ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/

团 体 标 准

T/XXX XXXX—XXXX

电力系统数据异常处置规范

Specification for Handling Abnormal Data of Power System

（征求意见稿）

（本草案完成时间：20260602）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

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》的规定起草。

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专利的责任。

本文件由广东电网有限责任公司东莞供电局提出。

本文件由珠海市自动化学会归口。

本文主要起草单位：广东电网有限责任公司东莞供电局、珠海澳大科技研究院、顺德职业技术大学。

本文件主要起草人：李诗美、罗金满、邹浙湘、汪杰、刘丰瑞、刘景荣、赵善龙、钟志明、梁浩波、梅傲琪、封祐钧、刘丽媛、余凌、张锐、叶思琪、高承芳、李晓霞、王湘女、李祺威、冷颖雄、陈浩玮。

电力系统数据异常处置规范

1 范围

本文件规定了电力系统在数据异常及网络攻击情况下的处置应用模型、处置方法、安全策略等。

本文件适用于城市综合能源系统（包括电力调度控制系统、新能源综合能源管理系统、电力物联网等）数字化系统的数据异常监测、网络安全监测与风险评估。

本文件依托东莞综合能源系统项目实践经验编制，内容适配珠海地区综合能源系统建设场景，可为相关单位开展数据异常监测、网络安全防护与风险评估工作提供技术参考。

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 18336-2015 信息技术 安全技术 信息技术安全评估准则

GB/T 25069-2022 信息安全技术 网络安全等级保护基本要求

GB/T 36572-2018 电力监控系统网络安全防护技术要求

DL/T 1455-2015 电力系统控制类软件安全性测评技术要求

DL/T 1970-2019 电力系统数据质量评价规范

DL/T 2277-2021 电力监控系统网络安全风险评估规范

3 术语和定义

GB/T 36572界定的以及下列术语和定义适用于本文件。

3.1

数据异常 Abnormal Data

电力系统运行过程中采集的数据偏离正常范围或模式的现象。数据异常可能由传感器故障、通信误差、设备故障以及恶意数据篡改等原因引起，通常表现为量测值超出阈值范围、不符合潮流平衡关系或与历史趋势明显不符。

3.2

信息网络攻击 Information Network Attack

针对电力系统信息通信网络的恶意入侵、破坏或未授权访问行为， c包括病毒木马感染、拒绝服务攻击、假数据注入、未经授权的控制指令插入等。网络攻击可能导致电力监控系统数据失真、设备失控或服务中断，从而危害电力系统的安全稳定运行。

3.3

风险评估 Risk Assessment

对电力系统在数据异常和网络攻击情形下面临的安全风险进行定性与定量分析的过程。风险评估综合考虑异常或攻击发生的可能性以及造成的影响程度，计算得到风险等级或风险值，用于指导安全防护决策和应急响应措施。

3.4

入侵检测系统 IDS, Intrusion Detection System

用于监视电力系统网络流量和主机活动，检测可疑行为或已知攻击特征的安全防护系统。当发现疑似网络攻击或违规操作时，入侵检测系统产生报警并记录相关信息，供安全管理人员分析处理。电力监控系统通常部署网络入侵检测和主机入侵检测组件，实现对网络层和主机层的全面监测。

3.5

潮流数据 Power Flow Data

电力系统中各节点和线路的电压、电流、有功功率、无功功率等运行状态参数集合，用于反映系统在给定时刻的稳态运行状态。潮流数据是系统运行分析、调度决策、电压控制和网络安全评估的基础，通常由能量管理系统（EMS）或调度自动化系统（DAS）实时采集并处理。潮流数据包括但不限于节点电压幅值与相角、支路功率流向、变压器分接头状态、电网频率等关键参数。

4 应用模型

4.1 概述

面向城市综合能源系统的网络攻击监测与安全防护系统，是针对城市能源系统多设备协同、高自动化运行特征设计的安全管控工具。从界面设计可见，系统核心定位是融合能源物理运行监控与网络空间安全防护，通过实时展示威胁指数、攻击趋势、设备异常等关键信息，辅助工作人员从 “单一运行监视” 转向 “全域安全态势感知”。

