团　　体　　标　　准

电力信息系统开源软件安全使用技术指南

（报批稿）

编制说明

2024-10-14

《电力信息系统开源软件安全使用技术指南》
（报批稿）编制说明

1 任务来源、协作单位

1.1 任务来源

计划批次：第一批

项目名称：《电力信息系统开源软件安全使用技术指南》

项目编号：

项目期限：

提出单位：云南电网有限责任公司

1.2 协作单位

牵头单位：云南电网有限责任公司

参编单位：云南电网有限责任公司,南方电网数字电网集团有限公司,国网浙江省电力有限公司电力科学研究院,工业和信息化部电子第一研究所,深圳开源互联网安全技术有限公司,华南理工大学

2 编制工作组简况

2.1 编制工作组及其成员情况

云南电网有限责任公司 - 业主单位

南方电网数字电网集团有限公司 - 建设单位

国网浙江省电力有限公司电力科学研究院 - 科研院所

工业和信息化部电子第一研究所 - 科研院所

深圳开源互联网安全技术有限公司 - 设计单位

华南理工大学 - 高校

2.2 标准主要起草人及其所做的工作

本文件主要起草人：胡健、王海林、张佳发、冯国聪、杨航、白彪、张诗军、钟伟杰、刘欣、母天石、邓子杰、肖鹏、杭菲璐、谢林江、廖周缘、孙章才、张莉娜，刘庆海，严雪伦，其中第1-3章节由张佳发、冯国聪、杨航、白彪主要编写，第4章节由胡健、邓子杰主要编写，第5章节由张佳发、张诗军、钟伟杰、刘欣、母天石、邓子杰、杭菲璐、谢林江主要编写，第6-7章节由胡健、肖鹏、廖周缘、孙章才、张莉娜主要编写，编写说明由张莉娜主要编写，全文检查以及整合主要由胡健、严雪伦负责进行。

3 起草阶段的主要工作内容

<u>编制过程信息</u>

初次沟通标准要求于2023年1月17日；于2023年2月9日完成初稿编写；于2023年2月13日开展初稿专家评审意见会；于2023年2月15日开会明确额外补充要求点；

于2023年2月20日完成稿件二次修订。

主要争议问题

优化标准中的措施，充分调研公司新型电力系统建设对开源软件的需求和使用场景，进一步明确开源软件适用范围；部分章节的相关性强弱，与总述内容对应性提升；具体章节描述优化。

送审稿审查后标准内容以及修改情况

于2023年6月19日共计收到来自于南网总调、广东电网有限责任公司汕头供电局、云南电网公司信息中心、云南电网有限责任公司普洱供电局、中山供电局、佛山供电局、广西电网、华南理工大学的28条专家修改意见。修改意见覆盖全篇标准文档内容，从格式规范性、标号使用问题、内容完整性、来源多样性、语义问题、描述问题、内容正确性等多个维度进行审查。28条专家建议中共计采纳并修改26条，2条修改意见被驳回，并于2023年6月26日之前完成全部修改意见的修订。

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

该标准的编制须确保采用电力行业公认的术语和标准，避免混淆和误解，增强指南的通用性和可理解性；需与电力信息系统的整体安全策略、现有架构及未来规划相协调，确保无缝集成和高效运行；充分考虑电力企业内部各部门间的协同工作需求，确保指南的实施能够促进部门间的有效沟通与协作；确保技术指南应适用于不同规模、不同类型的电力信息系统，满足不同用户群体的实际需求；明确开源软件安全使用的全流程，包括选型、部署、运维、升级等各个环节的规范和要求，确保操作的一致性和可重复性；保障所有技术要素和措施均围绕提高电力信息系统的整体安全性这一目标展开，形成统一的安全防护体系；严格遵守国家及电力行业关于信息安全、软件开发等方面的法律法规和标准规范；应明确界定电力信息系统开源软件安全使用的具体目标和预期成果，以解决实际问题为导向，提出具有针对性和可操作性的技术方案和措施。

