ICS 35.020
CCS M 10

团　　体　　标　　准

T/SZWSS 001—2025
T/SZSSIA 018—2025

深圳市水务基础设施工业控制系统网络安全技术规范

Technical specifications for network security of industrial control systems in Shenzhen's water infrastructure

2025-07-25 发布　　2025-08-01 实施

深圳市水务学会
深圳市智慧安防行业协会　　联合发布

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。

本文件由深圳市水务学会和深圳市智慧安防行业协会联合提出并归口。

本文件起草单位：深圳市智慧水务综合指挥调度和保障中心、深圳市水务科技发展有限公司、北京天融信网络安全技术有限公司、浙江大华技术股份有限公司、中国移动通信集团广东有限公司、北京启明星辰信息安全技术有限公司、杭州海康威视数字技术股份有限公司、深圳市广汇源环境水务有限公司、东深智水科技（深圳）股份有限公司、广东粤海水务股份有限公司、深圳市科荣软件股份有限公司、深圳市浩瑞泰科技有限公司、深圳市水务工程检测有限公司、中建四局安装工程有限公司、深圳市诚业通信技术有限公司、深圳市千里马安防软件工程有限公司、深圳市宇航光通科技有限公司、深圳市中安测标准技术有限公司、深圳市智联安防创新研究院。

本文件主要起草人：张涛、李金锋、曾庆彬、宋锐、张毅、朱威达、苏腾飞、田晓扬、白彦茹、唐芳艳、刘泽浩、王旭东、李炳舜、刘晓丹、杨宗国、陈正、彭龙、田旭、张宗坤、欧阳可萃、林若驹、彭木站、勾书贵、杨涛、张鹏、刘勇飞、陈尔烽、孟鹤、张立全、李锋、涂诚、杨春军、罗海超、马卫平、张万仓、吴金平、林淑娟、董丽丽、李婉娜、卢烜、黄光宗、赵宇芬。

深圳市水务基础设施工业控制系统网络安全技术规范

1 范围

本文件规定了深圳市水务基础设施工业控制系统（以下简称“深圳水务工控系统”）网络安全防护的安全防护对象、安全要求分级和安全防护要求。

本文件适用于深圳水务工控系统网络安全防护体系的设计、建设和运行维护工作。

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 22240 信息安全技术 网络安全等级保护定级指南
GB/T 25058 信息安全技术 网络安全等级保护实施指南
GB/T 25069 信息安全技术 术语
GB/T 28448 信息安全技术 网络安全等级保护测评要求
GB/T 36323 信息安全技术 工业控制系统安全管理基本要求
GB/T 36466 信息安全技术 工业控制系统风险评估实施指南

3 术语和定义

GB/T 22240、GB/T 25058、GB/T 25069、GB/T 28448、GB/T 36323、GB/T 36466 界定的以及下列术语和定义适用于本文件。

3.1

水务基础设施 water infrastructure

在供水生产、给水加压泵站、水质净化、排水防涝及污水泵站、引水输水工程泵站及水库、水库大坝、水闸、污泥厂、调蓄设施、堤防、闸坝、河道、临时水环境治理等水务业务中，对设备、设施进行自动控制的硬件和软件的集合。

3.2

工业控制系统 industrial control systems

由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统，包括SCADA、DCS、PLC等。

[来源：GB/T 37980—2019，3.1，有修改]

3.3

信息资源层 information resource layer

为组织决策层及员工提供决策运行手段，包括信息资源相关的财务、资产、人力等管理系统。

3.4

生产管理层 production management layer

用于对生产过程进行管理的功能层，如运行管理、调度管理等。

3.5

过程控制层 process monitoring layer

对工控系统进行组态、监控和管理的功能层，实现生产过程中的高级控制、故障诊断、质量评估等。

3.6

现场控制层 field control layer

对过程控制层（3.5）与现场设备层（3.7）之间的数据进行转换与处理的功能层，实现反馈控制、逻辑控制、顺序控制和批量控制等。

3.7

现场设备层 field device layer

执行现场控制层（3.6）设备发送的采集和控制命令的功能层，实现生产作业。

3.8

工业主机 industrial host

工业生产控制各业务环节涉及组态、工作流程和工艺管理、状态监控、运行数据采集以及重要信息存储等工作的设备。

注：工业主机包括工程师站、操作员站、服务器等。

[来源：GB/T 41400—2022，3.10]

