电气自动化控制系统的实时性与可靠性研究

桑 迪
沈阳地铁集团有限公司运营分公司 辽宁 沈阳 110000

摘 要：本文系统探讨了电气自动化控制系统中实时性与可靠性的内涵、影响因素、评估方法及优化策略。首先，从理论层面界定实时性与可靠性的定义，并分析二者之间的辩证关系；其次，深入剖析影响系统实时性与可靠性的硬件、软件、网络通信及环境因素；随后，介绍常用的性能评估指标与建模方法；在此基础上，提出提升系统实时性与可靠性的关键技术路径，包括冗余设计、容错机制、实时调度算法、确定性网络技术及智能诊断方法。

关键词：电气自动化；控制系统；实时性；可靠性；冗余设计；确定性网络；容错控制

引言

电气自动化控制系统融合计算机、自动控制、电力电子与通信技术，实现对电气设备及生产过程的自动监测、控制与管理，广泛应用于发电厂、轨道交通等场景，是现代工业基础设施的关键部分。在这些场景中，系统需在严格时间约束下完成关键任务，对实时性要求高；同时，长时间运行中要保持稳定，具备高可靠性。但实时性与可靠性并非总正相关，过度追求实时响应会削弱容错能力，提升可靠性又可能增加处理延迟。因此，如何实现二者动态平衡与协同优化，是电气自动化领域亟待解决的关键问题。本文将系统梳理相关理论基础等，为工业控制系统设计提供支撑与指导。

1 实时性与可靠性的内涵及其关系

1.1 实时性的定义与分类

实时性是指系统在规定的时间限制内完成指定任务的能力。根据时间约束的严格程度，实时系统可分为：①硬实时系统（HardReal-time）：任务必须在截止时间前完成，否则将导致灾难性后果（如核电站安全控制系统）。②软实时系统（SoftReal-time）：任务延迟虽不致命，但会影响系统性能或用户体验（如视频监控系统）[1]。③Firm实时系统：任务在截止时间后完成即失去价值，但不会造成系统崩溃（如某些数据采集任务）。在电气自动化中，保护控制、紧急制动等属于硬实时范畴，而状态监测、能耗统计等则多为软实时。

1.2 可靠性的定义与度量

可靠性是指系统在规定条件下和规定时间内无故障地完成规定功能的能力。常用度量指标包括：①可靠度（Reliability，R(t)）：系统在时间t内无故障运行的概率。②平均无故障时间（MTBF，MeanTimeBetween Failures）：系统两次故障之间的平均时间。③可用性（Availability）：系统处于可工作状态的时间比例，通常表示为$A=\frac{MTBF}{MTBF+MTTR}$，其中MTTR为平均修复时间。高可靠性系统通常具备故障检测、隔离与恢复（FDIR）能力。

1.3 实时性与可靠性的辩证关系

实时性与可靠性存在复杂的耦合关系：①正向协同：良好的实时调度可减少任务堆积，降低系统过载风险，从而提升可靠性；高可靠性硬件可减少故障中断，保障实时任务连续执行。②负向冲突：为提升可靠性而引入的冗余计算或通信校验会增加处理延迟，影响实时性；为满足硬实时要求而采用的高优先级抢占机制可能干扰低优先级监控任务，降低系统整体容错能力。因此，系统设计需在架构层面统筹考虑，实现“实时可靠一体化”设计。

2 影响实时性与可靠性的关键因素

2.1 硬件因素

硬件是系统性能的物理基础，其选型与质量直接决定了实时性与可靠性的上限。控制器的中央处理器主频、内存带宽以及专用协处理器（如FPGA）的配置，共同决定了任务处理的速度与并发能力。传感器与执行器的动态响应特性同样关键，例如电流互感器在短路暂态过程中的饱和特性会直接影响保护算法的判断速度与准确性，而伺服电机的机电时间常数则决定了其跟踪控制指令的快慢[2]。此外，电源系统的稳定性不容忽视，工业现场常见的电压暂降或瞬时断电可能导致控制器复位，造成控制中断甚至数据丢失。更为隐蔽但同样重要的是电磁兼容性（EMC）问题，在强电磁干扰环境下，如变频器附近或高压开关场，控制信号可能被噪声淹没，引发误动作或通信错误，严重威胁系统安全。

