ICS 35.240.50
CCS F07

团　　体　　标　　准

T/CERS 0100—2025

电力信息系统入网安全测试技术要求

Technical requirements for network access security test of electric power information system

2025－9－27 发布　　2025－9－27 实施

中国能源研究会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国能源研究会提出。

本文件由中国能源研究会标准工作办公室归口。

本文件起草单位：国网河南省电力公司信息通信分公司、云南电网有限责任公司信息中心、河南能汇信息科技有限公司、中能国研（北京）信息通信科技有限公司、中能国研(北京)电力科学研究院。

本文件主要起草人：巩锐、梅林、宋宁希、胡健、高峰、刘凯伦、郭曼、蔡頔、李璟瑜、肖鹏、宋瑞敏、刘佳峰、崔曼曼、陈何雄、刘静、梁志琴、黄慕夏。

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国能源研究会。

相关意见反馈联系方式：中国能源研究会标准执行办公室（E-mail: cers@cers.org.cn；电话：010-56284696）。

引　言

为贯彻落实国家相关网络安全政策法规要求，建立电力信息系统入网安全测试的技术要求，对电力信息系统的网络架构、操作系统、数据库、中间件、应用系统、移动应用和数据安全等方面提出了覆盖主要技术领域的安全测试要求，检验电力信息系统的网络架构、安全策略、设备配置等是否具备入网安全条件，在信息系统入网前减少和消除安全隐患，确保接入公司网络的电力信息系统及其相关软硬件安全、可靠，保障电力系统整体网络安全，保障电力信息基础设施安全、可靠、稳定、高效的运行，特制定本技术要求。

电力信息系统入网安全测试技术要求

1 范围

本文件规定了电力信息系统入网安全测试方法和测试技术要求。

本文件适用于新建、改建和扩建的电力信息系统安全规划设计和入网安全测试工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全风险 security risk

指各类应用系统及其赖以运行的基础网络、处理的数据和信息，因潜在威胁利用其软硬件缺陷、系统集成缺陷或安全管理薄弱环节，导致安全事件发生的可能性及可能造成的损失程度。

[来源：GB/T 25069—2022，3.164，有修改]

3.2

入网安全测试 network access security test

由具有相关网络安全专业服务资质的第三方机构，在系统上线投运前于最终运行环境组织实施的安全测试、评估，以验证产品符合安全需求定义。

3.3

电力信息系统 electric power information system

与电力企业的生产、运营、管理、控制相关的信息系统。

注：根据信息系统的责任单位、业务类型和业务重要性及物理位置差异等各种因素，可分为管理信息系统和电力监控系统。

[来源：GB/T 37138—2018]

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

APT：高级持续性威胁（Advanced Persistent Threat）

CPU：中央处理器（Central Processing Unit）

DLL：动态链接库（Dynamic Link Library）

HTTPS：安全的超文本传输协议（Hyper Text Transfer Protocol Secure）

IP：网际互连协议（Internet Protocol）

IPSec：互联网安全协议（Internet Protocol Security）

PTES：渗透测试执行标准（Penetration Testing Execution Standard）

SAM：安全账号管理器（Security Account Manager）

SSH：安全外壳协议（Secure Shell）

SSL/TLS：安全套接层（Secure Socket Layer/Transport Layer Security）

5 测试方法

5.1 方法要求

入网安全测试应记录并填写测试对象基本信息表（详见附录A表A.1），宜根据系统等级、风险评估结果等采取现场访谈、配置检查、漏洞扫描和渗透测试等方法组合进行。

5.2 现场访谈

与电力信息系统建设方、运营方、安全管理人员及开发厂商（如有）进行访谈，获取系统架构设计、数据流转路径、安全策略实施情况，以及安全管理制度执行记录。访谈内容应形成书面纪要并由测试方与被测方代表签字确认。

5.3 配置检查

依据基本技术要求对信息系统的网络设备、安全设备、操作系统、数据库、中间件以及应用软件进行安全配置合规性核查，对信息系统的安全现状进行综合分析评估，发现设备自身存在安全风险、漏洞和薄弱环节。检查结果应形成包含缺陷类型、设备位置及整改建议的核查记录表，对高危缺陷应现场验证整改有效性。

5.4 漏洞扫描

使用漏洞扫描工具，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测。扫描结果需经人工复现验证，确认漏洞真实存在性。

5.5 渗透测试

依据PTES框架，在授权范围内模拟APT攻击行为，评估计算机网络系统的弱点、技术缺陷或漏洞。测试过程不得影响系统正常运行，测试前应制定应急预案，发现的高危漏洞需提供漏洞验证截图及风险量化评估报告。

6 测试要求

6.1 入网安全测试总体要求

a) 在对电力信息系统进行入网测试时，应确保电力信息系统的数据架构、网络架构、安全防护和业务功能等符合如下要求。
   1） 数据架构方面：应检查系统业务模型数据的数据定义、结构及接口，确保满足跨系统数据交互安全性和兼容性需求；
   2） 网络架构方面：应检查系统应用数据存储，确保符合互联网业务、数据、安全、架构典型设计；应检查系统云平台部署架构，确保具备系统上云条件；应检查系统主要环节及核心部件，确保满足“n-1”架构要求；应检查用户权限管理，用户在登录主系统后，可以通过该认证机制访问其他相互信任的应用系统，无需再次登录；
   3） 安全防护方面：应检查第三方安全测试开展情况，包括功能与非功能测试、安全测试、渗透测试；应检查安全防护方案，确保防护措施与系统风险等级、业务连续性要求相匹配；应检查系统浏览器兼容性，确保满足业务用户操作体验并能够向前兼容；
   4） 业务功能方面：应检查业务功能实现情况，其中核心功能应全部经需求方确认。
b) 用到的检测仪器应经有检验资质的检测单位校验合格，并在检验有效期内。
c) 测试应由具有相关网络安全专业服务资质的第三方机构承担，如具有信息安全服务资质和通信网络安全服务能力评定等资质。
d) 信息系统入网安全测试人员应严格按照本文件规定的内容进行测试，将测试过程中获取的证据进行详细、准确地导出和记录，形成测试评分表（详见附录 A 表 A.2～A.9）。
e) 信息系统入网安全测试过程宜包含测试准备、测试实施、测试分析和测试总结等阶段（测试流程可参考附录 B）。
f) 信息系统入网安全测试结果判定与处理应符合以下要求：
   1） 测试合格：测试项中测试结果均符合测试要求和标准，则判定为测试合格，测试合格后由检测单位出具测试报告（模板见附录 C）；
   2） 测试不合格：若存在不符合项或高风险项，被测单位应根据测试要求和标准进行整改，并在整改完成后重新提交测试申请，直至测试合格。

