团　　体　　标　　准

电力企业网络安全自动化运营流程要求

（征求意见稿）

Requirement of Network Security Automation Operation Process of Electric Power Enterprises

编制说明

2025-04-15

《电力企业网络安全自动化运营流程要求》
（征求意见稿）编制说明

1 任务来源、协作单位

1.1 任务来源

2024 年 11 月 4 日，根据中国能源研究会下达的《关于 2024 年第二批中国能源研究会标准立项的通知》（中能研标〔2024]6 号），团体标准《电力企业网络安全自动化运营流程要求》予以立项，由中国能源研究会提出，中国能源研究会信息通信专委会技术归口。

1.2 协作单位

牵头单位：国网湖北省电力有限公司武汉供电公司

主要参编单位：国网湖北省电力有限公司武汉供电公司、华中科技大学、国网浙江省电力有限公司杭州供电公司

国网湖北电力省有限公司武汉供电公司作为牵头单位，负责组织协调编写单位，标准的前期技术调研、资料收集、标准目次编制、标准内容起草、反馈意见整理修改等工作。

牵头单位简介及与本标准相关的工作介绍：

国网湖北省电力有限公司武汉供电公司是国家电网有限公司在华中地区的核心能源保障企业，负责武汉地区电网建设、运维及供电服务。公司以数字化转型为驱动，构建“技术+生态+标准”三位一体的网络安全体系,成立国家电网首个地市层面网络安全监控班。近年来在电力网络安全创新及科技创新方面取得一系列优异成绩，在国家电网内率先开展网络安全数字化转型实践，全面整合各类系统资源，研发完成“基于人工智能技术的网络安全监测运营”，全方位保障电力核心业务的数据安全与通信可靠性，为新型电网建设构筑智能化安全基座。

参编单位单位简介及与本标准相关的工作介绍：

华中科技大学是国家教育部直属重点综合性大学，国家“211 工程”重点建设和“985 工程”建设高校之一，首批“双一流”建设高校。华中科技大学网络空间安全学院入选国家“一流网络安全学院建设示范项目高校”，信息安全专业入选国家级一流本科专业建设点，以第一名成绩通过一流网络安全学院建设示范项目评估。华中科技大学网络空间安全团队参与主持国家重点研发项目 5 个，青年及面上基金 15 个，军方项目 10 多项，本标准相关研究基础扎实，示范能力突出。

国网浙江省电力有限公司杭州供电公司是国家电网公司 34 家大型重点供电企业之一。杭州电网是浙江省负荷中心，为典型受端电网，80%的电力电量由省网受入，截至 2024 年底，35 千伏及以上变电站 484 座、容量 11259.8 万千伏安，规模约占全省 1/5，位列国网

系统省会城市第一。配网方面，建成世界一流配电网，全域供电可靠率99.9988%（年均停电 6.01 分钟），位居全国城市第一，媲美东京巴黎等世界先进城市，城区配网电缆化率96%，超过北京上海达到先进国家水平。电量方面，2024 年杭州全社会用电量1067 亿千瓦时，售电量 1008 亿千瓦时，用售电量均居国网系统省会城市第一。负荷方面，2024 年全社会最高负荷达到2215.5 万千瓦，历史首次突破2200 万千瓦。

