# 高精密自动化设备电气控制系统的模块化与安全设计研究

王泽华
华海清科（北京）科技有限公司　北京　100000

**摘　要：**本文聚焦于高精密自动化设备电气控制系统的两大核心议题：模块化设计与安全设计。首先，系统阐述了高精密设备对电气控制系统在精度、实时性、抗干扰性等方面的严苛要求，并分析了传统集中式架构在面对复杂需求时的局限性。其次，深入探讨了模块化设计理念，构建了包含电源管理、运动控制、逻辑控制、人机交互（HMI）及通信网络五大核心功能模块的系统架构，并详细论述了各模块的设计原则、技术选型与接口标准化策略。在此基础上，本文将功能安全理念深度融入系统设计全过程，依据IEC62061与ISO13849标准，提出了涵盖风险评估、安全回路设计、安全PLC/继电器应用以及软件层面安全机制的多层次安全防护体系。该方法不仅能显著提升系统的开发效率、可维护性与可扩展性，更能从根本上保障人员、设备与环境的安全，为高精密自动化装备的智能化、柔性化发展提供了坚实的技术支撑。

**关键词：**高精密自动化；电气控制系统；模块化设计；功能安全；IEC62061；安全PLC

## 引言

全球制造业向高质量、高效高柔转型，高精密自动化设备成为国家科技竞争力标志。这类设备要在微观尺度实现亚微米级操作精度，高度依赖复杂精密的电气控制系统，它是设备动作的“神经中枢”，关乎工艺稳定与产品质量。然而，其电气控制系统挑战巨大。要具备卓越动态性能，在高速运动中精准控制执行单元；运行环境有强干扰，对抗干扰和稳定性要求极高；人机协作增多，安全风险放大，失效后果严重。传统集中式或半集中式架构，硬件软件耦合度高，扩展维护难，升级成本高、周期长，且安全功能缺乏系统规划，难满足现代标准。为此，本文提出以模块化设计与功能安全设计作为高精密自动化设备电气控制系统的核心设计理念，二者相辅相成，可提升系统性能与安全性。

## 1 高精密自动化设备对电气控制系统的核心要求

高精密自动化设备对电气控制系统有核心要求：极致动态响应与控制精度是关键，需驱动伺服/直驱电机实现平滑轨迹跟踪，要求高采样频率、低控制环路延迟及先进算法补偿非线性特性与外部扰动；卓越实时性与确定性不可或缺，控制过程要严格实时确定，环节延迟可预测稳定，常采用实时操作系统或硬实时通信网络；强大抗干扰与电磁兼容能力是保障，设备内部易产生电磁干扰，需遵循严格EMC设计规范；高可靠性与可用性可减少经济损失，关键部件要冗余设计，具备自诊断和故障预警功能；全面功能安全性是人机共存基础，要可靠检测危险状态，在规定时间将设备带入安全状态，且安全功能独立于主控制逻辑。

## 2 电气控制系统的模块化架构设计

### 2.1 模块化设计原则

一是高内聚：每个模块内部的功能应紧密相关，共同完成一个特定的、完整的任务。二是低耦合：模块之间仅通过定义良好的、标准化的接口进行交互，尽量减少相互依赖。一个模块的变更不应轻易影响其他模块。三是可替换性与可复用性：模块应设计成“即插即用”的形式，便于在不同项目或同一项目的不同阶段进行替换或复用。四是标准化接口：模块间的通信协议、电气连接、机械安装等均需遵循统一标准。

### 2.2 核心功能模块划分

基于以上原则，一个典型的高精密自动化设备电气控制系统可划分为以下五大核心模块：

#### 2.2.1 电源管理模块

该模块通常由主电源分配单元、多路隔离稳压电源、不间断电源（UPS）以及可选的能量回馈单元构成。主电源分配单元负责对输入市电进行初步处理，集成断路器、滤波器和浪涌保护器（SPD），确保电网波动和瞬态干扰不会影响下游设备。为了防止不同子系统间的电源噪声相互串扰，必须采用多路相互隔离的直流稳压电源，分别为控制逻辑、伺服驱动、传感器和人机交互界面等提供各自所需的电压等级（如24VDC、±15VDC）。对于关键控制单元，如PLC和工控机，则需配备不间断电