系统界面涵盖风险评估、攻击路径可视化、告警管理、策略配置、平台运维等核心功能，可实现对城市能源系统中变电站、服务器、网络设备等关键资产的全生命周期安全管控，为东莞供电等城市能源运营主体提供 “检测 - 评估 - 响应 - 防护” 的闭环安全保障，是城市能源数字化运维的核心支撑平台。

4.2 结构

本系统遵循 “感知-分析-评估-防御” 四层逻辑架构，结合界面呈现的功能模块（安全策略、平台管理、风险评估、韧性评估等），整体由主界面监控平台、数据采集与处理层、智能检测与分析层、安全防护与响应层构成，各层级及核心模块功能如图1所示。：

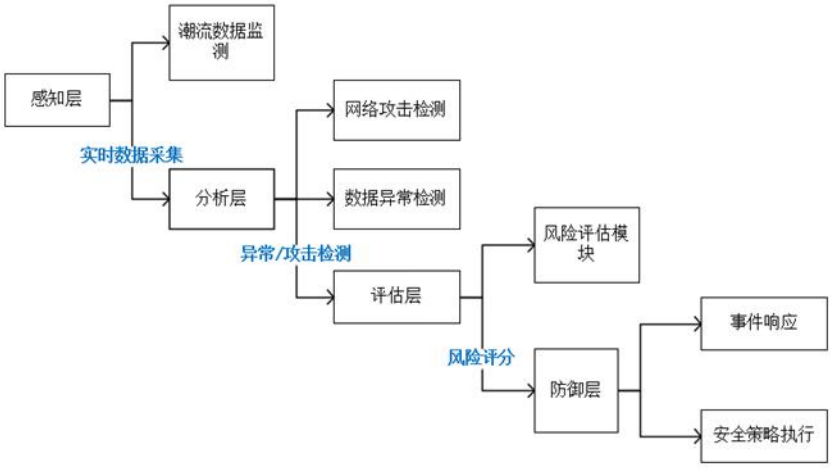

图 1 监控与安全防护系统整体架构图

潮流数据监测模块（Power Flow Monitoring Module）：实时采集城市综合能源系统中各类设备（含变电站、配电线路、储能装置、充电桩等）的运行数据，构建实时潮流分析图，实现功率流向、电压等级、电流分布的可视化展示和趋势分析。

a) 数据异常检测模块（Data Anomaly Detection Module）：基于规则与算法双重机制，识别因设备故障、通信异常或外部攻击引发的非正常运行数据，提供异常报警、影响范围评估与历史追踪功能。

b) 网络攻击检测模块（Network Attack Detection Module）：采用流量分析与特征匹配相结合的入侵检测技术（IDS），对 OT 与 IT 网络流量进行分区监测，能识别常见攻击如扫描、拒绝服务、命令注入等，对关键设备和通信链路建立动态风险模型。

c) 风险评估与报告模块（Risk Assessment and Reporting Module）：通过对潮流状态、数据异常与安全威胁事件的融合分析，建立风险等级评分体系，生成周期性风险评估报告，并对重点区域提出加固建议或应急处置预案。

d) 可视化拓扑展示平台（Topology Visualization Platform）：以城市典型 14 节点系统为示意，拓扑中心显示各节点连接与状态，四周分别集成“电压、电流实时曲线”“异常/攻击告警列表”“风险评分指标面板”，可交互、可缩放，辅助快速研判态势。

各模块通过企业服务总线或消息中间件进行通信，实现数据和结果的实时交互与共享。例如，网络攻击检测模块发现异常后可将信息发送给风险评估模块以更新风险等级，潮流监测模块获取异常检测模块标记的异常数据可在界面上高亮显示。这样，各功能模块有机协同，提升系统整体监测和防护能力。

