燃气行业大数据平台软件安全开发与运维优化

胡海迪

南京港华燃气有限公司，江苏南京，210000；

摘要：本研究基于软件全生命周期视角，聚焦燃气行业大数据平台安全开发与运维痛点。通过梳理行业实践与真实案例，发现部分企业存在开发流程简化、运维体系脱节等问题，安全防护与业务需求失衡。结合《城镇燃气工程智能化技术规范》等标准，提出嵌入安全校验的开发流程与动态运维优化策略，构建“开发-测试-部署-运维”闭环防护体系。实证表明，该方案可降低软件缺陷密度，提升平台抗攻击能力，为燃气行业数字化转型提供安全支撑。

关键词：燃气行业；大数据平台；安全开发；运维优化；网络安全

DOI：10.69979/3029-2727.26.03.079

引言

燃气行业大数据平台承载用户信息、管网运行、气量调度等敏感数据，软件安全直接关乎城市能源供给稳定。数字化转型深入推进背景下，平台功能迭代加速，安全风险也同步攀升。2020 年美国某天然气运营商遭勒索软件攻击（美国 CISA 公告 2020-02），造成 OT 网络瘫痪，无法获取实时运行数据。实则暴露了行业软件安全开发缺失、运维响应滞后的共性问题[1]。亟需从开发源头植入安全理念，同步优化运维机制，平衡业务效率与安全防护，这也是本研究的核心诉求。

本研究结合《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019，以下简称《等级保护基本要求》），融入 DevSecOps 开发理念，通过案例验证与实践总结，提出可操作的优化路径，弥补行业软件全流程管控短板[2]。

1 燃气行业大数据平台安全现状与核心矛盾

1.1 行业安全现状与突出问题

当前燃气行业大数据平台多集成GIS 系统、SCADA 系统等核心模块，数据交互频繁且类型复杂。《能源行业数据安全管理办法(试行)》（国能发安全〔2021〕36 号）明确，存储核心数据的平台需落实四级等保要求[3]。令人担忧的是，部分企业为压缩成本简化安全测试环节，仅在软件开发后期补充安全校验，导致潜在风险遗留至运维阶段。2024 年某中小型燃气企业便因省略模块间接口安全测试，平台上线后出现数据交互异常，泄露近千条用户缴费信息，被监管部门责令整改，这类因流程简化引发的安全事件在行业内占比超 20%，直观反映出流程管控缺位带来的严峻风险[4]。

从实践来看，北京燃气通州呼叫中心项目通过 DevOps 持续交付 2 级评估，搭建起全流程开发运维体系，为行业提供了可借鉴的范本。但多数中小型平台仍存在安全投入不足、技术储备薄弱等问题，安全防护水平参差不齐[5]。

1.2 核心现实矛盾

企业对开发效率的追求与安全流程的繁琐形成突出矛盾。短期实践中，部分团队为加快版本迭代，不仅跳过代码安全审计、渗透测试等环节，更将代码走查简化为形式化签字，如同部分审计机构未执行现场程序便出具报告的违规行为，仅依赖开发人员自检完成安全核验，将安全责任转嫁至运维端。这类行为易导致 SQL 注入、权限越界等隐蔽漏洞遗留，而运维团队缺乏开发阶段的信息同步，难以精准识别潜在风险点，形成“开发不管安全，运维被动兜底”的恶性循环[6]。

实践中还发现，行业标准落地存在偏差。《城镇燃气工程智能化技术规范》（CJJ/T268-2017，以下简称《燃气智能化规范》）要求安全与智能化系统同步建设，但部分项目因前期规划不足，安全模块与业务模块兼容性不足，增加运维难度[7]。

2 软件安全开发全流程优化路径

2.1 需求阶段安全需求梳理与合规规划

需求分析阶段同步开展安全需求梳理，结合燃气行业数据特性，明确核心数据加密、访问权限划分等要求。依据《工业控制系统信息安全防护指南》（工信部信软〔2016〕338 号，以下简称《工控安全指南》），建立

