

ICS 35.020
CCS L 04

T/ACCEM
团 体 标 准

T/ACCEM XXXX—2025

水电站计算机监控系统国产化改造技术导
则

Technical guidelines for localization transformation of computer monitoring system
in hydropower stations

(征求意见稿)

2025-XX-XX 发布

2025-XX-XX 实施

中国商业企业管理协会 发布

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川凉山水洛河电力开发有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：四川凉山水洛河电力开发有限公司、×××、×××。

本文件主要起草人：×××、×××、×××。

水电站计算机监控系统国产化改造技术导则

1 范围

本文件规定了水电站计算机监控系统国产化改造的技术要求，包括总体要求、系统设计、软硬件选型与配置、功能要求、性能指标、安全防护、调试与验收以及运行维护与升级等方面内容。

本文件适用于新建及已建水电站的计算机监控系统国产化改造工程。其他水利水电工程中涉及计算机监控系统国产化改造的部分，可参照本文件执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- GB/T 41782.2 物联网 系统互操作性 第2部分：网络连通性
- DL/T 578 水电厂计算机监控系统基本技术条件
- DL/T 5003 电力系统调度自动化设计规程
- NB/T 10880 梯级水电厂集中监控工程设计规范
- YD/T 3802—2020 电信网和互联网数据安全通用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 国产化改造 localization transformation

对水电站计算机监控系统的硬件设备、软件系统等进行更新替换，采用国产自主可控产品及技术，以实现系统核心技术自主掌控、提升系统性能与安全性的过程。

3.2 自主可控 independently controllable

系统所采用的硬件、软件等关键技术和产品，其研发、生产、维护等环节不受制于国外，具备自主知识产权，可确保系统的安全可靠运行及可持续发展。

3.3 冗余 redundant

为提高系统可靠性，对关键设备、部件或功能进行重复配置，当其中某一部分出现故障时，冗余部分能够自动接替工作，确保系统不间断运行。

4 总体要求

4.1 基本原则

4.1.1 自主可控

国产化改造应优先选用国产的硬件设备、软件系统及相关技术，确保核心技术自主可控。在系统设计、开发、集成等过程中，加强对国产技术的研究与应用，减少对国外技术的依赖。

4.1.2 安全可靠

国产化改造应采用冗余设计、容错技术等措施，提高系统的可靠性和稳定性，保障水电站安全运行。对关键设备和环节进行多重备份，确保在部分设备出现故障时，系统仍能正常运行，避免因系统故障导致的生产事故。

4.1.3 先进适用

国产化改造应采用成熟、先进的国产化技术和产品，确保系统具有良好的性能。同时，应充分考虑水电站的实际运行需求和特点，使系统功能实用、易于操作和维护，兼顾系统的扩展性与前瞻性。