3.9

主站 central station

水务生产管理单位的集中监控与管理中心，对生产管理单位各个系统子站（3.10）做控制与监控，也称中控室。独立的中控室包含SCADA主机、相关操作显示设备，以及辅助信息系统（如历史数据库）。

注：水务生产管理单位通常使用一个或多个中控室来监督或协调其操作。

3.10

子站 sub station

通信过程中数据提供端，即控制系统中的PLC、远程终端单元（RTU）和智能电子设备（IED），负责本地工控设备的监视和控制操作，通过通信网络（有线或无线）连接到主站（3.9）。

4 缩略语

下列缩略语适用于本文件。

PLC：可编程逻辑控制器（Programmable Logic Controller）

DCS：分布式控制系统（Distributed Control System）

SCADA：监控和数据采集系统（Supervisory Control and Data Acquisition system）

VPN：虚拟专用网（Virtual Private Network）

5 安全防护对象

本文件以深圳水务工控系统为安全防护对象，防护范围包括供水生产、给水加压泵站、水质净化、排水防涝及污水泵站、引水输水工程泵站及水库、水库大坝、水闸、污泥厂、调蓄设施、堤防、闸坝、河道、临时水环境治理等工控系统，深圳水务工控系统内容参见附录 A。

6 安全要求分级

根据深圳水务工控系统受到破坏后，可能对业务用户的合法权益、社会秩序和公共利益甚至国家安全产生影响的程度，深圳水务工控系统可分为一般重要工控系统和特别重要工控系统两种类型，并应符合表1的规定。

注：业务用户包括市民和企事业单位等组织。

表 1 深圳水务工控系统类型

序号	工控系统	影响程度	系统类型
1	水质净化工控系统	工控系统受到破坏后： a) 会对业务用户的合法权益造成严重损害或特别严重损害； b) 会对社会秩序和公共利益造成危害，但不会危害国家安全	一般重要工控系统
2	排水防涝及污水泵站、引水输水工程泵站工控系统		

表 1　深圳水务工控系统类型（续）

序号	工控系统	影响程度	系统类型
3	水库、水库大坝、水闸、污泥厂、调蓄设施、堤防、闸坝、河道、临时水环境治理	工控系统受到破坏后： a）　会对业务用户的合法权益造成严重损害或特别严重损害； b）　会对社会秩序和公共利益造成危害，但不会危害国家安全	一般重要工控系统
4	供水生产工控系统	工控系统受到破坏后： a）　会对社会秩序和公共利益造成严重危害； b）　会对国家安全造成危害	特别重要工控系统
5	给水加压泵站工控系统		

7　安全防护要求

7.1　通用要求

7.1.1　物理环境安全要求

物理环境满足以下安全要求：

a）　机房场地选址时，应避开发生火灾危险程度高的区域；
b）　机房应配置电池柜或 UPS，满足设备在断电后一定时间内正常运行要求；
c）　机房应位于具有防震、防风和防雨能力的建筑物内；
d）　机房宜设置在建筑物中间楼层；
e）　应将室外控制设备安装在采用金属材料制作且具有防盗能力的箱体或装置中；
f）　室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；
g）　机房出入口应配置电子门禁系统、视频监控系统；
h）　应采用防火材料封堵机房、现场机柜室的孔、洞。