   注：“高风险项”定义与测试项评分直接关联，任一测评项得分低于 100 分即视为存在高风险项（评分方法见附录 A.2～A.9）。

6.2 基础网络安全测试要求

6.2.1 结构安全测试要求：

a) 信息系统基础网络结构测试应确保符合 GB/T 22239-2019 中 9.1.2.1 的要求。
b) 应绘制与当前运行情况相符的系统网络拓扑结构图。
c) 系统网络拓扑结构应标明安全防护设备及网络设备的接线情况，并能清晰体现连接线两端的设备名称、端口号及 IP 地址。

6.2.2 网络边界安全等设备安全测试内容应包括身份鉴别、访问控制、安全审计和入侵防范。

a) 身份鉴别测试要求：
   1） 应核查已登录的系统用户的身份标识和鉴别，确保用户身份标识具有唯一性；
   2） 身份鉴别信息应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令复杂度需包含数字、大小写字母和特殊字符，口令有效期不超过 90 天；
   3） 应具有登录异常锁定功能，配置账户登录尝试 5 次后，应锁定账户或登录 IP 等；
   4） 应采取 SSH 或 HTTPS 方式进行远程管理。
b) 访问控制测试要求：
   1） 应核查用户最小权限需求设置对应的权限；

2） 应核查重命名、删除或禁用默认账户，应核查修改默认账户的默认口令；
3） 应核查多余的、过期的账户删除或停用情况，避免共享账户的存在。

c) 安全审计测试要求：
1） 应核查启动安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
2） 应核查审计记录，包括事件的日期和时间、用户、事件类型、事件结果及其他与审计相关的信息；
3） 应对审计记录保护进行核查，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录应保存 6 个月以上。

d) 入侵防范测试要求：
1） 应核查关闭不需要的系统服务、默认共享和高危端口；
2） 应核查通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制情况，网络地址范围不能超过整个 C 段。

6.3 操作系统安全测试要求

6.3.1 操作系统测试内容

操作系统测试内容应包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范和资源控制。

6.3.2 身份鉴别测试要求：

a) 应核查已登录的用户的身份标识和鉴别，确保身份标识具有唯一性。
b) 应对启用口令复杂度校验功能和强制定期更换的功能进行核查，要求账户口令长度应至少为 8 位，口令复杂度需包含数字、大小写字母和特殊字符，口令有效期不超过 90 天。
c) 应核查和测试登录失败处理功能，确保配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，会话超时时间为 15 分钟，登录失败锁定时间为 15 分钟，登录失败锁定阈值为 5 次。
d) 在远程管理时，应采取必要措施防止操作系统鉴别信息在网络传输过程中被窃听。

6.3.3 访问控制测试要求：

a) 访问控制测试应确保符合 GB/T 22239—2019 中 9.1.4.2 中的规定。
b) 应对 Windows 类操作系统安全控制选项进行检查，确保启用“不允许匿名枚举 SAM 账号与共享的匿名枚举”“不允许 SAM 账户的匿名枚举”与“不显示上次的用户名”。
c) 应对 Linux 类操作系统中禁止 ROOT 用户远程登录情况进行核查。

6.3.4 安全审计测试要求：

a) 安全审计测试应确保符合 GB/T 22239—2019 中 9.1.4.3 a)中的要求。
b) 应核查审计记录，包括事件的日期和时间、用户、事件类型、事件结果及其他与审计相关的信息。
c) 应对审计记录保护进行核查，确保定期备份，避免受到未预期的删除、修改或覆盖等，审计记录应保存 6 个月以上。

6.3.5 入侵防范测试要求：

a) 入侵防范测试应确保符合 GB/T 22239—2019 中 9.1.4.4 中的规定。
b) 应对漏洞进行核查和测试，确保已知的中、高风险漏洞不存在。

6.3.6 恶意代码防范测试要求：

a) 恶意代码防范测试应确保符合 GB/T 22239—2019 中 9.1.4.5 中的规定。
b) 应检查防恶意代码软件安装情况，并每周更新防恶意代码软件版本和恶意代码库。
c) 应检查防恶意代码软件统一管理功能及特征库定期更新功能。

6.3.7 资源控制测试要求：

a) 应检查通过设定终端接入方式、网络地址范围等方式限制终端登录情况。
b) 应检查通过监控系统对服务器主机用户的磁盘、CPU、内存等使用情况进行监控情况。

6.4 数据库安全测试要求

6.4.1 数据库测试内容

数据库安全测试应包括身份鉴别、访问控制、安全审计、入侵防范和备份及恢复。

6.4.2 身份鉴别测试要求：

a) 应核查已登录数据库的用户的身份标识和鉴别，确保身份标识具有唯一性。
b) 应对启用数据库口令复杂度校验功能和强制定期更换的功能进行核查，要求账户口令长度应至少为 8 位，口令复杂度需包含数字、大小写字母和特殊字符，口令有效期不超过 90 天。
c) 应核查和测试数据库登录失败处理功能，确保配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，会话超时时间为 15 分钟、登录失败锁定时间为 15 分钟、登录失败锁定阈值为 5 次。
d) 在远程管理时，应采取必要措施防止数据库鉴别信息在网络传输过程中被窃听。

