文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

信号系统软件升级风险评估指标体系构建与应用

梁爽　魏强　杨松
北京市地铁运营有限公司通信信号分公司
DOI:10.32629/etd.v6i11.17501

[摘　要] 信号系统作为轨道交通、工业控制等领域的核心中枢,软件升级是实现功能迭代与漏洞修复的关键手段,但升级过程伴随的风险可能引发系统瘫痪等严重后果。本文聚焦信号系统软件升级风险评估,基于全流程视角识别风险因素,运用故障树分析法提取关键风险并梳理传导机制。结合层次分析法与熵权法确定融合权重,建立综合评估模型。通过轨道交通信号系统升级案例验证,模型可精准识别高风险点,评估结果为风险防控提供科学依据,提升软件升级安全性与可靠性。
[关键词] 信号系统；软件升级；风险评估
中图分类号：U284　文献标识码：A

Construction and Application of a Risk Assessment Indicator System for Signal System Software Upgrades

Shuang Liang　Qiang Wei　Song Yang
Communication and Signal Branch, Beijing Metro Operation Co., Ltd.

[Abstract] As the core hub in fields such as rail transit and industrial control, signal systems rely on software upgrades for functional iteration and vulnerability remediation. However, the upgrade process carries risks that can lead to severe consequences, such as system failure. This paper focuses on risk assessment for signal system software upgrades. From a full-process perspective, risk factors are identified, and key risks along with their propagation mechanisms are extracted using fault tree analysis. A comprehensive evaluation model is established by determining integrated weights through the combination of the Analytic Hierarchy Process (AHP) and entropy weight method. Validated through a case study of a rail transit signal system upgrade, the model accurately identifies high-risk points. The assessment results provide a scientific basis for risk prevention and control, enhancing the safety and reliability of software upgrades.
[Key words] Signal System; Software Upgrade; Risk Assessment

引言

在轨道交通网络化运营与工业自动化深度发展的背景下,信号系统对运行精度与稳定性的要求持续提升,软件升级成为适配新场景、修复潜在漏洞的常态化工作。然而,信号系统软件具有实时性强、耦合度高的特性,升级过程中任何环节的疏漏都可能引发连锁反应,如某城市地铁信号系统升级时因兼容性问题导致运营中断40分钟,造成重大经济损失与社会影响。因此,构建科学的风险评估指标体系与评估模型,对保障信号系统软件升级安全、降低运营风险具有重要现实意义,也是推动信号系统运维规范化的必然需求。

1 信号系统软件升级风险评估理论基础

1.1信号系统软件升级核心特性

信号系统软件升级区别于通用软件,其核心特性体现在三个方面。一是强实时性要求,升级过程需严格控制中断时间,轨道交通信号系统升级通常需在夜间“天窗期”完成,单次升级中断不得超过4小时,否则将影响次日运营。二是高耦合性特征,软件与硬件设备、子系统间存在紧密关联,某地铁信号系统升级时曾因软件与联锁机不兼容,导致整个信号联锁系统失效。三是高可靠性标准,升级后软件需满足故障导向安全原则,任何功能异常都需触发安全保护机制。此外,升级流程具有不可逆性,部分老旧系统缺乏完善的回滚机制,一旦升级失败将难以恢复至初始状态,这些特性决定了信号系统软件升级必须建立严谨的风险管控体系。

1.2软件升级风险定义

结合信号系统特性,软件升级风险定义为在软件升级全流程中,因技术缺陷、管理疏漏、环境干扰等不确定因素,导致升级失败、系统功能异常、安全性能下降,进而引发运营中断、财产损失或安全事故的可能性及其影响程度的综合度量。该风险

文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

具有双重属性,一方面体现为风险发生的概率,如代码漏洞出现的几率、人员操作失误的频率；另一方面体现为风险后果的严重程度,包括经济损失、运营影响、安全危害等[1]。与通用软件相比,信号系统软件升级风险具有传导性强、影响范围广、后果严重等特点,例如：有些城市地铁信号系统升级时因配置错误引发信号系统故障,导致全线列车晚点2小时,影响乘客数万人次,因此风险定义需突出“安全导向”与“后果量化”的核心要求。

1.3风险评估核心理论

信号系统软件升级风险评估以风险管理理论为核心,融合系统工程理论与可靠性工程理论形成完整支撑体系。风险管理理论提供“风险识别—风险分析—风险评价—风险控制”的全流程框架,明确各阶段的核心任务与输出成果。系统工程理论强调从整体视角分析风险,将信号系统软件升级视为包含人员、技术、环境等要素的复杂系统,避免孤立评估单一风险因素。可靠性工程理论为风险量化提供方法支撑,通过故障模式与影响分析(FMEA)、故障树分析(FTA)等工具识别风险关联关系。此外,模糊数学理论解决了风险评估中部分指标难以精准量化的问题,层次分析法为多维度指标权重确定提供科学依据,这些理论共同构成风险评估的方法论基础,确保评估过程的系统性与科学性。

