ICS
点击此处添加中国标准文献分类号

团　　体　　标　　准

T/××× ××××—××××

电力信息系统开源软件安全使用技术规范

Technical Specifications for the Secure Use of Open - source Software in Power Information Systems

2024－××－××发布　　2024－××－××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给出的规则起草。

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专利的责任。

本文件起草单位：云南电网有限责任公司，华南理工大学，南方电网数字电网集团有限公司，海南电网公司，深圳开源互联网安全技术有限公司。

本文件主要起草人：胡健、王海林、张佳发、冯国聪、高英、杨航、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、高英、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。

本文件首次发布，自颁布之日起执行。

本文件由中国能源研究会负责解释。

本文件在执行过程中的意见或建议反馈至中国南方电网公司技术标准化委员会办公室（广东省广州市黄埔区科翔路 11 号南网科研基地，510663）

电力信息系统开源软件安全使用技术规范

1 范围

本文件规定了在能源电力信息系统中安全使用开源软件的操作规范和相关注意事项，能源电力信息系统建设过程中对开源软件的选型规范以及能源电力企业如何在软件供应链下游保障其内部所使用软件的安全。

本文件适用于南方电网公司各单位数字化系统建设过程中对开源软件使用的统一性、安全性、规范性以及如何正确选型和安全使用开源软件进行指导，为提升开源软件的质量以及成熟度提供一定程度的参考。

2 规范性引用文件

下列文件中的有关条款通过引用而成为本部分的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本部分，但提倡使用本部分的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本部分。

GB/T 36324-2018　　信息安全技术 工业控制系统信息安全分级规范

GB/T 37090-2018　　信息安全技术 病毒防治产品安全技术要求和测试评价方法

T/NIFA 7-2021　　金融行业开源软件评测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1 开源软件 open source software

允许用户直接访问源代码，通过开源许可证将软件复制、修改、再发布的权利向公众开放的软件项目。

[来源：T/NIFA 7-2021，3、5、6、7]

3.2 开源许可证 open source license

开源许可证采用契约和授权的方式指导和规范开源软件的权利、义务和责任，开源许可证声明了开源软件商业使用、分发、专利授权、承担责任、使用商标等方面的权利要求。

[来源：T/NIFA 7-2021，3.1、3.2、5.1、5.5]

3.3 衍生产品 derivative product

衍生产品指以开源软件为基础（或源自开源软件）的任何产品，无论是源代码或对象形式，也包括对原作品的编辑版本、注释、阐述或其他修改。

[来源：T/NIFA 7-2021，3.3、5.1]

3.4 贡献者 contributor

贡献者指创建、贡献创建或拥有涵盖软件的每个个人或法人实体。

[来源：T/NIFA 7-2021，3.4、5.3、5.16]

3.5 源代码 source code

程序包含源代码，并且必须允许以代码或已编译的形式发布。

[来源：T/NIFA 7-2021，3、5、7]

3.6 源代码形式 source code form

源代码形式指进行修改的首选形式，包括但不限于软件源代码、文档和配置文件。

[来源：T/NIFA 7-2021，3.6、3.8]

3.7 可靠性 reliability

预期行为和结果保持一致的特性。

[来源：GB/T 36324-2018，3.7、5.3、5.10、7.2]

3.8 修改 modifications

修改指以下任何一种形式：

a) 源代码形式中对于对涵盖软件内容的添加、删除或修改而产生的任何文件。

b) 源代码形式中添加包含涵盖软件的新文件。

[来源：T/NIFA 7-2021，3、5、6]

3.9 分发 redistribution

当软件是来自不同来源的程序集成后的软件发行版本中的其中一个组件时，许可证不能限制任何团体销售和分发该软件，并且不能向这样的销售或分发收取许可费和其他费用。

[来源：T/NIFA 7-2021，3.2、3.9、5.1、6.3]

3.10 后门 Backdoor program

开放特定的网络端口，等待攻击者连接，并接收攻击者的指令执行相应的恶意操作的恶意程序。

[来源：GB/T 37090-2018，3.10、5.14]

3.11 影响 Impact

事件的后果，对已达到的业务目标水平的不利改变。在信息安全中，一般指不测事件的后果。

[来源：GB/T 36324-2018，3.11、5.3、5.5、6.2、7.2、7.3]

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口 (Application Programming Interface Recovery Time Objective)

