方法和工具，并制定应急恢复措施。安全测评实施过程的风险控制手段

主要包括：

7.3.1 操作的申请和监护

在实施过程中必须遵守电力系统的相关操作章程，以防止敏感信息泄露和确保及时处理意外事件。

7.3.2 人员与数据管理

高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

7.3.3 制定应急预案

根据测评范围界定的电力监控系统情况，在实施前制定应急预案，加强系统在线应急处置能力。

7.3.4 关键业务系统风险控制

对影响较大的电力关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、检查和简单测试的方式进行。

7.4 具体内容包括

项目阶段名称	项目阶段工作内容
协助定级备案	确定已备案系统等级，优化系统 S/A/G 指标； 修订需调整系统的等级，优化系统 S/A/G 指标； 提交等级定级报告、备案表和自检表送公安部门备案
安全技术差距测评	针对甲方定级系统的物理安全、网络安全、主机安全、应用安全、数据安全和备份恢复 5 个技术层面进行现场测评和差距分析，记录相关的测评结果。
安全管理差距测评	针对甲方定级系统的安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理这 5 个管理层面进行现场测评和差距分析，并完善 5 个管理层面信息安全防护管理制度体系，记录相关的测评结果。
差距测评记录撰写、评标、定稿	依照《等级保护现场测评记录》中所记录的针对甲方系统的技术和管理测评结果，结合系统整体差距测评结果，按照公安部

	标准测评报告模板撰写测评记录，完成初稿后交由甲方和公安网监认证测评机构专家顾问小组进行评标，并最终定稿为下阶段自行开展整改加固工作提供可信依据。
整改方案指导、评标	依照《等级保护差距测评记录》中的测评结论和整改建议，结合针对甲方系统的实际情况，指导甲方设计系统整改方案，并由乙方与甲方就方案内容进行沟通和协商，提交公安网监认证测评机构进行评标并最终定稿，提交至公安局完成整改方案备案
等级保护测评	针对甲方系统配合公安网监在《等级保护差距测评记录》及《等级保护整改、加固报告》的基础上进行全面的信息安全等级保护测评。 等级保护测评包括，安全技术及安全管理测评两个方面。 根据现场访谈、配置核查的基础上通过先进的安全测试工具进行安全漏洞、应用系统代码漏洞的扫描及人工核查。
形成等级测评结论及测评报告备案提交	针对甲方系统测评在数据汇总分析的基础上，分析系统存在的问题，给出系统等级测评结论，编制《等级保护测评报告》提交当地公安网监部门备案。

8 工程量清单

（主要工作如下，但不限于此。本项目必需的其他工作应视为已包括在报价中，不再单独另计。）

序号	子产品/子服务名称	分项数量(单位:项)
一	350MW 发电机组 DCS 控制系统等级保护测评	数量（1 套）
1	系统定级备案（包括定级报告的编制）	1
2	等级保护差距测评（含差距测评、整改建议、整改核查及达标为止的全过程服务）	1
3	等级保护第三方验收测评服务	1
4	协助甲方向公安系统网监部门提交本项目等级保护验收测评报告并取得公安系统备案回执文件等相关工作	1

5	完成本项目所需的其他工作	1
二	**全厂 NCS 监控系统（含 AGC、AVC、PMU、电能采集等系统） 等级保护测评**	**数量（1 套）**
1	系统定级备案（包括定级报告的编制）	1
2	等级保护差距测评（含差距测评、整改建议、整改核查及达标为止的全过程服务）	1
3	等级保护第三方验收测评服务	1
4	协助甲方向公安系统网监部门提交本项目等级保护验收测评报告并取得公安系统备案回执文件等相关工作	1
5	完成本项目所需的其他工作	1
三	**全厂电力监控系统安全防护评估**	**数量（1 套）**

