ICS
F 07

中华人民共和国国家标准

GB/T 36047—2018

电力信息系统安全检查规范

Electr

2018-03-15 发布 2018-10-

中华人民共和国国家质量监督检
中 国 国 家 标 准 化 管 理 委 员 会

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　检查工作流程 …… 2
4.1　检查准备 …… 2
4.2　检查实施 …… 3
4.3　检查结果分析 …… 3
5　检查内容和检查方法 …… 3
5.1　组织体系 …… 3
5.2　规章制度 …… 4
5.3　资金保障 …… 5
5.4　人员安全管理 …… 5
5.5　服务外包管控 …… 6
5.6　关键信息资产管控 …… 7
5.7　信息系统建设安全 …… 8
5.8　信息系统运行安全管理 …… 8
5.9　应急管理 …… 9
5.10　安全分区防御体系 …… 10
5.11　网络安全防护 …… 12
5.12　主机和设备安全防护 …… 13
5.13　应用系统和数据安全防护 …… 14
5.14　物理环境安全防护 …… 15
5.15　业务连续性保护 …… 16
附录A（资料性附录）　风险分析方法 …… 17
A.1　定性分析 …… 17
A.2　定量分析 …… 19
参考文献 …… 23

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家电力监管委员会提出。

本标准由全国电力监管标准化技术委员会(SAC/TC 296)归口。

本标准起草单位：国家能源局信息中心、国家能源局华北监管局、国家能源局浙江监管办公室。

本标准主要起草人：梁建勇、胡红升、周志明、陈雪鸿、黄瑞意、陈红建、王鹏、温红子、叶世超、李焕、谷双魁、刘韧、朱朝阳、李凌、朱世顺、张五一、刘雪梅、陈华军、郑晓岚、张鑫、赵婷、季澍、王闻韫。

引　言

为规范电力信息系统安全的检查[redacted]的侵害，保障电力信息系统的安全稳定运行，保护国家关键信息基础设施的[redacted]全和电力行业信息系统安全的规定和要求，制定本[redacted]

电力信息系统安全检查规范

1 范围

本标准规定了电力信息安全检查工作的流程、方法和内容等。

本标准适用于行业网络与信息安全主管部门开展电力信息系统安全的检查工作，[illegible]电力企业在本集团(系统)范围内开展相关信息系统安全的自查工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 5271.8 信息技术词汇 第8部分：安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 5271.8、GB 17859—1999、GB/T 22239—2008 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

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。

[illegible]、业务类型和业务重要性及物理位置差异等各种因素，可分为管理信息类系统和控制类系统。

3.2

管理信息类系统 management information system

支持电力企业的经营、管理和运营的信息系统。

[illegible]系统。

注：如门户网站系统、电力营销管理系统、财务管理系统、人力资源管理系统、物流管理系统和质量管理系统等。本类系统往往部署于管理信息大区，与互联网的隔离强度为逻辑[illegible]隔离强于[illegible]隔离但弱于物理隔离。

3.3

生产控制类系统 production control system

用于监视和控制电网及电厂生产运行过程[illegible]的、基于计算机及网络技术的业务处理系统及智能设备。

注：如电力调度数据网络、电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装置、[illegible]油量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统等。本类系统原则上部署于生产控制大区，与互联网[illegible]的隔离强度近似于物理隔离。

3.4

控制区 control area

具有实时监控功能、纵向联接使用电力调度数据网的实[illegible]

全区域。

3.5

非控制区　non-control area

生产控制范围内，面在线运行但不直接参与控制作为电力生产过程的重要环节，供自联接使用电力调度数据网的非控制类子网的各业务系统构成的安全区域。

4　检查工作流程

4.1　检查准备

4.1.1　明确检查工作依据

检查工作依据包括国家信息安全规范性文件及标准、行业信息安全规范性文件及标准、主管机构要求等。

4.1.2　明确检查对象

检查工作范围包括被检查方、被检查系统、涉及的人员等，并通过调研形成调研表。

信息系统安全检查工作调研表应按包含以下要素进行设计：

a）　信息系统主要功能、部署检查对象网络拓扑结构、服务对象用户规模、业务周期、运行高峰期等；

b）　业务主管部门、建设situation、系统开发商和集成商、上线运行及系统升级时间等；

c）　定级情况、数据集中情况、灾备情况等。

4.1.3　明确检查工作内容

检查工作内容由检查方依据有关信息安全主管单位要求，结合被检查方信息化工作开展情况等进行确定。检查内容由两部分组成，一部分为基本检查内容，见第5章；另外一部分为补充检查内容，由检查方拟定。

根据检查对象的不同，检查内容进一步细分为：通用检查项（标记为G）、仅适用于管理信息类系统的检查项（标记为M）、仅适用于[illegible]的检查项（标记为C）。检查项目选择方法有全覆盖法、随机抽取法和重点项抽取法：全覆盖法即区分被检查系统为管理信息类系统还是生产控制类系统，选取相关全部备选检查项作为检查内容；随机抽取法即从备选检查项中随机抽取检查内容；重点项抽取法即从备选检查项中确定重点内容进行检查。

制定信息系统安全检查方案和信息系统安全检查工作表。信息系统安全检查方案一般包含概述、检查依据、技术思路、被检查系统的范围、业务情况、安全防护情况、检查内容和检查组成员、工作计划和内容安排等；信息系统安全检查工作表需列出所有检查内容。

在现场检查开始前，检查方宜提前将信息系统安全检查方案下发至被检查方，向被检查方介绍安全检查的意义和目的、检查流程和工作方法，明确被检查方应提供的基本资料，向被检查方说明检查工作自身的风险和规避方法。被检查方应积极配合，向检查方介绍本单位的信息化建设状况与发展情况，为检查人员的信息收集提供支持和协调，并备份数据和系统，制定应急预案。

由检查方统一组织实施检查工作，确定实施现场检查工作的人员和设备。委托第三方机构实施现场检查工作，检查方应在现场检查前对第三方服务机构及其委派人员的资质进行确认，并安排专人陪同。

4.2 检查实施

4.2.1 检查实施过程主要内容

要依据检查方案开展现场检查工作，通过人员访谈、文档查阅、配置核查、安全测试等检查方法，对信息系统的保护措施与本标准要求的符合情况取得分析与总结活动所需的资料。

在现场检查过程中，检查方需辨别检查项的不适用，即检查项所防范的威胁在被检查方中是否存在，如果不存在，则该检查项应标为不适用项。

检查方原则上不接触被检查设备，特殊检查方能否实施根据操作规程和检查需求对被检查对象进行核查操作。在进行验证测试和工具测试前，检查方应与被检查方充分沟通，提前采取预防措施，避免影响系统正常运行。

