江西赣能股份有限公司丰城发电厂

治安反恐综合防范、MIS 系统等保测评项目

技术规范书

二〇二四年八月

一、 总则

1.本技术规范书适用于江西赣能股份有限公司丰城发电厂（以下简称需方）治安反恐综合防范系统（该系统包含无人驾驶航空器反制设备，根据省反恐办《关于规范恐怖袭击重点目标设置使用反无人机主动防御系统申报评估有关事项的通知》要求需定为等保三级）的定级备案、网络安全测试、风险评估以及MIS系统（2016年定级为二级，2019年做过一次等保复评、2022年做过一次风险评估工作）网络安全等级保护复评、风险评估项目。此次测评的范围：以江西赣能股份有限公司丰城发电厂治安反恐综合防范系统、MIS系统（包括软件和硬件）为核心，数据流所经区域的主要网络设备、安全设备和服务器为对象；本次安全等保测评分为技术安全测评和管理安全测评，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、安全运维管理，共10个层面的安全测评；以及售后服务技术支持、上级机构网络攻防演练、网络安全检查前后的系统安全策略完善整改、网络安全风险评估以及网络安全培训等技术服务。

2. 本技术规范书提出了最低的有关要求，供方可以提供满足本项目的更高标准要求；供方的所有服务内容必须满足国家、行业有关电力监控、信息系统安全强制性标准。

3.不允许供方对项目进行外包或分包，否则视为违反合同，需方有权终止合同。

4.供方必须执行国家和行业相关的标准、规范，同时严格执行需方的各项管理制度。需方有权对供方在违反标准、规范、管理制度时进行经济考核。

5. 本项目所有与相关系统的分界点上工作均在供方负责的范围之内。

6.供方在事前必须到现场进行勘查了解，详细了解本项目系统目前的布置状况和运行状况，供方事前没有进行现场勘查了解的，视为进行过现场勘查了解。

7.供方在服务有效期内，技术有问题、人员力量不够或不服从管理，将严重影响到需方信息安全及设备的安全、稳定、经济运行且无法克服时，需方有权单方面解除合同。或需方有权另行委托施工队伍进行紧急处理，供方应担负全部委托费用及由此造成的损失。

8.本文件所使用的标准如遇与供方所执行的标准发生矛盾时，按较高标准执行。

9.本文件经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效力。

10.供方在提供技术服务时，不能影响现有应用系统正常运行；供方在项目实施前需给出详细的方案，对可能影响现有应用系统正常运行的操作提出可靠的解决方案或制定

应急预案等防范措施并报需方审核。

11. 技术服务所必须使用的软、硬件测试工具由供方提供，但必须有相应检测机构出具的合格证书。

12. 供方应具备的资质条件

供方应满足下列要求并提供下列相关资料，包括但不限于：

1)提供工商行政管理局登记注册并经年检（审）合格的营业执照或法人证书（复印件加盖公章）；

2)必须具有网络安全等级保护测评资质，提供《网络安全等级测评与检测评估机构服务认证证书》加盖公章；

3)必须具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书或公安部第一研究所颁发的网防服务中心证书或中国网络安全审查技术与认证中心颁发的网络安全应急服务资质；

4)具有中国网络安全审查技术与认证中心颁发的信息安全风险评估二级及以上证书和一名及以上 DJCP 高级测评师证书且相关证书加盖公章、提供用人合同、社保证明等；

5)具有近三年 50 套以上电力监控系统信息安全等保测评工作经验并附案例扫描件(国家能源局关于印发《电力行业网络安全等级保护管理办法》的通知国能发安全规[2022]101 号)；

6)近三年内没有重大经营活动违法记录，例如被“信用中国”网站列入失信被执行人和重大税收违法案件当事人名单及被“中国政府采购网”网站列入政府采购严重违法失信行为记录名单（处罚期限尚未届满的）等。

二、 工程概况

1. 项目依据

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行，其中第二十一条规定“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务”。

《网络安全等级保护条例》第二十三条规定：第三级以上网络的运营者应当每年开展一次网络安全等级测评，二级信息系统建议每两年开展一次测评；以及《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)第十三条规定：网络建设完成后，电力企业应当依据国家和行业有关标准或规范要求，定期对网络安全等级保护状况开展网络安全等级保护测评；第二级网络应当每两年进行一次等级保护测评，第三级及

以上网络应当每年进行一次等级保护测评。新建的第三级及以上网络应当在通过等级保护测评后投入运行。

《中华人民共和国计算机信息安全保护条例》（国务院 147 号令）和《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）确定了“实行信息安全等级保护制度”，明确信息系统单位 “谁主管谁负责，谁经营谁负责”的信息安全保障责任制。

公安部、国家保密局、国家密码管理局、国务院信息工作办公室还印发了《信息安全等级保护管理办法》（公通字[2007]43 号），明确了等级保护是我国开展信息安全保障工作的基本制度、基本国策和基本方法，确定了系统定级、备案、等保测评、安全建设整改、监督检查等工作流程及要求，为开展信息安全等级保护工作提供了规范保障。江西省公安厅、江西省发展和改革委员会、江西省财政厅还联合下发了《关于加强省级重要信息系统安全保障工作的通知》（赣公字[2015]55 号），对省重点单位重要信息系统等级保护工作部署和组织实施、信息系统定级、备案、等保测评、安全建设整改等工作明确了监督管理要求。

