ICS 35.240
CCS L 78

团　　体　　标　　准

T/×××　××××—××××

电力企业网络安全自动化运营流程要求

Requirement of network security automation operation process of electric power enterprises

××××－××－××发布　　××××－××－××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》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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位:国网湖北省电力有限公司武汉供电公司，华中科技大学网络空间安全学院，武汉金银湖实验室，国网浙江省省电力有限公司杭州供电公司

本文件主要起草人: 陈爽，石一辉，邢　骏，顾显俊，黄梦琦，覃思航，邹子旭，田聪，万珍，郭竞知，刘冲，李威，魏朝，陈俊龙，杨凯，付忠祥，朱东君，舒一峰，戴子城，韩兰胜，邹德清，陈元中，罗俊，倪夏冰

本文件首次发布。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)、中国能源研究会信息通信专业委员会标准工作委员会(E-mail:icc@cers.org.cn)。

引　言

近年来，随着数字化转型的深入推进，电力行业关键信息基础设施已成为网络攻击的重点目标，复杂多变的攻击手段严重威胁电力能源安全和国家稳定。面对海量数据处理压力、设备协同效率低下、自动化响应能力薄弱等问题，传统依赖人工操作的网络安全运营模式已难以应对快速演变的威胁态势，不仅导致运营效能低下、风险处置滞后，更易因人为疏漏造成关键资产暴露。

目前在电力企业网络安全运营中，仍缺少自动化运营流程标准，为突破当前电力企业网络安全运营困境，亟需制定相关标准予以规范。通过自动化技术实现威胁检测、分析研判、响应处置等全流程闭环管理，提升安全事件处理速度与准确性，降低人为操作风险，同时确保网络安全工作符合国家法律法规和行业监管要求。

标准的建立将规范电力企业安全运营的技术路径和管理框架，明确运营流程、数据交互等关键要素的标准化要求，可有效缩短安全事件处置周期，降低关键信息资产暴露风险，为电力行业数字化转型提供坚实的安全保障，护航电力行业安全可持续发展。

电力企业网络安全自动化运营流程要求

1 范围

本标准规定了电力企业网络安全自动化运营流程要求，借助自动化工具协助完成安全运营工作，工作涵盖从预防策略设定、安全威胁监测、自动化响应和自动化处置四个流程。

本标准适用于所有涉及网络运营的企业或机构使用。

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 20269-2006 信息安全技术 信息系统安全管理要求