被检查方应协助检查方完成[illegible]操作、协助检查人员实施[illegible]测试并提供有效建议、对检查结果进行确认、检查完成之后确认被检查[illegible]统工作正常等。

检查方根据被检查系统实际情况[illegible]与信息系统安全检查工作表，检查完成后应由检查方和被检查方共同签字确认。

4.2.2 检查[illegible]实施过程采用的方法

4.2.2.1 人员访谈：检查人员通过与信息系统有关人员（个人或群体）进行交流、讨论等活动，获取证据以证明信息系统安全防护措施是否[illegible]有效的一种方法。

4.2.2.2 文档查阅：检查人员通过对被被检查方支撑信息系统安全建设与运维的安全管理制度、记录等文档的核查，获取证据以证明信息系统安全的防护要求是否全面，防护规定是否得到执行。

4.2.2.3 配置核查：检查人员通过对被检查对象的配置进行查验，获取证据以证明信息系统安全防护措施是否有效的一种方法。

4.2.2.4 安全测试：检查人员使用预定的方法、工具使被检查对象产生特定的行为，通过查阅分析返回行为的结果，获取证据以证明信息系统安全防护措施是否有效的一种方法。在检查中也可不重新实施安全测试而利用已有的安全测试结果。

4.3 检查结果分析

检查结果分析是总结被检查系统整体安全防护能力的综合评价活动，根据现场检查[illegible]结果和[illegible]准的相关要求，定位整个[illegible]统的安全防护现状与本标准安[illegible]系统面临的风险，从而给出检查结论，形成检查报告和整改通知书。

在检查结果分析阶段，检查方对检查结果进行整理，编制信息系统安全[illegible]告和整改通知书，也可参见附录A的定量或定性风险分析方法，给出风险分析结果。

检查方应对检查过程中生成的过程文档进行归档保存，并严格管理。

5 检查内容和检查方法

5.1 组织体系

5.1.1 第一责任人确立（G）

5.1.1.1 检查项包括：电力企业主要负责人是否为本单位网络与信息安全的第一责任人。

5.1.1.2 检查方法：文档查阅，查阅电力企业信息安全文件中电力企业主要负责人是否为本单位网络与信息安全的第一责任人。

5.1.2 信息安全责任落实(G)

5.1.2.1 检查项包括

a) 是否设立信息安全主管、系统管理员、网络管理员、安全管理员等岗位；

b) 是否以文件的形式明确责任部门、责任人员的职责；

c) 如有专门监控系统，是否将监控系统安全防护工作及信息报送纳入日常安全生产管理体系，落实分级负责的责任制。

5.1.2.2 [illegible]文件。

5.1.3 专职机构及岗位设置(G)

5.1.3.1 检查项包括：电力企业是否成立工作领导机构，并设立网络与信息安全岗位，定义岗位职责，明确人员分工和技能要求，明确责任部门。

5.1.3.2 检查方法

a) 人员访谈，询问电力企业是否设置信息安全工作领导机构，并设立网络与信息安全岗位，定义岗位职责，明确人员分工和技能要求；

b) 文档查阅，查阅电力企业信息安全工作领导机构及岗位设置说明文件。

5.1.4 安全人员配置(G)

5.1.4.1 检查项包括：电力企业是否配备一定数量的专职信息安全工作人员。

5.1.4.2 检查方法：文档查阅，查阅电力企业岗位职责说明及人员岗位职责分配说明。

5.2 规章制度

5.2.1 整体策略及总体方案制定(G)

5.2.1.1 检查项包括：电力企业是否制定[illegible]案，是否说明了信息安全工作总体目标、范围、防[illegible]

5.2.1.2 检查方法：文档查阅，查阅电力企业信息安全整体策略和总体方案。

5.2.2 制度制定及体系完整性

5.2.2.1 检查项包括：电力企业是否针对信息安全工作制定基本安全管理制度，并以此为基础形成涵盖人员管理、资产管理、介质管理、建设安全管理、运行维护管理、外包服务管理、培训教育等方面的制度体系。

5.2.2.2 检查方法：文档查阅，查阅电力企业的基本管理制度文件，查看其内容是否涵盖人员管理、资产管理、介质管理、建设安全管理、运行维护管理、外包服务管理、培训教育等方面。

5.2.3 操作规程制定(G)

5.2.3.1 检查项包括：电力企业是否对信息安全运行维护人员执行的日常操作制定运维流程和操作规程。

5.2.3.2 检查方法：文档查阅，查阅电力企业制定的运维流程和操作规程文档。

5.2.4 制度发布(G)

5.2.4.1 检查项包括：电力企业是否通过正式、有效的方式发布信息安全管理制度。

5.2.4.2 检查方法如下：

a) 人员访谈，询问电力企业信息安全管理制度的发布方式；

b) 文档查阅，查阅电力企业信息安全管理制度发布方式相关记录。

5.3 资金保障

5.3.1 经费预算(G)

5.3.1.1 检查项包括：电力企业是否将信息安全建设费用(安全软硬件购置、系统安全功能开发、安全验证测试、安全咨询与培训、安全专项研究等)和运行维护费用(日常安全运维、监测分析、应急演练、应急保障、信息安全监督检查、测试评估等)纳入年度预算。

5.3.1.2 检查方法：文档查阅，查阅电力企业年度预算计划是否包括信息安全建设费用和运行维护费用。

5.3.2 安全建设经费投入(G)

5.3.2.1 检查项包括：电力企业用于信息安全建设的经费占整个信息系统建设总投入的比率。

5.3.2.2 检查方法：文档查阅，查阅并计算信息安全建设经费以及占年度信息化建设总投入的比率。

5.3.3 安全运维经费投入(G)

5.3.3.1 检查项包括：电力企业用于信息安全运行维护的经费占整个信息系统运行维护总投入的比率。

5.3.3.2 检查方法：文档查阅，查阅并计算信息安全运维经费以及占整个信息系统运行维护总投入的比率。

5.4 人员安全管理

5.4.1 安全培训与考核(G)

5.4.1.1 检查项包括：电力企业信息安全从业、信息系统设计、建设、运维等相关各类人员是否经培训考核合格后上岗，是否定期接受相应的政策规划和专业技术培训。

5.4.1.2 检查方法如下：

a) 人员访谈，询问电力企业信息安全从业、信息系统设计、建设、运维等相关各类人员是否经培训合格后上岗，是否定期接受相应的政策规划和专业技术培训；

b) 文档查阅，查阅参加安全培训的人员名单及成绩单。

5.4.2 保密协议签订(G)