OSI：开源许可证OSI认证是指开源项目所使用的许可证需要符合开源促进会（Open Source Initiative，OSI）所定义的开源标准，并通过OSI的审核认证。

RTO：恢复时间目标 (Recovery Point Objective)

RPO：恢复点目标 (Recovery Point Objective)

SBOM：软件物料清单 （Software Bill of Materials）

5 安全使用准则

本文件主要用于规范开源软件的选型、安全评估、安全监测、安全管理的技术要求，应考虑开源软件安全风险评估结果和组织对开源软件风险的接受程度，开源软件安全使用应遵循以下原则：

a) 应明确组织内部各部门在开源软件安全使用过程中的职责，确保每个环节都有明确的责任主体，以便在出现安全问题时能够快速响应和处理；
b) 应避免引入不必要的组件和依赖，优先选择代码量少、依赖关系简单的开源软件；
c) 应开展开源软件安全风险评估，结合组织对开源软件风险的接受程度，制定相应的风险应对策略；
d) 应建立持续的安全监测机制，实时跟踪开源软件的安全动态，包括新漏洞的发现、安全补丁的发布等；
e) 在使用开源软件处理电力信息系统中的数据时，应确保开源软件的数据存储、传输和处理方式符合电力行业的数据安全标准；
f) 应严格遵循国家法律法规、行业标准以及组织内部的规章制度，确保开源软件的使用符合知识产权、数据保护等相关要求。

6 管理体系要求

应建立完备的知识产权风险防范、开源风险防控、开源软件物料清单管理、开源软件威胁情报管理等体系。

6.1 管理制度

应建立完善的开源软件安全管理制度，包括以下内容：

a) 应制定适合本组织的开源软件安全管理计划，明确开源软件安全管理目标，从知识产权、漏洞风险、物料清单、威胁情报等方面进行规划；
b) 开源安全管理计划应形成文档并经审批后发送至相关人员；
c) 应制定开源软件安全管理制度，包括开源风险防控、开源软件物料清单管理、开源软件威胁情报管理等内容。

6.2 安全风险管理

应建立完善的开源软件安全风险管理机制，包括以下内容：

a) 应制定开源软件安全评估标准，定期开展开源软件安全风险评估，监测已有风险安全状况，制定风险解决方案；
b) 应根据开源软件的开源许可证、开源社区知识产权要求、能源电力企业使用场景，综合判断开源软件的知识产权风险；

c) 应建立和维护完整的开源软件物料清单(SBOM)，记录包括组件版本、许可证、依赖关系、安全风险等信息；
d) 应建立和供应链相关方、上级主管部门、安全监管部门的开源软件威胁情报获取和共享机制。

6.3 知识产权管理

应建立完善的开源软件知识产权风险管理机制，包括以下内容：

a) 应明确开源软件许可证识别和合规性审查流程，确保所有使用的开源软件均符合项目知识产权策略，并保留完整的许可证文件和声明；
b) 在推出开源相关的产品时，法务人员应做好产品审核，审核内容应包括：避免开源模块遗漏、按规定进行开源相关声明、保证获取源代码方式可用等；
c) 法务部门应准确解读企业常用的开源许可协议；
d) 法务部门解读许可协议时，应重点关注许可协议对术语的定义、软件再发布的规定、专利许可、专利报复、不担保条款、规定法律纠纷管辖地等；
e) 法务人员应跟踪分析已发生的开源纠纷案例，关注案件争议焦点、判决结果的分析、法官判决依据，宜掌握开源软件的诉讼动向，便于公司提前做好诉讼防控准备；
f) 应建立所使用的开源软件许可协议变更的跟踪机制，及时发现开源协议或开源产品变为闭源的情况。

6.4 自主可控管理

应建立完善的自主可控管理机制，包括以下内容：

a) 应建立多元化的开源软件供应链，减少对单一开源项目的依赖；
b) 应加强开源软件的自主研发能力，推动信创产业的自主可控发展；
c) 应积极参与国际开源社区的建设和合作，提升我国在全球开源领域的影响力和话语权；
d) 应建立所使用开源软件的维护机制，积极参与开源社区代码维护活动。