6.4.3 访问控制测试要求：

a) 应核查已登录的用户分配账户和权限。
b) 应核查重命名或删除默认账户，应检查修改默认账户的默认口令。
c) 应对多余的、过期的账户删除或停用进行核查，避免共享账户的存在。
d) 应对授予管理用户所需的最小权限进行核查和测试，实现管理用户的权限分离。

6.4.4 安全审计测试要求：

a) 应检查启用数据库审计功能，或通过第三方审计系统对数据库进行审计，审计范围应覆盖到数据库所有账户。
b) 应检查审计内容，包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。
c) 应检查审计记录，包括事件的日期、时间、类型、主体标识、客体标识和结果等。
d) 应对审计记录保护措施进行核查，避免受到未预期的删除、修改或覆盖等，审计记录应保存 6 个月以上。

6.4.5 入侵防范测试要求：

a) 应检查数据库最小安装的原则，确保仅安装需要的组件，并定期更新数据库补丁。
b) 应对加密保存数据库中的敏感字段进行检查，如：用户鉴别信息等。
c) 应核查通过设定网络地址范围对通过网络进行管理的管理终端进行限制的情况。
d) 应对漏洞进行核查和测试，确保已知的中、高风险漏洞不存在。

e) 应对数据库默认端口修改情况进行检查。

6.4.6 备份及恢复测试要求：

a) 应检查本地数据备份与恢复功能，确保定期对数据库进行备份（重要系统每天进行全备份或增量备份）。
b) 应对重要系统的数据库具备冗余能力进行检查。

6.5 中间件安全测试要求

6.5.1 中间件测试内容

中间件安全测试应包括身份鉴别、访问控制、安全审计和入侵防范。

6.5.2 身份鉴别测试要求：

a) 应核查已登录数据库的用户的身份标识和鉴别，确保身份标识具有唯一性。
b) 应对启用口令复杂度校验功能和强制定期更换的功能进行核查，口令长度和更换周期应满足：口令长度应至少为 8 位，口令复杂度需包含数字、大小写字母和特殊字符，口令有效期不超过 90 天。
c) 应核查和测试登录失败处理功能，确保配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，会话超时时间 15 分钟、登录失败锁定时间 15 分钟和登录失败锁定阈值 5 次。
d) 当核查方进行远程管理时，应采取必要措施防止中间件鉴别信息在网络传输过程中被窃听。

6.5.3 访问控制测试要求：

a) 应核查已登录用户的分配账户和权限，严格限制默认账户和特权账户的访问权限。
b) 应严格限制配置文件和日志文件的访问权限，禁止站点目录浏览。
c) 应核查重命名或删除默认账户，应修改默认账户的默认口令，并使修改后的口令满足复杂度要求。
d) 应对多余的、过期的账户删除或停用进行核查，避免共享账户的存在。
e) 应对授予管理用户所需的最小权限进行核查和测试，实现管理用户的权限分离。

6.5.4 安全审计测试要求：

a) 应核查启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
b) 应核查审计记录，包括事件的日期和时间、用户、事件类型、事件结果及其他与审计相关的信息。
c) 应对审计记录保护进行核查，确保定期备份，留存时间应不低于 6 个月，应对审计记录采取措施避免受到未预期的删除、修改或覆盖等进行测试。

6.5.5 入侵防范测试要求：

a) 应核查最小安装的原则，删除中间件不必要组件和缺省安装的无用文件。
b) 应对数据有效性检验功能进行核查和测试，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

6.6 应用系统安全测试要求

6.6.1 应用系统测试内容

应用系统安全测试应包括身份鉴别、访问控制、安全审计、资源控制、入侵防范、代码安全、应用行为和版本一致性。

6.6.2 身份鉴别测试要求：

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别。
b) 应对应用系统的用户标识唯一性进行检查，通过标识符可唯一确定用户身份。
c) 应对应用系统登录时同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别进行检查。
d) 对于口令、手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：
   1) 若采用口令作为验证要素，应对支持身份鉴别信息限制策略（如口令长度应至少为 8 位，口令复杂度需包含数字、大小写字母和特殊字符，口令有效期不超过 90 天等）的设置与检查功能进行检查；
   2) 若采用手势密码作为验证要素，应对手势密码设置连续的 4 个点进行检查；
   3) 若采用短信验证码作为验证要素，应检查短信验证码使用次数及时间，确保在规定时间内仅使用一次，短信验证码长度应不小于 6 位，且为数字或字母的随机组合，短信验证码所在的短信内容中，应告知用户短信验证码的用途；
   4) 若采用生物特征识别作为验证要素，应符合国家标准和相关信息安全管理要求，防止非法存储、复制和重放。
e) 应检查应用系统认证失败处理功能，可采取结束会话、限制失败登录次数和自动退出等措施。
f) 应核查非单点登录的应用系统，确保登录时增加附加随机码验证。
g) 在提示用户认证失败时，应检查模糊错误提示信息，防止在错误提示信息中泄露用户信息。
h) 在修改密码前，应对用户身份进行重新验证进行检查，如要求用户输入原密码，且应对原密码输入错误次数进行限制；修改密码时新密码不应与原密码相同。
i) 在重置密码时，应检查使用短信验证码、邮箱验证码或用户注册信息校核等方式，对用户身份进行校验。

6.6.3 访问控制测试要求：

a) 应核查授权主体配置访问控制策略，并严格限制默认账户的访问权限。
b) 应核查和测试删除或修改默认账号，如无法删除或修改，必须修改默认账号。
c) 应对访问控制功能进行核查，依据安全策略控制用户对文件、数据库表等客体的访问。
d) 应对授予不同账户为完成各自承担任务所需的最小权限进行核查，并在它们之间形成相互制约的关系，管理员账户不应参与业务流程。
e) 提供下载功能时，应严格限制用户下载文件的路径，避免用户非法下载应用系统其他文件。