7.1.2　通信网络安全要求

7.1.2.1　网络架构

网络架构满足以下安全要求：

a）　深圳水务工控系统应单独划分网络区域，并应与其他系统位于不同的网络区域；
b）　应根据深圳水务工控系统区域重要性和业务需求进行安全区域划分，系统不同层次之间、同一层次不同业务单元之间应划分为不同的安全区域，安全域划分见附录 B。

7.1.2.2　通信传输

通信传输满足以下安全要求：

a）　数据传输过程中安全设备不应对深圳水务工控系统的实时性产生影响；
b）　可采用校验技术或密码技术保证通信过程中数据的完整性。

7.1.3　区域边界安全要求

7.1.3.1　访问控制

访问控制满足以下安全要求：

a）　应在深圳水务工控系统与其他系统之间部署访问控制设备，配置访问控制策略；
b）　应支持常用工业协议数据包解析，阻止进出区域边界非法数据包和异常指令；
c）　禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

7.1.3.2　入侵防范

入侵防范满足以下安全要求：

a）　应能监视并识别系统边界和关键网络节点的常见攻击行为，如端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击等；

b) 应能发现针对深圳水务工控系统的入侵攻击行为，记录攻击源 IP、攻击类型、攻击目标、攻击时间等，并提供告警。

7.1.3.3 安全审计

安全审计满足以下安全要求：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖每个用户，对重要的用户操作行为和重要安全事件进行审计记录；
b) 应对远程访问的用户操作行为进行安全审计。

7.1.3.4 无线使用控制

无线使用控制满足以下安全要求：

a) 应对无线通信过程采取传输加密安全措施，实现传输报文的机密性保护；
b) 应对采用无线局域网或者广域网通信的用户（人员、软件进程或设备）提供唯一标识和鉴别。

7.1.4 计算环境安全要求

7.1.4.1 身份鉴别

身份鉴别满足以下安全要求：

a) 应对登录用户身份进行唯一标识，区分管理员、操作员等角色；
b) 宜具备双因子身份鉴别功能；
c) 当用户身份认证错误次数达到阈值时，应采取结束会话、限制非法登录次数等措施阻止认证行为。

7.1.4.2 访问控制

访问控制满足以下安全要求：

a) 应删除或禁用工业主机上多余或过期的账号，避免存在共享账号；
b) 应授予深圳水务工控系统管理用户所需的最小权限，实现管理用户的权限分离。

7.1.4.3 入侵防范

入侵防范满足以下安全要求：

a) 工业主机宜遵循最小安装的原则，仅安装与深圳水务工控系统业务相关的组件和应用程序，关闭不需要的服务、默认共享和高危端口；
b) 应能发现深圳水务工控系统中控制设备、工业主机等存在的已知漏洞，并在经过充分测试评估后，在不影响深圳水务工控系统安全稳定运行的前提下修补漏洞；如难以修复漏洞，应采取其他等效安全加固措施；
c) 应对工业主机上多余的软盘驱动、光盘驱动、USB 接口、串行口或网口等，进行关闭或者拆除，确需保留的应通过技术措施实施严格的监控管理；
d) 应对移动存储介质（包括但不限于移动硬盘、U 盘等）的接入使用进行权限管控，并明确介质的读写行为；
e) 工业主机以远程管理方式进行登录过程中，应采取信息加密的方式防止鉴别信息在网络传输过程中被窃取。

7.1.4.4 安全审计

安全审计满足以下安全要求：

a) 应对深圳水务工控系统的工业主机各系统操作日志和行为信息进行记录，避免受到未预期的删除、修改或覆盖等；
b) 留存相关日志数据不应少于 1 年。

7.1.4.5 数据安全

数据安全满足以下安全要求：

a) 可通过校验技术或密码技术保证传输过程中数据的完整性；
b) 应对工控系统生产数据、运行数据等重要数据进行备份容灾。

7.1.5 安全管理中心要求

宜每两年开展一次网络安全等级测评，对不符合要求的及时整改。

7.2 系统要求

7.2.1 一般重要工控系统安全要求

7.2.1.1 物理环境安全要求

物理环境满足以下安全要求：
a) 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内；
b) 应设置冗余或并行的电力电缆线路为计算机系统供电。