4.3 应用

面向城市综合能源系统网络攻击监测与安全防护系统的模型应用主要包括：

a) 城市能源运营中心：实现市级综合能源管理的统一监控和安全防护，适配包括配电网、微电网、新能源、电动汽车充电网络等异构系统。

b) 变电站与能源枢纽站：用于监控站控层设备运行与信息网络访问行为，提前发现潜在风险，规避操作错误与信息篡改风险。

c) 调度控制中心：支持高级态势感知决策，提升调度员对潮流异常与网络攻击事件的综合识别与响应能力。

d) 科研及运维单位：作为城市能源系统智能运维和安全分析的数据支撑平台，支撑后续故障推演、策略优化与安全演练。

5 处置方法

5.1 数据异常

5.1.1 概述

数据异常检测主要基于电力系统分析理论与数据驱动算法相结合，包括利用状态估计和潮流校核的方法识别物理不一致数据，以及采用统计学习方法检测异常模式。网络攻击检测主要采用入侵检测技术和大数据分析，对网络流量、主机日志进行特征匹配和异常行为分析。风险评估方法则将检测结果与电网运行模型相结合，量化安全风险。通过以上方法的综合运用，可实现对电网运行异常和网络安全事件的及时、准确检出。

5.1.2 方法

数据异常检测以电力系统稳态分析为基础，结合历史数据统计特征和机器学习模型，实现对异常工况的识别。常用方法如图2所示。

a) 状态估计残差分析：基于能量管理系统(EMS)的状态估计模型计算各量测值的估计值，与实际采集值进行比较。如果残差超过设定阈值，则判定相应量测可能存在异常。状态估计还可用于检测拓扑错误和量测互换错误，是经典的数据异常检测手段之一。

b) 规则校验与阈值判别：预先设定各监测参数的物理合理范围和越限阈值，对实时数据进行规则校验。例如电压偏差超过±5%额定值、频率偏离 50Hz 超过 0.2Hz 等即判定为异常。此类方法简单直接，适用于已知范围的异常检测。

c) 时间序列分析与预测：运用 ARIMA 模型、LSTM 神经网络等对关键量测数据进行短期预测，将预测值与实际值比较以发现异常偏差。若实际值偏离预测带来的置信区间，则认为发生异常。这种方法利用历史模式，提高了检测对渐变型异常的敏感性。

d) 多元相关分析：利用电力系统潮流方程等关联关系，对多点测量值进行整体一致性校验。例如变压器两侧有功之差应接近损耗、发电出力与总负荷及损耗应平衡等。若关联关系不成立，说明可能存在数据错误或异常事件。

通过以上多种方法的配合，数据异常检测模块能够对各类异常情况（如传感器漂移、采样误差、设备故障引起的数据异常，以及潜在的虚假数据注入攻击等）进行有效识别。检测到异常后，系统应记录异常数据的时间、地点和具体表现，并通知相关人员核查。必要时，系统可过滤掉明显异常的数据以避免其干扰后续控制决策。