5.4.2.1 检查项包括：电力企业是否与安全管理员、系统管理员、网络管理员等关键岗位的人员，电力监控系统(如有)相关设备及系统的开发单位和供应商签署保密协议。

5.4.2.2 检查方法如下：

a) 人员访谈，询问电力企业是否与安全管理员、系统管理员、网络管理员等关键岗位的人员，以及电力监控系统相关设备及系统的开发单位和供应商签署保密协议；

b) 文档查阅，查阅签署保密协议的人员名单及其岗位或单位。

5.4.3 人员审查(G)

5.4.3.1 检查项包括：电力企业是否对信息安全岗位人员和其他敏感岗位人员实施背景调查和人员审查。

5.4.3.2 检查方法如下：

a) 人员访谈，询问电力企业是否对信息安全岗位人员和其他敏感岗位人员实施身份、背景和资质审查；

b) 文档查阅，查阅电力企业对信息安全岗位人员和其他敏感岗位人员的身份、背景和资质进行审查的相关文档和记录。

5.4.4 岗位调整管控(G)

5.4.4.1 检查项包括：电力企业是否在信息安全岗位人员及其他敏感岗位人员离岗时执行权限回收和离岗承诺书签署。

5.4.4.2 检查方法如下：

a) 人员访谈，询问电力企业是否在信息安全岗位人员及其他敏感岗位人员离岗时执行权限回收和离岗承诺书签署；

b) 文档查阅，查阅信息安全岗位人员及其他敏感岗位人员的权限回收记录和离岗承诺书签署情况。

5.5 服务外包管控

5.5.1 外包服务协议(G)

5.5.1.1 检查项包括：电力企业与合约

5.5.1.2 检查方法：文档查阅，查阅外包服务协议中的信息安全管控和保密条款。

5.5.2 外部人员访问管理(G)

5.5.2.1 检查项包括：电力企业是否对外部人员访问机房等受控区域采取书面审批、人员陪同、进出登记等管控措施。

5.5.2.2 检查方法如下：

a) 人员访谈，询问电力企业是否对外部人员访问机房管控采取书面审批、人员陪同、进出登记等管控措施；

b) 文档查阅，查阅外部人员访问管理制度和访问登记记录。

5.5.3 远程服务管控(G)

5.5.3.1 检查项包括：电力企业是否采取远程服务，如采取审批、访问控制、在线监测、日志审计等管控措施。

5.5.3.2 检查方法如下：

a) 人员访谈，询问对远程服务访问采取的管控措施；

b) 文档查阅，查阅远程服务管控制度及远程服务管控的相关审计告警。

5.5.4 现场开发管控(G)

5.5.4.1 检查项包括：电力企业是否采取技术措施实现开发测试环境与实际生产运行环境物理分离，并对开发人员的活动范围和行为实施管控。

5.5.4.2 检查方法如下：

a) 人员访谈，询问是否将开发测试环境与实际生产运行环境物理分离；

b) 文档查阅，查阅开发人员的活动范围和行为管控策略。

5.6 关键信息资产管控

5.6.1 资产管理(G)

5.6.1.1 检查项包括：电力企业是否识别所有与信息系统相关的资产并编制了准确的资产清单，是否对每项资产明确管理责任人及其职责。

5.6.1.2 检查方法：文档查阅，查阅资产清单，检查是否识别所有与信息系统相关的资产，是否对每项资产明确管理责任人及其职责。

5.6.2 资产维修报废管理(G)

5.6.2.1 检查项包括：电力企业是否在系统、设备维修或报废时，选取了可信服务机构并对数据采取了备份、清除等有效保护措施。

5.6.2.2 检查方法：文档查阅，查阅系统、设备维修或报废管理制度和维修或报废记录。

5.7 信息系统建设安全管理

5.7.1 监督与审核(P)

5.7.1.1 检查项包括：

a) 电力调度机构、发电厂、变电站等运行单位的电力监控系统安全防护的技术监督单位对电力监控系统安全防护实施技术监督；

b) 电力调度机构、发电厂、变电站等运行单位的电力监控系统安全防护实施方案是否经本企业的上级专业管理部门和信息安全管理部门以及相应电力调度机构的审核，方案实施完成后是否由上述机构验收；

c) 接入电力调度数据网络的设备和应用系统，其接入技术方案和安全防护措施是否经直接负责的电力调度机构同意。

5.7.1.2 检查方法如下：

a) 人员访谈，访谈实施技术监督、审核、验收管理相关工作的流程；

b) 文档查阅，查阅审核、验收意见及相关材料。

5.7.2 上线安全测评(G)

5.7.2.1 检查项包括：电力企业信息系统是否在上线前通过信息安全测评。

5.7.2.2 检查方法：文档查阅，查阅全部信息系统列表，查阅并统计已通过信息安全测评的系统测评报告。

5.7.3 等级保护建设(G)

5.7.3.1 检查项包括：电力企业信息系统是否按要求开展信息安全等级保护建设。

5.7.3.2 检查方法：文档查阅，查阅全部信息系统列表，查阅已按要求开展信息安全等级保护建设的信息系统相关文档。

5.7.4 等级测评开展情况(G)

5.7.4.1 检查项包括：

a) 电力企业信息系统是否按要求开展等级测评；

b) 电力监控系统信息安全[illegible]

5.7.4.2 检查方法如下：

a) 人员访谈，询问电力企业信息系统开展等级测评的情况，其中电力监控系统信息安全等级测评工作是否与电力监控系统安全防护评估工作同步进行；

b) 文档查阅，查阅全部信息系统列表，查阅并统计已开展信息系统安全等级测评的系统数量，并查阅等级测评报告及电力监控系统安全防护评估报告。

5.7.5 风险评估(G)

5.7.5.1 检查项包括：电力企业信息系统是否按要求开展信息安全风险评估并完成信息安全隐患整改，电力监控系统(如有)安全防护评估是否按照行业要求开展；

5.7.5.2 检查方法如下：

a) 人员访谈，询问电力企业信息系统是否按要求开展信息安全风险评估并完成信息安全隐患整改，电力监控系统(如有)安全防护评估是否按照行业要求开展；

b) 文档查阅，查阅电力企业信息系统安全风险评估报告、电力监控系统(如有)安全防护评估报告、整改建设方案。

5.7.6 产品采购和使用(G)