7.2.1.2 通信网络安全要求

7.2.1.2.1 网络架构

网络架构满足以下安全要求：
a) 应将深圳水务工控系统与其他系统划分为两个区域，区域间采用安全技术隔离手段；
b) 应根据系统业务特点，将深圳水务工控系统内部划分为不同的安全域，安全域之间采用技术隔离手段，安全域划分见附录 B。

7.2.1.2.2 通信传输

通信传输满足以下安全要求：
a) 对于采用远程方式对深圳水务工控系统中 SCADA、PLC 等进行控制指令或相关数据交换时，应采用 VPN、加密认证等手段实现身份认证、访问控制和数据加密传输；
b) 宜采用校验技术或密码技术保证通信过程中数据的完整性。

7.2.1.3 区域边界安全要求

7.2.1.3.1 访问控制

访问控制满足以下安全要求：
a) 应对来自外部的访问源地址、目的地址、源端口、目的端口和协议等检查后，以允许或拒绝数据包出入；
b) 应支持对工业协议功能码、数据类型、值域等深度解析；
c) 应在深圳水务工控系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

7.2.1.3.2 入侵防范

应保证网络边界具备异常流量的识别、监控和审计机制。

7.2.1.3.3 安全审计

安全审计满足以下安全要求：
a) 应对主站、子站的网络通信关系进行访问基线建模，对非授权或越限访问进行告警；
b) 应对主站、子站之间的协议交互、通信流量等信息进行安全审计。

7.2.1.4 计算环境安全要求

7.2.1.4.1 身份鉴别

同 7.1.4.1。

7.2.1.4.2 访问控制

访问控制满足以下安全要求：

a) 仅允许主机执行已知安全程序，实时监控主机进程、服务、网络端口和外接设备状况；
b) 应及时阻止非授权应用或篡改信任应用的行为；
c) 应对工业主机关键系统文件、业务文件、注册表信息等进行安全防护，对文件和注册表的操作权限进行管控。

7.2.1.4.3 数据安全

应采用校验技术保证重要数据在传输过程中的完整性。

7.2.1.5 安全管理中心要求

同 7.1.5。

7.2.2 特别重要工控系统安全要求

7.2.2.1 物理环境安全要求

物理环境满足以下安全要求：
a) 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内；
b) 应设置冗余或并行的电力电缆线路为计算机系统供电；
c) 来访人员进入机房前应提出申请并通过审批,应记录其随身携带的设备、进出时间和工作内容,应有专人陪同并限制和监控其活动范围；

7.2.2.2 通信网络安全要求

7.2.2.2.1 网络架构

网络架构满足以下安全要求：
a) 应将深圳水务工控系统与其他系统划分为两个区域，区域间采用单向安全技术隔离手段；
b) 应根据系统业务特点，将系统内部划分为不同的安全域，安全域之间采用技术隔离手段，安全域划分见附录 B。

7.2.2.2.2 通信传输

通信传输满足以下安全要求：
a) 对于采用远程方式对深圳水务工控系统中 SCADA、PLC 等进行控制指令或相关数据交换时，应采用 VPN、加密认证等手段实现身份认证、访问控制和数据加密传输；
b) 应采用校验技术或密码技术保证通信过程中数据的完整性。

7.2.2.3 区域边界安全要求

7.2.2.3.1 访问控制

访问控制满足以下安全要求：
a) 应对来自外部的访问源地址、目的地址、源端口、目的端口和协议等检查，以允许或拒绝数据包出入；
b) 应支持对工业协议功能码、数据类型、值域等深度解析；
c) 应在深圳水务工控系统内安全域和安全域之间的边界防护机制失效时，及时进行报警；
d) 应保证边界防护设备删除多余或无效的访问控制规则，并保证访问控制规则权限最小化。

