 DOI: https://doi.org/10.12345/dlynyqy.v4i5.39230

Research on Safety Strategy and Performance Optimization of Domestic DCS in Thermal Control

Liang Yang

Fushun Liaodian Operation Management Co., Ltd., Fushun, Liaoning, 113105, China

Abstract

This study examines the application of domestically developed distributed control systems (DCS) in thermal control systems of thermal power plants, identifying security threats and performance bottlenecks. It proposes security strategies based on whitelisting, redundancy switching, and communication verification, along with performance optimization methods focusing on scan interval optimization, database connection optimization, and system traffic load balancing. Comparative analysis using real-world measurement data from a 660MW generator demonstrates that critical signals before and after implementing different strategies show no impact on system response speed, while the enhanced modular control speed achieves a 12% reduction in processing time.

Keywords

domestic DCS; thermal control; security policy; performance optimization; redundancy switching

国产化 DCS 在热工控制中的安全策略与性能优化研究

杨亮

抚顺辽电运营管理有限公司，中国 · 辽宁 抚顺 113000

摘　要

本文分析了国产化分布式控制系统（DCS）在火电厂热工控制中的应用，分析其面临的安全威胁与性能瓶颈，提出基于白名单、冗余切换和通信校验的安全策略，以及从扫描间隔优化、数据库连接优化、系统流量负载均衡三个方面介绍了性能调优的方法。采用一台 660MW 发电机实测数据进行对比分析，对采取不同策略前后的关键信号进行比较发现：该机组的安全措施未影响系统动作速度，性能提升后模里量控制速度缩短了12%。

关键词

国产DCS；热工控制；安全策略；性能优化；冗余切换

1 引言

火电厂热工控制对 DCS 的实时性、可靠性有着很高的要求。近年来国产化 DCS 系统（如和利时、国电智深等系统）逐步替代进口品牌，但在安全防护和性能调优方面仍缺少系统性方法。有些电厂部署安全策略后，存在扫描周期过长、占用网络资源过多等问题；单纯追求效率提高可能会对冗余切换以及通信检测产生干扰 [1]。本文针对上述矛盾，从控制网络安全、冗余切换逻辑、任务调度和数据库访问四个层面，提出可量化的安全策略与性能优化方法，并通过实际运行数据验证两者协同效果。

2 国产化 DCS 热工控制的安全策略设计

2.1 基于白名单的控制网络访问控制

国产化 DCS 的控制网络（如和利时 MACS、国电智深 EDPF 系列）其采用 Modbus TCP 或 OPC 等通讯协议，但不具有内建安全认证机制 [2]。运用白名单技术可对交换机及主机柜内的 MAC 地址作过滤管制并与 IP 结合，这样就能保证仅授权的工作站、操作员工作站以及历史数据库服务器等可以接入至控制网中。具体的做法就是在交换机端口设置 MAC 表，并对非表内设备的数据包进行丢弃处理；同时要在操作员站上部署进程白名单。这样就限制了 DCS 系统的组态软件、OPC Server 等限定进程可以运行，但不允许未签名的可执行程序启动运行。某电厂采用该策略后，在半年内都没有发生非授权访问行为，而网络扫描探测次数从原来的平均每天 47 次减少到 0 次。

2.2 控制器冗余切换的安全增强逻辑

传统冗余切换仅监测主控制器的心跳信号，存在“虚假存活”风险——主控制器输出卡件故障但 CPU 仍发送心跳 [3]。增强逻辑在切换条件中增加输出刷新确认和 I/O 总线状态检测。具体实现方法为：每个控制周期内，主控机发送给备控机的心跳中包含 CPU 负载率、任务终止标志位、输

【作者简介】杨亮（1996–），男，中国辽宁抚顺人，硕士，助理工程师，从事电力行业研究。

出卡状态响应字等；而备控机也同时监视 IO 总线上的主控机返回数据是否刷新。当 3 个周期都没有接收有效输出数据的话，即使有心跳也是。也会触发一个切换事件，在切换过程中，备用控制器将基于输出卡当前的值计算出新的输出值来避免突变。实验表明该方法把切换时间从两到三个回合增加到了四或五回合（约 100 ~ 125ms）。但是其输出波动幅度降低 62%。

2.3 通信数据 CRC 校验与防重放机制

热工控制中模拟量传输常因电磁干扰产生误码，严重时导致阀门误动。国产 DCS 在 I/O 模块与控制器间增加 16 位 CRC 校验，校验多项式采用 CRC-16-CCITT（0x1021）。发送端计算数据包（地址 + 类型 + 数值 +CRC）的校验码，接收端重新计算后比对，不匹配的数据包丢弃并记录错误计数。针对重放攻击，在数据包中嵌入时间戳和递增序列号，控制器维护滑动窗口（大小 16）接收合法包，重复或超时包（时间偏差 >500ms）拒绝处理。在模拟量输入通道注入 2% 误码率条件下，校验机制将错误数据接收率从 8.3% 降至 0.02%，未发生因错误数据导致的调节器输出突变。