2 信号系统软件升级风险识别与传导机制

2.1基于全流程的风险识别

基于信号系统软件升级“需求分析—版本开发—实验室测试验证—现场测试验证-预升级-正式升级现场部署—试运行—验收”全流程,采用文献研究法、案例分析法与专家评审法结合的方式识别风险。需求分析阶段风险包括需求描述模糊、与现有系统适配性考虑不足,某项目曾因需求遗漏“新增项目功能与既有调度指挥中心外部系统大屏工作站性能不匹配”,导致升级后数据传输中断。版本开发阶段风险涵盖代码漏洞、模块接口冲突,通过对100个升级案例统计,该阶段风险占比达35%。测试验证阶段风险体现为测试环境与现场环境差异大、测试用例覆盖不全,部分隐性缺陷未被检出。现场部署阶段风险包括硬件兼容性差、升级工艺不规范；试运行与验收阶段风险则涉及性能衰减、指标达标率低。全流程识别共得到43项初始风险因素,实现风险的全面覆盖。

2.2基于故障树的关键风险提取

以“信号系统软件升级失败”为顶事件构建故障树,将全流程识别的风险因素作为底事件,通过逻辑门连接形成风险关联结构。故障树分析中,采用最小割集法提取关键风险,最小割集反映导致顶事件发生的最简化风险组合。经计算,故障树共得到12个最小割集,其中“代码漏洞+测试覆盖不足”“硬件不兼容+部署工艺错误”“需求模糊+开发偏离”为高频最小割集。结合重要度分析,确定关键风险因素18项,包括软件与硬件匹配度、代码缺陷率、测试用例覆盖率、人员操作熟练度等。与初始风险因素相比,关键风险提取剔除了25项影响较小的风险,如“升级文档排版不规范”,使风险评估更聚焦核心环节,提升评估效率与精准度[2]。

2.3风险传导路径与影响机制

信号系统软件升级风险传导呈现“链式传导”与“辐射传导”双重特征,形成多路径传导网络。链式传导路径如“需求模糊→开发偏离→代码缺陷→测试未检出→部署后功能失效”,前一环节风险未得到控制将直接引发后续风险。辐射传导路径体现为单一风险因素影响多个环节,如“人员操作失误”可导致部署工艺错误、测试数据记录偏差等多重问题。风险影响机制表现为技术、管理、环境风险的相互耦合,技术风险是核心触发因素,管理风险加剧风险发生概率,环境风险放大风险后果。例如,硬件兼容性不足(技术风险)叠加现场施工空间狭小(环境风险)与监管不到位(管理风险),将使部署故障风险提升3倍,且故障修复时间延长50%,明确风险传导规律为后续指标体系构建提供依据。

3 信号系统软件升级风险评估指标体系构建

3.1指标体系构建原则

信号系统软件升级风险评估指标体系的构建需兼顾理论严谨性与实践可行性,遵循四大核心原则:科学性原则要求指标定义清晰、逻辑严密,既符合风险管理通用理论框架,又贴合信号系统技术特性。例如,技术风险维度需涵盖软件兼容性、代码缺陷率等量化指标,避免模糊表述;针对性原则强调聚焦关键风险因素,通过文献分析、历史事故追溯及专家访谈识别高频风险点,剔除与升级关联度低的冗余指标,如非核心功能模块的冗余设计风险;可操作性原则注重数据采集便利性与量化方法简易性,优先选择可直接通过测试工具、运维日志或问卷调研获取数据的指标,如硬件适配率可通过兼容性测试报告直接获取,避免依赖主观评价或复杂建模;动态性原则预留指标调整接口,针对不同类型信号系统的升级需求,灵活增减指标或调整权重,例如工业控制信号系统需强化环境适应性指标,而轨道交通系统需侧重安全完整性等级(SIL)合规性。构建思路以“风险维度—风险类别—具体指标”为层级逻辑,先依据风险属性划分技术、管理、环境、安全四大维度,再按升级流程与风险特征细分风险类别,最后将关键风险因素转化为具体评估指标。通过“初步筛选—专家论证—相关性分析”三步法优化指标,剔除冗余指标,确保体系的系统性与精简性。

3.2指标体系具体内容

构建的指标体系分为四个层级,一级指标为技术风险、管理风险、环境风险、安全风险；二级指标共12项,技术风险包含软件兼容性、代码质量等4项,管理风险涵盖计划管控、人员能力等3项,环境风险包括硬件环境、现场条件等2项,安全风险包含系统安全、数据安全等3项；三级指标共32项,如软件兼容性维度下的“软硬件匹配度”“子系统接口适配率”,代码质量维度下的“漏洞密度”“模块冲突率”,人员能力维度下的“操作人员资质达标率”“培训考核通过率”。各指标均明确数据来源,如“漏洞密度”来自第三方代码审计报告,“软硬件匹配度”通