9 技术资质及要求

9.1 乙方应取得由公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书，并须提供相关证明文件。乙方拟派的项目负责人须具有中级及以上的测评师证书，其他测评技术人员必须具有初级及以上测评师证书，并须提供相关证明文件。

9.2 乙方应已取得信息安全风险评估服务资质（中国网络安全审查技术与认证中心认可），并提供相关证明文件。

9.3 乙方的相关资质应得到甲方所在地的公安部门认可，出具的等级保护测评报告等相关文件必须符合公安部门关于信息系统安全等级保护备案的相关要求。

9.4 乙方应承诺在等级保护安全测评与风险评估过程中所使用的工具软件本身不能有任何安全隐患，对此应承担责任。同时提供的安全服务必须在技术上先进和成熟，使用工具软件版本是最新的，并且在等级保护测评过程中保证系统的稳定性。使用的技术装备、设备、设施等应符合国家对信息安全产品的要求。

9.5 乙方应具备完善的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

9.6 乙方为在中国境内注册成立并由中国公民、中国法人或国家投资的企事业单位（港澳台地区除外）；工作人员仅限于中国公民；法人及主要业务、技术人员无犯罪记录；对国家安全、社会秩序、公共利益不构成威胁。

9.7 乙方近三年（2023 年 5 月 1 日至递交磋商响应文件）具有 2 项同行业电力监控系统安全防护评估及等级保护测评业绩（提供相关证明材料）。

10 技术要求

10.1 服务团队技术要求

乙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。

10.2 驻场服务人员要求

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甲方的权益，否则甲方有权追究责任。

工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

10.3 技术支持服务要求

测评工作本身也会引入安全风险，必须加强测评过程中的风险控制。测评实施前，双方应充分讨论并明确测评对系统可能带来的风险和隐患，确定测评对象、测评方法和工具，并制定应急恢复措施。

10.3.1 操作的申请和监护

测评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。

10.3.2 人员与数据管理

重视测评保密工作，加强测评过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄露。

10.3.3 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，避免影响在线系统运行。

10.3.4 制定应急预案

根据被测评系统情况，在测评实施前制定应急预案，加强系统在线应急处置能力。

10.3.5 关键业务系统风险控制

11 项目质量要求

11.1 质量保证

在等级保护测评方案设计、实施、验收的各个阶段，均应满足电力系统正常稳定运行的要求。

对信息系统测评工作作出具体安排，严格管理流程，编写详细的差距评估和验收测评方案及时间计划，并就建立规范的测评流程、科学的测评方法、全面的测评内容、完善的测评工具、完备的测评指标体系和测评结果、有效的安全保密控制措施作出说明。严格落实人员安排，控制实施进度和项目质量，并能根据业主要求合理调整。

出具的相关报告应得到等级保护行业主管单位认定。报告正本一式四份。

11.2 安全要求

2.1 对所有参与系统开发和实施的人员进行技术交底和安全交底。

2.2 严格按照软件系统开发的相关规范实施。

2.3 不得对现有应用造成影响。

2.4 要对现有应用进行改动的需与系统管理员协调沟通。

11.3 工期要求

1.乙方自合同签订之日起 60 个工作日内完成信息系统评估工作，提交整改方案，并完成整改、验收测评。

2.乙方自合同签订之日起 90 个工作日内出具符合公安部门关于信息系统安全等级保护备案要求的测评报告及其他相关文件，并积极协助和配合甲方取得公安部门的信息系统安全等级保护备案证书。

3.因乙方相关资质或出具的相关报告不能取得甲方所在地公安部门认可，而导致甲方无法取得公安部门的信息系统安全等级保护备案证书的，由乙方自行负责与公安部门协调解决，由此产生的一切费用（如重新测评等）由乙方承担。