2 编制工作组简况

2.1 编制工作组及其成员情况

1.业主单位：国网湖北省电力有限公司武汉供电公司

编写组成员情况：

陈爽，正高级工程师，国网武汉供电公司三级职员。

石一辉，高级工程师，国网武汉供电公司总工程师。

邢骏，高级工程师，国网武汉供电公司信息通信分公司总经理。

顾显俊，高级工程师，国网武汉供电公司信息通信分公司副总经理。

黄梦琦，高级工程师，国网武汉供电公司信息通信分公司网络安全监控班班长。

覃思航，工程师，国网武汉供电公司信息通信分公司网络安全监控班主职。

田聪，国网武汉供电公司信息通信分公司网络安全监控班助手。

邹子旭，助理工程师，国网武汉供电公司信息通信分公司网络安全监控班副职。

万珍，工程师，国网武汉供电公司信息通信分公司技术安保室副主管。

郭竞知，工程师，国网武汉供电公司信息通信分公司技术安保室专责。

刘冲，国网武汉供电公司信息通信分公司技术安保室专责。

李威，国网武汉供电公司信息通信分公司网络安全监控班副职。

魏朝，国网武汉供电公司信息通信分公司网络安全监控班副职。

陈俊龙，助理工程师，国网武汉供电公司信息通信分公司网络安全监控班副职。

杨凯，国网武汉供电公司信息通信分公司网络安全监控班副职。

付忠祥，工程师，国网武汉供电公司信息通信分公司网络安全监控班副职。

2.科研院所：华中科技大学

编写组成员情况：

邹德清，教授/博导，华中科技大学网络空间安全学院执行院长。

韩兰胜，教授/博导，华中科技大学网络空间安全学院创新与实践中心主任。

朱东君，助理研究员，华中科技大学网络空间安全学院博士生。

舒一峰，渗透测试工程师，武汉金银湖实验室众测竞测技术业务部。

戴子城，华中科技大学网络空间安全学院博士生。

3.建设单位：国网浙江省电力有限公司杭州供电公司

陈元中，高级工程师，国网浙江省电力有限公司杭州供电公司信息通信分公司七级职员

倪夏冰，工程师，国网浙江省电力有限公司杭州供电公司信息通信分公司专职

罗俊，工程师，国网浙江省电力有限公司杭州供电公司信息通信分公司专职

2.2 标准主要起草人及其所做的工作

陈爽、石一辉：负责标准编制总体进度的管控、标准内容的审核等工作；

顾显俊、邢骏、邹德清、韩兰胜：负责标准指导及审核等工作；

黄梦琦、覃思航、朱东君：负责技术调研、资料收集、标准具体章节的编写、校核、反馈意见整理及格式规范等工作；

田聪、李威、陈俊龙、魏朝、邹子旭、舒一峰、戴子城、陈元中、罗俊、倪夏冰等：负责资料收集、具体章节内容的编写、提出修改建议和意见等工作。

其中第 1 章节由黄梦琦、覃思航主要编写，第 2、3 章节由田聪、李威、陈俊龙主要编写，第 3、4、5 章节由魏朝、邹子旭、舒一峰、戴子城主要编写，第 6、7 章节由朱东君、舒一峰、戴子城、陈元中、罗俊、倪夏冰主要编写，第 8、9 章节由朱东君、舒一峰、戴子城、李威、陈俊龙、魏朝主要编写，第 10 章节由黄梦琦、覃思航、顾显俊、邢骏、韩兰胜主要编写，编制说明由陈爽、石一辉、黄梦琦、舒一峰、邹子旭主要编写。

3 起草阶段的主要工作内容

2024 年 11 月，根据中国能源研究会下达的《关于 2024 年第二批中国能源研究会标准立项的通知》（中能研标〔2024]6 号），随后组织开展前期调研，召开专家研讨会，对标准的范围、深度、主要内容等进行初步讨论。

