

电气二次回路数字化改造中的信息可靠性保障措施研究

高 驰

江苏华电吴江热电有限公司 江苏 苏州 215221

【摘要】：电气二次回路数字化改造对电力系统的监控、保护与控制能力提出更高要求，信息可靠性成为影响系统运行质量的关键因素。研究围绕数字化背景下二次回路的信息传输特性、故障风险及系统脆弱环节展开，梳理数据链路、通信协议、终端设备等关键节点的可靠性影响机制，分析可能导致信息异常的技术与管理因素。依据电气二次系统结构特点，构建由数据采集层、通信层、应用层与安全管理层组成的多层次信息可靠性保障体系，并提出完善编码与校验机制、增强网络冗余配置、优化设备自诊断功能、提升网络安全防护能力等措施。研究旨在为电气二次系统数字化改造提供可实施的技术路径，提升整体系统的稳定性与可靠运行水平。

【关键词】：电气二次回路；数字化改造；信息可靠性；通信冗余；系统安全

DOI:10.12417/2811-0528.26.04.010

电气二次回路在电力系统中承担信息采集、控制执行与安全保护等核心功能，系统运行的精确性与稳定性高度依赖信息传输的可靠性。随着智能化和数字化技术的快速发展，传统二次回路在数据处理能力、通信性能以及抗干扰能力方面已难以满足现代电网的需求。数字化改造成为提高系统效率与运行安全的重要途径，同时也带来设备多样化、网络结构复杂化和信息风险增大的新挑战。如何在数字化环境下构建可靠的信息传输与处理机制，成为保障电力系统安全运行的关键研究问题。本研究围绕信息可靠性保障展开分析，旨在提出适用于数字化二次系统的技术措施和体系框架，为工程实践提供理论支持与方法参考。

1 数字化条件下电气二次系统运行格局的变动趋势

数字化技术的深度融入，使电气二次系统的运行方式呈现出结构重构与功能延伸的双重变化。传统以继电保护、测量、控制装置为核心的独立式架构，正逐步演化为以数据为中心、以网络通信为支撑的协同式系统。信息在系统内部的流动路径更加丰富，数据采集的颗粒度提升，实时性和连续性显著增强，使二次系统具备更强的运行状态感知能力。装置之间由点到点的逻辑连接转向由平台式的信息交换机制承载，系统的运行行为不再依赖单一设备，而是依靠整体化的数据链路实现保护、监测与控制功能的联动。

伴随数字化进程推进，电气二次系统的构成由原本的物理装置集合转变为软硬件融合的多层结构。过程层、间隔层、站控层之间的数据交互更加频繁，IEC 61850 等标准化模型推广后，系统在结构上的兼容性与扩展性得到提升，功能模块化程度不断提高^[1]。保护与控制单元能够通过标准化通信接口接入系统，实现设置值下发、状态监测与逻辑功能更新的远程管理。以往需要人工介入的信号校核与回路验证工作逐渐实现自动

化，推动二次系统运行模式向智能协同方向转变。

数字化条件下的运行格局还表现出对实时数据的依赖程度不断加深。系统运行状态由周期性监测向连续动态监测转型，事件记录、故障波形、运行参数等信息能够在短时间内完成收集与传输。快速数据链路的建成使保护动作判据由单点测量扩展到多源信息融合，动态计算能力增强，赋予系统更高的判别精度。各类智能终端在设备层形成数据节点，通过网络将信息汇聚至控制中心，为运行分析提供丰富的数据来源。在调度与运行管理层面，数字化推动二次系统具备更高的可视化能力与自适应能力。运行人员可以通过平台化界面查看设备状态、通信质量、逻辑链路结构与运行趋势，实现对于二次系统运行健康度的全周期评估。系统在面对负荷波动、设备老化或新能源接入等情景时具备更强的调整能力，为构建主动防御、协同控制的运行模式奠定基础。

2 信息处理链路中的薄弱环节与系统脆弱性表现

信息处理链路在数字化电气二次系统中承担数据传输、解析、存储与交互等关键功能，其完整性与稳定性直接影响保护、监控与控制功能的有效性。链路结构由多类设备、通信协议与软件模块构成，各环节间的耦合度不断提高，在运行环境复杂、电磁干扰强、设备性能参差不齐的条件下，更容易暴露脆弱点。链路中任一环节的异常都可能导致信息延迟、畸变或丢失，使系统在关键时刻无法准确识别运行状态，形成潜在的控制风险。在物理层中，通信介质老化、屏蔽不良及接地系统不完善，会使数据传输通道承受更高的干扰水平。光纤接续损耗、端面污染与网络设备端口老化会造成链路衰减升高，影响数据完整性。部分站内网络结构在改造中采用新旧设备混用方式，使链路质量不易统一保障，形成隐性风险点。物理层的不确定性使数据包在传输过程中可能出现误码率上升、抖动增大等问题，