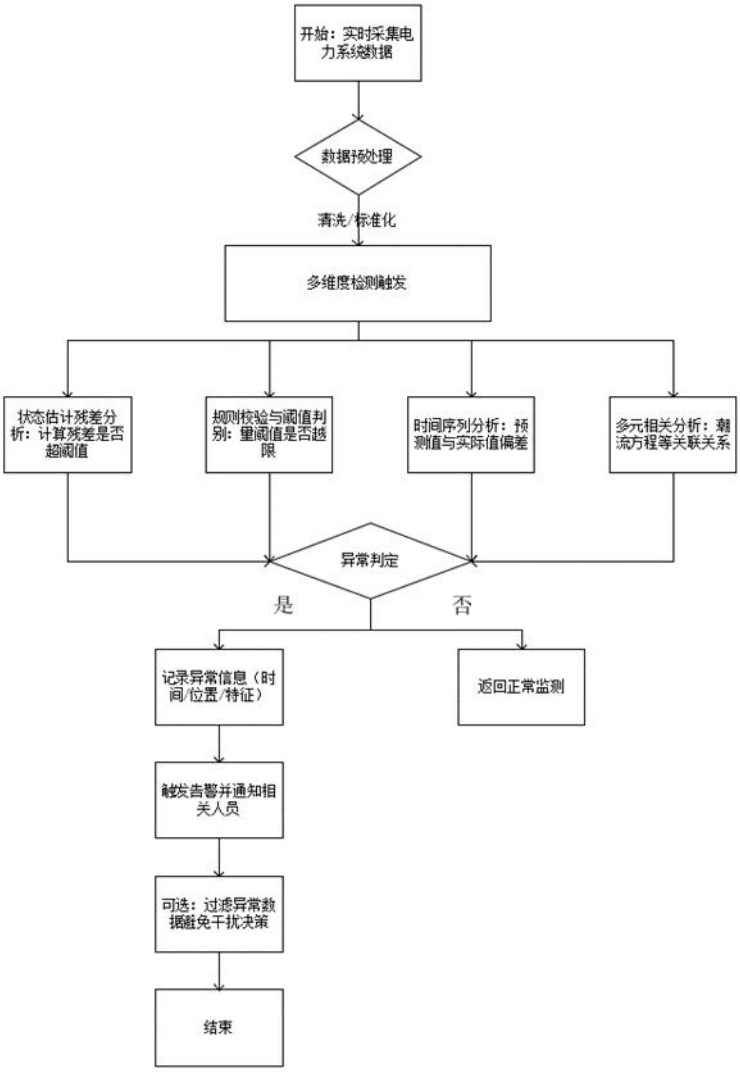

图 2　异常数据检测流程图

5.2　网络攻击

5.2.1　概述

网络攻击检测主要依托于入侵检测系统和安全监测平台，对网络通信数据和主机行为日志进行实时分析，以发现各类潜在的攻击活动。

5.2.2　方法

网络攻击检测模块应当7×24小时不间断运行。当判定发生网络攻击事件时，系统应记录事件详情，包括时间、涉及IP地址或设备、攻击类型特征等，并将警报推送给值班人员和安全管理系统。对于严重的攻击（如影响控制指令的假数据注入、针对调度主站的拒绝服务攻击等），系统在报警同时可执行预定义的紧急处置措施（见6.3），以最大程度减小攻击危害。

网络攻击检测以电力系统稳态分析为基础，结合历史数据统计特征和机器学习模型，实现对异常工况的识别：

a)　特征匹配检测：入侵检测系统内置已知攻击特征库（特征可以是恶意报文的字节模式、病毒木马的文件哈希、异常行为的序列等）。当监测到的网络流量或主机事件与特征库中的已知

攻击模式相匹配时，立即触发警报。例如检测到典型的 DDoS 攻击流量模式、蠕虫病毒传播签名或非法端口扫描特征等。

b) 异常行为分析：通过建立正常网络通信和主机活动的基线模型，检测偏离正常模式的异常行为。例如，监测控制网络中出现非常规的通信对话、数据流量在非常时间猛增、或控制指令通信频率异常等，都可能表明受到攻击。再如，关键服务器上的进程启停、账户权限变更等操作若与正常运维时段不符，则怀疑遭受入侵。

c) 流量和包内容深度检测：采用深度包检测（DPI）技术，对网络报文内容进行检查，识别隐藏于常规协议中的攻击载荷。结合电力应用协议规约（如 IEC 104、Modbus、DNP3 等）的解码规则，判断是否有畸形报文、越权命令或恶意负载混入正常通信。

d) 大数据关联分析：汇总来自不同区域、不同安全设备的日志，利用安全信息事件管理平台(SIEM)进行关联分析。例如，将变电站端安全网关日志与主站调度中心防火墙日志关联，可发现分散的可疑事件其实属于同一攻击链条，由此检测出更隐蔽的高级持续性威胁(APT)。