6.6.4 安全审计测试要求：

a) 应核查启用覆盖到每个用户的应用系统日志审计功能，审计日志内容应至少包含以下项：用户登录、登出、失败登录日志；管理员授权操作日志；创建、删除（注销）用户操作日志；重要业务操作。
b) 应核查日志记录，包括：主体、客体、事件类型，日期时间、描述、结果等。
c) 应对日志记录保护进行核查，禁止删除或修改日志记录，日志记录应保存 6 个月以上。

6.6.5 资源控制测试要求：

a) 应对应用系统空闲超时自动结束会话功能进行检查。
b) 应对应用系统最大并发会话连接数的限制情况进行检查。
c) 应对检查应用系统单个账户的多重并发会话数的限制情况进行检查。

6.6.6 入侵防范测试要求：

a) 应检查避免应用系统使用存在已知漏洞的系统组件与第三方组件，对存在可被利用的高、中风险安全漏洞进行检查，包括但不限于：DLL 劫持、消息 hook 注入、进程注入、命令执行等漏洞。
b) 应对植入会影响系统和其他软件功能的恶意代码进行检查，包括但不限于：蠕虫类、病毒类、木马类、后门类、僵尸类、间谍类、逻辑炸弹类、挖矿病毒类或勒索软件类等。
c) 应检查应用系统是否调用危险函数，包括但不限于：gets、strcpy、strcat、sprintf、scanf、sscanf、fscanf、vfscanf、vsprintf、vscanf、vsscanf、streadd、strecpy 等函数。
d) 应检查应用系统在使用第三方组件时，避免第三方组件未经授权收集应用系统信息和个人信息。
e) 应对提供数据有效性检验功能进行核查，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。
f) 服务端应具备文件上传白名单过滤功能，确保只允许白名单范围内的文件类型上传，禁止上传 asp、aspx、jsp、php、asa、cer 等脚本类型文件。
g) 应检查当应用系统出现异常时，向用户提示出错信息，但不应泄露用户 IP 地址、数据库类型、内部接口路径等敏感信息。
h) 应核查所有管理或者操作页面均需要进行登录认证，避免恶意攻击者或普通用户通过绕过登录认证进行非法操作。
i) 应对应用系统后台的访问源限制情况进行核查，控制粒度为 IP、端口级别。
j) 应核查未使用未经安全加固的开源后台管理程序。
k) 对存在应用发布，应对后台管理页面服务端口与应用系统页面服务端口分离情况进行检查。
l) 应对应用系统支持单个用户使用的资源限制情况进行检查，如会话连接数、上传文件个数、带宽使用量等。

6.6.7 代码安全测试要求：

a) 应严格控制第三方函数与插件的使用，并对外来代码进行源代码审计、漏洞扫描等详细的安全测试。
b) 应开展源代码审计，检查源代码中、高危安全漏洞、后门或恶意代码存在情况，源代码漏洞类型包括行为问题、路径错误、数据处理、错误的 API 协议实现、劣质代码、不充分的封装、安全功能缺陷、Web 问题等。

6.6.8 应用行为测试要求：

a) 应对拥有合法的知识产权或已取得合法充分的版权授权情况进行检查，确保非盗版软件、破解软件，不侵犯第三方知识产权。
b) 应核查鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
c) 应对仅采集和保存业务必需的用户个人信息进行检查。
d) 应对禁止未授权访问和非法使用用户个人信息进行检查。

6.6.9 版本一致性测试要求：

应核查入网电力信息系统的软件版本号、代码、配置文件及第三方组件与研发测试阶段通过安全验证的版本完全一致，禁止未经授权的代码修改、组件替换或配置变更。

6.7 移动应用安全测试要求

6.7.1 移动应用测试内容

移动应用安全测试应包括身份鉴别、访问控制、权限控制、安全审计、通信安全和代码安全。

6.7.2 身份鉴别测试要求：

a) 在用户访问移动应用程序业务前，应对用户身份鉴别进行检查，应具备鉴别失败处理功能，包括但不限于结束会话、锁定或超时注销。
b) 当鉴别失败时，应对提供通用的错误提示信息进行检查，避免提示信息被攻击者利用。
c) 当用户进行敏感操作前（如修改鉴别信息、转账支付等），应对再次鉴别用户身份进行检查，确保采用双因子认证方式。
d) 当移动应用程序支持口令登录功能时，应对提供口令复杂度校验功能进行检查，保证用户设置的口令达到一定的强度；移动应用程序应对用户设置的口令进行强度检测，至少包含 8 位字符，需包括大写字母、小写字母、数字和特殊字符中的至少三种。对安全要求较高的移动应用程序应提供双因子认证。
e) 应对具备的口令找回的验证机制进行检查，以防账户和口令被窃取或劫持。
f) 应对移动应用程序是否以明文的方式显示和存储用户口令进行检查，禁止默认缓存、填充用户口令信息。

6.7.3 访问控制测试要求：

a) 应对移动应用程序的用户细粒度访问权限划分进行检查，确保遵循最小授权原则，按照安全策略控制用户对业务功能、用户数据的访问。
b) 应对只有授权的用户才能访问移动应用程序敏感信息进行检查。

6.7.4 权限控制测试要求：

a) 应对移动应用程序申请权限时遵循最小权限原则进行检查，避免申请与其业务功能无关的其他权限。
b) 应检查移动应用程序申请敏感权限前，采用勾选/确认的主动方式征得用户同意，且用户拒绝后不影响相关业务的使用。
c) 应检查移动应用程序在动态申请权限时，弹出权限申请提示信息并说明相关权限的信息、目的及可能存在的风险；在用户确认后，方可向系统动态申请权限。
d) 应对服务端用户权限配置进行核查，以规避越权行为。
e) 应对服务端敏感数据访问权限控制进行核查和测试。

