电梯数字监管平台中的信息安全

刘声伦

429005********5037

摘要：随着城市化进程的加速与物联网、大数据、人工智能等技术的深度融合，电梯作为城市垂直交通的“主动脉”，其安全运行与智能化监管日益成为智慧城市建设的核心议题。电梯数字监管平台应运而生，通过实时数据采集、传输、分析与应用，实现了电梯安全监管从传统的人工、被动、滞后模式向智能化、主动化、预防性模式的根本性转变。然而，海量、多维、实时流动的数据在显著提升监管效能的同时，也使得平台面临前所未有的、严峻复杂的信息安全挑战。本文首先系统阐述了电梯数字监管平台的基本架构与核心功能，论证了信息安全保障对于平台可靠性、公信力及社会公共安全的极端重要性。继而，论文深入剖析了平台在物理感知层、网络传输层、平台应用层以及数据全生命周期管理中所面临的终端安全、通信安全、平台安全、数据安全及供应链安全等多维度、多层次的风险与威胁。在此基础上，本文从技术防护、管理策略、法规标准与人员意识四个层面，构建了一套系统化、纵深防御的信息安全保障体系框架，旨在为电梯数字监管平台的安全、可靠、可持续运行提供理论参考与实践指引。

关键词：电梯数字监管平台；物联网安全；数据安全；纵深防御；智慧城市；公共安全

DOI：10.69979/3041-0673.26.05.016

引言

在现代都市的肌体中，电梯是维系建筑功能、保障人员流动不可或缺的关键基础设施。据统计，我国电梯保有量、年产量及年增量均已位居世界首位，其运行安全直接关系到人民群众的生命财产安全与社会稳定。传统的电梯安全管理模式主要依赖定期检验、应急维修和事后追责，存在信息不对称、响应滞后、监管覆盖面有限等固有缺陷。新一代信息技术的迅猛发展，为破解这一难题提供了历史性机遇。以物联网、云计算、大数据和人工智能为技术基石的电梯数字监管平台，通过为电梯加装智能传感设备，实时采集运行状态、故障信息、视频数据等，并经由无线/有线网络汇聚至云端数据中心进行智能分析与处理，从而实现对电梯全生命周期、全状态信息的可知、可感、可控。这标志着电梯安全监管正式迈入数字化、网络化、智能化的新阶段。

然而，“凡有网络处，皆有风险生”。电梯数字监管平台本质上是一个复杂的“云-管-端”协同信息系统。其前端连接的成千上万部电梯物联网终端构成了庞大的攻击面；数据在不可控的公网或专网中长距离传输；海量的敏感数据（如实时运行数据、乘客音视频信息）在平台中心汇聚与存储；各类用户（监管机构、维保单位、使用单位、乘客）通过多样化的接口进行访问与交互。每一个环节都可能成为恶意攻击者的突破口。信息安全风险已不再仅仅是技术层面的数据泄露或系统瘫痪问题，更可能演化为导致电梯非正常停运、关键指令被篡改、公众隐私大规模泄露，甚至引发社会恐慌和公共安全事件的重大隐患。因此，构建与电梯数字监管平台发展相匹配的、坚固可靠的信息安全防护体系，已成为确保平台发挥其预期效能、护航智慧城市安全运行的先决条件和必然要求。

1 电梯数字监管平台架构与信息安全重要性

电梯数字监管平台通常采用分层架构设计，主要包括以下层次：

感知执行层：由安装在电梯各关键部位（如轿厢、机房、井道）的传感器（加速度、平层、门状态）、摄像头、物联网关等设备构成，负责实时采集电梯运行参数、故障代码、音视频等信息，并可能接收来自平台的控制指令。

网络传输层：负责将感知层数据通过移动通信网络（4G/5G）、窄带物联网（NB-IoT）、光纤专网或互联网等方式，安全、可靠地传输至云端平台。此层是数据流动的“大动脉”。

平台服务层（云端）：这是平台的核心，通常基于云计算（IaaS/PaaS/SaaS）架构构建。包含数据接入与存储、大数据分析引擎、故障诊断与预警模型、应急处置流程管理、可视化展示、对外 API 接口等模块，实现数据的汇聚、处理、分析与应用服务提供[1]。

