电气控制与机房维护的结合研究

夏 岩
宁夏回族自治区邮政业安全中心 宁夏 银川 750021

摘 要：网络安全是国家安全的重要组成部分，事关国计民生。随着信息技术的快速发展，电气控制与机房维护在保障企业信息数据安全和系统稳定运行中扮演着至关重要的角色。本文旨在探讨电气控制与机房维护的紧密结合，分析两者在保障系统可靠性、安全性和高效性方面的协同效应，筑牢网络及数据安全防线，并提出相应的管理策略和技术措施。

关键词：电气控制；机房维护；结合

引言：电气控制作为电力系统和自动化技术的核心，为机房内各类设备提供稳定可靠的电力供应和自动化管理；而机房维护则关注于硬件、软件、网络及环境的全面保障，确保机房设施的正常运行。将电气控制与机房维护紧密结合，对于提升整体系统的稳定性和安全性具有重要意义。在电气控制方面，确保了设备的精准运行和高效性能，保障生产过程的稳定与安全。通过精确的电气控制，能有效提高能源利用效率，降低能耗。而机房维护更是至关重要。良好的机房维护可延长设备寿命，减少故障发生概率。它保障了数据的安全存储与传输，为企业的信息化运作提供坚实基础。同时，能提升系统的可靠性和稳定性，确保在关键时刻不出现宕机等问题，为企业的持续发展保驾护航。

1 电气控制与机房维护的结合点

1.1 电源管理与分配。

电气控制中的电源管理系统（如UPS、发电机等）为机房提供不间断的电力支持，而机房维护则需定期检查这些设备的运行状态，确保其性能稳定。同时，机房内的配电系统也需根据电气控制的原则进行合理设计，确保电力分配的均衡性和安全性。

1.2 环境监控与调节。

电气控制中的温湿度控制系统可自动调节机房内的环境条件，而机房维护则需定期检查和校准这些系统，确保其准确性和可靠性。此外，机房内的环境监控设备（如温湿度传感器、烟雾探测器等）也是电气控制与机房维护的重要结合点，它们共同为机房的安全运行提供保障。

1.3 自动化控制与运维管理。

运用通过PLC（可编程逻辑控制器）、DCS（分散控制系统）等自动化控制设备，实现对机房内设备的远程监控和自动化操作。通过监控系统实时掌握设备状态和运行数据，及时发现并处理潜在问题，生成详细的能源使用报告和分析图表，帮助运维人员了解能源使用情况并制定相应的节能措施。减少人工干预和误操作的风险[1]。

2 现阶段基本情况

2.1 业务流程基本情况。

目前各快递企业信息系统服务器均部署在公司总部，宁夏省区快递公司自建小规模信息机房，配备防火墙、VPN等设备，通过信息安全系统登录企业总部访问业务系统，办公区员工电脑安装有企业分发的账号及密码，各快递网点仅有快递收派业务系统权限，收寄过程是通过企业专用设备登录企业分发的账号及密码后录入客户信息，信息录入成功后客户信息将加密保存，形成隐私面单。再次调取客户信息时已无法看到完整内容。

2.2 信息安全基本情况。

各寄递企业在省级的快递公司均未部署存储服务，业务系统建立在企业总部，快递公司访问业务系统均通过本地网络登录总部搭建的业务系统，如申通的鲁班系统、中通的火盾系统通过VPN网络访问总部业务系统。在员工PC终端设置了U盘等外部存储设备的管控，无法直接复制电脑数据，在需要调取客户信息是需向企业总部申请，由企业总部调取后转发至省级快递公司。快递公司内部无线WFI采用账号绑定机制，只有内部员工获取总部分发的登录账号才可以接入无线网络[2]。

3 机房维护常见的问题

3.1 企业机房环境设施差。

电底盒机房环境差，基础设施配置不全。机房内部存放杂物、线缆乱绕、交叉、甚至存在裸露线缆、接头松动等问题、灭火器不适配机房应用场景、未采用机柜PU，机柜内存有各种型号的电源插排并且连接混乱，有较大的消防隐患。因经费不足、人员专业能力不足等客观因素，致使机房基础环境设施不符合相关规定，无能