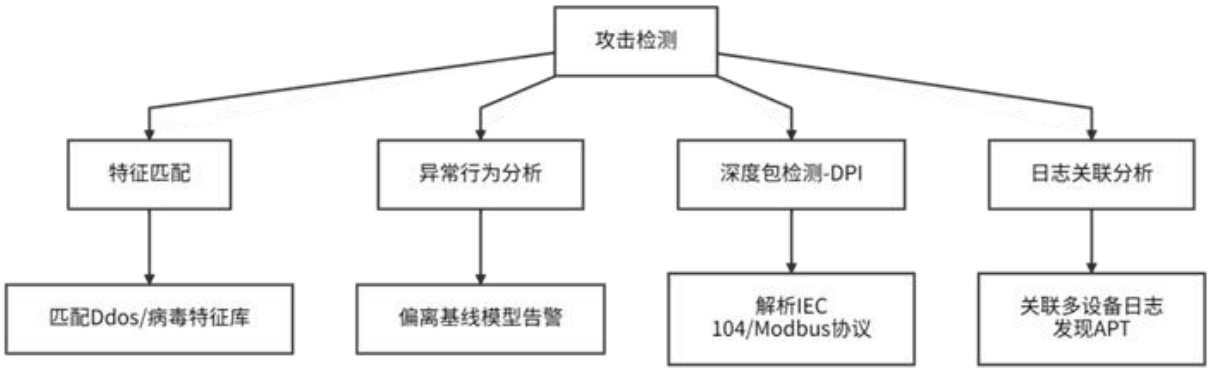

图 3　攻击检测示意图

5.3　风险评估

5.3.1　概述

将5.1、5.2数据异常和网络攻击检测的结果结合电力系统运行的重要性和脆弱性信息，给出定量的风险指标。其基本步骤包括：

a) 风险因子识别：根据电力系统运行结构，确定关键风险因子，例如重要变电站、输电断面过载风险、通信链路可靠性等。针对每个风险因子，收集其相关的监测数据和安全事件记录。

b) 风险度量模型：风险评分模型，将监测指标与风险等级对应。常用方法包括模糊综合评判和加权求和模型等，确保评分既反映事件频度又体现设备重要程度。单个风险因子的综合风险值（R）计算公式如下：

$$R = \sum_{i=1}^{n} (W_i \times S_i) \quad \cdots\cdots (1)$$

式中：

R：风险值（0-100 分，分值越高风险越高）；

W_i：第i项监测指标的权重（0-1，界面可配置，如控制中心 “脆弱评分” 权重 0.3）；

S_i：第i项监测指标的得分（0-100 分，直接取自界面数据，如脆弱点列表中“南部区域控制中心 #C02” 评分 89）；

n：该风险因子对应的监测指标数量。

c) 阈值划分等级：将计算得到的风险评分与预设阈值比较，划分风险等级（低、中、高、严重等）。阈值设定可依据历史统计和专家经验，例如风险评分 0-59 为低风险、60-79 为中等风险、80 以上为高风险。系统应支持对阈值和分级标准的调整，以符合不同单位安全管理要求。

d) 生成风险评估报告：系统定期（如每日或每周）自动生成风险评估报告，内容包括当前各监测对象的风险等级列表、与前期相比的变化趋势、主要的异常和攻击事件概述，以及相应的建议措施。报告格式应规范统一，便于归档和上报。

表 1　风险等级与界面联动表

风险评分区间（R）	风险等级	界面视觉标识	关联界面模块	处置要求
0-59	低风险	拓扑节点绿色、告警级别 “次要”（灰色）	常规监控列表	纳入日常巡检，每月复查数据趋势
60-79	中风险	拓扑节点黄色、告警级别 “警告”（黄色）	中风险项列表、脆弱点监控区	3个工作日内排查原因
80-94	高风险	拓扑节点橙色、告警级别 “重要”（橙色）	高优先级风险项列表、攻击事件详情	24小时内启动处置（如将攻击 IP 加入黑名单）
95-100	严重风险	拓扑节点红色、告警级别 “紧急”（红色）	紧急告警弹窗、高风险项置顶	立即停机排查，启动数据恢复

5.3.2　风险评估

风险评估方法如图4所示。当风险指标升高时，相关人员应引起重视并调查原因，针对高风险项及时采取整改措施，形成“检测-评估-响应”的闭环安全管理流程。

6　安全策略

6.1　概述

安全策略涵盖事前预防、事中响应和事后恢复三个阶段，旨在构建纵深防御体系，将异常和攻击造成的影响降至最低。电力监控系统的安全防护应遵循“安全分区、网络专用、横向隔离、纵向认证”等行业原则，结合实时监测手段形成完善的防御闭环。以下从防御策略、事件响应、持续运维三个方面阐述具体要求。

6.2　防御策略

电力系统运行单位应建立完善的网络与信息安全防御体系，提前部署各项防护措施：

a) 网络分区隔离(Network Segmentation and Isolation)：按照生产控制区和管理信息区进行网络分区，并根据安全域重要性进行纵深防护。生产控制大区内部划分控制区（安全区 I）和非控制区（安全区 II），不同区之间采用防火墙、安全隔离装置等措施实现逻辑隔离。同时，电力调度数据网应与企业办公网、公共互联网物理隔离或单向隔离，关键控制系统不直接暴露在外部网络中。

