城轨云系统安全防护与保障研究

孙 瑜[1] 王 龙[1] 王宇鑫[1]
SUN Yu WANG Long WANG Yuxin

摘 要 针对城轨云平台业务集中、系统结构复杂的特点和高实时性、高可用性和高安全性等综合运行要求，文章构建了集安全防护和运行保障为一体的城轨云平台信息系统的安全保障体系，根据城轨云平台业务特点从业务多层安全防护、高可用与容灾运行、安全态势感知三个方面进行了全局化设计，并且把安全事件、运行保障、制度管理等有机地结合起来，在城轨云平台中具体应用达到了提高攻击识别能力、加快故障恢复速度的效果，提升了城轨云平台的运行安全性及稳定性。

关键词 城轨云平台；智能物联；安全防护

doi：10.3969/j.issn.1672-9528.2026.05.018

0 引言

随着城市轨道交通持续向云化的方向发展，城轨云已经完全成为行车调度、设备监控、乘客服务等各种业务的主要承载平台[1-2]，如果运行出现问题，会影响整个城市公共交通的运行稳定[3]。而且相较于通用云平台而言，城轨云平台对于业务的实时性、系统可靠性和安全防护能力要求更高，安全问题会影响到正常的运行，而运行故障又会导致安全问题的发生，所以很难实现按照以往那种将二者割裂开的设计方法进行保障[4-5]。

对现有的研究大多是针对云平台的安全防护和高可用性架构以及运维管理来进行的，在访问控制[6]、入侵检测以及资源调度方面已经获得一定的进展，也为云平台提供了一定的稳定运行支撑，但是这些研究大多是从通用的云环境出发[7-9]，并且大部分是将安全防护和运行保障割裂开来的，缺乏对城轨云平台本身业务连续性和安全协同能力的直接关注[10]。

针对现状，以城轨云平台的业务特性和运行需要为基点，建立安全防护与运行保障相结合的研究架构。一方面基于统一的安全策略以及统一的运行控制逻辑，在运用态势感知技术的基础上，实现安全事件与运维操作的协同运行；另一方面从城轨云平台规划、部署、运行全过程入手，结合多维度的保障措施对其进行综合性的防护[11]。

1 相关工作

随着互联网应用的深化和网络空间战略地位的提升，新型攻击变得愈发复杂、隐蔽，攻击频率也在不断增长，网络空间已经成为国家安全博弈的新战场。明晰网络边界有利于具体防护策略的制定和实施。通常情况下，轨道交通生产网络与办公网络相互独立，而生产网络借助防火墙，将整个网络划分为安全生产网、运维管理网、办公区并制定相应的安全防护策略，达到有针对性的安全防护的目的。网络安全设计贯彻区域边界防护原则，在所有关键区域的边界部署防火墙、DDoS 等设备来实现该区域边界保护，将威胁控制在局部区域内。在应用服务器区域内部署网闸，通过网闸摆渡功能避免恶意程序实时连接，在园区内网的运维管理区部署堡垒机、漏洞扫描、日志审计、数据库审计、终端管理、终端杀毒等安全设备，满足企业业务系统三级等保要求。

目前对城市轨道交通运营安全管理、智能运维系统设计、云平台安全防护等领域的研究已经开展了相应探索。以上工作的开展，能够在一定程度上实现安全风险辨识、运维效率提升、等级保护落实及安全资源集约化的功能，在一定程度上为城轨云平台运行保障和安全建设提供有益借鉴[12-14]；然而目前的研究大多是对某一管理或某一方面的技术展开的单独研究，并没有从整体上对城轨云平台的安全防护与运行保障协同设计进行考虑。

2 安全防护与运行保障一体化体系设计

2.1 安全防护体系设计

为了满足城轨云平台业务并行运行、业务实时性和安全性的特点，以纵深防御为理念构建立体化多层次安全保障体系，在信息系统的网络层、主机和虚拟化层以及数据层通过联合各个不同层面来进行对信息系统的防护，在平台出入口和平台内部的核心点位分别设置下一代防火墙和虚拟防火墙；并把整个信息系统的网络根据业务属性分为管理域、业