2024 年 11 月，召开项目启动会，成立编制工作组，正式启动本标准编制工作。

2024 年 11 月-2025 年 3 月,编制工作组开展多轮研究讨论,编制标准各部分内容，以腾讯视频会议方式组织开展标准内部审查会议，形成标准初稿。

2025 年 3 月，中国能源研究会信息通信专业委员组织专家对初稿的形审和内容开展审查，根据评审专家意见进行修改。形成征求意见稿初稿。

2025 年 4 月，中国能源研究会信息通信专业委员会以函审的形式组织召开公开征求意见稿前审查会，对公开征求意见稿进行评审。

4 标准编制原则及与国家法律法规和强制性标准及有关标准的关系

4.1 标准编写原则

统一性：秉持在结构、格式和术语使用上的一致性原则，确保不同部分之间没有歧义，有助于正确理解和实施标准。

协调性：与国家法律法规及其它现行标准保持一致，确保不会与其他规定产生矛盾或重复，确保整体协调。

适用性：充分考虑行业特点和技术发展趋势，确保标准能够满足实际应用需求，适用于解决网络安全运营领域的问题。

规范性：严格遵守标准制定流程，使用明确的专业术语，提供清晰的操作指南，保证标准的质量和规范。

目的性：每项要求都有特定的目的，为解决某一具体问题或满足某项功能需求，确保标准具有明确的方向性和针对性。

4.2 本标准与标准编制和实施过程涉及到的法律法规、强制性标准的关系：

本标准符合现行法律、法规、政策及相关标准相关规定。

5 标准主要技术内容的论据或依据；修订标准时，应增加新、旧标准水平的对比情况

5.1 标准主要技术内容的论据或依据

本标准的主要技术内容主要依托于国网武汉公司及其他单位在网络安全运营领域多年积累的宝贵经验，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方面，规范网络安全自动化运营流程要求。通过调研最新的安全自动化编排、安全信息和事件管理等技术成果，广泛收集和分析实际运营中的挑战与需求，确保了本标准既符合当前网络安全自动化运营的最佳实践，又能适应未来技术发展趋势。同时，国网武汉公司在网络安全运营领域实施了多项项目，通过实际产品为本标准的编制提供了重要参考。综上所述，本标准融合了行业需求、调研成果以及国网武汉公司在网络安全运营领域的先进实践，组织提供了一套科学、系统且行之有效的流程要求，为能源企业的数字化转型打造了高效而可靠的安全保障。

5.2 修订标准时，应增加新、旧标准水平的对比

无。

6 主要试验（验证）的分析、综述报告，技术经济论证，预期的经济效果

6.1 主要试验（验证）的分析

无。

6.2 综述报告

无。

6.3 技术经济论证

通过引入自动化工具和优化的网络安全运营流程，能够显著降低能源企业的人力成本与响应时间，减少安全事件造成的经济损失；同时，增强企业的安全防护能力，保护关键信息基础设施免受网络威胁，确保业务连续性和数据完整性，从而为企业带来长期的经济效益和竞争力提升。此外，标准化的网络安全运营流程有助于促进技术创新和资源共享，推动整个行业的健康发展，具有显著的经济效益和社会效益。

6.4 预期的经济效果

通过实施本标准，能源企业可大幅降低网络安全运营的人力成本，预计人力投入减少 30%-50%，提高运营效率；快速检测与响应机制将有效缩短安全事件处理周期，降低因安全事故导致的直接经济损失；其次，增强的安全防护能力将保护企业免受潜在网络攻击，避免敏感数据泄露带来的法律风险和声誉损失，带来间接的经济效益。

7 采用国际标准的程度及水平的简要说明

无。

8 重大分歧意见的处理经过和依据

标准编制过程中充分征集了标委会委员和专家意见，所有意见均按照标准编制程序进行充分讨论，并提交了采纳意见，不存在重大分歧意见。

9　贯彻标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）

贯彻标准的要求：1.通过中国能源研究会平台加强标准宣贯，增强对标准的认知度和支持度。2.企业应根据自身情况开展网络安全运营现状评估，识别现有网络安全运营体系与标准之间的差距，明确改进方向。3.邀请能源企业权威机构或专家团队进行独立评审，提供专业意见和改进建议，确保标准实施的科学性和合理性。

后续跟进措施及建议：在标准实施过程中，提供必要的技术支持和解释服务，并及时帮助企业解决在标准执行过程中遇到的问题；根据技术发展和业务需求变化，适时评估并修订标准内容，保持其先进性和适用性。

10　其他应予说明的事项，如涉及专利的处理等

无。