6.7.5 安全审计测试要求：

a) 应对安全日志功能进行检查，确保具备。
b) 应对移动应用程序运营和产生的数据进行安全审计检查，包括但不限于运行记录、操作日志、安全日志。
c) 应对提供审计日志授权访问机制进行检查，审计日志应仅支持授权用户查阅。

d) 应对客户端日志数据加密保护进行检查，日志记录应保存 6 个月以上。
e) 客户端应删除与移动应用运行逻辑相关的日志数据。

6.7.6 通信安全测试要求：

a) 应对客户端与服务端在通信时采用的安全通信协议进行测试，例如 SSL/TLS、IPSec 等。
b) 应对服务端与移动应用、与其他服务端在通信时的通信数据加密保护进行检查。
c) 应查看服务端与移动应用、与其他服务端在通信时的通信数据已进行完整性校验。

6.7.7 代码安全测试要求：

a) 应检查客户端的源代码（包括 Java、C、Python、Lua 等语言的源代码）是否已进行混淆处理。
b) 应检查和测试客户端签名信息已进行安全校验。

6.8 数据安全测试要求

6.8.1 数据安全测试内容

数据安全测试应包括数据完整性、数据保密性、数据可用性、数据备份恢复和剩余信息保护。

6.8.2 数据完整性测试要求：

应核查已采用校验技术保证重要的业务数据在传输过程中的完整性。

6.8.3 数据保密性测试要求：

a) 应核查数据库中敏感数据已使用国家管理部门认可的密码算法进行加密。
b) 应核查密钥是否与数据分离存储、是否定期轮换、是否有严格的密钥访问控制权限。

6.8.4 数据可用性测试要求：

a) 应核查在正常业务运行和异常场景（如网络中断、设备故障等）下，授权人员均能及时访问所需数据。
b) 应核查已部署冗余机制（如双通道传输、主备存储节点），确保重要业务数据持续可访问。
c) 应核查对高优先级业务数据的访问请求已实施分级调度策略，保障紧急操作需求优先响应。
d) 应核查在数据存储、传输过程中已建立容错机制（如数据校验、断点续传），防止数据不可用。
e) 应核查电力信息系统已实现数据访问延迟的实时监控与告警功能。
f) 应核查电力信息系统对用户权限范围内的数据访问请求已提供完整的接口支持，包括实时查询、历史追溯等操作。
g) 应测试高并发场景下系统是否能正常响应，是否存在数据查询超时或失败的情况。

6.8.5 数据备份恢复测试要求：

a) 应核查已提供重要的业务数据的本地数据备份与恢复功能。
b) 应核查已提供异地数据备份功能，利用加密链路传输将重要数据定时批量传送至备用场地。
c) 应核查在遭受攻击或故障后，已通过备份数据快速恢复业务访问能力。
d) 应核查备份数据是否采用加密存储，防止备份泄露。

6.8.6 剩余信息保护测试要求：

应核查系统运行中产生的临时数据（如内存中的敏感数据、浏览器缓存、应用程序缓存）是否在会话结束后及时清除（如退出登录后，内存中的用户密码是否清零、浏览器缓存中是否残留未脱

敏的敏感信息等）。

附 录 A
（规范性）
测试记录表

表 A.1 测试对象基本信息

测试对象信息			
设备名称		设备类型	
设备型号		设备功能	
设备部署方式		设备部署环境	
设备网络接入方式		设备 IP 地址（如有）	
设备 MAC 地址（如有）		操作系统版本（如有）	
补丁安装情况（如有）		数据库版本（如有）	
中间件版本（如有）		与网络和业务应用相关的配置信息和端口开放信息（如有）	
终端用户情况（如有）		应用软件相关情况（如有）	
数据采集/存储/传输情况（如有）			
测试日期			

表 A.2 入网安全测试总体要求评分表

测试编号	测评项	标准	分值
1	6.1a 系统入网基础要求	1.数据架构满足跨系统数据交互安全性和兼容性需求。 2.网络架构满足互联网典型设计，具备上云条件，满足“n-1”架构要求，可通过认证机制访问其他相互信任的应用系统。 3.安全防护满足开展第三方测试，具有安全防护方案，系统浏览器具有兼容性。 4.业务功能满足核心功能全部实现。	100 分
2	6.1b 检测工具	1.检测仪器合格。 2.检测仪器在有效期内。	100 分
3	6.1c 服务资质	1.检测单位具备相关资质。	100 分
4	6.1d 测试结果判定	1.测试内容完整。 2.具有测试报告。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.3 基础网络安全测试要求评分表

测试编号	测试项	标准	分值
1	6.2.1 结构安全测试	1.网络结构满足 GB/T 22239-2019 中 9.1.2.1 的要求。 2.绘制有系统网络拓扑结构图。 3.系统网络拓扑结构符合公司规定。	100 分
2	6.2.2a 身份鉴别	1.身份标识具有唯一性。 2.身份鉴别信息具有复杂度且定期更换。 3.身份鉴别信息具有登录异常锁定功能。 4.采取 SSH 或 HTTPS 方式进行远程管理。	100 分

3	6.2.2b 访问控制	1.设置有用户最小权限。 2.修改默认账户的默认口令。 3.不存在共享账户。	100 分
4	6.2.2c 安全审计	1.启动安全审计功能。 2.具有审计记录。 3.审计记录已保护且定期备份。	100 分
5	6.2.2d 入侵防范	1.已关闭不需要的系统服务、默认共享和高危端口。 2.通过网络进行管理的管理终端已限制。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.4　操作系统安全测试要求评分表