4.售后要求

现场测评阶段完成后应进行以下议题：

①双方确认现场测评结果，对测评发现的问题进行沟通。

②双方明确整改范围，对整改建议书内容进行沟通。

③双方根据整改范围和整改计划，指导整改实施。

12 项目风险管理及安全职责

12.1 现场实施期间的安全管理

12.1.1 所有进入甲方现场的人员，均应遵守安全保密相关规定。

12.1.2 项目中为了安全保密的需要，在项目组所在的办公环境中，除甲方提供或允许的 U 盘，不允许出现其他存储介质。

12.1.3 在实施项目环境，除现场实施所使用的电脑设备，不允许其他人员携带电脑进入场地环境。

12.2 文档材料的安全管理

12.2.1 对于需要甲方提供的文档资料，项目实施人员需提出书面申请。

12.2.2 对借阅的纸质文档，需统一由专人妥善保管，使用完后返还甲方。

12.2.3 对借阅的电子文档，传递需通过甲方指定的 U 盘，保存在文档申请人及使用人员的笔记本上。项目组笔记本电脑应进行安全加固，安装防病毒及恶意代码软件并更新到最新，应设置安全级别高口令。使用完毕后在甲方人员监督下彻底删除。

12.3 信息保密职责

12.3.1 本项目乙方的测评组在项目离场时，笔记本及 U 盘等设备交由甲方人员检查确认后方可带出。

12.3.2 所有本地提供的纸质文档，在项目结束后，都要返给甲方提供人。

12.3.3 测评方须对测评工作中涉及的甲方的控制系统信息（如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档信息等）负保密责任。

12.3.4 本项目产生的测评报告等所有文档的处置权归甲方所有，测评方对其的引用与公开应得到甲方的授权。

12.4 例外情况

遇到列明的涉及保密方面的例外情况，双方就个案根据当时实际情况进行单独洽谈并协商处理。

13 项目各方职责

13.1 安全调查和评估的过程中，乙方如需甲方人员配合，乙方需要详细描述需要配合的内容。如需要甲方人员协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由乙方给出具体示例。甲方有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由乙方负完全责任。

13.2 乙方应在实施方案中详细描述项目过程中人员的组成及各自职责的划分。乙方应配置有经验的安全顾问人员进行本项目的服务工作，在协商确定项目组人员组成后未经甲方确认不允许随意更换。乙方应具备包含丰富安全保障经验的资深系统安全工程师的后台支持团队，对风险评估现场工作提供安全保障。

13.3 本项目中可能需要的软硬件平台（如笔记本电脑、评估软件等）均由乙方提供，

甲方将根据需要对设备进行必要的处理。乙方在服务期间未经甲方许可不得将设备带离甲方指定场所，也不得使用任何未经甲方确认的存储设备对评估数据进行复制。乙方在选择评估工具时应考虑与甲方设备所提供报告的一致性，且使用的评估工具应获得甲方同意确认。乙方必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由乙方负完全责任。

13.4 乙方应在加固建议中详细描述安全加固中需要人工参与的工作内容，以及可能对系统造成的影响。

13.5 乙方应向甲方提供详细的评估原始材料、各种表单及结果报告。

14 验收标准及其他

项目验收以甲方取得当地公安部门的信息系统等级保护验收测评备案回执证书为必要条件。

电力监控系统等级保护测评及风险评估项目的目标是输出等级保护测评报告与风险评估报告，该项目将产生一定数量的文档。乙方应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。

14.1 乙方完成项目应提供的文档列表（包含但不限于以下文档）：

序号	文档名称	份数	提交时间	备注
1	《甘能化（兰州新区）热电有限公司全厂 DCS 控制系统等级保护安全测评报告》	4 份	现场测评后 4 周	正式版
2	《甘能化（兰州新区）热电有限公司 NCS 系统等级保护安全测评报告》	4 份	现场测评后 4 周	正式版
3	《甘能化（兰州新区）热电有限公司电力监控系统安全防护评估报告》	4 份	现场测评后 4 周	正式版

15 其他

本规范中未列出的要求由双方共同讨论协商确定。