

电力系统及其自动化技术的安全控制问题及对策分析

陶诗琪

广西兴能电力建设有限公司 广西 玉林 537000

摘 要: 电力系统自动化智能化水平持续提升, 系统运行结构与数据交互模式更为复杂, 各类安全控制隐患逐步凸显。结合电力自动化体系的架构特征与运行逻辑, 本文从硬件设备、软件系统、数据传输及运维管理四个维度梳理现存安全问题, 逐层剖析隐患形成的核心成因, 针对性提出设备升级、技术优化、数据防护及运维完善的改良策略。整套内容可有效化解自动化系统运行短板, 提升电力系统安全控制质量与运行稳定性。

关键词: 电力系统; 自动化技术; 安全控制; 系统运维; 数据防护

引言: 新型电力系统建设持续推进, 自动化技术深度融入电网运行、调控、运维全流程, 大幅提升电力系统运行效率与智能化水平。系统架构升级与运行场景复杂化同步带来更多安全管控难题, 设备老化、技术架构缺陷、数据防护薄弱、运维体系疏漏等问题不断凸显。完善自动化安全控制体系, 排查并治理各类运行隐患, 能够有效强化电网抗风险能力, 保障电力系统持续平稳、安全、高效运转。

1 电力系统自动化安全控制体系架构

1.1 电力系统自动化运行结构组成

现代电力系统自动化由多个独立功能模块协同构成, 核心包含电力传输、智能调控、数据采集、自动运维四大板块, 分别对应电网能量输送、运行状态监管、运行数据归集、设备运维保障核心工作。从系统层级来看, 整套架构分为设备层、数据层与控制层。设备层为物理载体, 依托输配电设备与传感装置实现电力输送、原始数据采集。数据层负责归集、分类、规整各类运行数据, 形成标准化数据资源。控制层依托合规数据生成调控指令, 完成电网运行状态调节。各层级逐级衔接、相互配合, 形成完整闭环运行架构, 为自动化安全控制问题分析提供稳定的架构支撑^[1]。

1.2 自动化技术安全控制运行逻辑

电力系统自动化安全控制具备标准化的闭环运行逻辑, 整体流程分为系统监测、状态研判、智能调控、闭环防护四个核心环节。系统通过前端监测装置持续采集电网设备工况、电力传输参数及环境信息, 获取全面的运行数据。后台程序结合内置运算规则分析数据, 甄别电网运行异常状态与潜在风险。针对偏离标准的运行工况, 系统自动输出适配调控指令, 修正电网运行状态, 保障电力输送与设备运行稳定。防护机制同步约束异常工况, 遏制风险扩散。这套运行逻辑主要作用于电网稳

态维持、设备状态管理、运行风险防控, 明确的运行边界可适配多场景电网安全管控需求。

1.3 自动化安全控制的影响要素

电力系统自动化安全运行受内部、外部两类核心要素制约, 各类因素均可干扰安全控制工作的有效性。内部要素集中在设备与程序层面, 设备长期运行产生的老化、性能衰减会改变运行参数, 造成数据采集、指令执行出现偏差。系统程序存在的逻辑缺陷、运算漏洞, 会降低工况研判与智能调控的准确性。外部要素涵盖数据传输与环境人为干扰, 数据传输中的信号波动、链路异常会引发数据失真、信息缺失。环境变化、人工操作干预等不确定因素, 会扰乱系统正常运行节奏。各类要素可通过设备、数据、控制链路传导隐患, 直接影响自动化控制系统的运行可靠性, 引发电网安全运行问题。

2 电力系统自动化安全控制现存隐患

2.1 硬件设备层面的安全隐患

电力系统自动化各类硬件设备长期持续投入电网运行, 会逐步滋生各类安全隐患。隐患覆盖终端采集设备、智能调控装置、信号传输硬件及储能配套设备等全品类硬件设施。设备长期运转会出现部件老化、性能衰减等常规问题, 老旧硬件的运行参数难以匹配现代化电网的控制精度要求。部分场站硬件设备更新进度滞后, 硬件参数与新型自动化控制程序存在适配性不足的问题。不同批次、不同型号的硬件组件共同组网运行, 容易出现组件协同衔接偏差^[2]。硬件层面存在的各类缺陷会干扰数据采集、信号传输、指令执行等核心流程, 破坏自动化控制流程的完整性, 造成电网运行工况波动, 诱发系统运行不稳定问题。

2.2 软件系统层面的安全隐患

电力自动化软件体系包含调控软件、数据处理系统、智能控制程序多个核心模块, 各模块运行过程中普

遍存在不同程度的运行缺陷。软件长期运行会积累程序漏洞、代码冗余等问题,弱化系统运算与研判能力。部分电网沿用传统软件体系,系统架构与新型运行技术存在兼容性不足的问题。软件迭代更新进度滞后于电网升级速度,老旧程序无法适配全新的电网运行工况与控制需求。软件运行逻辑存在的设计缺陷、运算偏差,会干扰电力调度方案编制、设备状态监测、安全自动防护等核心工作。各类软件问题会持续累积,形成隐性运行风险,制约自动化系统安全稳定运行。