本标准并未涉及到法律法规以及强制性标准。

由于该标准维度在电力行业内属于空白区域，因此并未存在上位标准或者其他类似标准情况。

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

标准的主要技术内容包括在开源软件选型与评估维度分析开源软件的安全漏洞历史、社区活跃度、更新频率等指标，评估其潜在安全风险。确保所选开源软件与电力信息系统的现有架构、操作系统、数据库等兼容。从安全配置与部署维度遵循最小权限原则配置开源软件，仅授予必要的访问权限，对开源软件进行必要的安全加固，详细记录开源软件的安装、配置过程及关键参数设置，便于后续维护和审计。从持续监控与维护维度启用并合理配置日志记录功能，定期审查日志文件以发现潜在的安全威胁，定期使用自动化工具对开源软件进行漏洞扫描，并及时应用安全补丁，最后跟踪

开源软件的最新版本和更新日志，评估并决定是否进行版本升级。在应急响应与灾情恢复方面，针对可能的安全事件制定应急预案，明确应急响应流程和责任人，建立完善的数据备份与恢复机制，确保在发生安全事件时能够迅速恢复系统正常运行，并且在发生安全事件时，按照应急预案迅速响应并处理，同时记录事件处理过程和结果。最后在人员意识培训提升方面，对电力信息系统的使用人员进行开源软件安全使用培训，提高其安全意识和操作技能，并通过内部宣传渠道普及开源软件安全知识，营造良好的安全文化氛围。

编制思路主要围绕风险识别与评估、需求分析与规划、标准制定与规范、实施与验证、持续优化与改进这几个维度进行。首先对电力信息系统的整体安全环境进行评估，识别潜在的安全风险点，针对开源软件的使用场景进行风险评估，确定开源软件在电力信息系统中的安全地位。根据风险评估结果和实际需求，明确开源软件安全使用的目标和要求，制定详细的技术方案和实施计划，包括选型、部署、监控、维护等各个环节。参考国家及电力行业的相关标准和规范，制定适用于电力信息系统的开源软件安全使用规范，明确开源软件的选型标准、配置要求、监控指标、维护流程等具体规定。按照技术方案和实施计划逐步推进开源软件的安全使用工作，在实施过程中进行充分的测试和验证，确保各项措施的有效性和可靠性。定期对开源软件的安全使用情况进行评估和总结，根据评估结果和反馈意见持续优化和改进技术方案和实施计划，提高开源软件在电力信息系统中的安全性和稳定性。

5.2 修订标准时，应增加新、旧标准水平的对比

软件物料清单 SBOM 在电力行业的首批次推行实施需要进一步试验与研究。由于 SBOM 概念于近两年才开始在国内流行，因此该具体能力在各行业的具体实施经验仍旧缺乏，并且不同行业由于行业性质的不同，真实实施可能会存在区别，因此须进一步补充试验和研究以保证软件物料清单在电力行业有效落地。

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

试验设计

为了验证电力信息系统开源软件安全使用技术指南的有效性和可行性，我们设计了一系列试验，包括：

- 安全性验证：模拟常见的网络攻击场景，测试开源软件在配置安全加固后的防御能力。
- 兼容性测试：将开源软件部署在不同版本的操作系统和数据库环境中，验证其兼容性。
- 性能评估：通过压力测试和基准测试，评估开源软件在电力信息系统中的运行效率和稳定性。
- 应急响应测试：模拟安全事件，检验应急预案的可行性和响应速度。

试验结果

- 安全性验证：在模拟攻击下，所有经过安全加固的开源软件均能有效抵御常见网络攻击，未出现安全漏洞被利用的情况。
- 兼容性测试：开源软件在不同操作系统和数据库环境中的兼容性良好，未出现因兼容性问题导致的系统异常。
- 性能评估：经过优化配置的开源软件在电力信息系统中的运行效率稳定，能够满足业务需求，未出现明显的性能瓶颈。
- 应急响应测试：在模拟安全事件发生时，应急预案能够迅速启动并有效应对，将损失降至最低。

6.2 综述报告

通过一系列严格的试验验证，电力信息系统开源软件安全使用技术指南得到了充分的实践检验。结果表明，该指南提出的选型、配置、监控、维护等安全措施能够有效提升电力信息系统的安全性、稳定性和运行效率。同时，应急预案的制定和实施也显著提高了应对突发安全事件的能力。

6.3 技术经济论证

电力信息系统开源软件安全使用技术指南基于成熟的信息安全技术和开源软件生态，技术路线清晰明确，具有较高的技术可行性。同时，指南中的各项措施均经过试验验证，证明其在实际应用中能够发挥预期效果。