5.7.6.1 检查项包括：

a) 电力企业安全产品和密码产品的采购及使用是否符合国家有关规定；

b) 电力监控系统在设备选型及配置时，是否禁止选用经国家相关管理部门检测认定存在漏洞和风险的系统及设备；

c) 对于已经投入运行的系统及设备，是否按照相关要求及时进行升级改造，并加强相关系统及设备的运行管理和安全防护；

d) 生产控制大区中除安全接入区外，是否禁止选用具有无线通信功能的设备。

5.7.6.2 检查方法如下：

a) 人员访谈，访谈相关人员是否了解相关制度，是否存在不执行相关制度的特殊情况；

b) 文档查阅，查阅电力企业相关管理制度和资产清单等，检查其采购及使用是否符合国家有关规定；

c) 配置核查，核查在运系统及设备是否符合国家及行业相关要求，是否已按相关要求进行整改，并加强相关系统及设备的运行管理和安全防护。

5.7.7 核心产品专项测试

5.7.7.1 检查项包括：电力企业应用的信息安全产品、系统基础软件及关键应用软件、工业控制装置等在采购前是否经过了安全性测试。

5.7.7.2 检查方法：文档查阅，查阅电力企业应用的信息安全产品、系统基础软件及关键应用软件、工业控制装置等的安全性测试报告。

5.7.8 安全产品安全可靠(G)

5.7.8.1 检查项包括：电力企业安全保护级别为3级及以上的信息系统所采用信息安全产品安全可靠程度是否符合国家及行业相关文件要求。

5.7.8.2 检查方法：文档查阅，查阅电力企业信息安全产品清单。

5.8 信息系统运行安全管理

5.8.1 日常维护(G)

5.8.1.1 检查项包括：电力企业是否按照制定的规章制度、运维流程、操作规程等执行信息系统日常维

护并有详尽记录。

5.8.1.2 检查方法：文档查阅，查阅电力企业是否按照制定的规章制度、运维流程、操作规程等执行信息系统日常维护并有详尽记录。

5.8.2 安全审计(G)

5.8.2.1 检查项包括：电力企业是否对网络运行日志、操作系统日志、数据库访问日志、业务应用系统运行日志、安全设备和系统运行日志等进行集中收集、定期分析。

5.8.2.2 检查方法如下：

a) 文档查阅，查阅是否具备集中日志收集及定期分析报告；

b) 配置核查，检查电力企业对网络运行日志、操作系统日志、数据库访问日志、业务应用系统运行日志、安全设备和系统运行日志等进行集中收集的系统配置。

5.8.3 补丁管理(G)

5.8.3.1 检查项包括：电力企业是否按照补丁管理制度制定补丁升级策略，是否针对关键业务系统建立补丁升级测试环境或建立获取已测试补丁的有效渠道。

5.8.3.2 检查方法如下：

a) 文档查阅，查阅是否具备补丁管理制度，是否明确补丁升级策略，查阅是否具备补丁升级记录；

b) 配置核查，检查是否对关键业务系统建立补丁升级测试环境或建立获取已测试补丁的有效渠道；

c) 安全测试，在确保应用系统安全的前提下，使用扫描工具进行检查，查看电力企业是否针对关键业务系统进行补丁升级更新操作。

5.8.4 安全监测(M)

5.8.4.1 检查项包括：电力企业是否建立安全监测系统对互联网出口、面向互联网服务系统、重要信息系统及终端的安全运行情况等进行实时监测。

5.8.4.2 检查方法如下：

a) 文档查阅，查阅是否描述了安全监测系统的监测对象范围和监测内容，查阅是否具备安全监测报告；

b) 配置核查，检查安全监测系统的监测对象范围和监测内容。

5.9 应急管理

5.9.1 信息通报(C)

5.9.1.1 检查项包括：电力企业是否建立网络与信息安全信息通报机制，按要求向电力监管机构通报网络和信息系统安全状况。

5.9.1.2 检查方法：文档查阅，查阅是否通过制度建立网络与信息安全信息通报机制，是否明确需要通报的内容和范围，是否指定负责人员。

5.9.2 联合应急防护机制(P)

5.9.2.1 检查项包括：电力企业是否建立网络与信息安全联合防护和应急机制，是否与电力调度机构负责统一指挥调度范围内的电力监控系统安全应急处理。

5.9.2.2 检查方法：文档查阅，查阅电力企业网络与信息安全联合防护和应急机制。

5.9.3 应急预案制定(G)

5.9.3.1 检查项包括：[illegible]全及专项应急[illegible]

5.9.3.2 检查方法如下：

a) 人员访谈，询问是否制定了本单位网络与信息安全及专项应急预案及了解相关条款；

b) 文档查阅，查阅是否按照电力行业网络与信息安全应急预案，制定本单位网络与信息安全应急预案，是否明确启动应急预案的条件、应急处理流程、系统恢复流程、事后教育培训和定期审核更新等方面的内容。

5.9.4 应急演练(G)

5.9.4.1 检查项包括：电力企业是否实施年度应急演练，是否有演练脚本和演练实施记录文档。

5.9.4.2 检查方法：文档查阅，查阅是否制定应急演练制度，是否实施年度应急演练，是否有演练脚本和演练实施的记录文档。

5.9.5 应急资源配备(G)

5.9.5.1 检查项包括：电力企业是否根据信息安全工作需求，配置应急支援技术队伍并配置备机备件。

5.9.5.2 检查方法如下：

a) 人员访谈，询问是否具备应急支援技术队伍，是否具备应急备机备件并能正常工作；

b) 文档查阅，查阅应急支援技术队伍人员名单，查阅应急备机备件清单。

5.9.6 事件调查(G)

5.9.6.1 检查项包括：电力企业是否按照行业及本单位应急预案要求，配合或组织开展事件调查。

5.9.6.2 检查方法如下：

a) 人员访谈，询问电力企业是否曾配合或组织开展事件调查；

b) 文档查阅，查阅信息安全事件调查制度，查阅信息安全事件调查记录或报告是否记录引发安全事件的原因及事件调查过程。

5.10 安全分区防御体系

5.10.1 大区[illegible]隔(P)

5.10.1.1 检查项包括：

a) 电力企业是否按要求划分生产控制大区和管理信息大区；

b) 电力企业是否在生产控制大区与管理信息大区之间设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

5.10.1.2 检查方法如下：

a) 文档查阅，查阅电力企业网络拓扑结构图是否划分生产控制大区和管理信息大区，查阅单向隔离装置的检测报告或认证证书；

b) 配置核查，核查电力企业生产控制大区和管理信息大区的划分是否符合有关文件要求，并查验单向隔离装置是否配置有效。

5.10.2 生产控制大区内部逻辑隔离(P)