应用交互层：面向政府监管机构、电梯维保公司、

物业使用单位、乘客等不同角色，提供 Web 门户、移动 APP、大屏驾驶舱、短信/微信告警等多种形式的交互界面。

平台的信息安全重要性体现在三个方面：一是保障功能安全的基石。平台的核心目标是预防事故、保障电梯机械与电气安全。若平台自身遭受攻击导致数据篡改、预警失效或误发停梯指令，将直接损害其根本功能，甚至引发安全事故。二是保护公民隐私与数据的红线。平台处理的实时视频、乘梯记录等属于高度敏感的个人信息，一旦泄露将严重侵犯公民隐私权，可能引发法律纠纷与社会信任危机。三是维护公共秩序与社会稳定的防线。电梯是高频使用的公共设施，针对大规模电梯群的网络攻击可能造成城市交通局部瘫痪、公众恐慌，具有显著的公共安全与社会稳定外溢效应。

2 平台面临的多层次信息安全风险与挑战

电梯数字监管平台的信息安全风险贯穿于其整个体系架构与数据流程之中，呈现多层次、跨维度的特点。

2.1 感知终端层风险

物联网终端是平台最薄弱环节之一。风险包括：1)硬件安全薄弱：终端设备通常成本敏感，设计上可能缺乏安全芯片、物理防拆机制，易被非法替换或植入恶意硬件。2)固件/软件漏洞：终端操作系统或应用软件可能存在未修补的漏洞，成为攻击者获取控制权或发起僵尸网络攻击的入口。3)弱身份认证与访问控制：默认密码、硬编码密钥普遍存在，缺乏设备唯一身份标识与双向认证机制，易被仿冒接入[2]。4)数据本地安全：终端缓存的数据可能未经加密存储，在设备丢失或维修时导致数据泄露。

2.2 网络通信层风险

数据在传输过程中面临多种威胁：1)通信协议脆弱性：早期或定制化的物联网通信协议可能缺乏加密、完整性校验和防重放攻击机制，易被窃听、篡改或注入恶意数据。2)无线通信干扰与窃听：采用无线通信（如 4G/5G, WIFI）时，信号可能被干扰导致通信中断，或被截获破译。3)网络边界渗透：从公网到平台专网的边界若防护不当，可能成为攻击者横向移动进入核心区域的跳板。4)拒绝服务攻击（DoS/DDoS）：攻击者可能通过海量物联网终端或被控节点，向平台发起流量攻击，耗尽带宽或资源，导致合法服务中断。

2.3 平台服务层风险

云端平台集中了核心业务与数据，是攻击的主要目标：1)云基础设施安全：依赖的云计算平台（IaaS）自身的安全配置错误（如存储桶公开访问）、租户隔离失效等，可能导致数据泄露或服务受影响。2)应用与 API 漏洞：平台 Web 应用、微服务 API 可能存在的 SQL 注入、跨站脚本（XSS）、越权访问等漏洞，是攻击者渗透的常见途径。3)数据安全与隐私风险：海量数据在存储（数据库）、处理（数据分析引擎）和共享（对外提供数据服务）环节，面临未加密存储、未脱敏展示、违规越权访问、内部人员窃取等风险。4)供应链安全：平台开发、运维可能外包或使用大量第三方组件（开源库、中间件），其中隐藏的漏洞或后门会引入难以察觉的风险[3]。

2.4 管理与社会工程风险

“人”的因素往往是最不可控的环节：1)安全管理缺位：缺乏专门的安全团队、明确的安全责任体系、成文的安全管理制度和流程（如漏洞管理、应急响应）。2)权限管理混乱：内部账号权限分配过大、未遵循最小权限原则，离职人员账号未及时清理。3)社会工程学攻击：攻击者通过钓鱼邮件、假冒客服等手段，诱骗平台管理员或维保人员泄露凭证或执行恶意操作。4)安全合规挑战：平台需同时满足《网络安全法》、《数据安全法》、《个人信息保护法》以及电梯行业特定法规的要求，合规性建设复杂且持续。

3 构建纵深防御的信息安全保障体系框架

应对上述复杂风险，必须摒弃单一、孤立的防护措施，构建一个“技术与管理并重、防御与监测结合、覆盖全生命周期”的纵深防御体系。

3.1 技术防护层：构筑四道防线

终端安全加固防线：推行安全物联网终端标准，强制要求具备唯一可信身份标识、安全启动、硬件加密能力。实施固件签名与安全更新机制，确保固件完整性与可追溯性。加强物理防护，防止非法拆解与调试接口暴露。

通信安全加密防线：端到端强制使用高强度、轻量化的加密通信协议，保障数据传输的机密性与完整性。在网络边界部署下一代防火墙、入侵检测/防御系统（IDS/IPS），对异常流量和攻击行为进行实时监测与阻断。建立专网或虚拟专网（VPN），减少对公网的暴露。