7.2.2.3.2 入侵防范

入侵防范满足以下安全要求：
a) 应保证网络边界具备异常流量的识别、监控和审计机制；
b) 应在网络边界进行安全监测,识别网络边界的入侵行为,具备入侵行为阻断能力。

7.2.2.3.3 安全审计

安全审计满足以下安全要求：

a) 应对主站、子站的网络通信关系进行访问基线建模，对非授权或越限访问进行告警；
b) 应对主站、子站之间的协议交互、通信流量等信息进行安全审计；
c) 应对审计记录定期备份，避免受到未预期的删除、修改或覆盖等；
d) 审计记录留存时间不应少于一年。

7.2.2.4 计算环境安全要求

7.2.2.4.1 身份鉴别

身份识别满足以下安全要求：
a) 应对登录用户分配账户和权限；
b) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

7.2.2.4.2 访问控制

同 7.1.4.2。

7.2.2.4.3 数据安全

数据安全满足以下要求：
a) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性；
b) 应采用密码技术保证重要数据在存储过程中的保密性。

7.2.2.5 安全管理中心要求

7.2.2.5.1 集中管控

集中管控满足以下安全要求：
a) 应集中监测深圳水务工控系统中网络设备、安全设备、服务器等运行状况；
b) 应划分单独的安全管理区，集中管理分布在网络中的安全设备；
c) 应对深圳水务工控系统中的安全设备进行统一监控及策略统一配置。

7.2.2.5.2 监测预警

监测预警满足以下安全要求：
a) 应能对深圳水务工控系统中的资产、流量、日志、设备运行状态等相关的安全数据进行整合分析，以便关联资产、脆弱性、威胁等，对深圳水务工控系统安全态势全面掌控；
b) 宜建立工业网络安全态势感知平台，平台宜具备安全信息采集、威胁感知、分析展示等功能；
c) 应能对安全风险形成工单并下发预警通知。

7.2.2.5.3 安全测评

应每年开展一次网络安全等级测评，对不符合要求的及时整改。

附 录 A
（资料性）
深圳水务工控系统

A.1 概述

深圳水务工控系统是深圳市水务信息化建设的关键构成，系统范围涉及深圳市水务信息化建设中安全保障、基础设施、应用系统等多个环节。随着深圳市水利信息化快速发展，水务基础设施及业务应用逐步建设并不断完善，主要包括供水生产、水质净化、给水加压泵站、排水防涝及污水泵站以及其他工控系统。

A.2 供水生产工控系统

供水生产工控系统负责城市饮用水的监测和控制，以及原水、饮用水水质的日常检测和管理。

A.3 给水加压泵站工控系统

给水加压泵站工控系统负责对无人值守泵站进行数据采集和传输。

A.4 水质净化工控系统

水质净化工控系统负责对排水设施（含污水处理和中水回收再利用设施等）进行监测、控制和管理。

A.5 排水防涝及污水泵站工控系统

排水防涝及污水泵站工控系统负责对易涝区排涝泵站以及污水提升泵站进行数据采集、传输和监测控制。

A.6 引水输水工程泵站工控系统

引水输水工程泵站工控系统具有抽水、提水、输水等多种功能，对水流的流量、水位等参数进行采集、传输和监测控制。

A.7 其他业务工控系统

其他业务工控系统包括水库、水库大坝、水闸、污泥厂、调蓄设施、堤防、闸坝、河道、临时水环境治理等系统，即对水资源平衡、污水处理、水位调节、水位监测、防洪调度等环节进行监测、控制和管理的自动化应用。