2.3 数据传输层面的安全隐患

数据交互链路是电力自动化系统运行的核心载体,链路运行状态直接决定自动化控制的精准程度。电网运行场景复杂多变,数据传输链路容易受到外界环境与系统内部因素影响,出现多种异常问题。信道拥堵、链路故障、信号干扰等问题,会引发数据传输延迟、信息丢失等情况。数据传输协议不规范、交互口径不统一,会造成多源数据融合紊乱、数据内容失真等现象。异常数据流入系统运算流程,会误导工况研判与指令输出。数据传输故障会打乱自动化控制的整体节奏,降低电网调控精准度,给电力系统稳定运行带来负面干扰。

2.4 系统运维层面的安全隐患

日常运维工作是保障电力自动化系统稳定运行的关键,现阶段运维工作仍存在多处短板与漏洞。部分运维工作缺乏标准化流程约束,操作流程存在不规范、不严谨的问题。系统监测体系覆盖范围有限,无法全面捕捉设备、软件、数据链路的细微异常状态。隐患排查工作流于表面,细微故障与隐性风险难以得到彻底清理。系统检修、升级、维护工作存在滞后性,故障问题长期留存会持续扩大影响范围。传统运维模式适配性较弱,无法匹配高自动化、高精度电网的运行管控需求,逐步形成常态化安全控制短板,制约电力系统自动化安全管控质量提升。

3 电力系统自动化安全控制问题成因剖析

3.1 设备配套体系适配性不足

电力系统自动化技术持续迭代升级,电网智能化运行标准持续提高,传统硬件配套体系逐渐显露适配短板。多数传统场站的硬件更新节奏较为缓慢,设备服役周期偏长,整体性能参数难以对接新型自动化控制技术的运行标准。行业硬件配置标准更新速度滞后于电网智能化升级进度,老旧设备的技术参数、性能指标无法满足高精度调控的运行要求。电网改造升级过程中,新旧设备混合组网的情况较为普遍,不同生产标准、不同技术版本的硬件设备存在兼容壁垒^[3]。设备体系整体适配能

力的不足,会持续影响数据采集精度与指令执行效果,逐步衍生出设备运行不稳定、系统调控偏差等各类安全控制问题。

3.2 智能系统技术架构存在短板

现有电力自动化智能系统架构依托传统电网运行需求搭建,面对电网规模化扩容、运行工况复杂化的发展变化,逐步暴露多项固有技术局限。早期系统架构设计思路相对保守,整体拓展性与延展性不足,难以承载大容量、多维度的电网运行数据运算处理。程序开发逻辑偏向常规稳态工况调控,针对复杂波动工况的处理能力存在明显欠缺。智能调控算法的优化深度不足,对极端工况、隐性风险的研判能力较弱。技术架构层面的各类短板,让自动化系统无法全面适配现代电网的复杂运行场景,持续催生各类隐性安全运行隐患。

3.3 数据安全防护体系不完善

电力自动化系统的数据交互规模持续扩大,现有数据安全防护体系存在明显的结构性漏洞。数据加密机制设置较为简单,加密等级无法适配多源异构数据的传输存储需求。数据校验机制不够完善,针对异常数据、篡改数据的甄别能力有限,错误数据可直接参与系统运算。常态化数据备份机制落实不到位,数据存储容错率偏低,故障场景下容易出现数据丢失问题。链路防护手段较为单一,动态化、全方位的防护体系处于缺失状态,应对复杂网络干扰、外界侵入的防护能力薄弱。防护体系的不完善是各类数据安全问题的深层诱因,直接削弱自动化控制的运行稳定性。

3.4 安全运维管理体系不健全

电力自动化系统安全控制出现的各类隐患,根源在于运维管理体系存在结构性缺陷。部分场站尚未搭建适配智能化电网的专属运维机制,整体管控规则较为松散。运维作业缺少统一规范的流程标准,作业执行随意度偏高,容易出现操作疏漏、隐患遗漏等问题。常态化的日常巡查、状态监测、风险管控机制不够完善,长效管控力度不足。传统运维管理模式侧重故障事后维修,前置预判与主动防控能力薄弱,和现代化自动化电网的运行管控需求存在明显差距。管理层面的各类漏洞,会持续放大设备、软件、数据层面的细小缺陷,转化为系统性安全控制隐患。