从而影响上层通信协议的稳定运行。

在数据链路层和传输层中，协议帧解析错误、报文拥塞与网络拓扑的不合理设置，会导致延时不可控与实时性下降。部分设备仍采用相对封闭的通信栈结构，协议兼容性不足，造成不同厂家的装置在数据交互中存在潜在冲突^[2]。交换机规则配置不当、VLAN 划分不合理或端口负载不均，也会导致报文冲突与队列阻塞。当高频采样数据集中涌入系统时，链路缺乏有效的流控措施会使关键保护报文的优先级无法保证，从而出现保护误动或拒动风险。

在应用层，逻辑处理模块的可靠性成为新的脆弱环节。保护装置的软件算法、状态机逻辑与数据滤波策略存在差异，当处理大量实时数据时，可能出现运算过载、数据缓存溢出或逻辑判断延迟。一些智能终端的自诊断机制不完善，无法及时发现内部故障，使系统运行状态监测出现盲区。数据服务器和应用平台在高并发场景下，也可能因资源调度不合理导致响应性能下降，影响整体系统的协调性。信息链路在安全防护方面的脆弱性同样值得关注。数字化系统高度依赖网络通信，当认证机制薄弱或访问控制策略不完善时，链路易受到恶意报文、非法访问或错误配置带来的影响。网络攻击并不一定表现为损坏设备，也可能通过制造延时或流量干扰影响保护与控制功能的正常执行，而这类隐性安全风险往往不易被及时识别。

3 面向多层次结构的信息可靠性提升路径构建

面向数字化电气二次系统构建多层次的信息可靠性提升路径，需要在系统架构、通信机制、设备功能以及管理流程等多方面形成协同作用，使各层级在信息传输与处理过程中具备足够的冗余度、稳定性与自适应能力。多层次结构的理念强调过程层、间隔层和站控层在功能上既相互独立又紧密协作，通过分层解耦的方式提升系统的韧性，使信息在跨层流动时具备可校验性、可控性与可恢复性，从而构建更加可靠的信息链路。

在过程层，信息可靠性提升路径的核心是提高数据采集与采样传输的确定性。高精度采样装置需具备稳定的时钟同步能力，使测量数据保持严格的时间一致性。智能采集单元应具备本地缓存与异常隔离功能，当现场干扰导致瞬时数据质量下降时能够主动标识与过滤，避免错误数据进入上层系统。过程层通信网络应采用确定性交换机制和高可靠链路结构，通过冗余拓扑、链路自愈与毫秒级切换技术保证实时数据持续可用，使保护与控制功能不受瞬时链路波动影响。间隔层在多层次体系中承担数据汇聚、逻辑处理与控制执行的重要角色，信息可靠性提升路径需关注逻辑处理的稳定性与交互机制的规范化^[3]。保护与控制单元应采用可扩展的软件逻辑框架，使算法更新与参数调整在不中断系统运行的条件下完成。数据交互应基于标准化对象模型，实现不同厂商设备间的互操作性，避免因解析

差异导致的数据丢失或延时。间隔层设备还需具备完善的自诊断与运行健康度评估能力，当通信异常、硬件故障或逻辑偏差发生时能够及时报警并采取隔离措施，以防止异常向上层传播。

站控层在整体可靠性路径构建中发挥协调与管理作用，重点在于平台化系统的调度能力、数据管理能力与安全控制能力。站控系统应建立多源数据融合模型，通过趋势分析与异常识别提高对链路状态和设备运行状况的感知深度。数据服务器需配置高可靠存储结构和资源动态调度机制，使长时间运行下的数据处理能力保持稳定。站控通信平台应设置严格的访问控制与分级权限策略，通过加密认证、指令校核和安全日志记录等手段提升整体链路的安全性，确保控制指令与运行数据的完整性与可追溯性。

4 技术措施应用后的系统性能验证与工程成效

技术措施的实施使电气二次系统在运行性能上呈现出结构性改善，信息链路的稳定性与数据处理的可靠性得到了有效验证。通过对多层级架构实施冗余设计、链路优化和逻辑增强等技术措施，系统在不同运行场景下表现出更强的抗干扰能力和自适应能力。实时数据传输的连续性显著提升，关键报文在高负荷状态下仍能保持稳定的延时水平，确保保护和控制功能在复杂电网条件下能够保持准确响应。技术措施的应用还促进了事件记录与状态监测信息的精确度，使运行人员对系统动态的掌握更加全面。