过兼容性测试获取，“现场施工温度”由现场传感器实时采集，确保指标可落地实施[3]。

3.3指标量化标准与分级

采用定量与定性相结合的方式制定指标量化标准，定量指标明确数值范围，定性指标通过模糊打分转化为量化值。将风险等级划分为极低(1分)、低(2分)、中(3分)、高(4分)、极高(5分)五个等级。定量指标如“漏洞密度”，≤0.1个/千行代码为极低风险，0.1-0.3个/千行代码为低风险，0.3-0.5个/千行代码为中风险，0.5-0.8个/千行代码为高风险，＞0.8个/千行代码为极高风险；“升级计划完成率”≥95%为极低风险，85%-95%为低风险，75%-85%为中风险，65%-75%为高风险，＜65%为极高风险。定性指标如“人员操作规范性”，通过专家打分确定等级，操作流程完全符合规范为极低风险，偶有轻微偏差为低风险，存在明显疏漏为中风险，频繁违规操作为高风险，引发操作事故为极高风险。

4 风险评估模型建立与权重确定

4.1层次分析法确定主观权重

采用层次分析法确定主观权重，构建“目标层—准则层—指标层”的层次结构模型，目标层为信号系统软件升级总体风险，准则层为四大一级指标，指标层为二级与三级指标。邀请10位专家(含5位信号系统运维专家、3位软件开发专家、2位风险评估专家)构建判断矩阵，采用1-9标度法表示指标重要程度。通过一致性检验确保判断矩阵合理性，一致性比例CR＜0.1为检验通过。计算得到一级指标权重：技术风险0.42，管理风险0.25，安全风险0.23，环境风险0.10，体现技术风险为核心风险。二级指标中“软件兼容性”“代码质量”“系统安全”权重较高，分别为0.15、0.12、0.09，与关键风险识别结果一致，反映主观权重的科学性。

4.2熵权法确定客观权重

熵权法通过指标数据的信息熵反映客观权重，熵值越小说明指标信息效用越大，权重越高。收集15个信号系统软件升级项目的指标数据，建立数据矩阵并进行标准化处理，消除量纲影响。计算各指标信息熵与差异系数，差异系数越大权重越高。客观权重计算结果显示，一级指标中技术风险0.38，管理风险0.27，安全风险0.22，环境风险0.13，与主观权重整体趋势一致，但环境风险权重略高，原因是样本中多个项目因环境因素导致升级延迟，体现客观数据的影响。三级指标中“硬件适配率”“测试用例覆盖率”客观权重较高，分别为0.06、0.05，与实际工程中这两项指标对升级结果的显著影响相符[4]。

4.3融合权重与评估模型建立

采用线性加权法融合主观与客观权重，设定主观权重系数0.6、客观权重系数0.4，计算公式为：融合权重=0.6×主观权重+0.4×客观权重。融合后一级指标权重：技术风险0.404，管理风险0.258，安全风险0.226，环境风险0.112。基于融合权重建立模糊综合评估模型，构建模糊评判矩阵，通过权重向量与评判矩阵的合成运算得到各层级风险评估值，最终汇总为总体风险等级。以某轨道交通信号系统升级项目为例，模型计算得到总体风险值3.2分，对应中风险等级，核心风险点为“软件与外部接口厂家大屏工作站硬件兼容性不足”“测试环境与现场列车数量差异大”，与项目实际升级过程中出现的问题完全吻合，验证了模型的有效性。

5 结束语

本文围绕信号系统软件升级风险评估展开研究，通过全流程风险识别与故障树分析，精准提取关键风险因素，构建了包含4个一级指标、12个二级指标、32个三级指标的完整评估指标体系，明确了各指标的量化标准与分级。结合层次分析法与熵权法确定融合权重，建立的模糊综合评估模型实现了主观经验与客观数据的有机结合。未来研究可引入机器学习算法优化评估模型，提升风险预测能力；针对不同类型信号系统细化指标体系，增强适配性，为信号系统软件升级安全提供更全面的技术支撑，推动运维管理向智能化、精准化转型。

[参考文献]

[1]黄柒光,梁宇.城市轨道交通信号系统ATS升级/回退自动化工具研究与设计[J].铁道通信信号,2019,55(6):95-98.

[2]赵文天,崔凯,尉安宇.地铁信号系统更新改造方案研究[J].铁路通信信号工程技术,2025,22(10):94-100.

[3]王锋.CBTC信号系统信息安全问题分析[J].铁路通信信号工程技术,2023,20(1):95-98,109.

[4]张娟,邓瑛.地铁信号系统维护管理策略[J].网络安全技术与应用,2022(1):111-112.