

智慧导览机器人辅助运行安全风险识别与防控技术研究

吴晓杰 顾欣 赵玉涛 范志龙

华电河北新能源有限公司, 河北 石家庄 050000

[摘要]随着智慧导览机器人越来越多地应用于各类公共场所如博物馆、景区、商场、电力营业厅、变电站等, 其服务过程中所面临的安全隐患也不容小觑。本论文从导览机器人的工作方式及功能出发, 对其运行过程中存在的一些主要问题进行探讨, 即对环境的适应性较差、导航定位不够精准、人机交互稳定性差以及网络信息安全方面的问题, 进而提出加强安全风险辨识能力、提升自主感知与避障水平、改善导航定位与控制技术、增强网络安全防护及数据安全保障力度、实现智能化维护管理等一系列措施来更好地保证机器人的正常运转。

[关键词]智慧导览机器人; 安全风险识别; 防控技术

DOI: 10.33142/sca.v9i6.19809

中图分类号: TP242

文献标识码: A

Research on Safety Risk Identification and Prevention Technology for Intelligent Navigation Robot Assisted Operation

WU Xiaojie, GU Xin, ZHAO Yutao, FAN Zhilong

Huadian Hebei New Energy Co., Ltd., Shijiazhuang, Hebei, 050000, China

Abstract: With the increasing application of smart navigation robots in various public places such as museums, scenic spots, shopping malls, power service halls, substations, etc., the safety hazards faced in their service process cannot be underestimated. Starting from the working mode and functions of guided robots, this paper explores some of the main problems that exist during their operation, namely poor adaptability to the environment, inaccurate navigation positioning, poor stability of human-computer interaction, and issues related to network information security. Furthermore, a series of measures are proposed to better ensure the normal operation of robots, including strengthening the ability to identify security risks, improving autonomous perception and obstacle avoidance, improving navigation positioning and control technology, enhancing network security protection and data security, and achieving intelligent maintenance and management.

Keywords: smart navigation robot; security risk identification; prevention and control technology

引言

伴随着人工智能、多模态感知以及自主导航技术的发展进步, 在博物馆、科技馆、景区、商场、电力营业厅、智慧变电站等地, 越来越多的智慧导览机器人参与到指引、解说、答疑、电力设备巡检等工作当中。T/SZRA 001-2026《轮式柔性导览机器人技术规范》对机器人提出了建图、定位、自主导航、避障、越障、语音交互、触觉交互、急停等功能要求, 同时对于位置精度提出小于等于 10cm, 对于姿态角精度小于等于 5°, 对于急停的距离小于等于 0.5m。但是由于公共场所环境复杂、人群众多、电磁环境多种多样(尤其是变电站内存在强电磁干扰环境), 使得智慧导览机器人在协助工作时也存在诸多安全隐患。具身智能的安全涉及从感知到认知再到决策以及执行的全过

程问题, 在保证数据安全及模型鲁棒性的基础上还要解决物理行为不可控以及任务目标偏移等问题。研究智慧导览机器人辅助运行的安全风险识别及防控方法对保护人们的人身安全以及电力设备安全具有重要作用。

1 导览机器人运行模式与功能特点

智慧导览机器人的工作方式主要有三种: 自主巡航导览、定点讲解及跟随引导。自主巡航时, 机器人根据预先设定路线行走, 遇到障碍物可避开; 定点讲解时, 机器人停留在某处为人们答疑解惑; 跟随引导时, 机器人能够识别并且跟踪一个游客。从功能上看, 机器人集成了多种传感器环境感知技术、语音交流技术和路径计算技术。北京人形机器人创新中心推出的中国首套全自主无人化人形机器人导览方案, “慧思开物”通用具身智能平台为其提

供了强有力支持,在此基础上实现了全自主导览、拟人化交流、多机器人协调控制以及整个家庭物联网设备协同工作的强大功能。多模态融合感知系统是“感知基石”,可以准确获取环境中的语义信息以及几何结构,从而帮助导览机器人进行任务制定及路径规划。慧思开物平台打造的“感知-决策-执行”的全流程解决方案,基于以大模型为代表的具身“大脑”以及基于数据驱动的具身“小脑”,让导览机器人可以辨别行人、展品、障碍物等物体,具备良好的定位能力和行走能力。随着大模型的发展,导览机器人已经可以承担更为繁重的工作,在博物馆、政府机关等地方得到应用。