在过程层，采用高精度时钟同步和确定性通信机制后，故障录波数据的对时偏差明显缩小，数据完整度提高，保护动作依据更加可靠。链路冗余切换技术的应用使瞬时网络抖动对系统影响大幅降低，保护装置在链路异常期间依然能够基于本地数据保持功能连续，减少误动和拒动概率^[4]。实际运行记录显示，在多扰动并发的场景下，过程层数据的稳定性较改造前有明显提升，为上层逻辑处理提供了高质量输入。间隔层的功能优化进一步增强了逻辑执行的准确性与控制行为的可预期性。标准化对象模型实现了跨设备的数据一致性，逻辑处理模块的稳定性提高，使控制指令执行更加迅速和可信。自诊断机制的介入使设备能够提前识别潜在异常，通过本地隔离和告警策略避免故障扩大化。数据交互在高频操作期间仍能保持顺畅，交换机流量管理与优先级策略保证了关键报文的通道资源，使系统在动态负载波动中维持良好的操作性能。

站控层在技术措施作用下呈现出更高的系统协调能力。数据平台的融合处理使运行趋势分析和设备健康度评估更加精准，异常识别速度大幅提升。安全控制策略的实施提高了指令发布的可靠性，重要控制流程的校核与验证机制减少了人为错误与链路异常带来的风险。整体系统在长期运行中表现出更低

的故障率与更高的稳定性，工程成效显示多层次措施能够为数字化电气二次系统构建稳固的信息加工通道，从而提升系统的整体运行质量。

5 数字化二次系统信息可靠性的未来发展方向

随着电网运行场景的多样化和动态性增强，信息链路需要具备更强的弹性与可预测性，使系统在高波动、高负荷甚至异常条件下仍能维持稳定的数据交互能力。未来的链路结构将更加注重确定性传输技术，通过精确调度通信资源，使关键报文在复杂网络环境中仍能获得可保障的带宽与固定的时延范围。同时，边缘计算与本地自治能力的提升，使过程层和间隔层具备更高的独立运行能力，即使在站控通信短暂中断的场景下，也能通过本地逻辑维持必要的保护与控制功能。

智能化技术的进一步渗透将深刻重塑信息可靠性的实现路径。人工智能辅助的异常检测技术能够对链路状态、数据分布与设备行为进行持续分析，通过多维度特征识别潜在隐患，并在早期阶段给出介入提示^[5]。自适应算法将参与逻辑策略优化，使保护门槛、数据过滤策略和资源调度模式能够根据运行环境自动调整，提高系统对不确定性的响应能力。同时，数字孪生技术将成为未来提高可靠性的重要手段，通过构建高精度虚拟模型，对链路特性、装置行为和系统负荷进行仿真，使参

数优化和控制策略能够在虚拟空间中充分验证后再投入实际运行。

在系统结构层面，未来的二次系统将呈现更深层的融合趋势。一次与二次信息的交互将更加紧密，实时模型与状态估计技术在站控层得到强化，通过更精准的设备状态感知提升逻辑判断的有效性。多站点、跨区域的信息联动将推动分布式二次系统形成协同网络，使保护范围扩大、控制策略更具整体性。以安全为中心的架构理念将贯穿系统生命周期，可信计算、访问控制体系和多级安全校核机制将构成新的安全保障框架，使信息在传输、存储和处理过程中的真实性与完整性得到进一步加强。

6 结语

数字化背景下的电气二次系统正在经历深度变革，信息可靠性已成为支撑保护、控制与监测功能稳定运行的核心要素。多层次结构的构建、链路薄弱环节的识别、技术措施的应用与成效验证，为提升整体系统性能奠定了坚实基础。随着智能化、融合化与安全化技术不断发展，信息处理链路将具备更高的稳定性与自主运行能力。未来的二次系统将在更复杂的电网环境中展现更强的韧性与适应力，实现运行效率与安全水平的持续提升。

参考文献：

- [1] 于冰,崔大林,李巧荣,等.一种应用数字孪生技术对二次回路建模的方法研究[J].环境技术,2025,43(07):72-76.
- [2] 顾乃胜,亓润.电气二次回路故障诊断技术研究[J].机械工业标准化与质量,2025,(01):38-40+48.
- [3] 杨灿丽.继电保护电气二次回路隐患排查分析[J].中国设备工程,2024,(23):145-147.
- [4] 胡骁.电力系统中电气二次回路常见故障及防范分析[J].办公自动化,2024,29(17):84-86.
- [5] 章琦,王宝山,康金,等.继电保护电气二次回路隐患排查分析[J].电站系统工程,2023,39(04):80-81+84.