自 2007 年起，国家电监会陆续下发了《关于开展电力行业信息系统安全等级保护定级工作的通知》和《电力行业信息系统安全等级保护基本要求》等文件要求，督促开展等级保护工作。国务院发展和改革委员会还颁布了《电力监控系统安全防护规定》（第 14 号令）、国家能源局《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》（国能安全[2015] 36 号）和国家能源局《关于开展电力监控系统安全防护专项检查工作的通知(国能综安全》〔2016〕92 号)等行业规范文件以规范电力行业网络安全工作。

基于以上原因，需分别对需方治安反恐综合防范系统及 MIS 系统进行等保定级、备案、测评、复评及网络安全风险评估、出具整改方案等工作。

2.测评目标简介

2.1 治安反恐综合防范系统（拟定三级）

该系统于 2023 年底开始建设、2024 年 8 月投入试用，采用安防综合管理平台，对各个安防子系统进行集中管控，统一数据库对所有子系统前端的采集数据进行存储与分发，并提供统一的操作界面，实现各子系统的资源共享、业务整合与联动等，系统满足《电力系统治安反恐要求第二部分：火力发电企业》文件及国家、地方关于治安反恐防范综合管理系统信息化建设的法规及标准的要求；项目规划建设本着“高起点、高效率”的

原则，以安防事件的事前防范、事中处理、事后分析提供有效的技术支持为基本要求，建立起“人防部署到位、物防设施完善、技术手段先进、应急处置高效”的集管理、防范、控制于一体的安全保障体系，对各类事件做到预知、预判、预防、预警和有效处置，切实加强安全保障和应急响应能力。以安防综合管理平台为核心，集成视频监控、周界报警、出入口控制、电子巡查、反无人机主动防御、一键报警、访客一体机等系统，通过管理平台的统一协调实现各应用子系统间的资源共享与信息互通，从而达到管理便捷性、数据直观性，实现各应用子系统之间的智能化联动和处置突发事件的应急指挥。

2.2 MIS 系统

该系统于 2008 年投用，2016 年首次进行等保测评工作，定级为二级并在江西省公安厅进行了备案，2019 年做过一次等保复评、2022 年做过一次风险评估工作，随着#7/8 机组 2022 年双投以及 2023 年丰城二期、三期发电厂的合并，不但 MIS 系统的网络结构发生了变化，企业名称和法人也发生了变更；另外根据属地化管理原则，需将该系统重新在宜春市公安局进行备案。系统主要包括企业信息管理(SMS，主要实现运行人员订餐、食堂消费、短信平台、非生产缺陷管理、干部值班记录、电子公告、企业内部宣传报导等功能)、生产管理(主要实现运行值班记录、生产小指标统计机组经济指标统计等功能)、电能计量、燃料管理系统和内部门户网站等，对火力发电企业大量的原始生产、管理数据进行收集、整理、统计、存储，以便事后查询、分析汇总等方面的工作。该系统是以办公管理为基础，生产管理和经营管理为中心的综合管理系统，全面实现成本控制，提高经济效益，实现现代化管理的信息系统，它为企业提供辅助决策信息。

3. 工程实施具体方案

3.1 等保测评服务。分别对需方治安反恐综合防范系统开展网络安全定级、备案、测试、安全防护评估、安全整改方案设计和技术支持等服务，以及 MIS 系统进行复测、变更备案单位、安全防护评估、安全整改方案设计和技术支持等服务。综合应用各种合理技术和工具，进行系统漏洞挖掘、工具测试、验证分析。

3.1.1 访谈：测评人员与被测评系统有关人员进行交流、讨论等活动，获取相关证据，了解有关信息。可能涉及的访谈人员角色包括网络安全主管、系统管理员、网络管理员、安全管理员等。

3.1.2 核查：核查可细分为文档审查、实地察看和配置核查等形式。其中，文档审查主要关注各类管理文档（包括但不限于安全策略类、管理制度类、操作规程类、执行表单类）是否齐全，内容涵盖是否全面，符合要求。实地察看主要是指测评人员到相应的

场所（办公场所、机房环境等），通过实地观察基础设施和物理环境状况等方面的安全情况。配置核查是指测评人员利用上机验证的方式核查网络设备、安全设备、应用系统、主机系统、数据库系统以及各设备的配置是否正确。

3.1.3 测试：用技术工具对系统进行测试，包括基于网络和系统的漏洞扫描、网络协议抓包分析、渗透性测试等。

3.2 其它网络安全服务

3.2.1 安全风险评估服务。包括风险要素评估、风险分析和计算阶段、风险决策和安全建议。提供整改建议书，配合需方根据评估建议进行整改实施。

3.2.2 本年度剩余时间里相关部门或上级单位网安演练、检查事前、事中、事后的技术服务。

3.2.3 本年度剩余时间里突发网络安全事故/事件应急响应服务。根据需方应急保障体系建设要求，指定具备网络安全应急处置技术能力的人员作为需方应急保障专家库成员，在发生网络安全事故/事件时，供方负责安排专业技术服务人员配合需方对安全事故/事件进行响应、抑制、解决的安全服务。