安全需求优先级评估机制，将管网运行数据、用户隐私数据保护列为最高优先级[8]。

采用安全需求矩阵梳理要点，矩阵维度按“数据级别-功能模块-威胁类型”三维构建，明确每个功能模块的量化安全指标：核心管网运行数据采用 AES-256 加密算法，接口访问频率限制为单 IP 每分钟不超过 60 次，用户隐私数据脱敏后留存时长不超过 90 天。同步对接《等级保护基本要求》中“数据分类分级保护”条款，结合燃气行业数据仓分层特性，明确 ods 源数据层、dwd 明细数据层、dws 汇总数据层的差异化安全管控要求，ods 层需保留原始数据加密备份，dwd 层强化字段级脱敏，dws 层限制关联查询权限，开展全链路合规性预校验。同时联动运维团队参与需求评审，结合过往运维中出现的接口权限混乱、加密密钥管理薄弱等问题，提前预判运维阶段可能出现的安全隐患，形成需求评审意见清单并闭环整改。

2.2 开发阶段安全嵌入实践

引入 DevSecOps 开发模式，将安全工具集成至开发流水线。在编码环节，配置 SonarQube 等主流静态代码分析工具，实时扫描语法漏洞、逻辑缺陷，针对空指针引用、未授权访问等高危代码自动拦截并标注风险等级。针对燃气平台常用的 Java、Python 语言，定制行业专属代码规范，明确 Java 代码安全命名、异常捕获机制，Python 数据传输加密校验规则，重点防范 SQL 注入、跨站脚本及数据脱敏不彻底等攻击场景，要求核心业务模块代码安全扫描通过率必须达到 98%以上方可提交。

模块开发完成后，开展单元安全测试，由开发人员与安全人员协同验证。针对 Java 语言选用 JUnit 框架，Python 语言则采用 TestNG 框架，搭建针对性单元安全测试体系，设计覆盖正常业务流、异常输入、权限越界等 8 类场景的测试用例，重点校验核心函数的参数合法性与返回值安全性。同步启动代码审查流程，通过 GitLab MergeRequest 记录问题，按“阻塞漏洞-逻辑缺陷-风格问题”分级标注优先级，高优先级问题直接阻塞代码合并，修复后需经安全人员复核签字方可放行。借鉴北京燃气实践经验搭建自动化测试环境，集成 Postman 工具实现 API 接口批量校验，通过 Newman 命令行工具将测试流程嵌入 CI/CD 流水线，自动生成测试报告并标注漏洞类型与修复建议，测试与审查均达标后方可进入集成阶段，确保单元层面安全无死角。

2.3 测试与部署阶段安全验证及风险管控

测试阶段强化渗透测试与压力测试融合，采用黑盒测试与白盒测试双模式开展检测：黑盒测试模拟外部黑客无差别攻击，重点检测用户登录、数据查询等公开接口的抗攻击能力；白盒测试基于源码层面，针对 SCADA 系统与大数据平台的对接模块开展专项检测，排查数据交互过程中的逻辑漏洞。针对大数据存储模块，专项开展数据加密有效性测试，验证传输加密、存储加密及密钥轮换机制的合规性，确保符合《等级保护基本要求》中数据传输与存储的安全要求。对测试发现的漏洞按 CVSS 评分分级处置：评分≥9.0 的高危漏洞，24 小时内完成整改后用 Nessus 工具专项复测，漏洞消除率 100%方可闭环；4.0-8.0 为中危漏洞，纳入下一轮迭代计划；<4.0 为低危漏洞，评估影响后选择性整改。

部署阶段采用灰度发布模式，按“10%内部用户→30%区域用户→60%全量用户”分三批次上线功能模块，每批次上线后预留 24 小时观察期。同步启用安全监测工具，实时采集接口响应时长、异常访问 IP 数量、数据传输完整性等指标。回滚机制采用“版本快照+数据备份”双重保障：部署前对系统进行全量快照，备份核心数据库并离线存储；一旦监测到数据泄露、接口瘫痪等安全问题，触发自动回滚指令，3 分钟内恢复至稳定版本，同时记录异常日志供后续溯源分析，最大限度降低部署对业务运营的影响。

3 运维安全体系迭代与优化策略

3.1 构建动态运维监测与闭环管理体系

搭建集中式安全管理中心，整合日志分析、流量监测、漏洞扫描等工具，实现对平台运行状态的实时监控。针对燃气平台 7×24 小时运行特性，设置分级告警机制，高危告警 15 分钟内响应，中低危告警 4 小时内处置。

