ICS 13.060.30
CCS P 41

团　　体　　标　　准

T/CAPS XXX—202X

基于智慧水务的污水厂自动化控制系统

Automated control system for wastewater treatment plant based on smart water management

（征求意见稿）

202X-XX-XX 发布　　202X-XX-XX 实施

中国生产力学会　　发 布

目　　次

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。

本文件由中国生产力学会标准化工作委员会提出。

本文件由中国生产力学会归口。

本文件起草单位：。

本文件主要起草人：。

基于智慧水务的污水厂自动化控制系统

1 范围

本文件规定了基于智慧水务的污水厂自动化控制系统（以下简称“系统”）的总体要求、系统架构、功能要求、性能要求、安全要求和运行维护要求。

本文件适用于新建、改建、扩建的城镇污水处理厂、工业园区污水处理厂智慧化自动化控制系统的设计、建设和运维。

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 17626（所有部分） 电磁兼容 试验和测量技术

GB/T 20279 网络安全技术 网络和终端隔离产品技术规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28742 污水处理设备安全技术规范

GB/T 28743 污水处理容器设备 通用技术条件

GB/T 30976.2 工业控制系统信息安全 第2部分：验收规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧水务 smart water management

通过物联网、大数据、人工智能、数字孪生、边缘计算等新一代信息技术，与水务生产、运营、管理、服务全流程深度融合，实现水务系统全要素数字化管控、智能决策与优化调度的现代化水务运营模式。

3.2

污水厂自动化控制系统 automated control system for wastewater treatment plant

以污水厂处理工艺为核心，集数据采集、过程控制、连锁保护、智能优化、运营管理于一体的软硬件集成系统。

3.3

数据采集与监控系统 supervisory control and data acquisition; SCADA

以计算机技术为基础，对生产过程进行实时数据采集、监控、报警、趋势分析与远程控制的工业控制系统。

3.4

智能优化控制 intelligent optimal control

基于人工智能算法、工艺机理模型，结合进水水质、水量、环境参数等多源数据，实现污水厂全工艺段的自适应调节、协同优化与节能降耗的先进控制模式。

4 缩略语

下列符号与缩略语适用于本文件。

COD：化学需氧量（Chemical Oxygen Demand）
DCS：分布式控制系统（Distributed Control System）
DO：溶解氧（Dissolved Oxygen）
IO：输入/输出（Input/Output）
MLSS：混合液悬浮固体浓度（Mixed Liquor Suspended Solids）
MTBF：平均无故障时间（Mean Time Between Failures）
ORP：氧化还原电位（Oxidation-Reduction Potential）
PLC：可编程逻辑控制器（Programmable Logic Controller）
TP：总磷（Total Phosphorus）
TN：总氮（Total Nitrogen）
UPS：不间断电源（Uninterruptible Power Supply）

5 总体要求

5.1 设计原则

5.1.1 可靠性原则

系统应采用冗余容错设计，核心设备与链路具备故障自愈能力，适应污水厂高湿、高腐蚀、强干扰的恶劣运行环境，保障全年连续稳定运行。

5.1.2 先进性原则

系统应适配行业主流智慧水务技术，兼顾技术成熟度与前瞻性，支持人工智能、数字孪生等技术的迭代升级，满足污水厂中长期发展需求。

5.1.3 开放性原则

系统应采用标准化的通信协议与数据接口，兼容不同厂商的设备与系统，支持跨平台数据互通与功能扩展。

5.1.4 可扩展性原则

系统硬件、软件均应具备模块化扩展能力，满足污水厂工艺改造、产能提升、功能新增的扩容需求。

5.1.5 安全性原则

系统应符合国家网络安全、生产安全、环境保护相关法规与标准要求，构建全链路安全防护体系，保障生产控制安全、数据安全与网络安全。

5.1.6 易用性原则

系统应具备友好的人机交互界面，操作逻辑符合污水厂运营习惯，功能模块清晰，降低运维人员的学习与操作门槛。

5.2 一般要求

5.2.1 系统应实现污水厂全工艺段的自动化闭环控制，减少人工干预，提升控制稳定性。构建智慧化管控体系，实现水质水量智能调控、能耗药耗智能优化、设备全生命周期管理，达成节能降耗、提质增效的目标。