测试编号	测试项	标准	分值
1	6.3.2 身份鉴别	1.身份标识具有唯一性。 2.身份鉴别信息具有复杂度且定期更换。 3.身份鉴别信息具有登录失败处理功能。 4.远程管理具备防窃听措施。	100 分
2	6.3.3 访问控制	1.访问控制满足 GB/T 22239—2019 中 9.1.4.2 中的规定。 2.操控系统安全控制选项启用“不允许匿名枚举 SAM 账号与共享的匿名枚举”“不允许 SAM 账户的匿名枚举”与“不显示上次的用户名”3.禁止 ROOT 用户远程登录。	100 分
3	6.3.4 安全审计	1.安全审计满足 GB/T 22239—2019 中 9.1.4.3 a)中的要求。 2.具有审计记录。 3.审计记录已保护且定期备份。	100 分
4	6.3.5 入侵防范	1.入侵防范满足 GB/T 22239—2019 中 9.1.4.4 中的规定。 2.不存在已知的中、高风险漏洞。	100 分
5	6.3.6 恶意代码防范	1.恶意代码防范满足 GB/T 22239—2019 中 9.1.4.5 中的规定。 2.安装防恶意代码软件。 3.具备防恶意代码软件统一管理功能及特征库定期更新功能。	100 分
6	6.3.7 资源控制	1.通过设定终端接入方式、网络地址范围等方式限制终端登录。 2.通过监控系统对服务器主机用户的磁盘、CPU、内存等使用情况进行监控。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.5　数据库安全测试要求评分表

测试编号	测试项	标准	分值
1	6.4.2 身份鉴别	1.身份标识具有唯一性。 2.具有复杂度且定期更换。 3.具备登录失败处理功能。 4.远程管理具备防窃听措施。	100 分

2	6.4.3 访问控制	1.已登录用户分配账户和权限控制。 2.不存在默认登录口令。 3.不存在共享账户。 4.管理用户权限分离。	100 分
3	6.4.4 安全审计	1.启用数据库审计功能。 2.审计内容全面。 3.审计记录完整。 4.具备审计记录保护措施。	100 分
4	6.4.5 入侵防范	1.满足数据库最小安装的原则。 2.加密保存数据库中的敏感字段。 3.通过网络进行管理的管理终端已限制。 4.不存在已知的中、高风险漏洞。 5.数据库默认端口已修改。	100 分
5	6.4.6 备份及恢复	1.具备本地数据备份与恢复功能。 2.数据库具备冗余能力。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.6　中间件安全测试要求评分表

测试编号	测试项	标准	分值
1	6.5.2 身份鉴别	1.身份标识具有唯一性。 2.具有复杂度且定期更换。 3.具备登录失败处理功能。 4.远程管理具备防窃听措施。	100 分
2	6.5.3 访问控制	1.严格限制默认账户和特权账户的访问权限。 2.严格限制配置文件和日志文件的访问权限。 3.不存在默认口令。 4.不存在共享账户。 5.管理用户权限分离。	100 分
3	6.5.4 安全审计	1.启用数据库审计功能。 2.审计记录完整。 3.具备审计记录保护措施。	100 分
4	6.5.5 入侵防范	1.满足最小安装的原则。 2.具备数据有效性检验功能。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.7　应用系统安全测试要求评分表

测试编号	测试项	标准	分值
1	6.6.2 身份鉴别	1.提供专用的登录控制模块。 2.身份标识具有唯一性。 3.采用两种或两种以上组合的鉴别技术实现用户身份鉴别。 4.口令、手势密码、短信验证码、生物特征信息等不同验证要素或验证要素组合需满足相关需求。 5.具备认证失败处理功能。 6.登录时增加附加随机码验证。 7.具有模糊错误提示信息。	100 分

		8.修改密码前对用户身份重新验证。 9.修改密码时采取不同方式对用户身份校验。	
2	6.6.3 访问控制	1.严格限制默认账户的访问权限。 2.不存在默认账号。 3.具备访问控制功能。 4.不同账户为各自承担任务所需的最小权限。 5.严格限制用户下载文件的路径。	100 分
3	6.6.4 安全审计	1.启用应用系统日志审计功能。 2.审计记录完整。 3.具备审计记录保护措施。	100 分
4	6.6.5 资源控制	1.应用系统具备空闲超时自动结束会话功能。 2.对应用系统最大并发会话连接数进行限制。 3.对单个账户的多重并发会话数进行限制。	100 分
5	6.6.6 入侵防范	1.不存在可被利用的高、中风险安全漏洞。 2.不存在会影响系统和其他软件功能的恶意代码。 3.应用系统不存在调用危险函数情况。 4.第三方组件未经授权不应收集应用系统信息和个人信息。 5.具备数据有效性检验功能。 6.服务端应具备文件上传白名单过滤功能。 7.提示错误信息不应泄露用户或应用软件的敏感信息。 8.所有管理或者操作页面均需要进行登录认证。 9.应用系统后台的访问源限制控制粒度为 IP、端口级别。 10.未使用开源的后台管理程序。 11.后台管理页面服务端口与应用系统页面服务端口应分离。 12.限制应用系统的单个用户使用的资源。	100 分
6	6.6.7 代码安全	1.严格控制第三方函数与插件的使用。 2.开展源代码审计，源代码不存在中、高危安全漏洞、后门或恶意代码。	100 分
7	6.6.8 应用行为	1.不侵犯第三方知识产权。 2.鉴别信息所在的存储空间被释放或重新分配。 3.仅采集和保存业务必需的用户个人信息。 4.禁止未授权访问和非法使用用户个人信息。	100 分
8	6.6.9 版本一致性	入网电力信息系统与研发测试阶段通过安全测试版本一致	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.8　移动应用安全测试要求评分表

测试编号	测试项	标准	分值
1	6.7.2 身份鉴别	1.具备鉴别失败处理功能。 2.提供通用的错误提示信息。 3.进行敏感操作前采用双因子认证方式。 4.具有复杂度且定期更换。 5.具备的口令找回的验证机制进行检查。 6.以明文的方式显示和存储用户口令。	100 分
2	6.7.3 访问控制	1.遵循最小授权原则。 2.只有授权的用户才能访问移动应用程序敏感信息。	100 分
3	6.7.4 权限控制	1.遵循最小权限原则。 2.申请敏感权限采用勾选/确认的主动方式征得用户同意。	100 分