b) 访问控制与认证 (Access Control and Authentication)：对电力监控系统的所有访问接口实施严密的访问控制策略。采用白名单机制限制仅授权的设备和账号接入控制网络，对远程维护等特殊访问应通过 VPN 加密通道并在安全接入区部署入侵防御设备。关键业务系统和设备启用双因子认证和数字证书机制，确保只有可信身份才能执行敏感操作。

c) 安全监测部署 (Security Monitoring Deployment)：在变电站站控层、调度主站等关键节点部署入侵检测和安全监视装置，实现对网络流量和主机行为的持续监测（参考 5.3）。结合安全信息管理平台集中汇总分析各处警报，实现全面的态势感知。对于重要服务器和控制站，宜安装主机入侵检测(HIDS)代理，以发现异常的进程活动或权限变更。

d) 冗余与容错设计 (Redundancy and Fault Tolerance Design)：对于关键的监控通信链路和设备，应采取冗余备份和容错设计，避免单点故障被攻击者利用导致系统失效。例如，调度主站与变电站通信可设置双通道并附以加密认证装置，一条通道受攻击中断时自动切换至备用通道。重要的数据采集设备配置备用冗余模块，防止主模块被攻击瘫痪后采集中断。

e) 定期安全审查 (Regular Security Audits)：制定计划定期对电力监控系统进行安全检查和渗透测试，包括漏洞扫描、配置核查和社交工程测试等。及时修补系统和网络设备已知漏洞，更新防病毒库和入侵检测特征库。针对检测发现的新型威胁，及时调整防护策略和技术措施，保持防御体系的有效性和先进性。

6.3　事件响应与恢复

良好的事件响应能力可以将异常和攻击的危害降到最低。各单位应根据本标准制定详细的事故应急预案并定期演练，使运维人员熟悉响应流程。应急预案中明确各类事件的响应分级、责任分工、技术手段和通信联络机制等，确保真正发生突发情况时能够迅速、有序地应对。当监测系统检测到严重的数据异常或网络攻击事件时，必须立即启动应急响应预案，控制事态发展并尽快恢复系统正常运行：

a) 告警通知与决策支持 (Alert Notification and Decision Support)：检测到异常/攻击后，系统立即通过多种渠道发送告警通知，包括在监控界面弹出警示窗口、向运维人员手机发送短信或 App 推送、触发调度大屏声光报警等。通知应包含基本情况和初步建议处置措施。值班人员接到告警后，应快速评估事件影响范围和严重程度，必要时逐级上报启动更高级别的应急响应。

b) 隔离与切换 (Isolation and Switching)：对于怀疑受到网络攻击的设备或网络段，应迅速隔离以阻断攻击扩散。例如隔离被攻陷的调度终端，从交换机上关闭异常流量端口，启用通信网络的预备通道等。同时，对发生严重数据异常的设备（如传感器故障导致错误数据）应从自动控制回路中切除，改由人工监控接管，避免错误数据自动影响调节动作。

c) 故障甄别与溯源 (Incident Investigation and Traceback)：应急响应小组对事件进行调查甄别，判断异常是由设备故障误报还是真实攻击所致。如果确认发生网络入侵攻击，利用日志和取证工具对攻击路径进行溯源分析，查找攻击源头和可能的后门痕迹。如果是内部人员误操作或设备故障导致的数据异常，则安排检修更换相关设备并完善运行规程。

d) 恢复与验证 (Recovery and Verification)：在攻击被阻断或异常原因消除后，逐步恢复被隔离的网络连接和设备投入，密切监视恢复过程中的系统状态。恢复过程中优先保障发供电安全，对次要系统可延后恢复以确保主系统稳定。所有恢复完成后，应对整个事件处理过程进行验证测试，确认系统功能和安全防护措施均正常有效。同时保存事件日志和处理记录，为事后分析和改进提供依据。