初期投入方面，虽然开源软件本身免费，但安全加固、人员培训、应急演练等初期投入仍需一定成本。然而，与购买商业软件相比，这些成本仍然较低。长期效益方面，通过实施指南中的各项措施，电力信息系统能够显著提升安全性、稳定性和运行效率，减少因安全事件导致的损失。长期来看，这些效益将远远超过初期投入。并且使用开源软件并遵循安全使用指南有助于降低因软件漏洞被利用而引发的安全风险，减少潜在的经济损失和法律风险。

6.4 预期的经济效果

该标准实施后可能可以带来的经济效益主要包括以下 4 个方面：

1) 减少安全事件损失：通过加强开源软件的安全使用和管理，显著降低因安全漏洞被利用而引发的安全事件频率和损失程度。
2) 提升业务处理效率：优化后的电力信息系统运行更加稳定高效，有助于提升业务处理速度和客户满意度。
3) 降低软件成本：利用开源软件替代部分商业软件，降低软件采购成本和维护费用。
4) 增强企业竞争力：通过提升电力信息系统的安全性和稳定性，增强企业的品牌形象和市场竞争力。

7 采用国际标准的程度及水平的简要说明

本标准并未采用任何国际标准或国外标准。

8 重大分歧意见的处理经过和依据

本标准在完整编制过程中并未出现重大的分歧意见。

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）

为了贯彻标准的要求，电力企业须从组织措施、技术措施以及过渡办法三个方面着手。组织措施方面主要包含以下 4 个维度：

一、 成立专项工作组

- 成立由信息安全专家、系统管理员、开发人员等多部门人员组成的专项工作组，负责标准的解读、推广和实施工作。
- 明确工作组的职责、分工和协作机制，确保各项任务得到有效执行。

二、 制定实施计划

- 根据企业实际情况，制定详细的实施计划，明确时间节点、责任人和具体任务。
- 确保实施计划与企业整体信息安全战略相协调，避免资源浪费和重复劳动。

三、 加强培训与教育

- 对全体员工进行开源软件安全使用知识的培训，提高员工的安全意识和操作技能。
- 定期组织安全演练和应急响应培训，提升员工的应急处理能力。

四、 建立考核机制

- 将开源软件安全使用情况纳入员工绩效考核体系，对违反安全规定的行为进行惩罚。
- 鼓励员工积极参与开源软件安全使用工作，对表现突出的个人或团队给予奖励。

技术实施方面主要包含以下 4 个维度：

一、 开展安全评估与加固

- 对现有电力信息系统中使用的开源软件进行全面的安全评估，识别潜在的安全漏洞和风险点。
- 针对评估结果制定相应的加固措施，包括更新补丁、修改配置、加强访问控制等。

二、 实施监控与审计

- 建立完善的监控体系，对开源软件的运行状态进行实时监控，及时发现并处理异常行为。

- 定期对开源软件的使用情况进行审计，确保符合安全规范和要求。

三、 强化访问控制

- 实施严格的访问控制策略，对访问开源软件的用户进行身份验证和权限管理。
- 禁止未经授权的访问和操作，防止敏感信息泄露和非法篡改。

四、 推进安全更新与升级

- 密切关注开源软件的更新动态，及时获取最新的安全补丁和修复程序。
- 对电力信息系统中使用的开源软件进行定期更新和升级，确保系统的安全性和稳定性。

过渡办法方面从以下 3 个维度着手：

一、 逐步替换

- 对于存在严重安全漏洞或无法满足安全需求的开源软件，应逐步替换为更安全的软件或解决方案。
- 在替换过程中，应充分考虑系统的兼容性和稳定性，确保业务不受影响。

二、 临时隔离

- 对于暂时无法替换或更新的开源软件，可以考虑采取临时隔离措施。
- 通过设置网络隔离、访问控制等手段，限制潜在的安全威胁对系统的影响范围。

三、 加强文档管理

- 在过渡期间，加强对开源软件使用文档的管理和更新工作。
- 确保所有相关人员都能够及时获取最新的使用指南和安全规范信息。

10 其他应予说明的事项，如涉及专利的处理等

无。