伺服控制器的安全保护设计

谢 林 卢 洲 陈松波
零八一电子集团有限公司，四川 成都 611731

[摘要]文中以跟踪雷达伺服控制器为例，描述了伺服控制器安全保护的主要类型和设计要点，是伺服控制器设计必须重点关注的事项。完备的伺服控制器安全保护设计，是保障人员设备安全、构筑产品可靠性、提升用户满意度的关键。

[关键词]跟踪雷达；伺服控制器；安全保护；设计要点
DOI：10.33142/sca.v8i9.17959 中图分类号：TM301 文献标识码：A

Design of Safety Protection for Servo Controller

XIE Lin, LU Zhou, CHEN Songbo
Lingbayi Electronics Group Co., Ltd., Chengdu, Sichuan, 611731, China

Abstract: Taking the tracking radar servo controller as an example, this article describes the main types and design points of servo controller safety protection, which is a key concern in servo controller design. A complete servo controller safety protection design is the key to ensuring personnel and equipment safety, building product reliability, and improving user satisfaction.

Keywords: tracking radar; servo controller; safety protection; design key points

引言

伺服控制器主要用于驱动电机拖动负载完成预定的动作，鉴于其高电压、大电流及负载惯量大的特点，安全保护设计是其核心之一。一个优秀的伺服控制器设计，不仅要保障人员与设备安全，更要确保系统的工作连续性，最终实现卓越的用户体验。本文以跟踪雷达伺服控制器为例，深入剖析其安全保护设计的主要类型与关键要点。

1 主要类型

跟踪雷达主要通过方位与俯仰伺服控制器，分别驱动雷达天线在方位与俯仰上运动，以实现对目标的精确跟踪。为确保这一过程的稳定可靠，伺服控制器的安全保护设计至关重要，其实现方式主要可归纳为以下几种类型：

（1）电气安全保护。
（2）人员安全保护。
（3）电流保护。
（4）电压保护。
（5）过载保护。
（6）跳闸处理及防护。
（7）电子结构设计保护。
（8）系统设计与冗余保护。

2 设计要点

2.1 电气安全保护

电气安全保护设计旨在通过设计消除风险，核心是杜绝人员在安装、调试、操作及维护时发生误操作或意外接触裸露导电体的可能性，伺服控制器在设计时应综合考虑以下要点：

（1）接口防误与隔离

①采用不同针数、定位槽或插针/插孔结构的插头，防止误插；

②暴露的针状插头/插座在断开时应不带电；

③电压超过 36V 的测试点，其导电部位应凹入不小于探针直径的深度。

（2）高压电路安全

①高压电容器须配备放电装置，确保停机后 2 秒内电压降至 36V 以下；

②25V 以上电源汇流条须加装防护或隔离屏障，防止意外短路；

③高压电源与使能信号须配备状态指示灯。

（3）绝缘、漏电与防护

①设备漏电流需控制在 5mA 以内；若无法避免更大漏电，需设置明确警示；

②内部电路与外部端口须采用防雷设计，高压电路应

增加瞬态抑制二极管和压敏电阻；

③直流电源输入端需设计防反接保护，且电源端子应与机壳隔离。

（4）警示标识

在高电压、大电流、易发热等危险部位，设置醒目、持久的安全警示标识。

2.2 人员安全保护

为保障人员在雷达系统调试、操作和维护过程中的安全，防止机械伤害、高空坠落和电磁辐射等风险，伺服控制器在设计时应综合考虑以下要点：

（1）机械运动防护，防止天线意外转动与倒伏

①硬件互锁，在雷达天线座附近设置 “人在车顶”物理拨动开关。当维护人员需近距离作业时，必须激活此开关。该信号将送达伺服控制器，强制禁止天线转动，建立一道可靠的硬件安全屏障。