平台与数据核心防线：平台安全：遵循安全开发生命周期（SDL），对平台应用进行代码审计与渗透测试。实施严格的微服务 API 网关管理，进行身份认证、鉴权、

限流与监控。对云服务进行安全配置基线核查与持续监控。数据安全：对静态数据和动态数据实施分类分级管理与加密。对敏感个人信息进行去标识化、脱敏处理。建立数据访问审计日志，对所有数据操作行为进行记录、分析与异常告警[4]。

安全监测与响应：部署安全信息和事件管理（SIEM）系统，汇聚终端、网络、平台各层日志，利用大数据分析技术进行关联分析，实现威胁的实时感知、预警和自动化应急响应。

3.2 管理策略层：夯实安全基石

健全安全治理体系：明确平台运营单位主要负责人为信息安全第一责任人，设立专职安全管理岗位，建立跨部门的安全协调机制。

完善制度与流程：制定覆盖物理安全、网络安全、数据安全、开发安全、运维安全、应急响应、供应链安全的全套管理制度与操作流程，并定期评审更新。

严格的权限与访问控制：实施基于角色的访问控制（RBAC）和最小权限原则。对特权账号进行多因素认证和操作堡垒机管控。

持续的漏洞与补丁管理：建立涵盖自有系统、第三方组件的资产清单，持续跟踪漏洞信息，制定并严格执行补丁更新策略与流程。

供应链安全管理：将安全要求纳入供应商合同，对关键第三方组件进行安全评估，监控其安全状况。

3.3 法规标准与合规层：明确安全准绳

遵循国家法律法规：严格依照《网络安全法》、《数据安全法》、《个人信息保护法》以及关键信息基础设施保护相关条例开展安全建设，履行等级保护定级、备案、测评义务[5]。

对接行业标准规范：积极参与和遵循电梯物联网、智慧电梯等领域正在制定的国家和行业信息安全技术标准，使安全建设有据可依。

建立内部合规审计：定期开展内部安全审计与合规性检查，确保各项安全措施有效落地，并做好迎接外部监管检查的准备。

3.4 人员意识与培训层：筑牢人的防火墙

分角色安全培训：针对平台开发人员、运维人员、管理人员、维保人员及普通用户，设计不同内容的安全意识与技能培训课程，定期考核。

模拟攻防与演练：定期开展钓鱼邮件模拟、红蓝对抗演练和网络安全应急演练，提升全员对攻击的识别能力和实战化应急响应水平。

培育安全文化：通过宣传、激励等方式，将“安全第一”的理念融入组织文化，使安全成为每个人的自觉行为。

4 结语

电梯数字监管平台的健康发展，安全是前提，更是生命线。本文系统论述了平台信息安全保障的极端重要性，深度剖析了其从“端”到“云”、从技术到管理所面临的立体化风险图谱。面对这些挑战，任何单一的“银弹”式解决方案都难以奏效，必须坚持系统观念，构建一个融合先进技术、严谨管理、合规遵循和全员意识于一体的纵深防御信息安全保障体系。这要求平台相关各方——包括设备制造商、平台开发商、网络运营商、物业服务企业、维保单位以及政府监管部门——协同努力，明确责任，持续投入。

未来，随着 5G、边缘计算、数字孪生、人工智能技术在电梯监管中更深入的应用，新的安全场景与挑战也将不断涌现。因此，电梯数字监管平台的信息安全建设必将是一个动态演进、持续优化的长期过程。只有将安全思维贯穿于平台规划、设计、建设、运营、维护的全过程，才能真正筑牢这道守护城市垂直交通命脉的数字安全屏障，让科技创新更好地赋能电梯安全，惠及民生，保障社会公共安全，为智慧城市的稳健运行奠定坚实的基础。

参考文献

[1]张绪鹏. 智慧电梯框架下的知识图谱的应用场景[J].中国特种设备安全,2025,41(12):47-52.

[2]张绪鹏. 电梯数字监管平台中的信息安全[J].西部特种设备,2025,8(06):61-67.

[3]张绪鹏,安辉,吴晓昱. 某产业集聚区特种设备数字监管技术创新实践[J].劳动保护,2025,(12):53-55.

[4]叶升,金樟民,张才. 电梯安全监管“温州模式”的探索与思考[J].中国市场监管研究,2021,(10):28-30+57.

[5]邱伟星. 数字赋能助力电梯安全监管提“智”增效[J].福建质量技术监督,2021,(08):26.