5.2.2 系统应适配城镇污水处理厂主流处理工艺，包括但不限于 AAO、多级 AO、SBR、MBR、氧化沟、CASS，可根据工艺特点定制化开发控制逻辑，保障工艺适配性。

6 系统架构

6.1 层级架构

系统应采用分层分布式架构，划分为感知层、边缘控制层、网络传输层、平台层、应用层五个层级，系统层级架构见图1。

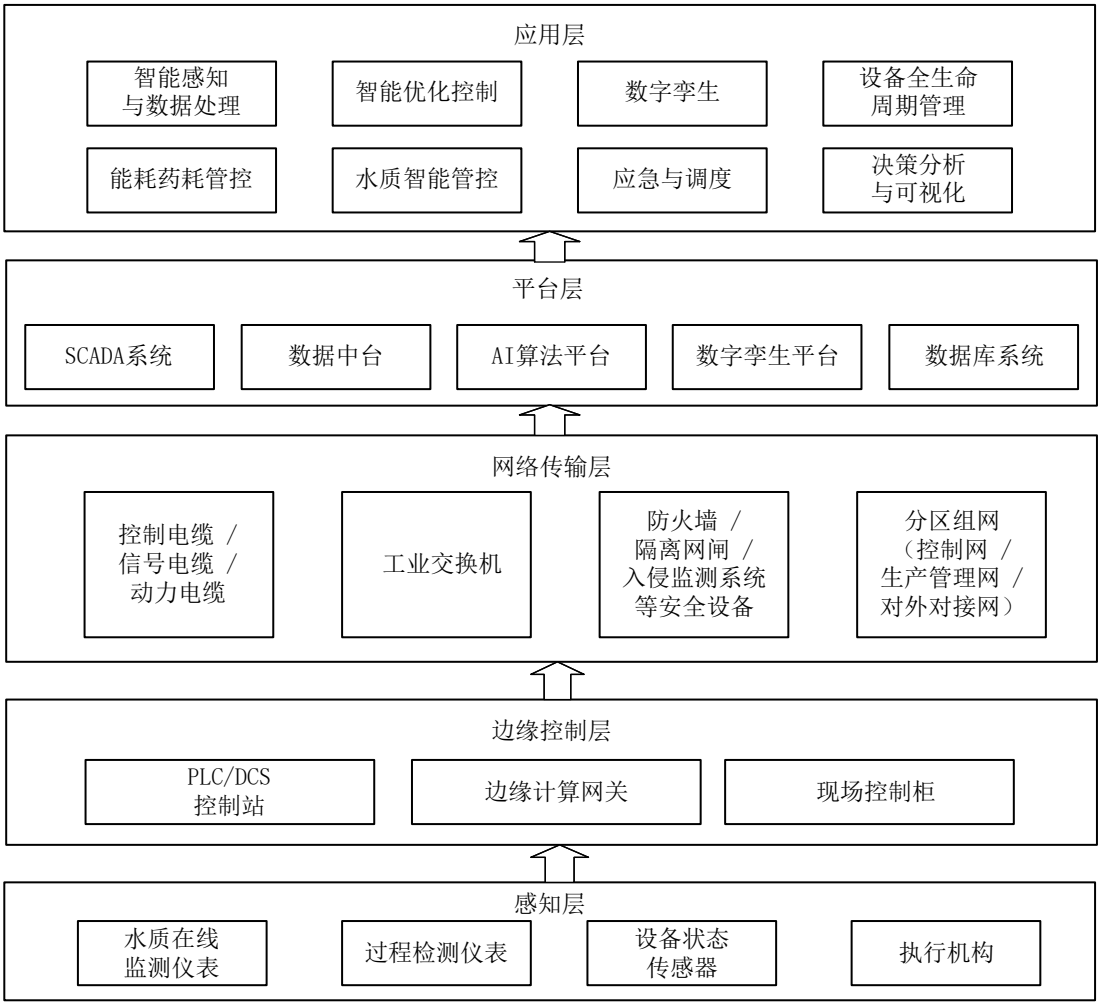

图1　系统层级架构图

a)　感知层：
　1)　包括水质在线监测仪表、过程监测仪表、设备状态传感器、执行机构等；
　2)　应具备高可靠性、高防护等级、高采集精度，支持标准化通信协议，数据采集频率与精度满足工艺控制与智慧化分析需求。
b)　边缘控制层：
　1)　包括 PLC/DCS 控制站、边缘计算网关、现场控制柜等；
　2)　应采用工业级硬件，核心控制器具备冗余配置，控制逻辑独立于上层平台，上层系统故障不影响本地基础控制功能，满足工业现场实时控制需求。
c)　网络传输层：
　1)　包括控制电缆、信号电缆、动力电缆、工业交换机、防火墙、隔离网闸、入侵监测系统等；
　2)　应采用分区组网架构，划分为控制网、生产管理网、对外对接网，各网络区域之间实现安全隔离，传输带宽与冗余能力满足系统实时性与可靠性要求。
d)　平台层：
　1)　包括 SCADA 系统、数据中台、AI 算法平台、数字孪生平台、数据库系统等；
　2)　应具备高并发、高可用、高扩展能力，支持多源数据融合处理，算法模型可迭代优化，功能模块可灵活编排，为上层应用提供稳定的能力支撑。
e)　应用层：

1) 包括生产监控、智能优化控制、设备全生命周期管理、能耗药耗管理、水质智能管控、应急与调度、决策分析与可视化、移动端应用等模块；
2) 应贴合污水厂运营管理实际需求，功能模块边界清晰，操作便捷，支持权限分级管控，满足不同岗位人员的使用需求。

6.2 硬件要求

6.2.1 通用要求