源（UPS），以确保在突发断电时能够执行安全停机程序并保存关键数据[1]。在大功率、频繁启停的应用场景下，引入能量回馈单元可以将制动过程中产生的能量高效地回馈至电网，从而显著提升整机的能源利用效率。

2.2.2 运动控制模块

通常由一个高性能的运动控制器和多个伺服或步进驱动器协同工作。运动控制器作为大脑，负责运行复杂的轨迹规划、多轴插补等先进算法，并通过硬实时工业以太网（如EtherCAT）以极高的频率向各轴驱动器发送精确的位置、速度或转矩指令。伺服驱动器则作为执行者，接收这些指令后驱动电机运转，并通过高分辨率编码器（如EnDat、BiSS-C接口）实时反馈电机的实际位置，从而构成一个高速闭环控制系统。为了满足高精密应用对动态响应和确定性的严苛要求，整个运动控制链路，从控制器到驱动器再到电机，都必须选用支持高级控制模式（如PVT、电子凸轮CAM）的高端产品，并确保其间的通信协议具备微秒级的同步精度和极低的通信抖动。

2.2.3 逻辑控制与安全模块

主逻辑控制器（通常为PLC或工业CPU）负责处理所有非实时的逻辑任务，例如管理大量的数字和模拟IO点、执行设备的状态机切换、处理报警信息以及与上位管理系统进行数据交换。而安全控制器则是一个完全独立且经过国际安全认证的子系统，其唯一使命就是监控所有与安全相关的输入信号（如急停按钮、安全门锁、安全光幕等），并在检测到任何危险状态时，立即通过专用的安全输出通道（如STO信号）直接切断危险源的动力[2]。安全控制器与主逻辑控制器之间可以通过PROFIsafe或FSoE等安全通信协议交换必要的状态信息，但安全回路的最终决策权和执行权必须始终保持独立，不受主控制器任何故障的影响，这是功能安全设计的根本原则。

2.2.4 人机交互（HMI）

该模块主要由工业触摸屏（HMI）构成，它提供直观、友好的图形化操作界面，使操作员能够方便地进行参数设置、实时监控设备运行状态、查看历史报警记录以及执行手动调试等操作。除了屏幕操作外，在设备本体的关键位置还应设置本地操作面板（LOP），配备必要的物理按钮和状态指示灯，用于紧急情况下的快速干预和基本状态确认。为了适应现代工厂的信息化需求，HMI还应支持通过OPCUA等开放、安全的标准协议，将设备的生产数据、OEE指标等信息无缝上传至MES或SCADA系统，实现远程监控和大数据分析。

2.2.5 通信网络模块

一个典型的高精密控制系统可以采用分层的网络架构。底层是硬实时控制网络，通常选用EtherCAT或PROFINETIRT等工业以太网技术，专门用于承载对时间极度敏感的数据流，如运动控制指令、高速IO刷新和编码器反馈，确保微秒级的同步精度和确定性。上层则是标准以太网，用于处理HMI画面刷新、PLC程序下载、设备数据采集以及远程维护等非实时或软实时的通信任务。对于一些简单的外围传感器或执行器，为了降低成本和布线复杂度，也可以酌情采用CANopen或Modbus等传统的现场总线进行连接，形成一个高效、灵活且经济的混合网络拓扑。

## 3 基于功能安全标准的电气安全设计

3.1 安全生命周期与风险评估

其第一步也是最关键的一步是进行全面的风险评估（RiskAssessment）。工程师需要系统地识别设备在其预期使用乃至可合理预见的误用情况下，所有可能存在的危险源，例如挤压、剪切、电击、激光辐射等。随后，对每一种危险进行风险分析，综合考虑伤害的严重程度和发生的可能性，最终确定其风险等级，并用性能等级（PL）或安全完整性等级（SIL）来量化。这份风险评估报告是后续所有安全设计工作的根本依据，它明确规定了需要实现哪些安全功能以及这些功能必须达到的性能水平。

3.2 安全回路的独立性与冗余设计

功能安全标准的核心原则之一是“独立性”。这意味着安全相关部分（SRP/CS）必须在物理或逻辑上与主控制系统分离，以确保主系统的任何故障都不会危及安全功能的执行。在硬件实现上，安全输入器件（如急停按钮）必须采用常闭触点设计，并直接接入安全控制器的专用安全输入通道，中间不得经过普通PLC的IO点。同样，安全输出（如驱动器的STO信号）也必须由安全控制器直接驱动[3]。为了达到更高的安全等级（如PLe或SIL3），安全回路普遍采用冗余设计，即构建双通道甚至三通道的监测路径。安全控制器会持续对各个通道的状态进行交叉比较和监测，一旦发现通道间出现不一致（这通常是某个通道已发生危险失效的征兆），便会立即触发安全停机，从而将系统的危险失效概率降至最低。