2 智慧导览机器人运行存在的问题

2.1 环境适应能力不足问题

环境适应能力不足是最主要的安全隐患。强光变化造成视觉 SLAM 失效,浓密树林造成 GPS 信号被阻挡,玻璃幕墙对激光雷达造成反射干扰。在电力变电站中,设备密集、地面湿滑、电缆沟盖板众多,且存在强电磁干扰,对机器人的环境适应性提出了更高要求。传统导览机器人在复杂的室内环境中容易出现对于移动障碍物避让不够灵敏的问题,“导航-交互”一体式的解决方案需要结合激光雷达、摄像头、IMU 等多种传感器的数据进行 SLAM 深度融合,在此基础上采用综合方法来避开复杂环境中的障碍物^[1]。在风景名胜区内,由于树木密集、GPS 信号易被遮挡的情况,对准确导航以及安全行驶提出了更高的要求。电力行业的变电站同样存在 GPS 信号遮挡问题,为此地面电力巡检机器人采用北斗三号 RTK 差分定位与激光/视觉 SLAM 融合导航方案,实现在无 GPS 地下场景中±2cm 的定位精度。地面湿滑、有坡度或者狭窄的道路都是长期存在的问题。

2.2 导航定位精度不足问题

导航定位精度不高会造成安全问题。T/SZRA 001-2026 要求位置误差不超过 10cm、姿态角误差不超过 5°,但是很难一直达到这个标准。在电力巡检领域,对定位精度的要求更为严苛——地面电力巡检机器人设计标准要求开阔场景平面定位精度±1cm,高程精度±2cm,以避免误碰带电设备。视觉 SLAM 在低纹理情况下容易失败,惯性测量单元漂移导致误差增加。具身智能系统的感知-决策-执行形成一个环路,在这个过程中存在风险传递的过程,因此导航定位的小误差会在之后被无限放大成为大问题。例如,在变电站巡检中,定位误差的累积可能导致机器人偏离预定路径,误入带电间隔或造成设备损坏。跟随模式下目标移动速度快造成反应迟缓,机器人就会走错

道路进入不允许通行的地方。

2.3 人机交互稳定性问题

人机交互稳定性不足带来诸多问题。T/SZRA 001-2026 要求头部/颈部最大允许力小于等于 10N,躯干小于等于 20N,四肢小于等于 30N,手部小于等于 5N,但是突然的撞击还是会超过这个数值。此外,基于视觉-语言-动作模型的机器人会遇到新的安全隐患:被感染的 VLA 模型可以在感知输入上施加对抗性干扰并将其转换为有害的动作,在视觉、语言和状态等多个方面都存在风险。在电力操作机器人中,VLA 模型被用于开关柜操作、变电柜状态识别等关键任务,一旦模型遭受对抗性攻击,可能引发开关误操作、设备状态错判等严重后果。VLA 的安全问题有不可逆的危害、多种类型的攻击面以及长时间运行中累积的误差,语义对齐并不意味着动作对齐,同样的一个危险命令在文字上会被阻止,但是在执行层面却没有限制^[2]。例如,一句“检查开关状态”在文字上无害,但若攻击者通过视觉贴片诱导机器人错误识别开关位置,则可能导致误操作,危及电网安全。

2.4 网络安全防护不足问题

网络安全防护薄弱也是新型风险。GB/T 45502-2025《服务机器人信息安全通用要求》已于 2025 年 10 月发布并开始施行,提出了服务机器人的安全要求以及检测方法等,但是市场上大部分产品的防护能力仍然较弱。在电力行业,智能巡检机器人通过 5G 网络将高清视频、红外图像等敏感数据实时回传至集控中心,这些通信链路可能成为攻击者的突破口,一旦被控制,攻击者可通过篡改路径指令使机器人撞击关键设备。一位安全专家对其所在市场上一款商用具身智能机器人进行了一次渗透测试,在短短不到 8 个小时的时间内就发现了全部问题并最终成功实现对其控制。类似的渗透测试在电力巡检机器人上也暴露出远程控制权限缺失、通信加密不足等问题。在 GEEKCON2025 的安全极客大赛上也展示了两台机器人被“劫持”的情况,其中一个连接网络的机器人被黑客控制之后,另一个不连接网络的机器人也通过近距离的方式被“劫持”,供黑客随意摆弄。对于电力行业而言,这种“劫持”风险直接威胁电网运行安全——一台被控制的巡检机器人可能故意撞击变压器或误拉隔离开关,造成大面积停电事故。数字世界的安全隐患可以立即转变为对人身危害甚至是威胁到人们的生命安全。