1. 青岛地铁运营有限公司 山东青岛 266000

务域和数据域；结合白名单访问控制技术和策略优先级，从上述 3 个不同层面对越域访问过程进行精准管控。具体的越域访问综合风险可以表示为：

$$R_i = \sum_{j=1}^{N_i} \omega_{i,j} P_{i,j} (1 - E_{i,j}) \tag{1}$$

式中：R_i 表示第 i 类城轨云平台业务的网络访问风险；$\omega_{i,j}$ 表示业务重要性权重；$P_{i,j}$ 与 $E_{i,j}$ 分别表示异常访问概率与防护有效度。

2.1.1 关键技术实现细节

采用“静态基础名单 + 动态适配名单”的双层架构。静态基础名单城轨云平台影响行车及客运服务的核心业务流程预先配置，涵盖固定通信 IP、端口及协议；动态适配名单通过实时流量分析与业务状态感知自动更新，例如当乘客服务系统新增移动支付接口时，系统通过业务注册信息自动校验接口合法性，并将其对应的访问源 IP、通信端口添加至临时白名单，有效期随接口服务生命周期动态调整，超时未使用则自动移除。同时，建立白名单变更审计日志，记录变更主体、时间、原因及影响范围，确保可追溯性。

在主机与虚拟化层，将统一为主机和虚拟机实例部署主机入侵防御代理，然后将安全基线下发至虚拟化安全管理模块中，采用集中的方式进行系统、端口、服务进程管控，利用补丁更新、漏洞扫描等方式降低虚拟化环境的横向渗透风险。整体防护效果可表示为：

$$S = \frac{\sum_{K=1}^{M} \alpha_k C_k V_k}{\sum_{K=1}^{M} \alpha_k} \tag{2}$$

式中：S 表示主机与虚拟化层综合防护水平；α_k 表示实例业务权重；C_k 与 V_k 分别表示安全基线符合度与漏洞暴露因子。数据层对存储资源启用 AES-256 静态加密，并利用集中式密钥管理的方式，达到多业务并行情况下，不同业务间的数据隔离及防止数据暴露的风险。

2.1.2 服务器与虚拟化层防护技术优化

针对不同业务类型的虚拟机实例制定差异化安全基线，例如行车调度业务虚拟机禁用等非必要端口、关闭远程桌面服务，乘客信息系统虚拟机强化应用程序权限管控、开启实时日志审计。通过每 2 h 对实例进行基线合规性扫描，扫描结果与标准基线比对，生成合规性报告，对不合规项自动触发修复指令，无法自动修复的则推送至运维工单系统，要求人工处理并限定修复时限。

数据层对存储资源启用 AES-256 静态加密，采用集中式密钥管理系统（KMS），实现多业务并行情况下不同业务间的数据隔离及降低数据暴露的风险。

2.2 运行保障体系设计

对于城轨云平台高可用、连续运行的要求，基于上述分析，在基础架构层采用双活或多活并存的模式；业务运行在容器集群或者虚拟化资源池上，平台调度资源；结合接入层的软硬件负载均衡以及节点的健康检测，动态调度业务流量，避免因为某个节点或某台服务器发生故障造成单一系统的核心业务受到影响，进而保证全网的安全稳定运行。平台整体运行可用度计算方法：

$$A = \frac{\sum_{i=1}^{N} w_i u_i h_i}{\sum_{i=1}^{N} w_i} \tag{3}$$

式中：w_i 表示节点承载业务的重要性权重；u_i 与 h_i 分别表示节点资源可用率与健康状态因子。

2.2.1 双活架构数据同步技术

以智慧供电调度类业务为例，采用基于 Paxos 算法的分布式一致性协议实现双活数据中心的数据同步。设置主数据中心、备用数据中心，两者通过大于 10 Gbit/s 高速光纤链路连接，数据同步采用“实时同步 + 异步校验”模式。行车调度指令、列车运行状态等核心数据先写入主数据中心，同时通过 Paxos 算法同步至备用数据中心，确保数据一致性；历史运行日志等非核心数据采用异步同步，降低链路压力。当主数据中心节点故障时，备用数据中心通过健康检测机制，在 3 s 内感知故障，自动接管业务，实现无感知切换。同时，建立数据同步冲突解决机制，当主备中心数据出现差异时，以时间戳最新、签名合法的数据为准，确保业务数据准确性。

