ICS 国际标准分类号
CCS 中国标准文献分类号

团　　体　　标　　准

T/CES XXX-XXXX

电力数据元件安全审核规范

Specification of security auditing for power data component

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电工技术学会　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》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。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会能源智慧化工作组归口。

本文件起草单位国网信通亿力科技有限责任公司、中国计算机学会数据治理与发展技术委员会、新疆思极信息技术有限公司、中电（郑州）数据产业有限公司。

本文件主要起草人：解福文、陆志鹏、陈婧、舒路、郑忠龙、朱友卫、陈琳、国丽、张昭、刘文亮、郑剑毅、梅超、赵宁、肖润南、韩如意、王飞、周文婷、张海波、孙若寒、马文龙。

本文件为首次发布。

电力数据元件安全审核规范

1 范围

本文件规定了电力数据元件安全审核的总体要求、安全审核流程、安全审核技术要求和人员管理要求。

本文件适用于数据运营商进行电力数据元件的安全审核。

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 30276—2020 信息安全技术 网络安全漏洞管理规范

GB/T 34943—2017 C/C++语言源代码漏洞测试规范

GB/T 34944—2017 Java语言源代码漏洞测试规范

GB/T 34946—2017 C#语言源代码漏洞测试规范

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 39412—2020 信息安全技术 代码安全审计规范

GB/T 43697—2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

代码安全审计 code security audit

对代码进行安全分析，以发现代码安全缺陷或违反代码安全规范的动作。

[来源：GB/T 39412—2020，3.1.1]

3.2

脚本恶意程序 malicious script program

使用脚本语言编写的，并在脚本执行环境中运行的恶意程序。

[来源：GB/T 37988—2019，2.8]

3.3

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

[来源：GB/T 43697—2024，3.5]

3.4

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注1：敏感个人信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、用电信息、交易信息、14岁以下（含）儿童的个人信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

[来源：GB/T 35273—2020，3.2，有修改]

3.5

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[来源：GB/T 35273—2020，3.14]

3.6

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

[来源：GB/T 35273—2020，3.15]

3.7

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019，3.12]

3.8

电力数据元件安全审核 security auditing for power data component

通过对电力数据元件开发过程中影响电力数据资源申请、电力数据元件模型开发、电力数据元件发布三阶段的数据安全因素进行审核的活动。

3.9

数据运营商 data operator

对数据进行收集、处理、存储、保护、使用和处置等活动，并提供数据价值开发和运营管理的市场主体。

3.10

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康或公共安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：GB/T 43697—2024，3.2，有修改]

3.11

电力数据元件 power data component

具有一定主题，通过对电力数据资源脱敏处理后，根据需要由若干相关字段形成的数据集或由电力数据资源的关联字段通过建模形成的数据特征。

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

Apache Shiro：强大且易用的 Java 安全框架，提供了一系列的安全特性，包括认证、授权、密码学、会话管理等。

FastJson：阿里巴巴的开源库，用于对 JSON 格式的数据进行解析和打包。

Log4j2：Java 日志框架（Logging for Java）

hash 算法：散列算法（Hash Algorithm）

5 安全审核流程

5.1 流程规范

电力数据元件安全审核流程见图1，电力数据元件安全审核分三个阶段，电力数据资源申请阶段、电力数据元件模型开发阶段、电力数据元件发布阶段。数据运营商对每个阶段存在的安全风险进行审核。

