智能化电梯控制系统的网络安全风险评估与防护策略

任玉荣　王陈欢　王剑平
浙江省特种设备科学研究院　浙江杭州　310000

摘　要：在中国经济飞速发展的今天，城市化进程也在加速推进，电梯是高层建筑与公共设施之间重要的垂直交通工具之一，已成为日常生活必不可少的组成部分。在智能化技术快速发展的今天，传统电梯已经逐渐朝着智能化和网络化的方向发展，智能化电梯控制系统因其方便和高效等优点而被广泛使用。但是智能电梯系统联网的特点也给网络安全带来危险。当电梯控制系统受到恶意攻击时，不但有可能使电梯不能正常工作，而且还会给人身安全带来严重的威胁。所以，深入剖析智能化电梯控制系统网络安全风险，提出行之有效的防护策略具有一定的实际意义与研究价值，文章就此展开了探讨。

关键词：智能化；电梯控制系统；网络安全；风险评估；防护策略

引言

智能化电梯控制系统融合物联网（IoT），云计算和大数据等先进技术手段，可对电梯进行远程监控，实时分析运行状态和自动报警故障。这一智能化管理在提升电梯运行效率与安全性的同时，也使电梯系统面临着更多网络安全威胁。近年来世界上多次出现对工业控制系统及物联网设备进行网络攻击，表明网络安全问题越来越严重。鉴于电梯控制系统是关键基础设施的组成部分，我们不能忽视其网络安全方面的问题。电梯系统一旦被黑客攻击轻则造成电梯运行不正常，严重时甚至会造成大范围安全事故。特别是在智能楼宇系统集成化的今天，电梯这一关键环节的安全与否直接影响着整个楼宇能否正常工作。所以在促进智能化电梯不断发展的过程中，对智能电梯控制系统网络安全防护策略进行研究和制定就成了确保智能建筑安全运行所面临的一项重要任务。

一、智能化电梯控制系统概述

智能化电梯控制系统以现代信息技术为依托，通过融合物联网、大数据和人工智能等多种先进技术对电梯进行自动化管理和远程监控。系统核心部分由电梯控制器、传感器、通讯模块、后台管理平台等构成。电梯控制器承担着电梯整体运行调度和保证电梯安全平稳运行的任务；传感器的主要功能是对电梯的各种状态，如速度、位置和重量等进行实时监控，从而为我们提供准确的运行信息；通讯模块负责向后台管理平台传送这些数据，以便管理人员对电梯运行情况进行远程监测。智能化电梯控制系统以实时数据分析和自动化决策为工作原理，通过实时监测电梯运行状态并进行数据采集，可以在检测到故障苗头后及时发出警报，电梯甚至在出现故障之前进行了自动调整，这大大增强了电梯的工作效率和安全性。同时该系统还具有远程维护与升级等功能，降低人工干预需求。另外，该系统能够根据乘客流量的变化对电梯的调度策略进行动态调整，减少了电力的消耗并提高了运行效率。这一智能化管理方式在显著提高电梯系统运作效率的同时，还对现代建筑高效运行起到了重要支撑。

二、智能化电梯控制系统的网络安全风险分析

（一）常见的网络安全风险类型

智能化电梯控制系统联网运行时面临着各种网络安全风险，其常见类型有数据泄露，拒绝服务攻击，恶意软件感染及信号劫持。所谓数据泄露就是未经许可的人利用漏洞来获取电梯运行数据，维护记录或者用户隐私等系统敏感信息的行为，这些信息可能会用于非法目的而造成对系统的误用或者损害。拒绝服务攻击属于另一种危险类型，黑客会通过对电梯控制系统提出大量无效请求而使系统资源消耗殆尽，从而使电梯控制功能处于瘫痪状态，极大地影响了电梯正常工作。恶意软件的感染是指攻击者通过互联网植入恶意软件，这些软件有可能破坏电梯控制系统的正常运作、篡改数据，甚至可能导致电梯设备失效或误操作。信号劫持带来的危险是攻击者可以截获和修改系统间的通信信号使控制命令遭到篡改，这给电梯运行带来了直接的威胁。由于智能电梯系统对网络通信的依赖，上述风险给系统的稳定性与安全性带来严峻挑战，会造成电梯运行中断、数据丢失等