平台运行时会引入分布式容错机制，将一些关键业务组件做无状态化部署，并且把这些业务状态集中存放在高可靠的数据库集群内，在节点或者实例发生故障时，由调度系统进行实例重建并接管业务，保证服务能正常地继续运转；而灾备则是生产数据会实时或者准实时地同步到主数据中心和异地灾备中心，按照业务的重要性来设置恢复时间目标（RTO）和数据恢复点目标（RPO），这样就可以避免出现数据丢失的风险。平台运行恢复能力体现为：

$$G = \sum_{k=1}^{M} \beta_k \frac{1}{\mathrm{TRO}_k + \lambda \mathrm{RPO}_k} \tag{4}$$

式中：β_k 为业务重要性权重；λ 为恢复时间与数据完整性平衡系数。集中监控与告警联动机制为调度与切换策略提供实时支撑，保障城轨云平台稳定运行。

2.2.2 分布式容错与灾备优化

通过无状态化部署实现行车调度、供电调度等关键业务组件的无状态设计，将会话状态、业务配置等数据存储在分布式缓存集群中，缓存集群采用主从复制 + 哨兵模式保障高可用。当组件实例故障时，调度系统通过容器编排工具快速重建实例，新实例从缓存集群读取状态数据，10 s 内即可接管业务，无需人工干预。

2.3 安全与运行保障的协同设计

通过安全防护、运行保障一体化运维需求，统一部署城

轨云安全态势感知平台到统一城轨云平台，对统一城轨云安全防护、运行保障等产生的安全日志和运行日志统一采集入库并进行集中关联分析；根据不同等级业务的业务需求，设置相应的日志采集策略；基于关联分析技术将业务运行中出现的攻击行为和运行异常统一建模，并结合综合事件视图展现业务系统相关的安全态势及运行动态。

$$R=\sum_{i=1}^{N}\gamma_i e_i r_i \tag{5}$$

式中：R 表示事件综合风险值；γ_i 表示业务重要性权重；e_i 与 r_i 分别表示事件严重度与影响范围因子。

这时若风险评分大于阈值，则联动控制模块将联动启动处置机制对该虚拟机进行隔离，联动进行业务迁移、策略收敛及流量重定向等操作；同时该系统也会更新对应的监控状态以及告警信息，并产生完整闭环处置过程。定义协同处置效率：

$$C=\frac{\sum_{j=1}^{M}\delta_j(T_j^0-T_j^1)}{\sum_{j=1}^{M}\delta_j} \tag{6}$$

式中：δ_j 表示业务重要性权重；T_j^0 与 T_j^1 表示处置前后事件影响持续时间。该机制可在异常扩散前完成干预，提升城轨云平台的连续运行能力与风险处置效率。

2.4 安全态势感知技术架构

安全态势感知技术采用数据采集、关联分析、态势呈现、处置联动的四层架构，数据采集层通过网络探针、日志转发器多源采集系统、应用、安全设备等日志及流量、会话信息，按业务等级动态调整采集频率，经加密压缩传输至日志存储集群；关联分析层结合规则引擎与轻量化随机森林 AI 模型，通过模式匹配识别已知威胁、AI 预测未知威胁与复杂攻击，以分钟级为时间窗口保障分析时效性；态势呈现层借助可视化仪表盘，多维度展示攻击统计、运行监控、风险分布等全网安全态势；处置联动层建立分级响应机制，按事件风险等级自动触发防护规则调整、实例隔离等操作，高风险事件同步启动应急响应流程，实现安全与运行事件的精准识别、快速处置及全流程闭环管控。

3 保障体系效果评估

3.1 实验评估

利用城轨云平台测试中心，部署行车调度、设备监控、乘客信息等业务；通过向系统注入端口扫描、异常访问、数据篡改等攻击行为及节点下线、链路中断等运行故障，检验城轨云平台的安全防护及运行保障能力。

安全态势感知平台把安全日志、运行日志统一收集汇总起来进行分析，并联动触发实例隔离、业务迁移、流量重定向等处置手段，整体化记录响应过程及恢复过程，实际评估效果如图 1 所示。