4.1.4 兼容扩展

系统应能与水电站现有设备和系统兼容，实现无缝对接，最大程度利用现有资源，避免重复投资。具备良好的扩展性，支持功能的增加和硬件的升级，方便后续系统的优化和改进。

4.2 改造目标

4.2.1 实现核心软硬件国产化替代

国产化改造应对水电站计算机监控系统的核心硬件，进行国产化替换，降低系统对国外产品的依赖，提高系统的自主性和安全性。

4.2.2 提升系统实时性、可靠性及安全性

4.2.2.1 应通过优化系统架构、选用高性能硬件设备和先进软件技术，提升系统的数据采集、处理和传输速度，确保控制命令的及时响应，满足水电站实时监控的要求。

4.2.2.2 加强系统的冗余设计和容错能力，提高系统的可靠性。

4.2.2.3 采用先进的安全防护技术，防范网络攻击、数据泄露等安全风险，保障系统和电站运行的安全。

4.2.3 保障与现有系统兼容，具备可扩展性

4.2.3.1 改造后的系统应能与水电站现有的自动化系统、通信系统等良好兼容，实现数据共享和协同工作。

4.2.3.2 系统架构和设计应充分考虑未来的发展需求，具备灵活的扩展性，便于后续增加新的功能模块、接入新的设备，适应水电站规模扩大或技术升级的需要。

5 系统设计

5.1 系统架构

5.1.1 分层分布式架构

应采用分层分布式系统架构，分为站控层、现地控制层和网络层。各层功能相对独立，又通过网络实现紧密协作，提高系统的可靠性和可维护性。

——站控层负责整个电站的集中监控、数据管理和人机交互，实现对电站设备的远程操作和调度；

——现地控制层直接面向现场设备，完成数据采集、控制执行和设备保护等功能；

——网络层负责站控层与现地控制层之间的数据传输和通信连接。

5.1.2 5.1.2 全分布数据库

采用全分布数据库技术，将数据分散存储在各个节点上，每个节点都能独立管理和维护本地数据。通过数据同步机制，确保各节点数据的一致性和完整性。

5.1.3 5.1.3 开放互联

系统与其他体系的网络连通性应符合GB/T 41782. 2的要求，实现系统间的互联互通和资源共享，便于构建综合的水电自动化管控平台。

5.2 硬件设计

5.2.1 PLC 组态软件及配套 PLC 国产器件

国产化改造后PLC应由硬件和软件构成。

——硬件：CPU 模块、外围接口模块。硬件结构见图 1 所示。

——软件：嵌入式实时操作系统、IDE 集成开发环境和 Runtime 运行时环境系统。

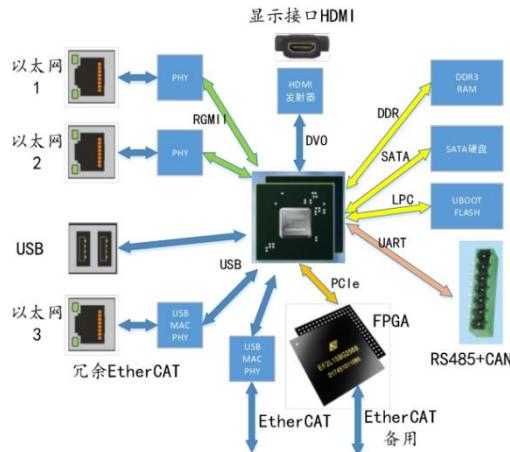


图 1 硬件结构图

5.2.2 关键设备冗余配置

关键硬件设备，如服务器、通信设备、电源模块等，应采用冗余配置方式。如配备双机热备服务器、通信网络采用冗余链路设计、电源模块采用冗余电源。

5.2.3 抗干扰与自诊断能力

硬件设备应具备良好的抗干扰能力，满足水电站复杂电磁环境下的运行要求。

——设备采用电磁兼容性设计，确保数据采集和传输的准确性。

——硬件系统应具备自诊断功能，能够实时监测设备的运行状态，自动检测故障并进行定位，及时发出报警信息，便于维护人员快速处理，提高系统的可维护性。

5.3 软件设计

5.3.1 国产操作系统与数据库选用

5.3.1.1 操作系统应选用国产的成熟产品，如麒麟操作系统。

5.3.1.2 数据库管理系统宜采用国产达梦数据库等，能够满足水电站监控系统对数据存储、管理和查询的需求，实现数据的高效处理和安全存储。

5.3.2 组态软件功能要求

组态软件支持 IEC61131-3规定的五种语言和C/C++高级语言编程，可在多系统上运行。支持常见的现场总线协议，实现与各种现场设备的通信连接。

6 软硬件选型与配置

6.1 硬件选型

6.1.1 国产自主可控产品

6.1.1.1 服务器、PLC、网络设备（交换机、路由器等）、数据采集设备等硬件，应优先选用国产自主可控产品。

6.1.1.2 产品应经过严格的测试和验证，具备良好的性能、可靠性和稳定性，满足水电站监控系统长期运行的要求。

6.1.2 6.1.2 性能匹配与冗余可靠

硬件设备的性能应与水电站监控系统的规模、数据处理量、控制要求等相匹配。

——服务器应具备足够的计算能力和内存容量，以满足大量数据的存储和快速处理需求；

——PLC 的运算速度和 I/O 点数应满足现场设备的数据采集和控制要求。

6.1.3 兼容扩展要求

6.1.3.1 硬件设备应具备良好的兼容性和扩展性，能够与现有系统中的其他设备协同工作，避免出现兼容性问题。

6.1.3.2 设备应预留足够的接口和扩展槽，便于后续增加新的功能模块或接入新的设备，满足系统功能扩展和升级的需求。