		3.在动态申请权限时采用弹出权限申请提示信息并说明相关权限的信息、目的及可能存在的风险。 4.对用户进行权限配置，不存在越权行为。 5.对敏感数据进行访问权限控制。	
4	6.7.5 安全审计	1.具备安全审计功能。 2.对移动应用程序运营和产生的数据进行安全审计。 3.具备审计日志授权访问机制。 4.客户端日志数据进行加密保护且保存 6 个月。 5.删除与移动应用运行逻辑相关的日志数据。	100 分
5	6.7.6 通信安全	1.客户端与服务端进行通信时采用安全通信协议。 2.通信时对通信数据进行加密保护。 3.通信时对通信数据进行完整性校验。	100 分
6	6.7.7 代码安全	1.客户端的源代码进行混淆处理进行核查和测试。 2.客户端签名信息进行安全校验。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

表 A.9　数据安全测试要求评分表

测试编号	测试项	标准	分值
1	6.8.2 数据完整性	1.采用校验技术保证业务数据在传输过程中的完整性。	100 分
2	6.8.3 数据保密性	1.使用国家管理部门认可的密码算法进行加密。 2.密钥与数据分离存储，密钥定期更换且具有严格访问控制权。	100 分
3	6.8.4 数据可用性	1.在正常业务运行和异常场景下，授权人员能及时访问所需数据。 2.已部署冗余机制，确保重要业务数据持续可访问。 3.对优先级业务数据的访问请求实施分级调度策略。 4.在数据存储、传输过程中已建立容错机制。 5.具备数据访问延迟的实时监控与告警功能。 6.用户权限范围内的数据访问请求具有完整的接口支持。 7.高并发场景下系统正常响应，不存在数据查询或失败情况。	100 分
4	6.8.5 数据备份恢复	1.重要的业务数据具备本地数据备份与恢复功能。 2.具备异地数据备份功能。 3.具备通过备份数据快速恢复业务访问能力。 4.异地备份数据采用加密存储。	100 分
5	6.8.6 剩余信息保护	1.信息系统运行产生的临时数据在会话结束后及时清除。	100 分
评分依据与方法： 1.根据测试项是否满足测试要求和标准给予测试项分值。 2.若测试项中测试结果均符合测试要求和标准，则测试合格，得分为 100 分；每存在一项不符合测试要求或标准的，则减 10 分。 3.只要有一个测评项得分低于 100 分，即视为存在高风险项，则不符合入网测试要求，被测系统不宜接入公司网络。			

附 录 B
（资料性）
测试流程

B.1 测试流程要求

信息系统入网安全测评流程图具体见图1。

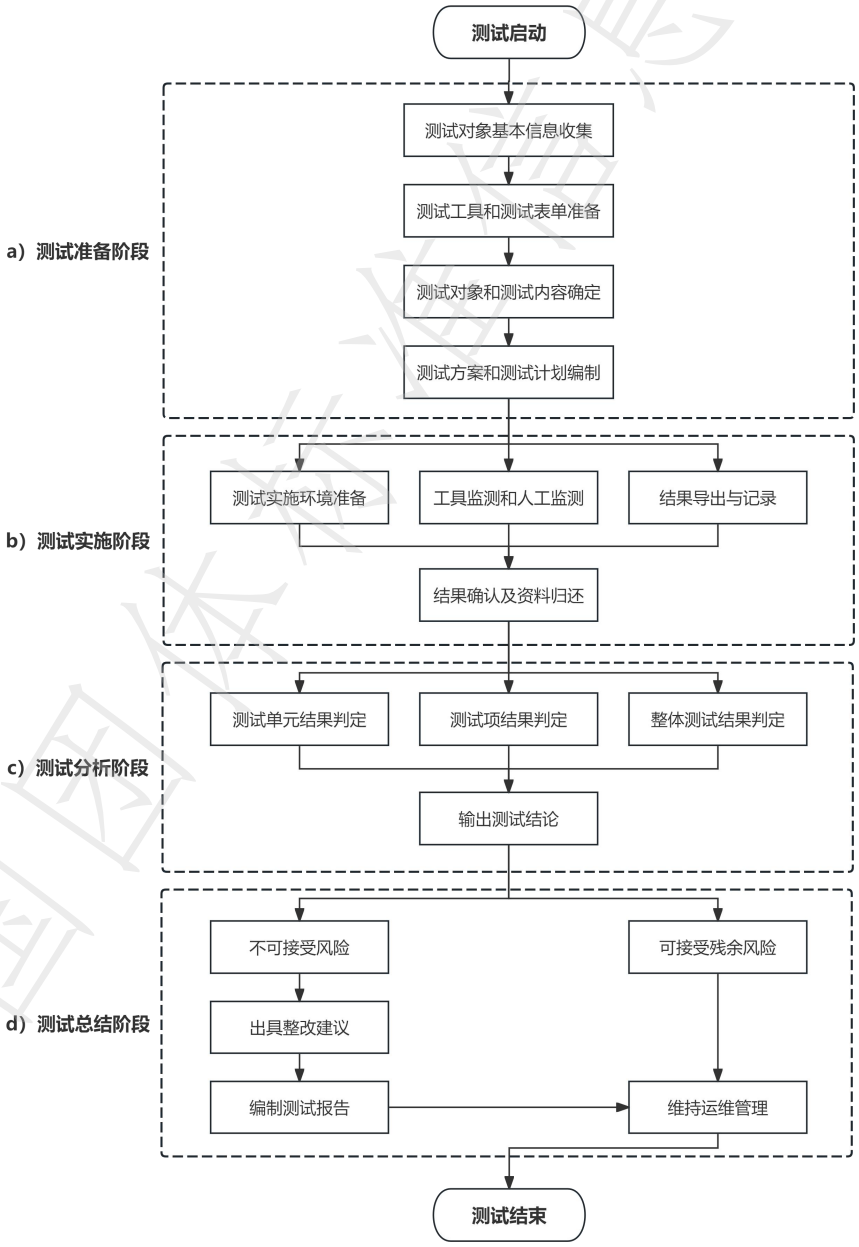

图 1 测评流程图

B.2 测试准备阶段

测试准备阶段的工作应包括如下内容：

a) 测试对象基本信息收集。测试人员应对被测对象相关信息、框架结构、部署环境等内容进行调研，了解业务真正的安全需求，填写测试对象基本信息表（详见附录 A 表 A.1）。测试对象调研信息包括：设备名称、设备类型、设备型号、设备版本、设备功能；设备部署方式、设备部署环境、设备网络接入方式、设备 IP 地址（如有）、设备 MAC 地址（如有）；操作系统版本（如有）、补丁安装情况（如有）、数据库版本（如有）、中间件版本（如有）；与网络和业务应用相关的配置信息和端口开放信息（如有）；终端用户情况（如有）；应用软件相关情况（如有）；数据采集/存储/传输情况（如有）。