6.4 安全运维

数据异常与网络安全的防护是一个持续的过程，需要在日常运维中贯彻安全管理措施，形成长效机制：

a) 安全策略更新：随着电力系统运行工况和外部威胁形势变化，定期评估现有安全策略的适用性，及时更新防护策略库和检测规则库。特别地，根据风险评估报告中发现的薄弱环节（见 5.4），调整安全资源配置和监控重点，使运维策略动态适应最新的风险状况。

b) 人员培训和意识：定期对调度运行人员和运维人员开展网络安全和数据异常应对培训，提高其安全意识和技能。培训内容包括本标准的要求、典型攻击手法、异常工况案例、应急响应流程等。通过演练和考试确保人员掌握必要的知识，在实际场景中能够正确判断和处理。

c) 日志管理与审计：建立健全日志留存和审计制度。电力监控系统的操作日志、网络日志、异常检测和攻击检测日志等应集中保存，保存期限符合国家标准要求（一般不少于 6 个月）。定期由独立部门对日志进行审计分析，检查是否存在未发现的异常模式或安全隐患，并将审计结果纳入安全绩效考核。

d) 持续改进机制：设置安全管理反馈机制，每当发生数据异常或安全事件，无论大小，都记录在案并召开事后分析会，评估现有检测与防护体系的有效性。如有措施不当或漏洞，及时更新本标准相关的企业实施细则和技术配置，持续改进系统能力。同时关注行业最新标准和技术动态，逐步采用更先进的检测算法和防御手段（如人工智能分析 (artificial intelligence analysis)、零信任架构 (Zero Trust Architecture)等）以提升安全水平。

附 录 A
（资料性）
数据异常主要类型及处置建议

A.1 数据异常分类

表A.1列出了数据异常的主要分类。

表 A.1 数据异常分类

分类维度	异常类型	定义	关联检测方法
异常表现	数值越限异常	量测数据超出电力设备或系统的额定物理范围	规则校验与阈值判别
异常表现	时序失准异常	数据随时间变化的趋势偏离历史规律，或存在突变、停滞	时间序列分析与预测
异常表现	逻辑矛盾异常	多组关联数据违反电力系统物理规律或数学关系	多元相关分析
异常表现	数据缺失异常	数据采集中断或未获取有效量测值	规则校验与阈值判别、状态估计残差分析（补全数据后验证）

A.2 数据异常常见原因及初步处置建议

表A.2列出了数据异常常见原因及初步处置建议。

表 A.2 数据异常常见原因及初步处置建议

异常根源	典型特征	初步处置建议	适用场景
传感器故障	数据固定不变、波动无规律；更换传感器后数据恢复正常	1. 暂停该传感器数据用于控制决策； 2. 更换同型号传感器并进行现场校准； 3.用状态估计结果补全故障时段数据。	电压互感器、电流互感器、温度传感器等量测设备故障
通信异常	数据间歇性缺失、延迟超 5s；通信链路指示灯异常	1. 检查通信链路（如光纤、4G 模块）连接状态； 2. 重启通信网关或重新配置通信参数； 3.启用备用通信通道（如有）。	SCADA 系统与变电站、新能源场站间的通信中断
设备故障	异常数据伴随设备告警	1. 联动设备监控系统确认设备状态； 2. 安排运维人员现场巡检； 3. 若影响系统稳定，启动设备停运预案。	变压器过载、线路短路导致的电流 / 功率异常
恶意篡改	异常数据具有针对性；多节点数据同时出现逻辑矛盾	1. 立即隔离疑似被篡改数据的采集终端； 2. 对比历史数据与备用数据源； 3.触发网络攻击检测模块排查是否存在注入攻击。	虚假数据注入、终端被劫持导致的数据异常）