6.2 软件选型

6.2.1 国产系统

操作系统、数据库管理系统、监控软件、组态软件等软件，应采用国产产品。

——国产操作系统应具备完善的功能、良好的稳定性和安全性，支持多任务处理和实时响应；

——国产数据库应能够高效存储和管理大量的历史数据和实时数据，提供可靠的数据查询和分析功能；

——监控软件和组态软件应具备丰富的功能模块、友好的用户界面和便捷的开发工具，满足水电站监控系统的应用需求。

6.2.2 实时数据处理与多任务调度

6.2.2.1 软件系统应具备强大的实时数据处理能力，能够快速采集、处理和存储现场设备上传的实时数据，并及时将处理结果反馈给用户或用于控制决策。

6.2.2.2 软件系统应支持基于优先级的多任务调度机制，确保关键任务（如控制命令执行、报警处理等）能够得到优先处理，保证系统的实时性和可靠性。

6.2.3 跨平台兼容

软件应具备跨平台兼容性，能够在不同的硬件架构和操作系统上稳定运行。

7 系统功能要求

7.1 数据采集与处理

7.1.1 实时采集

7.1.1.1 监控系统应能够实时采集水电站各类设备的运行数据，包括电气量、非电气量、开关量。

7.1.1.2 采集频率应满足水电站运行监控的要求，确保及时获取设备的最新状态信息。

7.1.2 滤波与校验

7.1.2.1 应具备对采集到的数据自动进行滤波处理，去除噪声干扰，提高数据的准确性和可靠性。

7.1.2.2 应具备采用数据校验算法，对数据的完整性、合理性进行自动校验，及时发现和纠正错误数据，保证数据质量。对于异常数据，应进行标记和记录，并发出报警信息，提醒运维人员关注。

7.2 安全监视

7.2.1 设备状态监视

7.2.1.1 实时监视水电站设备的运行状态，包括机组、变压器、开关设备、辅助设备等。通过图形化界面、数据报表等方式，直观展示设备的运行参数、工作状态和健康状况。

7.2.1.2 设备的异常状态（如温度过高、振动过大、压力异常等）进行实时监测和预警，及时发现设备故障隐患，保障设备安全运行。

7.2.2 报警信息处理

7.2.2.1 系统应具备完善的报警机制，对设备故障、异常工况等产生的报警信息进行实时采集、分类、处理和显示。

7.2.2.2 根据报警的严重程度，应设置不同的报警级别，并采用不同的报警方式（如声光报警、短信通知、弹窗提示等），确保运行人员能够及时获取重要报警信息。

7.2.2.3 系统应对报警信息自动进行记录和存储，便于后续查询和分析，为故障诊断和设备维护提供依据。

7.3 控制调节

7.3.1 远程控制

7.3.1.1 监控系统应具备远程控制功能，运行人员可通过站控层操作界面，对水电站设备进行远程操作。

7.3.1.2 远程控制操作应具备严格的权限管理和操作流程，确保操作的安全性和准确性。

7.3.1.3 操作过程中，系统应实时反馈设备的操作状态和执行结果，便于运行人员确认操作是否成功。

7.3.2 顺序控制

7.3.2.1 应支持顺序控制功能，能够按照预设的操作流程，自动完成对水电站设备的一系列操作。

7.3.2.2 顺序控制流程应具备可靠性和灵活性，可根据实际运行需求进行编辑、调试和优化，提高设备操作的效率和准确性，减少人为操作失误。

7.3.3 AGC/AVC 控制

具备自动发电控制（AGC）和自动电压控制（AVC）功能，且AGC/AVC控制功能应具备高精度、快速响应和良好的稳定性，满足电力系统对水电站运行的要求。

——AGC根据电力系统调度指令和水电站的实际运行情况，自动调节机组的有功功率输出，实现水电站在电力系统中的经济运行和负荷分配；

——AVC根据系统电压要求和水电站的无功功率储备，自动调节机组的无功功率输出和变压器的分接头位置，维持水电站及电力系统的电压稳定。

7.4 通信功能

7.4.1 支持主流协议

监控系统应支持多种主流通信协议，实现与不同厂家设备、外部系统之间的数据通信和信息交互。通过标准化的通信协议，确保系统的开放性和兼容性。

7.4.2 与外部系统数据交互

能够与电力调度自动化系统、水情自动测报系统、继电保护及故障信息管理系统、电能量计量系统等外部系统进行数据交互。

8 系统性能指标

8.1 可靠性

8.1.1 MTBF 与 MTTR 要求

系统的平均无故障时间应符合DL/T 578、DL/T 5003以及NB/T 10880的规定。

8.1.2 关键部件冗余

8.1.2.1 服务器、通信设备、PLC等关键部件，采用冗余配置方式，确保在单个部件出现故障时，系统仍能正常工作，整体性能符合DL/T 578和DL/T 5003的要求。