3 智慧导览机器人安全风险防控优化对策

3.1 完善安全风险识别体系

完善风险识别是防控基石。可以依据环境感知、导航

决策、人机交互、网络通信四个方面进行分类。具身智能的安全框架需要从“技术可控”到“系统协同”再到

“社会对齐”，建立具有鲁棒性和适应性的系统。如表1所示。

表1 智慧导览机器人辅助运行典型安全风险识别表

风险类别	风险来源	具体风险描述	风险等级	初步防控措施
环境感知	光照变化	低光照导致视觉 SLAM 失效	高	多模态融合，红外补光辅助
环境感知	透明障碍物	玻璃幕墙导致激光雷达透射漏检	高	超声波+视觉补充检测
导航决策	信号遮挡	GPS 遮挡定位误差扩大	中	激光 SLAM+IMU 融合定位
导航决策	长时漂移	惯性导航误差累积	中	定期回环检测，设置定位基准点
人机交互	指令攻击	LLM 越狱攻击诱导危险动作	高	语义安全过滤，敏感指令二次确认
人机交互	物理碰撞	运动与人流轨迹冲突	高	限速降速，急停距离 $\leq 0.5\text{m}$
网络安全	远程控制	隐藏管理接口被利用篡改参数	高	关闭非必要接口，双向身份验证
网络安全	固件篡改	未签名固件植入恶意程序	中	可信启动链+固件签名验证

3.2 提高智能感知与避障能力

提高智能感知与避障能力是智慧导览机器人在新能源场站实现安全运行的关键。针对华电河北新能源光伏及风电场多风沙、强日照、设备密集等特点，单一传感器易受干扰，需构建多源异构融合感知体系。中国华电基于“低成本感知、高可靠应用”准则，深度整合多传感器融合与计算机视觉技术，打造了“场站感知+区域决策”的智慧管理生态。机器人应融合激光雷达、视觉相机、毫米波雷达及 RTK 高精度定位，采用紧耦合 SLAM 算法，在光伏阵列重复纹理或风机阴影区实现厘米级建模与鲁棒定位。中国电科院打造的电力具身智能大模型，将多模态数据融合感知与端到端动作生成统一，提供精准的“空间感”与“方向感”，使其在密集设备中灵活避障。机器人还需实时识别运维车辆、施工人员等动态障碍物并预判轨迹，遇拥堵自动重规划路径。目前华电河北冀北新能源已在场站部署集成 AI 识别的智能机器人，并与山火监测、无人机系统互联互通，形成空天地协同感知网络。通过上述技术集成，智慧导览机器人可替代人工在高温、高寒、高风险环境下安全作业，为新能源场站无人化运行提供可靠保障。

3.3 优化导航定位与控制技术

导航定位及控制对智慧导览机器人的正常工作起决定作用，从技术上讲，需采用“全局参考定位+局部实时定位+自主定位校正”的多层次定位方案。SLAM 是使机器人能够实现自主导航的关键技术，通过激光雷达、IMU 以及摄像头等设备完成未知环境中精确定位以及建图功能，在室内场馆等无 GNSS 信号环境下主要使用激光 SLAM 进行环境栅格化建图，并结合视觉特征点提高闭环检测鲁棒性。在电力变电站中，由于金属设备密集、电磁干扰强烈，GNSS 信号常被遮挡，更依赖激光 SLAM 与视觉 SLAM 的深度融合。慧思开物平台所构建的“感知-

决策-执行”的端到端技术框架，在基于 AI 大模型的具身“大脑”以及基于数据训练的小脑的驱动下可以准确获取到周围环境中的语义属性以及几何属性，在客流量较大时可自主进行路径的选择，使任务适应当前环境变化。在变电站巡检中，当多台机器人同时作业或人员进入设备区时，机器人应能自主调整路径，避免与带电设备发生危险接近。对于长时间漂移的问题，可以在场站的重要位置部署 UWB 基站或者二维码视觉参考点以提供绝对位置的信息。电力行业可在变电站的关键设备间隔、转角处部署 UWB 定位标签或二维码参考点，将定位精度控制在 $\pm 2\text{cm}$ 以内。而在运动方面，根据 T/SZRA 001-2026 的要求急停的距离小于等于 0.5m ，停留的时间小于等于 1s ，应该围绕这个目标去改进运动控制算法，在出现意外情况的时候可以及时地停下来。对于电力巡检机器人，急停距离要求更为严格，通常要求 $\leq 0.2\text{m}$ ，以防止与带电设备发生碰撞。