7 使用安全要求

7.1 开源软件选型

开源软件选型应综合考虑许可证版权协议、兼容性、扩展性、替代性、开源社区支持、服务支持、市场占有率、功能等维度：

a) 选型时应选用可合法修改代码的、可闭源使用的、可合法修改代码并重新分发的许可证版本协议；
b) 选型时应考虑开源软件点对点兼容性，保障系统与现有技术栈的兼容性（JDK、Node的版本要求），并可重用已有的代码和功能；
c) 选型时应考虑开源软件的扩展性，保障系统的设计扩展点，易于二次开发；
d) 选型时应考虑开源软件的替代性，应与同类型功能相似的软件进行试点比较；
e) 选型时应考虑开源软件社区的支持能力，应具备活跃的开源社区，如邮件列表、论坛等；
f) 选型时应考虑开源软件的更新频率，应长期关注更新频率频繁的开源软件并开展案例分析活动；
g) 选型时应考虑开源软件的开源生态圈，选择开源软件或技术前应对其所属生态圈及相关工具进行综合分析；
h) 选型时应考虑开源软件的服务支持能力，应从官方文档、商业支持以及成熟案例三个层面充分考虑其服务支持能力；

i） 选型时应考虑开源软件的市场占有率，宜参考第三方扩展资源选取市场占有率高的开源软件；
j） 选型时应考虑开源软件的功能性，应选择功能可直接使用、少量二次开发后可使用的开源软件，以此节约人力以及时间成本。应选取可提供完备的扩展开发接口、二次开发接口的开源软件，以满足二次开发需求；
k） 选型时应考虑开源软件社区是否针对软件开展安全测评，并提供安全评审报告；
l） 选型时应选择相对比较成熟的主流的开源软件；
m） 选型时应选择具备高关注度、版本更新、漏洞修复、漏洞公告发布及时的开源软件；
n） 选型时应优先选择生态系统比较完备、有基金会支持、有业界主流厂商积极参与贡献和选用的开源软件。

7.2 供应商选择

应通过对开源软件供应商的资质的评估结果来保障该供应商所提供的开源软件的质量以及合规性：
a） 应对供应商服务水平能力进行评估；
b） 应对供应商财务状况好坏进行分析评定；
c） 应对供应商流水进行分析评定；
d） 应对供应商人员组成以及人员流动进行审核；
e） 应对供应商能力进行评级，并开展供应商评审管理。

7.3 安全检测

7.3.1 完整性校验

在开源软件下载过程中，应确保开源软件代码和安装包的完整性，避免未经授权的修改：
a） 应保证开源软件来源于官方发布渠道；
b） 应使用加密算法对开源软件代码和安装包进行加密传输；
c） 应使用官方的校验方法对软件代码和安装包的完整性进行校验。

7.3.2 安全风险检测

应在引入开源软件前进行全面的安全风险检测，具体检测内容应包括：
a） 应明确开源软件需满足的基本安全要求，并根据基本安全要求进行安全风险检测，出具检测报告；
b） 应使用软件成分分析工具对开源软件的漏洞风险、开源许可证风险等安全风险进行检测；
c） 应使用静态应用程序安全检测工具对开源软件进行代码规范检测；
d） 应使用动态应用程序安全检测工具对开源软件进行应用安全漏洞检测；
e） 应使用交互式应用程序安全检测工具对开源软件进行应用安全漏洞、逻辑漏洞、数据安全风险检测；
f） 应对检测到的安全风险及时修复，不应使用存在高危漏洞、许可证风险、安全后门的开源软件，如果安全风险无法修复，应制定安全加固方案。

7.3.3 安全功能检测

在引入开源软件前应检测开源软件安全功能的完整性，至少包括以下功能：
a） 应具备对用户身份认证和鉴权的能力；
b） 应具备对非授权访问的控制和隔离能力；
c） 开源软件应记录用户操作日志，并具备取证审计的能力；
d） 开源软件的操作记录应具备不被修改或删除的能力；

e) 应用于涉密系统的开源软件，数据传输与存储过程应进行加密；
f) 应用于涉密系统的开源软件，应使用国密算法保障其安全性。

7.3.4 代码逻辑审查

在引入开源软件前应进行代码逻辑安全审查，确保不存在逻辑漏洞，审查内容包括：
a) 应对代码逻辑开展检查，代码逻辑应简洁明了，符合业务逻辑；
b) 应对函数需要解决的问题，函数的输入输出等维度进行检查，保证函数模块的可复用性高；
c) 应对开源代码的框架进行检查，保证框架逻辑性达标；
d) 应对重复使用的模块进行检查，保证此类模块已经被封装为函数或类。

