# 电网调度自动化系统的安全问题分析

李洁荣

（国网河南省电力公司开封供电公司，河南 开封 475000）

**摘　要**　电网调度自动化系统的安全问题涵盖了多个方面，包括网络安全、设备安全、数据安全等，这些问题的存在可能会对电力系统的正常运行和稳定性造成严重影响，甚至导致安全事故的发生。因此，必须认真对待这些安全问题，并采取有效的措施来加强系统的安全性。本文结合实际，在分析电网调度自动化系统安全控制意义的同时，对相关的安全问题与建议进行解析，以期为相关人员提供借鉴。

**关键词**　电网调度；自动化系统；安全问题；人员操作安全；物理安全

**中图分类号**：TM76　　**文献标识码**：A　　**文章编号**：1007-0745(2023)08-0025-03

随着信息技术的迅猛发展和电力系统的现代化进程，电网调度自动化系统在电力行业中扮演着至关重要的角色。该系统利用先进的计算机技术和通信技术，实现了电力系统的远程监控、调度和控制，为电力运行提供了高效、精确的支持。但是，随着电网调度自动化系统的广泛应用，安全问题也日益凸显。所以分析系统安全问题，明确系统安全控制方法非常重要。

## 1 电网调度自动化系统安全控制意义

### 1.1 保障电力系统的稳定运行

电网调度自动化系统是电力系统的关键组成部分，其安全控制能够有效地防止安全漏洞、网络攻击和恶意操作等对系统运行的威胁。通过实施严密的安全措施，可以保障电力系统的稳定运行，提高供电可靠性和供电质量。

### 1.2 防范安全事故的发生

电网调度自动化系统的安全控制能够及时发现和排除潜在的安全隐患，减少安全事故的发生概率。通过加强设备的物理安全、完善的访问控制和权限管理，以及及时的故障诊断和维护，可以有效地减少设备故障和操作错误导致的安全风险。

### 1.3 保护关键数据的安全性

电网调度自动化系统涉及大量的关键数据，包括供电信息、负荷数据、能源交易数据等。安全控制能够保护这些数据的完整性、准确性和保密性，防止数据被篡改、泄露或损坏，确保数据在传输和存储过程中的安全性。这对于电力系统的运行决策和管理具有重要的意义。

### 1.4 提高系统的响应速度和效率

安全控制能够加强对电网调度自动化系统的监测和审计，及时发现和处理异常事件，提高系统的响应速度和效率。通过实施自动化的安全控制策略，可以减少人为因素的干扰和错误，提高系统运行的稳定性和可靠性[1]。

## 2 电网调度自动化系统的安全问题分析

电网调度自动化系统是现代电力系统运行和管理的关键组成部分，然而，它也面临着一系列的安全问题。这些问题可能导致系统运行中断、数据泄露、信息篡改等严重后果。以下是电网调度自动化系统存在的主要安全问题。

### 2.1 人员操作安全问题

在电网调度自动化系统的运行过程中，人员操作是关键环节之一，但也存在一些安全问题需要引起重视。以下是电网调度自动化系统人员操作存在的主要安全问题：（1）由于人为因素，操作员可能会错误地执行操作或误解操作指令，导致系统出现异常或故障。误操作可能包括错误的设备控制、错误的参数设置或误判系统状态等，可能对电网调度自动化系统的稳定性和安全性产生负面影响。（2）未经授权的人员可能试图访问电网调度自动化系统，执行未经授权的操作。这可能导致系统的敏感信息被窃取、篡改或操纵，从而对电网运行和数据安全造成风险。（3）操作员使用的密码可能存在泄露、弱密码设置或共享密码等问题。这可能使得恶意人员能够利用操作员的账户进行非法访问、数据篡改或未经授权的操作。（4）电网调度自动化系统的操作员可能存在内部威胁，如故意破坏、盗取敏感数据或滥用权限等，这可能对系统的稳定性和安全性造成严重影响。（5）管理人员可能错误地授权操作员执行不当操作或超出其权限范围的操作，这可能导致操作员误用系统功能或执行潜在危险的操作，

增加系统遭受攻击或故障的风险。（6）操作员缺乏对电网调度自动化系统安全重要性的充分认识和培训，可能导致他们忽视安全措施或不遵守安全操作规程，这可能使得系统容易受到攻击或发生人为错误。（7）操作员在执行工作时可能接触到敏感信息，如系统配置、操作记录或用户数据。不适当的信息管理或信息泄露可能导致系统安全受到威胁，同时也可能损害用户的隐私权。