5.10.2.1 检查项包括：

a) 电力企业是否按要求在生产控制大区内部控制区与非控制区之间采用国密硬件防火墙，具有访问控制功能的设备或等效功能的设施进行逻辑隔离；

b) 生产控制大区内部各系统间是否采用 VLAN 和访问控制等安全措施限制系统间的直接互联。

5.10.2.2 检查方法如下：

a) 人员访谈，询问生产控制大区内部所采取的访问控制措施；

b) 文档查阅，查阅网络拓扑结构图是否在生产控制大区内部控制区与非控制区之间采用逻辑隔离产品，查阅逻辑隔离产品的检测报告或认证证书；

c) 配置核查，核查逻辑隔离产品配置及策略是否有效。

5.10.3 纵向认证(P)

5.10.3.1 检查项包括：电力企业是否按要求在生产控制大区与广域网的纵向交接处设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关。

5.10.3.2 检查方法如下：

a) 文档查阅，查阅网络拓扑结构图是否在生产控制大区与广域网的纵向交接处设置电力专用纵向加密认证装置或加密认证网关，查阅电力专用纵向加密认证装置或加密认证网关的检测报告或认证证书；

b) 配置核查，核查电力企业的纵向加密认证产品或加密认证网关产品配置及策略是否有效；

c) 安全测试，在确保应用系统的安全前提下，通过抓包工具捕获传输数据包，查看是否加密。

5.10.4 电力调度数字证书及安全标签使用(P)

5.10.4.1 检查项包括：

a) 电力企业是否依照电力调度管理体制建立基于公钥技术的分布式电力调度数字证书及安全标签，生产控制大区中的重要业务系统是否采用认证加密机制；

b) 电力调度机构是否指定专人负责管理本级调度数字证书系统。

5.10.4.2 检查方法如下：

a) 人员访谈，访谈是否建立基于公钥技术的分布式电力调度数字证书及安全标签，是否指定专人负责管理本级调度数字证书系统；

b) 文档查阅，查阅生产控制大区中的重要业务系统网络拓扑结构图中是否采取认证加密措施；

c) 配置核查，核查分布式电力调度数字证书及安全标签的配置是否合理，认证加密机制是否有效。

5.10.5 跨区连接管控(P)

5.10.5.1 检查项包括：电力企业是否禁止未通过电力专用横向单向隔离装置将生产控制大区和管理信息大区网络直接连接的情况。

5.10.5.2 检查方法如下：

a) 文档查阅，查阅网络拓扑结构图是否与实际网络相符，是否不存在未通过电力专用横向单向隔离装置将生产控制大区和管理信息大区网络直接连接的情况；

b) 配置核查，核查横向单向隔离装置的配置是否合理且有效；

c) 安全测试，利用相关命令语句等测试是否存在未通过电力专用横向单向隔离装置的大区间连通情况。

5.10.6 安全接入区

5.10.6.1 检查项包括：

a) 生产控制大区的业务系统在与其终端的纵向联接中是否使用无线通信网、电力企业其他数据网(非电力调度数据网)或者外部公用数据网的虚拟专用网络方式(VPN)等进行通信，采取加上所述方式进行通信的是否设立了安全接入区；

b) 安全接入区与生产控制大区中其他部分的联接处是否设置经国家指定部门检测认证的电力专用横向单向安全隔离装置且进行有效配置。

5.10.6.2 检查方法如下：

a) 人员访谈，访谈生产控制大区的业务系统是否存在需要通过非电力调度数据网与其终端通信的情况；如果有，是否已设立了安全接入区，并在安全接入区与生产控制大区中其他部分的联接处设置经国家指定部门检测认证的电力专用横向单向安全隔离装置；

b) 文档查阅，查阅网络拓扑结构图是否通过设置安全接入区实现与其终端的非电力调度数据网的通信连接；

c) 配置核查，核查电力企业是否在安全接入区与生产控制大区中其他部分的联接处设置经国家指定部门检测认证的电力专用横向单向安全隔离装置并进行有效配置。

5.10.7 敏感信息隔离(M)

5.10.7.1 检查项包括：电力企业是否通过独立的网络和终端处理敏感信息，与互联网之间有信息交换时边界防护强度强于逻辑隔离。

5.10.7.2 检查方法如下：

a) 文档查阅，查看网络拓扑结构图是否通过独立的网络和终端处理敏感信息，以及隔离装置的技术说明文档；

b) 配置核查，核查内部网络和外部网络信息通信交换的防护强度是否强于逻辑隔离。

5.11 网络安全防护

5.11.1 网络专用(P)

5.11.1.1 检查项包括：电力调度数据网是否在专用通道上使用独立的网络设备组网，是否在物理层面上实现与电力企业其他数据网及外部公用数据网的安全隔离。

5.11.1.2 检查方法如下：

a) 文档查阅，查阅电力调度数据网网络拓扑结构图是否使用独立的网络设备组网；

b) 配置核查，核查电力调度数据网是否在物理层面上实现与电力企业其他数据网及外部公用数据网的安全隔离。

5.11.2 生产控制大区防护(P)

5.11.2.1 检查项包括：电力企业是否在生产控制大区内部采取安全审计、恶意代码防范、入侵检测、非授权网络接入管控等技术措施实施安全防护。

5.11.2.2 检查方法如下：

a) 文档查阅，查阅网络拓扑结构图是否在生产控制大区内部采取安全防护措施；

b) 配置核查，检查生产控制大区网络边界的安全审计、入侵检测、非授权网络接入管控等防护设备配置情况。

5.11.3 管理信息大区防护(M)

5.11.3.1 检查项包括：电力企业是否在管理信息大区内部采取技术措施实施安全防护。

5.11.3.2 检查方

a) 文档查阅，查阅电力企业网络拓扑结构图是否在管理信息大区内部署恶意防护措施；

b) 配置核查，检查管理信息大区网络边界的入侵检测、ARP 防范、非授权网络接入管控、集中运维操作审计等安全监防护配置情况。

5.11.4 互联网出口统一管理(M)

5.11.4.1 检查项包括：电力企业管理信息大区的互联网出口是否统一管理。

5.11.4.2 检查方法：文档查阅，查阅网络拓扑结构图，电力企业管理信息大区的互联网出口是否统一管理。

5.11.5 互联网出口安全管控(M)

5.11.5.1 检查项包括：电力企业互联网出口是否采取访问控制、入侵防御、上网行为管理等必要的安全防护措施且针对第 2 级以上系统访问控制粒度达到端口级。

5.11.5.2 检查方法如下：

a) 文档查阅，查阅网络拓扑结构图中互联网出口的访问控制产品配置情况；

b) 配置核查，检查互联网出口是否采取访问控制、入侵防御、上网行为管理等必要安全防护措施且针对第 2 级以上系统访问控制粒度达到端口级。

5.11.6 无线网络安全应用(G)