3.3 安全PLC与安全继电器的应用

在具体的硬件选型上，安全PLC和安全继电器是两种主流方案。安全PLC适用于逻辑复杂、安全功能众多且需要与上位系统深度集成的场合。它集成了安全逻辑处理、安全通信和安全IO管理功能，编程灵活，易于实现

复杂的互锁、顺序控制和状态管理。相比之下，安全继电器则以其结构简单、成本低廉、接线直观和极高的固有可靠性，成为逻辑简单、点数较少的安全回路（如单个急停回路）的理想选择。在实际的高精密设备中，往往采用两者结合的混合架构：由安全PLC负责处理全局性的、复杂的整体安全逻辑，而将那些对响应时间要求极为苛刻的关键安全功能（如直接切断伺服动力）交由专用的安全继电器或利用驱动器内置的安全功能来实现，以此兼顾灵活性与极致的可靠性。

3.4 软件层面的安全机制

功能安全不仅关乎硬件，软件同样是不可或缺的一环。安全PLC中的安全应用程序必须遵循特定的安全编程指南，并经过严格的测试、验证和文档化，以确保其逻辑的正确性和鲁棒性。此外，无论是主控制器还是安全控制器，都应内置看门狗（Watchdog）定时器机制。看门狗会周期性地被正常运行的程序复位，一旦程序因任何原因跑飞或陷入死循环而无法按时复位看门狗，定时器超时后便会强制系统复位或进入预设的安全状态[4]。在安全控制器之间或安全控制器与主控制器之间的安全通信中，必须采用带有循环冗余校验（CRC）等机制的安全协议，以确保传输数据的完整性和真实性，有效防止因通信错误或数据篡改而导致的误动作。

## 4 模块化与安全设计的协同与融合

模块化与安全设计并非割裂，而是可以深度融合，相互促进。安全功能本身就可以被视为一个独立的、关键的功能模块，这使其能够自然地融入到整体的模块化架构之中。通过将安全控制封装成一个独立的“安全控制模块”，可以有效地将其与其他功能模块（如运动控制、逻辑控制）解耦，极大地简化了系统集成的复杂度，同时也使得安全功能的验证、测试和认证过程变得更加清晰和高效。在定义各个功能模块之间的接口时，就必须前瞻性地将安全信号的传递方式纳入考量。例如，运动控制模块在设计之初就应提供符合国际安全标准的STO、SS1等安全输入接口，并明确定义其电气特性和时序要求。更进一步，如果每个关键模块（尤其是安全模块和运动控制模块）都能够单独获得权威机构的安全认证，那么在进行系统级集成时，工程师只需专注于验证模块间的接口兼容性和整体安全逻辑的正确性，这将大大缩短整个产品的安全认证周期，加速产品上市进程。

## 5 结语

本文聚焦高精密自动化设备电气控制系统，研究其模块化与安全设计方法。传统设计方法难以满足高精密、可靠、安全的综合需求。引入模块化设计理念，把系统分解为电源等五大核心功能模块，可提升开发效率、可维护性、可扩展性及技术先进性。同时，将功能安全理念贯穿系统全生命周期，按相关标准构建独立、冗余且认证的安全控制子系统，是保障安全的关键。模块化与安全设计可有机融合，把安全功能当作关键模块，在接口定义时融入安全考量，能实现安全与性能统一。未来，新技术发展下系统将更智能自适应，在保证性能与安全前提下，深化模块化、标准化和智能化是值得持续探索的方向。

## 参考文献

[1]覃荣波.机械自动化设备电气控制系统的创新设计与性能优化[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.南宁产投涂碳制造有限责任公司;,2025:278-280.

[2]冯德思.非标自动化设备电气控制设计的标准化[J].自动化应用,2023,64(24):135-137.

[3]肖冠.电气自动化设备管理设计问题及前景[J].家庭生活指南,2019,(06):191.

[4]陈良富.电气设备连接线自动控制系统设计与验证[J].电气技术与经济,2025,(09):340-342.