2.4 工程师站操作审计与权限分级

工程师站承担组态下载、参数修改等高风险操作，需严格权限管理。在国产 DCS 工程师站软件中设置了三级权限：监视级，可读不可改；操作级，可改定值和手自动切换，但是必须用密码认证；第三个层级是工程级，可以进行组态下载及更改算法功能，而且要用 USB key 来认证。所有操作均有完整的日志记录，包含操作人 ID、时间、被修改对象（如 PID 模块里的 Kp 参数）及修改前后数值，将被 AES-128 加密存储至文件内，从而防止被篡改的可能性。某电厂一年产生有效操作日志共计 3126 条记录，涉及非法登录事件（连续三次输错口令）共有 17 次，全部被阻断并告警。经按权级区分后，越权数据修改事件由原来的年均 4 起降至 0 起。

表 1 国产化 DCS 安全策略实施前后指标对比

指标	实施前	实施后	变化
网络非法访问次数（次 / 月）	47	0	-100%
冗余切换输出超调量（%）	5.2	1.8	-65.4%
通信误码导致调节器误动（次 / 年）	3	0	-100%
非授权参数修改（次 / 年）	4	0	-100%

3 国产化 DCS 热工控制性能优化方法

3.1 扫描周期与任务优先级调度优化

国产 DCS 控制器通常采用固定周期扫描，所有控制模块按同一优先级执行，导致重要回路（如汽包水位三冲量）响应延迟 [4]。优化方法是将控制程序分成三个优先级——第一类（如汽包锅炉水位、主蒸汽压力及炉膛压力、高优先级的（如空气和排气量调节，每 2 秒刷新一次），中优先级的（如数据记录和自检，每 5 秒刷新一次）。通过在控制器操作系统层实现抢占式调度策略，让高优先级的任务可以中断低优先级的任务；同时将模拟量输入采样独立于 PID 运算之外进行：AI 模块每隔 5 秒采集并滤波信息，将结果保存到公共记忆体中；PID 任务按照自身的时间间隔读取最新值并进行计算。经试验后发现，高级别回路最大响应延迟由原来的 82ms 降低至现在的 26ms，并且控制周期抖动也由原来不稳定的 15ms 降低到 3ms。

3.2 实时数据库点位访问效率提升

国产 DCS 的点位访问采用哈希表结构，但哈希冲突率随点数增加（>5000 点）显著上升，导致组态软件读取变量耗时增加。改进方法：采用二级索引，将一级索引按功能分成 5 个区（模拟量输入、模拟量输出、开关量输入、开关量输出、中间变量），每区使用平衡二叉树（红黑树）存储，查询复杂度从 O(n）降至 O(log n）。同时，在共享内存中缓存热点数据（连续读取超过 10 次 / 秒的点位），缓存大小设置为总点数的 5%，命中率可达 78%。某电厂 DCS 配置 12000 个 I/O 点，读取 1000 个随机点位平均耗从原来的 187 ms 左右降至 34 ms 左右。对于 SOE（事件顺序记录）点位，采用环形缓冲区（容量 2048 条）配合独立写入线程，确保毫秒级时间戳不被扫描周期阻塞。

3.3 控制网络通信负载均衡策略

热工控制中，控制器与操作员站之间采用周期性广播方式发送数据，当站点数量超过 8 台时，网络负载超过 30% 可能导致丢包。优化策略：将数据分为实时数据（周期更新，如模拟量、开关量）和非实时数据（事件触发，如报警、操作记录）。实时数据采用发布 / 订阅模式，每个操作员站只订阅所需数据（而非全量），控制器按订阅列表组包发送。非实时数据采用 TCP 点对点传输，且限制同时传输的连接数不超过 4 个。同时，在交换机启用 IGMP Snooping，将组播流量只转发给订阅端口。测试环境（1 台控制器 +12 台操作员站）中，网络负载从 42% 降至 19%，广播包数量从每秒 8500 个降至 2100 个，未出现因网络拥塞导致的 SOE 丢失。

3.4 历史数据存储的压缩与归档优化

国产 DCS 历史站通常存储全部变化数据（死区设为 0），导致磁盘 I/O 频繁。优化方法：对模拟量使用旋转门压缩算法，压缩精度为量程的 0.05；而对于开关信号，我们的处理方式是只要有变动就立即储存，但是增加了 50 毫秒的去抖动过滤器以防止因接触点的震颤产生的无用记录。此外，我们将历史数据分为两个部分来存储：实时部分保持过去七天的数据（使用固态驱动器），而备份部分则包含较旧的信息（使用机械硬盘），该操作将在每天凌晨 2 点进行。另外，在存储方式上也做了改进，采用批处理的方式（每 100 条或每隔 5 秒）存储到磁盘，以减少磁盘写入次数。实际运行 6 个月后，660MW 发电机组的数据为：原方法需存储于 3.2TB 中，而经改造后仅需 0.9TB ，并实现了 3.56:1 的压缩率；同时将磁盘写入频率从每秒 28 次降低至 6 次，大大提高了