②声光预警，伺服控制器在驱动天线转动前自动触发安装在天线上的蜂鸣器进行声光报警，预先提醒周边人员注意并及时撤离至安全距离。

③失电保护，为大型天线的俯仰电机配备失电制动器。在意外断电时，制动器立即生效，防止天线因重力作用发生倒伏或加速下滑，造成压伤或撞击伤害。

（2）高空作业防护，防止人员坠落

跟踪雷达本身尺寸较大或部署于高处，在设计阶段必须集成防高空坠落设施（如护栏、安全绳锚点等），从根本上降低维修人员的高空作业风险。

（3）电磁辐射防护，避免人员受到辐射伤害

在跟踪雷达系统安装布局时，应优先考虑规划人员活动区域，确保调试和维护位置尽量避开雷达辐射主瓣区域，从源头上减少人员暴露在强电磁场下的风险。

2.3 电流保护

伺服控制器的电流保护，主要分为过电流保护、欠电流保护。诱发的原因可能是内部/外部故障引起、负载的变化、参数设置不当、测量误差过大等，在设计时应综合考虑以下要点：

（1）设置与额定功率相匹配的熔断器，设置与额定功率匹配的熔断器，作为电路保护的最后防线，在系统保护失效时及时切断电源。设计中应优先确保系统保护功能有效，避免熔断器动作；在低压或可恢复性故障回路中，可选用自恢复熔断器以提升系统可维护性；

（2）伺服控制器实时监测功率驱动模块状态，一旦收到过流故障信号，立即关闭功率输出，设备依靠惯性自由减速停止，避免硬件损坏；

（3）系统参数设置需统筹空载、低负载与高负载等多种工况，支持根据不同负载状态自适应调整运行参数，确保系统在全工况范围内的稳定与效率；

（4）通过多负载切换及高低温环境试验，提前识别并校准潜在测量误差，防止因测量偏差引发系统误动作；

（5）利用对欠电流与过电流状态的实时监控，系统可准确识别设备作业状态并触发流程切换，从而实现全过程智能保护与控制。例如在电动起子应用中，过电流表示“扭矩到达、螺丝拧紧完成”，欠电流则指示“异常空转”。

2.4 电压保护

伺服控制器的电压保护，主要分为过电压保护、欠电压保护。诱发的原因可能是输入电源异常、泄放电阻异常、再生制动能量积累异常、功率驱动模块异常、瞬时负载过大等，在设计时应综合考虑以下要点：

（1）输入电源保护

①外接浪涌抑制器，有效隔离来自外部电网的瞬时过电压冲击；

②采用三相交流供电时，配置相序保护器，实时检测相序错误与缺相状态。

（2）线路与连接保障

依据电流、电压及环境要求，选用规格匹配的电缆与接插件，确保传输的稳定与可靠性。

（3）电压异常管理

①实时监测输入电压，在检测到过压或欠压时，立即关闭功率驱动输出；

②针对不允许突然断电的关键设备，需选配伺服专用UPS，保障连续运行；

③设置合理的瞬时掉电与过压忍耐时间，在设定时长内的电压波动系统不报警、不停机，避免误动作。

（4）能量泄放与过压防护

①精确计算并选型泄放电阻的阻值与功率，确保当母线电压超过泄放电压保护阈值时，能迅速泄放能量；

②设定合理的电机减速时间，防止因减速过快导致再生能量瞬间回馈，超出泄放能力而引发母线过电压。

2.5 过载保护

伺服控制器的过载保护是一个关键的安全功能，可以有效防止功率驱动模块、电机因超出其承载能力而损坏，在设计时应综合考虑以下要点：

（1）温度监控，系统实时监控功率驱动模块、泄放电阻及电机温度。当温度超过安全阈值时，伺服控制器立即报警并停机。功率驱动模块通常内置温度传感器，可直接监测并上报温度；若泄放电阻或电机因结构、成本等因

素无法安装传感器，伺服控制器可通过热模型算法，实时计算其发热与散热量，间接估算当前温度，实现全面保护；

（2）功率过载保护，系统持续检测输出功率（电压×电流），若瞬时功率持续超过额定值，将立即触发功率过载保护，防止设备损坏；

（3）针对 S2 短时工作制电机（如油源电机），伺服控制器内置运行时间管理功能，严格限制电机单次连续运行的最长时间及两次运行之间的最短间隔，避免电机因累积过热而烧毁。

2.6 跳闸处理及防护

在控制系统中，伺服控制器需要平衡保护机制与运行连续性之间的关键矛盾：当检测到严重故障时，必须立即跳闸以保护电机和设备安全；但频繁跳闸意味着整个运动系统停止工作。因此，现代智能控制器采用分级保护策略，通过实时监测系统参数，仅对危及设备安全的真故障触发跳闸，而对瞬时异常启用自适应调节功能，最大限度维持系统持续运行。在设计时应综合考虑以下要点：

（1）瞬时异常自适应调节功能，应对短期干扰

①过电流自适应调节，当检测到电流超过安全阈值时，伺服控制器不会立即跳闸，而是主动限制输出电流或降低速度/电流给定，此时电机会短暂“憋住”或速度略降，但不会停止转动，待异常消失后自动恢复正常转动。