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 25069-2022 信息安全技术 术语

GB/T 28827.3-2012 信息技术服务 运行维护 第3部分:应急响应规范

GB/T 30276-2020 信息安全技术 网络安全漏洞管理规范

GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求

GB/T 43269-2023 信息安全技术 网络安全应急能力评估准则

GB/T 43698-2024 网络安全技术 软件供应链安全要求

DL/T 2614—2023 电力行业网络安全等级保护基本要求

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

资产 asset

对个人、组织或政府具有价值的任何东西。

3.2

漏洞 vulnerability

一种系统、软件、网络或其他信息技术产品中存在的弱点或缺陷。

3.3

安全策略 security policy

用于治理某一组织及其系统内管理、保护并分发影响安全及有关元素的资产(包括敏感信息)的一组规则、指导和实践。

3.4

风险评估 risk assessment
风险识别、风险分析和风险评价的整个过程。

3.5

用户行为分析 user and entity behavior analytics
一种检测和响应用户异常行为的技术。

3.6

安全编排 security orchestration
将不同的安全工具和服务协调起来，以自动化的方式响应安全事件的过程。

3.7

剧本 playbook
定义了一系列预设步骤和操作来指导安全编排响应和处理的指导手册。

3.8

业务连续性 business continuity
一种确保关键业务功能在面对业务中断时能够持续运行或迅速恢复的能力。

3.9

安全加固 security reinforcement
通过技术和管理措施增强信息系统安全性的一系列措施。

4 缩略语

以下缩略语适用于本文件

EDR：端点检测和响应（Endpoint Detection and Response）

UEBA：用户和实体行为分析（User and Entity Behavior Analytics）

IDS：入侵检测系统（Intrusion Detection Systems）

SOAR：安全编排与自动化响应（Security Orchestration, Automation and Response）

IPS：入侵防御系统（Intrusion Prevention System）

SIEM：安全信息和事件管理（Security Information and Event Management）

5 电力企业网络安全自动化运营场景

在电力企业网络安全运营过程中，应从实际出发，立足当前网络安全运营痛点，提升复杂场景下的安全运营效率，可以通过自动化技术进行优化的常见场景如下表1。

表1 常见安全运营场景

场景	描述	应有能力
告警压缩	在该场景中，通过特定算法或规则，将因相同原因触发的无效和重复告警合并为单一告警，压缩告警数量。	诊断能力
故障分析	在该场景中，通过数据配置、综合分析等方法对系统或设备出现的异常情况进行检测、诊断，以确定问题根源。	决策、描述能力
故障预测	在该场景中，通过分析历史数据和实时监控信息，运用统计或机器学习方法，提前预判系统或设备可能发生的故障。	自我学习
异常检测	在该场景中，通过异常行为检测、监测系统运行状态或数据分析，识别出与正常模式不符的异常行为或事件。	感知、分析能力
流程优化	在该场景中，通过机器人、自动化响应工具对运营流程进行优化，有效代替人工并减低成本。	自我执行
应急响应	在该场景中，在突发网络安全事件发生时，迅速启动应急预案，组织协调各方资源，采取有效措施控制事态发展，减少损失，恢复秩序。	协调组织能力
态势感知	在该场景中，通过收集和分析来自多个源的信息，实时了解和评估当前环境状态，预测未来趋势，为决策提供支持。	感知、描述、诊断、决策能力，自我学习，自适应
数据分析	在该场景中，通过统计分析、数据挖掘等技术手段，从大量原始数据中提取有价值信息和洞见，帮助做出更有选择。	分析能力
日常巡检	在该场景中，利用自动化技术，定期检查设备或系统的运行状态，自动发现潜在问题并生成报告。	自我执行
安全运营编排	在该场景中，利用安全编排工具和数据分析技术整合安全资源与流程，实现对安全事件的快速响应和处理	自我执行
知识库应用	在该场景中，对大量信息进行组织和管理，提供快速准确的知识检索与推荐，辅助用户解决问题	分析能力

自动化运营场景通过应用新型技术来建设，围绕效率提升、质量保证的运营目标，旨在实现自动化监测、及时预警、精准故障定位与快速响应处理等功能，从而增强系统的稳定性和安全性，降低运营成本，提高服务质量。在场景实现时，应具备以下几个方面的要求：

a）应明确场景实现的具体目标，例如提高管理质量、缩短故障恢复时间、增强运维效率、减少人力成本、改善用户体验等；

b）应具备评估场景实现的可行性能力，考虑成本效益比、所需资源投入等因素；

c）应根据场景的复杂性、技术挑战、数据质量、资源可用性和需求紧急程度，规划场景实施的阶段与步骤；

d）应按照既定方案，开发、优化并建设所需能力，同时确保这些能力具有良好的可复用性；

e）对于需要自动化和批量操作的场景，应设置合理的限制条件，设计安全控制节点，并具备有回滚机制；

f）应具备测试验收能力，验证各项关键性能指标，如资源分配速度、问题根源识别精度、异常警告的准确性等；

g）应建立评价体系，组织各方对自动化运营场景的效果进行评估，确认其是否达到预期目标；

应制定具体的改进策略和升级计划，持续优化，快速迭代。

6 电力企业网络安全自动化运营参考流程要求

电力企业网络安全自动化运营是通过集成自动化工具和技术，实现对安全威胁的快速检测、响应和修复的过程，分为预防策略设定、安全威胁监测、自动化响应和自动化处置四个阶段。该流程要求从预先设定的安全策略和控制措施，到实时监控网络和系统的异常活动，再到检测到威胁后的自动化响应以及事件后的处置和恢复，确保组织能够高效应对安全挑战，减少安全事件的影响，并提升整体的安全防护水平。电力企业网络安全自动化运营流程要求的总体架构图如图1所示。