一系列问题，甚至会危害到乘客生命安全。所以对网络安全风险进行识别和保护是非常关键的。

（二）典型网络攻击手段及其影响

智能电梯控制系统经常遭遇各种网络攻击，这些攻击不仅可能干扰系统的正常工作，还可能对人的生命安全带来潜在风险。数据窃取是常见攻击方式之一，黑客利用漏洞侵入系统获取运行数据、设备配置或者用户隐私等信息，并可能利用这些数据进行非法使用，从而造成信息泄露以及经济损失。拒绝服务攻击（DoS）也构成了一个明显的安全威胁。攻击者会通过发送大量不实的请求来耗尽系统资源，这将导致电梯无法有效地响应控制命令，从而引发电梯的停机或瘫痪，进一步影响乘客的正常出行。恶意软件攻击也是一种危险的攻击方式，攻击者可能会通过恶意代码的植入篡改电梯的控制指令从而使得电梯产生异常的行为，即使是在特定的情况下也会造成电梯的失控而造成严重的安全隐患。控制信号劫持还是一种高风险的手段，黑客会通过截获和篡改控制信号等手段使得电梯实际运行情况与控制指令不符，如允许电梯无指令运行或者停车等，这些行为都会给乘客安全带来直接威胁。对于这些攻击方式，需要对智能电梯系统进行有效防护，否则就会造成系统停运，数据泄露或者人员伤亡事故的严重后果。

三、智能化电梯控制系统的网络安全风险评估要点

（一）风险评估的基本方法与模型

在电梯控制系统风险评估中使用了各种基本的方法和模型来综合辨识并分析系统中可能存在的网络安全威胁。其中，威胁建模就是关键手段之一，它通过对系统进行威胁建模来辨识系统潜在攻击路径以及薄弱环节。这一过程一般都是与系统实际架构相结合来分析外部攻击者有可能以何种方式或者路径进入到系统中去，以有助于发现容易受到攻击的部件或者功能。攻击路径分析作为风险评估的又一种重要手段，通过对可能攻击链的仿真来揭示初始攻击点至关键系统资源之间可能存在的攻击路径。通过这样的分析可以直观的知道攻击者有可能会使用什么样的步骤以及系统漏洞，从而有助于管理者预先堵死这些攻击方式。

漏洞评估模型更多地关注于对系统内已知和可能存在的漏洞进行评价，并结合过去的攻击记录和最新的漏洞数据库，来探讨这些漏洞被利用的潜在风险及其带来的影响。通过对系统中各个部件进行漏洞评估，可将漏洞严重程度划分为几类，并着重考虑可能使用频率高的高危漏洞。另外，在风险评估中可引入定量分析方法并利用数学模型来计算各风险发生的概率和潜在损失，有助于管理者对总体风险水平进行定量分析。这些基本方法和模型为电梯控制系统网络安全问题提供一个结构化分析框架，以保证管理者能对潜在威胁进行准确地识别和处理。

（二）电梯控制系统的风险评估步骤

电梯控制系统风险评估步骤为系统化流程，其目的在于发现可能存在的网络安全威胁和制定有效应对对策。首先，有必要对电梯系统内的各种资产进行详细的识别和分类，这包括但不限于硬件设备、软件系统、通信网络以及敏感数据等。这样的资产识别将有助于更准确地确定系统的关键组件和可能受到攻击的具体位置。其次是威胁分析和评价，通过深入剖析系统可能遇到的网络攻击种类来判断何种攻击手段会威胁到特定资产，如数据泄露、拒绝服务攻击或者植入恶意软件。通过这种分析可以清楚地认识到威胁产生的根源以及可能的攻击方式。在评估时，需要综合考虑系统漏洞来划分风险等级，定量或者定性地评价每一种威胁可能产生的影响及其出现的可能性，从而判断哪一种威胁风险优先级更高。最后根据评估结果产生详细风险评估报告并对各高风险项提出相关安全改进建议或者防护措施。该流程有助于管理者对电梯控制系统网络安全现状有一个整体的认识，并对优先需强化的安全领域有一个清晰的认识，从而保证系统面临网络威胁有充分的防护能力并降低可能存在的安全隐患。

四、智能化电梯控制系统的网络安全防护策略

（一）物理层安全防护策略

物理层安全防护策略为确保智能化电梯控制系统网络安全提供了依据，其主要内容包括硬件设备安全以及物理环境保护。硬件安全在物理层保护中处于核心地位，关键硬件如电梯控制器，传感器和通信设备都要求有抗破坏性设计以避免未经许可的人对其进行暴露或者篡改。这可通过采用专用硬件加密芯片，建立防拆卸装置和应用抗干扰技术等措施实现，以保证该装置在恶劣环境或者遭受人为破坏的情况下仍能正常运行。另外，设备接入管理在物理层防护方面也不容忽视。为避免非授权设备进入系统，要对每一个接入点都实施严格的身份认证与访问控制。通过给每一个硬件设备分配一个唯一数字证书或者加密密钥来保证仅可信设备能够和系统通信。