附 录 B
（资料性）
深圳水务工控系统层级及安全域划分

B.1 水务基础设施工控系统层级划分

深圳水务工控系统整体上可划分为五层，分别为现场设备层、现场控制层、过程控制层、生产管理层、信息资源层（部分生产管理单位可能会将部分层次进行合并），划分示意图见图B.1，划分内容如下：

a) 现场设备层，包括工艺相关的仪器仪表阀门，负责水位、压力、流量等过程参数的测量和执行控制设备的指令；
b) 现场控制层由生产管理单位中工控系统的控制设备构成，主要包括现场逻辑控制设备；
c) 过程控制层由调度中心操作员站、数据服务器等组成；
d) 生产管理层由工艺管理、制造执行等系统功能单元，用于对生产过程进行管理；
e) 信息资源层主要包括财务管理、企业资源计划等系统功能单元，用于为水务生产管理单位决策层提供决策运行手段。

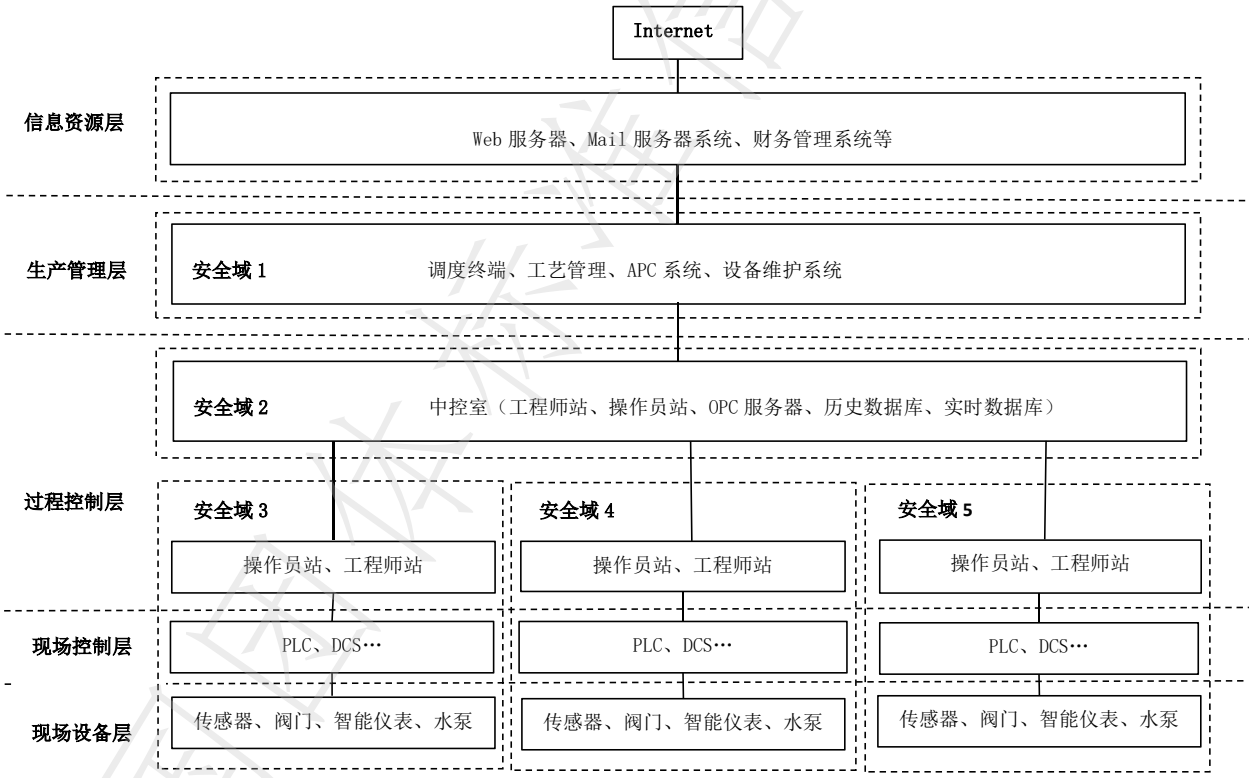

图 B.1 水务基础设施工控系统层级及安全域划分示意图

B.2 水务基础设施工控系统安全域划分

深圳水务工控系统进行安全域划分时，遵循以下原则：

a) 将具体控制区域划分为一个安全域（可根据业务子系统或网络类型再次划分为多个安全域）；
b) 对于不涉及具体控制的区域（如调度），可划分为单独的安全域；
c) 对全市的水务工控系统，按业务特点划分为不同的安全域（如供水、净水等）；
d) 具体到（某个工控系统中）指定的某个生产管理单位，满足以下要求：
   1) 工控系统拓扑为集中式，可根据业务特点的划分，将该生产管理单位工控系统划分为一个或多个安全域；
   2) 工控系统拓扑为非集中式，根据控制区域，将该生产管理单位工控系统划分为多个安全域。

注：涉及到控制过程的安全域重要程度较高，IT及调度相关安全域重要程度相对较低。

B.3 集中式和非集中式工控系统

水务行业不同区域和不同业务子系统，根据国家监管部门和业务主管部门要求，以及子系统的重要程度、子系统特点、行业发展趋势等因素，可分为集中式和非集中式，见表B.1。

表 B.1 工控系统集中式控制与非集中式控制的区别

序号	内容	集中式控制	非集中式控制
1	网络拓扑	一个中控室，通过一个交换机连接所有 PLC	各个子站的主机和 PLC 接到一个交换机上，多个子站交换机连到中控室