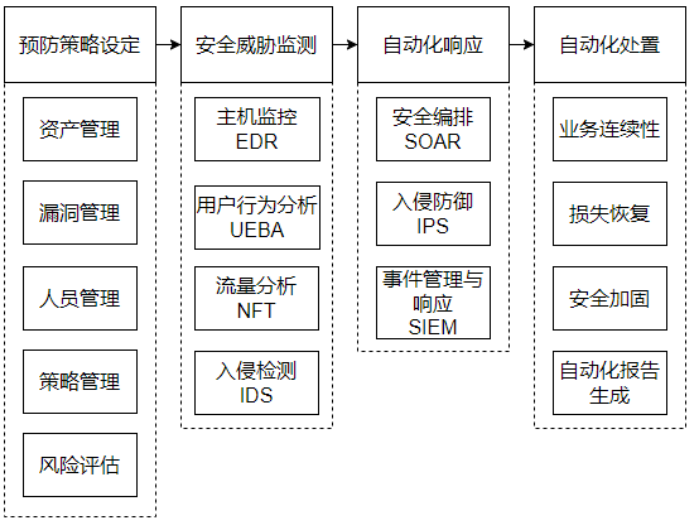

图1 电力企业网络安全自动化运营流程要求总体架构

7 预防策略设定阶段

7.1 资产管理

有效的资产管理应该具备以下功能：

a) 应具备自动发现和记录资产的能力，支持根据资产的重要性、敏感度等因素对其进行分类；

b) 应具备记录资产的基本信息，自动跟踪资产生命周期的能力；

c) 应具备资产可追溯性，支持监控资产变更并记录变更历史；

d) 应能直观显示资产之间的逻辑和物理关系，帮助理解资产之间的相互影响；

e) 应能定期评估资产状态，自动报告可能存在的风险。

7.2 漏洞管理

漏洞管理的主要目的是识别、评估、修复和跟踪信息系统中存在的漏洞，应具备以下功能：

a) 应具备自动执行对资产的漏洞扫描、检测并识别系统漏洞的能力；

b) 应具备对识别漏洞的危害程度、利用难易度、紧迫程度的自动评估能力；

c) 应具备自动生成漏洞报告并发送相关人员的能力；

d) 应能够自动或手动应用安全补丁、跟踪修复进度并进行复测扫描；

e) 应能够对无安全补丁的漏洞进行标记并提醒采取临时防护措施；

f) 应能够展示漏洞流转状态，管理漏洞全生命周期；

g) 应能够集成外部威胁情报源，并自动更新内部漏洞知识库。

7.3 人员管理

网络安全运营流程中的人员管理应具备以下功能：

a）应具备用户账户的创建、修改、禁用和删除等管理权限，能够管理用户账户的访问控制权限；

b）应配备包括系统管理员、安全管理员在内的不同角色，并明确各角色的权限职责；

c）应遵守人员身份与访问管理原则，包括最小权限原则、多因素认证、特权访问管理等。

7.4 策略管理

策略管理涉及到制定、实施、监督和更新一系列安全策略的过程，应具备以下功能：

a）应具备策略的制定、发布、传播与停用能力；

b）应具备可行性，能够保证安全策略落地；

c）应具备可执行性，策略能够转化为具体的控制措施和技术手段；

d）应具备审计能力，确保策略符合规范和要求，并定期检查策略的执行情况；

e）应具备统一的安全策略库，支持对策略进行展现、查询和分析。

7.5 风险评估

风险评估能够帮助组织识别、分析、评估和优先处理安全运营流程中面临的潜在风险，应具备以下功能：

a）应具备物理环境风险评估的能力，包括温湿度、供电状态、漏水、烟雾等；

b）应具备供应链风险评估能力，包括供应商资质、交货周期、物流稳定性、原材料质量等关键供应链节点；

c）应具备对每一种威胁结合脆弱性进行量化分析和风险评级的能力；

d）应具备根据风险的严重程度和可能性的排序能力；

e）应能够制定风险应对措施，包括风险规避、风险转移、风险缓解、风险接受等措施；

f）应具备持续的风险监控机制和风险告警机制；

g）应支持自动化或半自动化生成风险评估报告。

8 安全威胁监测阶段

8.1 主机监控

主机监控是为了确保服务器和终端设备的健康运行，并及时发现潜在的安全威胁，应具备以下功能：

a）应能够监测主机的核心指标，确保资源使用合理，跟踪网络接口的入出流量，检测异常通信模式；