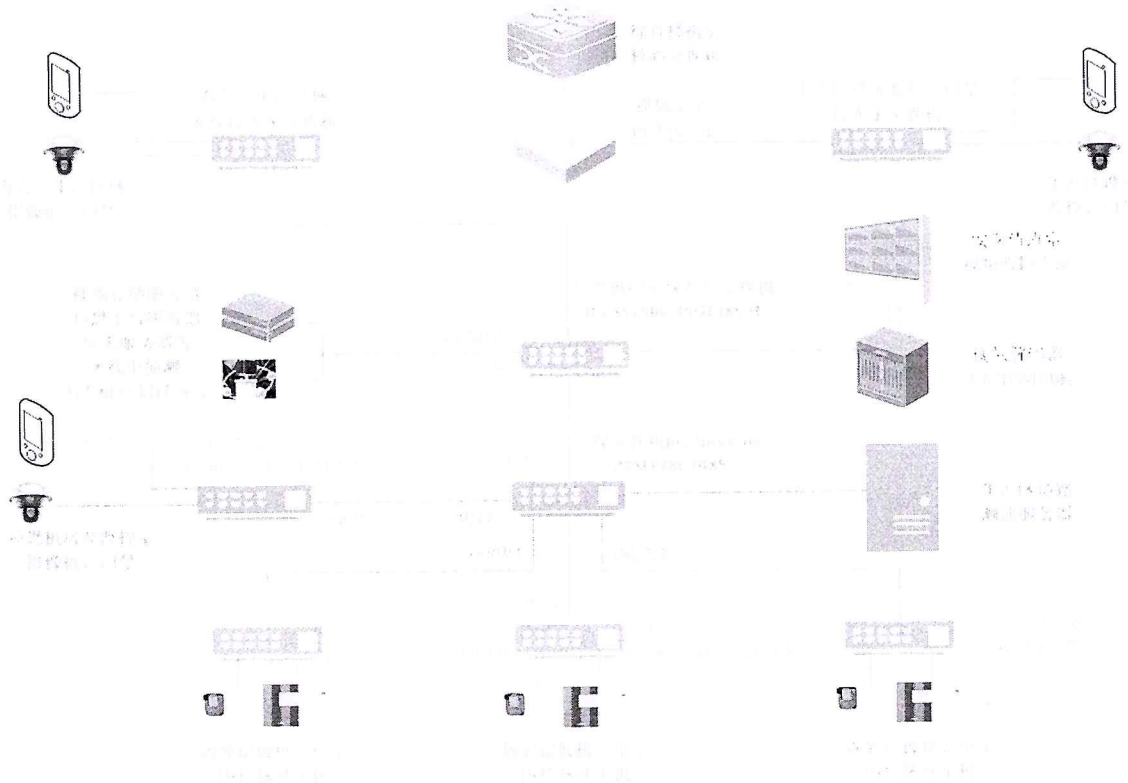
3.2.4 一次线下网络安全培训。安排具备相关认证的安全技术专家进行授课，提供信息安全意识教育、信息安全技能培训、信息安全管理制度及标准培训等全方位的安全培训，全面提升需方人员的信息安全技能及意识水平。