8.1.2.2 冗余部件应具备自动切换功能，并保证在切换过程中数据不丢失、控制不中断，提高系统的容错能力和可靠性。

8.2 实时性

8.2.1 数据刷新时间

系统的数据刷新时间应满足水电站运行监控的实时性要求，画面数据刷新时间应小于2 s，确保运行人员能够及时获取设备的最新运行状态信息。

8.2.2 8.2.2 控制命令响应时间

控制命令的响应时间应不超过3 s。从运行人员发出控制命令到设备执行相应动作并反馈执行结果的时间间隔应在规定范围内。

8.3 数据采集精度

数据采集精度应满足水电站运行参数监测的要求，确保采集到的设备运行数据准确可靠，为设备状态分析、故障诊断和控制决策提供准确的数据支持。

8.4 安全性

8.4.1 防攻击能力

系统应具备有效的防攻击能力，采用防火墙、入侵检测系统、安全审计等安全防护措施，防范外部网络攻击和恶意软件入侵。

8.4.2 权限管理

建立严格的用户权限管理机制，对不同用户设置不同的操作权限，包括数据查看、控制操作、系统配置等权限。

8.4.3 故障自诊断

系统应具备完善的故障自诊断功能，能够实时监测系统硬件设备、软件系统的运行状态，自动检测故障并进行定位和报警。

9 安全防护

9.1 遵循安全原则

严格遵循“安全分区、网络专用、横向隔离、纵向认证”的原则进行系统安全防护设计。

9.2 网络专用

9.2.1 生产控制大区应采用独立的专用网络，与管理信息大区及外部公共网络物理隔离，保障系统的安全性与稳定性。

9.2.2 网络拓扑结构设计要合理，充分考虑冗余和备用链路，防止单点故障。

9.2.3 网络地址应进行合理规划，采用私有地址空间，并严格限制网络访问权限，只允许授权设备和用户接入生产控制大区网络。

9.3 横向隔离

在生产控制大区与管理信息大区之间，以及生产控制大区内部不同安全区之间，应部署横向隔离装置。

9.4 纵向认证

建立完善的纵向认证体系，实现对上下级调度机构与水电站监控系统之间通信的身份认证和数据加密。应在通信链路两端部署数字证书认证系统，对通信双方进行身份验证，只有通过认证的设备才能建立通信连接。

9.5 数据加密

9.5.1 数据安全应符合GB/T 35273—2020第4章的规定，在数据处理过程中采取措施保护用户隐私，避免敏感信息泄露。

9.5.2 密码强度应符合 GB/T 39786—2021 第 8 章的要求。

9.5.3 采集、传输和存储的敏感数据（如控制指令、用户信息等）应进行加密处理，加密算法应符合 YD/T 3802—2020 第 8 章、第 9 章、第 10 章的规定。

9.6 安全审计

应部署安全审计系统，对水电站计算机监控系统的操作行为、网络流量、设备运行状态等进行全面审计和监测。

——安全审计系统应能实时采集和分析各类安全事件日志，包括用户登录、操作记录、系统故障报警等信息。

——安全审计系统应具备完善的日志存储和查询功能，以便后续对安全事件进行追溯和分析。

9.7 防病毒与恶意软件

在水电站计算机监控系统的各类设备，如服务器、工作站、现地控制单元等，均应安装防病毒软件和恶意软件防护工具。

10 调试与验收

10.1 调试准备

在系统调试前，应完成系统的安装工作，包括硬件设备的安装、软件系统的部署以及网络布线等。同时，应制定详细的调试计划，调试计划应包括调试步骤、调试方法、调试工具、时间安排以及安全注意事项等内容。