4 电力系统自动化安全控制优化对策

4.1 优化硬件设备配套升级体系

硬件设备是电力自动化系统运行的物理基础,设备老化、适配性差、组件衔接不畅等问题,是诱发系统安全隐患的重要因素。结合电网智能化升级的整体趋势,

搭建常态化的设备升级与运维优化体系,从源头改善硬件运行短板。结合现代电网精细化运行管控要求,修订完善硬件设备适配标准,统一各类自动化终端采集设备、智能调控设备、信号传输及储能配套设备的技术规范。制定分层分批的更新改造方案,有序推进老旧落后设备迭代更替,淘汰性能衰减、参数不达标的硬件设施。持续优化整套硬件配套架构,理顺不同类型设备的组网逻辑,弱化新旧设备、不同型号设备的运行壁垒。搭建全覆盖的设备状态监测机制,对设备运行工况、性能损耗、组件运行状态开展长期跟踪记录^[4]。依托监测数据掌握设备运行变化规律,提前排查潜在故障风险,持续提升硬件设备运行稳定性与场景适配能力,夯实自动化系统安全运行的硬件基础。

4.2 完善智能化系统技术架构

老旧固化的技术架构与程序逻辑缺陷,会大幅降低电力自动化系统的调控精度与运行可靠性。针对现有智能系统暴露的技术短板,全方位优化软件体系与整体技术架构。梳理智能调控程序的底层运行逻辑,修正不合理的程序设计思路,全面排查并修补系统运行过程中存在的代码漏洞与逻辑缺陷,清理冗余程序内容。建立常态化的系统迭代升级机制,结合电网规模化、复杂化的运行变化,持续更新系统运算规则与调控算法。不断拓展系统运行承载力与兼容能力,解决新旧技术体系衔接不畅、工况适配不足等问题。持续提升自动化控制系统的运算精度、运行稳定性与智能化水平,让系统可以高效应对复杂电网工况与各类极端运行场景。依托技术架构的全面优化,补齐系统运行短板,从技术层面杜绝各类隐性安全隐患,保障电网智能调控工作有序推进。

4.3 构建全方位数据安全防护体系

数据是电力自动化智能调控的核心依据,数据链路的各类安全问题会直接干扰电网正常运行。围绕数据采集、传输、交互、应用全流程,搭建全链路、多层次的数据安全防护机制。升级传统数据防护模式,优化分级数据加密技术,针对不同类型的电力运行数据设置差异化加密标准,筑牢数据传输与存储的安全屏障。完善数据传输校验与异常筛查流程,精准甄别失真、错误、异常数据,阻断问题数据进入系统运算环节。优化常态化数据备份机制,搭建多渠道、多终端的数据存储架构,

降低数据丢失、损毁的风险。构建动态化数据防护模式,强化数据交互全流程管控,精准应对外界干扰、网络入侵等各类安全威胁,有效规避数据延迟、失真、泄露等问题,持续保障自动化控制数据的精准性与安全性。

4.4 健全常态化安全运维管控机制

科学完善的运维管理模式,是保障电力自动化系统长期稳定运行的关键手段。针对现阶段运维流程不规范、隐患排查不彻底、管控覆盖不全等短板,全面优化传统运维管理模式。制定标准化、规范化的运维作业流程,细化设备巡检、软件核查、链路检测、隐患整治等各环节工作细则,统一运维作业执行标准。拓宽系统运行监测范围,实现硬件设备、软件程序、数据传输链路的全方位动态监管,及时捕捉细微异常与隐性故障。建立长效化隐患排查与系统维护机制,对排查发现的安全问题分类梳理、限时整改,彻底清除系统运行漏洞。转变被动维修的运维模式,强化前置预判与主动防控,结合系统运行状态提前开展设备维护与系统优化。全方位补齐运维管理短板,提升运维工作的规范性与全面性,为电力自动化系统安全稳定运行提供长效管理保障。

结束语

电力系统自动化安全控制隐患源自设备、技术、数据、管理多个层面,各类短板相互交织,共同影响电网整体运行质量。通过升级硬件配套体系、优化智能系统架构、搭建全维度数据防护机制、健全常态化运维管控模式,可系统性补齐安全控制漏洞。多维度优化方案能够适配现代电网自动化运行需求,强化电力系统安全防护能力,为电网稳定有序运行提供坚实保障。

参考文献

- [1]吴家蔚,杨光,高康康. 电力系统及其自动化技术的安全控制问题及对策分析[J]. 电工材料,2025(4):84-86,91.
- [2]冯怡文. 电力系统及其自动化技术的安全控制问题及对策分析[J]. 中国科技纵横,2024(9):5-7.
- [3]鲁翼齐,孟德港. 电力系统及其自动化技术的安全控制问题及对策[J]. 消费电子,2025(20):203-205.
- [4]王仲海. 电力系统及其自动化技术的安全控制问题及对策[J]. 电力设备管理,2024(14):247-249.