3.2.5 提供网络安全基础教育视频宣传片及大约 1000 道题目的网络安全基础知识考试题库及答案，要求视频宣传片基本对应题库。

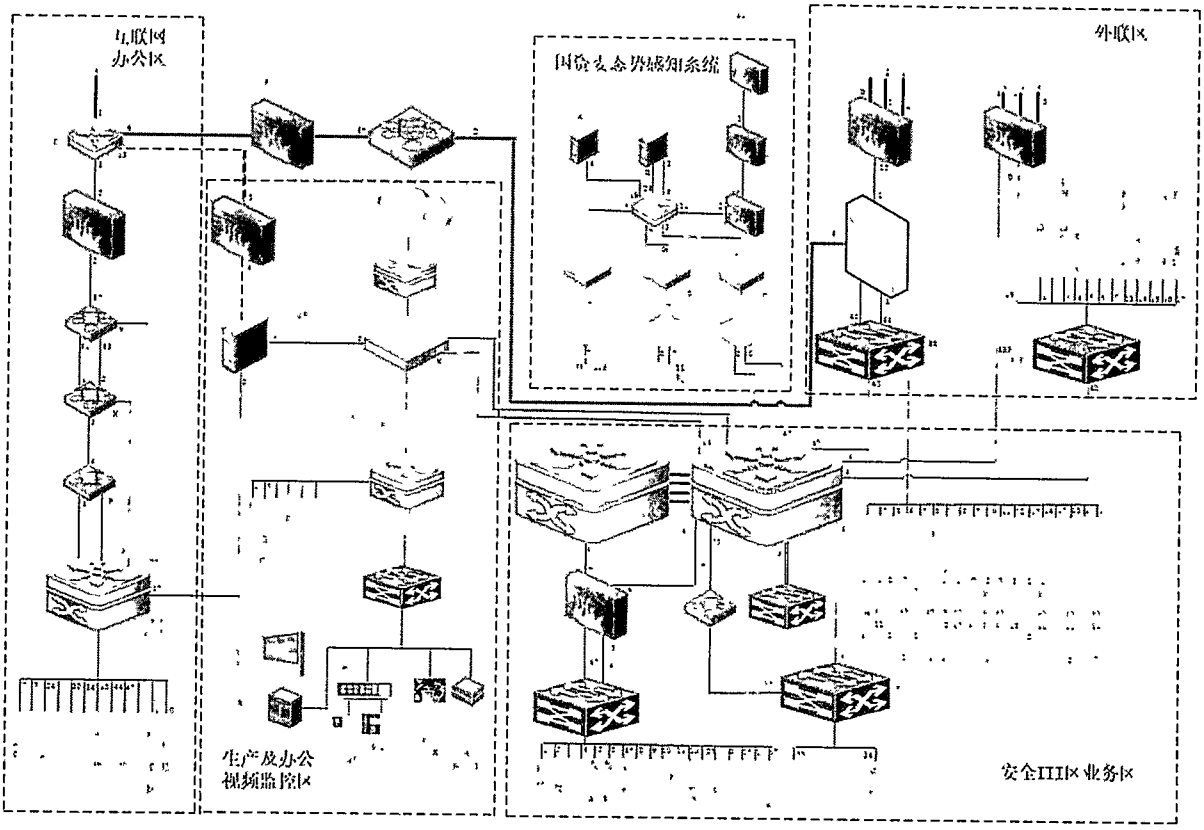
4. 治安反恐综合防范系统、MIS 系统网络拓扑图

4.1 治安反恐综合防范系统网络拓扑图

传输网络系统主要作用是接入各类监控、门禁、入侵报警、反无设备，为中心管理平台的各项应用提供基础保障，能够更好的服务于各类用户。网络结构如下图所示：

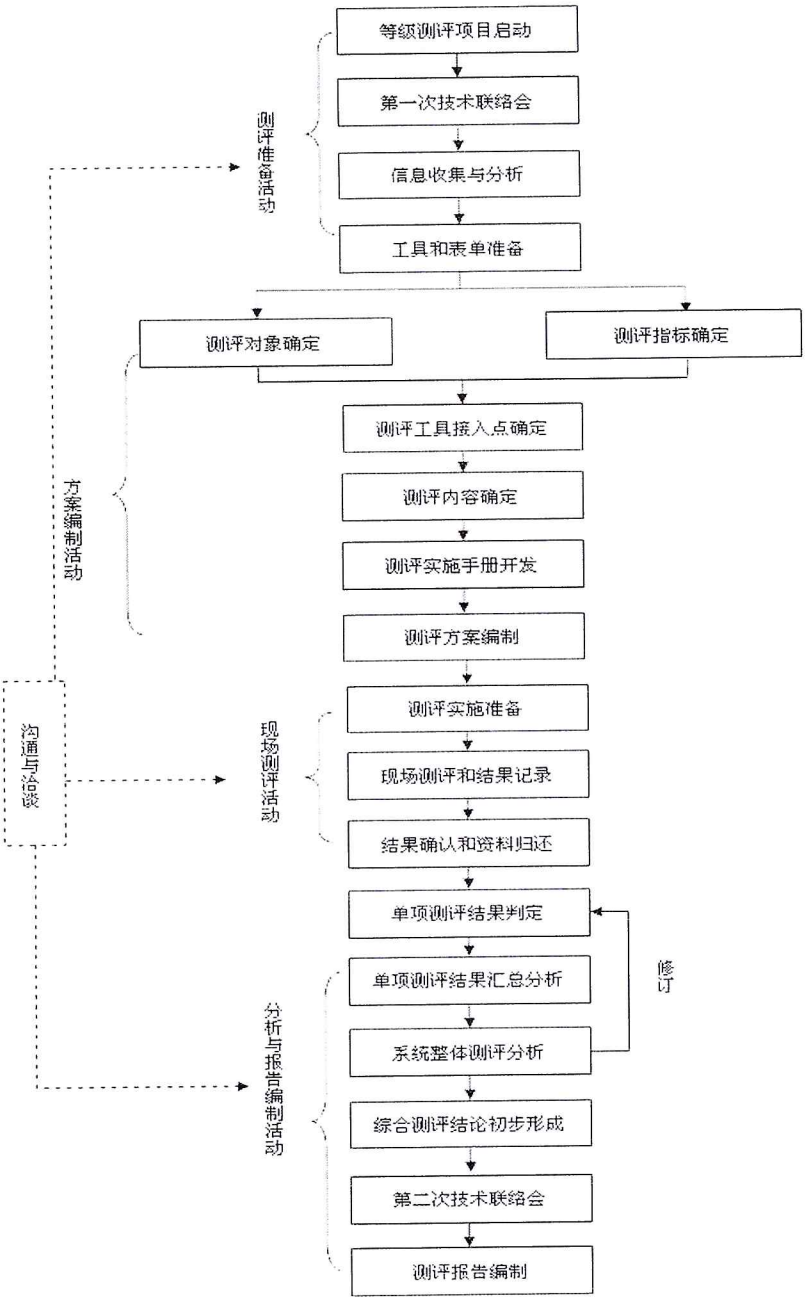


4.2.MIS 系统网络拓扑图



5.测评流程

需方治安反恐综合防范系统、MIS 系统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，配合需方根据测评范围进行整改实施。