附 录 B
（资料性）
网络攻击主要类型

B.1 网络攻击类型

表B列出了常见网络攻击的核心类型及对应说明。

表 B.1 网络攻击类型

攻击类型	攻击名称	说明
网络层攻击	DDoS 攻击	通过控制大量设备向目标发送海量请求，耗尽目标服务器带宽或资源，导致其无法正常服务。
应用层注入攻击	SQL 注入	利用应用程序输入验证漏洞，将恶意 SQL 语句注入到数据库查询中，非法读取、修改或删除数据。
应用层注入攻击	XSS 攻击	向网页中注入恶意脚本，当用户访问页面时脚本执行，窃取用户 Cookie、账号信息等敏感数据。
跨站请求攻击	CSRF 跨站请求伪造	利用用户已登录的身份，诱导其点击恶意链接或访问恶意页面，以用户名义发起非本意的操作。
服务器端请求攻击	SSRF 服务器端请求伪造	诱导服务器向攻击者指定的地址发起请求，可能导致内网资源暴露、端口扫描或数据泄露。
地址欺骗攻击	ARP 欺骗	伪造 ARP 数据包，篡改设备 ARP 缓存表，使目标将数据发送到攻击者设备，实现流量劫持或监听。
地址欺骗攻击	DNS 欺骗 / 投毒	篡改 DNS 解析结果，将目标域名指向恶意 IP，导致用户访问钓鱼网站或被劫持流量。
应用层漏洞攻击	文件上传漏洞	利用应用程序对上传文件的校验缺陷，上传恶意脚本文件到服务器，进而控制服务器。
应用层漏洞攻击	目录遍历攻击	利用 URL 参数或输入缺陷，构造特殊路径访问服务器上未授权的目录和文件，窃取敏感信息。
应用层漏洞攻击	API 滥用攻击	违反 API 使用规则（如超量调用、越权访问），或利用 API 设计缺陷，获取敏感数据或干扰服务。
应用层漏洞攻击	XML 外部实体注入	利用 XML 解析器对外部实体的支持，注入恶意外部实体，读取服务器文件、发起内网请求或执行代码。
应用层漏洞攻击	反序列化漏洞	利用应用程序对序列化数据的解析缺陷，注入恶意序列化数据，执行恶意代码或控制服务器。
应用层漏洞攻击	文件包含漏洞	利用应用程序对文件包含功能的校验缺陷，包含外部恶意文件并执行，获取服务器权限。
网络探测攻击	端口扫描与探测	扫描目标设备开放的端口及端口上运行的服务，收集目标网络信息，为后续攻击做准备。
命令执行攻击	命令注入	利用应用程序对用户输入的处理缺陷，注入系统命令并执行，控制目标设备或窃取数据。
网络监听攻击	网络嗅探	捕获网络中传输的数据包，解析数据包中的敏感信息（如账号密码、聊天内容），实现数据窃取。
内存漏洞攻击	缓冲区溢出	向程序缓冲区写入超出其容量的数据，覆盖相邻内存区域，执行恶意代码或获取系统权限。
认证破解攻击	暴力破解	通过自动化工具尝试大量账号密码组合，破解用户认证，非法登录目标系统或账号。
恶意软件攻击	恶意软件（病毒、蠕虫、木马、勒索软件、挖矿恶意软件）	包含多种恶意程序：病毒依附文件传播破坏；蠕虫自主传播；木马克制设备；勒索软件加密文件索财；挖矿恶意软件占用资源挖矿。

附 录 C
（资料性）
安全策略规则

C.1 安全策略规则

表C.1列出了安全策略通用规则。

表 C.1 安全策略规则

规则类别	核心策略要点
基础网络安全通用规则	网络分区隔离（生产控制区与管理信息区等域划分、网络边界隔离）、通信加密、网络架构冗余设计等。
访问控制通用规则	账号权限遵循 “最小必要” 原则、多因子身份认证、设备 / 用户接入白名单管理、远程访问加密与管控等。
安全监测通用规则	入侵检测与防御系统（IDS/IPS）部署、日志集中审计与分析、网络流量异常监测、电力专用协议专项检测等。
设备与数据安全通用规则	设备全生命周期安全管理（台账、固件 / 软件升级测试、退役数据清除）、数据加密存储与传输、数据备份与恢复有效性验证等。
应急响应通用规则	安全事件分级处置流程、灾难恢复演练与验证、应急预案动态更新、攻击事件溯源与复盘等。
日常运维通用规则	定期漏洞扫描与修复、系统配置合规性核查、安全策略周期性更新、恶意代码（病毒、木马等）防护与查杀等。
人员安全通用规则	安全培训与考核、操作权限与安全责任划分、应急演练参与要求、违规操作行为约束等。
物理安全通用规则	机房物理访问控制（门禁、视频监控）、设备物理防护（防盗窃、防破坏）、环境安全（防火、防水、温湿度控制）等。
密码应用通用规则	国密算法强制应用（数据加密、身份认证等场景）、密码设备合规性验证、密钥全生命周期安全管理（生成、存储、使用、销毁）等。
合规与审计通用规则	网络安全等级保护等合规要求落地、定期合规性自查与外部审计、审计结果闭环整改、合规证据留存与管理等。