6.2.1.1 系统所有硬件设备应优先选用工业级产品，具备出厂合格证明、检测报告，严禁使用淘汰、非标产品。

6.2.1.2 硬件设备应适应污水厂现场环境，具备良好的防腐、防潮、防尘、抗干扰能力，电磁兼容性应符合 GB/T 17626（所有部分）相关要求。

6.2.1.3 核心硬件设备应具备冗余配置，单点故障不影响系统整体运行，设备选型应兼顾通用性与可维护性，降低运维成本。

6.2.2 感知层硬件要求

6.2.2.1 水质在线监测仪表应符合以下要求：

a) 精度要求：
   1) DO 仪测量精度应不大于±0.1 mg/L；
   2) pH 计测量精度应不大于±0.02pH；
   3) 浊度仪测量精度应不大于±2%FS；
   4) 氨氮、TP、TN 等在线分析仪测量误差应不大于±5%FS。
b) 现场安装仪表防护等级应达到 IP65 及以上，水下安装仪表防护等级应不低于 IP68；
c) 支持 Modbus、OPC UA 等标准化通信协议，应具备自动清洗、温度补偿功能。

6.2.2.2 压力、液位、流量、温度等过程监测仪表，测量精度应不大于±0.5%FS，防护等级应达到 IP65 及以上，适应污水厂腐蚀、结垢工况。

6.2.2.3 振动、温度、转速、泄漏等设备状态传感器，测量精度满足设备状态监测要求，防护等级应不低于 IP65，抗干扰能力强，可长期稳定运行。

6.2.2.4 水泵、阀门、鼓风机、计量泵等执行机构的控制精度满足工艺要求，响应时间应不超过 2 s，防护等级应不低于 IP65，具备手动/自动控制功能，反馈信号准确，故障报警功能完善。

6.2.3 边缘控制层硬件要求

6.2.3.1 PLC/DCS 控制器应符合以下要求：

a) 应采用工业级 32 位及以上处理器，主控系统 CPU 正常运行负荷应不大于 60%；
b) 核心工艺段控制器应采用双机热备冗余配置，冗余切换无扰动；
c) IO 点位预留应不少于 15%；
d) 应具备掉电程序保持功能。