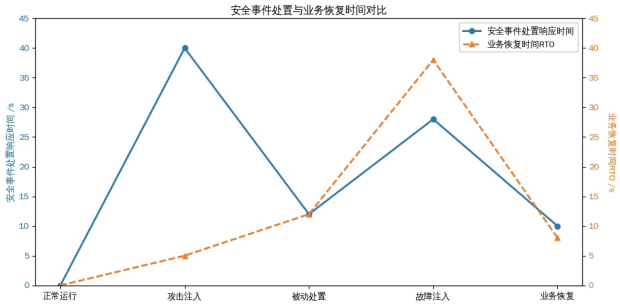

图 1 城轨云平台实验评估结果

如图 1 所示，在正常运行时，两者的数据都是 0，系统是在正常的运行状态中。当进入攻击注入之后，安全响应时间达到了 18 s，而业务恢复时间只有 3 s，说明被侵入后迅速对攻击进行了处理，没有对业务造成较大的危害。进入联动处置阶段以后，虽然安全响应时间有所下降，但是 RTO 却开始逐渐提高，表明此时安全管控的干预以及业务处理出现了一定偏差，也在一定程度上打破了原有的平衡。当出现故障注入之后，RTO 达到了 42 s，也是全阶段里最高的。最后经过业务恢复之后，安全响应时间和 RTO 分别降到 4 s 和 8 s，此时系统处于正常的状态当中。

3.2 评估指标

（1）安全防护覆盖率以端口扫描、异常访问和数据篡改等攻击为统计对象，通过安全态势感知平台对防火墙、入侵防御系统和主机安全日志进行统一去重处理，计算成功阻断并记录的攻击次数占攻击总次数的比例，用于评估多层安全防护效果；（2）系统可用性依据集中监控平台统计的业务实例运行状态，计算业务处于可调度、可访问状态的时间占实验总时长的比例，用于衡量高可用与容错机制对连续运行的支撑能力；（3）故障恢复时间以节点失效至业务恢复稳定运行的时间差进行统计，用于评估实例重建与业务接管效率；（4）自动运维响应时间为告警触发到隔离、迁移、策略收敛结束的时间差；（5）安全事件处理效率是完成闭环处置的事件数量占被识别事件总量的比例。相关评估结果如表 1 所示。

表 1 城轨云平台安全防护与运行保障体系评估结果

评估指标	指标定义说明	实验结果
安全防护覆盖率	成功阻断并记录的攻击事件数 / 攻击注入总次数	96.8%
系统可用性	业务可调度、可访问状态时长 / 实验总运行时长	99.92%
故障恢复时间（RTO）	节点失效至业务恢复稳定运行的时间	42 s
自动化运维响应时间	告警触发至完成隔离或迁移操作的时间	8 s
安全事件处理效率	已闭环处置事件数 / 识别到的安全事件总数	94.5%

从表 1 可以看出，安全防护覆盖率为 96.8%，说明该多层防御安全防护体系可以有效地针对不同类型的攻击注入实施保护；系统可用性达到了 99.92%，说明在安全事件或者故障发生的时候，能够保证核心业务系统依然可以正常稳定地运行；故障恢复时间为 42 s，自动化运维响应时间为 8 s，能够及时有效地恢复；安全事件处理效率为 94.5%，说明能够较快地完成安全事件的发现并开展后续处置工作，形成了比较完整的闭环处理机制。

4 相关措施

为了提高信息安全，防止端口暴露带来的安全隐患，结合 IP 安全策略，对一些高危和不常用的端口进行关闭，避免由此产生的安全隐患。因此在互联网接入区额外部署 IPS、上网行为管理、WAF 防火墙等安全防护设备。园区通过网络探针和诱捕系统，采集终端和网络的信息，发送到安全态势感知平台。该平台通过智能算法对收集到的信息进行综合分析和研判，统一呈现全网安全态势，并将需要处置的安全事件下发给控制器处理，最终实现整网的一体分析、一体决策、一体处置。定期出具报表，分析网络流量的分布情况，作为制定安全策略的依据。当信息支撑网中的服务器、主机和系统受到来自互联网的攻击时，通过网络行为审计系统追溯攻击的痕迹，配合公安网监人员查找互联网攻击源头。