物理隔离也很重要，尤其是电梯控制系统和外部网络之间的联系部分。通过实施如防火墙和网络分段等网络隔离手段，能够有效地阻止外来攻击者通过网络入口

直接侵入控制系统。另外，电梯机房及控制设备存放场所要有限制访问权限，安装监控设备，建立报警系统等严密的物理安全措施以防物理入侵对安全造成威胁。通过上述物理层安全防护措施可以有效地降低电梯控制系统因硬件损坏，非授权接入或者物理入侵等原因带来的安全风险。

（二）网络层安全防护策略

网络层安全防护策略是智能化电梯控制系统安全体系的关键，其主要目的在于保证系统数据传输时不受网络攻击以及不被擅自接入。网络分段与隔离是首要策略，通过将电梯控制系统与外部网络进行物理或逻辑上的隔离，可以有效阻止外部攻击者直接进入电梯系统。经过分段处理的网络可以有效地限制攻击的范围，即便是在某一特定区域受到攻击的情况下，其余部分依然能够维持正常的运行状态。此外，通过采用防火墙和虚拟专用网（VPN）等先进技术，确保了系统内各个区域间的通讯安全性，从而有效地避免了可能发生的横向攻击。

加密通信和身份认证对于网络层的安全保护至关重要。为了确保数据在传输时不被窃取或篡改，系统应当采纳如高级加密标准（AES）和传输层安全协议（TLS）这样的先进加密技术，以保障数据在传输过程中的保密性和完整性。与此同时，每一个接入到网络中的设备与用户必须经过严格的身份认证机制来保证仅有被许可的人与设备才能接入到控制系统。采用双因素认证和基于公钥基础设施（PKI）的数字证书认证可以进一步提高网络访问的安全性，防止未经授权的人员利用网络漏洞侵入系统。另外，入侵检测和防御系统还应该部署到网络层以便对可能出现的网络威胁进行实时监测和及时反应。通过在网络层采取这些防护措施可以有效地减少网络攻击给电梯控制系统带来的冲击，保证系统平稳安全地运行。

（三）应用层安全防护策略

应用层安全防护策略对于保障智能化电梯控制系统应用程序及软件平台的安全运行具有十分重要意义。

首先，安全开发生命周期（SDL）构成了应用层防护的核心要素，通过在软件开发过程的各个环节中嵌入安全审查和测试机制，该系统确保了应用程序从设计阶段到部署阶段都严格遵循安全标准。开发者需严格审查代码安全，发现和修补潜在安全漏洞以预防因代码缺陷造成系统漏洞。另外，将威胁建模引入到软件的设计阶段，可以预先识别出可能存在的安全风险并有助于开发团队从前期开始采取有效的措施来减少风险。

其次，安全补丁的管理和更新机制又是应用层保护的关键环节。系统内应用软件及操作系统需经常更新，才能面对新的安全威胁。借助自动化补丁管理工具能够保证系统时刻处于最新安全防护状态以避免攻击者对已知漏洞的侵入。为避免补丁更新时出错，需要执行严格的检测与验证程序以保证每一次更新均不影响正常工作。

另外，访问控制策略也是非常重要的，一个系统要对不同用户、不同设备建立严格的访问权限以保证只有被授权者才能对具体功能进行操作。智能电梯控制系统在这些应用层的安全保护策略下，能够有效地规避应用层面上的安全风险并降低因软件漏洞或者权限管理不到位而导致安全事件的发生。

结束语

智能化的电梯控制系统对现代建筑起到了至关重要的作用，但是它的网络安全问题却越来越突出。通过综合风险评估辨识出系统所面对的网络威胁及其脆弱点可以为建立有效防护策略打下坚实的基础。文章重点对智能化电梯系统网络安全风险展开深入剖析，涉及物理层。网络层和应用层的保护措施。在硬件安全保障、加密通信、漏洞管理、身份认证等方面，改进后的防护策略能够显著提高电梯控制系统整体安全水平。在今后物联网与人工智能的深入发展下，电梯控制系统安全防护也需要不断地更新与优化，才能应对网络威胁的变化。

参考文献

[1]鲁军.电梯检测控制系统安全问题与防护策略研究[J].产品可靠性报告，2023（5）：146-148.

[2]刘帅，赵楠.电梯检测控制系统安全问题与防护策略分析[J].科学咨询，2021，000（004）：23.

[3]田铮.基于风险的电梯责任保险机理及定价优化研究[D].中国矿业大学（北京），2021.

[4]张雷.浅谈电梯检验的安全问题与策略[J].中国科技期刊数据库工业A，2023.

[5]赵治宇.浅谈电梯机械故障的解决措施及其防护[J].名城绘，2020，000（010）：P.1-1.