5.11.6.1 检查项包括：电力企业应用无线网络承载业务的信息系统类型(管理类信息系统或生产控制类系统)，是否采取设置安全接入区、身份认证、完整性保护、机密性保护等必要的安全防护措施。

5.11.6.2 检查方法如下：

a) 人员访谈，询问应用无线网络承载业务的信息系统中采取了哪些安全防护措施；

b) 文档查阅，查阅网络拓扑结构图中，应用无线网络承载业务的信息系统采取的安全防护情况；

c) 配置核查，检查应用无线网络承载业务的信息系统中采取的安全防护措施。

5.11.7 移动式设备安全接入(G)

5.11.7.1 检查项包括：电力企业是否针对移动式设备接入采取了安全性检测、书面审批、统一接入管控、访问控制、在线监测、日志审计等必要的管控措施。

5.11.7.2 检查方法如下：

a) 人员访谈，询问对移动式设备接入采取哪些控制措施；

b) 文档查阅，查阅管理制度是否要求移动终端接入前采取安全性检测、书面审批、统一接入管控、访问控制、在线监测、日志审计等管控措施；

c) 配置核查，检查移动终端接入相关访问控制、日志审计记录。

5.12 主机和设备安全防护

5.12.1 补丁更新(G)

5.12.1.1 检查项包括：电力企业是否针对操作系统补丁更新制定了相关更新管理制度。

5.12.1.2 检查方法如下：

a) 文档查阅，查阅补丁更新管理制度，主机补丁更新频率；

b) 配置核查，检查主机操作系统和网络设备的补丁更新情况；

c) 安全测试，在确保不影响业务系统正常运行的情况下，检查主机操作系统和网络设备的补丁更新情况。

5.12.2 恶意代码防护(G)

5.12.2.1 检查项包括：电力企业是否按照恶意代码管理制度要求进行恶意代码检测和可更新恶意代码库的更新。

5.12.2.2 检查方法如下：

a) 文档查阅，查阅恶意代码防范管理制度和更新频率；

b) 配置核查，检查恶意代码检测程序和可更新恶意代码库的更新情况。

5.12.3 系统安全整改加固(G)

5.12.3.1 检查项包括：电力企业主机和设备中是否对等级保护测评、风险评估、信息安全检查等工作中发现的问题进行安全整改加固。

5.12.3.2 检查方法如下：

a) 文档查阅，查阅等级保护测评、风险评估、信息安全检查等工作的安全问题报告，查阅安全整改加固实施工作报告；

b) 配置核查，检查与验证电力企业对等级保护测评、风险评估、信息安全检查等工作中发现的问题进行安全整改加固的实施情况。

5.12.4 移动存储介质管理(G)

5.12.4.1 检查项包括：电力企业是否设置限制和管理移动存储介质使用的管理和技术措施，是否对移动存储介质的分发、注册、使用、存放、销毁实施管理，是否禁止移动存储介质在生产控制大区和管理信息大区的混用。

5.12.4.2 检查方法如下：

a) 文档查阅，查阅移动存储介质安全管理制度；

b) 安全测试，验证系统中是否具备移动存储介质管理技术措施。

5.12.5 办公终端管控(M)

5.12.5.1 检查项包括：电力企业办公终端是否实施安全管控(如病毒软件)。

5.12.5.2 检查方法如下：

a) 人员访谈，询问电力企业采取了何种终端安全管理措施；

b) 文档查阅，查阅电力企业的终端安全管理制度；

c) 配置核查，核查办公终端安全管控措施情况。

5.12.6 主机和设备账号口令管理(G)

5.12.6.1 检查项包括：电力企业主机和设备中口令设置是否符合口令管理制度要求。

5.12.6.2 检查方法如下：

a) 文档查阅，查阅主机和设备安全检测报告；

b) 配置核查，检查并统计符合口令管理要求制度要求的主机数量。

5.13 应用系统和数据安全防护

5.13.1 应用系统安全功能及配置(G)

5.13.1.1 检查项包括：电力企业应用系统是否在等级保护测评、风险评估、信息安全检查等工作中未发

现安全功能及配置方面存在严重问题。

5.13.1.2 检查方法如下：文档查阅，查阅应用系统安全检测报告，统计未发现安全功能及配置方面存在严重问题的系统数量。

5.13.2 面向互联网服务系统安全监控和攻击防御(M)

5.13.2.1 检查项包括：电力企业面向互联网服务的信息系统是否按要求采取安全监控和攻击防御等措施。

5.13.2.2 检查方法如下：

a) 文档查阅，查阅面向互联网服务的信息系统数量；

b) 配置核查，检查并统计面向互联网服务的信息系统中采取安全监控和攻击防御等措施的系统清单。

5.13.3 面向互联网服务系统周期测试(M)

5.13.3.1 检查项包括：电力企业面向互联网服务的系统是否按要求进行周期性信息安全测试。

5.13.3.2 检查方法：文档查阅，查阅面向互联网服务的信息系统清单，查阅面向互联网服务的信息系统检测报告，统计未发现安全功能及配置方面存在严重问题的系统数量。

5.13.4 应用系统账号口令管理(C)

5.13.4.1 检查项包括：电力企业应用系统中账号口令是否有口令管理制度的要求。

5.13.4.2 检查方法如下：

a) 文档查阅，查阅应用系统安全检测报告；

b) 配置核查，检查符合口令管理制度要求的应用系统清单；

c) 安全测试，在确保应用系统的安全前提下，使用暴力破解方式验证应用系统中账号是否有弱口令。

5.13.5 重要数据安全保护保护(C)

5.13.5.1 检查项包括：电力企业是否采用加密或其他有效措施实现对系统管理数据、鉴别信息和重要业务数据的完整性和机密性保护。

5.13.5.2 检查方法如下：

a) 文档查阅，查阅应用系统设计文档对于系统管理数据、鉴别信息和重要业务数据的完整性和机密性保护措施；

b) 配置核查，检查应用系统是否采用加密或其他有效措施实现对系统管理数据、鉴别信息和重要业务数据的完整性和机密性保护。

5.14 物理环境安全防护

5.14.1 检查项

检查是否通过电力企业的机房中是否按照等级保护要求落实物理安全防护。

5.14.2 检查方法

检查方法如下：

a) 文档查阅，查阅等级测评报告等并统计按照等级保护要求落实物理安全防护的机房；

b) 配置核查，实地查看电力企业机房的物理安全防护是否按照

5.15 业务连续性保护

5.15.1 硬件冗余(G)