b) 测试工具和测试表单准备。测试人员应根据被测对象基本信息的收集与分析，初步确定测试工作中使用的测试工具和测试记录表。

c) 测试对象和测试内容确定。测试人员应根据被测对象基本信息的收集与分析，确定测试工作的具体测试对象及测试内容。

d) 测试方案和测试计划编制。测试人员应编制电力信息系统入网安全测试方案和测试计划，内容应包括但不限于测试对象、测试依据、测试内容、测试方法、测试工具、测试计划、测试人员等。

B.3 测试实施阶段

测试实施阶段的工作应包括如下内容：

a) 测试实施环境准备。测试实施阶段开始时，测试人员应进行测试工具的部署和调试，保证测试工具输出结果的可靠性。

b) 工具检测和人工检测及结果导出、记录。测试人员按照本技术要求规定的测试要求开展测试，并将测试过程中获取的证据进行详细、准确地导出和记录，形成测试评分表。

c) 结果确认及资料归还。测试实施阶段完成时，测试人员应与被测单位确认测试实施阶段全部完成且形成对应的测试记录，并确认测试实施阶段记录的证据准确性。确认测试实施工作完成后，测试人员应归还测试对象的相关资料、移交相关权限。

B.4 测试分析阶段

测试分析阶段的工作应包括如下内容：

a) 测试单元结果判定。测试人员应首先通过证据分析，给出每一个测试单元的判定结果。

b) 测试项结果判定。测试人员应根据测试单元的判定结果确定每一个测试项的判定结果。

c) 整体测试结果判定。测试人员应根据测试项的判定结果确定电力信息系统准入测试的整体结果。

d) 输出测试结论。测试人员应根据整体测试结果给出电力信息系统准入测试的结论。

B.5 测试总结阶段

测试总结阶段的工作应包括如下内容：

a) 出具测试报告。在测试总结阶段，测试人员应根据测试记录和结果判定，编制测试报告。

b) 测试报告内容。测试报告应包括：测试对象信息，包括设备名称、版本号、操作系统平台（如有）、被测单位信息等；测试机构和测试人员信息，包括测试机构名称、测试人员基本信息等；测试环境信息，包括测试地点、测试时间、测试工具等；测试总体结论，包括测试项总体符合情况、测试项符合率、测试通过结果等；测试项符合情况，包括测试范围、每个测试项的

测试过程简述、符合情况判定等；安全风险分析；安全建议等。

C

附 录 C
（资料性）
电力信息系统入网安全测试报告

XXXX（公司名称）

电力信息系统入网安全测试报告

年 月 日

（测试总结阶段，测试机构应组织测试人员依据测试记录，通过测试结果分析及符合性判定，形成包含测试结论、安全风险分析和整改建议的正式测试报告。应有六部分内容组成。）

1、测试对象基本信息

描述测试对象基本信息，内容包括但不限于设备名称、版本号、操作系统平台（如有）、被测单位信息等情况。

2、测试工作内容

具体描述测试工作内容，内容包括但不限于测试依据（原理）、测试必要性、工作范围、测试方法、测试工具、测试计划（含时间、地点）、测试流程、测试机构及人员。

3、信息系统入网安全测试项

记录信息系统入网测试安全项内容，包括电力信息系统的网络架构、操作系统、数据库、中间件、应用系统、移动应用和数据安全等方面。

4、安全风险分析

测试报告应采用风险分析的方法对测评结果中存在安全问题进行分析，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对测评对象安全造成影响的程度，综合评价这些不符合项或部分符合项对测评对象造成的安全风险。风险分析主要内容包括安全风险项、已加固风险项、测试通过项和测试不适用项。

5、测试结论

应结合各类测评记录表和测评结果的风险分析给出电力信息系统入网测评结论。

1）符合电力信息系统入网要求：测评对象中所有测评项得分均为100分，且未发现中/高风险项，低风险项需记录并整改。

2）不符合电力信息系统入网要求：测评对象中存在不符合要求项，测评结果中部分测评项得分未达到100分，或存在安全问题。

6、安全建议

结合安全风险分析及测试结论，提出相对应的安全建议。

参 考 文 献

[1] GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价

[2] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

[3] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

[4] GB/T 25069—2022 信息安全技术 术语

[5] GB/T 37138—2018 电力信息系统安全等级保护实施指南

[6] Q/GDW 11445—2015 国家电网公司管理信息系统安全基线要求

[7] 国家能源局.《电力监控系统安全防护总体方案》：国能安全〔2015〕36号.[EB/OL].(2015-02-04)(2024-10-08)https://d.wanfangdata.com.cn/claw/G000260170

[8] 国家能源局.《电力行业网络安全管理办法》：国能发安全规〔2022〕100号.[EB/OL].(2022-11-16)(2024-10-08).http://zfxxgk.nea.gov.cn/2022-11/16/c_1310683245.htm

[9] 国家能源局.《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.[EB/OL].(2022-11-16)(2024-10-08).https://zfxxgk.nea.gov.cn/2022-11/16/c_1310683235.htm

[10] 国家发改委.《电力监控系统安全防护规定》：国家发改委2024年第27号令.[EB/OL].（2024-11-25）（2025-01-07）.https://www.ndrc.gov.cn/xxgk/zcfb/fzggwl/202412/t20241211_1394960.html