6.2.3.2 边缘计算网关应符合以下要求：

a) 应采用工业级硬件，具备双核及以上处理器，内存不小于 2 GB，存储不小于 8 GB；
b) 支持多协议转换，兼容主流 PLC、仪表、传感器的通信协议；
c) 应具备边缘数据预处理、本地逻辑运算、断点续传的功能；
d) 防护等级应不低于 IP30，宽温宽压设计，适应现场环境。

6.2.3.3 现场控制柜应符合以下要求：

a) 柜体宜采用 304 不锈钢材质,防护等级应不低于 IP54,户外安装柜体防护等级应不低于 IP65；
b) 柜内动力回路与控制回路分开布线，具备防干扰、散热、防雷、接地措施；
c) 柜内配置人机交互终端，可实现本地参数设置、设备控制、状态监控；
d) 所有回路均配备标识，标识清晰、永久、不易脱落。

6.2.4 网络传输层硬件要求

6.2.4.1 工业交换机应符合以下要求：

a) 应采用工业级产品，主控系统采用千兆光纤环网交换机，支持环网冗余协议，环网自愈时间应符合工业环网协议标准，保障网络高可用性；
b) 防护等级不低于 IP30，宽温宽压设计，具备防雷、抗干扰能力；
c) 端口数量预不少于 20%，支持 VLAN 划分、QoS 流量管理。

6.2.4.2 防火墙、隔离网闸、入侵检测系统等安全设备，应符合 GB/T 20279 的相关要求。控制网与管理网之间应采用工业防火墙隔离，生产网与互联网之间应采用单向隔离网闸。

6.2.4.3 控制电缆、信号电缆、动力电缆应分开敷设。信号电缆应采用屏蔽电缆，屏蔽层单端可靠接地，厂区主干传输应采用单模光纤，传输带宽千兆及以上，光纤芯数预留不少于 50%。

6.2.5 平台层硬件要求

6.2.5.1 应采用企业级机架式服务器，核心服务器采用双机热备或集群部署，双路 CPU，内存不应小于 32 GB，硬盘采用 RAID 冗余配置。双路冗余电源，支持热插拔，具备良好的扩展性。服务器机房配备精密空调、UPS、消防、防雷系统。

6.2.5.2 应采用企业级存储阵列，支持时序数据、关系型数据、文件数据的统一存储。存储容量满足 3 年以上原始数据存储需求，预留扩容空间，支持 RAID 冗余配置，具备数据备份、快照、容灾功能。

6.2.5.3 应采用工业级或企业级工控机与监控终端，四核及以上处理器，内存不少于 8 GB，硬盘不少于 512 GB。双网口设计，分别接入控制网与管理网，具备良好的稳定性，支持 7×24 h 连续运行。

6.2.5.4 应采用 LED 或 LCD 拼接大屏显示系统，分辨率不低于 1920×1080、亮度均匀、色彩还原准确，支持多画面分割、任意开窗、信号切换，满足全厂运行态势可视化展示需求。

6.3 软件要求

6.3.1 通用要求

6.3.1.1 软件应采用模块化、组件化设计，具备良好的开放性与可扩展性，支持功能模块的新增、修改与迭代，不影响系统整体运行。

6.3.1.2 软件应具备完善的容错能力，单个功能模块故障不影响系统整体运行，具备数据备份与恢复功能，保障数据安全。

6.3.1.3 软件应具备友好的人机交互界面，操作逻辑清晰、支持中文界面，具备操作引导与帮助功能。

6.3.2 系统软件要求

6.3.2.1 操作系统应进行安全加固，关闭不必要的端口与服务，定期更新安全补丁。

6.3.2.2 应采用时序数据库存储工艺实时数据，关系型数据库存储业务管理数据，支持海量数据的高速存储、查询与分析。具备数据备份、归档、清理功能，保障数据库稳定运行。