7.3.5 开源许可证合规审查

7.3.5.1 开源许可证使用合规

在引入开源软件前应审查开源许可证的使用合规，至少包括以下内容：
a) 应优先使用开放源码促进会（OSI）认可的开源许可证；
b) 禁止修改开源许可协议条款；
c) 软件产品包含多个开源软件许可证时，应避免使用许可证条款存在冲突的开源许可证，存在冲突的开源许可证清单见表A.1；
d) 不应使用处于过期状态的许可证；
e) 应优先使用满足以下要求的开源许可证：
   1）授予专利权；
   2）允许商业使用；
   3）允许修改及修改后再发布；
   4）允许修改源代码后在个人和组织内部使用；
   5）该许可证下的代码允许被分发给第三方；
f) 应核查软件产品源代码使用是否符合其开源许可证，在专利、商标、著作权、源代码开源等方面的要求；
g) 应确定开源代码所遵循的开源许可协议和企业产品的盈利模式不存在冲突。

7.3.5.2 开源许可证声明合规

在引入开源软件前应检查开源许可证声明的合规性，开源许可证声明应包含以下内容：
a) 适用该许可证的软件名称和版本；
b) 开源许可证类型；
c) 许可证有效期；
d) 软件的著作权信息，包括软件作者或版权持有人的署名；
e) 用户使用、复制、修改、分发软件的具体条款和限制。

7.3.5.3 开源许可证条款合规

在引入开源软件前应核查开源许可证条款，开源许可证条款应具备以下几个方面的开源软件及其衍生品使用权利和限制的说明：
a) 对于基于开源软件产品对外提供服务方面的权利和限制；
b) 对于衍生产品许可证变更方面的权利和限制；
c) 对于衍生产品变更代码及变更后再开源方面的权利和限制；
d) 对于发布商业衍生产品方面的权利和限制；

e) 对于开源软件及其衍生产品版权归属方面的权利和限制；
f) 对于开源软件及其衍生产品专利归属方面的权利和限制；
g) 对于开源软件及其衍生产品商标归属方面的权利和限制。

7.4 安全评估

7.4.1 安全评估内容

应对开源项目成熟度进行评估，分析开源项目的可靠性：
a) 评估开源软件的可用性，应确保软件功能和操作应符合用户预期；
b) 评估开源软件的项目质量，应确保项目代码遵循行业开发标准、项目具备自动化测试工具、项目遵循严格的发布流程；
c) 评估开源软件的性能，应确保软件项目性能应能够满足正常的批量或并发使用需求；
d) 评估开源软件文档材料的规范性，应确保项目应具备规范的使用文档和开发文档；
e) 评估开源软件的社区建设情况，应确保项目的社区人数须达到一定数量，社区活跃度宜维持在较高的程度；
f) 评估开源软件的社区管理制度执行情况，应确保社区具备可执行的版本更新制度、贡献管理制度、公共渠道沟通和反馈制度；
g) 评估开源软件社区的类型，如第三方中立基金会建设、企业联合共建、单一企业建设和个人建设，应确保开源社区的持续运营能力；
h) 评估开源软件的服务与支持能力，应确保项目具备专职人员做社区服务，用户遇到问题须有途径获得社区帮助；
i) 评估开源软件的许可证信息，应确保项目应具备清晰的许可证说明；
j) 评估开源软件的用户验证成果，应确保项目应已经有用户在实际生产环境中进行使用；
k) 评估开源软件支持的语言类型，应确保开源软件所支持的开发语言满足所应用的项目需要；
l) 评估开源软件的通用性,应确保开源软件能支撑所应用项目的其他框架(如云计算、大数据等)；
m) 评估开源软件的可维护性，应确保具备支持开源软件开发、测试和使用的相关工具。

7.4.2 行业认可度

应在引入开源软件前进行安全评估，评估项应涵盖开源软件在电力行业的应用情况，包括以下内容：
a) 开源软件被业界认可和接受程度；
b) 应用开源软件的企业规模和数量；
c) 应用开源软件的业务系统安全状况；
d) 应用开源软件的业务系统的重要性；
e) 开源软件使用者对开源软件的满意程度。