2.2 软件因素

软件是系统功能的载体，其架构与实现方式对性能

影响深远。操作系统的类型是首要考量，通用操作系统如Windows或标准Linux内核缺乏确定性的任务调度机制，难以满足硬实时要求；而实时操作系统（RTOS）如VxWorks、FreeRTOS或经过PREEMPT_RT补丁改造的RT-Linux，则能提供微秒级的中断响应和任务切换能力，是工业控制领域的首选。在此基础上，任务调度算法的选择至关重要，固定优先级调度（如Rate-Monotonic）因其简单可预测而被广泛应用，而最早截止时间优先（EDF）算法则在理论上具有更高的处理器利用率。此外，软件的整体架构设计也影响深远，采用模块化、低耦合的设计原则，不仅便于开发与维护，更能在局部模块发生故障时有效隔离影响范围，防止故障蔓延，从而提升系统整体的可靠性。

2.3 网络通信因素

随着控制系统向分布式、网络化方向发展，工业通信网络已成为影响实时性与可靠性的核心环节。现代系统普遍依赖工业以太网（如PROFINET、EtherCAT）进行高速数据交互，但网络性能的不确定性成为主要挑战。通信延迟由传输延迟、排队延迟和处理延迟共同构成，其总和必须小于控制任务的允许延迟。更关键的是延迟的抖动（Jitter），即延迟的波动性，它会破坏多节点间的同步精度，对运动控制等应用尤为致命。同时，网络的丢包率与误码率直接关系到数据的完整性，一个错误的控制指令可能导致灾难性后果。网络拓扑结构的选择也至关重要，星型拓扑结构简单但存在单点故障风险，而环网或双总线拓扑则能提供路径冗余，在链路故障时实现快速切换，显著提升系统可用性。

2.4 环境与人为因素

除了技术层面的因素，外部环境与人为操作同样不可忽视。工业现场的高温、高湿、粉尘或腐蚀性气体会加速电子元器件的老化，缩短设备寿命，增加故障概率。剧烈的机械振动也可能导致接插件松动或焊点疲劳，引发间歇性故障。此外，操作人员的技术水平与维护规程的执行情况也是影响系统可靠性的重要变量。不当的操作指令、错误的参数配置或缺乏定期的预防性维护，都可能成为系统失效的诱因。因此，一个高可靠、高实时的系统，不仅需要先进的技术，还需要完善的运维管理体系作为支撑。

3 实时性与可靠性的评估方法

3.1 实时性评估指标

对实时性的评估，核心在于量化任务的时间行为。任务响应时间是最直观的指标，它衡量从外部事件触发到系统完成相应处理的全过程耗时。对于硬实时系统，最坏情况执行时间（WCET）是关键参数，它代表了任务在所有可能输入和系统状态下所需的最大执行时间，是进行可调度性分析的基础。在分布式系统中，端到端延迟更为重要，它涵盖了从传感器采样、网络传输、控制器计算到执行器动作的完整闭环延迟。为了在设计阶段验证系统能否满足所有时间约束，工程师常采用调度可行性分析方法，如经典的Liu&Layland界限，通过比较任务集的总利用率与理论上限，来判断其是否可被调度。

3.2 可靠性评估方法

可靠性评估旨在预测和量化系统在生命周期内的失效行为。故障树分析（FTA）是一种自上而下的逻辑演绎方法，通过构建“顶事件”（系统失效）与“底事件”（元器件失效）之间的逻辑门关系，识别导致系统失效的关键路径。可靠性框图（RBD）则采用自下而上的方式，将系统分解为串、并联的功能模块，利用概率论计算整体可靠度。对于具有复杂状态转移特性的系统，马尔可夫模型能更精确地描述其从正常到故障再到修复的动态过程。当系统过于复杂难以解析建模时，蒙特卡洛仿真通过大量随机抽样模拟系统长期运行，能有效估计MTBF、可用性等指标。

3.3 联合建模方法

鉴于实时性与可靠性相互交织的特性，单一维度的评估已显不足，联合建模成为研究热点。时间Petri网（TimedPetriNets）通过为变迁赋予时间戳，能够同时刻画事件的逻辑关系与时序约束，适用于对控制流程进行形式化验证。随机实时自动机（StochasticTimed Automata）则进一步将概率引入模型，能够分析在随机故障干扰下系统的实时行为。此外，基于UML或SysML的模型驱动工程（MDE）方法，支持从高层需求到详细设计的全流程建模，并可集成实时性与可靠性分析插件，实现“设计即验证”的开发范式，极大提升了复杂系统的设计效率与质量。