6.3.2.3 应采用成熟稳定的企业级中间件，包括消息中间件、应用中间件、接口中间件，支持高并发数据处理，保障系统各模块之间的稳定交互。

6.3.3 基础控制软件要求

6.3.3.1 PLC/DCS 编程软件应支持 LD、FBD、ST、SFC 等多种编程语言，具备在线编程、仿真、调试、故障诊断功能。

6.3.3.2 控制程序应采用结构化、模块化编程，逻辑清晰，注释完整，便于维护与修改。核心控制逻辑与连锁保护程序应独立运行。

6.3.3.3 组态软件应具备图形化编辑功能，支持自定义工艺流程画面、趋势画面、报警画面，具备丰富的控件库与动画效果，满足现场监控需求。

6.3.4 SCADA 系统软件要求

6.3.4.1 应具备全厂设备、仪表数据的实时采集功能，采集频率可自定义，最低采集周期 100 ms。

6.3.4.2 应支持全厂工艺流程可视化监控，设备状态、运行参数、工艺数据实时展示，支持远程控制与参数设置。

6.3.4.3 应支持分级报警、阈值自定义、报警弹窗、声光提示、报警确认、报警查询、报警统计分析的功能，报警记录不可篡改，存储周期不少于 1 年。

6.3.4.4 应支持实时与历史趋势查询，趋势曲线可缩放、对比、导出，数据查询周期可自定义，最小时间分辨率不大于 1 s。
6.3.4.5 应支持三级及以上权限分级管理，所有操作生成不可篡改的日志，存储周期不少于 1 年。
6.3.4.6 应支持自定义报表模板，自动生成日、月、年生产运行报表，支持报表查询、导出、打印。

6.3.5 智慧水务平台软件要求

6.3.5.1 数据中台应具备数据汇聚、治理、建模、服务、资产管理功能，实现多源数据的统一管理服务。
6.3.5.2 AI 算法平台应具备算法模型开发、训练、部署、迭代、管理全流程功能，内置污水厂专用算法模型，支持算法模型在线更新，不影响系统正常运行。
6.3.5.3 数字孪生平台应具备三维建模、模型驱动、实时数据接入、模拟仿真、工况推演功能，支持与 SCADA 系统、设备管理系统、业务系统的数据联动。
6.3.5.4 业务应用模块应具备第 7 章规定的所有智慧化功能，模块之间数据互通，功能协同，可根据灵活配置。

7 功能要求

7.1 自动化控制功能

7.1.1 预处理单元

7.1.1.1 应根据格栅前后液位差或运行时间，自动控制格栅机启停及配套设备联动，并具备渣满报警、过载保护等安全联锁功能。
7.1.1.2 应根据集水池液位、进水流量自动控制进水泵启停台数与变频转速，实现恒液位控制与水泵轮换运行。
7.1.1.3 应自动控制沉砂池曝气、提砂、砂水分离全流程运行，自动控制初沉池刮吸泥机启停与排泥周期，配套污泥泵联动运行。

7.1.2 生化处理单元

7.1.2.1 应根据生化池 DO、ORP、进水水质水量、出水水质指标实现曝气风量闭环调节，支持分区独立控制。
7.1.2.2 应根据生化池 MLSS、污泥沉降比、回流比自动控制内、外回流泵启停与转速，实现回流比精准调节。根据 MLSS、污泥龄、沉淀池液位自动控制剩余污泥排放量。
7.1.2.3 应根据进水水质、ORP、出水 TN 指标自动控制厌氧/缺氧区搅拌器启停与碳源投加量。

7.1.3 深度处理单元

7.1.3.1 应根据进水流量、浊度、TP 指标，自动控制絮凝剂投加量，实现精准加药。
7.1.3.2 应根据滤池液位、过滤水头、运行时间，自动控制滤池的过滤与反冲洗全流程，实现恒水位过滤。
7.1.3.3 应根据出水流量、余氯/紫外线剂量指标，自动控制消毒剂投加量或紫外线灯管功率，保障出水消毒效果，具备药剂泄漏报警与应急处置功能。
7.1.3.4 应根据进水水质、出水 COD 指标，自动控制氧化剂投加量、反应时间，实现处理效果与运行成本的协同优化。
7.1.3.5 应根据进泥量、污泥浓度，自动控制浓缩机启停与运行，配套加药系统联动运行。