7.4.3 社区活跃度

应在引入开源软件前进行安全评估，评估项应涵盖开源软件的社区活跃度，包括以下内容：
a) 开源软件受到关注、加星和拷贝等操作的情况；
b) 开源软件的提交与合并请求数量；
c) 开源软件近三年每季度贡献者数量变化情况，包括外部和内部的比例；
d) 开源软件近三年每季度提交数量变化情况；
e) 开源软件贡献者数量及其等级分布情况；
f) 开源项目采用者数量；

g) 开源项目的流行程度，包括项目网站的访问者，Github的关注者，社交网络关注者，新闻提及，活动频率等；
h) 开源项目的影响程度，包括贡献者的多样性，下载数，外部贡献公司数量，采用数量，衍生的商业产品的数量和质量；
i) 应关注开源软件近一年的版本发布数量和版本号；
j) 应关注开源软件近三个版本的发布时间间隔；
k) 应关注开源软件近一年每季度的代码贡献量变化情况；
l) 应关注开源软件近一年每季度的提交问题和修复问题数量变化情况。

7.4.4 开源软件关注度

应在引入开源软件前进行安全评估，评估项应涵盖开源软件的受关注程度，包括以下内容：
a) 相关的文献数量（包括学术文献、专利等）；
b) 相关的实体书和电子书数量；
c) 相关的微信、微博等公众号的文章数量；
d) 相关的论坛网页数量；
e) 相关词条在搜索引擎的检索结果数量；
f) 相关词条在技术社区的检索结果数量；
g) 相关词条在网络百科全书的记录情况。

7.4.5 贡献者情况

应在引入开源软件前进行安全评估，评估项应涵盖贡献者数量及影响力，包括以下内容：
a) 对开源软件源码有贡献或进行运营的公司信息；
b) 对开源软件源码有贡献的公司数量；
c) 参与软件开发的公司的影响力，评估其经营业绩情况、是否上市、市值估计等。

7.5 部署安装

开源软件部署安装应满足以下要求：
a) 应在部署安装开源软件前确保相关技术文档的完备性和质量；
b) 开源软件相关技术文档应包括功能说明、调用方法说明、部署说明、版本迭代说明等文件；
c) 开源软件配置应满足能源电力企业网络安全管理相关规定。

7.6 运行维护

7.6.1 软件更新

开源软件更新应满足以下要求：
a) 开源软件使用期间应定期检查其版本更新、配置变更情况；
b) 开源软件变更时应制定安全评估计划，确保不存在高危安全漏洞和不安全的配置项；
c) 针对影响面较广的开源软件，更改、调试等操作前应通知相关部门，预留充分的准备时间，制定详细的变更方案；
d) 应对开源软件的变更操作进行记录，包括操作时间、人员、结果等内容；
e) 在对软件进行更改、升级、配置等操作前，应做好充分备份或应急措施。

7.6.2 安全监测

应对开源软件及其所包含的组件、数据的使用过程中开展安全监测，包括以下内容：

a) 应对开源软件及其运行环境进行安全漏洞监测；
b) 应对私自卸载、改装、屏蔽漏洞扫描工具等违规行为进行管控；
c) 应对开源软件供应链进行监测，及时发现开源软件运行维护中断风险；
d) 应定期监测开源软件版本更新、发布频率、代码量变化等可能影响开源软件稳定性的情况。

7.6.3 入侵防御

运营者应采取相关技术措施，对已经尝试、正在发生或已经发生的开源软件入侵/攻击行为快速做出响应，并且中断、调整或隔离不正常或具有伤害性的攻击/非授权访问行为：

a) 应在关键网络节点处检测、防止或限制对开源软件发起的网络攻击行为；
b) 应采取技术措施对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析；
c) 当检测到攻击行为时,记录攻击源卫、攻击类型,攻击目标、攻击时间,在发生严重入侵事件时应提供报警。

7.6.4 漏洞管理

应对开源软件的安全漏洞进行统一管理，包括以下内容：

a) 开源软件使用过程中,所产生的漏洞应尽快根据漏洞结果报告的建议修复方式进行漏洞的修复工作，负责人有义务监督并管理整个漏洞修复的实施过程；
b) 应对开源软件已修复的漏洞、漏洞安全等级、造成生产事故情况、社会影响情况等内容进行记录留档；
c) 应对残留的高危漏洞进行定期监测，确保现有的安全加固方案有效；
d) 开源软件使用前后所产生的漏洞结果报告，应由专人负责统计和管理，经专业人员评估后第一时间提交给有关部门的负责人。