三、 项目内容、范围

1.具体内容

1.1 依据国家信息安全等级保护领导小组下发的等级保护标准和国家能源局、电力行业要求，对需方治安反恐综合防范系统进行等级评定、测试和安全防护风险评估、对需方 MIS 系统进行等保复测和安全防护风险评估，提交《等保测评报告》、《安全防护风险评估报告》和《安全整改方案》、《定级报告》、《备案表》、公安机关颁发的《信息系统安全等级保护备案证明》并获取备案证书(包括 MIS 系统由省公安厅变更备案到

宜春市公安局)。

1.2 如果本次测评不能达到相应等级保护要求，供方应在向需方提交合理合规的《安全建设整改方案》，待需方完成整改后继续免费完成本次测评服务，直到被测评系统达到相应等级保护要求。

1.3 供方需在项目实施前提交《三措两案》供需方审核，以保证项目实施过程不影响被测评系统的正常运行，同时适合国家和电力行业的相关法律法规的管理规定，满足上级机构的规定和要求，否则产生的损失全部由供方负责承担。

1.4 协助被测评单位完成本年度剩余时间内政府机关或相关单位网络攻防演练、网络安全检查事前事中事后的技术服务，完善网络安全管理制度、应急预案；

1.5 开展信息安全技术和等级保护政策培训，安排具备相关认证的安全技术专家进行授课，提供信息安全意识教育、信息安全技能培训、信息安全管理制度及标准培训等全方位的安全培训，为期 1 天。

1.6 本年度剩余时间内突发事故/事件应急响应，在发生安全事件时，需由高级技术服务人员配合安全事件进行响应、抑制、解决的安全服务。

2. 具体要求

按照信息系统安全等级保护测评服务标准规范，针对治安反恐综合防范及 MIS 系统开展等级评定、备案、网络安全测试和安全防护评估等工作。通过等保测评明确信息安全保障重点，积极落实相关信息安全保障条件，并落实信息安全责任，建立信息安全等级保护工作长效机制，切实提高需方信息安全防护能力、隐患发现能力、应急处置能力，为需方信息化发展提供可靠保障。本次项目将实施过程分为八个关键过程：

- 信息系统定级、评审、备案、获取证书(包括 MIS 系统由省公安厅变更到宜春市公安局备案证书)
- 信息系统等级保护差距分析和等保测评报告
- 信息系统安全风险评估报告
- 信息系统安全等级保护建设整改方案设计
- 相关部门或上级单位网安演练、检查事前、事中、事后的技术服务
- 网络安全事件应急服务
- 一次线下网络安全培训
- 提供网络安全基础教育视频宣传片及大约 1000 道题目的网络安全基础知识考试题库及答案,要求视频宣传片基本对应题库。

通过开展以上工作，检验和提升需方信息系统综合安全防护能力，明确信息安全保障重点，建立信息安全工作长效机制，切实提高需方信息系统安全防护能力，为系统提供可靠信息安全保障。

2.1 定级备案

服务对象：治安反恐综合防范系统、MIS 系统。

定级工作将严格遵循《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2020），深入调研掌握信息系统的应用部署实际情况，按照国家有关管理规范和标准要求，细致分析各信息系统安全域及管理边界，合理划分信息系统范围，科学开展信息系统重要性程度分析，准确判定信息系统安全等级，编制《定级报告》和《备案表》，并按照定级备案流程，向主管部门、监管机关就信息系统定级进行审批备案，获得监管机关颁发的《信息系统安全等级保护备案证明》。

项目交付成果（包括但不限于）：监管机关颁发的《信息系统安全等级保护备案证明》。

2.2 信息系统测试

本次等级保护测评应覆盖到被测系统的安全物理环境、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、安全建设管理和系安全运维管理共 10 个层面。

(a) 安全物理环境

安全物理环境测评主要涉及的控制点内容：物理位置、物理访问控制、防盗窃和破坏、防雷、防火、防水和防潮、防静电、温湿度控制、电力供应及电磁防护等方面。

测评对象(包括但不限于)：机房及机房相关设备设施、验收类文档、机房管理等。

(b) 安全通信网络

安全通信网络测评主要涉及的控制点内容：网络架构、通信传输和可信验证。

测评对象（包括但不限于）：路由器、交换机、无线接入设备、防火墙等提供网络通信功能的设备或组件、综合网管系统、相关设计验收文档等。

(c)安全区域边界

安全区域边界测评主要涉及的控制点：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证。

测评对象（包括但不限于）：网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件、抗 APT 攻击系统、抗 DDoS 攻击系统和入侵保护系统或相关组件、防病毒网关、UTM 和终端管理系统或相关设备等。

(d)安全计算环境

安全计算环境测评主要的控制点内容包括：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、数据备份恢复、剩余信息保护和个人信息保护等。

测评对象（包括但不限于）：

终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）移动终端、移动终端管理系统、移动终端管理客户端感知节点设备、网关节点设备、控制设备、业务应用系统、委托第三方定制开发业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等、提供可信验证的设备或组件、提供集中审计功能的系统等。