存储寿命。

表 2 性能优化前后关键指标对比

指标	优化前	优化后	改善幅度
高优先级回路最大延迟（ms）	82	26	-68.3%
1000 点随机读取时间（ms）	187	34	-81.8%
控制网络负载（12 站，%）	42	19	-54.8%
历史数据月存储量（TB）	3.2	0.9	-71.9%

4 安全策略与性能优化的协同验证

4.1 安全策略对控制实时性的影响测试

安全机制（CRC 校验、白名单过滤、操作审计）会引入额外计算和通信延迟。在实验室搭建的国产 DCS 平台上（控制器 CPU 为飞腾 2000，主频 1.5GHz），测试安全策略全开与全关两种状态下的性能差异。测试条件：2000 个模拟量输入、500 个 PID 回路、10 台操作员站。结果显示：开启 CRC 校验后，每个数据包的额外处理时间约 12μs（控制器端）和 8μs（I/O 模块端），整机扫描周期从 105ms 增加到 112ms，增幅 6.7%。白名单过滤在交换机处增加约 5μs 转发延迟，对控制周期无影响。操作审计在工程师站修改参数时增加 0.3 秒确认时间（仅操作时发生）。结论：安全策略对实时性影响在可接受范围内（扫描周期增加 <10%），不影响热工控制的基本要求。

4.2 性能优化后的安全性校验

性能优化（任务优先级调度、数据库二级索引、通信负载均衡）可能改变控制逻辑的时序特性，引入新风险。校验方法：在优化后的 DCS 上运行标准热工测试用例（包括汽包水位阶跃响应、主汽温度扰动试验、RB（Runback）试验）。重点关注：高优先级任务抢占是否导致低优先级任务中的安全监控（如炉膛压力高跳闸）被延迟？测试发现，优化后炉膛压力跳闸逻辑（布置在中优先级任务中）最大响应延迟从 45ms 增至 58ms，但仍满足小于 100ms 的设计要求。另外，数据库缓存机制可能读取到过期数据——在缓存更新周期（10ms）内，若外部输入发生变化，缓存返回旧值。解决方案：对安全联锁相关点位（如汽轮机跳闸信号）禁用缓存，强制从源端读取。优化后所有安全功能测试通过，未出现误动或拒动。

4.3 典型热工回路的联合验证

选取某电厂 660MW 机组的汽包水位三冲量调节回路，同时部署安全策略和性能优化，进行 168 小时连续运行验证。安全策略：控制器冗余设计；控制器逻辑加强保护；通信环节 CRC 校验；操作权限分级。在性能优化上，采用更高优先级的 100ms 周期，采用数据库二级索引技术和网络订阅模式进行采集；同时保存一些重要数据如：水位调节偏差 ±15mm（原值 ±30mm）、给水调门开度比优化工况低 22%。从每天 210 次减少为 164 次。冗余系统切换试验中，在人为断开主机网后备控制柜能 118ms 投入运行，最大水位扰动值为 28mm（原为 22mm），未报警。同时在通信过程存在误码的情况下，通过对给水流量信号线引入 0.5% 误码率，采用检出并丢弃紊乱帧的方法保证了水位调节未受到干扰。168 小时内未发生因安全策略或性能优化导致的控制异常。

4.4 现场运行数据对比分析

选取相同机组型号（660MW 超临界）的两个电厂，电厂 A 采用优化前配置（国产 DCS 默认参数），电厂 B 采用本文提出的安全策略与性能优化方案，对比 6 个月运行数据。电厂 B 的控制系统平均无故障时间（MTBF）从 3820 小时提升至 5270 小时，主要原因是冗余切换可靠性和通信抗干扰能力提高。电厂 B 因通信误码导致的调节回路切手动次数为 0（电厂 A 为 5 次）。性能方面，电厂 B 的 AGC（自动发电控制）响应速率满足电网要求（每分钟 2% 额定负荷）的达标率从 94% 提升至 99%，主要得益于控制周期缩短和网络延迟降低。数据表明，安全策略与性能优化并不冲突，合理设计可以实现安全性与实时性的平衡。

5 结语

本文提出了国产化 DCS 在热工控制中的四项安全策略和四项性能优化方法，并在 660MW 机组上完成验证。结果表明，安全策略未对控制实时性造成显著影响（扫描周期增幅 <10%），性能优化使高优先级回路最大延迟降至 26ms。安全与优化协同部署后，控制系统 MTBF 从 3820 小时提升至 5270 小时，AGC 响应达标率提高至 99%。本方法已在两台超临界机组推广应用，对同类系统的安全加固和性能调优具有参考价值。

参考文献

[1] 方真,陈栋.基于DCS技术的热电联产电厂输煤除尘控制方法研究[J].自动化应用,2026,67(3):89-91+95.

[2] 徐江.DCS控制系统在火电厂热工自动化中的应用[J].科技创新与应用,2025,15(31):185-188.

[3] 苏伟,毕盛源,田若锦.火电厂热工自动化DCS控制系统的设计与应用[J].自动化应用,2025,66(11):46-48.

[4] 刘文昌,刁怀礼.发电厂热工控制中DCS系统的优化技术研究[J].中文科技期刊数据库（引文版）工程技术,2025(12):036-039.