

浅谈船舶电气自动化控制安全性问题

刘 松

武汉听涛海洋工程有限责任公司 湖北 武汉 430000

摘 要：随着船舶工业朝着智能化、大型化、高效化方向飞速发展，船舶电气自动化控制技术的应用日益广泛。它在提升船舶运行效率、优化航行性能、降低人力成本等诸多方面发挥着关键作用。然而，船舶运行环境复杂多变，电气自动化控制系统面临着诸多安全性挑战，一旦出现故障，不仅会影响船舶正常航行，甚至可能引发严重的海难事故。本文深入剖析船舶电气自动化控制中的安全性问题，详细阐述相应的防范措施，旨在提升船舶电气自动化控制系统的安全性与可靠性，保障船舶航行安全，推动船舶工业可持续发展。

关键词：船舶电气；自动化控制；安全性；故障防范

引言：在全球经济一体化进程加速的当下，海洋运输作为国际贸易的主要载体，承担着海量货物的周转任务。船舶作为海洋运输的核心工具，其技术水平的不断革新是提高运输效率、保障航行安全的关键驱动力。船舶电气自动化控制技术应运而生，它实现了船舶动力系统、导航系统、舱室环境控制系统等多领域的智能化管控，极大地减轻了船员劳动强度，提高了船舶运营精准度。但与此同时，船舶长期航行于海洋环境，面临着高温、高湿、高盐雾以及复杂电磁环境等恶劣条件，电气自动化控制系统犹如在“险滩”中前行，安全性问题备受瞩目。深入探究这些问题并寻求有效解决之道，对于维护船舶的正常运行、保护船员生命财产安全以及海洋生态环境具有举足轻重的意义。

1 船舶电气自动化控制安全性问题剖析

1.1 硬件故障风险

1.1.1 电气元件老化与损坏

船舶电气系统中的各类元件，如接触器、继电器、断路器、传感器等，长期在恶劣环境下运行，频繁承受电应力、机械应力以及化学腐蚀作用。高温加速元件绝缘材料老化，降低其绝缘性能，易引发短路故障；高湿、盐雾环境使金属部件生锈腐蚀，接触电阻增大，导致发热甚至断路；机械振动可能造成元件引脚松动、焊点开裂，影响信号传输与电路通断控制。例如，某远洋货船的机舱温度传感器，因长期处于高温、高湿且伴有油雾的环境，引脚腐蚀断裂，致使温度监测数据失真，船舶主机冷却系统未能及时调整冷却水量，主机温度过高，险些造成停机事故。

1.1.2 电源系统不稳定

船舶电源供应的稳定性直接关乎电气自动化系统的正常运行。海上航行时，发电机组可能因原动机故障、

调速器失灵、负载突变等原因，输出电压、频率波动超出允许范围。电压过高可能击穿电气设备绝缘，过低则使设备无法正常启动或运行异常；频率波动影响异步电动机转速稳定性，进而干扰泵、风机等设备的正常工作，甚至引发共振，损坏设备。此外，蓄电池作为备用电源，若充放电管理不善，出现过充、过放或极板硫化等问题，在主电源故障时无法及时可靠供电，将导致关键系统瘫痪，如船舶应急照明、通信导航系统失效，给船舶安全带来巨大隐患^[1]。

1.2 软件漏洞隐患

1.2.1 程序错误与逻辑缺陷

船舶电气自动化控制软件通常较为复杂，涵盖大量控制算法、逻辑判断以及数据处理模块。在软件开发过程中，由于程序员疏忽、需求理解偏差或测试不充分，可能遗留程序错误与逻辑缺陷。例如，在船舶自动舵系统软件中，对舵角反馈信号的处理逻辑错误，当舵机实际达到最大舵角时，控制系统未能及时停止指令输出，导致舵机持续过载运转，损坏舵机设备，影响船舶操纵性能，在复杂海况下极易引发碰撞事故。

1.2.2 软件兼容性问题

随着船舶电气设备不断升级换代，新安装的自动化控制软件可能与原有系统软件或硬件存在兼容性问题。不同厂家生产的设备，其通信协议、数据格式、操作系统版本各异，若软件集成过程未充分考虑兼容性，可能出现数据传输错误、设备无法协同工作甚至死机等现象。如船舶机舱监测报警系统升级后，新软件与部分老旧传感器通信异常，频繁误报警，干扰船员对设备真实运行状态的判断，延误故障处理时机。

1.3 电磁干扰危害

1.3.1 内部电磁干扰

船舶自身电气设备众多,如大功率电机、变压器、变频器等,在运行过程中会产生强烈的电磁辐射。这些电磁场相互叠加,干扰附近敏感电子设备的正常工作。例如,船舶电力推进系统中的变频器,采用高频PWM调制技术,会产生丰富的高次谐波,通过电源线、信号线传导至机舱控制系统中的PLC、工控机等设备,造成数据采集误差、控制指令错乱,影响船舶推进系统的稳定运行,甚至引发失控风险^[2]。