b）应部署EDR系统，实时检测并响应潜在威胁，提供详细的事件上下文，帮助快速定位问题根源；

c）应支持识别异常行为模式，如未知恶意软件的活动等；

d）应支持实时监控正在运行的进程和服务，发现并阻止未授权或可疑进程；

e）应确保在主机监控过程中监控数据的安全传输和存储，保护敏感信息。

8.2 用户行为分析

用户行为分析主要用于检测和响应异常用户行为。通过对用户和实体（如服务器、应用程序等）的历史行为模式进行分析，识别出偏离正常行为模式的活动，从而发现潜在的安全威胁。用户行为分析应具备以下功能：

a）应支持实时监控用户的活动，如登录尝试、文件访问、应用程序使用等；

b）应部署UEBA系统，支持识别偏离正常行为模式的活动；

c) 应具备实时性，及时分析发现用户异常行为并响应异常活动；

d) 应支持预定义响应，当检测到异常行为时，自动执行预定义的响应措施；

e) 应确保用户隐私和数据安全，在行为分析过程中确保个人信息不受泄露。

8.3 流量分析

流量分析是网络安全监控中的一个重要环节，可以及时发现潜在的安全威胁，并采取相应的措施。流量分析应具备以下功能：

a) 应支持实时监控网络中的流量，识别异常流量并分析异常流量中未知的威胁；

b) 应支持回溯历史网络流量，识别并匹配已知恶意威胁；

c) 应支持深度解析流量中的协议内容，分析流量中的行为模式；

d) 应支持预设过滤规则，过滤不合法流量；

e) 应提供图形化的流量分析视图，展示网络中的数据流走向，显示流量随时间的变化趋势。

8.4 入侵检测

入侵检测侧重于检测入侵攻击行为，帮助识别潜在的安全威胁，应具备以下功能：

a) 应部署IDS，实时监测网络流量或主机系统日志，检测异常模式或攻击；

b) 应支持解析网络协议，识别潜在的网络攻击行为；

c) 应具备实时性，确保在检测到攻击行为的第一时间进行告警，防止更大的损失；

d) 应用支持从外部威胁情报源获取最新的威胁信息，将威胁情报应用于检测规则，提高检测精度。

9 自动化响应阶段

9.1 安全编排

安全编排技术通过协调不同的安全工具和服务来优化安全事件的处理流程，将整个安全运营流程上的组件和设备串联起来，实现组件设备的自动化响应与处置，从而有效地提高响应效率和质量。以下是安全编排在响应阶段应具备的功能和要求：

a) 应支持根据不同的安全事件类型，预定义自动化响应剧本，根据事件的严重性和具体情况，动态调整响应策略；

b) 应部署SOAR系统，根据剧本流程，当前置事件发生时，应能够按照剧本自动触发后置操作，实现安全运营自动化调用；

c) 应具备流程管理功能，实时跟踪事件的执行进度；

d) 应具备自动化报告生成功能，生成详细的事件处理报告，记录事件详情和处理结果；

e) 应具备集成工具和服务的功能，包括内部安全工具或自定义程序等。

9.2 入侵防御

入侵防御是在检测到潜在威胁后立即采取行动阻止威胁进一步扩散的安全措施，能够实时拦截和阻止攻击，从而保护网络和系统的安全。以下是入侵防御在响应阶段应具备的功能和要求：