力优化网络拓补结构。

3.2 企业机房管理存在安全隐患。

安全管理弱，网络安全意识不足。未配备任何制冷设备，机房设备电源由楼层市电底盒引出，未配置独立配电箱。未配备任何制冷设备，机房内部过热，部分设备已经严重过热；机房内部存放有其他单位的网络机柜，虽进行人员出入登记，但存在极大的信息泄露安全隐患。机房窗户密封不严，地面灰尘较多，灰尘会对机房精密设备的运行产生严重影响。机房未铺设防静电地板。未建立机房管理制度，对进出机房的人员进行身份验证和登记。未安装电子门禁系统及视频监控系统，无法有效控制进入机房人员。

3.3 企业网络设备安全防护能力不强。

企业配备互联网防火墙、广域网防火墙业务防火墙和入侵防御系统，但在配置上存在安全风险，设备服役年限较长，软件版本过低，无法有效保障办公网络安全稳定。网络结构乱，网络配置优化不深。比如某企业申请的100M移动互联网专线经调研检测未达到预期的使用效果。各普遍存在无线WIFI、视频监控接入办公网络的情况，不利于网络的持续稳定运行。

3.4 企业网络安全管理意识不强。

快递行业作为服务密集型产业，员工数量众多且流动性大，在调研中发现各快递企业普遍对网络及数据安全的重要性认识不够，一是企业机房管理混乱。机房内部存放杂物、线缆杂乱无序、灭火器不适配机房应用场景，有较大的消防隐患；个别企业机房长期无人打扫，灰尘遍布，严重影响设备使用寿命；二是企业培训缺失。快递企业在收派各个环节均会有大量数据产生，不管是企业管理人员或者末端快递员，都有接触数据信息的条件，但调研中发现企业对员工缺乏网络及信息安全相关培训，员工对网络安全意识防范不强。

3.5 企业数据处理流程不规范。

企业从数据收集、存储、传输、使用直至销毁，每一个环节都需严格遵守相关操作规范和流程控制。然而在实际操作中，部分快递企业存在流程缺失、执行不严等问题，如快递公司下设的网点、第三方驿站等未对数据进行加密处理便进行传输、未定期对存储介质进行安全检查、未制定明确的数据销毁政策等。这些不规范的操作不仅增加了信息泄露的风险，还可能导致数据被非法获取、篡改或滥用，给用户和企业带来不可估量的损失。

3.6 企业网络安全管理制度不健全。

完备的管理制度能压实职工的网络和数据安全责任。在调研中发现，一部分企业存在网络和数据安全管理组织机构不健全、管理制度缺失的问题，一部分企业尽管建立了相关管理制度，但制度内容空泛、职责边界不明确，指导工作意义不大。

4 诊疗优化内容

4.1 明确信息安全责任。

首要任务是确立企业全体员工在信息安全领域的清晰职责分工。通过建立责任到人的管理机制，使每位员工都能深刻理解其岗位所承载的信息安全责任。这不仅有助于提升整体信息安全防护水平，还能在发生安全事件时迅速定位责任，采取有效应对措施。

4.2 制定信息安全政策。

详尽的信息安全政策是体系构建的基石。政策需覆盖数据生命周期的各个环节，包括但不限于数据的收集、存储、处理、传输及最终销毁。每一环节都应设定明确的操作规范与标准，确保所有操作均符合国家法律法规及行业监管要求。

4.3 实施权限精细管理。

合理的权限分配是减少信息泄露风险的关键。企业应根据员工职责与岗位需求，实施精细化的权限管理策略。遵循最小权限原则，仅授予员工完成工作所必需的信息系统访问权限，避免权限过大导致的潜在风险。同时，定期对权限进行审查与调整，确保权限分配的合理性与时效性[3]。

4.4 加强机房安全管理。

选配专业人员对机房加强管理，管理人员应具备机房设备运维检修、机房网络拓扑结构梳理调整等基础管理能力。同时，建立机房相关管理制度和各类台账，重视机房各类应急防护工作，如防火、防水、防黑客攻击等，有效避免各类事故发生。移除各企业机房内堆积杂物和垃圾，全面清理机房环境卫生。

4.5 提高网络安全意识。

企业要牢固树立风险意识，切实担负起网络安全工作责任，分解细化任务，层层落实责任，在学网、懂网、用网中化被动为主动，不断增强网络安全的保障能力。明确网络安全的主要目标、基本要求、工作任务、保护措施，让“网络信息人人共享、网络安全人人有责”的意识落地生根，筑牢网络安全防线，营造安全、和谐、稳定的网络环境。

4.6 设备检测与清洁常态化。

结合电气控制与机房维护的需求，制定全面的维护计划。涵盖电源系统、配电系统、环境监控系统、自动化控制系统等方面，确保各项维护工作有序进行。同时，对机房内的硬件设备进行检查，包括防火墙、路由