1.3.2 外部电磁干扰

除船舶内部电磁源外,外界环境中的电磁信号也对船舶电气自动化系统构成威胁。例如,在靠近通信基站、雷达站或军事管制区域航行时,高强度的射频信号可能耦合进入船舶通信、导航、电子海图等系统,使设备显示异常、信号中断或产生错误导航信息,误导船舶航行方向,增加碰撞、搁浅等事故发生概率。

1.4 网络安全威胁

1.4.1 网络攻击风险

随着船舶数字化、网络化进程加快,船舶电气自动化系统逐渐接入互联网或卫星通信网络,用于远程监控、软件升级、数据传输等功能,这也为黑客攻击打开了“方便之门”。恶意攻击者可能通过网络漏洞入侵船舶控制系统,篡改控制指令、窃取船舶航行数据、破坏关键设备运行参数,使船舶陷入危险境地。如曾发生的一起案例,黑客攻击某油轮的压载水控制系统,恶意调整压载水舱液位,导致船舶重心失衡,严重倾斜,险些造成原油泄漏事故。

1.4.2 数据泄露隐患

船舶运营过程中会产生大量敏感数据,包括货物信息、船员信息、船舶航行轨迹等,这些数据存储于自动化控制系统的数据库中。若网络安全防护不到位,数据可能被窃取、篡改或泄露,不仅侵犯个人隐私、商业机密,还可能被不法分子利用,危害国家安全。例如,航运公司内部网络遭受黑客攻击,船舶货物清单、装卸计划等数据泄露,不法分子借此进行货物盗窃、走私等违法活动,扰乱航运市场秩序。

1.5 人为操作失误因素

1.5.1 船员专业技能不足

船舶电气自动化技术日新月异,对船员专业素养提出了更高要求。部分船员未能及时跟上技术更新步伐,对新型电气设备操作不熟练,在设备调试、参数设定、故障排查等环节容易出现失误。例如,在操作船舶电力管理系统(PMS)时,船员因不熟悉新软件界面与功能,误将重要负载的供电优先级设置错误,当主电源出

现故障切换至备用电源时,关键设备供电中断,影响船舶安全航行。

1.5.2 违规操作行为

在实际航行中,一些船员为图方便或赶时间,违反电气设备操作规程,如在未切断电源的情况下进行设备检修、私拉乱接电线、超功率使用电器等。这些违规行为极易引发电气火灾、短路故障,对船舶安全构成直接威胁。如某客船船员违规在船员舱室使用大功率电炉,过载引发电线起火,若火势蔓延,将危及全船乘客与船员生命安全。

2 船舶电气自动化控制安全性防范措施

2.1 优化硬件设计与维护

2.1.1 选用高品质、耐环境电气元件

在船舶电气系统设计选型阶段,优先选用符合船用标准、具备高可靠性、耐高温、耐高湿、抗盐雾腐蚀的电气元件。如采用密封型继电器、防水型传感器,外壳选用不锈钢或经过特殊防腐处理的材料;对于关键设备,可适当提高元件冗余配置,实现故障切换,提高系统容错能力。同时,建立严格的元件采购质量管控体系,对进货元件进行抽检,确保质量达标^[3]。

2.1.2 加强电源系统稳定性保障

为船舶发电机组配备高精度调速器、电压调节器,实时监测并调整机组输出电压、频率,使其稳定在额定范围内。采用不间断电源(UPS)作为关键设备的过渡电源,确保在主电源短暂波动或切换期间,设备供电不间断;优化蓄电池管理系统,通过智能充放电控制技术,防止蓄电池过充、过放,定期进行活化维护,延长蓄电池使用寿命,保障备用电源可靠。

2.2 强化软件测试与升级

2.2.1 严格软件开发流程管控

遵循软件工程规范,采用模块化、结构化设计方法,降低软件复杂度;在开发过程中,进行代码审查、静态分析,及时发现潜在程序错误;完成软件开发后,进行全面功能测试、边界值测试、异常情况测试,模拟船舶各种运行工况,确保软件逻辑正确、运行稳定。例如,在船舶自动化电站控制系统软件测试中,模拟发电机过载、短路、调速器失灵等多种故障情况,检验软件的故障诊断与处理能力。

2.2.2 持续关注软件兼容性与更新

建立软件兼容性评估机制,在新设备或软件安装前,对其与现有系统的兼容性进行详细测试,提前解决潜在问题;密切关注软件供应商发布的补丁、升级版本,及时更新,修复已知漏洞,优化软件性能;同时,