(e)安全管理中心

安全管理中心测评的控制点包括系统管理、审计管理、安全管理和集中管控。

测评对象（包括但不限于）：提供集中系统管理功能的系统、综合安全审计系统、数据库审计系统等提供集中审计功能的系统、综合网管系统等提供运行状态监测功能的系统等。

(f)安全管理机构

安全管理机构测评的控制点主要包括：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。

测评对象（包括但不限于）：网络安全主管、岗位职责文档、人员配备文档、各类授权审批记录、检查记录及报告等。

(g)安全管理制度

安全管理制度测评主要控制点：安全策略、管理制度、制定和发布、评审和修订。

测评对象(包括但不限于)：网络安全管理、管理制度类文档、发布、评审记录等。

(h)安全管理人员

安全管理人员测评的控制点包括：人员录用、人员离岗、安全意识教育及培训和外部人员访问管理。

测评对象（包括但不限于）：网络安全主管、岗位安全协议、保密协议、各类记录类文档等。

(i)安全建设管理

安全建设管理测评的控制点包括：系统定级和备案、安全方案设计、产品采购和使

用、工程实施、测试验收、系统交付、等级测评和服务供应商选择。

测评对象（包括但不限于）：系统建设负责人、各类设计文档、表单记录文档等。

(j)安全运维管理

安全运维管理测评的控制点包括：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、密码管理、变更管理、备份与恢复管理、安全事件管理、应急预案管理和外包运维管理。

测评对象（包括但不限于）：资产管理员、介质管理员、网络管理员、系统管理员等相关人员以及各类记录表单文档等。

（k）检测工具

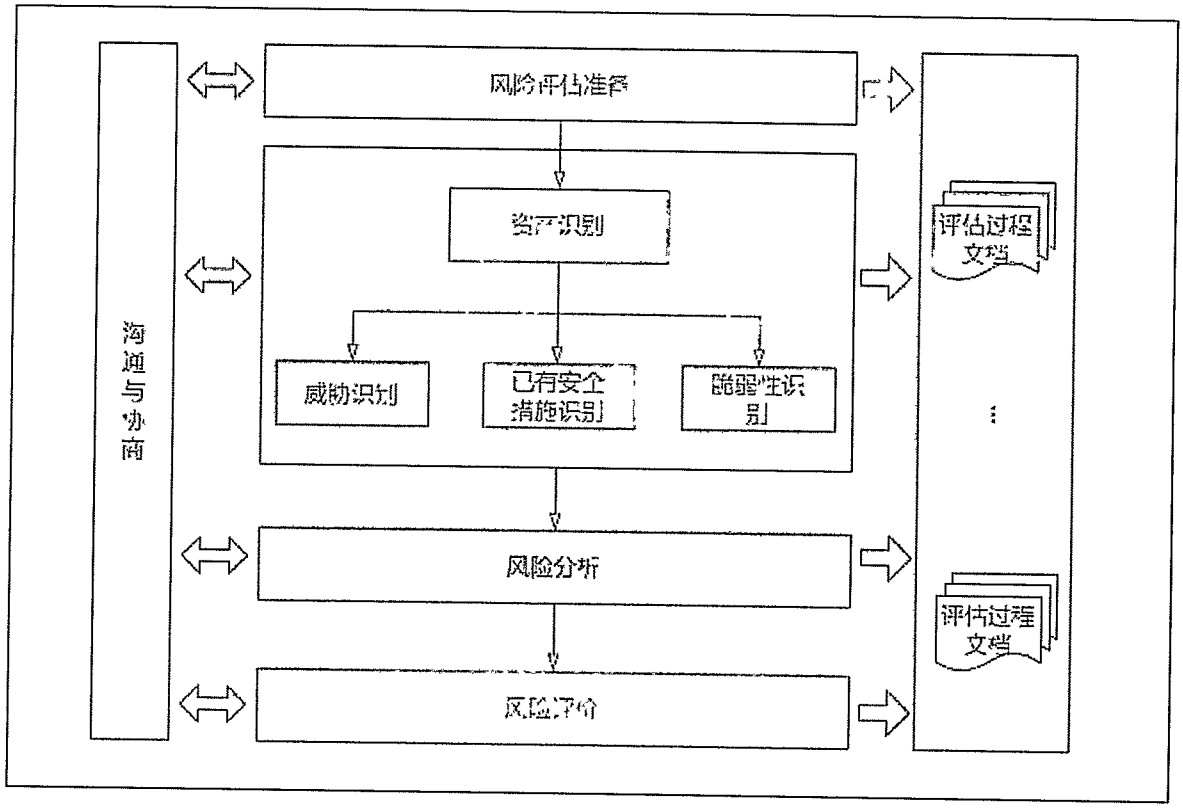
通过采用恶意代码检测工具、漏洞扫描工具、WEB 日志安全分析工具、预警检测系统、渗透测试工具、网络流量分析工具等对网络、主机等进行检查、渗透测试分析。