器、交换机等设备的运行状态；检查设备是否存在异常和故障，包括设备的运行噪音、温度、风扇转速等。对异常设备进行排查维修，保障机房设备运行稳定。对机房内网络设备进行清洁，清除设备上的灰尘和杂物，朵物确保设备正常通风。同时，清洁服务器风扇滤网，防止积尘影响风扇散热效果[4]。

4.7 网络优化及故障排查。

将企业机房连接在办公网络上的无线WIFI拆除并重新配置到独立于办公网的互联网设备上，保障办公网的安全。针对企业提出的设备故障及网络故障问题，逐个进行排查，化解网络安全隐患，提高网络性能、有效保障业务连能续性，并帮助各市绘制优化后的网络结构拓扑图。

4.8 进行线缆梳理。

梳理机房网线、光纤、电源线走向，根据现场环境对所有线缆进行整理、捆扎并制作、粘贴标签；拆除机柜内多余线缆、小交换机、光猫等设备；拆除机柜内不同型号的电源插排替换为机柜专用PDU。

4.9 落实机房建设标准。

机房基础设施完善不仅能保障机房的设备安全稳定运行，也能为机房运维人员提供安全的工作环境。需定期对机房内的电气系统、设备、环境等进行巡检和保养，确保各项设施处于良好的工作状态。巡检过程中应重点关注电气系统的安全性能、设备的运行效率以及环境的适宜性等方面。一是需铺设防静电地板。防止人体在接触主机、键盘等设备后导致静电荷释放，干扰设备运行及其内部电元件被击穿。二是需配置独立配电箱，有效的避免因其他供电区域电源故障而引起的机房设备运行中断、故障、损坏等现象。三是需配备制冷设备。机房内设备高度密集且不间断运行，不及时消除设备产生的热量，会导致设备过热，影响设备寿命。四是需增配气体灭火器（如二氧化碳灭火器），更适合用于保护重要设备和精密仪器免受损害。

4.10 建立健全机房安全管理制度。

利用现代信息技术手段，建立完善的监控系统，对机房内的电气系统、设备运行状态、环境参数等进行实时监测和预警。严格执行机房人员进出审批、登记制度，外来人员一律进行登记，无关人员不得入内；机房内服务器、网络设备、UPS电源、空调等重要设施由专人严格按照规定操作，严禁随意开关；维护人员应严格遵守机房操作规程，对各类设备、设施实行规范操作，并做好日常维护和保养，注意机房内日常温度、湿度、电压等参数变化，发现异常及时采取相应措施；保持机房整洁、卫生。机房设备摆放整齐有序。规范机房设备使用。机房带电设备较多，日常维护工作不要带电操作，应急带电操作也必须两人以上且装备绝缘设备才可进行，要时刻警惕触电的可能性，日常维护要规范使用设备、工具，不触及安全底线。

4.11 强化网络安全应急能力。

定期组织企业员工参加信息安全意识教育及技能培训，内容涵盖最新的信息安全威胁、防护策略及应急处置措施等。提高员工对信息安全的重视程度及应对能力。同时，设立考核机制以严肃责任落实，确保每位员工都能在日常工作中重视信息安全工作，全力守护用户个人信息。重视网络及数据安全防护，增强安全意识，制定网络和信息设备遭遇火灾、水患、黑客入侵、数据泄露等突发情况时的应急预案，并每年进行一到两次的应急演练，确保遭遇突发情况时可以最大程度的保护网络和数据安全。

结论

电气控制与机房维护的紧密结合是保障企业信息系统稳定运行的关键。通过提高网络安全意识，设备检测与清洁常态化，网络优化及故障排查，梳理线缆，落实机房建设标准和建立健全机房安全管理制度等措施，可以显著提升机房设施的稳定性和安全性，降低运维成本和能耗，提高运维效率和管理水平，为企业的发展提供坚实的支撑。

参考文献

[1]王金,王长春.高校云机房网络维护以及故障排除方法[J].好家长,2019,(11):137-138.

[2]郭俊文.机房通信网络安全隐患及防护技术分析[J].通信电源技术,2020,(08):55-57.

[3]王书田.计算机机房管理存在的问题及对策探讨[J].网络安全技术与应用,2019,(12):107-108.

[4]陈玉芬.高校实验室机房的建设与管理[J].电脑知识与技术,2019,(07):61-62.