7.6.5 资产管理

7.6.5.1 SBOM 管理

应制定详细的开源软件物料清单，包含以下内容：

a) 应包含组件标识、时间戳、创建者信息、组件版本信息、哈希值、许可证信息、组件来源信息；
b) 应包含组件之间的直接及间接依赖关系；
c) 应包含清单标识、清单版本、清单创建者、清单创建工具、清单创建时间等清单信息；
d) 应包含许可证类型、版本、有效期、OST 认证的信息；
e) 应包含高危及以上漏洞信息，包括漏洞名称、漏洞等级、漏洞描述、漏洞处置方案、漏洞关联组件等；
f) 应包含组件获取方式、下载链接、是否自研等组件信息；
g) 应包含开源软件构建配置部署的相关信息；
h) 应包含父级组件、子级组件以及变体组件信息；
i) 应包含具有详细谱系信息的组件的数字签名信息。

7.6.5.2 供应链清单管理

应对开源软件供应链清单进行统一管理，清单包含以下内容：

a) 应包含软件信息、供应商信息、软件物料清单标识、软件获取时间、许可证数量等信息；
b) 应包含开源软件配置项信息。

7.6.6 威胁情报

应对开源软件安全威胁情报进行获取、识别提取、融合评价以及情报关联分析：

a) 开源威胁情报源应包括技术文章、暗网深网、web 开源信息、社交媒体、公共代码库 bug 及漏洞报告、论坛、博客等；
b) 应对威胁情报源进行定期监测，保证情报信息的时效性和准确性；
c) 应对获取到的威胁情报进行关联分析和去伪去重，按照规范格式生成情报信息；
d) 应对经研判确认真实的威胁情报建立预警机制，及时通知相关开源软件使用和运营部门进行排查处置；
e) 应定期对威胁情报的质量开展评价，根据评价结果优化情报管理机制。

7.6.7 应急响应

对于重要的业务，运营者应建立所使用的开源技术的备份方案，确保备份方案在安全和功能性方面都能满足业务要求。

7.6.8 二次开发

对开源软件代码进行二次开发时，应满足以下要求：

a) 电力企业对在开源代码基础上进行二次开发的软件项目，应采用模块形式进行链接，不宜将开源代码直接加入程序；
b) 技术部门应对软件开发使用的各种开源代码进行记录，包括项目名称、开源代码模块名称、版本、作者、出处、使用许可协议类型等，长期跟踪管理开源代码的使用情况。

附 录 A
（资料性）
开源许可证兼容性

A.1 开源许可证兼容性

备注：（下方内容可以对应到兼容性列表中有[1][2][3]的项）

[1]LGPLv2.1允许把代码重新按照GPLv2以后的GPL许可证发布。所以如果可以把LGPL的代码按照合适的GPL版本发布，即可组合两方代码。

[2]MPL的代码和GPL系列的代码组合的结果是MPL协议的代码遵循MPL协议，GPL系列的代码遵循GPL系列协议，所以原来按照MPL发布的那些文件还是可以使用MPL条款，组合而成的作品整体上可以按照GPL系列的许可证发布。

[3]查看双方的许可证协议中是否包含一个条款允许将协议升级到稍后的版本。例如，LGPLv2.1和GPLv3是不兼容的，但如果两方的许可证协议中都包含“可以升级到更高版本”的条款，那么LGPLv2.1就可以升级到LGPLv3，LGPLv3和GPLv3，AGPLv3是兼容的。