5.15.1.1 检查项包括：电力企业是否提供重要信息系统网络设备、通信线路和数据处理系统的硬件冗余。

5.15.1.2 检查方法如下：

a) 文档查阅，查阅网络拓扑结构图是否标明了重要信息系统网络设备、通信线路和数据处理系统硬件冗余；

b) 配置核查，检查重要信息系统网络设备、通信线路和数据处理系统的硬件冗余情况。

5.15.2 系统和数据备份(G)

5.15.2.1 检查项包括：电力企业重要信息系统是否实施数据级和系统级备份，备份介质是否场外存放。

5.15.2.2 检查方法如下：

a) 人员访谈，询问重要信息系统数据备份的级别和备份的场所；

b) 配置核查，检查重要信息系统数据备份策略是否为数据级和系统级，备份介质存储的位置是否在本电力企业场所之外。

5.15.3 异地灾备(G)

5.15.3.1 检查项包括：电力企业是否提供异地数据备份功能，三级信息系统是否实现关键数据定时批量传送至备用场地，四级信息系统是否实现业务应用实时无缝切换。

5.15.3.2 检查方法如下：

a) 人员访谈，询问是否提供异地数据备份功能，是否具有正在运行的第三级和第四级信息系统；

b) 配置核查，检查异地数据备份功能的情况，检查三级信息系统是否实现关键数据定时批量传送至备用场地，四级信息系统是否实现业务应用实时无缝切换。

5.15.4 恢复测试(M)

5.15.4.1 检查项包括：电力企业是否按照恢复测试要求，定期实施恢复测试演练，并检查和测试备份介质的有效性。

5.15.4.2 检查方法：文档查阅，查阅是否制定恢复测试管理制度，是否定期对备份数据进行恢复测试演练，查阅备份恢复测试记录。

附　录　A
（资料性附录）
风险分析方法

A.1　定性分析

定性分析方法如下：

a）　判断安全问题发生的可能性，可能性的取值范围为高、中和低，见表 A.1。

表 A.1　安全问题发生的可能性取值

标识	定　　义
高	安全问题出现的频率较高（或≥1 次/月）；或在大多数情况下很有可能会发生；或可以证实会发生，或其实现条件较容易被攻击者获得
中	安全问题出现的频率中等（或>1 次/半年）；或在某种情况下可能会发生，或被证实曾经发生过，或其实现条件难以被攻击者获得
低	安全问题出现的频率较小；或一般不太可能发生；或没有被证实发生过，或其实现条件很难被攻击者获得

b）　判断安全问题被威胁利用后，对信息系统安全造成的影响程度，影响程度取值范围为高、中和低，见表 A.2。

表 A.2　安全问题对信息系统安全造成的影响程度取值

标识	定　　义
高	如果安全问题出现，将对信息系统造成重大损害
中	如果安全问题出现，将对信息系统造成一般损害
低	如果安全问题出现，将对信息系统造成较小或轻微损害

c）　综合 a）和 b）的结果对信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低，见表 A.3。

表 A.3　信息系统面临的安全风险取值

标识	描　　述
高	一旦发生将产生较为严重的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
中	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
低	一旦发生造成的影响程度较低甚至几乎不存在，一般仅限于组织内部，通过较为简单的手段很快能解决