保留软件旧版本备份,以便在升级出现问题时能够快速恢复,确保船舶电气自动化控制系统正常运行。

2.3 增强电磁屏蔽策略深化

2.3.1 优化船舶电气设备布局的精细化考量

在船舶设计的初期阶段,电气设备的布局规划就需细致入微,以最大化地减少电磁干扰。大功率、强电磁干扰源设备,如发电机、大型电动机等,应被精心安排在与敏感电子设备(如导航设备、通讯系统等)尽可能远的区域,通过物理距离来削弱电磁辐射的影响。此外,利用金属屏蔽罩和线槽对敏感信号线和电源线进行包裹,不仅能有效阻断电磁干扰的传播路径,还能通过屏蔽层的可靠接地,将干扰电流引入大地,进一步降低电磁干扰。在机舱等电磁环境复杂的重点区域,采取敷设电磁屏蔽地板和天花板的措施,可以构建一个相对封闭的电磁防护空间。这种空间能够显著降低外界电磁干扰对内部敏感设备的影响,确保设备在恶劣电磁环境中仍能稳定工作^[4]。

2.3.2 电磁干扰滤波器的精准选择与定期维护

在船舶电气系统的进线端、关键设备的电源输入端以及信号接口处,安装电磁干扰滤波器是提升设备抗电磁干扰能力的关键步骤。滤波器的选择需根据电磁干扰的频段特性进行,低通、高通、带通或带阻滤波器应被精准地应用于不同的场景,以滤除电源线、信号线上的高频干扰成分。为确保滤波器的持续有效工作,定期的性能检测是必不可少的。通过检测,可以及时发现并更换失效的滤波器,防止因滤波器失效而导致的电磁干扰问题。这种定期的维护措施,对于保持船舶电气系统的整体稳定性和可靠性至关重要。

2.4 构建网络安全防护体系

2.4.1 网络隔离与访问控制

将船舶电气自动化控制系统划分为不同安全区域,如机舱控制系统、驾驶台导航系统、船舶办公网络等,采用防火墙、网闸等设备进行隔离,限制区域间不必要的网络访问;设置严格的用户身份认证机制,为船员、管理人员、远程维护人员分配不同权限账号,采用密码、指纹、数字证书等多因素认证方式,防止非法登录;定期更新网络设备固件,修复安全漏洞,确保网络边界安全。

2.4.2 入侵检测与数据加密

部署入侵检测系统(IDS)/入侵防范系统(IPS),实时监测网络流量,对异常流量、攻击行为进行识别报警,并自动采取阻断措施;对船舶关键数据,如航行数

据、设备运行参数、货物信息等,在存储与传输过程中进行加密处理,采用对称加密与非对称加密相结合的算法,确保数据机密性、完整性,防止数据被窃取、篡改^[5]。

2.5 加强人员培训

2.5.1 专业技能培训常态化

航运企业应定期组织船员参加船舶电气自动化技术培训课程,邀请专家、设备厂商技术人员授课,内容涵盖新型电气设备原理、操作方法、故障诊断与排除技巧等;在船舶上新设备安装调试阶段,安排船员全程参与学习,使其熟悉设备安装流程、调试要点,为后续独立操作与维护奠定基础;通过实际案例分析、模拟操作训练等方式,提高船员解决实际问题的能力。

2.5.2 安全意识教育强化

将电气安全操作规程、网络安全知识纳入船员日常培训体系,通过安全讲座、宣传手册、事故警示片等形式,强化船员安全意识;定期开展安全演练,模拟电气火灾、网络攻击等应急场景,让船员熟练掌握应急处置流程,提高风险防范能力;建立安全考核机制,将船员安全操作表现与绩效挂钩,激励船员自觉遵守安全规定。

结论:船舶电气自动化控制安全性问题是一个涉及硬件、软件、电磁环境、网络通信以及人员等多方面的复杂系统工程。通过深入剖析各类安全性问题,针对性地采取优化硬件设计与维护、强化软件测试与升级、增强电磁屏蔽、构建网络安全防护体系以及加强人员培训等防范措施,能够有效提升船舶电气自动化控制系统的安全性及可靠性。在未来船舶工业发展中,随着技术不断创新,新的安全性挑战必将接踵而至,持续关注、深入研究并及时解决这些问题,是保障船舶航行安全、推动海洋运输事业蓬勃发展的永恒主题,为全球经济繁荣保驾护航。

参考文献

- [1]张一鸣,李华.船舶电气自动化系统硬件故障诊断与容错技术研究[J].船舶工程,2024(06):75-78.
- [2]刘悦,陈杰.面向船舶电气自动化控制的软件可靠性评估与优化策略[J].中国造船,2024(05):62-65.
- [3]王强,赵刚.船舶电磁环境对电气自动化设备干扰特性及防护措施[J].船舶电力推进,2024(04):55-58.
- [4]孙晓琳.船舶网络安全威胁态势感知与智能防御体系构建[J].航海技术,2024(03):48-51.
- [5]周浩,吴迪.船员人为因素对船舶电气自动化控制安全影响及培训对策[J].水运管理,2024(02):30-33.