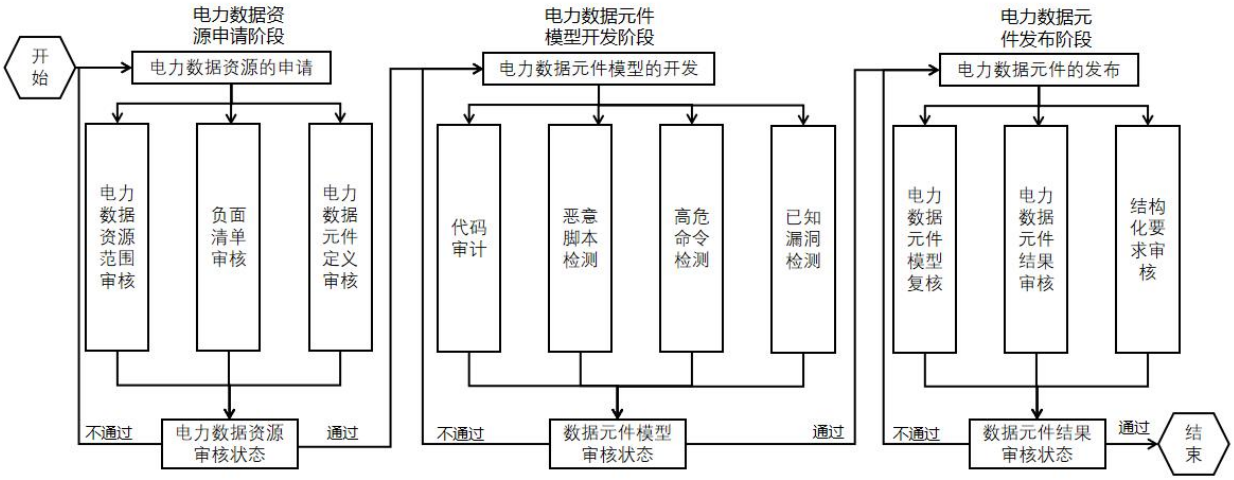

图1 电力数据元件安全审核流程

5.2 电力数据资源申请审核

数据运营商对电力数据资源范围、负面清单、电力数据元件定义进行审核。当该阶段电力数据范围、负面清单、电力数据元件定义等审核项满足要求时，电力数据资源审核状态为通过；否则不通过，返回重新申请电力数据资源，当对审核结果有异议时，可内提交书面申诉材料，由数据运营商进行复核并作出最终裁定。

电力数据资源合规率指标：（电力数据资源满足要求的审核项数/电力数据资源总审核项数）×100%

目标值：100%

5.3 电力数据元件模型开发审核

数据运营商对电力数据元件模型进行代码审计、脚本恶意程序检测、高危命令检测和已知漏洞检测。当该阶段代码审计、脚本恶意程序检测、高危命令检测和已知漏洞检测等审核项满足要求时，元件模型审核状态为通过；否则不通过，返回重新开发电力数据元件模型，当对审核结果有异议时，可内提交书面申诉材料，由数据运营商进行复核并作出最终裁定。

电力数据元件模型开发合规率指标:(电力数据元件模型通过审核的检测项数/电力数据元件模型总检测项数)×100%

目标值：100%

5.4 电力数据元件发布审核

数据运营商对电力数据元件进行电力数据元件模型复核、电力数据元件结果审核和结构化要求审核。当该阶段电力数据元件模型复核、电力数据元件结果审核和结构化要求等审核项满足要求时，元件结果审核状态为通过，安全审核结束；否则不通过，重新发布数据元件，当对审核结果有异议时，可内提交书面申诉材料，由数据运营商进行复核并作出最终裁定。

电力数据元件发布合规率指标:（电力数据元件通过审核的项数/电力数据元件总审核项数）×100%

目标值：100%

6 安全审核技术要求

6.1 电力数据资源申请阶段

6.1.1 电力数据资源范围审核

数据运营商对电力数据资源和电力数据元件开发人员进行安全管控，包括以下保护措施：

a) 对电力数据资源进行分类分级。数据分类参考 GB/T 38667，按照个人信息、公共数据、企业数据三个维度；数据分级根据《数据安全法》相关法律法规分级要求，电力数据从高到低分为核心数据、重要数据和一般数据；
b) 对电力数据资源重要数据、个人信息和商业秘密进行检测时，数据运营商应对数据进行数据脱敏，常见方法见附录 A 中表 A.1；
c) 申请的电力数据资源范围与电力数据元件开发人员的权限保持一致。

6.1.2 负面清单审核

数据运营商须尽到电力数据资源审核义务，包括以下保护措施：

a) 建立电力数据资源负面清单；
b) 申请的电力数据资源不含负面清单内容。

6.1.3 电力数据元件定义审核

数据运营商须尽到电力数据元件定义审核义务，包括以下保护措施：

a) 电力数据元件的定义符合电力数据元件元数据要求；
b) 电力数据元件的名称和描述内容不含违反国家法律法规，危害国家安全统一、国家主权和领土完整、民族团结、社会稳定、公序良俗、社会公德以及侮辱、诽谤、淫秽等信息。

6.2 电力数据元件模型开发阶段

6.2.1 代码审计

针对电力数据元件模型代码的源码或二进制文件中的代码质量以及形成漏洞的各种脆弱性因素进行检测。具体代码安全审计要求按照GB/T 39412—2020中的审计方法执行。