2	控制模式	通常由中控室实现对工控系统的集中监测和控制功能，应急状态时可以在现场控制	通常由子站内的工业主机进行现场控制，中控室仅实现监测功能，不直接进行控制
3	安全域划分	可将整个工控系统划分为一个安全域	每个子站可以划分为一个安全域；中控室单独划分为一个安全域；（如果对业务有影响，也可将全厂划分为一个安全域）

B.4 水务基础设施工控系统有人值守站工控系统层级及安全域划分

在安全域划分时，考虑系统功能差异及资产地理位置等因素，根据安全防护需求，生产管理单位网络系统可分为多个安全域，见图B.1，并满足以下要求：

a) 将生产管理层单独划分为安全域 1，该区资产包括各类生产管理系统及主机和服务器；
b) 将过程控制层的集中过程控制部分划分为安全域 2，该区资产包括各类过程控制系统与设备；
c) 考虑具体的业务子站系统，以及不同的工控设备和控制对象因素，可将包含不同被控装置的过程控制层、现场控制层及现场设备层划分为不同的安全域 3、安全域 4.....安全域 n；以安全域 3 为例，该安全域覆盖了 3 个功能层，包含了过程控制层的操作员站和相关设备、现场控制层的工控系统设备（PLC、SCADA 等）和现场设备层的工业设备（传感器、水泵、阀门等）；
d) 明确各安全域的区域边界，采用隔离技术对安全域进行隔离。

B.5 水务基础设施工控系统无人值守站工控系统层级及安全域划分

B.5.1 无人值守站工控系统划分为三层，分别为现场设备层、现场控制层、数据采集层，划分示意图见图B.2，划分内容如下：

a) 第一层为现场设备层，包括各种传感器、阀门以及水泵等；
b) 第二层为现场控制层，包括可编程控制器 PLC、HMI，提供上传数据接口，并将重要数据直接上传至中控室；
c) 第三层为数据采集层（对应过程控制层和生产管理层），包括数据采集服务器，展示屏幕，历史数据服务器等。

注：对于无人值守站，管理人员在中控室即可远程监测水池水位或进站压力、加压泵组工作状态、出站流量、出站压力等，但不对系统做任何控制。对系统的控制操作（如泵站的启停控制等），需要运维人员根据具体情况，在设备现场通过现场操作员站进行操作。因此，水务基础设施工控系统无人值守站与有人值守站层次及安全域划分有所不同。