②过电压自适应调节，当检测到电压超过安全阈值时，伺服控制器不会立即跳闸，而是主动调整速度的减速曲线、主动调整泄放电阻的接通占空比，此时电机会更平滑的降速，但不会因为停止转动而影响整个系统工作的连续性。

③失速自适应调节，当检测到电机转速因负载瞬时异常过大而导致转速异常下降时，伺服控制器不会立即跳闸，而是主动增加输出电流或降低速度给定，避免因负载瞬时异常导致的跳闸，保证整个系统工作的连续性。

④滤波与抗干扰算法，从硬件上对电流反馈、电压反馈等的采集电路的进行滤波处理，从软件上对读取到的电流反馈、电压反馈进行抗干扰处理，剔除瞬时的电磁干扰而导致的误报警、误跳闸。

（2）预警与预防性维护，管理长期风险

①设置多级预警阈值，设置一个比“跳闸阈值”更小的“仅报警阈值”，当设备达到“仅报警阈值”且未达到“跳闸阈值”时，设备进行预警而不跳闸，提醒操作人员检查设备状态或减轻负载，避免设备状态的进一步恶化而导致跳闸。

②设计预测性保护提醒，伺服控制器可根据通过算法实时对系统的历史数据、当前状态、当前命令进行分析计算，可在设备实际达到“跳闸阈值”前进行预测/预警，提醒操作人员检查设备状态或减轻负载，避免设备状态的进一步恶化而导致跳闸。

2.7 电子结构设计保护

伺服控制器在电子结构设计方面的安全保护措施是构建其整体安全性的物理基石，在设计时应综合考虑以下要点：

（1）EMC 设计

①良好的接地设计，提供独立的、低阻抗的保护接地端子，并与外壳可靠连接，为漏电流和干扰提供泄放路径，保障人员防触电安全；同时设计清晰的信号地（数字地、模拟地）、电源地、屏蔽地传输路径，确保 EMC 性能。

②良好的屏蔽设计，合理控制盖板孔洞、盖板壁厚、盖板间接缝的尺寸，在防止内部电磁信号向外辐射干扰其他设备的同时，增强自身抵御外部电磁干扰的能力。

③合理的分区与隔腔设计，保证组合内高压功率部分与低压控制部分进行物理隔离，防止高压功率噪声干扰敏感的弱电控制/反馈信号，降低误操作风险，提高抗干扰能力。

④电源输入串接滤波器，在接口处使用电磁密封衬垫，对关键电路加装屏蔽罩，阻断电磁干扰的传播路径。

（2）散热管理

设计上需综合考虑功耗、成本与空间等因素，灵活采用被动散热、强迫散热、混合散热等方案。

①被动散热方案适用于设备功耗不高且对静音和可靠性有极致要求的场合，不依赖与任何外部动力(如风机、水泵)等，仅通过散热器自身的物理特性（如传导、自然对流、热辐射）来散发热量，常见的是散热底座、散热齿、均热板等。

②强迫散热方案适用于设备发热量大且能接受一定的噪音的场合，需要消耗外部能量，通过风机、水泵等动力装置来强制加快冷却介质（空气或液体）的流动，大幅提升热量散发效率，常见的是散热风机、一体式水冷系统。

③混合散热方案融合了被动散热与强迫散热的优势。在低负载或低温状态下，系统自动切换至被动散热模式，风机与水泵停止运行，实现静音与节能；当负载升高或温度达到设定阈值时，系统迅速启动风机与水泵，增强散热效率，有效抑制设备温度上升，确保系统稳定运行。