7.1.4 污泥脱水系统

7.1.4.1 应根据进泥量、污泥浓度，自动控制污泥进料泵、絮凝剂投加量、脱水机运行频率，实现脱水全流程自动化控制。
7.1.4.2 应自动控制污泥输送机、料仓料位，实现污泥输送、储存的自动化管控，具备料位超限报警与连锁保护功能。

7.1.5 公用工程单元

7.1.5.1　应根据生化池需气量、总管压力，自动控制鼓风机的启停台数与导叶/变频调节，实现恒压供气，具备风机振动、温度、压力超限报警与连锁保护功能。
7.1.5.2　应实现各类药剂的溶解、稀释、投加全流程自动化控制，具备药剂液位低限报警、计量泵故障报警与备用泵自动切换功能。
7.1.5.3　应根据除臭区域臭气浓度、风机压力，自动控制风机变频与喷淋系统运行，实现达标排放与节能运行。
7.1.5.4　应实现全厂配电系统的实时监控，具备电压、电流、功率、电能实时采集，过载、短路、漏电报警与连锁保护功能。

7.2　智慧化应用功能

7.2.1　智能感知与数据处理

7.2.1.1　应实现多源数据融合处理，支持水质、水量、设备、能耗、环境等多维度数据的统一采集与标准化治理。
7.2.1.2　应具备异常数据自动识别、清洗、补全功能，保障分析与控制的准确性。
7.2.1.3　应支持边缘端数据预处理,降低平台层计算压力与网络传输带宽占用,提升数据处理实时性。
7.2.1.4　应具备数据质量管控功能，对采集数据的完整性、准确性、一致性、时效性进行实时监控与预警。

7.2.2　智能优化控制

7.2.2.1　应基于 AI 算法与工艺机理模型，结合进水水质、水量、环境温度、出水水质指标，构建溶解氧预测模型，实现前馈—反馈协同的智能曝气控制。
7.2.2.2　应构建絮凝剂、碳源、消毒剂等药剂的投加预测模型，基于进水水质、水量、出水指标实时优化投加量，实现精准加药。
7.2.2.3　应基于污泥龄、MLSS、污泥沉降性能等参数，智能优化剩余污泥排放量，保障生化系统污泥浓度稳定，减少污泥处理能耗。
7.2.2.4　应实现预处理、生化处理、深度处理、污泥处理全工艺段协同优化，基于进水负荷动态调整各单元运行参数，在满足出水达标前提下，追求综合运行成本最低。

7.2.3　数字孪生

7.2.3.1　应构建全厂 1:1 三维数字孪生模型，覆盖工艺管线、设备、构筑物、仪表等全要素。
7.2.3.2　应实现物理实体与虚拟模型的实时数据同步，数据同步延迟不大于 5 s，实现全厂运行工况的数字化映射与可视化。
7.2.3.3　应具备工艺模拟仿真功能，支持不同进水负荷、运行参数下的工况推演，预测出水水质与能耗变化。
7.2.3.4　应具备虚拟调试与故障模拟功能，可在虚拟模型中开展控制逻辑调试、故障场景模拟，为现场运维与应急处置提供培训与指导。

7.2.4　设备全生命周期管理

7.2.4.1　应实现全厂设备的数字化台账管理，覆盖设备采购、安装、调试、运行、维护、报废全生命周期。
7.2.4.2　应具备智能巡检功能，支持线上巡检任务闭环管理，可配套智能巡检设备，实现巡检数据实时上传与异常预警。
7.2.4.3　应具备设备故障诊断与预测性维护功能，基于设备运行数据、振动、温度等状态参数，智能识别设备异常状态，提前预警设备故障，自动生成维护建议。
7.2.4.4　应具备备品备件智能管理功能，实现库存监控、出入库管理、低库存预警、采购计划自动生成。