### 2.2 物理安全问题

在电网调度自动化系统中，设备故障可能引发一系列安全问题，需要引起重视。以下是一些设备故障可能导致的安全问题：（1）设备故障可能导致电网调度自动化系统的停电或断电，从而造成对电网的监控和控制中断，可能导致电力供应不稳定或无法及时响应紧急情况。（2）设备故障可能导致电网调度自动化系统中的数据丢失或损坏，这可能导致数据不完整、不准确或无法恢复，影响系统的运行和决策能力。（3）设备故障可能导致电网调度自动化系统的响应时间延长，无法及时对电网状态做出反应，影响对电网的监测和控制能力。（4）设备故障可能导致系统中的安全漏洞被暴露，黑客可以利用这些漏洞进行攻击、入侵或破坏系统。（5）设备故障可能导致通信链路中断或数据传输错误，影响系统与其他设备或终端的正常通信，可能导致误操作或信息丢失。（6）设备故障可能导致防护措施失效或减弱，例如防火墙、入侵检测系统等，使得系统容易受到恶意攻击和未经授权的访问。

### 2.3 网络安全问题

电网调度自动化系统作为关键的基础设施之一，面临着多种网络安全问题。这些问题可能会给系统的安全性、稳定性和可靠性带来威胁。以下是一些常见的电网调度自动化系统存在的网络安全问题：（1）缺乏有效的认证和访问控制机制可能导致未经授权的用户访问系统。恶意用户或黑客可能利用弱密码、共享账户或其他手段绕过认证机制，进入系统并执行未经授权的操作。（2）电网调度自动化系统可能受到恶意软件和病毒的攻击。这些恶意软件可以通过网络传播，并对系统造成破坏、数据丢失或不可用。例如，勒索软件、木马病毒和蠕虫病毒等可能会导致系统崩溃或关键数据泄露。（3）系统中存在未修补或未发现的网络漏洞和弱点可能被黑客或攻击者利用。这些漏洞可能来自操作系统、网络设备、应用程序等方面，攻击者可以利用漏洞入侵系统、执行恶意代码或获取敏感信息。（4）未加密的数据传输和存储可能导致信息泄露的风险。黑客可以截取数据包、窃取敏感信息或篡改数据，从而影响系统的运行和准确性。数据的完整性和保密性对于电网调度自动化系统至关重要[2]。

### 2.4 数据完整性安全问题

电网调度自动化系统的数据完整性安全问题是指在系统运行过程中可能遇到的数据完整性方面的安全隐患。以下是一些常见的数据完整性安全问题：（1）数据损坏是指数据在存储或传输过程中发生错误或被破坏的情况。这可能是由于硬件故障、软件错误、人为操作失误或恶意攻击等原因导致的。数据损坏可能导致数据的完整性丧失，进而影响电网调度和运行的准确性和可靠性。（2）数据丢失是指数据在存储或传输过程中无法恢复或丢失的情况。这可能是由于系统故障、意外删除、未经授权的访问或恶意攻击等原因导致的。数据丢失会导致关键信息的缺失，影响对电网运行状态的准确监测和调度决策的制定。（3）数据篡改是指未经授权的个人或恶意攻击者对数据进行恶意修改或篡改的行为。数据篡改可能导致系统中存储的数据与实际情况不符，进而对电网调度和运行产生误导和风险。（4）数据冲突是指当多个数据源同时提交数据时，由于数据内容、格式或时间戳等方面的不一致性，可能导致数据冲突的情况。数据冲突可能使系统操作人员难以确定正确的数据，并对电网调度和运行的决策产生混淆和困扰。（5）数据漏洞是指系统中存在潜在的漏洞或弱点，使得未经授权的个人可以利用这些漏洞来获取、篡改或破坏数据的完整性。数据漏洞可能源于系统设计缺陷、安全措施不足或人为失误等因素。

## 3 电网调度自动化系统的安全控制建议

### 3.1 人员操作安全问题控制措施

针对电网调度自动化系统人员操作存在的安全问题，以下是一些详细的控制措施，以确保系统的安全性和可靠性：（1）为操作员提供全面的培训，使其熟悉系统的操作和安全要求，并加强他们对安全意识的培养。定期组织安全意识培训和演练，以提高操作员对安全风险的识别和应对能力。（2）实施严格的访问控制机制，确保只有经过授权的人员能够访问系统，并根据工作职责划分权限级别。限制操作员的权限，使其只能执行其职责所需的操作，防止误操作或滥用权限。（3）要求操作员使用强密码，并定期更新密码。禁止共享密码或将密码存储在不安全的地方。引入多因素认证，如指纹识别或硬件令牌，以增加身份验证的安全性。（4）建立完善的审计日志系统，记录操作员的操作活动，包括登录、操作记录、参数设置等。定期审查审计日志，及时发现异常操作或安全事件。