（3）环境适应性

①采用金属外壳、加强筋与坚固安装支脚，有效抵御运输及运行中的振动与冲击，防止结构变形损伤内部元件。

②通过密封机箱、密封垫圈及灌胶工艺，实现 IP65 等高防护等级，阻止污染物侵入；并选用耐腐蚀材料，结合表面防盐雾处理，增强系统抗腐蚀能力。

③关键重型与易损部件均布置在靠近安装点的位置，并加装减震器，以降低振动带来的影响。

④为针对极端低温工况，预设加热机制，确保关键部件温度维持在正常工作范围；同时，针对高海拔低气压环境，需优化散热设计，并在必要时采用密封加压方案，保障散热效能。

（4）测试性与维护性设计

①为伺服制动器状态、高压电源开关、电机使能等安全关键信号专门设置测试点与 LED 状态指示灯。维护人员无需开箱，即可通过外部测量或目视观察快速判断设备运行状态。

②在机箱上预设测试插口或维护开关，支持在不改动现有系统接线的前提下，便捷接入测试设备或模拟特定故障，极大简化了诊断流程。

③将继电器、泄放电阻等需定期检视的安全部件，集中布置于易于触及、检查和更换的位置，可有效降低维护复杂度与时间成本。

2.8 系统设计与冗余保护

系统设计与冗余保护是提升整体可靠性的高层次安全策略。为确保系统在各种工况下的稳定与安全，设计时应综合考虑以下要点：

（1）机械运动保护

①锁定机构保护，雷达跟踪器应配备方位与俯仰机械锁定机构。行军时锁定天线，工作时解除。设计中应设置与锁定机构对应的到位开关，当天线处于锁定状态时，伺服控制器被强制禁止功率输出（即禁止开启伺服使能），从而在硬件层面避免因误操作导致的结构件损坏。

②运动限位保护，跟踪雷达的俯仰运动应设有电气与机械双重止档。伺服控制器需实时检测电气止档信号；一旦天线到达电气止档，控制器立即输出反向速度给定，驱动天线减速并反向运动，使其安全离开限位点，避免因撞击机械止档而造成结构性损伤。

③传动柔性设计，针对采用精密齿轮与减速器的传动系统，伺服控制器应融入柔性控制算法（如平滑加减速、转矩前馈），以抑制输出激烈振荡，保护齿轮和减速器免受冲击损伤。

（2）系统级安全功能

①安全扭矩关断，通过独立的高可靠性硬件回路实现安全扭矩关断功能。该功能可绕过软件逻辑，直接切断电机扭矩输出，具有极快的响应速度，设计时应符合 SIL 安全完整性等级/PL 性能等级中的相应标准要求。

②安全连锁设计，可分为平台与环境安全连锁、人员操作安全连锁、系统内部状态连锁等。平台与环境安全连锁为空间层级别安全连锁，主要是确保雷达天线转动不会造成人员、设备损伤，可根据需要设置“人在车顶”“系统展开完成”等开关；人员操作安全连锁为操作层级别的安全连锁，此层级将关键安全决策交于操作手，操作手可通过“转动”“停止”“急停”等开关进行转动控制；系统内部状态连锁为健康层级别的安全连锁，伺服系统内部的各项参数无异常时将执行接收到的转动指令。

（3）系统可靠性提升

①冗余备份设计，在极端重要的应用场景中，采用双路供电、双编码器反馈乃至双控制器架构等高可用性设计。当主系统发生故障时，备用系统能实现无缝接管或执行安全停机流程，最大限度保障任务连续性。

②故障诊断与预警，系统应具备完善的故障记录与预警能力。详细记录历史故障代码及发生时的系统状态参数（如电流、电压、位置），为维护提供数据支撑。同时，系统能在关键参数接近保护阈值时发出早期预警，实现预测性维护。

3 结束语

综上所述，跟踪雷达伺服控制器的安全保护设计是一个涵盖电气、机械、功能与系统的多层次、纵深防御体系设计。从基础的过流、过压保护，到中层的安全连锁、制动保持，再到顶层的冗余架构与功能安全（SIL/PL）设计，每一环节都至关重要。在设计过程中，必须秉持“失效安全”的核心原则，以周密细致的工程态度处理每一个潜在风险。唯有通过系统性的安全设计与严谨的工程实现，才能铸就伺服控制器卓越的安全性与可靠性，最终从根本上提升整个产品质量与市场竞争力。

[参考文献]

[1]王德纯,丁家会,程望东.精密跟踪测量雷达技术[M].北京:电子工业出版社,2006.

[2]李志强.无刷直流电机无位置传感器控制及四开关逆变器控制研究[D].天津:天津大学,2009.

[3]孙健.高精度综合标定转台电控系统研究[D].吉林:长春理工大学,2009.

作者简介：谢林（1988.10—），毕业院校：西北工业大学，所学专业：信息工程，当前就职单位：零八一电子集团有限公司，职称级别：中级工程师；卢洲（1986.7—），毕业院校：南京理工大学，所学专业：自动化，当前就职单位：零八一电子集团有限公司，职称级别：中级工程师；陈松波（1985.12—），毕业院校：中南大学，所学专业：测控技术与仪器，当前就职单位：零八一电子集团有限公司，职务：机电研究所所长，职称级别：高级工程师。