在收集充足数据之后，对现场测评获得的数据进行汇总分析，形成等级测评项目的最终结论，并编制最终的《网络安全等级保护等级测评报告》。

工作过程文件及项目交付成果(不限于)：《网络安全等级保护等级测评报告》。

2.3 安全防护风险评估

安全防护风险评估实施流程分为启动准备阶段、风险要素评估、风险分析和计算阶段、风险决策和安全建议。提供整改建议书，配合需方根据评估建议进行整改实施。



1）标准依据：《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》

2）评估工作过程

准备阶段工作是对评估实施有效性的保证；

风险要素识别阶段工作主要是对评估活动中的各类关键要素资产、威胁、脆弱性、安全措施进行识别与赋值；

风险分析阶段工作主要是对识别阶段中获得的各类信息进行关联分析，并计算风险值；

风险处置建议工作主要针对评估出的风险，提出相应的处置建议，以及按照处置建议实施安全加固后进行残余风险处置等内容。

3）编制阶段

风险评估的准备阶段的主要工作内容有：培训与编制计划。

培训一般指评估方根据评估目标，对项目组进行培训。所有培训均采用培训记录方式进行留档备案。

风险评估计划由项目组组长与被评估方进行充分沟通，编制出本次风险评估项目计划草案，一般包括工作目标、评估范围、项目实施的团队、评估的依据和方法、本次风险评估工作成果等内容。草案提交整个风险评估小组进行会议审定，项目组组长按照审

定意见进行修改，形成风险评估方案。

4）风险评估内容：

资产识别

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的分析，最终确定信息系统的重要性级别。

威胁识别

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。

脆弱性识别

脆弱性可从技术和管理两个方面进行识别。

技术方面，可从物理环境、网络、主机系统、应用系统、数据等方面识别资产的脆弱性；

管理方面，可从安全管理机构、安全管理策略、安全管理制度、人员安全管理、系统运维管理等方面识别其脆弱性。

已有安全措施确认

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、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。

风险分析

风险评估的结果进行等级化处理，根据所采用的风险计算方法（明确：风险计算方法），计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。

安全加固

风险分析工作完成之后生成安全风险清单，基于风险清单确认风险是否可接受，如果不可接受，协助客户整改，按照风险问题的不同提供相应整改支撑工作。

安全应急能力评估

对系统的安全有效性、业务的连续性和备用、灾备能力进行评估。

备用与容灾能力的建设情况，包括系统的冗余设备部署、设备配置的备份情况等；

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；

全面安全管理评估

全面安全管理评估是从管理角度对单位电力系统概况进行评估，重点检查安全防护规定落实情况；

制度建立及主管领导、管理机构和工作人员履职情况，信息安全责任制落实情况；

运维人员的安全管控情况；

电力系统安全防护评估工作开展情况；

信息安全宣传教育、领导干部及各级人员网络与信息安全基础培训、信息安全人员专业技术培训情况等。

2.4 整改方案设计

具体要求：依照《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号），严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，在系统测评工作的基础上，对被测单位信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全整改方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全整改技术方案设计、安全整改管理体系设计、信息系统安全产品选型及技术指标建议、安全整改项目实施计划、项目预算，整改后可能存在的其他问题； 出具方案后，需以此方案为基础，开展安全整改咨询和系统加固工作，最终使被测单位安全管理和技术两方面达到相应等级的保护要求。

工作过程文件及交付成果(包括但不限于)：《信息安全等级保护安全整改方案》。

2.5 突发网络安全事件应急响应

本年度剩余时间里突发网络安全事故/事件应急响应服务。根据需方应急保障体系建设要求，指定具备网络安全应急处置技术能力的人员作为需方应急保障专家库成员，在发生网络安全事故/事件时，需由高级技术服务人员配合需方对进行响应、抑制、解

决的安全服务。当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事故/事件时，高级技术服务人员第一时间赶到事故/事件现场，最短时间内使网络信息系统恢复正常工作，帮助查找入侵来源，进行入侵分析，给出入侵事故/事件过程报告，同时给出解决方案与防范报告。应急响应服务包含大规模病毒爆发响应、系统入侵事故/事件响应、主机、网络异常响应、拒绝服务攻击响应。当时间发生时，需在 1 小时响应，按照准备预防、检测、遏制、根除、恢复、跟踪总结的流程进行，从第三方角度提供《应急响应分析报告》，在事故/事件发生后，作为第三方机构客观分析各类安全设备厂家在事件中的状态，避免相互推诿和相关责任，出具事故/事件分析报告，以供用户或监管机关作为证据备查，为用户提升管理安全效率。在突发/重大信息安全事故/事件后对包括计算机运行在内的业务运行进行维持或恢复。在服务周期范围内，提供不限次数现场应急响应服务。团队中应包括两名或以上中国信息安全认证中心颁发证书的应急服务专业工程师实施，工作经验丰富技术人员完成实施工作，根据每次应急响应的情况，必要时提供软、硬件设备参与应急响应工作，并进行分析，出具《网络安全事故/事件分析与处置报告》。同时，尽可能地减少和控制住网络安全事件的损失，提供有效的响应和恢复指导，并努力防止安全事件的发生，具体支持内容以及可支持的应急相应类型见下表：

类型	内容	任务完成标准
系统入侵类应急服务	查找黑客入侵的方式（环境脆弱点）	描述入侵痕迹并找到被入侵系统脆弱点 证明通过该脆弱点可实现入侵
	系统加固并提供解决方案	帮助用户加固操作系统 提供用户可操作的系统加固方案
	溯源入侵者	通过数据或者阻止正在实施的入侵等方式证明一个 IP 为本次入侵源。 说明：IP 到人的定位涉及国家管理部门工作，本应急任务不涵盖
恶意代码类应急服务(病毒、	发现恶意代码所属种类并清除	提取被入侵系统中的恶意代码样本体。 使目标系统处于未被感染状态。