a) 应支持实时监控网络流量，分析网络协议，实时检测异常行为和已知威胁并立即响应处置；

b) 应部署IPS，当检测到威胁时能够采取措施阻止攻击的进一步进行；

c) 应支持预定义防御规则，当检测到入侵攻击时，能够根据预定义规则自动响应。

9.3 事件管理与响应

事件管理与响应是确保组织能够快速有效地处理安全事件的关键环节，当检测到特定类型的事件后可以自动执行预定义的响应动作。以下是事件管理与响应在响应阶段应具备的功能和要求：

a) 应具备事件管理功能，包括事件分类、事件关联分析、事件优先级排序等；

b) 应具备自动化响应功能，当检测到安全事件时，自动执行预定义的响应措施；

c) 应明确任务分配，具备高效处理事件的能力；

d) 应部署SIEM系统，实现日志管理、实时监控、威胁检测和事件的自动化响应；

e) 应具备自动生成详细的事件处理报告的能力，记录事件的详细信息和处理过程。

10 自动化处置阶段

10.1 业务连续性

业务连续性是在发生安全事件后，组织的核心业务能够迅速恢复并继续运行的关键。保证业务连续性应做到以下几个方面的内容：

a) 支持评估安全事件对业务运作的影响，根据业务重要性和紧急程度对受影响的业务流程进行优先级排序；

b) 应具备应急响应能力，支持为不同类型的事件制定详细的应急响应预案，包括恢复流程、资源调配等；

c) 支持功能验证与性能验证，确保业务正常、稳定运行。

10.2 损失恢复

损失恢复是确保在发生安全事件后能够最大限度地减少损失，并恢复受影响业务的过程。损失恢复应做到以下几个方面的内容：

a) 应支持评估安全事件对业务、系统、数据等方面的影响范围，计算直接经济损失和潜在的间接经济损失；

b) 应具备数据恢复功能，支持利用备份数据恢复受损的数据，确保数据的完整性和可用性；

c) 应具备系统恢复功能，支持恢复受影响的服务或应用程序，确保其正常运行；

d) 应具备硬件恢复功能，支持替换或修复受损的硬件设备，恢复系统的物理完整性；

e) 应具备容灾机制，支持建立灾难恢复中心，确保在主站点无法使用时能够迅速切换。

10.3 安全加固

安全加固是指在发生安全事件后，通过一系列技术和管理措施，加强对系统、网络和应用程序的安全防护，防止类似事件再次发生。安全加固应做到以下几个方面的内容：

a) 应及时修补相关漏洞，确保操作系统、应用程序和第三方组件及时安装官方发布的安全补丁；

b) 应及时重新配置网络设备和应用程序的安全设置，加固安全策略；

c) 应具备数据安全审计能力，加密敏感数据，加强数据备份策略；

d) 应及时检查相关安全设备的运行状态，保证设备的健康运行。

10.4 自动化报告生成

自动化报告生成是对整个运营过程的准确记录，为后续分析、审计和改进提供了依据。自动化报告生成应做到以下几个方面的内容：

a) 支持根据实际需求自定义报告模板，适应不同的场景和需求；

b) 支持从各种来源自动收集相关的日志和事件数据，将来自不同来源的数据整合；

c) 应具备自动化生成报告能力，根据设备的告警、输出和运营的处理结果自动生成报告；

d) 应具备自动化消息通知能力，支持将生成的报告自动分发给相关人员或部门。

11 自动化运营数据要求

11.1 自动化运营数据来源

实现电力企业网络安全自动化运营需要不同来源的多维数据，包括但不限于以下来源：

a) 来源于入侵检测系统、防火墙、异常行为检测等设备产生的数据，例如：入侵尝试记录、防火墙日志、异常行为报告、安全事件警报等；

b) 来源于态势感知设备、日志设备、流量分析设备产生的数据，例如：威胁源数据、漏洞分布数据、应用操作记录、网络流量、网络性能指标等；

c) 来源于网关设备、终端管理设备、网络控制器等设备产生的数据，例如：网络配置信息、设备性能指标、网络流量统计数据等；

d) 来源于电力应用系统的业务数据，例如电力用户数据、电网运行数据、电力交易数据、故障维修记录、设备状态数据等。