——硬件设备进行外观检查，确保设备无损坏、安装牢固，各接口连接正确。

——软件系统进行完整性检查，确认软件版本正确、安装文件齐全。

10.2 单体调试

10.2.1 硬件设备调试

对服务器、PLC、交换机、数据采集设备等硬件设备进行单体调试。

——检查设备的基本功能是否正常；

——PLC 的 I/O 模块数据采集和输出功能测试；

——交换机的端口状态检查、网络连通性测试。

10.2.2 软件系统调试

对操作系统、数据库管理系统、监控软件、组态软件等软件系统进行单体调试。

——检查操作系统的安装是否正确，各项服务是否正常启动；

——数据库管理系统进行初始化配置，创建数据库用户、数据库表等，进行数据插入、查询、更新、删除等操作测试，确保数据库功能正常；

——监控软件和组态软件进行功能调试，包括画面显示、数据采集与处理、报警功能、控制操作等。

10.3 系统联调

在硬件设备和软件系统单体调试完成且功能正常的基础上，进行系统联调。按照系统设计要求，将各个硬件设备和软件系统进行集成，建立站控层与现地控制层之间的通信连接，实现数据的传输和交互。对系统的整体功能进行测试，包括数据采集与处理、安全监视、控制调节、通信功能等。

10.4 验收测试

10.4.1 测试方案制定

应组织成立由运行维护人员、技术专家以及相关管理部门人员等组成的验收小组。验收小组根据系统设计文件、技术规范以及调试报告等资料，制定详细的验收测试方案。

10.4.2 功能测试

按照验收测试方案，对水电站计算机监控系统的功能进行全面测试。

- 数据采集功能测试：检查系统是否能实时、准确地采集水电站各类设备的运行数据；
- 安全监视功能测试：模拟设备的各种运行状态和故障情况，检查系统能否及时发现并准确显示设备状态变化和报警信息，报警信息的分类、分级是否合理；
- 控制调节功能测试：进行远程控制操作、顺序控制操作以及 AGC/AVC 控制功能测试，检查控制命令的执行是否准确、可靠，控制效果是否符合预期；
- 通信功能测试：检查系统与外部系统之间的数据通信是否正常，通信协议是否符合标准，数据交互的准确性和及时性是否满足要求。

10.4.3 性能测试

对系统的性能指标进行测试，主要包括可靠性、实时性、准确性和安全性等方面。

- 可靠性测试：通过模拟系统硬件故障、软件错误等情况，检查系统的冗余切换功能是否正常，系统在故障情况下能否保持不间断运行，记录系统的平均无故障时间（MTBF）和平均修复时间（MTTR），判断是否符合设计要求；
- 实时性测试：测试系统的数据刷新时间、控制命令响应时间等，检查是否满足水电站运行监控的实时性要求；
- 准确性测试：对数据采集精度进行再次验证，确保模拟量采集精度达到规定等级，同时检查系统对设备状态判断的准确性；
- 安全性测试：采用专业的安全测试工具和方法，对系统的防攻击能力、权限管理、故障自诊断等安全防护功能进行测试，检查系统是否存在安全漏洞，能否有效防范各类安全风险。

11 运行维护与升级

11.1 运行维护制度建立

11.1.1 应依据 GB/T 36626—2018 第 5 章的规定，建立系统的安全运维体系，并收集安全评估和事件处理的反馈意见，不断改进安全管理措施，提升系统的整体安全性。

11.1.2 应依据 GB/T 36626—2018 第 8 章的规定，建立系统的安全运维规程。持续监控系统的安全状态，及时发现和处理安全问题。

11.2 日常运行维护

11.2.1 设备巡检

运行维护人员按照规定的巡检周期和内容，对水电站计算机监控系统的硬件设备进行巡检。巡检内容包括但不限于设备外观检查、设备的运行状态检查、设备的环境检查等。

11.2.2 数据备份与恢复

定期对水电站计算机监控系统中的重要数据进行备份，包括历史数据、实时数据、系统配置数据、用户数据等。数据备份宜采用全量备份和增量备份相结合的方式，全量备份每周进行一次，增量备份每天进行一次。

11.2.3 软件维护

应对水电站计算机监控系统中的软件进行定期维护，包括操作系统、数据库管理系统、监控软件、组态软件等。及时安装软件供应商发布的安全补丁和升级程序，修复软件漏洞，提高软件的安全性和稳定性。

11.3 故障处理

当水电站计算机监控系统发生故障时，运行维护人员应按照故障处理流程及时进行处理。