定期开展安全巡检，每月进行一次全量漏洞扫描，每季度开展一次应急演练。建立巡检台账，对发现的问题闭环管理，避免同类问题重复出现。

3.2 优化运维与开发协同机制

建立开发与运维团队的常态化沟通机制，每周召开安全复盘会议，同步漏洞整改情况与功能迭代计划。将运维过程中发现的安全问题反馈至开发端，纳入下一轮开发优化需求，形成“开发-运维”双向反馈闭环。

事实上，运维团队需参与软件开发全流程评审，提

前掌握模块架构与安全设计，提升运维过程中的风险识别与处置能力。同时开发团队预留运维接口，便于运维工具对接与安全配置调整。

4 案例验证与实践效果

以2023年北京燃气通州呼叫中心建设项目为案例，该项目服务通州区域 12 万燃气用户，核心需求是实现呼叫应答、故障报修、气量查询等业务与大数据平台的实时联动，开发难点集中在多系统对接的数据一致性保障与接口安全防护。项目采用 DevOps 开发模式嵌入安全管控流程，将 SonarQube、JUnit 等工具集成至开发流水线，同时在终端接入层内置 SE-SIM 安全芯片，支持国密 SM4 算法实现端到端加密。针对 SCADA 系统与呼叫平台的对接模块，额外增设数据脱敏前置校验环节，从源头避免敏感数据直传风险。项目依据《DevOps 成熟度模型》通过持续交付 2 级评估，实施后需求耗费时长缩短 30%，编译构建时长压缩 40%，软件缺陷密度降至 0.8 个/千行代码，较行业平均水平低 0.5 个/千行代码，核心数据传输加密合规率达 100%。

项目运维阶段构建动态监测体系，针对燃气呼叫中心高频数据交互场景，实现 SQL 注入、跨站脚本等攻击行为的实时拦截，累计拦截异常访问请求 1200 余次，攻击拦截率达 99.2%。通过日志分析工具精准定位 3 处潜在权限越界漏洞，漏洞处置效率较行业平均水平提升 50%，处置时长缩短 2.5 小时。同时实现核心数据加密合规率 100%，系统全年可用性达 99.98%，未发生数据泄露、系统瘫痪等安全事件。该案例充分证明，开发阶段安全管控与运维优化的深度融合，既能提升开发效率，又能强化平台在真实业务场景中的安全防护能力，具备较强的行业推广价值。

5 结论与展望

燃气行业大数据平台软件开发阶段的安全管控与运维优化，需打破开发与运维的割裂壁垒，构建全生命周期安全管控体系。本研究提出的安全开发路径与运维策略，结合行业标准与实践案例，可有效破解企业安全与效率的平衡难题。

短期实践中，企业需加大安全技术投入与人员培训，逐步落实全流程安全管控，可优先针对核心业务模块推广 DevSecOps 模式，组建专职安全开发团队；长期来看，需紧跟行业标准更新与技术发展，将零信任架构、AI 安全检测等前沿技术融入平台开发——零信任架构通过最小权限分配、持续身份核验强化访问安全，AI 技术借鉴光纤感知领域的算法经验，实时识别异常编码行为与潜在攻击链路，提升安全防护的智能化水平。同时应建立行业安全开发共享机制，规避同类漏洞重复出现，唯有将安全理念深度融入软件开发与运维各环节，才能为燃气行业数字化转型筑牢安全根基。

参考文献

[1]刘铭炎.智慧燃气大数据平台的建设及应用[J].化工管理,2023(20):80-83.
[2]杜萍.基于大数据的安全管理系统在燃气发电厂中的应用[J].无线互联科技,2018(20):153-155.
[3]刁洪涛,虞维超,王凯鸿,等.天然气管网运行数据应用平台建设[J].油气储运,2024,43(10):1129-1137.
[4]孙广义,李德龙,刘丽.燃气工程智能化运维体系构建及风险预警机制研究[J].美食,2025(13):249-250.
[5]戴绘,邵郁文.中小型燃气企业网络安全等级保护实践与探索[J].天津科技,2024,51(9):52-55.
[6]陈国,高翔,戴旭.基于密码技术的智能燃气行业物联网数据安全体系架构与应用[J].城市燃气,2021(S01):100-103.
[7]李中阳.基于NB-IoT的智慧燃气物联网系统框架设计与研究[J].自动化与仪表,2023,38(5):102-106.
[8]郭东,许明,张丽.燃气行业 SCADA 系统安全防护研究[J].化工设计通讯,2020(8):154-154,168.