11.2 数据类型要求

面向电力企业网络与信息系统的自动化安全运营数据需要统一的数据模型表示，从而实现数据的统一管理与复用性，以下是网络安全自动化运营应支持的12类数据类型：

a) 基础信息数据：包括网络拓扑结构、设备清单、资产属性、系统配置等；

b) 日志数据：涵盖各类网络设备、安全设备、终端设备和应用系统的操作日志、安全日志、系统日志等；

c) 流量数据：包括网络流量的详细信息，如数据包大小、协议类型、源IP、目的IP、端口号等；

d) 安全事件数据：记录各类安全事件，如入侵尝试、恶意软件检测、异常行为报警等；

e) 威胁情报数据：包括最新的漏洞信息、攻击手法、恶意软件样本等；

f) 用户行为数据：记录用户的登录行为、操作行为、访问记录等；

g) 性能指标数据：包括设备性能指标（CPU、内存、磁盘使用率等）、网络性能指标（延迟、丢包率、带宽使用情况等）；

h) 配置变更数据：记录系统配置的变更历史，包括变更时间、变更内容、变更人等；

i) 业务数据：涵盖电力用户的用电数据、电网运行数据、交易数据等；

j) 环境数据：包括物理环境数据（温度、湿度、风速等）和电磁环境数据；

k) 维护和故障数据：记录设备的维护历史、故障记录、维修过程等；

l) 客户业务数据：包括电力用户基础信息、电力订单数据、电力交易数据等。

11.3 数据协议要求

电力企业网络安全自动化运营的数据采集应支持多种数据传输协议，包括但不限于：

a) SNMP协议；

b) MQTT协议；

c) Syslog协议；

d) HTTP/HTTPS协议；

e) UDP协议；

f) BACnet协议；

g) Kafka协议；

h) FTP/SFTP协议。

11.4 数据安全要求

电力企业网络安全自动化运营的数据在传输、存储、使用过程中应保证数据隐私和安全性，以下是满足数据安全应满足的要求：

a) 对于数据中含有的个人敏感信息部分，应采取脱敏或加密的安全措施，防止敏感信息泄露；

b) 应具备数据细粒度访问控制措施，实施基于角色的访问控制和最小权限原则，确保用户只能访问其工作所需的最小数据集；

c) 应具备数据分类分级规范，支持对数据进行分类和分级，明确数据的敏感性和重要性，以便根据不同类型和级别的数据采取不同的保护措施；

d) 对于敏感数据在数据库中存储时，应使用国密或通用加密标准算法进行加密；

e) 应具备数据备份机制和数据恢复能力，对重要数据进行定期备份，支持在数据损失时能够快速恢复数据；

f) 应具备数据生命周期管理能力，制定数据保留策略，明确数据的保留期限和销毁方式，确保不再需要的数据能够安全地被销毁。

参 考 文 献

[1] GB/T 20269-2006　信息安全技术 信息系统安全管理要求
[2] GB/T 20984-2022　信息安全技术 信息安全风险评估方法
[3] GB/T 20986-2023　信息安全技术 网络安全事件分类分级指南
[4] GB/T 25069-2022　信息安全技术 术语
[5] GB/T 28827.3-2012 信息技术服务 运行维护 第3部分:应急响应规范
[6] GB/T 30276-2020　信息安全技术 网络安全漏洞管理规范
[7] GB/T 36626-2018　信息安全技术 信息系统安全运维管理指南
[8] GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求
[9] GB/T 43269-2023　信息安全技术 网络安全应急能力评估准则
[10] GB/T 43698-2024　网络安全技术 软件供应链安全要求
[11] DL/T 2614—2023 电力行业网络安全等级保护基本要求
[12] 国家发展改革委2024年第27号令 电力监控系统安全防护规定
[13] 国能发安全规〔2022〕100号 电力行业网络安全管理办法
[14] 国能发安全〔2024〕34号 电力网络安全事件应急预案