6.2.2 脚本恶意程序检测

针对电力数据元件模型代码源码或二进制文件识别检测脚本恶意程序并处理，检测内容包含但不限于：

a) 反弹 Shell 类恶意代码；
b) 命令注入类恶意代码；
c) 代码执行类恶意代码；
d) 非法文件上传类恶意代码。

6.2.3 高危命令检测

针对彻底删除、清除、关闭、切换类命令进行检测，避免因操作不当导致系统运行异常、重要文件被删除、配置被清除、无法登录等现象发生。

6.2.4 已知漏洞检测

检测Java、Python、C/C++等常见语言已知漏洞，包括但不限于Log4j2、Apache Shiro、Strusts2、Dom4J、FastJson、FasterXML、Jackson-databind、Pickle库、Subprocess库、野指针、内存泄漏等漏洞，并能根据网络环境变化及时调整更新漏洞库。已知漏洞管理按照GB/T 30276—2020中的管理办法执行。已知漏洞检测应符合但不限于GB/T 34944—2017、GB/T 34946—2017、GB/T 34943—2017中的漏洞测试内容。通过与权威漏洞数据源（如 CVE、NVD、CNVD 等）同步更新，实现漏洞库动态更新，建立漏洞状态动态维护机制，保障漏洞及时、准确修复。

6.3 电力数据元件发布阶段

6.3.1 电力数据元件模型复核

电力数据元件在生产过程不断加载电力数据元件模型，保证电力数据元件模型能安全运行，因此对电力数据元件模型进行复核。针对电力数据元件模型进行以下安全审核检测：

a) 消除电力数据元件模型检测出来的安全风险；
b) 电力数据元件模型二次审核。

6.3.2 电力数据元件结果审核

针对电力数据元件结果应进行以下安全审核检测：

a) 电力数据元件结果是否含违反国家法律法规，危害国家安全统一、国家主权和领土完整、民族团结、社会稳定、公序良俗、社会公德、电力安全以及侮辱、诽谤、淫秽等信息；
b) 电力数据元件结果是否含国家重要数据、个人敏感信息或商业秘密，常见敏感信息见附录 A 中表 A.2；
c) 电力数据元件结果与电力数据资源的相似性和相关性；
d) 新发布的电力数据元件与已有电力数据元件的关联性；
e) 电力数据元件结果是否可逆。

注1：相似性检测包括原始数据字段与元件结果中字符型内容重复度。相关性检测主要针对元件模型中对单个数值型原始特征采用函数变换如线性变换、平方等方式进行开发，这种容易通过元件结果反推原始数据。

注2：不能逆检测包括防止元件开发商通过加密手段、同分布变化、拆分或合并等手段将原始数据复原，比如采用

加密算法生成元件再逆回原始数据、将原始数据拆成多个部分分批出去、将多组原始数据拼接出去等。

6.3.3 结构化要求审核

检测电力数据元件是否符合电力数据元件的结构要求标准。

7 人员管理职责要求

电力数据元件的安全审核由数据运营商进行统筹管理，安排专职技术人员承担具体安全审核管理工作。安全审核人员应具备去标识化、匿名化、代码审计和数据水印等安全专业知识，熟悉电力数据元件安全审核管理相应的操作流程。安全审核人员应具备注册信息安全专业人员（CISP）、注册信息系统审计师（CISA）等资质认证。

安全审核人员主要职责包括：

a） 对电力数据元件开发商资质和授权使用的电力数据资源范围进行审查和管理；
b） 审核电力数据元件模型安全性和可靠性；
c） 审核电力数据元件是否包含敏感个人信息或国家重要数据；
d） 人工复核电力数据元件审核结果；
e） 熟悉国家数据安全相关的法律法规；
f） 客观记录并反馈安全缺陷问题，不应隐瞒；
g） 对数据、代码等相关内容保守秘密，不应泄露相关信息。

附 录 A
（资料性）
数据样本脱敏方法与常见脱敏信息

A.1 数据样本脱敏方法

常见的样本脱敏方法见表A.1。

表 A.1 常见数据样本脱敏方法

脱敏方法	说明	示例
遮蔽	保持数据长度和格式不变，对部分内容进行遮掩	如：掩盖手机号码的第四位到第七位，13500010001→135****0001
替换	以敏感数据作为输入，通过特定函数形成新的替换数据	如：女性用字母Z代替，女→Z
规整	将数据按照大小规整到预定义的多个档位	如：0-10 万、10-30 万、30 万以上
散列	对原始数据取散列值，使用散列值来代替原始数据	常用 hash 算法，如 SM3 等 如：123456→ 3de741f445dd357bea4e6c3fe6437036f62b5e3ec0f00d62796edb4305ed627f
重写	参考原始数据的特征，重新生成数据。重写与整体替换较为类似，但替换后的数据与原始数据存在特定规则的映射关系，而重写生成的数据与原始数据则一般不具有映射关系	对居民身份证号码、电话号码，可在一定范围内按照规则随机生成构造数据
匿名化	使用K匿名化和L多样性的方法	K匿名化通过扰动和泛化的方法使得每一个准标识符都至少对应k个实例，使数据主体不能唯一识别