蠕虫、木马、间谍软件）	发现恶意代码攻入的方式（环境脆弱点）	证明通过该脆弱点可以实现恶意代码传播
	有目的的恶意代码植入的溯源（木马、间谍软件）	证明一个 IP 为该恶意代码的传输源 说明：IP 到人的定位涉及国家管理部门工作，本应急任务不涵盖
	提供恶意代码防护方案	提供该类恶意代码攻击的长期防护方案，方案操作性强。
数据安全类应急服务	恢复数据	恢复用户所丢失的数据
	数据泄露途径分析（发现数据保护脆弱点）	发现脆弱点，证明该脆弱点可导致数据安全风险
	提供数据安全保护方案	提供该类数据安全风险的长期防护方案，方案操作性强。
拒绝服务攻击类应急服务	判断拒绝服务的攻击类型并提供解决建议	通过现场数据报文及相关原理报告证实用户所遭受拒绝服务的攻击类型。 提供针对该类型拒绝服务攻击的解决建议。
	使用技术手段及硬件设备防御拒绝服务攻击	使用技术手段及硬件产品帮助用户抵御住该次拒绝服务攻击。
	追溯拒绝服务攻击源（国内仅我们可做此应急服务）	使用独创技术手段追溯拒绝服务攻击真实源 IP。 说明：IP 到人的定位涉及国家管理部门工作，本应急任务不涵盖

工作过程文件及项目交付成果（包括但不限于）：《安全事件分析与处置报告》。
提交要求：按需

2.6 网络安全技术和等级保护知识培训

网络安全培训工作：安排具备相关认证的安全技术专家进行授课，提供网络安全意识教育、信息安全技能培训、信息安全管理制度及标准培训等全方位的安全培训，全面提升用户人员的信息安全技能及意识水平。培训内容包括但不限于：目前国内外安全现

状、安全意识、安全事件分析、安全管理体系建设、安全保障体系建设、网络安全等级保护 2.0 标准分析解读，培训次数根据实际情况确定，具体培训内容包括以下：

培训课程

序号	主要内容	时长	具体内容
1	网络安全法律法规及等级保护制度介绍	30 分钟	介绍网络安全概念、相关法律法规及等级保护工作内容、等级保护级别划分、等级保护的意义、等级保护相关政策、等级保护的五个环节
2	网络安全意识培训	15 分钟	网络安全常识，网络安全与普通人的关系及群众应知应会的网络安全知识、个人网络安全防护基本技能等
3	公安部网安局“两高一弱”(高危漏洞、高危端口、弱密码)专项整治行动案例介绍	15 分钟	结合案例阐明“两高一弱”的安全隐患及防护方法
4	计算机病毒、木马知识	10	介绍计算机病毒、木马的危害、防范措施等

工作过程文件及项目交付成果（包括但不限于）：培训方案或课件等。

提交要求：按需

3.供货范围（包括但不限于此）

3.1 依据国家信息安全等级保护领导小组下发的等级保护标准和国家能源局等电力行业要求，对需方治安反恐综合防范系统、MIS 系统进行等保测评和安全防护风险评估，提交《等保测评报告》、《安全防护风险评估报告》和《安全整改方案》、《定级报告》、《备案表》、《备案证明》，并保证获取备案证书。

3.2 服务期内相关部门或上级单位网安演练、网安检查事前、事中、事后的技术服务工作记录清单。

3.3 如果服务期内需方发生网络安全事故/事件，供方需提交《网络安全事故/事件应急响应分析报告》、《网络安全事故/事件分析与处置报告》。

3.4 此次项目要求给出详细的分项报价，项目实施过程中因现场条件不具备，而没有实施的分项项目，在项目决算时应将相应的分项项目费用扣除。

序号	项目名称	要求	单位	数量
1	治安反恐综合防范系统备案、等保测评、风险评估、整改方案	对治安反恐综合防范系统（三级）开展网络安全定级、测试、安全防护评估、安全整改方案设计和技术服务等	项	1
2	MIS系统重新备案、等保复测、风险评估、整改方案	对MIS系统（二级）开展网络安全定级、测试、安全防护评估、安全整改方案设计和技术服务等	项	1
3	突发网络安全事故/事件应急响应（合同生效日-2024.12.31）	在发生安全事件时，需由高级技术服务人员配合对安全事件进行响应、抑制、解决的安全服务。当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，高级技术服务人员第一时间赶到事件现场，最短时间内使网络信息系统恢复正常工作，帮助查找入侵来源，进行入侵分析，给出入侵事故过程报告，同时给出解决方案与防范报告	项	1
4	网安演练、检查前、后的技术服务（合同生效日-2024.12.31）	需方接受相关部门或上级单位网安演练、检查工作时，供方提供事前、事中、事后技术服务并作好服务工作记录	项	1
5	信息安全技术和等级保护培训	安排具备相关认证的安全技术专家进行授课，提供信息安全意识教育、信息安全技能培训、信息安全管理制度及标准培训等全方位的安全培训，全面提升用户人员的信息安全技能及意识水平。培训内容包括但不限于：目前国内外安全现状、安全意识、安全事件分析、安全管理体系建设、安全保障体系建设、等保2.0标准分析解读	项	1
6	网络安全基础教育视频宣传片及试题库	视频宣传片与约1000道题目的网络安全基础知识考试题库及答案大体相同	项	1