在管理设计中，项目严格贯彻“全流程闭环管控”原则：在制度层面，制定《IT 运维管理规范》《数据安全操作手册》《人员权限管理办法》等制度，明确设备采购、系统部署、数据备份、故障处置等各环节的标准流程；在流程层面，通过 IT 服务管理平台（ITSM）实现运维流程线上化，从故障申报、工单分配、处理跟进到验收归档，形成全流程追踪，确保故障响应时间达标在人员层面，实施“最小权限 + 定期轮岗”机制，按岗位需求分配系统操作权限，每季度开展人员操作审计与安全培训，强化合规意识，全面满足企业 IT 管理与等保合规的双重要求。

5 结论

基于城轨云平台的安全性和可用性实际需求，搭建了一套安全防护和运行保障一体化的信息系统保障体系。基于纵深防御的体系结构进一步加强多层面安全防护，并且将高可用、容灾及自动化运维等措施综合考虑进城轨云平台中，并加入安全态势感知手段以确保城轨云平台发生安全事故或出现问题时能够根据安全防护和应急处置的要求采取及时应对措施，并且相关手段应用到城轨云平台的整个生命周期内。通过试验验证可知，采用本论文提出的体系后可较好地保证城轨云平台在遭受入侵、发生故障等问题后的安全状态以及运营工作得以继续，为提高城轨云平台运行的可靠性与预防城轨云平台遭受侵害提供一定技术依据。

参考文献：

[1] 张雷，徐倩，何积丰，等 . 面向城轨云平台边界安全防护的动态信任管理方法 [J]. 同济大学学报 (自然科学版), 2024, 52(2): 157-165.

[2] 王皓 . 智慧城轨云平台和数据平台及网络安全融合协同技术研究 [J]. 都市快轨交通 ,2022,35(6):64-68.

[3] 彭轶华，刘明远，郜帅，等 . 轨道交通行业网络空间安全现状与未来发展 [J]. 中国工程科学 ,2023,25(6):137-149.

[4] 韦妙鸳，何靓俊，虞腾飞，等 . 基于城市轨道交通的云网安一体化平台方案研究 [J]. 中国新通信 ,2022,24(23):45-47.

[5] 张威，司鑫悦 . 城市轨道交通云平台网络安全体系研究 [J]. 现代城市轨道交通 ,2022(7):34-38.

[6] 史永飞 . 云内云外融合网络安全纵深防御体系研究 [J]. 都市快轨交通 ,2022,35(6):59-63.

[7] 杜宏民，唐汐 . 城市轨道交通多场段智能管控系统数据云平台的设计与应用 [J]. 城市轨道交通研究 , 2023, 26(10): 176-181.

[8] 吴正中，邓能文，王晓东，等 . 基于云平台的城市轨道交通自动化集成系统架构与实践 [J]. 都市快轨交通 , 2023, 36(6): 22-28.

[9] 陈青云 . 智慧城市轨道交通云原生探讨 [J]. 城市轨道交通研究 ,2023,26(6):12-16.

[10] 葛淑云，周伟，陈盼盼，等 . 城轨云工程质量验收标准的研究 [J]. 铁路通信信号工程技术 ,2022,19(3):65-69.

[11] 许锡伟，陈炜，陈冠麟，等 . 数智化地铁安全应急保障系统建设研究 [J]. 都市快轨交通 ,2024,37(2):54-59.

[12] 赵奕雄，车健，方艺清 . 城市轨道交通运营安全管理问题与对策研究 [J]. 运输经理世界 ,2025(29):1-3.

[13] 雷云鹏 . 城市轨道交通跨专业智能运维系统设计及应用 [J]. 城市轨道交通研究 ,2022,25(11):140-142.

[14] 蔡晶晶 . 基于等级保护规范的媒体云平台安全优化实践 [J]. 网络空间安全 ,2024,15(3):50-55.

【作者简介】

孙瑜（1989—），男，山东青岛人，本科，工程师，研究方向：工业互联网。

王龙（1989—），男，山东青岛人，硕士，高级工程师，研究方向：工业互联网。

王宇鑫（1995—），男，山东青岛人，本科，工程师，研究方向：工业互联网与网络安全。

（收稿日期：2026-01-27　修回日期：2026-04-28）