7.2.5　能耗药耗管控

7.2.5.1　应实现全厂电耗、药耗、水耗的实时采集、分项计量、统计分析，支持按工艺单元、设备、时间段核算。
7.2.5.2　应具备单耗对标管理功能，支持与设计值、行业先进值、历史最优值对标，超限自动预警。
7.2.5.3　应具备能耗药耗成本核算功能，自动生成日、月、年成本报表，智能分析异常原因并生成优化建议。

7.2.6　水质智能管控

7.2.6.1　应实现进水、过程段、出水全流程水质指标实时监控，水质指标超标分级预警，预警响应时间不大于 2 s。
7.2.6.2　应具备出水水质智能预测功能，可预测未来 24 h 出水水质指标，提前规避超标风险。
7.2.6.3　应具备水质异常溯源功能，当出水水质超标时，智能定位异常原因，生成处置方案。

7.2.7　应急与调度

7.2.7.1　应构建数字化应急预案库，覆盖进水超标、设备故障、停电、药剂泄漏、雨季水量冲击等典型应急场景。
7.2.7.2　应具备异常工况智能识别与联动处置功能，当发生应急场景时自动触发应急预案，下发控制指令。
7.2.7.3　应具备雨季水量智能调度功能，结合降雨量预报、进水水量变化，智能调整运行工况，提升抗冲击负荷能力。
7.2.7.4　应具备应急指挥功能，支持应急事件全流程管理与事后复盘。

7.2.8　决策分析与可视化

7.2.8.1　应具备全厂运行态势可视化大屏，集中展示生产运行、水质、能耗、设备、报警等核心指标，支持多维度数据钻取。
7.2.8.2　应具备多维度统计分析功能，自动生成各类生产、运维、成本报表，支持自定义配置。
7.2.8.3　应具备运营决策分析功能，智能分析运行瓶颈，生成优化方案，为运营管理决策提供数据支撑。

8　性能要求

8.1　控制性能

系统控制性能应满足以下要求：
a)　模拟量控制回路稳态误差应不超过±1%；
b)　联锁保护动作时间应不大于 500 ms；
c)　系统核心工艺段自动控制投运率应不低于 95%；
d)　手动/自动切换应实现无扰切换，切换过程引起的控制参数波动应不超过正常范围的±5%。

8.2　数据性能

系统数据性能应满足以下要求：
a)　数据采集准确率应不低于 98%；
b)　控制网数据传输时延应不超过 50 ms；
c)　管理网数据传输时延应不超过 200 ms；
d)　数据完整性应不低于 99.99%；
e)　原始数据存储周期应不低于 3 年，报警记录、操作日志、审计日志存储周期应不低于 1 年。

8.3　可靠性

系统可靠性应满足以下要求：
a)　系统核心控制器 MTBF 应不低于 50 000 h；
b)　系统年可用率应不低于 99.9%；
c)　核心控制系统故障恢复时间应不超过 30 min，平台系统故障恢复时间应不超过 2 h；

d) 设备冗余切换时间应不超过 500 ms，切换无扰动；
e) UPS 备用供电时间应不低于 4 h。

8.4 实时性

系统实时性应满足以下要求：
a) SCADA 画面刷新时间应不超过 1 s；
b) 报警响应时间应不超过 2 s；
c) 控制指令执行响应时间应不超过 1 s。

8.5 智慧化性能

系统智慧化性能应满足以下要求：
a) 出水水质 24 h 预测准确率应不低于 95%；
b) 设备故障预警准确率应不低于 90%；
c) 曝气系统优化节能率应不低于 10%；
d) 综合药耗降低率应不低于 8%。