4 提升实时性与可靠性的关键技术

4.1 冗余与容错设计

冗余是提升可靠性的经典策略，其核心思想是通过增加额外的资源来掩盖故障。硬件冗余最为直接，如采用双机热备架构，当主控制器失效时，备用机可无缝接管；在安全关键系统中，常采用“三取二”（2oo3）表决机制，三个独立通道同时工作，输出结果由多数决定，可容忍单通道故障。软件冗余则通过N版本编程实现，即由不同团队开发功能相同但实现各异的程序版本，通过比较其输出来检测软件缺陷[3]。信息冗余主要体现在通信层面，通过添加循环冗余校验（CRC）码或采

用前向纠错（FEC）技术，可以在接收端检测甚至纠正传输错误。时间冗余则通过重传或任务重执行来应对瞬时性故障，确保关键操作最终成功。

4.2 实时操作系统与调度优化

选择合适的实时操作系统是保障实时性的第一步。在此基础上，调度算法的优化是关键。对于混合关键性系统，即同时包含硬实时和软实时任务的系统，采用混合关键性调度策略，可以在系统负载正常时兼顾所有任务，而在高负载时优先保障高关键任务的执行。此外，对于周期性极强的控制任务，采用静态调度表（如AUTOSAR架构中的ScheduleTable）可以预先规划好每个时间槽的任务，彻底消除动态调度带来的不确定性，实现极致的确定性。

4.3 确定性网络技术

网络的不确定性是分布式控制系统的主要瓶颈。时间敏感网络（TSN）技术的出现为此提供了革命性解决方案。TSN基于IEEE802.1系列标准，通过时间感知整形器（TAS）、帧抢占、流量调度等机制，为关键流量预留专用时隙，确保其传输延迟和抖动在微秒级范围内。OPCUAoverTSN的结合，更是将语义互操作性与确定性通信融为一体，为构建开放、统一的工业互联网奠定了基础。在无线场景下，5G的超可靠低时延通信（URLLC）特性，能够提供低于1毫秒的空口延迟和高达99.999%的可靠性，为移动机器人、AGV等应用开辟了新可能。

4.4 智能诊断与预测性维护

传统的“事后维修”模式已无法满足现代高可用系统的需求。借助机器学习技术，系统可以对海量运行数据进行实时分析，实现异常检测与故障预警。例如，利用长短期记忆网络（LSTM）可以学习设备正常运行的时序模式，一旦出现偏离即可发出预警。更进一步，基于数字孪生（DigitalTwin）技术，可以在虚拟空间中构建物理系统的精确映射，通过仿真预测其未来健康状态，并制定最优的维护策略，实现从“被动维修”到“预测性维护”的转变[4]。这种主动健康管理能力，不仅能预防突发故障，还能在系统性能轻微退化时自适应调整控制参数，维持整体性能稳定。

4.5 安全与信息安全融合

在万物互联的时代，网络安全已成为影响系统可靠性的新维度。针对工业控制系统的网络攻击，如拒绝服务（DoS）攻击或恶意指令注入，可能直接导致控制失效。因此，必须将功能安全（如IEC61508标准）与信息安全（如IEC62443标准）进行深度融合设计。这包括在硬件层面实现安全启动，确保固件未被篡改；在通信层面采用TLS/DTLS等加密协议保障数据机密性与完整性；在系统层面实施严格的访问控制与权限管理，遵循最小权限原则。只有构建起纵深防御体系，才能在开放互联的环境中，同时保障系统的功能安全与信息安全。

5 结语

电气自动化控制系统的实时性与可靠性是现代工业安全高效运行的双重基石。本文系统阐述了二者的技术内涵，揭示了其既协同又冲突的辩证关系，并深入剖析了影响性能的硬件、软件、网络及环境等多维因素。研究表明，单一技术手段难以兼顾双重目标，必须采取系统性思维，通过冗余容错设计、实时调度优化、确定性网络构建、智能诊断预测以及安全信息融合等多维度协同策略，方能实现性能的全面提升。未来，随着边缘智能、云边协同、自愈控制等新技术的深度融合，电气自动化控制系统将不断突破现有性能边界，为智能制造、能源转型等国家战略提供更加坚实、可靠、智能的技术支撑。

参考文献

[1]刘侠.电气自动化控制系统的可靠性分析与提升策略研究[J].中国井矿盐,2025,56(04):28-29.

[2]宋小平.基于PLC的电气自动化控制系统设计与优化[C]//广西大学广西县域经济发展研究院.2025年第三届工程技术数智赋能县域经济城乡融合发展学术交流会论文集.杭州萨萌科技有限公司;,2025:266-267.

[3]马忠兴.电力系统中电气自动化控制技术的应用研究[J].中国科技投资,2025,(16):41-43.

[4]廖建伟.电气自动化控制系统设计研究[J].科技资讯,2024,22(23):105-107.