A.2 敏感信息举例

常见的敏感信息见表A.2。

表 A.2 常见敏感信息

类别	敏感字段
个人基本信息	居民身份证号码
	社会保障号码
	军官证
	驾驶证
	工作证
	出入证
	居住证
	护照/台胞证等有效证件号码

表A.2　常见敏感信息（续）

个人基本信息	电话号码
	微信、QQ等即时通信账号
	电子邮箱
	姓名
	国籍
	种族
	民族
	宗教信仰
	出生日期或年龄
	工作单位
	婚姻状况
	健康状况
	学历
	常住户口所在地住址或家庭地址
	违法犯罪记录
网络身份标识信息	网络身份账号
	网络地址
	个人数字证书
个人健康信息	病症
	住院志
	医嘱单
	检验报告
	手术及麻醉记录
	护理记录
	用药记录
	药物食物过敏信息
	生育信息
	以往病史
	诊治情况
	家族病史
	现病史
	传染病史
	体重
	身高
	肺活量
个人教育工作信息	个人职业
	职位
	工作单位
	学历

表A.2　常见敏感信息（续）

个人教育工作信息	学位
	教育经历
	工作经历
	培训记录
	成绩单等
个人财产信息	银行账户
	鉴别信息（口令）
	存款信息（包括资金数量支付收款记录等）
	信贷记录
	征信信息
	交易记录和消费记录流水等
	虚拟货币
	虚拟交易
	游戏类兑换码等虚拟财产信息
	收入和支付记录
	证券账户数据
	房屋登记数据
	车辆登记数据
	保险单
个人通信信息	通信记录和内容
	短信
	彩信
	电子邮件以及描述个人通信的数据等
联系人信息	通讯录
	好友列表
	群列表
	电子邮件地址列表
个人上网记录	个人上网记录
个人常用设备	硬件序列号
	设备MAC地址
	软件列表
	唯一设备识别码
个人位置信息	行踪轨迹
	精准定位信息
	住宿信息
	经纬度
商业秘密	企业客户数据
	财务数据
	产销数据

表A.2　常见敏感信息（续）

	货源数据
	工艺配方
	技术方法
	计算机程序
经营业务信息	重大决策
	经营规划
	生产工艺
	流程配方
	知识产权
	合同名称
	合同编号
	合同金额
	合同关键技术
	单位名称
	法人及股东信息
	股东出资
	公司注册资本
	方案图纸
	内部程序的源代码
	内部的安全管理策略
	重要会议纪要
	财务预算报告及各类财务报表、统计报表
发电信息	月度装机容量
	火电发电量
	火电燃煤发电量
	火电燃气发电量
	火电燃油发电量
	火电供热发电量
	水电发电量
用电信息	如年度全社会用电量
	用户名称
	用户用电量
	月均用电金额
	各用电分类的尖峰电价
	各用电分类的低估电价
	月度最大负荷
	季度最大负荷
	年度最大负荷
电力交易信息	月度申报电量

	各交易时段成交电价及均价
	交易类型
	交易量
	交易占比
	市场成员名称
	日结算电类
	日结算电价
内部管理信息	增值税税号
	增值税账号
	内部的质量管理方法
	对客户定价方法及销售策略
	网络管理员账号
	网络管理员密码
	业务服务器账号
	业务服务器密码
	服务站点用户名
	服务站点密码
人事管理信息	人事档案
	职员工资性收入
	对外签署的各种协议

参 考 文 献

[1] GB/T 35274—2023 信息安全技术 大数据服务安全能力要求
[2] GB/T 27029—2022 合格评定 审定与核查机构通用原则和要求
[3] GB/T 30283—2022 信息安全技术 信息安全服务 分类与代码
[4] GB/T 31506—2022 信息安全技术 政务网站系统安全指南
[5] GB/T 41388—2022 信息安全技术 可信执行环境 基本安全规范
[6] GB/T 41389—2022 信息安全技术 SM9密码算法使用规范
[7] GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
[8] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[9] GB/T 35273—2020 信息安全技术 个人信息安全规范
[10] GB/T 38667—2020 信息技术 大数据 数据分类指南
[11] GB/T 37964—2019 信息安全技术 个人信息去标识化指南
[12] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型