LGPL+与GPL+代表许可证授予用户将许可证升级到未来版本的权利，例如LGPLv2.1+意味着用户可以把许可证升级到LGPLv2.1之后的版本。

表 A.1 合并/修改代码的许可证兼容性

两方代码是否可以组合	MIT License	BSD 2-Clause	BSD 3-Clause	Apache 2.0	MPL 2.0	LGPL v2.1	LGPL v2.1+	LGPL v3	GPL v2	GPL v2+	GPL v3	AGPL v3
MIT License	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以
BSD 2-Clause	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以
BSD 3-Clause	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以	可以
Apache 2.0	组合需遵循 Apache 2.0	组合需遵循 Apache 2.0	组合需遵循 Apache 2.0	可以	可以	组合需遵循 GPL v3[1]	组合需遵循 GPL v3[1]	可以	不可以	组合需遵循 GPL v3[3]	可以	可以
MPL 2.0	组合需遵循 MPL 2.0	组合需遵循 MPL 2.0	组合需遵循 MPL 2.0	组合需遵循 MPL 2.0	可以	可以[2]	可以[2]	可以[2]	可以[2]	可以[2]	可以[2]	可以[2]
LGPL v2.1	组合需遵循 LGPL v2.1	组合需遵循 LGPL v2.1	组合需遵循 LGPL v2.1	组合需遵循 LGPL v2.1	可以[2]	可以	组合需遵循 LGPL v2.1	组合需遵循 GPL v3[1][3]	可以	可以	可以	可以
LGPL v2.1+	组合需遵循 LGPLv2.1+	组合需遵循 LGPLv2.1+	组合需遵循 LGPLv2.1+	组合需遵循 LGPLv2.1+	可以[2]	可以	可以	可以	可以	可以	可以	可以
LGPL v3	组合需遵循 LGPLv3	组合需遵循 LGPLv3	组合需遵循 LGPLv3	组合需遵循 LGPLv3	可以[2]	组合需遵循 GPLv3[1][3]	组合需遵循 LGPLv3	可以	不可以	组合需遵循 GPLv3[3]	可以	可以
GPLv2	组合需遵循 GPLv2	组合需遵循 GPLv2	组合需遵循 GPLv2	组合需遵循 GPLv2	可以[2]	组合需遵循 GPLv2[1]	组合需遵循 GPLv2[1]	不可以	可以	组合需遵循 GPLv2	不可以	不可以

GPLv2+	组合需遵循GPLv2+	组合需遵循GPLv2+	组合需遵循GPLv2+	组合需遵循GPLv2+	可以[2]	组合需遵循GPLv2+[1]	组合需遵循GPLv2+[1]	组合需遵循GPLv3[1][3]	可以	可以	可以	可以
GPLv3	组合需遵循GPLv3	组合需遵循GPLv3	组合需遵循GPLv3	组合需遵循GPLv3	可以[2]	组合需遵循GPLv3[1]	组合需遵循GPLv3[1]	组合需遵循GPLv3[1][3]	不可以	组合需遵循GPLv3[3]	可以	可以
AGPLv3	组合需遵循AGPLv3	组合需遵循AGPLv3	组合需遵循AGPLv3	组合需遵循AGPLv3	可以[2]	组合需遵循AGPLv3[1][3]	组合需遵循AGPLv3[1][3]	组合需遵循AGPLv3[1][3]	不可以	组合需遵循AGPLv3[3]	组合需遵循AGPLv3	可以

A.2开源许可证特性

A 表 2 常用开源许可证的特性

开源许可证	商业使用	分发代码	内部使用	专利授权	合并代码	修改代码	使用库	不允许修改许可协议	许可证的分类
MIT License	√	√	√						开放型许可证
BSD 2-Clause	√	√	√						
BSD 3-Clause	√	√	√						
Apache 2.0	√	√	√	√					
MPL 2.0	√	√	√	√	√	√		需分析使用场景	弱传染性许可证
LGPLv2.1	√	√	√		√	√		需分析使用场景	
LGPLv3	√	√	√	√	√	√		需分析使用场景	
GPLv2	√	√	√		√	√	√	√	传染性许可证
GPLv3	√	√	√	√	√	√	√	√	
AGPLv3	√	√	需分析网络使用场景	√	√	√	√	√	强传染性许可证

参 考 文 献

[1] GB/T 11457-2006 信息技术 软件工程术语
[2] GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求
[3] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[4] GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
[5] GB/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求
[6] GB/T 36324-2018 信息安全技术 工业控制系统信息安全分级规范
[7] GB/T 37932-2019 信息安全技术 数据交易服务安全要求
[8] GB/T 42927-2023 金融行业开源软件评测规范
[9] SJ/T 11235 软件能力成熟度模型
[10] T/SIA 003-2017 软件产品评估标准
[11] Q/CSG 2152003-2021 中国南方电网有限责任公司网络安全管理办法
[12]《开源许可证兼容性指南》