3.4 加强网络安全与数据保护

加强网络安全与数据保护是智慧导览机器人在新能源场站安全运行的重要保障。针对华电河北新能源风光场站接入终端多、无线传输风险高等特点，需构建覆盖数据采集、传输、存储、处理全生命周期的纵深防护体系。遵循电力监控系统“安全分区、网络专用、横向隔离、纵向认证”的十六字原则，机器人在巡检中采集的设备参数、红外图像、无人机协同画面等敏感数据，必须采用国密算法进行端到端加密传输，并经由正向隔离装置从生产控制区单向传输至管理信息区，再经安全加密后上送云平台，确保生产控制区外的攻击指令无法侵入内网。参照国家标准 GB/T 45502-2025《服务机器人信息安全通用要求》，应对机器人的身份认证、访问控制及 USB 等外设接口实施白名单管控，防止非法设备接入；同时部署工业防火墙与工业审计系统，实现外设病毒查杀、接入授权、数据保

护与日志留存,保障场站网络与数据不被非法篡改^[3]。在数据存储层面,机器人采集的历史巡检数据及设备台账应进行分级分类存储,关键数据采用加密数据库并定期备份至异地容灾节点,防止因硬件故障或恶意攻击导致数据丢失。《能源行业数据安全管理办法(试行)》自2026年7月1日起施行,要求数据处理者建立健全数据安全管理制度,定期开展安全评估。河北华电冀北新能源已提前完成下属19个风光电场的等保测评与安全防护评估,对智慧导览机器人的接入方案进行了专项渗透测试与漏洞扫描,为机器人的合规运行奠定了坚实基础。通过上述覆盖“端-管-云-存”的多层防护措施,智慧导览机器人可在无人值守场站中实现安全、可靠的数据交互,确保发电设备7×24h智能监测数据真实可信、异常预警秒级可达,有力支撑华电河北新能源的智慧场站数字化转型。

3.5 建立智能化运维管理机制

智能化运维管理制度是保证智慧导览机器人正常工作的必要条件。“慧思开物”通用具身智能平台具有全局调度能力,在此基础上提供支持MQTT、TCP/IP等多种通信方式的开放接口,使导览机器人可以自己控制整个园区内的所有物联网设备,例如当机器人带领顾客到达某个重要区域后,可以自动开启该处的灯,大屏播放相关视频以及展示的内容也同时开始播放,整个过程几乎无延迟,只需要50ms左右^[4]。在智能变电站中,巡检机器人可与站内物联网设备联动,如自动开启设备间照明、调节摄像机预置位、触发环境监测传感器等,实现全站智能化协同。从运维角度出发,要制定每日检查、每周检查及每月检查的工作计划,其中日常检查主要是对传感器进行清洁、检查电池电量以及急停按钮是否正常工作;每周检查是对各个齿轮组磨损情况及各固定部件情况进行检查;每月检查是进行全方面导航精度校准以及全面系统检测等。电力行业应针对变电站环境特点,增加对机器人绝缘性能、电磁兼容性的专项检查。2026年2月28日发布的《人形机器

人与具身智能标准体系(2026版)》规定了安全类强制标准包括机械碰撞保护、夹持危险防护、运动极限限位、电气等方面内容,并对功能安全提出ISO26262、IEC61508的要求并且有故障检测和紧急停止的要求。电力巡检机器人还应符合DL/T 1498-2016《变电站智能机器人巡检系统技术规范》等相关电力行业标准。

4 结语

智慧导览机器人辅助运行的安全风险识别与防控是包括感知、导航、交互、通信及运维等方面的技术综合性工作。对导览机器人的工作方式以及其自身的特点进行分析,总结出环境适应能力差、导航定位精度低、人机交互不稳定以及网络信息安全等问题作为主要的风险点,并针对这些风险提出相应的解决方案,即完善风险识别机制、提升智能化感知与防撞能力、增强导航定位与控制技术、强化网络信息安全及数据安全保障、实行智能化运维管理等措施,多种措施相互配合、逐层推进,形成从头到尾的整体化安全防护机制。在电力行业,上述防控措施同样适用于变电站巡检机器人、电力营业厅导览机器人等场景,对于保障电网安全稳定运行具有重要意义。

[参考文献]

- [1]梅术龙,朱林峰,潘小芳,等.智慧导览机器人的研究与应用[J].新型工业化,2021,11(11):90-93.
- [2]贾迪.博物馆导览机器人人机交互系统的设计与实现[D].北京:北京交通大学,2020.
- [3]葛希迦.室内导览机器人多传感器融合系统设计与导航试验研究[D].金华:浙江师范大学,2023.
- [4]李哲,林驰,郭晓明.高校智能导览机器人创新应用[J].中国教育网络,2023(6):76-77.

作者简介:吴晓杰(1993—),男,河南辉县人,工程师,华北水利水电大学热能与动力工程(水动方向)专业毕业,现就职于华电河北新能源有限公司,从事新能源场站集控调度管理工作。