监控系统的运行状态，检测异常行为或未经授权的访问。（5）建立严格的内部安全控制机制，包括背景调查、权限审批和内部监察等。对操作员进行定期的安全背景调查，确保他们的可信度和诚信度。定期进行权限审批，防止不当操作或超越权限的行为。（6）对操作员工作场所进行物理安全控制，限制未经授权人员的进入。安装安全摄像头和入侵检测系统，监控操作员的活动，并及时发现和应对潜在的物理安全威胁[3-4]。

### 3.2 物理安全问题处理措施

针对电网调度自动化系统设备本身存在的安全问题，以下是一些对策措施：（1）建立设备监控系统，实时监测设备状态，包括温度、电压、电流等参数，及时发现异常情况并采取相应的维护和修复措施，确保设备的正常运行。（2）定期对系统数据进行备份，并确保备份数据的完整性和可靠性。同时，建立恢复机制，能够快速恢复系统数据和配置，以防止数据丢失或损坏对系统安全造成的影响。（3）确保设备安全防护措施的有效性，包括更新设备固件和软件补丁、设置强密码、限制设备访问权限、使用加密通信等，以减少设备受到恶意攻击的风险。（4）建立定期的设备维护计划，对设备进行定期检查、维护和校准，以确保设备的正常运行和可靠性。（5）为操作人员提供相关的培训和教育，提高他们对设备安全的认识和意识，确保正确操作设备，并能够及时处理设备故障和应对安全问题。（6）建立安全审计和日志监测机制，对设备的操作记录和事件日志进行监控和分析，及时发现异常行为和潜在安全威胁，并采取相应的应对措施。（7）定期评估和审查设备安全性，并根据最新的安全标准和技术发展进行设备的更新和升级，以保持设备的安全性和适应性。

### 3.3 网络安全控制措施

电网调度自动化系统在网络安全方面需要重视认证和访问控制、恶意软件和病毒攻击、网络漏洞和弱点、信息泄露和数据篡改以及社会工程攻击等问题。通过采取综合的网络安全措施，如强化认证机制、实施网络防火墙、定期更新和修补漏洞、加密数据传输和存储等，可以有效降低这些风险。（1）强化用户认证机制，使用复杂密码、多因素认证等方式提高系统的安全性。实施严格的访问控制策略，限制用户权限，确保只有授权人员可以访问系统。（2）定期更新和维护系统的防病毒软件，确保及时发现和清除恶意软件。提高用户的安全意识，教育用户不打开可疑的电子邮件附件或点击未知来源的链接。（3）定期进行漏洞扫描和安全评估，及时修补系统中发现的漏洞。加强网络设备和应用程序的安全配置，关闭不必要的服务和端口，限制对外访问。（4）使用加密技术保护数据传输和存储，确保敏感信息的机密性和完整性。实施访问控制策略，限制对数据的修改和删除权限，确保数据的可靠性和一致性。

### 3.4 数据完整性安全控制

针对电网调度自动化系统数据完整性安全问题，可以采取以下对策来降低风险和保障数据的完整性：（1）建立定期的数据备份机制，确保数据的定期备份，并设置可靠的数据恢复策略，以防止数据损坏或丢失的情况发生。备份数据应存储在安全可靠的地方，并进行定期测试以确保可恢复性。（2）建立严格的访问控制机制，限制对系统数据的访问权限，并分配不同级别的权限给不同的用户。确保只有经过授权的人员才能访问、修改或删除数据，以减少数据被恶意篡改或误操作的风险。（3）采用数据完整性校验的技术手段，如数据校验和哈希算法等，对数据进行验证和校验，以确保数据在存储和传输过程中没有被篡改或损坏。定期进行数据完整性的检查和验证，及时发现和处理数据完整性问题。（4）安全培训与意识提升：开展定期的安全培训活动，提升系统操作人员的安全意识和技能，加强对数据完整性的重视和保护意识。教育人员不在未经授权的环境下使用个人设备，避免不当操作导致数据完整性问题。（5）建立安全审计和监测机制，对电网调度自动化系统中的数据操作和访问进行监测和审计。及时发现异常行为和潜在威胁，并采取相应的应对措施，保障数据的完整性和安全性[5]。

## 4 结语

总之，在电网调度自动化系统运行的环节，难免有一些问题影响到系统稳定。所以，需要结合实际选择科学的控制方法，保证系统的运行效果。

## 参考文献：

[1] 王甜.电网调度自动化系统的安全策略[J].集成电路应用,2020,37(11):136-137.
[2] 李昱潼.电力调度自动化二次系统安全防护技术[J].自动化应用,2019(08):56-57,84.
[3] 张明.电网调度自动化系统的应用对策[J].企业改革与管理,2017(23):204.
[4] 刘军.调度自动化系统及数据网络的安全防护[J].中国战略新兴产业,2017(32):75.
[5] 黄国庆,陈雪阳.基于电网调度自动化系统的可靠性应用研究[J].建材与装饰,2017(52):236-237.