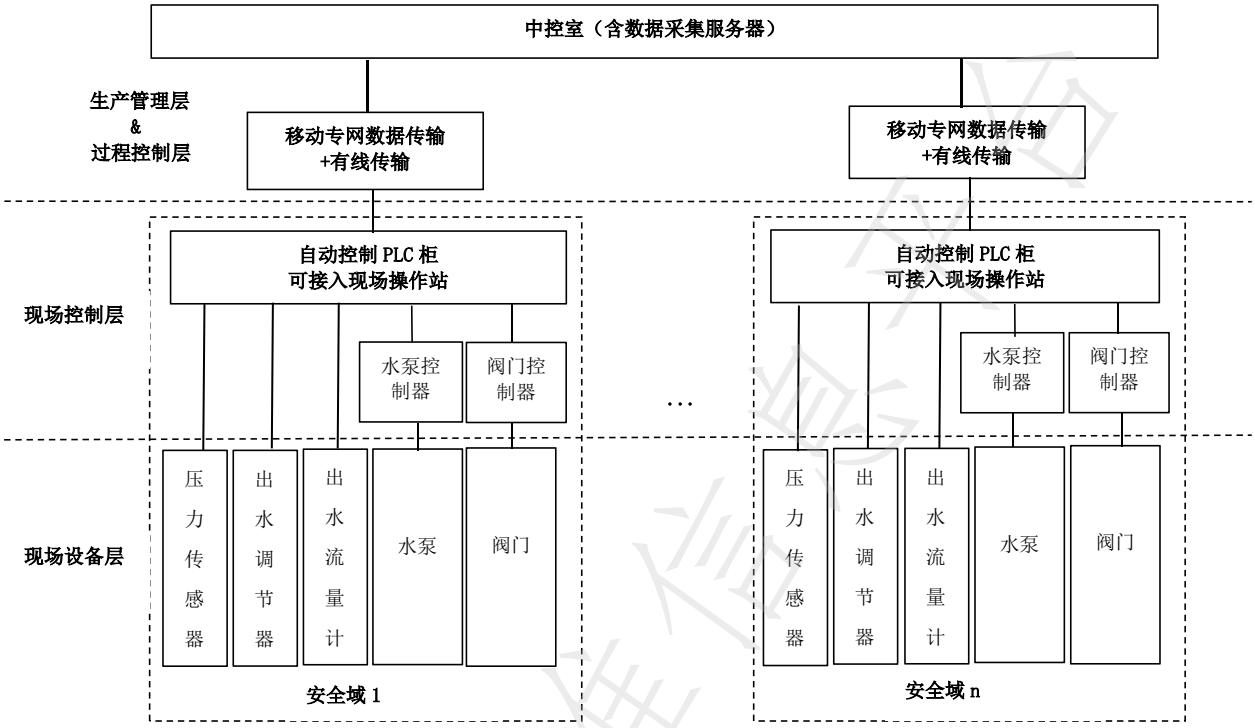

图 B.2　无人值守站工控系统层级及安全域划分示意图

B.5.2　在进行安全域划分时，可根据实际业务，将具体某一系统现场控制层的PLC，以及现场设备划分为一个安全域。

B.6　其他情况说明

其他情况说明内容如下：

a)　基于网络成本、业务备份保护或业务扩容需求等考虑，水务基础设施工控系统可采用星型网络、环形网络或双星型网络等组网方式。这些组网方式，对工控系统的层次和安全区域划分没有影响；

b)　工控系统可采用光纤或其他有线网络，也可根据业务需要采用无线网络连接。

参 考 文 献

[1] IEC 62264—1：2013 EN/FR 企业控制系统集成 第 1 部分：模型和术语
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 39204 信息安全技术 关键信息基础设施安全保护要求
[4] GB/T 37980—2019 信息安全技术 工业控制统安全检查指南
[5] GB/T 39786—2021 信息安全技术信息系统密码应用基本要求
[6] GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型
[7] SL/T 803—2020 水利网络安全保护技术规范