9 安全要求

9.1 硬件安全要求

9.1.1 系统核心设备应采用双路独立电源供电，配套 UPS 不间断电源，满足系统故障时执行安全停机程序及数据保存的需求。
9.1.2 系统应设置独立的保护接地、工作接地、防雷接地，共用接地体时接地电阻不大于 4 Ω，单独设置接地体时保护接地电阻不大于 4 Ω，防雷接地电阻不大于 10 Ω。所有现场设备、控制柜、仪表均应可靠接地，接地线路径清晰，标识明确。
9.1.3 所有硬件设备的安全防护应符合 GB/T 28742 要求，容器设备应符合 GB/T 28743 要求。

9.2 软件安全要求

9.2.1 软件应具备完善的身份认证功能，支持账号密码、USB Key、数字证书等多因素认证，具备账号锁定、密码定期更换提醒功能。
9.2.2 软件应具备防篡改功能，核心程序、控制逻辑、报警记录、操作日志应具备防篡改保护，未经授权不得修改。
9.2.3 软件应具备完善的备份与恢复功能，支持定时自动备份与手动备份，备份数据应异地存储，系统故障时可快速恢复，数据恢复时间不超过 2 h。
9.2.4 软件应具备版本管理功能，所有程序、模型、配置文件的修改均应记录版本信息，具备版本回滚功能。

9.3 网络安全要求

9.3.1 系统网络安全应符合 GB/T 22239 的相关要求，工业控制系统信息安全防护符合 GB/T 30976.2 的要求，构建边界防护、区域隔离、终端加固、数据安全、审计追溯的全链路安全防护体系。
9.3.2 应部署防火墙、入侵检测/防御系统，实现访问控制、入侵检测、恶意代码防护。跨区域数据传输应进行身份认证与加密，未经授权的访问与数据传输应被拦截并报警。
9.3.3 所有工控终端、服务器应进行安全加固，关闭不必要的端口与服务，定期更新病毒库与安全补丁。
9.3.4 应建立统一的身份认证体系，采用最小权限原则分配访问权限，严禁越权访问与操作。部署安全审计系统，对网络访问、系统操作、设备控制、数据传输、报警事件进行全流程审计，审计日志不可篡改，定期开展安全审计分析，发现安全隐患及时处置。
9.3.5 应建立数据全生命周期安全管理体系，敏感数据加密存储与传输，个人信息数据脱敏处理。核心数据应定期备份，异地存储，具备数据容灾与恢复能力。
9.3.6 应制定网络安全应急预案，覆盖网络攻击、病毒感染、系统瘫痪、数据泄露等典型安全事件，

定期开展应急演练。建立常态化安全运维机制，定期开展漏洞扫描、渗透测试、风险评估，及时修复安全漏洞。

10 运行维护要求

10.1 运行管理

10.1.1 应建立日常巡检制度，每 12 h 对系统核心设备运行状态、仪表数据、报警信息进行巡检，及时处置异常情况，巡检记录完整存档。

10.1.2 应制定设备故障专项应急预案，明确处置流程与责任分工，定期开展应急演练，保障设备与工艺系统安全。

10.2 维护保养

10.2.1 应建立系统全生命周期维护保养制度，明确日常清洁、定期紧固润滑、功能测试、数据备份、安全补丁更新等内容与周期。

10.2.2 应定期开展监测仪表计量校准，校准周期每年不少于 1 次，关键仪表每 6 个月不少于 1 次。校准应由具备资质的机构或人员执行，不合格仪表应及时维修或更换。

10.2.3 应基于设备状态监测数据与故障预警信息，对核心设备开展预测性维护，提前处置隐患，降低故障停机风险。

10.2.4 应建立设备故障闭环处置机制，故障发生后及时响应、快速定位、修复处置，形成包含原因分析与预防措施的故障处置报告。

10.2.5 应建立备品备件管理制度，针对核心控制器、关键仪表、易损执行机构等储备足量备件，明确库存定额与出入库管理要求，保障故障维修及时性。

10.3 档案管理

应建立设备档案管理制度，对设备采购、安装调试、校准报告、维护记录、升级改造等技术资料统一归档。档案应采用纸质与电子版双备份保存，保存期限不少于设备使用寿命。