d）　雷达图展示系统安全问题的风险分布及各类检查项的安全问题分布，如图 A.1、图 A.2 所示。

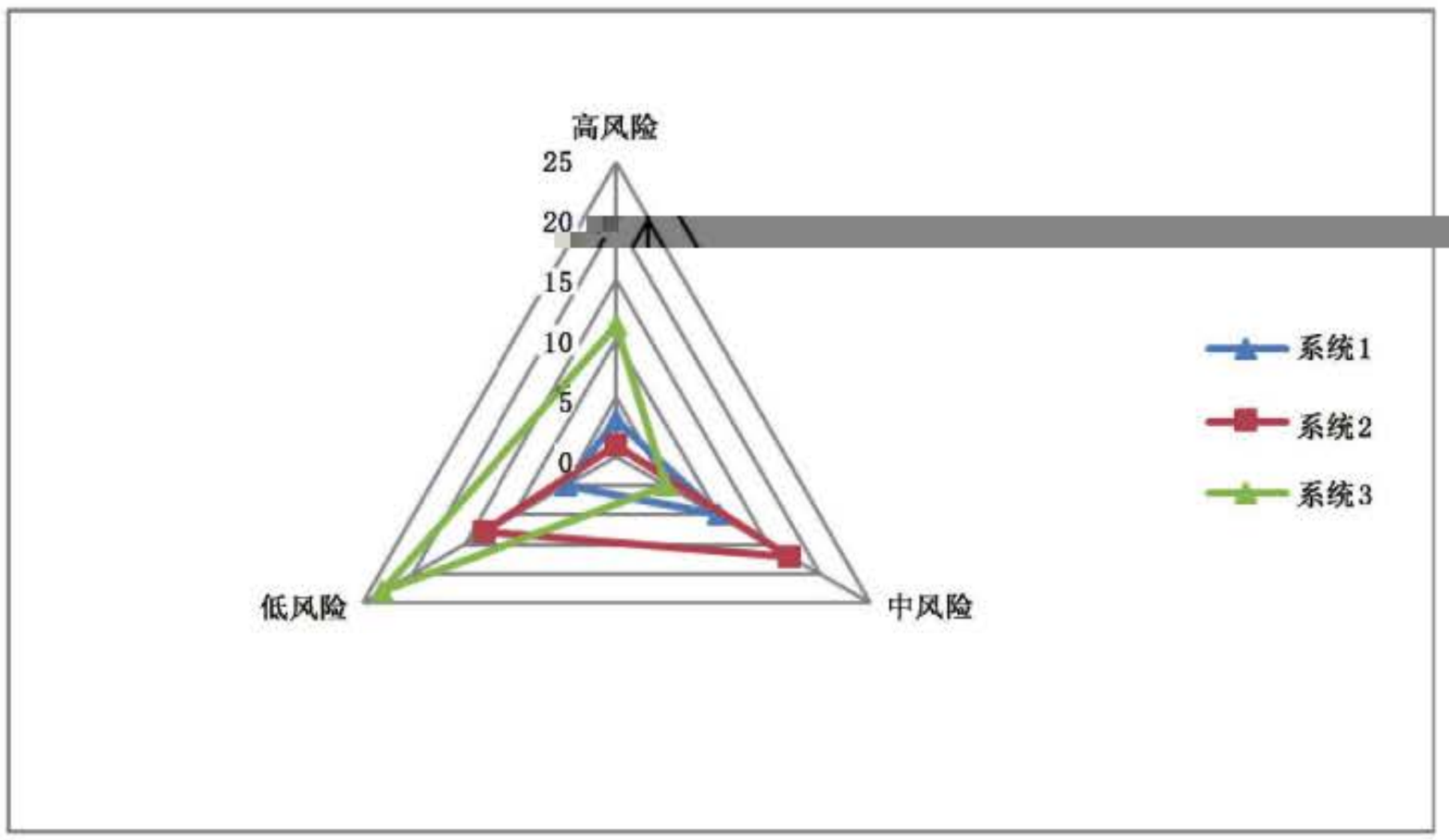

图 A.1　安全问题风险分布图

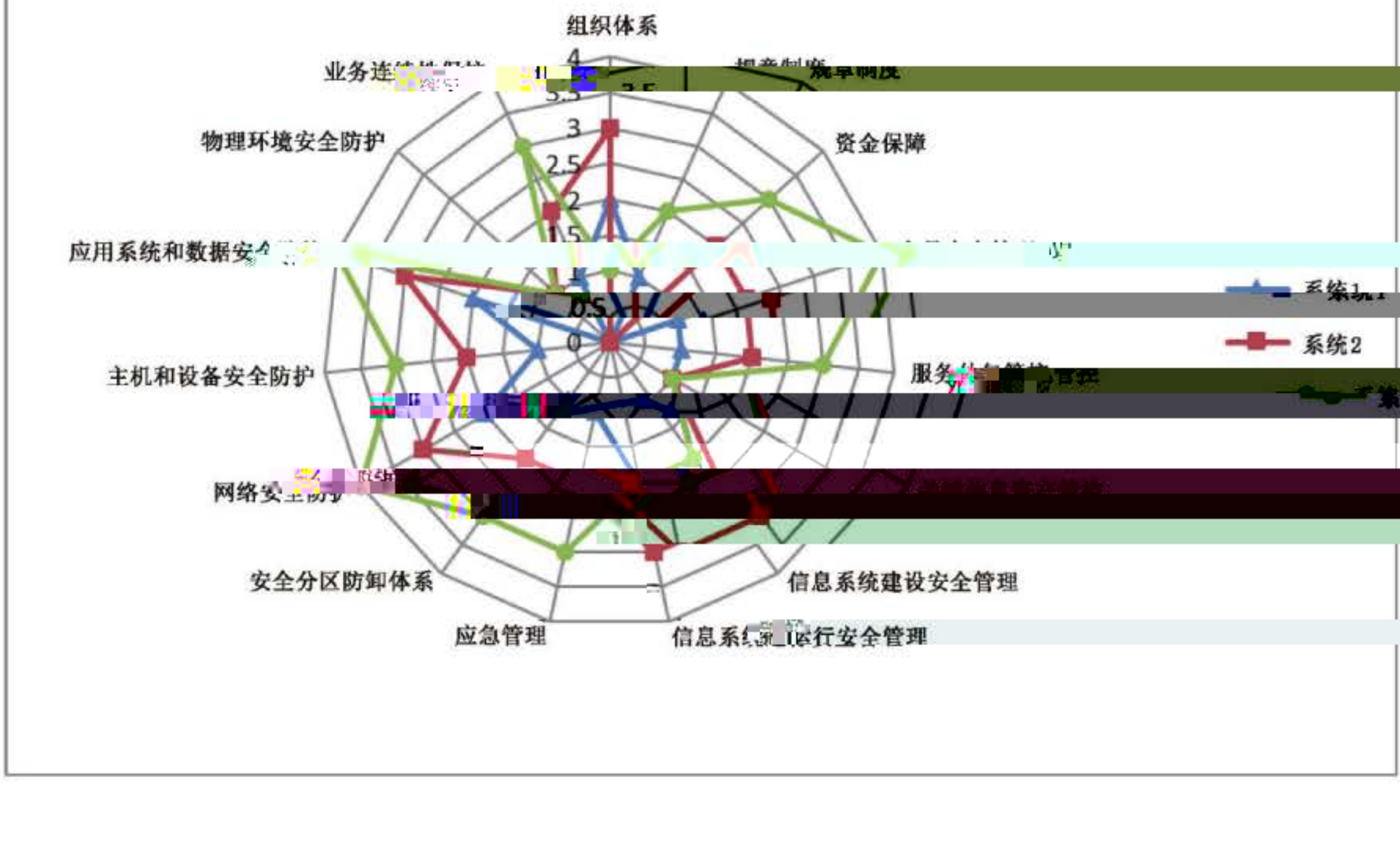

图 A.2　检查项问题分布图

A.2　定量分析

根据电力企业信息安全工作实际情况是否符合检查项描述，为检查项赋予权重值（V_{ij}），根据检查结果判定赋予量化值（P_{ij}），见表 A.4，安全检查结果量化（ISL）由式（A.1）计算求得：

表 A.4（续）

检查类	检查项	[illegible]	[illegible]
应急管[illegible]	应急预案制定	1	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	应急演练	1	符[illegible]合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	应急资[illegible]	[illegible]	符合：$P_{ij}=1$ [illegible] 不符合：$P_{ij}=0$
	事件调查	1	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
安全分区防御体系	大区间隔离	2	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	生产控制大区内部逻辑隔离	2	符[illegible]$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	纵向认证	2	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	电力调度数字证书使用	2	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	跨区连接管控	1	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	安全接入区	1	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	敏感信息隔离	2	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
网络安全防护	网络专用	2	符合：$P_{ij}=1$ 部分符合：$P_{ij}=0.5$ 不符合：$P_{ij}=0$
	生产控制大区防护	2	符合：$P_{ij}=1$ 部分符[illegible] 不符合：$P_{ij}=0$

参 考 文 献

[1] 信息安全等级保护[illegible]法(公通字[2007]43号)
[2] 关于加强工业控制系统信息安全管理的通知(工信部协[2011]451号)
[3] 电力行业信[illegible]息[2012]62号)
[4] 电力监控系统安全防护规定(国家发改委令2014年第14号)
[5] 电力行业网络与信息安全管理办法(国能安全[2014]317号)
[6] 电力行业信息安全等级保护管理办法(国能安全[2014]318号)

中华人民共和国
国家标准
电力信息系统安全检查规范
GB/T 36047—2018
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
书号:155066·1-5982

版权专有 侵权必究

GB/T 36047-2018